



ESPAÑA (SPAIN) : Trusted List

Tsl Id: TSL20260520

Valid until nextUpdate value: 2026-11-16T04:00:00Z

TSL signed on: 2026-05-20T07:52:18Z

TSL Scheme Information

TSL Id	<i>TSL20260520</i>
TSLTag	<i>http://uri.etsi.org/19612/TSLTag</i>
TSL Version Identifier	<i>6</i>
TSL Sequence Number	<i>186</i>
TSL Type	<i>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric</i>

Scheme Operator Name

Name	<i>[es]</i>	<i>MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION DIGITAL</i>
Name	<i>[en]</i>	<i>MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION</i>

PostalAddress

Street Address	<i>[en]</i>	<i>Poeta Joan Maragall, 41</i>
Locality	<i>[en]</i>	<i>Madrid</i>
State Or Province	<i>[en]</i>	<i>Madrid</i>
Postal Code	<i>[en]</i>	<i>28020</i>
Country Name	<i>[en]</i>	<i>ES</i>

PostalAddress

Street Address	<i>[es]</i>	<i>Poeta Joan Maragall, 41</i>
Locality	<i>[es]</i>	<i>Madrid</i>
State Or Province	<i>[es]</i>	<i>Madrid</i>
Postal Code	<i>[es]</i>	<i>28020</i>
Country Name	<i>[es]</i>	<i>ES</i>

ElectronicAddress

URI	<i>[en]</i>	<i>https://avance.digital.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx</i>
URI	<i>[en]</i>	<i>mailto:sgsd@economia.gob.es</i>

Scheme Name

Name [en] *ES:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

Name [es] *ES:Lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados que supervisa el Estado miembro de expedición, junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.*

Scheme Information URI

URI [es] <https://avance.digital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI.aspx>

URI [en] <https://avance.digital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI.aspx>

Status Determination Approach <http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate>

Scheme Type Community Rules

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/ES>

Scheme Territory ES

Policy Or Legal Notice

TSL Legal Notice [en] *The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

TSL Legal Notice [es] *El marco jurídico aplicable a la presente lista de confianza es el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.*

Historical Information Period 65535

Pointer to other TSL - EUROPEAN UNION

1.EU TSL - MimeType: application/vnd.etsi.tsl+xml

TSL Location <https://ec.europa.eu/tools/lotl/eu-lotl.xml>

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	3
Serial Number:	566117616430214055757992355472683005220982589151
X509 Certificate	-----BEGIN CERTIFICATE----- MIIH9DCCBdygAwIBAgIUUymXhngntZgl4PHVh4juzinh8wDOYIKoZlhvcNAQENBQAwXzELMAkG A1UEBhMCUqFkxJAoBgNVBAAwMURpZ2l0YWVxYTAuWduElicnRkZmijYWRvcmeGRGlnaXRhdDEKMCIG A1UEAwwREHRSVpRBTjWR0qUUVyRTEiCSUVEEENBIE-cvMBADTjOMQOYjNjeykDkyMoXDTj3MDQy NjEyNDkyMlowggFKMQswCQYDVQOGEWJHUjE9MDQGA1UECww0O2YvdGlnaWNhdGlGUHJvZm5lZSAt IF1YWxpZmluZCBkZjX0awZpZjZ0ZSAHE1bWVlcjEjMCEGA1UEYQw1EjVJWecmJMU001AWWKSZ QTFCTFVRQVJlZmVhZDaaBgNVBAAwMEduVUk5b0RUPjE0NTQ4KTAnBgNVBAskMEYudG10 bGVZcW50Q2RlRmUgU1RBRVlUTjZlFNUOUZCS0wKwYKozIhvcNAQkBFh5hcG9zdG95b3MuYXK8 YWRhc0B1Y3idjKvcGZuZkUeDAQBgNVBAAQOM80F0TEFFOVMeJAQBgNVBACmCUFOTj1NUT0xPzEd M8sGA1UECwwUUmVhZ3RlUW50RE1hmFrCZW1bmQxQSA9BgNVBAMMEUFTj1NUT0xPzYjBBUEX8BREFT MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCCQAQEA5La9o3bz0LdR1R01Mhtrd6BLKxak Jxlgpic11hh1BR3uYGVzVwfsrmjQeI/RkbjMoNzakjo40vPhUjB90J7TJLgwZ5ghkPz0+vcg4yvc Lod4QnGcTEsh5f5Z2gwPzKXevl0234QRCw74jsk47wd7Yv4x1kvs1T0ds08ZF8kmzUj 7abdzisH3/uR+JHkhhbljm+MspETNN+Nva7dunh214lHlEjnyTEPQAdsgz+cRk8yLQ1YYS6I R3pif8MvXzh7WmjY9AZPd3C0BSZ0v05KB6RyOk+6MREWY9auZ2KQ0anyrCns5NjU5S58T WwPpQ0DQQA84kU7CCArtUwDA1YVRDTAQHBAIwDA8BgNVHSMGEGAwbBz5FAHBE0ej0flov zVxnlxpFDChgYKwYBBQJHAQEegB4MEYGCCSGAQAUF8ZChjpdhRwczoVl3fjY51nMS5kaWdp dGfSc2lnb5wdC9ESUdjVEFMU0JH1fVQJXKjFRENBRZcUdM4GCcSGAQAUF8ZABhjdHw czovL3fjY51nMS5kaWdpdGfSc2lnb5wdC9v3WwMCSGA1UEQOMCBHmfwb3N0L2vcy5hcGxh ZGF0QGVLMvY1cm9wY35ldTBF8gNVHSAEWDBMWDCGcysGAQAQBg9cd8BAEBMCGwJkYKwYBBQJHAQEW Gmhd0Hbz0l8vgtpLmRpZ2l0YWVxZWduLnB0MBAGDSGAQAQBg9cd8BAIBAQAEEAMK8BwOA+xAAQW H0YDVR0BBWf4YKwYBBQJHAwGCGcSGAQAUF8wMEMesGA1UdhwREMEWOKA+oDyC0mhd8Bz0Bv cWNLHlWcXlMmRpZ2l0YWVxZWduLnB0L0RlR0lUOUxTSUd0UUVBTEIGSUVUeQ0FHMS5jcmwWH0YDVR00 BBYEFHgmw4edYtE2rtYu+8+Up7LgWYcMA4GA1UdDwEibWQEAwIGQ0CB0wYKwYBBQJHAQMegc1w gcMwCA1YGB4C0RgEBWAgBg9QkAYBDA7B97E4U5GAQYwC0YHBAQ0RgE47B97E4U5GAQYwDxU FihodHRwczoVl3fjY51nMS5kaWdpdGfSc2lnb5wdC9ORFNKcH0ucGRmEwJwD0AUFihodHRwczoV L3fjY51nMS5kaWdpdGfSc2lnb5wdC9ORFNZVW4ucGRmEwJdAV8gRgBGF0CLAJAjbGcCAIvS S0EBMUCcSGAQAUF8wCMAK8BwOA+vj0WwDOYIKoZlhvcNAQENBQADopIBALU37pY7W5ZwRxB B5pGTGTC+XcWytkuyvRjVU+hVDSyVCZE+4+EPB2mRuzkEe2M3jMpdzwaNHe2YU9jCkoUFD7V LIdiRG00MnXde2BAQNIvA0S8LwR3DNATs1rPb0X073WCNq0wUllgLLCFXHHpzsK2ym12+h Yq4A8aR2jdn2vX051fT5hzbzVamM6+41LKmo5R5Gc869slSS35BmWm3LaJQJ0IT hW5K0wIXBP/PA+sQDYp9gHur1nLUWUg60B8foYwMOTmYlcupR80ZxtfUJ1WSZEpdlXZk0dWVDN jj8p0RF0B5i7DdpfS57p8KcndD0vQkYCapRFLKj69gKVK6B6OKHfOCtmA6CLapW89+JPC nrywN68p+MNqez2lV8icbJUE+kw6PHCR64MwmmHfCe6BB9oTKSWWWClZhsygdJ0+5J DS63b0F0dnZUV2qhlZIVOROC0jCw57kYS8vWAgB6ccAhYNaaUhl1mKGqo2ip0o5HhG5VfN Rc+CyIMNDUGAHp9fAD93u6jQcJdsZKraWZA6tmddp0b71R6HfRbs/QzeA4R7ChMM0FXD Zfpz6kEYpbLU0sh79fmoNRxmCqKMcKpQil0lg6dKLUVYCl0q08zk
Signature algorithm:	SHA512withRSA
Issuer CN:	DIGITALSIGN QUALIFIED CA G1
Issuer O:	DigitalSign Certificadora Digital
Issuer C:	PT
Subject CN:	APOSTOLOS APLADAS
Subject OU:	RemoteQSCDManagement
Subject GIVEN NAME:	APOSTOLOS
Subject SURNAME:	APLADAS
Subject E:	apostolos.apladas@ec.europa.eu
Subject OU:	Entitlement - EC STATUTORY STAFF
Subject O:	EUROPEAN COMMISSION
Subject 2.5.4.97:	LEIXG-254900ZNYA1FLUQ9U393
Subject OU:	Certificate Profile - Qualified Certificate - Member
Subject C:	GR
Valid from:	Fri Apr 26 14:49:22 CEST 2024

Valid to:	<i>Mon Apr 26 14:49:22 CEST 2027</i>
Public Key:	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:80:82:DA:F6:8D:D8:83:3D:25:FD:D4:75:47:4D:4C:84:8B:6B:77:A0:4B:93:16:A4:27:19:6A:A6:79:5C:D6:18:53:F1:1D:EE:60:68:D2:57:07:EC:9A:34:1E:8B:F6:24:6E:33:28:37:36:A4:8E:8E:2F:A0:F8:54:20:90:5A:F7:4E:D3:24:B1:80:65:28:21:7E:4A:74:FA:F7:20:E9:27:82:2E:87:40:41:AB:46:EE:21:2C:87:91:6B:E6:E6:60:C0:FA:4B:5C:4C:62:97:4D:B7:E1:04:5C:C3:B9:09:80:8E:24:EF:07:7B:62:F5:C0:8F:59:2F:E7:32:D3:16:8E:AC:3A:BF:19:17:D9:26:DA:85:35:EE:06:DD:66:2B:08:1F:7F:EE:47:E2:47:92:48:5B:96:39:BE:32:CA:44:4C:D3:7E:36:F6:8B:76:E8:64:CF:5E:25:96:1F:C4:26:BC:93:10:F4:0B:01:D8:20:CF:E7:11:90:19:32:2D:0D:58:61:2E:A2:47:7A:62:7E:8B:0C:8D:7C:C7:62:5C:09:63:D0:33:3C:D7:77:73:40:52:D8:EB:F4:E6:40:7A:85:1C:8E:91:AF:BA:31:11:16:63:D6:94:D8:62:BF:43:46:A7:CA:83:42:9E:CE:4D:FD:45:EC:E7:CF:53:C2:B5:A9:D1:02:03:01:00:01</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14</i>
Authority Info Access	<i>https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b</i> <i>https://qca-g1.digitalsign.pt/ocsp</i>
Subject Alternative Name	<i>apostolos.apladas@ec.europa.eu</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.25596.4.1.1</i> <i>CPS pointer: https://pki.digitalsign.pt</i> <i>Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4</i> <i>Policy OID: 0.4.0.194112.1.2</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
CRL Distribution Points	<i>https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl</i>
Subject Key Identifier	<i>71:BF:9B:0E:1E:75:8F:ED:4F:3A:D8:BB:EF:3E:52:9E:CB:81:6C:86</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_QcSSCD</i>
Key Usage:	<i>nonRepudiation</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>B6:3D:41:67:44:E7:09:8B:F9:EC:2C:AA:59:6A:93:BC:24:68:E3:7F:82:84:BA:65:E C:C0:61:71:1B:CB:AA:18</i>

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	<i>3</i>
Serial Number:	<i>416260670660158992857603279521251626757860879766</i>

TSL Scheme Operator certificate fields details

Version: 3

Serial Number: 21267647932559404339035760224263512027

X509 Certificate

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer SERIAL NUMBER: 201803

Issuer CN: *Citizen CA*
Issuer O: *Certipost N.V./S.A.*
Issuer L: *Brussels*
Issuer C: *BE*
Subject SERIAL NUMBER: *72020329970*
Subject GIVEN NAME: *Patrick Jean*
Subject SURNAME: *Kremer*
Subject CN: *Patrick Kremer (Signature)*
Subject C: *BE*
Valid from: *Sat Jun 02 00:04:19 CEST 2018*
Valid to: *Wed May 31 01:59:59 CEST 2028*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AF:88:3B:56:88:83:63:86:AC:DD:1E:0B:3C:E8:3B:B8:F1:F9:8A:71:F3:69:53:0E:C0:56:FF:F1:83:96:F8:02:15:30:7C:FF:57:97:49:03:37:93:2A:F8:4B:1B:94:B8:3E:4E:8A:77:61:3E:87:5F:05:95:1A:27:A7:BD:06:BF:6F:A2:8E:D9:0F:93:86:50:91:F7:83:D3:27:2E:01:B2:D7:88:DC:76:4B:87:DC:E4:61:BD:2C:62:5A:7C:32:60:06:04:D0:B9:09:B5:68:35:4B:0D:0E:B9:DE:6A:91:E6:D0:0E:FA:01:1F:EA:F8:3B:CD:11:12:2F:73:24:61:70:14:AB:E4:BF:5A:87:04:68:6A:48:85:E3:55:00:5D:E2:3D:29:2F:11:ED:CB:BD:48:C5:FF:15:C7:58:5E:1A:32:FA:86:2B:A9:17:1A:C7:9A:4D:C9:FD:86:04:DB:71:E8:96:D8:F0:22:12:BF:9E:0D:33:5C:CE:4C:06:04:31:57:C3:39:A7:18:53:CC:45:EC:F7:3B:D9:3F:8C:82:A1:85:AF:13:CA:50:D2:7C:8F:CC:5F:73:83:B7:47:54:DE:3B:C9:10:A3:C8:7D:42:62:C4:13:DE:87:13:09:33:05:B1:4E:31:5B:36:EF:C2:2B:BB:49:F2:A4:F6:8B:54:B8:55:02:03:01:00:01*
Authority Key Identifier *D9:34:21:3E:3A:42:25:6D:E1:BB:BF:BE:47:4C:F8:02:AD:E3:2F:54*
Authority Info Access *http://certs.eid.belgium.be/citizen201803.crt*
http://ocsp.eid.belgium.be/2
Certificate Policies *Policy OID: 2.16.56.12.1.1.2.1*
CPS pointer: http://repository.eid.belgium.be
CPS text: [Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage soumis à des limitations de responsabilité, voir CPS - Verwendung unterliegt Haftungsbeschränkungen, gemäss CPS]
Policy OID: 0.4.0.194112.1.2
CRL Distribution Points *http://crl.eid.belgium.be/aidc201803.crl*
Extended Key Usage *id_kp_emailProtection*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_QcSSCD
Key Usage: *nonRepudiation*
Thumbprint algorithm: *SHA-256*
Thumbprint: *D2:06:4F:DD:70:F6:98:2D:CC:51:6B:86:D9:D5:C5:6A:EA:93:94:17:C6:24:B2:E4:78:C0:B2:9D:E5:4F:84:74*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: 3

Serial Number: 660862747298009142807362633871991440505734410485

X509 Certificate

[illegible][illegible][illegible]

TSL Scheme Operator certificate fields details

Version:	3
Serial Number:	643978552848424008220551052528366836395685220683
X509 Certificate	-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Signature algorithm:	<i>SHA512withRSA</i>
Issuer CN:	<i>DIGITALSIGN QUALIFIED CA G1</i>
Issuer O:	<i>DigitalSign Certificadora Digital</i>
Issuer C:	<i>PT</i>
Subject CN:	<i>IOANNA KALOGEROPOULOU</i>
Subject OU:	<i>RemoteQSCDManagement</i>
Subject GIVEN NAME:	<i>IOANNA</i>
Subject SURNAME:	<i>KALOGEROPOULOU</i>
Subject E:	<i>Ioanna.KALOGEROPOULOU@ec.europa.eu</i>
Subject OU:	<i>Entitlement - EC STATUTORY STAFF</i>
Subject O:	<i>EUROPEAN COMMISSION</i>
Subject 2.5.4.97:	<i>LEIXG-254900ZNYA1FLUQ9U393</i>
Subject OU:	<i>Certificate Profile - Qualified Certificate - Member</i>
Subject C:	<i>GR</i>
Valid from:	<i>Mon Nov 24 10:56:41 CET 2025</i>
Valid to:	<i>Fri Nov 23 10:56:41 CET 2029</i>
Public Key:	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:08:E6:B5:E9:AB:A4:69:4F:B2:80:8C:D6:D5:5F:54:80:98:88:22:84:78:8A:1D:6F:2E:A7:28:4D:0A:7E:44:8C:28:08:04:A2:EF:8E:66:32:79:07:CE:55:98:40:8B:8B:CF:30:44:01:85:0D:4A:FA:93:EE:D2:7A:DC:FD:13:FA:98:74:58:73:FF:71:89:C3:5D:17:80:48:91:73:07:73:69:FB:CA:33:D0:EB:5C:51:64:19:84:6A:29:29:09:EB:BF:EC:2A:AD:49:28:4E:DB:0A:46:CC:67:F0:7C:48:34:54:27:6B:DE:4A:84:52:FE:80:89:1A:1B:9F:6A:B0:19:3B:15:D4:C2:BC:DB:EF:6D:C1:4F:04:06:91:AA:FF:1B:46:3B:72:8D:5E:55:05:D7:EA:11:B2:E2:69:CF:17:7E:80:3E:F1:BD:E3:5A:7F:22:EA:0C:33:92:18:EB:5D:21:FC:8D:73:07:90:C5:22:00:15:12:2D:07:9E:50:A8:2D:F4:3A:A2:A2:5C:BF:4D:56:7C:62:84:22:1A:69:A1:EA:61:BA:14:84:EC:4A:90:D0:92:C8:B9:FF:33:76:E9:F2:63:F3:26:BF:3E:22:B7:68:C5:57:F4:10:7F:54:7C:ED:2B:69:2F:B0:22:70:2E:41:48:25:9F:89:7C:83:EF:02:03:01:00:01</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14</i>
Authority Info Access	<i>https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b</i> <i>https://qca-g1.digitalsign.pt/ocsp</i>
Subject Alternative Name	<i>Ioanna.KALOGEROPOULOU@ec.europa.eu</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.25596.4.1.1</i> <i>CPS pointer: https://pki.digitalsign.pt</i> <i>Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4</i> <i>Policy OID: 0.4.0.194112.1.2</i>

TSL Scheme Operator certificate fields details

[illegible]

-----END CERTIFICATE-----

SHA512withRSA

DIGITALSIGN QUALIFIED CA G1

DigitalSign Certificadora Digital

PT

EUROPEAN COMMISSION

EU-TRUST@ec.europa.eu

EUROPEAN COMMISSION

Subject 2.5.4.97:	<i>LEIXG-254900ZNYA1FLUQ9U393</i>
Subject OU:	<i>Directorate-General for Digital Services</i>
Subject OU:	<i>Certificate Profile - Qualified Certificate - Organization</i>
Subject C:	<i>LU</i>
Valid from:	<i>Wed Dec 17 15:31:54 CET 2025</i>
Valid to:	<i>Mon Dec 17 15:31:54 CET 2029</i>
Public Key:	<i>30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A2:60:BB:24:AD:7E:BC:BF:88:36:EA:BC:66:ED:85:D8:55:AA:92:32:43:7A:74:E1:5E:61:56:0C:D6:58:A1:11:9E:9E:73:37:80:14:DC:4D:65:8E:A2:83:50:58:C4:B5:4C:B3:AA:5E:9C:DF:49:ED:0C:82:52:F4:89:D8:0A:A7:7B:07:E6:15:CB:E0:1D:FD:85:E4:48:1D:52:34:D7:30:AC:A3:32:F5:68:84:FF:1C:46:07:0D:C2:80:CE:0F:23:55:DE:D3:03:6D:2C:47:55:D8:3B:3C:D8:42:D5:9C:4E:7D:8D:E7:C5:0B:5C:CD:E6:0C:7B:60:B9:48:D5:8E:37:DC:87:21:EC:AA:28:EF:0D:08:19:B8:C8:60:36:87:55:19:9B:4F:89:FE:58:36:D7:C5:07:5D:0C:91:DA:49:3D:69:88:57:16:5D:1D:3B:00:91:1E:84:B5:1D:A3:21:81:94:D5:F8:83:47:BA:00:F0:E8:64:BD:29:1D:03:46:49:82:FD:A3:42:21:39:3E:73:6A:FC:DA:EE:DD:74:07:D4:14:EF:E9:07:A0:F2:94:89:54:58:B4:F8:98:80:C3:24:78:8C:8B:70:EF:82:F5:A3:21:62:49:F1:8C:86:9E:E1:38:CA:02:55:EC:5B:20:B7:EE:EE:7C:94:BB:12:BA:7E:01:74:C0:34:7B:E6:18:00:96:BD:E1:F4:32:5C:DC:40:1A:B6:A3:57:8A:57:15:49:59:3A:D0:08:EC:67:2E:2C:7C:D2:53:2E:64:1E:F2:8D:C3:A0:5E:39:7D:1D:6E:B2:73:EC:77:4A:14:A0:7A:AB:3F:31:72:FF:05:B3:71:62:66:B6:D8:1F:F3:AF:E4:D9:A8:71:6E:70:C4:3E:08:16:04:A6:DD:9B:51:74:2B:FD:D1:E1:98:6C:58:46:81:BF:5F:BA:3F:74:93:18:02:93:DD:36:75:BE:76:4A:B9:8B:39:3A:F7:8A:EC:44:B6:23:A1:9E:E6:E2:F9:E9:9A:4D:E4:FB:E1:0E:65:23:6C:3A:24:83:A1:A1:06:5E:27:0E:DD:88:50:EE:0F:76:DD:A6:C1:F4:4D:39:05:6F:80:75:B8:C9:A2:28:02:FC:80:4D:21:D1:9B:68:62:30:81:4D:35:A3:80:60:85:05:80:D0:34:F0:92:D4:84:C9:12:3F:C9:1C:54:97:69:8D:18:EA:47:EA:90:10:E3:BD:D5:A7:21:A4:6F:72:6C:8B:1E:49:36:1F:1E:80:CD:32:13:CB:16:76:D0:7B:51:51:18:A2:2A:01:A9:F2:29:D9:2C:1F:85:7E:3D:F9:F0:51:7B:9B:4C:41:58:AB:DE:9A:30:C1:02:03:01:00:01</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14</i>
Authority Info Access	<i>https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b</i> <i>https://qca-g1.digitalsign.pt/ocsp</i>
Subject Alternative Name	<i>EU-TRUST@ec.europa.eu</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.25596.4.1.1</i> <i>CPS pointer: https://pki.digitalsign.pt</i> <i>Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6</i> <i>Policy OID: 0.4.0.194112.1.3</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_QcSSCD</i>
CRL Distribution Points	<i>https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl</i>
Subject Key Identifier	<i>87:0C:D6:49:AD:97:46:06:15:25:F2:77:C7:6C:7F:C2:D2:97:4A:05</i>
Key Usage:	<i>nonRepudiation</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>23:61:03:F0:3A:80:31:AE:8F:47:F9:05:9B:F8:DE:38:56:4C:DB:FE:BE:DD:E4:A5:97:D5:0F:89:80:AA:65:3B</i>
TSL Type	<i>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists</i>
Scheme Territory	<i>EU</i>

Mime Type*application/vnd.etsi.tsl+xml***Scheme Operator Name****Name***[en]**European Commission***Scheme Type Community Rules****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists***List Issue Date Time***2026-05-20T03:00:00Z***Next Update****date Time***2026-11-16T04:00:00Z***Distribution Points****URI***https://tsl.digital.gob.es/TSL.xml*

1 - TSP: Banco Santander, S.A.**TSP Name**

Name *[en]* *Banco Santander, S.A.*

Name *[es]* *Banco Santander, S.A.*

TSP Trade Name

Name *[en]* *VATES-A39000013*

Name *[en]* *Santander*

Name *[es]* *Santander*

Name *[en]* *Banco Santander Central Hispano, S.A. CIF: A-39000013*

Name *[en]* *Banco Santander S.A. CIF: A-39000013*

PostalAddress

Street Address *[es]* *Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*

Locality *[es]* *Boadilla del Monte*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28660*

Country Name *[es]* *ES*

PostalAddress

Street Address *[en]* *Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*

Locality *[en]* *Boadilla del Monte*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28660*

Country Name *[en]* *ES*

ElectronicAddress

URI *[en]* *http://www.gruposantander.es*

URI *[en]* *mailto:certificacion.universitaria@gruposantander.com*

Subject CN: *WG10 Qualified Identification Root CA*
Subject OU: *Direccion de Universidades*
Subject O: *Banco Santander Central Hispano, S.A. CIF: A-39000013*
Subject L: *Paseo de Pereda, 9-12*
Subject ST: *Santander - Spain*
Valid from: *Thu Nov 24 01:00:00 CET 2005*
Valid to: *Tue Nov 24 00:59:59 CET 2015*
Public Key: *30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:84:DF:D8:3E:76:FD:FC:94:D3:8D:44:2D:2C:98:E0:19:AF:2E:9E:EE:8E:19:3D:98:85:CD:F4:13:CD:90:84:4B:6A:78:C0:38:55:8C:50:88:28:97:25:9F:AE:AF:23:89:26:09:43:31:EC:51:38:7E:89:9F:A8:AB:8D:45:41:AB:D8:C9:06:77:1A:C1:F3:6D:59:8E:E9:46:6A:CE:16:19:46:E5:FB:6A:F7:1D:3B:FC:AE:07:10:11:DA:81:77:D1:D0:F2:8C:09:11:D5:03:8A:1B:64:65:AE:95:9D:FA:07:FC:16:42:3C:A0:2A:F3:97:2B:53:83:03:B8:7D:37:99:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Subject Alternative Name *CN=Private1-33*
Subject Key Identifier *20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*
Authority Key Identifier *20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *1C:F1:AE:29:72:6D:13:08:73:8F:07:B6:80:8A:89:AB:29:C5:CC:BF:F8:C4:19:D3:5C:71:D9:68:AE:3D:1B:D1*

X509SubjectName

Subject CN: *WG10 Qualified Identification Root CA*
Subject OU: *Direccion de Universidades*
Subject O: *Banco Santander Central Hispano, S.A. CIF: A-39000013*
Subject L: *Paseo de Pereda, 9-12*
Subject ST: *Santander - Spain*

Service Status

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

1.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

1.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA

Name	[en]	Qualified Certificates issued by CA WG10 Qualified Identification Root CA

Service digital identities**X509SubjectName**

Subject CN:	WG10 Qualified Identification Root CA
Subject OU:	Direccion de Universidades
Subject O:	Banco Santander Central Hispano, S.A. CIF: A-39000013
Subject L:	Paseo de Pereda, 9-12
Subject ST:	Santander - Spain

X509SKI

X509 SK I	IP/W1W8ZvuE0swpmarZPn3cRB24=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time	2015-11-24T01:00:00Z

1.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA

Name [en] *Qualified Certificates issued by CA WG10 Qualified Identification Root CA*

Service digital identities

X509SubjectName

Subject CN: *WG10 Qualified Identification Root CA*

Subject OU: *Direccion de Universidades*

Subject O: *Banco Santander Central Hispano, S.A. CIF: A-39000013*

Subject L: *Paseo de Pereda, 9-12*

Subject ST: *Santander - Spain*

X509SKI

X509 SK I *IP/W1W8ZvuE0swpmarZPn3cRB24=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-04-13T00:00:00Z*

1.2 - Service (withdrawn): Santander Digital Signature

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Santander Digital Signature*

Name [es] *Santander Digital Signature*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4828055370659501092*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CB:C6:89:C8:7A:63:FA:73:23:A7:60:7C:C7:C4:57:B3:B4:50:57:2B:EF:A4:74:70:B6:1C:35:BF:07:9B:60:0B*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2018-10-22T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

1.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

1.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Santander Digital Signature*

Name *[es]* *Santander Digital Signature*

Service digital identities

X509SubjectName

Subject CN: *Santander Digital Signature*

Subject OU: *Dirección de Universidades*

Subject O: *Banco Santander S.A. CIF: A-39000013*

Subject L: *Paseo de Pereda 9-12*

Subject ST: *Santander*

Subject C: *ES*

X509SKI

X509 SK I *S4y6oi6+9bMkvmbUTUiOvV3/v60=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

1.2.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

1.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	<i>Santander Digital Signature</i>

Name	[es]	<i>Santander Digital Signature</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>Santander Digital Signature</i>
Subject OU:	<i>Dirección de Universidades</i>
Subject O:	<i>Banco Santander S.A. CIF: A-39000013</i>
Subject L:	<i>Paseo de Pereda 9-12</i>
Subject ST:	<i>Santander</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>S4y6oi6+9bMkvmbUTUiOvV3/v60=</i>

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	<i>2016-01-24T23:00:00Z</i>

1.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2

2 - TSP: Dirección General de la Policía

TSP Name

Name [en] *Dirección General de la Policía*

Name [es] *Dirección General de la Policía*

TSP Trade Name

Name [en] *VATES-S2816015H*

Name [en] *Dirección General de la Policía*

Name [es] *Dirección General de la Policía*

Name [en] *DIRECCION GENERAL DE LA POLICIA*

PostalAddress

Street Address [es] *C/Miguel Ángel nº 5*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Postal Code [es] *28010*

Country Name [es] *ES*

PostalAddress

Street Address [en] *C/Miguel Ángel nº 5*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28010*

Country Name [en] *ES*

ElectronicAddress

URI [en] *http://www.dnielectronico.es*

URI [en] *mailto:dnielectronico@dnielectronico.es*

TSP Information URI

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	[en]		A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]		Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[en]	Qualified Certificates issued by subordinated CA under the root CA

Name	[es]	Certificados Reconocidos emitido por CAs subordinadas de la CA Root

Certificate fields details

Version: 3

Serial Number: 1093088852834654238833120296104474059

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: AC RAIZ DNIE

Issuer OU: *DNIE*

Issuer O: DIRECCION GENERAL DE LA POLICIA

Issuer C: *ES*

Subject CN: AC RAIZ DNIF

Subject OU:	DNIE
Subject O:	DIRECCION GENERAL DE LA POLICIA
Subject C:	ES
Valid from:	Thu Feb 16 11:37:25 CET 2006
Valid to:	Fri Feb 08 23:59:59 CET 2036
Public Key:	30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:00:AD:0C:C3:A3:20:07:A3:63:FF:F7:34:A0:CD:EE:6A:54:08:17:5D:B1:01:15:A7:E6:B9:5F:8A:71:FF:0C:2:1D:EA:37:F3:DE:93:7F:D6:05:4D:84:B2:D5:D7:1C:0C:F4:C4:91:70:40:0E:5A:C8:98:A4:80:E8:0D:33:CD:07:F3:B7:F5:AC:A1:38:7A:C0:66:54:24:FC:52:C C:30:F2:C3:C4:A1:2C:76:BF:C1:C0:BF:82:F1:9B:F0:68:7A:13:40:C8:97:BC:1C:25:07:08:0A:B7:96:EF:CC:29:54:E0:E6:65:2D:EA:B2:2E:B1:09:69:12:4E:30:D5:D8:F8:BC:00:80:2F:4D: 93:0F:CD:2E:57:1B:33:BB:9F:4E:C4:A5:CB:79:A7:F8:E2:34:18:B6:20:9E:1B:9F:5D:A7:C9:3A:AD:45:64:B3:18:CE:11:12:9C:6D:1E:55:45:28:84:9C:57:67:4D:F9:CB:E2:8B:8F:58:09:D 4:39:FF:C8:36:02:3B:E2:0C:65:7F:15:0E:7D:C1:07:DD:A9:22:DF:91:00:C4:6C:71:34:74:DC:39:EA:EA:4F:44:69:7F:58:D8:58:0A:52:71:2B:EC:A9:1D:50:74:33:F9:29:6A:FA:FE:99:F4:E7: CC:45:4D:CA:5A:25:A2:12:E3:CE:D7:38:05:39:F0:1A:09:F5:76:59:CE:62:6F:7A:34:0D:2C:D1:BC:04:12:EC:3D:53:C8:FA:D0:02:CB:CE:3D:21:B5:C5:E0:39:33:65:CF:39:53:C9:9B:46:F 9:9D:33:F3:59:80:08:41:BE:6F:4B:A0:FA:4A:CE:A4:76:1C:85:E2:AF:AF:14:9D:65:AC:F7:F7:97:E4:33:49:A6:AF:BE:CE:2B:37:F1:2E:C1:73:05:9C:9C:60:4C:9D:30:0D:97:54:9E:81:62:BB: E7:E0:2F:F7:14:07:14:A9:77:91:E9:DC:91:95:8E:D3:88:90:33:A7:6F:71:C3:14:69:FA:A6:2D:01:1E:1B:EA:D3:2E:E2:7F:08:DC:CF:E7:22:F0:F1:41:A3:01:92:E5:80:D3:BE:A9:62:46:55:8B: 0B:34:34:EC:DC:21:15:AA:EF:D6:22:5E:89:F5:51:92:13:2A:6F:80:16:D9:B1:0D:D9:2E:F8:10:B8:C2:FE:52:45:33:9C:1D:38:7C:DC:15:69:34:73:BF:A0:2C:BB:11:7B:94:CD:F8:37:2D:6F:3 D:EF:83:5A:C6:1E:9B:74:49:8F:D9:C2:8D:BE:16:76:50:C8:5A:D1:25:16:F6:F6:CC:8C:9C:5A:30:9E:65:8E:D0:9A:48:93:D7:FA:68:0D:75:31:87:F9:F7:02:03:01:00:01
Basic Constraints	IsCA: true
Subject Key Identifier	8E:45:F4:9F:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA
Certificate Policies	Policy OID: 2.5.29.32.0 CPS pointer: http://www.dnie.es/dpc
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	73:97:10:C5:24:5E:33:EC:8A:24:3A:1B:20:04:8F:C9:D5:F4:52:85:99:21:38:45:C1 :64:D0:04:B8:B6:67:F9
Certificate fields details	
Version:	3
Serial Number:	1023669171620362353858443562596147092
X509 Certificate	-----BEGIN CERTIFICATE----- MIIFvzCA6egAwIBAgIQAMUmyW4QIO1DTIe1+2efIDANBghkhiC9w0BAQsFADBDMQswCOYDVOQO EwJFuzEoMcyGAIUECqwrREISRUNDSU9OEdFTKVSOUwqREUgTEegUE9MSUNJQTENMasGA1UECwwE RE5jRTEVMBMGAIUEAwMMQUimgUkFjWIBETkFMB4XDTA2MDIxNjEwMzcyNVoXDTM2MDIwODIyNTk1 OjowXTELMAkGA1UEBmRCRVMsK04mBgNVBAAcMHORUKVDOOITBHRUSUFKFMIEFEXBIFBTEID SUXETALBqNVBAsMBEROSUUXfATBqNVBAMMDEDFJBFBSvqRE5jRTECCAlwDOYIKoZihvcNAQEB BQADggIPADCCAgQcCqgBAIAAQTzDoyAho2P9z5gze5qVAgXxbEBfaffmuV+Kcf8Mwh3qNPeK3jW BU2ESXHXAZoXjfwCAsayikjOgNM8AH711K4e5BmVCT8UswKvLDkXEsuIbWL+CBZwehOt QMXvBwIbwgKt5bvzCIU4OZileqYrEJaRjOMNXY+LwAgC9Nkw/NLicbM7uME7Ept5p/viNBiz j4bn12nyTqRrWScMAREpxthVfKt5cv2dN+cvii49YCD05/Bg20jDGVFOF059wOfdgSLKQDE bHE0DNW35upPRGj/WNYrCjKw+ypHb90M/kpav+mfTnZEVfbcjais487XOAU58Bq9XZZmjlv eQNLNG8BBLsPVPI+AcY849ibXF4DkZc85U8mbRvmdMNZqAfbvm9LoPpKzqR2HXir68UnWws 93+X5DNpqt++zis3857BcwWcnGBMnTANI15eqWK75+Av9xQHFkI3kenckZW004IQMDyccMufafm LQEG++TLUjC2p5yLw8UgZALigNo+aiWkOVtglNDTs3CEVouWii69VGS5ypvgB8ZsQ3ZLvgQ uML+UKUznB04fNwVaTrzv6Asuxf7IM34Ny1vPe+DwsYem3Rj9nCb4WdIDWtElFvb2zlycWjCe Zb7QmkiT1/poDXUkh/n3AgMBAAGjB5MABGA1UdEwEBwQFMAMBAf8wDgYDVROPAQH/BAQDAgEG MB0GA1UdOgQWBBSORR5fKXlsFzwFHbYBSDoG3uA3BgNVHSAEMDAuMCwGBFUdIAAwDAibggg BgEFFBQCARYWaHR0CDovL3d3dy5kbmllMnVzL2RwYzANBgkqhkiG9w0BAQsFAAOCAGAF/n5Mo3T NqhtHhYEm8Wbdh8NmPrU4owmsjL740t0RHRuRS5/48IYak7/krIGFVyZ1AqMSCWjcw30+G3Qx7 hSKTsZKEGwgnZ9aD1TW66y5UKxHwYlOVRi9hCtd089qu33vcslJNXLXKO6jR4N1Yp gXGWSkmK3K9aXOCbXPHUg7btK0VdGzSL0NXYnwZawf9J0s91pOIOI/XTRZ/EE6BEYYwbaNA 4IsTMFNkdor0VwsN418i08ba8gEKM029CqHyCB4VzLlIOHvL6rVQ8NtkOgt/ozx1Xo0zzjY6j DgaC2Rz2p6xvVMI1SN9vNnItIAK8reQMTh+vb8YFVxUxU/8VxZLH478jvSEUdNvznk8 P5gnwHSLk61eMUB3rxCS1sgUf7n9Kmu8IWk0xu+4y1j0V/OZy6egpTwNDR+Urt+joikLNgF09i8F jFQ45iNj7VM0AsbjSicpVmbis58Re7m3yr0bJmQ0VDzMQM2hFYh9uRUVOiQ8LQqVFK8VodNYxh FWT+svyMuxb520fCbaIABluE08ba7RvNlcTWW0bK29g1ThvFGZr8ZE09/ceeKocpyfYoe+Q Bx3200AGbMhFN1E30K0rua2628QZv5YKZL45hMDN4MvTN30nzB5XIIeH4avjG9CQ=
Signature algorithm:	SHA256withRSA
Issuer CN:	AC RAIZ DNIE
Issuer OU:	DNIE
Issuer O:	DIRECCION GENERAL DE LA POLICIA

Issuer C: *ES*

Subject CN: *AC RAIZ DNIE*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Valid from: *Thu Feb 16 11:37:25 CET 2006*

Valid to: *Fri Feb 08 23:59:59 CET 2036*

Public Key:

```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:00:AD:0C:C3:A3:20:07:A3:63:FF:F7:34:A0:CD:EE:6A:54:08:17:5D:B1:01:15:A7:E6:B9:5F:8A:71:FF:0C:C2:1D:EA:37:F3:DE:93:7F:D6:05:4D:84:B2:D5:D7:1C:0C:F4:C4:91:70:40:0E:5A:C8:98:A4:80:E8:0D:33:C0:07:F3:B7:F5:AC:A1:38:7A:C0:66:54:24:FC:52:C3:30:2A:F2:C3:C4:A1:2C:76:BF:C1:C0:BF:82:F1:9B:F0:68:7A:13:40:C8:97:BC:1C:25:07:08:0A:B7:96:EF:CC:29:54:E0:E6:65:2D:EA:B2:2E:81:09:69:12:4E:30:D5:D8:F8:BC:00:80:2F:4D:C9:0F:CD:2E:57:18:33:BB:9F:30:4E:C4:A5:C8:79:A7:FB:E2:34:18:86:20:9E:18:9F:5D:A7:C9:3A:AD:45:64:B3:18:CE:11:12:9C:6D:1E:55:45:28:84:9C:57:67:4D:F9:CB:E2:8B:8F:58:09:D4:39:FF:C8:36:02:38:E2:0C:65:7F:15:0E:7D:C1:07:DD:A9:22:DF:91:00:C4:6C:71:34:74:DC:39:EA:E4:4F:44:69:7F:58:D8:58:0A:52:71:2B:EC:A9:1D:50:74:33:F9:29:6A:FA:FE:99:F4:E7:CC:45:45:6D:CA:5A:25:A2:12:E3:CE:D7:38:05:39:F0:1A:09:F5:76:59:CE:62:6F:7A:34:0D:2C:D1:BC:04:12:EC:3D:53:C8:FA:D0:02:C8:CE:3D:21:85:C5:E0:39:33:65:CF:39:53:C9:98:46:F9:9D:33:F3:59:80:08:41:BE:6F:4B:A0:FA:4A:CE:A4:76:1C:85:E2:AF:AF:14:9D:65:AC:F7:F7:97:E4:33:49:A6:AF:BE:CE:2B:37:F1:2E:C1:73:05:9C:9C:60:4C:9D:30:0D:97:54:9E:81:62:BB:F7:E0:2F:F7:14:07:14:A9:77:91:F9:DC:91:95:8E:D3:88:90:33:47:6F:71:C3:14:69:FA:A6:2D:01:1E:1B:EA:03:2E:E2:7F:08:DC:CF:E7:22:F0:F1:41:A3:01:92:E5:80:D3:BE:A9:62:A8:55:88:0B:34:34:EC:DC:21:15:AA:EF:D6:22:5E:89:F5:51:92:13:2A:6F:80:16:D9:B1:0D:D9:2E:F8:10:B8:C2:FE:52:45:33:9C:1D:38:7C:DC:15:69:34:73:BF:A0:2C:8B:11:7B:94:CD:F8:37:2D:6F:3D:EF:83:5A:C6:1E:9B:74:49:8F:D9:C2:8D:BE:16:76:50:C8:5A:D1:25:16:F6:F6:CC:8C:9C:5A:30:9E:65:8E:D0:9A:48:93:D7:FA:68:0D:75:31:87:F9:F7:02:03:01:00:01
```

Basic Constraints *IsCA: true*

Subject Key Identifier *8E:45:F4:9F:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.dnie.es/dpc>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F5:79:21:10:81:7A:86:D4:FE:24:4A:C2:A8:B1:0B:5B:0B:F4:CE:86:26:66:1A:B9:84:47:0A:87:87:98:30:F5*

X509SubjectName

Subject CN: *AC RAIZ DNIE*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-09-14T00:00:00Z*

Scheme Service Definition URI

URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt
URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt
URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt
URI	[en]	http://www.dnielectronico.es/PDFs/Políticas_de_Certificacion_v2.1.pdf
URI	[es]	http://www.dnielectronico.es/PDFs/Políticas_de_Certificacion_v2.1.pdf
URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt
URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt
URI	[en]	https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt
URI	[es]	https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt

2.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC

2.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

2.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:2.16.724.1.2.2.2.11*

Description

2.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by subordinated CA under the root CA*

Name [es] *Certificados Reconocidos emitido por CAs subordinadas de la CA Root*

Service digital identities**X509SubjectName**

Subject CN: *AC RAIZ DNIE*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

X509SKI

X509 SK I *jkX0n3PF/y8bBdsBR2AbA4qBt7o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

2.1.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.1.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:2.16.724.1.2.2.2.11

Description

2.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by subordinated CA under the root CA

Name	[es]	Certificados Reconocidos emitido por CAs subordinadas de la CA Root

Service digital identities

X509SubjectName

Subject CN:	AC RAIZ DNIE

Subject OU:	DNIE

Subject O:	DIRECCION GENERAL DE LA POLICIA

Subject C:	ES

X509SKI

X509 SK I	jkX0n3PF/y8bBdsBR2AbA4qBt7o=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2006-12-11T00:00:00Z

2.1.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

Basic Constraints *IsCA: true*

Subject Key Identifier *0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.policia.es/dpc>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: 97:E9:F2:C6:2C:95:F1:F0:FF:B0:A6:DF:29:C4:E7:64:7E:C9:06:FB:62:D3:62:26:FD:81:1D:41:22:74:6C:89

Certificate fields details

Version: 3

Serial Number: 1009759735754786940203842089657449054

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: AC RAIZ DGP

Issuer OU: CNP

Issuer 0: DIRECCION GENERAL DE LA POLICIA

Issuer C: *FS*

Subject CN: AC RAIZ DGP

Subject OU: CNP

Subject O: DIRECCION GENERAL DE LA POLICIA

Subject C: ES

Valid from: Thu Jan 25 13:05:08 CET 2007

Valid to: Sun Jan 25 13:05:08 CET 2037

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:80:10:F5:B7:5E:B3:30:9C:6F:A3:1B:88:0E:5C:AD:EA:97:E0:CC:F9:A6:7C:93:05:BC:FC:A8:8F:40:0E:C6:3C:81:8B:A7:F8:EC:AF:ED:85:5F:E9:31:AB:50:AA:31:9A:7B:76:23:F3:7B:A9:BF:86:05:CA:0A:BF:8D:4D:36:11:E1:08:79:04:04:7F:E4:09:F8:1F:8B:5F:EA:06:2C:F6:D4:E6:0F:3F:58:57:85:72:75:C2:E0:98:36:8A:93:FB:2F:6A:9C:11:F0:35:F3:40:2C:4F:55:2A:98:74:DC:EE:44:48:DC:DE:82:25:96:62:1E:43:38:86:98:DF:DE:F8:2C:0B:15:10:B5:7C:3E:5C:06:58:B5:A4:5B:8C:53:BA:F6:D4:D2:75:BA:5B:5C:DE:1F:BC:E4:30:1C:D9:5E:9C:5D:46:33:1B:22:87:BB:60:19:4C:11:95:8D:84:55:F8:7B:10:66:2F:5E:DD:A6:B6:91:E2:10:87:92:A7:5B:36:58:1C:73:82:25:94:D4:88:9F:88:3A:35:F2:89:59:BF:CE:7D:A0:79:0D:04:3D:2C:C7:A2:05:3C:F8:A7:FE:C2:0D:B8:CD:4C:E9:A0:51:C1:CE:F6:E5:C3:20:66:62:32:34:33:87:66:4A:84:C4:BF:03:35:48:93:CD:76:33:AA:BE:D1:F0:7F:A4:9F:9F:51:60:BC:08:12:67:D1:40:B9:0A:C7:26:25:65:E1:5B:88:E2:39:9F:B5:33:DE:F2:80:35:C4:D8:52:E0:82:98:0D:3E:64:0F:44:4A:5A:F3:F2:40:3A:7C:75:74:F9:F3:1E:3D:4D:58:9E:87:22:24:EE:5F:15:7F:E3:C6:D4:9C:3A:AA:D0:B7:E2:BE:80:69:88:4E:E6:DA:94:1A:0B:EC:4D:86:CE:CD:C2:98:AB:67:BB:23:87:F8:A1:4E:FF:CA:8B:D4:5C:61:9F:75:AA:94:A8:DE:ED:D0:54:86:90:08:FF:B7:66:E1:1D:9B:17:8A:F2:D4:D9:EA:65:63:9B:0A:E0:5F:2A:AC:8B:F3:40:F1:FB:AC:DA:1A:C4:E8:ED:40:4B:35:D7:00:E2:C5:C0:AC:9A:00:31:4A:87:6F:FE:FB:AE:AB:B8:E5:D5:89:22:14:00:E5:5D:EA:A2:5C:28:C3:0B:93:75:9C:02:D5:E7:36:01:6C:00:EA:03:1F:DA:E7:21:34:9B:0F:59:69:90:AE:45:EF:92:1B:86:AC:8E:F9:E9:C2:B0:81:1E:F2:DB:6E:75:EE:AF:C1:F4:C3:71:EC:89:EC:65:B3:1B:39:65:30:42:E7:A2:DD:47:28:22:00:85:B3:64:D6:09:88:71:1C:D9:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.policia.es/dpc

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1F:30:4D:5D:DA:90:47:60:C4:B8:D6:2F:14:F5:19:62:A7:06:CD:C0:2C:5B:70:F1:50:33:A0:4F:CD:36:45:B8*

X509SubjectName

Subject CN: AC RAIZ DGP

Subject OU: CNP

Subject O: DIRECCION GENERAL DE LA POLICIA

Subject C: ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2022-06-29T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://www.policia.es/DPC/dpc.pdf*

URI	[es]	http://www.policia.es/DPC/dpc.pdf
URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[en]	https://www.policia.es/certs/AC_DGP_001-SHA1.crt
URI	[es]	https://www.policia.es/certs/AC_DGP_001-SHA1.crt
URI	[en]	https://www.policia.es/certs/AC_DGP_001-SHA2.cer
URI	[es]	https://www.policia.es/certs/AC_DGP_001-SHA2.cer
URI	[en]	https://www.policia.es/certs/AC_DGP_002-SHA1.crt
URI	[es]	https://www.policia.es/certs/AC_DGP_002-SHA1.crt
URI	[en]	https://www.policia.es/certs/AC_DGP_002-SHA2.cer
URI	[es]	https://www.policia.es/certs/AC_DGP_002-SHA2.cer

2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC

2.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

2.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

2.2.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>**2.2.5 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name

[en]

Qualified Certificates issued by subordinated CA under the root CA for Public Administration

Name

[es]

*Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP***Service digital identities****X509SubjectName**

Subject CN:

AC RAIZ DGP

Subject OU:

CNP

Subject O:

DIRECCION GENERAL DE LA POLICIA

Subject C:

*ES***X509SKI**

X509 SK I

*Dpx24aluiTNB8uM+bFsWRb29ho4=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time***2018-07-16T00:00:00Z***2.2.5.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>**2.2.5.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

2.2.5.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

2.2.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

2.2.6 - History instance n.2 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by subordinated CA under the root CA for Public Administration

Name	[es]	Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP

Service digital identities**X509SubjectName**

Subject CN:	AC RAIZ DGP

Subject OU:	CNP

Subject O:	DIRECCION GENERAL DE LA POLICIA

Subject C:	ES

X509SKI

X509 SK I	Dpx24aluiTNB8uM+bFsWRb29ho4=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

2.2.6.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC

2.2.6.6 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:2.16.724.1.2.1.102.36

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:2.16.724.1.2.1.102.37

2.2.6.7 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

2.2.7 - History instance n.3 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by subordinated CA under the root CA for Public Administration

Name	[es]	Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP

Service digital identities**X509SubjectName**

Subject CN:	AC RAIZ DGP

Subject OU:	CNP

Subject O:	DIRECCION GENERAL DE LA POLICIA

Subject C:	ES

X509SKI

X509 SK I

Dpx24aluiTNB8uM+bFsWRb29ho4=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2014-03-17T00:00:00Z

2.2.7.8 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>**2.2.7.9 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description [en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[OIDsURN]

urn:oid:2.16.724.1.2.1.102.36

Policy Identifier:

Identifier

[OIDsURN]

urn:oid:2.16.724.1.2.1.102.37

2.3 - Service (granted): Qualified Certificates issued by subordinated CA under the root CA DNle 2

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en]

Qualified Certificates issued by subordinated CA under the root CA DNle 2

Certificate Policies *Policy OID: 2.5.29.32.0*
 CPS pointer: http://pki.policia.es/dnie/publicaciones/dpc

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C5:C3:80:EB:92:40:FB:36:A1:6E:15:F5:D6:BA:D0:BF:61:1F:6D:03:F0:EF:24:22:99
 :19:E7:D2:D8:12:6C:11*

X509SubjectName

Subject CN: *AC RAIZ DNIE 2*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
 [es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en] http://pki.policia.es/dnie/certs/AC004.crt*

URI *[es] http://pki.policia.es/dnie/certs/AC004.crt*

URI *[en] http://pki.policia.es/dnie/certs/AC005.crt*

URI *[es] http://pki.policia.es/dnie/certs/AC005.crt*

URI *[en] http://pki.policia.es/dnie/certs/AC006.crt*

URI *[es] http://pki.policia.es/dnie/certs/AC006.crt*

URI *[en] http://pki.policia.es/dnie/publicaciones/dpc*

URI *[es] http://pki.policia.es/dnie/publicaciones/dpc*

2.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

2.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

2.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:2.16.724.1.2.2.2.11

Description

2.3.4 - History instance n.1 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by subordinated CA under the root CA DNIE 2

Name	[es]	Certificados Reconocidos emitido por CAs subordinadas de la CA Root DNIE 2

Service digital identities

X509SubjectName

Subject CN:	AC RAIZ DNIE 2

Subject OU:	DNIE

Subject O:	DIRECCION GENERAL DE LA POLICIA

Subject C:	ES

X509SKI

X509 SK I	U9xuYqTOExt34lehWqQPsocS8js=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC

2.4 - Service (granted): Qualified Certificates issued by AC DGP 004

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	Qualified Certificates issued by AC DGP 004

Name [es] *Certificados cualificados emitidos por AC DGP 004*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 31794812614395090018704226159857973009

X509 Certificate -----BEGIN CERTIFICATE-----

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: AC RAIZ DGP 2

Issuer 2.5.4.97: *VATES-S2816015H*

Issuer OU: *CNP*
Issuer O: *DIRECCION GENERAL DE LA POLICIA*
Issuer C: *ES*
Subject CN: *AC DGP 004*
Subject 2.5.4.97: *VATES-S2816015H*
Subject OU: *CNP*
Subject O: *DIRECCION GENERAL DE LA POLICIA*
Subject C: *ES*
Valid from: *Thu Aug 02 12:50:02 CEST 2018*
Valid to: *Tue Aug 02 12:50:02 CEST 2033*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AE:0E:E5:97:40:F6:30:0C:AF:28:DD:1C:97:A0:34:11:31:67:25:54:8C:84:9D:
0F:04:21:11:D2:BA:8A:61:40:47:FC:D7:87:BF:2E:8F:1D:61:88:48:00:FC:8C:46:97:AA:F2:8D:81:6C:9D:00:DA:E1:11:1A:85:E9:8A:1A:8A:D6:3B:47:EC:09:94:F6:CA:75:34:BD:46:78:87:1
1:CF:70:7D:B1:01:04:69:29:88:A4:C9:19:33:64:AC:CE:45:68:F3:FD:B9:2A:B7:D9:8C:64:BF:0A:43:33:2E:4A:82:82:8A:02:6A:9D:B0:0F:E8:AF:9C:3A:31:12:83:05:AD:59:0B:D6:76:4B:1D
:B9:EF:F5:15:58:75:96:7D:EB:D4:65:86:3A:04:5D:CB:25:86:2E:D2:AA:73:A9:88:42:33:A4:48:8E:B7:68:EF:8D:8D:52:25:74:1D:CB:84:74:1D:01:D2:54:FA:F9:F9:F8:F7:1E:0E:A2:28:EF:7
C:96:9C:F8:AA:EB:5E:34:4C:62:88:78:AA:2C:1A:24:F3:85:54:0C:84:B1:3B:58:72:6C:E5:99:76:5C:21:0C:96:6D:C2:3D:F6:FE:3C:20:82:26:D4:82:DF:E8:17:58:16:08:41:B1:AF:12:F5:
46:50:92:57:7F:B4:DD:67:1F:98:7E:76:6A:64:2E:DE:88:73:04:70:15:CD:5C:EC:ED:36:42:EC:58:A4:4F:40:D5:A8:0A:1F:01:8D:86:BC:DS:D6:38:04:6A:2F:AB:3C:F2:79:12:E1:8E:39:7A:C
8:19:76:49:85:E1:05:DE:8F:05:3A:F8:44:7F:5C:F7:F8:97:E7:2C:1E:48:CB:B1:82:58:1B:39:12:D0:D4:6A:38:82:28:E5:DE:F7:C1:83:98:13:EA:7C:FB:01:28:D0:91:85:78:F2:2E:47:55:E1:A
D:83:04:6E:7F:09:AA:4E:92:2A:7E:6A:06:C3:8C:3B:16:AC:2A:37:10:50:C9:B1:AE:ED:EA:FE:CS:5A:05:1C:80:27:2F:35:15:9D:E8:60:B1:03:68:EB:F3:2F:4E:02:28:34:06:88:F9:7D:AB:7D:
E8:4D:9C:D6:21:68:B3:0F:E2:5C:9E:53:D3:04:21:4A:5F:90:77:1B:B4:94:EE:50:3D:2D:B5:F2:F1:8E:AB:45:44:43:3F:71:88:A6:19:3A:68:77:CD:2E:70:5D:BF:F2:E5:C5:EF:E3:25:F0:30:4D
:E0:8D:DE:57:1F:89:AA:17:A0:B9:19:F8:D7:27:DF:8E:98:67:D2:F3:40:E6:29:A7:25:80:0B:87:8F:91:E0:DA:BA:5C:9B:45:68:26:14:59:CE:0D:7F:1D:02:03:01:00:01

```

Subject Key Identifier *0D:A7:E4:C0:B4:D7:97:E4:74:DC:86:7C:52:FE:F4:DE:32:62:32:BC*
Authority Info Access
http://ocsp.policia.es
http://pki.policia.es/cnp/certs/ACRaiz2.crt
Authority Key Identifier *93:80:EB:56:AD:4B:CF:B1:91:0E:2B:34:CE:3C:62:16:1E:87:BF:80*
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: http://pki.policia.es/cnp/publicaciones/dpc
Basic Constraints
IsCA: true - Path length: 0
CRL Distribution Points
http://pki.policia.es/cnp/crls/ARL.crl
ldap://ldap.policia.es/CN=CRL,CN=AC%20RAIZ%20DGP%20,OI=VATES-S2816015H,OU=CNP,O=DIRECCION%20GENERAL%20DE%20LA%20POLICIA,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *6A:D4:3C:81:5C:D8:47:AF:82:B1:80:A2:A0:BD:39:02:B3:52:0E:19:CF:0E:D2:10:D8:00:99:E5:97:42:99:00*
X509SubjectName
Subject CN: *AC DGP 004*

Subject 2.5.4.97: *VATES-S2816015H*

Subject OU: *CNP*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

X509SKI

X509 SK I *DafkwLTXI+R03IZ8Uv703jjiMrw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-08-06T00:00:00Z*

2.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

2.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC DGP 004*

Name *[es]* *Certificados cualificados emitidos por AC DGP 004*

Service digital identities

X509SubjectName

Subject CN: *AC DGP 004*

Subject 2.5.4.97: VATES-S2816015H

Subject OU: CNP

Subject O: DIRECCION GENERAL DE LA POLICIA

Subject C: ES

X509SKI

X509 SK I DafkwLTXI+R03IZ8Uv703jjiMrw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-01-15T01:00:00Z

2.4.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

2.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

2.4.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

2.5 - Service (granted): OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>

Service type description	[en]	A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.
	[es]	A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.

Service Name

Name	[en]	OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2
Name	[es]	Respuestas OCSP emitidas por Autoridad de Certificación AC RAIZ DNIE 2

Service digital identities

Certificate fields details

Version:	3
Serial Number:	57300804758115330416592336794492330659

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIFZzCA8OgAwIBAgIQKxu7y2HP5CR5RV09XtviozANBgkqhkiG9w0BAQsFADBFMQswCQYDVQVQ^Q
EWwFuzEoMCYGA1UECgwFR5RUND5U90IEFTKvSQUwgrEUGTEegUE9MSUNJOTENMAsGA1UECwwE
RES5RTEyXMBUaGUeAwwwOQUMgUkFjWIBETkFIIDWhhcHMtMwOT3MTAYjA1WIBFMAwswCQYDVQ^Q
GEWwFuzEoMCYGA1UECgwFR5RUND5U90IEFTKvSQUwgrEUGTEegUE9MSUNJOTENMAsGA1UEC^W
wERE5RTEyXMBUaGUeAwwwOQUMgUkFjWIBETkFIIDWhhcHMtMwOT3MTAYjA1WIBFMAwswCQY^Q
DQEBAAUAA4CDWAwgK4AnCAQDQ2C2ORPjINm93wUyLTulZkzv39R/lec3055ay3i2yPq
wVbToNaRYKDaXpUVvix2nU8zFkYvh6CAnzh3M6FaFWCz2PHKATSLHp5OJwUMDeCOM0UvQeu1usEe
LXg8vzir5go7FQd3ngAZE1y9DZENipNekiVWqspMtK1txTirO5UGK78MnikuuB9yjszbnY7ly6
1Iv6us8Y2E0FFDjlrtpihRKFL0Ameho2gPpwM15DXtwszFaU4+ukd4CCeU0he5RuU
Q4+AGQWqj+mUapyMkGhBs6E8WLqVODWxZLrcnusWjdxvFKeGPTL1aj0FxiP6Mzs9V1j/buTbFN
Fv3o30AC42cwnQOLVzjRsEsu6auCQljHdXjtdFZQOikQjzYBUj3iDdGQ3mWzmxXOp5DuMHasobK
QIBDP7ZdXZercodnP0lWMSUaoypAOwD6LZdVkiUu9R0453LzUAngE9F5WxWTK3jGp1Z2Teh
CzUCz9HTOC95Yuyx1Z2ptvOzuapY5c2CzA3USO/CfCYvmNjhaeS0sBx6P+IS0SYgL6Z8aCpVL
DQBH1Lub9rSOWvbFfpdZ6iWUdX4dzAgmjgWN9VKgrOHsW1u4whoaw3NadWysjpdOqq5wz5w49o
Z9uDFN64cYR3+ +vdsof3MTvODAQABqGSMICPMAsA1UdeE8iwGFMAMBA8wDq1QVR0PACWJ
BAQDAqEGMB0GA1UdDgQWBRT3G5ipMATG3fgh6FapA+ yhxLwmZNBGNVHSAERjBEEMEIGBFUdIAAw
OjA4BgrBgqEFBQcCARYsaHR0cDowl3Bra55wb2xpY2ihLmVzL2RuaWUvcHVibGllYWNPb25icy9k
cGhwDOYKozlincNAQELBQAQDgpiBACeV8sVBAISaKrfuq5lqm0PZv1V8qRepYkHKQJjiWM9/s
yHsdI345hDryAJ2m8/BvY06aN0REMz1XAYWhUQT32D0k0fMnZ9SpqyWFW6GMPfcp9D00Qsqik
QojPWPloBgVZ6zCzKeGIMdF5fooy5wj/w0stNFidGC1WdFdWTksmt4KlrEa43lvgSGPqEr8nIV
QoStetoh7mywu4D30jbsyIUOP3UMY026km09Qv9B0LdfVo+ T3LlUrYXt4qjEA7A5
Kkp850Uy0WiWPOZG557jeh1KdkCm5jcChbHIA3vylYeaS0IPccXjr+ +rSsa9K0K/cOPHosCT0
sl2MOV3c25UGzacKVVSWaAGK4aPWwGc1binGdbhdw53M2NP0kKC9ONHA+DbK80gm/dCH68DcyQI
jUE2OyeGaA2719RmCViPnMwCqH5pM4f05jD5hQHT0z+ 712DXAt1nyVDi0z7K7Wpaa6
R/Lw8ghV9SE65fiOBw8ZTiuDEi9mN2u06LqmoF63FOCZSAQ2Nv4E/Ks7G/TM9K2f4ftYLn/m
GAxKf5fUjI0pNuZgaSEY7la3Nc175+ vYnxxn2jJiIKfBnBgKwP/r4Z2SDVnXFgb7dgQeOg6o10x
VvABlea0t8VEty3SEfmxvLhkGQ3h
-----END CERTIFICATE-----

Signature algorithm:	SHA256withRSA
Issuer CN:	AC RAIZ DNIE 2
Issuer OU:	DNIE
Issuer O:	DIRECCION GENERAL DE LA POLICIA
Issuer C:	ES
Subject CN:	AC RAIZ DNIE 2
Subject OU:	DNIE
Subject O:	DIRECCION GENERAL DE LA POLICIA
Subject C:	ES
Valid from:	Fri Sep 27 12:26:05 CEST 2013
Valid to:	Sun Sep 27 12:26:05 CEST 2043
Public Key:	30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DB:64:2F:DB:45:FA:65:FE:23:73:9F:FD:F0:52:B6:08:7E:E2:F6:CE:4C:D5:DE:86:91:FC:8A:1C:DF:44:B9:6B:2D:E2:0F:23:E0:C1:96:D3:40:D6:91:60:A0:DA:5E:95:15:9E:95:F6:9D:4F:33:1E:96:2F:87:A0:80:9F:38:77:33:A1:5A:15:67:36:AC:F1:54:02:D4:88:1E:9E:4E:27:05:0C:0D:E0:8E:33:45:2F:41:E8:B5:BA:C1:1E:2D:78:3C:BF:38:AB:E6:A4:38:15:07:77:9E:00:19:13:5C:BD:0D:91:0D:8A:93:5E:92:55:56:AA:CA:4C:B4:AD:7F:B7:14:E2:AC:EE:54:18:AE:FC:32:72:0A:BA:E0:7D:CA:3B:33:6E:76:3B:22:EC:BA:97:55:63:EA:CS:12:B7:C8:58:CE:31:2D:FC:51:43:6C:92:2B:6E:DA:62:85:12:85:08:B3:80:99:E8:68:DA:A3:CF:C0:CD:79:0D:74:F0:B1:9B:05:69:4F:F8:FA:E9:1D:E0:20:9E:51:B8:5E:ES:1B:AE:43:8F:90:19:05:AA:8F:E9:94:6A:9C:9C:90:68:41:B3:A1:3C:58:8A:95:38:3C:31:64:84:DC:9E:E8:16:8C:97:71:8C:52:9E:1B:F4:CB:D5:A8:F4:16:DC:62:3F:A3:33:B3:D5:75:8F:F6:EE:4D:B1:4D:16:FD:E8:DF:40:02:E3:67:30:9D:04:14:57:38:D1:B0:4B:2E:E9:AB:82:40:96:C9:1D:D5:E3:85:D1:59:41:08:B1:42:3C:DB:05:42:77:88:38:46:43:79:96:CE:6C:57:3A:9E:43:B8:C1:DA:4A:86:CA:D2:20:43:3F:B6:43:B5:86:70:72:87:66:3D:D8:D6:94:CE:54:6A:8C:A9:00:EC:D6:0E:CE:8B:65:D5:64:21:48:8F:75:16:FB:E5:FD:CB:89:90:27:80:4F:45:E5:9C:56:4C:4D:E3:1A:9D:3F:D9:3E:A1:0B:35:1C:65:8F:47:4C:E1:8D:49:8B:B2:C7:56:69:B6:F3:B3:BA:00:2B:63:97:36:70:06:77:51:23:8F:08:57:18:7E:F9:8D:26:16:9E:4A:8B:01:C7:A3:FE:21:28:B4:49:8B:08:E9:90:5A:0A:95:4B:0D:00:61:D4:BB:9B:F6:B4:90:5A:F6:C5:7C:8A:5D:67:A8:96:51:D5:F8:77:30:2A:98:98:16:37:D5:4A:82:B3:87:B1:6D:6E:E2:F8:68:68:0D:CD:01:D5:B2:B2:3A:6F:74:EA:AA:E7:0C:D2:C3:8F:68:67:DB:83:14:D7:78:71:84:6B:DF:EF:AF:75:AA:08:7F:73:13:BD:02:03:01:00:01
Basic Constraints	IsCA: true

Subject Key Identifier *53:DC:6E:62:A4:CE:13:1B:77:E0:87:A1:5A:A4:0F:B2:87:12:F0:9B*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://pki.policia.es/dnie/publicaciones/dpc

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C5:C3:80:EB:92:40:FB:36:A1:6E:15:F5:D6:BA:D0:BF:61:1F:6D:03:F0:EF:24:22:99:19:E7:D2:D8:12:6C:11*

X509SubjectName

Subject CN: *AC RAIZ DNIE 2*

Subject OU: *DNIE*

Subject O: *DIRECCION GENERAL DE LA POLICIA*

Subject C: *ES*

X509SKI

X509 SK I *U9xuYqTOExt34lehWqQPsocS8Js=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-04-21T00:00:00Z*

2.5.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3 - TSP: Agencia Notarial de Certificación S.L. Unipersonal

TSP Name

Name *[en]* *Agencia Notarial de Certificación S.L. Unipersonal*

Name *[es]* *Agencia Notarial de Certificación S.L. Unipersonal*

TSP Trade Name

Name *[en]* *VATES-B83395988*

Name *[en]* *ANCERT - Agencia Notarial de Certificación*

Name *[es]* *ANCERT - Agencia Notarial de Certificación*

Name *[en]* *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Name *[en]* *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Name *[en]* *Agencia Notarial de Certificación S.L.Unipersonal*

Name *[en]* *Centro Tecnológico del Notariado*

PostalAddress

Street Address *[en]* *Calle Campezo, nº 1, Edificio 6, pl. 2ª*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28022*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Calle Campezo, nº 1, Edificio 6, pl. 2ª*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28022*

Country Name *[es]* *ES*

ElectronicAddress

Issuer C: *ES*
Subject CN: *ANCERT Corporativos Personales V2*
Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*
Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*
Subject C: *ES*
Valid from: *Tue Jun 21 12:09:32 CEST 2016*
Valid to: *Sat May 25 02:01:00 CEST 2030*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:1C:82:F7:32:F5:D5:C6:16:D4:79:97:80:21:21:A1:F4:45:50:94:88:85:E5:
FF:1E:D7:E9:7F:05:00:31:A6:60:E9:CD:73:F8:98:1E:C1:25:AD:31:C1:AE:A2:20:5A:42:53:77:C3:F5:A3:FC:9D:49:FA:03:23:12:25:86:67:69:CC:5C:56:C4:72:0E:CF:75:47:C6:E3:44:F3:FA:
:6F:5A:64:03:7D:B6:92:14:D6:73:9F:4C:72:16:01:A9:FF:DE:70:1B:EC:E8:1B:6F:25:18:6C:A4:D7:2E:88:02:3A:B5:D8:A0:30:29:40:99:2F:F6:42:F4:F9:CF:76:CB:4D:69:61:F3:6C:05:A6:F0:
:F8:F9:92:92:76:23:73:C2:5D:9F:DA:6A:BE:A5:E3:29:98:80:FC:29:07:E8:96:AD:8D:87:FE:1C:EA:2B:4A:67:07:25:5A:77:A9:94:AD:1A:8A:7C:23:65:C2:09:14:36:5F:6A:58:A1:69:BE:A3:7
5:8E:29:3A:CC:2F:21:CC:72:7C:44:8D:05:0C:8D:EC:8A:2D:F6:EC:55:21:E4:F3:90:85:75:F8:9E:9B:A5:C1:8A:FE:9B:B3:2A:8B:18:75:36:BB:84:8C:1D:F8:AF:E2:3F:A3:BA:F3:59:F5:76:70:
C3:31:47:D7:1D:26:22:34:96:57:F0:CC:60:34:99:F8:9F:84:10:1A:0A:52:99:4D:80:42:86:DF:2B:B5:BC:A4:6C:A0:B8:C4:FF:F8:0E:B9:43:67:6E:A1:56:19:A1:B4:0C:AA:89:DB:E7:7E:70:D
5:56:3D:CA:77:C4:28:03:13:3C:7A:F2:5D:C1:3D:7E:D0:B7:5E:0B:DF:E4:E9:57:90:67:41:68:65:84:DD:21:89:F2:CF:BB:A7:B6:EE:D4:D7:7C:2E:39:80:09:FC:DE:31:2F:1F:79:82:77:F5:60:
70:16:DC:67:B5:20:C8:4F:ED:CD:4D:0D:21:29:4D:14:62:8D:AB:79:DE:CB:8A:B6:33:7E:BC:A3:88:43:16:94:23:82:66:C2:52:D6:48:20:F1:FE:8F:9E:08:AD:12:04:E2:EC:E6:47:58:89:13:
3F:79:A5:AC:6E:7F:C3:8C:4F:A1:F8:20:61:AF:68:98:56:62:64:E1:EA:A0:AE:CB:16:20:D4:A5:F6:5F:EC:4F:78:A4:79:D8:E6:5F:4F:57:F8:1E:B8:0F:2B:61:C5:BF:49:AA:A1:9B:41:54:70:C2:
64:6D:CB:26:A1:6D:EB:4F:58:EB:8C:2B:2A:FC:D2:11:CB:9B:F8:92:09:8C:FD:D0:82:76:98:D6:B9:C7:E1:8C:B4:6D:96:5D:90:17:25:56:1F:8E:10:55:02:03:01:00:01

```

Authority Info Access *http://ocsp.ac.ancert.com/ocsp.xuda*
http://www.ancert.com/pki/v2/certs/ANCERTPRIV_V2.crt
Authority Key Identifier *FD:3C:6A:79:66:15:3C:00:BB:D2:36:A2:62:A6:58:E6:1A:E0:33:AF*
Basic Constraints *IsCA: true - Path length: 0*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18920.2.1*
CPS pointer: https://www.ancert.com/cps
CRL Distribution Points *http://www.ancert.com/crl/ANCERTPRIV_V2.crl*
http://www2.ancert.com/crl/ANCERTPRIV_V2.crl
http://www3.ancert.com/crl/ANCERTPRIV_V2.crl
Subject Key Identifier *5F:EE:DD:29:03:01:43:69:C8:1E:3D:5B:81:7E:A5:F3:A1:76:AC:F8*
Subject Alternative Name *pki.explotacion@ancert.com*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *AE:9E:FF:CD:7B:83:0D:9A:7A:6D:F0:90:7E:DF:CE:FE:5D:C8:8A:A5:CC:B7:04:5F:03:FD:67:1C:BD:E5:B4:B7*

Certificate fields details

Version: *3*
Serial Number: *151806557225635609738953006987710450500*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8A:C2:CF:DE:0B:8A:60:12:51:8A:A3:BC:EF:89:55:26:B1:A5:29:B4:F6:39:54:4B:23:2C:DD:62:8D:81:5D:71*

X509SubjectName

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2018-02-15T01:00:00Z*

3.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Corporativos Personales v.2*

Name *[en]* *Personal Corporate Certificate v2*

Service digital identities**X509SubjectName**

Subject CN: *ANCERT Corporativos Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: ES

X509SKI

X509 SK I X+7dKQMBQ2nIHj1bgX6l86F2rPg=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

3.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] Certificados Corporativos Personales v.2

Name [en] Personal Corporate Certificate v2

Service digital identities

X509SubjectName

Subject CN: ANCERT Corporativos Personales V2

Subject O: Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Subject L: Paseo del General Martinez Campos 46 6a planta 28010 Madrid

Subject C: ES

X509SKI

X509 SK I X+7dKQMBQ2nIHj1bgX6l86F2rPg=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2010-11-16T00:00:00Z

Version: 3

Serial Number: 135466428519879488225880736606914916039

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANCERT Corporaciones de Derecho Publico V2*

Issuer O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Valid from: *Thu May 27 10:04:55 CEST 2010*

Valid to: *Wed May 27 10:04:56 CEST 2020*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9D:2D:43:09:E6:65:6B:83:A6:CB:97:A2:03:43:B1:BF:CA:24:74:6F:E8:3A:F6:45:6B:AB:72:0C:4D:56:77:11:E5:65:C4:B4:04:00:11:D1:64:56:F6:9E:AB:B3:A6:36:42:3F:32:12:F3:27:12:61:A2:50:A2:E7:1C:65:1B:C6:89:E3:FE:C6:2A:15:1C:AE:25:EF:D4:EE:5B:8B:8F:9D:13:09:E4:4E:EE:73:11:6D:C5:58:AB:40:79:50:C2:FB:84:71:A6:64:A9:22:BC:40:8A:38:51:11:F9:CD:3B:1A:BF:A2:10:9D:64:05:B2:1D:90:FF:30:CB:2E:9B:11:F1:F3:8B:0E:03:D8:5F:E9:26:61:D0:21:6A:93:D9:4D:16:27:8A:69:41:38:CE:BE:88:F5:B1:9A:34:E7:47:BC:D6:A4:B6:AD:93:77:53:7D:2F:65:93:EC:41:6D:61:FE:22:C6:CB:C7:C7:75:F5:CB:CB:0F:66:A2:1A:66:8E:56:95:7C:02:D3:5F:43:FF:94:2A:EA:6E:FE:E0:B3:D5:8A:7C:99:A7:5F:C9:CA:30:CE:A5:3A:5A:93:5C:D1:20:30:79:4B:55:E1:98:06:40:5A:C0:9C:CD:A7:59:F1:C2:9C:47:6B:6B:4C:CD:63:F3:B7:81:E5:C7:50:AB:33:9D:4B:0F:8B:4A:38:2D:28:1B:2A:F0:0B:99:F9:9E:FB:3C:06:77:6E:17:4F:B6:DD:EC:79:8B:B9:B0:4C:17:3A:D2:ED:73:AF:05:73:23:06:64:9B:EE:36:9E:CF:8F:3B:F5:86:47:00:C4:27:CB:56:36:60:06:DA:3D:74:EE:BA:A7:75:C5:9F:39:AC:C5:B1:FF:A7:60:CF:D1:F9:3B:A2:FB:C7:AF:C9:0A:BD:7A:01:47:58:CE:90:95:E3:30:7A:FC:30:55:5F:D4:BB:4B:46:45:41:E9:24:C2:89:BF:C2:8F:43:27:19:73:D7:06:7F:66:E0:F6:0D:CB:E5:6F:5F:E9:AF:2E:CE:AD:AB:E9:EC:9C:D2:4A:0C:71:D8:56:15:EE:2E:1C:AA:22:1A:44:19:F7:8B:1E:44:E5:A6:03:B2:B9:75:E7:54:4F:54:A8:C5:68:C9:55:99:62:24:16:BF:2E:7B:CC:26:4E:27:2B:A7:27:9B:6B:29:52:3F:AD:89:02:F3:F4:8E:8D:DA:38:EE:33:C9:8B:FE:89:E5:94:13:F5:F2:C5:37:D6:BB:FA:B1:7B:17:63:1C:70:CC:B9:D6:F7:C5:C2:41:6A:62:89:4D:7F:0A:30:12:B3:36:6C:D3:58:88:EF:F3:71:F8:9D:D3:BF:FA:41:A1:E4:4B:FD:BC:27:35:02:03:01:00:01

Authority Key Identifier *40:C8:73:80:39:5C:42:7F:08:43:C3:DC:C7:F5:EE:80:EC:ED:FE:D9*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18920.3.1*
CPS pointer: <https://www.ancert.com/cps>

CRL Distribution Points *http://www.ancert.com/crl/ANCERTPUB_V2.crl*
http://www2.ancert.com/crl/ANCERTPUB_V2.crl
http://www3.ancert.com/crl/ANCERTPUB_V2.crl

Subject Key Identifier *C0:BA:BA:37:3B:43:72:09:BC:5B:3B:36:D6:B2:DE:2D:F6:4B:7C:C8*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *26:18:A9:AC:8D:B2:5F:36:4F:DB:37:C3:9D:B3:93:AC:00:11:1A:BE:57:64:8F:EF:65:7D:75:1C:66:02:21:D2*

X509SubjectName

Subject CN: *ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2018-02-15T01:00:00Z*

3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es] Certificados Personales de Corporaciones de Derecho Público v.2*

Name *[en] Qualified Personal Certificates for Public Corporations v2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *wLq6NztDcgm8Wzs21rLeLfZLfMg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.2.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

3.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	<i>Certificados Personales de Corporaciones de Derecho Público v.2</i>

Name	[en]	<i>Qualified Personal Certificates for Public Corporations v2</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>ANCERT Corporaciones de Derecho Publico Personales V2</i>

Subject O:	<i>Agencia Notarial de Certificacion S.L.U. - CIF B83395988</i>

Subject L:	<i>Paseo del General Martinez Campos 46 6a planta 28010 Madrid</i>

Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>wLq6NztDcgm8Wzs21rLeLfZLfMg=</i>

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	<i>2010-11-16T00:00:00Z</i>

3.3 - Service (granted): Certificados Notariales Reconocidos para personas físicas v.2

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[es]	<i>Certificados Notariales Reconocidos para personas físicas v.2</i>

[illegible]

Basic Constraints	<i>IsCA: true - Path length: 0</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.18920.1.1</i> <i>CPS pointer: https://www.ancert.com/cps</i>
CRL Distribution Points	<i>http://www.ancert.com/crl/ANCERTNOT_V2.crl</i> <i>http://www2.ancert.com/crl/ANCERTNOT_V2.crl</i> <i>http://www3.ancert.com/crl/ANCERTNOT_V2.crl</i>
Subject Key Identifier	<i>6F:1B:B8:64:97:1D:3C:F5:87:BA:05:A8:FF:EC:F8:E8:F7:94:D8:63</i>
Subject Alternative Name	<i>pki.explotacion@ancert.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>C4:47:25:08:C3:BC:68:9F:C5:9E:8B:F7:7A:6D:DE:DF:BB:29:A4:33:16:BD:09:46:D5:44:E5:4D:FC:00:15:35</i>

X509SubjectName

Subject CN:	<i>ANCERT Certificados Notariales Personales V2</i>
Subject O:	<i>Agencia Notarial de Certificacion S.L.U. - CIF B83395988</i>
Subject L:	<i>Paseo del General Martinez Campos 46 6a planta 28010 Madrid</i>
Subject C:	<i>ES</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time	<i>2016-06-30T22:00:00Z</i>

3.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

3.3.2 - History instance n.1 - Status: undersupervision

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service Name

Name *[es]* *Certificados Notariales Reconocidos para personas físicas v.2*

Name *[en]* *Qualified Notarial Certificates for individuals v.2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *bxu4ZJcdPPWHugWo/+z46PeU2GM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-11-16T00:00:00Z*

3.4 - Service (granted): Certificados Notariales Reconocidos para personas jurídicas v.2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Notariales Reconocidos para personas jurídicas v.2*

Name *[en]* *Qualified Notarial Certificates for legal person v.2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *80355812110946286783278297140241042538*

Subject Key Identifier *08:A1:2C:68:35:80:A4:FF:9C:AB:11:6C:0B:33:99:2D:71:19:AA:30*

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0C:A8:B7:A0:15:06:CA:FA:A1:87:9E:74:91:C6:62:F8:26:4E:B3:A2:F1:F0:E0:65:7D:A3:D6:A9:12:FF:14:87*

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Corporativos V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2019-10-28T01:00:00Z*

3.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1*

3.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**3.4.4 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[es]

*Certificados Notariales Reconocidos para personas jurídicas v.2***Name**

[en]

*Qualified Notarial Certificates for legal person v.2***Service digital identities****X509SubjectName****Subject CN:***ANCERT Certificados Notariales Corporativos V2***Subject O:***Agencia Notarial de Certificacion S.L.U. - CIF B83395988***Subject L:***Paseo del General Martinez Campos 46 6a planta 28010 Madrid***Subject C:***ES***X509SKI****X509 SK I***CKEsaDWApP+cqxFsCzOZLXEZqjA=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time***2016-06-30T22:00:00Z***3.4.4.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description**

[en]

undefined.

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1***3.4.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.4.5 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Notariales Reconocidos para personas jurídicas v.2*

Name [en] *Qualified Notarial Certificates for legal person v.2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Corporativos V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *CKEsaDWApP+cqxFsCzOZLXEZqjA=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2010-11-16T00:00:00Z*

3.4.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1*

Valid from: Tue Jun 21 12:27:52 CEST 2016

Valid to: Sat May 25 02:01:00 CEST 2030

Public Key:

```
30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C0:FF:C5:1B:06:CE:8B:CC:C7:81:FA:8C:55:B8:50:F3:7D:03:C8:0B:A2:02:B6:
50:10:AB:5E:B3:B1:7F:E1:D1:EF:A2:47:0E:3A:97:26:06:BF:64:9C:F6:02:C4:14:C6:8F:39:F7:ED:5E:CA:69:71:78:C0:AD:4F:D7:25:C7:03:34:CB:8C:BA:51:D0:72:E1:44:FA:F9:E2:1E:5C:95:
:30:DF:85:A6:EE:75:03:CC:09:B7:B8:B8:2D:34:45:5E:30:6F:0B:78:76:6E:51:68:67:26:17:98:8D:C5:61:45:F5:D0:E2:65:06:2C:8A:F0:1C:EF:D5:30:75:9B:70:10:F6:A1:11:A9:CA:29:FF:A
A:BA:08:C7:2B:0A:01:1F:CC:53:20:33:45:A7:D9:34:4D:69:13:14:5C:8D:C9:02:92:90:95:0E:6B:35:E2:9C:44:F7:C2:0C:4E:EB:A3:4B:76:B4:E5:C5:9C:B9:E9:51:B7:EB:8E:1D:DE:69:68:68
:28:06:DD:1E:31:24:DD:5C:FA:DA:4E:8A:A2:B4:A1:DD:A0:F0:C8:FD:02:7F:12:C6:2B:6E:C1:45:73:1D:F8:9F:68:B4:BE:33:04:8B:70:1D:C9:8B:10:EC:A4:9F:00:80:41:22:95:7B:E7:72:50:
05:06:87:C2:5D:B1:35:D6:3F:3F:B8:1D:31:E5:32:CB:3A:1D:F8:3F:DC:63:EF:55:CD:5E:55:ED:3C:B1:31:AE:02:EF:5E:CF:C3:71:A2:92:65:30:47:45:CA:31:9E:2F:8C:6D:76:5F:5F:CE:7B:D
0:41:F8:87:F8:89:12:F4:13:70:87:FC:F0:E5:A4:9F:A2:D0:35:32:E9:07:B3:50:54:77:57:3D:E6:71:DA:8F:DA:66:E4:E6:AF:57:04:E9:FF:0E:93:0E:88:6A:9F:61:86:C5:46:0D:23:09:00:0F:4F
:3C:26:31:E4:54:C5:44:72:C6:D1:F8:DA:73:8B:30:F0:D5:2C:3A:F1:0F:ED:09:46:2F:93:1C:5F:74:42:81:8E:15:C2:4D:8B:DA:C1:97:1B:36:5F:47:07:02:73:2A:35:60:54:1B:57:63:E7:5E:2
6:95:B3:8D:F0:62:D5:BF:94:3E:E5:4B:11:6F:F8:1C:A3:A1:15:6B:6C:CA:72:D1:0A:92:0C:34:51:33:27:6A:E2:5C:D6:25:52:55:D8:8C:A2:79:47:ED:C1:9D:33:E9:03:78:DE:F3:D7:01:89:9D
:69:81:E0:67:5C:C6:9F:34:A7:60:DB:8A:6F:5E:25:14:A6:C4:CF:C4:AD:FB:07:DB:6A:AF:67:0C:18:A2:E2:16:67:36:E2:0A:23:03:81:22:6B:A2:5A:5B:02:03:01:00:01
```

Authority Info Access

<http://ocsp.ac.ancert.com/ocsp.xuda>

http://www.ancert.com/pki/v2/certs/ANCERTCGN_V2.crt

Authority Key Identifier 05:6E:E1:A1:9A:EE:07:AF:CE:F5:B4:D3:65:3D:04:50:E2:D0:9B:44

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.4.2

CPS pointer: <https://www.ancert.com/cps>

CRL Distribution Points

http://www.ancert.com/crl/ANCERTCGN_V2.crl

http://www2.ancert.com/crl/ANCERTCGN_V2.crl

http://www3.ancert.com/crl/ANCERTCGN_V2.crl

Subject Key Identifier 74:9A:49:8D:DA:48:C6:80:28:D3:48:9B:CE:57:72:91:2A:EB:03:93

Subject Alternative Name *pki.explotacion@ancert.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E7:18:F6:7C:8B:1F:8E:1F:C0:17:6A:36:1C:98:E6:29:9F:D3:F4:39:CF:A4:6E:DD:B4:6A:57:B4:AC:08:B4:43*

X509SubjectName

Subject CN: *ANCERT Certificados para empleados V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2019-08-08T00:00:00Z*

3.5.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

3.5.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.18920.4.2.1.3.1

Description**3.5.3 - History instance n.1 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Reconocidos para empleados del Consejo General del Notariado v.2

Name	[en]	Qualified Certificates for the Spanish Notarial Council employees v.2

Service digital identities**X509SubjectName**

Subject CN:	ANCERT Certificados para empleados V2
Subject O:	Agencia Notarial de Certificacion S.L.U. - CIF B83395988
Subject L:	Paseo del General Martinez Campos 46 6a planta 28010 Madrid
Subject C:	ES

X509SKI

X509 SK I	dJpjjdpIxoAo00ibzldykSrrA5M=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

3.5.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Reconocidos para empleados del Consejo General del Notariado v.2*

Name [en] *Qualified Certificates for the Spanish Notarial Council employees v.2*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados para empleados V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *dJpJdplxoAo00ibzldykSrrA5M=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2010-11-16T00:00:00Z

3.6 - Service (granted): Certificados Reconocidos de Notario v.2

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Authority Info Access	<i>http://ocsp.ac.ancert.com/ocsp.xuda</i> <i>http://www.ancert.com/pki/v2/certs/ANCERTCGN_V2.crt</i>
Authority Key Identifier	<i>05:6E:E1:A1:9A:EE:07:AF:CE:F5:B4:D3:65:3D:04:50:E2:D0:9B:44</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.18920.4.1</i> <i>CPS pointer: https://www.ancert.com/cps</i>
CRL Distribution Points	<i>http://www.ancert.com/crl/ANCERTCGN_V2.crl</i> <i>http://www2.ancert.com/crl/ANCERTCGN_V2.crl</i> <i>http://www3.ancert.com/crl/ANCERTCGN_V2.crl</i>
Subject Key Identifier	<i>5F:93:40:B5:38:08:24:CE:F0:BF:23:4E:B9:2F:95:13:68:AE:84:FB</i>
Subject Alternative Name	<i>pki.explotacion@ancert.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>A8:85:EC:82:18:B1:C9:67:30:B0:26:4E:CF:BB:DE:E0:6C:97:B7:01:FA:F8:0D:CC:B2:69:20:F5:E7:27:AD:73</i>

X509SubjectName

Subject CN:	<i>ANCERT Certificados FERN V2</i>
Subject O:	<i>Agencia Notarial de Certificacion S.L.U. - CIF B83395988</i>
Subject L:	<i>Paseo del General Martinez Campos 46 6a planta 28010 Madrid</i>
Subject C:	<i>ES</i>

Service Status

Service Status		<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

Status Starting Time *2019-08-08T00:00:00Z*

3.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

3.6.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.1.1.3.1

Description

3.6.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] Certificados Reconocidos de Notario v.2

Name [en] Spanish Notaries Qualified Certificates v.2

Service digital identities

X509SubjectName

Subject CN: ANCERT Certificados FERN V2

Subject O: Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Subject L: Paseo del General Martinez Campos 46 6a planta 28010 Madrid

Subject C: ES

X509SKI

X509 SK I X5NAtTglJM7wvyNOuS+VE2iuhPs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

3.6.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos de Notario v.2*

Name *[en]* *Spanish Notaries Qualified Certificates v.2*

Service digital identities**X509SubjectName**

Subject CN: *ANCERT Certificados FERN V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

X509SKI

X509 SK I *X5NAtTgIJM7wvyNOuS+VE2iuhPs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-11-16T00:00:00Z*

3.7 - Service (withdrawn): Certificados Notariales Reconocidos para personas físicas

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[es]* *Certificados Notariales Reconocidos para personas físicas*

Name *[en]* *Qualified Notarial Certificates for individuals*

Service digital identities**Certificate fields details**

Version: *3*

Subject Alternative Name *ancert@ancert.com*

Subject Key Identifier *A5:12:7F:B7:43:DB:51:29:67:C6:76:95:EA:EF:D9:E3:75:C5:C1:35*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D7:90:51:96:05:C9:5A:B0:01:18:BD:98:62:29:0A:E9:AF:02:47:3F:22:33:76:B8:EA:33:D3:1A:60:FE:9F:C5*

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Personales*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

3.7.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.1.1.1*

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.1.2.1*

3.7.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**3.7.3 - History instance n.1 - Status: supervisionceased****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name

[es]

Certificados Notariales Reconocidos para personas físicas

Name

[en]

Qualified Notarial Certificates for individuals

Service digital identities**X509SubjectName**

Subject CN:

ANCERT Certificados Notariales Personales

Subject O:

Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

Subject L:

Paseo del General Martinez Campos 46-6a planta

Subject ST:

Madrid

Subject C:

ES

X509SKI

X509 SK I

pRJ/t0PbUSInxnaV6u/Z43XFWTU=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time**

2015-03-09T23:00:00Z

3.7.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description

[en]

it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.1.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.1.2.1

3.7.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Notariales Reconocidos para personas físicas*

Name [en] *Qualified Notarial Certificates for individuals*

Service digital identities**X509SubjectName**

Subject CN: *ANCERT Certificados Notariales Personales*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *pRj/t0PbUSInxnaV6u/Z43XFwTU=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2004-11-25T00:00:00Z*

3.7.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Tue Feb 22 11:34:42 CET 2011*

Valid to: *Mon Feb 22 11:34:43 CET 2021*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:66:5D:46:B2:DA:19:4B:6D:27:C9:E8:51:8A:CB:3C:8C:5B:1A:3D:DC:8A:F5:E7:C9:FA:5C:3A:ED:3C:63:82:ED:A1:EE:AF:8F:12:55:86:ED:8D:04:60:20:EE:53:00:E7:03:31:6C:73:31:E8:8E:34:05:72:E0:C7:F4:D9:5D:0C:BC:EE:C0:7A:16:17:78:80:68:03:79:11:CD:77:D3:43:E6:20:42:0F:DD:28:31:F5:75:D7:12:31:23:D4:3D:75:2A:BA:6A:30:22:63:D4:D2:98:FC:6A:65:F3:86:F3:08:3F:C7:2B:47:C8:03:40:2C:A7:D1:87:A6:B4:90:42:51:F5:C8:00:9D:E9:3E:89:20:3F:92:51:49:FC:5A:BD:1A:38:6E:6E:ED:F8:FC:89:15:49:C0:1A:B4:8F:64:A3:03:42:37:8A:A4:31:03:48:7D:EF:F6:35:19:83:0F:24:65:78:FA:88:3E:9D:6E:E3:1C:9E:31:93:B3:79:7D:30:45:3E:1F:C5:38:E2:CB:D1:17:C6:F2:87:47:E3:4D:54:C7:07:92:2E:15:05:6E:E9:6C:88:DE:A8:28:25:4F:DC:C7:11:9A:45:ED:37:56:FD:97:9C:01:C8:B1:E9:CB:87:46:EC:27:72:4E:04:F1:6C:2C:DB:38:9A:C6:DE:B5:59:02:03:01:00:01

Authority Key Identifier *84:F7:FA:72:5E:88:64:66:1D:28:8C:B0:77:BD:0C:6A:9F:4C:4D:62*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies
Policy OID: 1.3.6.1.4.1.18920.1.3
CPS pointer: <http://www.ancert.com/cps>
CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]

CRL Distribution Points
<http://www.ancert.com/crl/ANCERTNOT.crl>
<http://www2.ancert.com/crl/ANCERTNOT.crl>
<http://www3.ancert.com/crl/ANCERTNOT.crl>

Subject Alternative Name *ancert@ancert.com*

Subject Key Identifier *51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *39:35:94:82:D2:AE:7D:F8:48:A1:E5:6D:E1:84:EB:9B:FA:B9:D9:83:09:C3:CD:2E:D0:97:A1:8C:BE:07:F2:40*

Certificate fields details

Version: *3*

Serial Number: *126356436681186619492921660190540379841*

Subject Key Identifier *51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *13:77:15:68:2F:A1:69:5F:25:EA:BC:C0:21:60:B7:2E:34:ED:9A:D3:E9:68:9E:17:7E:2A:E4:3F:83:3E:FC:13*

X509SubjectName

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2018-02-15T01:00:00Z*

3.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1*

3.8.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.18920.1.3.2.1*

3.8.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.8.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Notarial Certificates for legal person*

Name [es] *Certificados Notariales Reconocidos para personas jurídicas*

Service digital identities**X509SubjectName**

Subject CN: *ANCERT Certificados Notariales Corporativos*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *URorbi/OSjhedaI2Ue6MN10TjK0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.8.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.1.3.1.1*

3.8.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	[en]	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	[es]	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.1.3.2.1*

3.8.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.8.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	<i>Qualified Notarial Certificates for legal person</i>
Name	[es]	<i>Certificados Notariales Reconocidos para personas jurídicas</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>ANCERT Certificados Notariales Corporativos</i>
Subject O:	<i>Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988</i>
Subject L:	<i>Paseo del General Martinez Campos 46-6a planta</i>

Subject ST: Madrid

Subject C: ES

X509SKI

X509 SK I URorbi/OSjhedaI2Ue6MN10TjK0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2004-11-25T00:00:00Z

3.8.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

3.8.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.1.3.2.1

Version:	3
Serial Number:	141846559623262997341610771385374835874
X509 Certificate	-----BEGIN CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *ANCERT Certificados CGN*

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Issuer C: *ES*

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Thu Feb 12 16:03:47 CET 2004*

Valid to: *Sun Feb 12 16:03:39 CET 2012*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D7:A0:84:CC:F5:03:17:87:24:93:6B:4A:7D:80:22:18:E1:52:4B:D1:42:04:E9:35:3F:6F:13:25:A1:00:3A:8E:98:77:68:40:05:BF:0E:7D:15:30:28:AB:D9:4B:61:6E:2F:85:B2:FC:C8:24:6E:EE:F5:7D:12:74:13:C7:BF:F8:BA:52:80:09:D2:A5:A4:27:23:C8:D0:89:78:74:26:39:36:23:1C:6C:AF:CF:83:D2:95:85:06:41:D3:4D:A5:E8:87:5C:33:88:30:00:41:85:55:A8:93:2A:13:F2:74:68:C9:60:B1:56:A3:BF:C7:23:2F:58:A6:05:24:57:CE:CD:A9:1F:59:F0:8C:27:5B:A6:C3:8F:96:D5:1C:CC:4C:F5:00:84:A5:A5:60:FA:80:03:86:18:E4:B1:7B:47:63:0F:0E:5B:67:07:F0:43:2D:17:EB:BC:E9:23:75:C6:BE:5A:EE:38:99:E9:11:A4:47:9E:C5:28:7E:5B:D3:0A:EC:FD:95:DE:34:0C:9A:87:5D:5B:6A:63:30:3D:29:77:95:59:E9:EC:E8:32:C6:A8:9C:79:2B:08:0C:44:ED:07:2D:17:2B:F7:DC:2E:68:CF:48:68:E5:B4:E1:85:4C:33:2B:6E:5E:3B:64:D3:1E:C3:1E:1D:F8:E1:86:E2:B4:3B:D1:D9:02:03:01:00:01

Authority Key Identifier *EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies
Policy OID: 1.3.6.1.4.1.18920.4.2
CPS pointer: <http://www.ancert.com/cps>
CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]

CRL Distribution Points
<http://www.ancert.com/crl/ANCERTCGN.crl>
<http://www2.ancert.com/crl/ANCERTCGN.crl>
<http://www3.ancert.com/crl/ANCERTCGN.crl>

Subject Alternative Name *ancert@ancert.com*

Subject Key Identifier *56:3D:DB:0E:C5:F0:3D:D3:54:B0:03:A0:E1:FD:DB:67:9F:7D:09:AF*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *56:3D:81:58:24:D9:1A:E6:BA:83:AE:08:6A:B5:29:59:80:7D:51:09:8C:25:75:93:38:A3:7D:28:0E:7D:8B:A1*

X509SubjectName

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: Paseo del General Martinez Campos 46-6a planta

Subject ST: Madrid

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2018-02-15T01:00:00Z

3.9.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.2.1.1

3.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.9.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates for the Spanish Notarial Council employees

Name [es] Certificados Reconocidos para empleados del Consejo General del Notariado

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

3.9.3.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] [es]	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i> <i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

3.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.9.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates for the Spanish Notarial Council employees*

Name [es] *Certificados Reconocidos para empleados del Consejo General del Notariado*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados para empleados*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2004-11-24T23:00:00Z*

3.9.4.3 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

3.10 - Service (withdrawn): Qualified Certificates for Public Corporations

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Certificate Policies*Policy OID: 1.3.6.1.4.1.18920.3.1**CPS pointer: <http://www.ancert.com/cps>**CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]***CRL Distribution Points***<http://www.ancert.com/crl/ANCERTPUB.crl>**<http://www2.ancert.com/crl/ANCERTPUB.crl>**<http://www3.ancert.com/crl/ANCERTPUB.crl>***Subject Alternative Name***ancert@ancert.com***Subject Key Identifier***90:8C:75:66:37:AE:74:23:3A:5A:D8:27:C1:A2:56:CB:EB:D5:2B:90***Key Usage:***digitalSignature - keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***60:66:75:6C:46:17:4D:9A:4F:CB:86:86:73:35:86:51:87:F8:A4:96:BD:EF:A4:6A:FB:DA:B2:9A:18:70:B6:B4***X509SubjectName****Subject CN:***ANCERT Certificados para Corporaciones de Derecho Publico***Subject O:***Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988***Subject L:***Paseo del General Martinez Campos 46-6a planta***Subject ST:***Madrid***Subject C:***ES***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2016-06-30T22:00:00Z***3.10.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]****Qualifier type description** [en]*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.18920.3.1.1.1*

3.10.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.10.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates for Public Corporations*

Name [es] *Certificados Reconocidos para Corporaciones de Derecho Público*

Service digital identities**X509SubjectName**

Subject CN: *ANCERT Certificados para Corporaciones de Derecho Publico*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *klx1ZjeudCM6WtgnwaJWy+vVK5A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-03-09T23:00:00Z*

3.10.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	<i>[en]</i>	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	<i>[es]</i>	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.18920.3.1.1.1*

3.10.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualifed Certificates for Public Corporations*

Name *[es]* *Certificados Reconocidos para Corporaciones de Derecho Público*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados para Corporaciones de Derecho Publico*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *klx1ZjeudCM6WtgnwaJWy+vVK5A=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.10.4.2 - Extension (critical): Qualifiers [QCStatement]

[es]

Criteria list assert=atLeastOne

Identifier

urn:oid:1.3.6.1.4.1.18920.3.1.1.1

Service Type Identifier

Service type description [en]

[es]

Name [en]

Name [es]

Certificate fields details

Version:

3

Serial Number:

41933658679553044710456659287286375906

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer CN:

ANCERT Certificados CGN

Issuer O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Issuer C: *ES*
Subject CN: *ANCERT Certificados FERN*
Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*
Subject L: *Paseo del General Martinez Campos 46-6a planta*
Subject ST: *Madrid*
Subject C: *ES*
Valid from: *Thu Feb 12 15:53:10 CET 2004*
Valid to: *Wed Feb 12 15:53:02 CET 2014*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:92:4F:82:14:E3:C1:78:92:57:AA:A0:E4:28:99:D6:48:3C:C9:08:2E:75:AD:CB:1A:5D:F2:FA:35:C3:F1:74:5E:66:A6:93:0F:4D:BA:8A:A2:3D:6C:33:4B:62:CF:0A:7D:95:B8:7A:17:5A:71:9F:A0:5D:19:6C:66:20:F2:49:AB:85:68:AS:DF:3E:94:23:83:C2:09:C6:C9:ACA:B:2B:E9:BD:76:7D:CD:5B:33:2E:74:2F:9E:C3:F5:79:EE:5D:84:53:C9:6B:EE:E8:9B:2D:E3:F3:2D:DE:07:05:3C:4B:E2:3A:96:29:E2:6C:5D:F3:09:8A:8B:B4:A5:72:E9:0E:3E:A1:7A:C7:92:C5:B1:31:71:AC:4F:0C:42:4F:B4:77:FB:0E:09:81:CB:87:44:80:38:8C:BE:8B:8C:22:37:1E:B7:87:5F:17:25:1A:93:7B:C4:86:38:D2:B5:F9:FB:BE:B3:3A:B9:94:BD:4A:FC:17:50:7F:B3:8F:B6:06:16:E5:31:BE:50:96:5A:F6:3C:F3:16:EC:7A:0A:42:1C:1A:FC:C6:9F:1F:14:03:DA:EF:94:48:81:01:EF:C3:8F:2C:BB:A5:1E:25:F0:5B:55:F3:8D:4A:F7:86:64:87:BA:F8:20:62:3D:57:61:64:C9:EC:F3:8D:83:28:AC:BD:11:95:02:03:01:00:01*
Authority Key Identifier *EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*
Basic Constraints *IsCA: true - Path length: 0*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18920.4.1*
CPS pointer: <http://www.ancert.com/cps>
CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]
CRL Distribution Points *<http://www.ancert.com/crl/ANCERTCGN.crl>*
<http://www2.ancert.com/crl/ANCERTCGN.crl>
<http://www3.ancert.com/crl/ANCERTCGN.crl>
Subject Alternative Name *ancert@ancert.com*
Subject Key Identifier *99:E5:5C:82:BA:18:E5:8C:F7:88:1B:DE:D0:C2:AD:6D:46:B2:B8:A6*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *76:C5:27:32:7D:E2:A2:E3:CD:8C:1B:A8:58:2E:EB:C7:18:88:E1:13:06:01:9F:D8:7F:18:D7:7E:55:FC:85:4E*
X509SubjectName
Subject CN: *ANCERT Certificados FERN*
Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: Paseo del General Martinez Campos 46-6a planta

Subject ST: Madrid

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2016-06-30T22:00:00Z

3.11.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18920.4.1.1.1

3.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.11.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Spanish Notaries Qualified Certificates

Name [es] Certificados Reconocidos de Notario

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados FERN*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *meVcgroY5Yz3iBve0MKtbUayuKY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-03-09T23:00:00Z*

3.11.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.4.1.1.1*

3.11.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Spanish Notaries Qualified Certificates*

Name [es] *Certificados Reconocidos de Notario*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Certificados FERN*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *meVcgroY5Yz3iBve0MKtbUayuKY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2004-11-25T00:00:00Z*

3.11.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	[es]	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18920.4.1.1.1*

3.12 - Service (withdrawn): Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name	[es]	<i>Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»</i>
Name	[en]	<i>Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»</i>

Authority Key Identifier	<i>DB:35:B9:31:1F:FD:F7:7C:C3:17:0D:C9:CB:C8:55:0B:EA:15:7C:0A</i>
Basic Constraints	<i>IsCA: false</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.18920.1.2.3.3.1</i>
CRL Distribution Points	<i>http://www.ancert.com/crl/ANCERTCS_V2.crl</i> <i>http://www2.ancert.com/crl/ANCERTCS_V2.crl</i> <i>http://www3.ancert.com/crl/ANCERTCS_V2.crl</i>
Subject Key Identifier	<i>5A:A8:47:D1:6F:86:F3:86:AF:CD:FB:B1:9D:87:41:78:15:C0:E1:95</i>
Subject Alternative Name	<i>pki.explotacion@ancert.com</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>26:AE:01:6C:AC:51:81:94:43:93:AC:4E:06:0E:44:FD:AE:A1:34:7A:0C:18:D8:CC:B1:65:BF:80:EF:A5:80:AE</i>

X509SubjectName

Subject CN:	<i>ANCERT Qualified Time-stamp Authority G2</i>
Subject 2.5.4.97:	<i>VATES-B83395988</i>
Subject O:	<i>Agencia Notarial de Certificación S.L. Unipersonal</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>WqhH0W+G84avzfuxnYdBeBXA4ZU=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2026-05-20T03:00:00Z</i>

3.12.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name <i>[es]</i>	<i>Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»</i>

Name [en] *Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»*

Service digital identities

X509SubjectName

Subject CN: *ANCERT Qualified Time-stamp Authority G2*

Subject 2.5.4.97: *VATES-B83395988*

Subject O: *Agencia Notarial de Certificación S.L. Unipersonal*

Subject C: *ES*

X509SKI

X509 SK I *WqhH0W+G84avzfuxnYdBeBXA4ZU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-10-23T02:00:00Z*

3.13 - Service (granted): Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G3 (TSA/TSU)»

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G3 (TSA/TSU)»*

Name [es] *Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G3 (TSA/TSU)»*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *145149370721419421080210732569931012876*

CRL Distribution Points
http://www.ancert.com/crl/ANCERTCS_V2.crl
http://www2.ancert.com/crl/ANCERTCS_V2.crl
http://www3.ancert.com/crl/ANCERTCS_V2.crl

Subject Key Identifier 89:FE:A3:4D:2D:28:6F:7C:1F:74:08:FA:83:93:9D:37:20:23:A5:D9

Subject Alternative Name pki.explotacion@ancert.com

Key Usage: digitalSignature

Thumbprint algorithm: SHA-256

Thumbprint: FA:5D:65:4B:DE:85:11:94:77:02:9D:CA:CF:C3:2F:3F:9E:DE:91:21:05:14:1A:3F:11:A2:2A:B3:33:CA:39:49

X509SubjectName

Subject CN: Qualified Time-stamp Authority G3

Subject 2.5.4.97: VATES-B83395988

Subject O: Agencia Notarial de Certificación S.L.Unipersonal

Subject C: ES

X509SKI

X509 SK I if6jTS0ob3wfdAj6g5OdNyAjpdk=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
 [es] undefined.

Status Starting Time 2024-12-03T00:00:00Z

3.14 - Service (granted): Qualified certificates issued by Centro Tecnológico del Notariado CA-QC Corporativos

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
 [es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified certificates issued by Centro Tecnológico del Notariado CA-QC Corporativos

Authority Key Identifier	<i>4A:86:C0:25:B1:43:28:63:50:04:FD:A6:29:AA:20:D5:E1:0D:D2:ED</i>
Authority Info Access	<i>http://tsp.ctnotariado.com/cacerts/CTNotariadoRootCA-QC.cer</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://tsp.ctnotariado.com/cps</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
CRL Distribution Points	<i>http://tsp.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl</i> <i>http://tsp2.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl</i>
Subject Key Identifier	<i>95:63:65:45:F4:75:E8:AB:C7:46:E2:32:74:54:CC:32:53:EF:DE:0A</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>39:E3:79:DB:8A:2F:67:CC:5C:6E:8C:CF:E0:52:6C:74:ED:D9:77:E9:F8:55:04:2F:32:E2:1C:54:6E:0F:14:8C</i>

X509SubjectName

Subject CN:	<i>Centro Tecnológico del Notariado CA-QC Corporativos</i>
Subject 2.5.4.97:	<i>VATES-B83395988</i>
Subject O:	<i>Agencia Notarial de Certificación S.L. Unipersonal</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>IWNIRfR16KvHRuIydFTMMIPv3go=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2025-10-02T02:00:00Z</i>

3.14.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

Subject O: *Agencia Notarial de Certificación S.L. Unipersonal*

Subject C: *ES*

Valid from: *Wed Mar 12 12:31:21 CET 2025*

Valid to: *Sat Mar 10 12:11:05 CET 2035*

Public Key:

```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C6:A0:9B:E5:E7:0C:87:70:8B:4B:07:5B:4E:74:CA:38:37:72:ED:8D:75:12:FE:
62:70:0F:ED:B3:6C:E3:2A:0B:DC:2A:11:15:84:FC:CB:77:C8:07:7B:77:AB:DE:A0:10:FA:CB:1C:F8:CB:06:61:ED:B2:E6:A9:81:F4:1F:EE:EF:03:33:35:77:05:CD:3A:20:65:80:4E:8B:C8:BF:3
D:79:F7:95:EA:36:80:8D:A9:D4:66:FB:50:09:00:CD:94:64:AF:CB:AB:17:4C:1A:E2:C1:B4:E9:8A:38:68:66:33:EA:FA:72:8B:FD:1E:2C:0D:25:9C:18:FE:C8:86:17:F2:80:9D:31:53:93:15:2E
22:A5:F6:57:52:92:81:33:8A:C4:94:3D:EF:C9:31:29:DA:ED:F8:9D:18:3F:10:90:E3:58:C3:9D:F3:98:94:DE:6A:8D:E5:F8:66:32:39:9B:93:78:C1:51:54:BF:BC:76:9A:3D:13:E2:F1:AE:0D:2
0:1A:D0:88:27:26:3C:50:F1:B0:1B:C4:2D:2B:DD:AB:D5:27:69:84:F4:12:26:1B:57:E5:BE:82:55:21:8C:C2:9A:F9:1D:1E:FC:59:59:FA:59:93:D0:FC:2A:69:72:53:11:EF:E3:44:03:5F:D4:73
05:7D:38:A4:1D:E3:4F:12:A1:C3:EA:D6:38:AB:76:81:F6:E0:CF:32:36:38:62:E6:5F:97:15:AA:B4:CC:B3:9C:D0:14:3E:65:F6:C2:03:59:F6:A7:83:A9:C5:D8:99:11:FD:0D:01:D6:57:5A:AE:0
2:A9:58:F1:F7:D5:A5:5B:C9:9B:CD:7D:C9:81:D8:3C:FD:FA:83:ED:AD:6A:59:0F:40:FA:C8:79:74:12:C2:C5:B5:29:40:9B:AC:6A:4B:37:BA:AD:06:A9:45:B2:8E:37:AB:92:F8:42:87:79:E8:D
6:D6:E3:AF:9F:5E:85:CF:64:82:AB:C1:D8:62:C8:74:7D:1F:FD:4C:80:05:37:38:C6:E7:D3:85:AE:98:85:B6:74:60:54:D9:7E:AC:73:36:14:C7:91:1A:64:36:26:45:6D:C6:8D:7C:35:57:7D:C
A:65:73:F1:F7:5C:CD:7F:05:D6:B6:C4:73:2C:F6:01:46:45:28:91:E5:6B:D0:68:91:8E:13:DC:A6:FD:C5:A9:1B:A3:AC:AC:BB:04:DD:F8:D6:88:48:A9:E9:5F:91:3C:D6:9B:0A:54:80:7B:9B:E
5:3F:C1:02:52:05:F3:B1:8F:65:AA:B4:52:55:2A:50:57:E4:70:52:1A:92:24:DD:8F:3A:38:C0:F5:59:46:E7:F7:65:EA:31:27:AF:F7:F4:D6:64:DB:2C:D1:22:A3:02:03:01:00:01
```

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *4A:86:C0:25:B1:43:28:63:50:04:FD:A6:29:AA:20:D5:E1:0D:D2:ED*

Authority Info Access *<http://tsp.ctnotariado.com/cacerts/CTNotariadoRootCA-QC.cer>*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://tsp.ctnotariado.com/cps>

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *<http://tsp.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl>*
<http://tsp2.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl>

Subject Key Identifier *FD:08:C9:85:4F:83:DA:38:0D:A4:15:B7:D5:E9:82:0A:19:99:1F:C2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DC:27:26:48:C1:F4:7B:25:94:D1:17:48:5C:66:CA:F2:ED:48:06:09:9C:89:EC:35:6D:C4:36:FC:19:BC:C3:BB*

X509SubjectName

Subject CN: *Centro Tecnológico del Notariado CA-QC No Corporativos*

Subject 2.5.4.97: *VATES-B83395988*

Subject O: *Agencia Notarial de Certificación S.L. Unipersonal*

Subject C: *ES*

X509SKI

X509 SK I */QjJhU+D2jgNpBW31emCChmZH8I=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-10-02T02:00:00Z

3.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.15.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

3.16 - Service (granted): Qualified electronic timestamps issued by Centro Tecnológico del Notariado QTSA G1

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified electronic timestamps issued by Centro Tecnológico del Notariado QTSA G1

Name [es] Sellos cualificados de tiempo electrónico emitidos por Centro Tecnológico del Notariado QTSA G1

Service digital identities

Certificate fields details

Version: 3

Serial Number: 646583246195332779307327357024710998860821620940

Subject Key Identifier *9B:EE:C2:C5:53:5B:F3:F4:FC:2F:F8:0A:30:8E:5F:4B:AA:19:C8:A1*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C2:49:15:C7:D5:C7:2C:8A:CE:58:94:E6:D5:E8:15:3E:80:D8:1B:BA:F0:7E:FE:9C:C9:8C:27:E4:75:4F:7D:FD*

X509SubjectName

Subject CN: *Centro Tecnológico del Notariado QTSA G1*

Subject 2.5.4.97: *VATES-B83395988*

Subject O: *Agencia Notarial de Certificación S.L. Unipersonal*

Subject C: *ES*

X509SKI

X509 SK I *m+7CxVNB8/T8L/gKMI5fS6oZyKE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-10-02T02:00:00Z*

4 - TSP: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio (FNMT-RCM)

TSP Name

Name	[en]	<i>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio (FNMT-RCM)</i>
Name	[es]	<i>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio (FNMT-RCM)</i>

TSP Trade Name

Name	[en]	<i>VATES-Q2826004J</i>
Name	[en]	<i>CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)</i>
Name	[es]	<i>CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)</i>
Name	[en]	<i>FNMT</i>
Name	[es]	<i>FNMT</i>
Name	[en]	<i>FNMT-RCM</i>
Name	[es]	<i>FNMT-RCM</i>
Name	[en]	<i>FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA</i>
Name	[es]	<i>FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA</i>
Name	[en]	<i>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, E.P.E, M.P (FNMT-RCM)</i>

PostalAddress

Street Address	[en]	<i>C/ Jorge Juan, 106</i>
Locality	[en]	<i>Madrid</i>
State Or Province	[en]	<i>Madrid</i>
Postal Code	[en]	<i>28009</i>
Country Name	[en]	<i>ES</i>

PostalAddress

URI	[en]	http://www.cert.fnmt.es
URI	[en]	mailto:ceres@fnmt.es

URI	[en]	http://www.cert.fnmt.es/en/home
URI	[es]	http://www.cert.fnmt.es

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[en]	Qualified certificates for individuals issued by FNMT-RCM
Name	[es]	Certificados reconocidos para personas físicas emitidos por la FNMT-RCM

Version: 3

Serial Number: 921770777

[illegible]

Signature algorithm: *SHA1withRSA*

Issuer OU: *FNMT Clase 2 CA*

Issuer O: *FNMT*

Issuer C: *ES*

Subject OU: *FNMT Clase 2 CA*

Subject O: *FNMT*

Subject C: *ES*

Valid from: *Thu Mar 18 15:56:19 CET 1999*

Valid to: *Mon Mar 18 16:26:19 CET 2019*

Public Key: *30:81:9D:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:81:8B:00:30:81:87:02:81:81:00:98:3F:AD:19:36:93:3D:3E:FE:76:42:14:FD:35:6F:F1:FA:AD:22:7A:58:E3:46:D0:5D:C6:5A:F9:62:2D:8F:31:5E:FE:B4:30:FE:50:74:AC:D6:90:1D:E0:62:C6:49:DD:14:12:7D:71:0B:AC:06:C1:3F:D7:06:87:E0:90:89:D6:E5:E3:03:B2:F2:27:B1:9F:33:C8:AA:68:36:4A:A3:C4:3F:79:41:9D:89:46:2F:28:3E:63:D4:38:56:91:AA:1D:B1:0D:42:75:4D:F3:87:4E:E3:0F:4D:CC:B4:6C:BF:62:13:87:EA:D0:98:8E:B6:E2:FF:19:F4:94:09:D5:96:61:02:01:03*

CRL Distribution Points *C=ES,O=FNMT,OU=FNMT Clase 2 CA,CN=CRL1*

Authority Key Identifier *40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*

Subject Key Identifier *40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*

Basic Constraints *IsCA: true*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *62:B9:26:72:66:21:28:32:A8:E2:2D:AB:93:3D:91:C7:01:12:74:AC:F7:17:03:F9:C
C:97:83:37:51:A6:E9:4F*

X509SubjectName

Subject OU: *FNMT Clase 2 CA*

Subject O: *FNMT*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2017-09-12T00:00:00Z*

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

TSP Service Definition URI

URI [en] <http://www.ceres.fnmt.es/dpc>

URI [es] <http://www.ceres.fnmt.es/dpc>

4.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.1.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified certificates for individuals issued by FNMT-RCM*

Name [es] *Certificados reconocidos para personas físicas emitidos por la FNMT-RCM*

Service digital identities

X509SubjectName

Subject OU: *FNMT Clase 2 CA*

Subject O: *FNMT*

Subject C: *ES*

X509SKI

X509 SK I *QJp2Rjd0B8SsFMsejU86RXww12E=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

4.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates for individuals issued by FNMT-RCM

Name	[es]	Certificados reconocidos para personas físicas emitidos por la FNMT-RCM

Service digital identities**X509SubjectName**

Subject OU:	FNMT Clase 2 CA

Subject O:	FNMT

Subject C:	ES

X509SKI

X509 SK I	QJp2Rjd0B8SsFMsejU86RXww12E=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2004-11-25T00:00:00Z

4.2 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[es]	Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes

Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities

Service digital identities

Certificate fields details

Version: 3

Serial Number: 16

X509 Certificate -----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject OU: *AC APE*

Subject O: *FNMT-RCM*

Subject C: ES

Valid from: *Wed Nov 05 13:18:40 CET 2008*

Valid to: *Fri Nov 03 16:38:33 CET 2023*[illegible]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier 63:4B:74:5B:07:BF:E8:66:D1:5A:2C:5F:CB:F9:79:6E:A0:8C:AE:27

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.cert.fnmt.es/dpcs/>

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

FD:01:90:1F:E7:C4:F5:14:D6:36:DF:64:C0:74:4A:A4:02:9D:B9:16:A3:6F:28:47:4C:84:0E:68:07:93:6A:1E

X509SubjectName**Subject OU:**

AC APE

Subject O:

FNMT-RCM

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI**URI** [en]

https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

URI [es]

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

TSP Service Definition URI**URI** [es]

http://www.ceres.fnmt.es/dpc

URI [en]

http://www.ceres.fnmt.es/dpc

4.2.1 - Extension (critical): Qualifiers [NotQualified]**Qualifier type description** [en]

undefined.

[es]

undefined.

Criteria list assert=atLeastOne**Policy Identifier:****Identifier**

[OIDsURN]

urn:oid:1.3.6.1.4.1.5734.3.13

4.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**4.2.3 - History instance n.1 - Status: supervisionceased****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[es]

*Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes***Name**

[en]

*Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities***Service digital identities****X509SubjectName****Subject OU:**

AC APE

Subject O:

FNMT-RCM

Subject C:

ES

X509SKI**X509 SK I**

Y0t0Wwe/6GbRWixfy/I5bqCMric=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time**

2016-05-29T22:00:00Z

4.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]**Qualifier type description** [en]*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es]

*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.***Criteria list assert=atLeastOne**

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.5734.3.13

4.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*

Name [en] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

Service digital identities**X509SubjectName**

Subject OU: AC APE

Subject O: FNMT-RCM

Subject C: ES

X509SKI

X509 SK I Y0t0Wwe/6GbRWixfy/I5bqCMric=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2010-06-07T00:00:00Z

4.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne**Policy Identifier:**

Public Key:

30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:9F:76:2A:75:63:52:3B:64:69:10:65:1C:90:C0:85:7A:E2:65:F9:FF:2D:25:2E:BD:5B:D7:B9:F9:49:FD:AF:0A:29:07:81:89:C1:2A:FF:45:FE:12:63:00:1D:E8:F3:E7:60:0C:2C:4A:87:FC:CE:4A:E4:92:1D:4D:02:19:B3:9A:9B:38:00:37:6B:E2:80:28:56:F4:51:69:92:B9:6E:EB:BC:A4:23:59:C7:DD:C8:04:F7:80:8F:A3:F1:A7:CC:F1:FB:3C:CF:79:9A:E2:62:EA:AD:54:87:70:04:E4:8C:E8:3C:C9:A3:37:9B:57:0A:6C:E9:90:8B:79:27:F4:73:81:02:03:01:00:01

Basic Constraints

IsCA: true

Subject Key Identifier

F3:D8:1C:CC:5B:ED:FD:47:0F:42:E3:C0:DE:54:73:D4:99:6F:48:EF

Certificate Policies

Policy OID: 1.3.6.1.4.1.5734.3.8

CPS pointer: <http://www.cert.fnmt.es/dpcs/fm/dpc.pdf>

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/Jorge Juan 106- 28009-Madrid-España)]

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

51:EC:D3:8A:33:C7:B4:93:12:97:95:97:20:AF:B3:E9:E7:CD:41:CD:C1:70:09:52:D1:95:88:BD:EC:79:DF:87

X509SubjectName**Subject OU:**

AC FIRMA MOVIL

Subject O:

FNMT

Subject C:

ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI [en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

TSP Service Definition URI

URI [en]

<http://www.ceres.fnmt.es/dpc>

URI [es]

<http://www.ceres.fnmt.es/dpc>

4.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**4.3.2 - History instance n.1 - Status: supervisionceased****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[es]

*Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles***Name**

[en]

*Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones***Service digital identities****X509SubjectName****Subject OU:**

AC FIRMA MOVIL

Subject O:

FNMT

Subject C:

ES

X509SKI**X509 SK I**

89gczFvt/UcPQuPA3IRz1JlvSO8=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time**

2015-02-24T23:00:00Z

4.3.3 - History instance n.2 - Status: undersupervision**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[es]

*Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles***Name**

[en]

*Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones***Service digital identities****X509SubjectName****Subject OU:**

AC FIRMA MOVIL

Issuer OU: AC RAIZ FNMT-RCM
Issuer O: FNMT-RCM
Issuer C: ES
Subject CN: AC Administración Pública
Subject SERIAL NUMBER: Q2826004J
Subject OU: CERES
Subject O: FNMT-RCM
Subject C: ES
Valid from: Fri May 21 11:26:24 CEST 2010
Valid to: Sat May 21 11:52:26 CEST 2022
Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:CA:4F:C3:75:DC:CE:83:D5:61:EF:BF:2A:70:94:DB:EF:F2:00:BF:2D:24:57:D9:9A:D7:C2:F8:1F:53:FA:09:48:C9:F4:4D:70:1F:08:07:70:21:46:0D:F2:DD:06:A1:F4:51:56:FE:E6:E4:00:F5:95:58:34:E2:C3:FE:79:E2:BA:5A:99:7B:F3:83:92:88:27:9E:10:F9:06:08:CD:DF:2D:2F:39:8F:3C:59:2D:86:77:D1:A0:C4:32:E3:17:78:F7:C4:71:14:F6:2F:AD:37:B4:F8:87:91:E1:B1:A2:CA:88:67:93:B4:81:59:25:91:9C:1F:4D:D9:BC:87:2A:6C:7B:E3:51:EC:3B:1E:2D:C3:CA:E3:04:DD:98:97:16:C7:03:7E:C5:E5:16:53:3D:48:70:77:AB:8B:AB:44:FA:92:C3:65:A7:BA:1C:96:47:98:AC:27:85:09:8E:02:6A:C0:8E:0D:F4:D7:F0:48:63:98:8B:E5:9F:50:00:08:EF:2C:7E:EA:A7:8A:29:05:4B:17:8D:87:57:92:8C:34:98:63:D0:1F:5A:31:CF:92:88:04:89:A3:F4:33:8B:85:96:10:21:71:7E:46:0A:1F:0A:12:39:7D:67:D3:9B:02:F9:1D:E0:9A:E1:EC:E4:1C:9F:DB:F3:D9:E2:D6:98:F3:BA:C1:02:03:01:00:01
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier 14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D
Authority Key Identifier F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.cert.fnmt.es/dpcs/>
CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]
Authority Info Access *<http://ocspape.cert.fnmt.es/ocspape/OcspResponder>*
<http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt>
CRL Distribution Points *<ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>*
<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 18:A4:3C:51:D0:81:74:C3:A6:D8:5F:1C:13:18:BD:29:09:75:3E:75:D9:1C:F6:59:9F:73:34:7B:00:70:28:90

Certificate fields details

Authority Info Access
<http://ocspape.cert.fnmt.es/ocspape/OcspResponder>
<http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt>

CRL Distribution Points
<ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>
<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>

Key Usage:
 keyCertSign - cRLSign

Thumbprint algorithm:
 SHA-256

Thumbprint:
 83:0F:F2:05:AE:69:48:50:59:C3:FB:23:76:A7:F2:F9:EE:1C:2A:61:DE:25:9D:D0:9D:0B:B6:AD:69:F8:88:32

X509SubjectName

Subject CN:
 AC Administración Pública

Subject SERIAL NUMBER:
 Q2826004J

Subject OU:
 CERES

Subject O:
 FNMT-RCM

Subject C:
 ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
 [es] undefined.

Status Starting Time
 2022-10-10T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

TSP Service Definition URI

URI [en] <http://www.ceres.fnmt.es/dpc>

URI [es] <http://www.ceres.fnmt.es/dpc>

4.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
 [es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.5734.3.3.3.2

4.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

4.4.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.5734.3.3.10.1

Description		

4.4.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

4.4.6 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name	

Name *[es]* *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

Name *[en]* *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

X509SubjectName

Subject CN: *AC Administración Pública*

Subject SERIAL NUMBER: *Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *FBHitSu5jJitaNMxVEDkWF8DG30=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-07-15T00:00:00Z*

4.4.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.4.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.4.6.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

4.4.6.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.5734.3.3.10.1

Description		

4.4.6.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

4.4.7 - History instance n.2 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	<i>Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)</i>

Name	[en]	<i>Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>AC Administración Pública</i>

Subject SERIAL NUMBER:	<i>Q2826004J</i>

Subject OU:	<i>CERES</i>

Subject O:	<i>FNMT-RCM</i>

Subject C: ES

X509SKI

X509 SK I FBHitSu5jjitaNMxVEDkWF8DG30=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2017-09-27T10:00:00Z

4.4.7.6 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.3.2

4.4.7.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.4.7.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

4.4.7.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.10.1

Description

4.4.8 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

Name *[en]* *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities**X509SubjectName**

Subject CN: *AC Administración Pública*

Subject SERIAL NUMBER: *Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *FBHitSu5jjitaNMxVEDkWF8DG30=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

4.4.8.10 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

4.4.8.11 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.4.9 - History instance n.4 - Status: undersupervision

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

Name [en] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

Service digital identities

X509SubjectName

Subject CN: AC Administración Pública

Subject SERIAL NUMBER: Q2826004J

Subject OU: CERES

Subject O: FNMT-RCM

Subject C: ES

X509SKI

X509 SK I FBHitSu5jjitaNMxVEDkWF8DG30=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2011-07-27T00:00:00Z

4.4.9.12 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Tue Nov 02 13:44:11 CET 2010*

Valid to: *Sun Nov 02 13:44:11 CET 2025*

Public Key:

30:82:02:22:30:00:06:09:2A:86:4B:8F:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:7A:00:BE:68:09:B9:58:7F:EA:4C:4A:33:81:D8:8F:59:DB:85:B2:ED:D1:2D:9C:7D:54:72:0C:98:D7:75:21:4B:E0:F2:16:C2:AC:EC:F4:F4:32:E0:3E:AB:65:9C:95:AB:AC:53:DA:D7:18:3C:8E:6F:81:FF:91:BD:22:FF:6D:69:00:63:A8:E4:F0:E8:90:33:D1:62:F4:07:CC:D E:7B:15:66:B9:5A:DE:0C:E6:43:BF:49:8D:4A:97:18:3D:1E:FB:A6:67:D6:50:CF:00:4D:AF:62:C6:55:38:F3:B4:2E:E9:D6:EC:E0:33:F9:55:49:77:3B:D9:73:F8:DF:59:93:59:EE:42:45:3C:00: 45:50:5F:79:F7:06:86:49:AF:F2:FA:E9:05:FA:05:1D:7E:24:7F:D3:DE:2B:5D:1E:A1:9C:76:EE:E4:B3:06:E6:65:71:5C:79:01:2F:64:1E:54:6E:29:63:E4:E1:CB:F8:CC:3A:3E:25:17:D2:DE:63: 07:44:31:AC:82:24:35:6E:59:31:44:C1:61:2E:02:F0:60:9C:A5:9F:C5:21:DD:55:36:09:56:24:F5:8D:31:50:51:88:8A:98:81:F2:E1:6D:8A:37:49:8C:76:BD:0C:02:F9:E4:5E:3B:15:5A:C8:E1 :AA:2D:5C:87:E6:C4:A7:94:76:5A:F8:78:DC:AB:47:67:C9:5F:C0:8E:7A:B6:45:0C:ED:04:01:15:38:96:85:B9:BE:99:AE:CD:58:A2:8A:E4:FA:83:53:94:80:09:12:9E:23:59:29:32:7C:F6:3C:C F:3D:9E:86:7D:B9:AF:2D:9E:60:BB:A1:CD:DD:5C:6A:EF:C9:92:5C:F4:C3:09:44:33:A3:C7:B6:2D:4C:E4:A9:17:59:F3:32:75:19:BD:60:C0:50:E3:1A:F6:BE:DB:DE:13:A6:22:AC:4E:5C:4F:6 4:E9:2C:72:89:E0:AD:6D:4C:BA:6A:80:C5:0A:51:E0:A1:D6:00:1F:E5:92:F6:1E:70:65:03:09:B4:4B:E2:9D:20:C5:3E:04:48:22:0A:24:71:4D:DE:57:02:78:76:2F:E9:CB:9C:50:98:02:85:8D :98:0C:C6:CC:DE:C0:8A:A9:5C:75:86:04:A5:6F:6A:1F:94:28:3D:07:4D:D7:BA:80:8C:24:8B:8C:72:F4:C5:44:FD:2E:E6:80:88:81:D8:FD:65:B6:27:11:12:31:87:BF:74:05:E9:34:D8:51:3B: 1E:E2:3D:5B:8C:AB:9B:3F:69:B9:58:AE:2D:A9:1E:CA:91:70:B4:88:F8:24:2A:7C:75:F9:E9:D5:F7:AA:92:D4:67:AB:DA:FC:B3:2A:8C:6D:07:1D:EF:32:01:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *47:ED:F8:63:F0:99:AF:5E:FE:7E:0E:5C:58:CB:FE:E2:35:37:A6:BD*

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Authority Info Access *http://ocspISAcA.cert.fnmt.es/ocspISAcA/OcspResponder*
http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.cert.fnmt.es/dpcs/
CPS text: [Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).]

CRL Distribution Points *ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint*
http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *05:2B:EB:BD:CD:5C:84:7B:FA:0F:6F:B0:EA:22:46:B5:5B:A9:EE:55:E0:2A:2D:48:0B:87:FC:2F:34:2C:84:43*

X509SubjectName

Subject CN: *ISA CA*

Subject O: *FNMT-RCM*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en] <https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

TSP Service Definition URI

URI [en] <http://www.ceres.fnmt.es/dpc>

URI [es] <http://www.ceres.fnmt.es/dpc>

4.5.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.5.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

Name [en] *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

Service digital identities**X509SubjectName**

Subject CN: *ISA CA*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *R+34Y/CZr17+fg5cWMv+4jU3pr0=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time *2016-05-29T22:00:00Z*

4.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

Name *[en]* *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

Service digital identities**X509SubjectName**

Subject CN: *ISA CA*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *R+34Y/CZr17+fg5cWMv+4jU3pr0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-07-27T00:00:00Z*

4.6 - Service (granted): Qualified certificates for individuals issued by AC FNMT Usuarios

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates for individuals issued by AC FNMT Usuarios*

Name *[es]* *Certificados Reconocidos para personas físicas emitidos por AC FNMT Usuarios*

Service digital identities**Certificate fields details**

Version: *3*

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

60:12:93:CA:20:B0:9A:03:29:5D:19:62:56:C6:95:3F:F9:EB:A8:11:DB:8E:3C:E1:40:41:3C:1B:FF:E9:A8:69

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI [en]

https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

URI [es]

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

TSP Service Definition URI

URI [en]

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

URI [es]

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

4.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.6.2 - History instance n.1 - Status: undersupervision**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en]

Qualified certificates for individuals issued by AC FNMT Usuarios

Name [es]

Certificados Reconocidos para personas físicas emitidos por AC FNMT Usuarios

Service digital identities**X509SubjectName**

Subject CN: *AC FNMT Usuarios*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *sdRPxCN5+kQFCcbrOc/oNbC4IGQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-01-01T23:00:00Z*

4.7 - Service (granted): Qualified certificates issued by AC Representación

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by AC Representación*

Name *[es]* *Certificados cualificados emitidos por AC Representación*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *129946737925237468182436074897133262369*

CRL Distribution Points

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

8F:D1:6A:17:99:44:D5:D1:D4:20:AF:09:40:5E:DA:7A:BF:2A:9C:74:28:83:E8:C2:F8:9E:0D:90:AF:AF:75:4B

X509SubjectName**Subject CN:**

AC Representación

Subject OU:

CERES

Subject O:

FNMT-RCM

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2023-02-06T00:00:00Z

Scheme Service Definition URI**URI**

[en]

https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

URI

[es]

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

4.7.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI**

[en]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.7.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI**

[en]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

4.7.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by AC Representación*

Name *[es]* *Certificados Reconocidos emitidos por AC Representación*

Service digital identities**X509SubjectName**

Subject CN: *AC Representación*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *3FCWn9cxickR5O+WX/ZfgIJGYIM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

4.7.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.7.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by AC Representación*

Name *[es]* *Certificados Reconocidos emitidos por AC Representación*

Service digital identities

Signature algorithm: *SHA256withRSA*

Issuer OU: *AC RAIZ FNMT-RCM*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject OU: *AC Componentes Informáticos*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Mon Jun 24 12:52:59 CEST 2013*

Valid to: *Sat Jun 24 12:52:59 CEST 2028*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:97:57:1F:2B:75:B1:7B:FF:16:38:E0:26:92:AB:3C:C6:A3:90:61:BF:30:3C:92:7C:42:FF:72:89:61:5C:D3:7F:E0:A4:3A:F3:31:31:40:EE:BF:C6:F4:87:7F:0C:0E:E8:E6:FD:12:99:84:13:4E:59:82:A1:C4:5D:D4:E8:56:55:85:C4:7D:C4:E0:9C:8A:E4:BF:82:84:FC:D2:6D:C1:07:2C:40:29:C6:C6:36:46:84:8C:20:38:5D:19:20:94:36:80:17:10:87:11:9D:3A:30:E9:EF:5E:C4:8E:64:37:CF:61:A8:5B:43:75:45:09:5C:9C:26:E8:65:1D:D0:30:4A:99:9C:79:0C:1C:45:89:11:E9:88:17:C1:38:B2:CC:23:46:8A:F3:0A:02:64:52:DD:D2:2D:A8:33:A6:0D:6F:E7:C6:20:C5:A8:F2:5D:F1:55:98:EC:61:64:C1:B6:C0:7A:A6:08:77:C1:63:37:CC:DF:BD:A7:EE:9E:C0:7D:48:B1:64:52:33:CF:31:EA:9F:98:2E:C1:76:1E:C7:33:12:E9:68:E5:D1:3B:01:F6:D3:57:26:95:E6:E2:3E:49:F4:C5:21:71:5C:5A:B0:86:1A:FA:C8:DF:14:41:86:77:3B:FF:B1:74:72:EB:4B:A0:D2:F7:E0:89:50:5E:9D:D3:D8:A3:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65*

Authority Info Access *http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder*
http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt

Authority Key Identifier *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.cert.fnmt.es/dpcs/
CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points *ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint*
http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F0:38:42:1F:07:F2:0D:63:A2:0D:36:91:E5:A1:78:AB:84:59:EB:E5:70:C1:64:7B:76:90:55:4E:F2:38:76:AB*

X509SubjectName

Subject OU: *AC Componentes Informáticos*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *GfhYLxTWpsybBJglDUzXqwCng2U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-02-28T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

4.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

4.8.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC Componentes Informáticos*

Name [es] *Certificados cualificados emitidos por AC Componentes informáticos*

Service digital identities

X509SubjectName

Subject OU: *AC Componentes Informáticos*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *GfhYLxTWpsybBjglDUzXqwCng2U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-09-12T00:00:00Z*

4.8.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.9 - Service (withdrawn): Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

Name *[es]* *Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *28295960146001875498465664804547762024*

Subject Key Identifier *A1:F6:70:6D:CC:7E:8D:3B:CC:3C:93:E2:DE:94:9B:B1:45:9F:1F:9F*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Authority Key Identifier *19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65*

CRL Distribution Points *ldap:///ldapcomp.cert.fnmt.es/CN=CRL1,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint*
http://www.cert.fnmt.es/crlscomp/CRL1.crl

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *08:F2:93:4C:39:4D:89:DD:B0:CF:C3:86:AA:F5:C5:2E:4F:17:AF:BB:BE:1C:67:A0:36:11:13:2F:80:BE:B7:A9*

X509SubjectName

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

Subject C: *ES*

X509SKI

X509 SK I *ofZwbcx+jTvMPJPi3pSbsUWfH58=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-02-28T00:00:00Z*

4.9.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

Name [es] *Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

Service digital identities

X509SubjectName

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

Subject C: *ES*

X509SKI

X509 SK I *ofZwbcx+jTvMPJPi3pSbsUWfH58=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-09-12T00:00:00Z*

4.10 - Service (granted): Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1*

Name [es] *Certificados cualificados emitidos por AC SERVIDORES SEGUROS TIPO1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *107052318472807923832373279208241425243*

Signature algorithm:

SHA384withECDSA

Issuer CN:

AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Issuer 2.5.4.97:

VATES-O28260041

Issuer OU:

Ceres

Issuer 0:

FNMT-RCM

Issuer C:

ES

Subject CN:

AC SERVIDORES SEGUROS TIPO1

Subject 2.5.4.97:

VATES-028260041

Subject OU:

Ceres

Subject 0:

FNMT-RCM

Subject C:

ES

Valid from:

Thu Dec 20 11:15:49 CET 2018

Valid to:

Tue Dec 20 11:15:49 CET 2033

Public Key:

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:3B:18:86:43:6F:3E:4E:8F:9C:72:51:60:C2:D1:61:DF:45:AE:5F:8D:A6:03:B1:FD:E1:AA:6C:91:A1:6C:6C:8B:98:90:68:6D:A4:68:AC:3F:6E:76:1E:5B:57:A2:E8:88:42:FC:8E:8B:B4:8F:07:D9:7B:AD:6B:CE:7A:E4:64:90:91:FE:F2:39:CC:A8:5D:E4:4B:D2:AA:DD:A9:27:93:3A:EB:B4:B1:CC:84:9E:74:D2:73:FF:D3:03:B4:FF:CR:B3

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

8C:42:32:40:F9:79:3F:6B:13:C1:75:C6:5D:EE:86:22:44:39:6F:77

Certificate Policies

Policy OID: 2.5.29.32.0

Authority Info Access

<http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder>
<http://www.cert.fnmt.es/certs/ACRAIZSERVIDORESSEGUROS.crt>

CRL Distribution Points

<http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl>

Authority Key Identifier

01:B9:2F:FF:BF:11:86:60:F2:4F:D0:41:6E:AB:73:1F:E7:D2:6E:49

Key Usage:

keyCertSign - *cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1E:DB:6B:D9:12:74:88:2D:B7:95:BF:C5:14:F8:AA:BE:10:AD:95:5C:BC:CF:D3:FD:5A:5B:5F:EB:B2:CE:5B:68*

X509SubjectName

Subject CN: *AC SERVIDORES SEGUROS TIPO1*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *jElyQPI5P2sTwXXGxe6GikQ5b3c=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2019-07-15T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

4.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

4.11 - Service (granted): Servicio Cualificado de certificados de sello emitidos por "AC Unidades de Sellado de Tiempo"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[es]

Servicio Cualificado de certificados de sello emitidos por "AC Unidades de Sellado de Tiempo"

Name

[en]

Qualified Certificates esal issued by "AC Unidades de Sellado de Tiempo"

Service digital identities

Certificate fields details

Version:

3

Serial Number:

59717140960880169574663461521964308570

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer OU:

AC RAIZ FNMT-RCM

Issuer O:

FNMT-RCM

Issuer C:

ES

Subject CN:

AC Unidades de Sellado de Tiempo

Subject 2.5.4.97:

VATES-Q2826004/

Subject OU:

Ceres

Subject O:

FNMT-RCM

Subject C:

ES

Valid from:

Thu Nov 28 09:50:02 CET 2019

Valid to:

Wed Nov 28 09:50:02 CET 2029

Public Key:

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C8:46:B4:18:21:48:77:8F:F4:18:DD:1F:F0:B8:2C:5C:11:96:C8:21:26:3A:CA:E6:4D:06:CA:3B:D3:EF:34:71:7A:43:59:60:D0:77:3F:CE:EC:00:C5:20:B7:81:FE:C8:20:65:5B:6E:00:D2:A2:33:8F:72:A9:CA:BF:92:4E:4F:80:11:68:1F:EA:52:18:D2:A8:28:0A:79:32:98:08:A2:D6:DF:C9:10:42:D3:F0:F4:DD:48:60:6C:0C:36:14:18:6A:5D:C4:36:E8:F8:90:63:B5:79:D6:97:8A:C2:40:4D:78:FE:47:A6:88:E1:ED:A1:E8:38:21:70:C9:C3:9E:F1:42:BF:EF:BD:77:1F:F7:CB:ED:01:6D:88:89:A3:F3:C5:79:36:42:1D:9E:1A:5A:D0:B8:DB:CB:39:6F:C7:F7:7C:8E:C2:76:E5:6A:3B:60:47:60:8F:84:E2:89:36:CB:FD:79:60:CE:68:60:D9:95:43:D8:34:78:B8:67:68:AD:26:F2:DD:86:44:01:32:1C:19:AD:87:3F:63:BA:F5:8D:E7:51:98:88:95:E7:AE:20:A0:77:5B:58:52:A1:1A:B8:85:90:57:87:FD:9A:E7:20:12:9E:CC:21:30:9C:D1:F7:CC:CC:08:DF:A8:A3:BF:26:E4:9F:19:90:D9:7C:F2:CF:C4:B4:0C:2A:5B:FC:95:2F:46:39:61:69:DD:9C:BF:55:C7:E8:F3:A3:C4:4C:AE:FB:EB:34:64:55:8B:62:91:69:B8:A6:9E:35:57:8A:20:85:43:AF:90:75:C0:CB:18:0A:92:0F:55:76:DA:BC:C0:4F:AC:33:4C:6F:4B:E1:DD:6E:31:87:B6:DA:5D:8B:1B:BA:33:88:6B:01:B4:60:67:28:05:61:50:1F:2E:2C:65:DE:A8:49:D5:6D:30:D7:1C:72:E0:03:88:04:07:5A:00:CD:3F:7D:88:7C:38:ED:75:93:C8:A2:6E:37:8A:07:DC:5C:9A:E1:0A:EF:2A:E4:E7:88:83:F9:69:80:BA:21:88:96:68:E0:E4:4A:81:CF:A7:F0:0E:2E:65:C3:1E:59:79:89:23:96:0D:24:D4:29:E2:D8:6D:0F:99:45:84:F9:75:32:93:DB:56:E9:86:9B:53:C6:34:FC:10:C4:41:B8:E5:EA:37:95:CB:58:D7:F4:03:28:00:DE:26:E4:2A:9D:92:8F:E2:14:48:87:F9:2B:78:4A:42:73:A5:FE:B4:D9:46:21:8F:FD:8A:25:23:C5:08:62:70:84:D4:9D:D9:13:10:20:0C:68:E8:26:7F:E1:B5:17:8D:73:5B:46:76:66:BF:95:33:48:0E:22:3E:3B:1C:CE:A3:02:03:01:00:01

Basic Constraints

isCA: true - Path length: 0

Authority Info Access

<http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder>
<http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt>

Subject Key Identifier

40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5

Authority Key Identifier

F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: <http://www.cert.fnmt.es/dpcs/>

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]

CRL Distribution Points

<ldap:///ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>
<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

9C:E6:30:B3:5F:8A:E2:C6:41:9E:73:4A:D9:D2:FA:30:47:6D:D9:E7:39:4B:1E:93:B2:7F:83:F7:76:A0:24:EA

X509SubjectName**Subject CN:**

AC Unidades de Sellado de Tiempo

Subject 2.5.4.97:

VATES-Q2826004]

Subject OU:

Ceres

Subject O:

FNMT-RCM

Subject C:

ES

X509SKI**X509 SK I**

QLIVBKhPf2CQ7RGVJcMI+lr0hdU=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time 2020-06-15T22:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

4.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

4.12 - Service (granted): Servicio Cualificado de certificados emitidos por “AC Sector Público”

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Servicio Cualificado de certificados emitidos por “AC Sector Público”

Name [en] Qualified Certificates issued by “AC Sector Público”

Service digital identities

Certificate fields details

Version: 3

Serial Number: 69791624804545296306732150382596141970

Certificate Policies*Policy OID: 2.5.29.32.0**CPS pointer: <http://www.cert.fnmt.es/dpcs/>**CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)]***CRL Distribution Points***ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint**<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***82:65:75:6D:D5:CD:8A:37:EE:61:E4:03:51:28:8E:4B:16:A8:9D:D2:48:C1:EC:4E:BA:25:AA:F1:61:AB:F4:98***X509SubjectName****Subject CN:***AC Sector Público***Subject 2.5.4.97:***VATES-Q2826004J***Subject OU:***Ceres***Subject O:***FNMT-RCM***Subject C:***ES***X509SKI****X509 SK I***5wTucJERkkT5DpKPVkMeBx2/Bjw=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2024-08-22T00:00:00Z***Scheme Service Definition URI****URI***[en]**<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI***[es]**<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***4.12.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.12.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

4.12.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.5734.3.17.5>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.5734.3.17.6>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.5734.3.17.8>

Description

Description

4.12.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Servicio Cualificado de certificados emitidos por "AC Sector Público"*

Name [en] *Qualified Certificates issued by "AC Sector Público"*

Service digital identities

X509SubjectName

Subject CN: *AC Sector Público*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

X509SKI

X509 SK I *5wTucJERkkT5DpKPVkMeBx2/BJw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-07-28T00:00:00Z*

4.12.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.5734.3.17.5*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.5734.3.17.6*

Description**4.12.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.12.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**4.12.5 - History instance n.2 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[es]

*Servicio Cualificado de certificados emitidos por “AC Sector Público”***Name**

[en]

*Qualified Certificates issued by “AC Sector Público”***Service digital identities****X509SubjectName****Subject CN:***AC Sector Público***Subject 2.5.4.97:***VATES-Q2826004J***Subject OU:***Ceres***Subject O:***FNMT-RCM***Subject C:***ES***X509SKI****X509 SK I***5wTucJERkkT5DpKPVkMeBx2/Bjw=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time***2020-06-15T22:00:00Z***4.12.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]****Qualifier type description**

[en]

undefined.

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.5734.3.17.5***Description**

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Unidades de Sellado de Tiempo*

Issuer 2.5.4.97: *VATES-Q2826004J*

Issuer OU: *Ceres*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Fri Jun 19 12:40:38 CEST 2020*

Valid to: *Thu Jun 19 12:40:38 CEST 2025*

Public Key: *30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:B9:11:D1:00:47:E6:2A:6D:8B:06:1D:59:DE:0C:9B:B3:27:B9:76:2F:B2:50:91:1E:8E:30:8D:07:F2:C9:0B:0E:CF:14:C7:19:13:96:2E:93:DE:A5:0B:06:75:05:02:8D:E7:61:89:AA:CC:A3:6E:ED:76:57:A4:DE:ED:3B:94:47:29:C4:7B:CF:0A:3A:AF:B5:92:5A:B4:2A:47:0F:00:7D:B7:8B:CF:56:EF:10:39:E3:95:94:6B:E7:5E:06:7E:F6:14:56:EB:6F:B1:06:8D:B2:51:AB:6D:19:53:04:ED:71:4D:3A:91:27:CF:DE:CC:97:E7:B2:7D:4A:BD:64:2D:63:B0:9A:CF:DF:54:57:E3:1D:ED:7D:B3:F3:32:0A:92:83:05:93:FB:8D:2D:E6:32:D0:6E:8D:E9:BD:87:7A:B8:7B:80:7F:6E:0D:72:AD:B3:C3:B8:92:E9:99:F2:1D:1C:1F:61:42:03:7D:1F:6F:F2:36:E6:EB:CE:52:13:20:1B:44:5E:80:23:2B:42:7D:EC:56:ED:E9:8B:C9:D5:68:DD:82:82:32:B7:29:7E:F3:B3:1D:CF:16:4C:AA:E2:1A:20:14:52:78:6D:8D:FD:D7:58:0E:45:5B:EE:04:B5:68:AA:5F:08:BA:76:0D:6A:5D:29:44:1C:A2:49:32:F6:87:1A:3C:CC:57:40:E9:F9:90:8C:A5:64:A9:27:2A:F5:A6:7B:E7:37:11:DE:27:1C:7E:E4:65:78:3B:4E:8D:3E:5B:86:2E:C2:ED:33:FC:FD:49:D1:99:A1:C8:7E:D0:55:FB:E7:83:C4:1C:AD:6B:BF:9D:1C:A8:B6:B4:D0:8E:D9:35:2C:02:C8:A2:82:ED:95:70:AD:EF:D4:AC:E3:52:C5:89:54:CC:58:DB:97:92:2E:83:55:62:B7:13:D4:F4:EE:8A:C5:E3:4A:5A:57:BE:62:9A:06:52:A0:CF:A6:ES:10:98:67:CC:30:19:8F:13:91:65:DB:9E:AD:D5:BD:DC:A7:CC:6E:75:02:03:01:00:01*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *F1:0E:77:4D:0A:32:E7:69:A5:90:00:1A:E4:A0:15:CF:BB:89:00:D2*

Authority Key Identifier *40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://www.cert.fnmt.es/crlsacst/CRL.crl*

Certificate Policies*Policy OID: 1.3.6.1.4.1.5734.3.18.1**CPS pointer: <http://www.cert.fnmt.es/dpcs/>**CPS text: [Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)]**Policy OID: 0.4.0.194112.1.1***Authority Info Access***<http://www.cert.fnmt.es/certs/ACST.crt>**<http://ocspst.cert.fnmt.es/ocspst/OcspResponder>***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***88:15:87:C2:7E:44:DC:07:DA:A3:92:D2:5B:CC:81:38:53:F2:03:63:46:31:65:86:86:87:EE:BC:DB:71:D7:55***X509SubjectName****Subject CN:***AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020***Subject 2.5.4.97:***VATES-Q2826004J***Subject OU:***CERES***Subject O:***FNMT-RCM***Subject L:***MADRID***Subject C:***ES***X509SKI****X509 SK I***8Q53TQoy52mlkAAa5KAVz7uJANI=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-07-17T02:00:00Z***Scheme Service Definition URI****URI** [en]*<https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI** [es]*<https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

4.13.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020*

Name *[en]* *Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020*

Service digital identities**X509SubjectName**

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *CERES*

Subject O: *FNMT-RCM*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *8Q53TQoy52mlkAAa5KAVz7uJANI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-07-28T00:00:00Z*

4.14 - Service (granted): Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2023

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2023*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:8B:48:57:1B:98:FF:99:E4:CC:06:B5:14:8A:C3:BE:EB:09:43:8B:94:14:21:15:0F:85:21:8E:6A:8C:CB:85:00:41:D5:7D:FE:02:C5:D9:2B:95:BE:DD:AC:86:AC:08:D5:2C:DA:7D:CB:57:D9:7F:57:DD:E3:86:39:CD:31:55:A6:9F:FB:68:6F:7B:E6:8E:37:32:E6:A8:DE:06:CF:6D:7D:DF:3D:D8:D6:7E:3E:74:46:C3:93:DE:0E:53:B7:E6:48:61:98:2F:89:0B:79:5A:0E:0C:B4:F9:43:0A:99:63:7B:62:79:38:CD:3F:63:46:95:DD:9C:F1:80:EA:33:80:9C:73:FB:A7:C9:BC:AF:72:E4:8F:99:ED:FE:1F:F5:6C:8B:F1:95:D0:7B:7E:A3:A0:D0:DE:BD:23:FD:F0:1D:FE:84:1D:AF:57:DD:E3:D1:89:C9:9B:D6:A7:CC:38:91:BC:B9:60:71:D1:22:28:20:34:B2:C6:E0:3D:A4:9D:43:59:18:58:EA:3D:46:17:CD:5B:87:07:54:87:BE:12:69:92:A3:DE:8F:BA:F3:8F:85:92:63:0E:95:34:35:33:85:F3:CF:6E:85:8D:2E:D5:82:0E:79:98:8D:98:B2:20:87:CE:3D:29:AF:A9:95:E5:D0:39:88:F4:00:08:3F:3D:2E:D1:93:07:CF:CA:88:35:53:B3:BC:EA:36:06:AE:DD:BF:7C:55:BC:B5:17:59:7C:AE:65:BA:12:13:50:FC:CB:4C:C5:AD:94:17:62:F8:29:F7:39:1B:29:03:DD:86:F8:60:2E:9B:E1:BD:E0:A6:EB:EE:53:FF:AE:0F:86:6D:4C:C3:42:38:D0:61:72:67:66:8B:55:04:CC:A1:62:CE:F0:44:69:E1:48:B2:BE:7C:8D:24:C6:76:6A:1B:6D:F7:5A:EF:90:72:54:B3:FB:8A:99:44:01:0F:7B:18:2B:BE:E2:70:9A:4C:08:51:07:31:0E:D7:DE:71:02:68:56:AA:0A:C3:8C:3D:02:03:01:00:01

Basic Constraints*IsCA: false***Extended Key Usage***id_kp_timeStamping***Subject Key Identifier***55:AE:72:11:BE:BE:48:BB:65:90:14:6A:DC:C9:83:6C:2E:BE:42:15***Authority Key Identifier***40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5***QCStatements - crit. = false***id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15***CRL Distribution Points***http://www.cert.fnmt.es/crlsacst/CRL.crl***Certificate Policies***Policy OID: 1.3.6.1.4.1.5734.3.18.2**CPS pointer: http://www.cert.fnmt.es/dpcs/**CPS text: [Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)]**Policy OID: 0.4.0.194112.1.1***Authority Info Access***http://www.cert.fnmt.es/certs/ACST.crt**http://ocspst.cert.fnmt.es/ocspst/OcspResponder***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***FC:FD:3D:F4:90:B9:A2:1B:3F:AD:58:20:11:A2:E6:D0:39:56:17:96:AC:5D:85:0D:01:B6:5A:C5:DD:A4:A3:E9***X509SubjectName****Subject CN:***AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2023***Subject 2.5.4.97:***VATES-Q2826004J***Subject OU:***CERES***Subject O:***FNMT-RCM***Subject L:***MADRID***Subject C:***ES***X509SKI**

Issuer O: *FNMT-RCM*
Issuer C: *ES*
Subject CN: *AC CONSULARES G2*
Subject 2.5.4.97: *VATES-Q2826004J*
Subject O: *FNMT-RCM*
Subject C: *ES*
Valid from: *Thu Oct 10 13:06:37 CEST 2024*
Valid to: *Fri Oct 07 13:06:36 CEST 2039*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:AF:AF:DC:9A:F4:CB:B7:E7:DD:F2:1A:8F:BB:BF:E5:76:94:72:DD:49:37:20:60:FA:3F:B6:FC:26:81:03:D2:D1:54:45:8C:59:3B:E9:18:4E:29:C8:E8:0D:95:81:EF:4A:F6:F7:91:A8:E9:C1:5C:91:38:5C:E5:4E:A6:1E:B7:56*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *E2:29:99:47:2A:FF:5B:26:8A:C8:34:41:66:45:AF:52:3A:08:F1:80*
Authority Info Access *http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt*
http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder
Certificate Policies *Policy OID: 2.5.29.32.0*
Extended Key Usage *id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
CRL Distribution Points *http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl*
Subject Key Identifier *10:42:D5:BC:5A:C0:8B:BF:58:DF:2E:1D:94:A3:F2:E5:22:69:17:79*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *5D:E9:08:51:A1:A2:23:5C:51:5B:86:36:C6:A6:85:99:03:17:CD:4F:30:EF:4A:57:3E:08:EC:07:AA:F1:82:4C*

X509SubjectName

Subject CN: *AC CONSULARES G2*
Subject 2.5.4.97: *VATES-Q2826004J*
Subject O: *FNMT-RCM*
Subject C: *ES*

X509SKI

X509 SK I

EELVvFrAi79Y3y4dIKPy5SjpF3k=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2025-05-21T00:00:00Z

4.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.16 - Service (granted): Qualified certificates issued by AC USUARIOS G2

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en]

Qualified certificates issued by AC USUARIOS G2

Name *[es]*

Certificados cualificados emitidos por AC USUARIOS G2

Service digital identities

Certificate fields details

Version:

3

Serial Number:

535704898679124250761366620772703936040318962089

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

*****END CERTIFICATE*****

Signature algorithm:

SHA384withECDSA

Issuer CN:

AC RAIZ FNMT-RCM G2

Issuer 2.5.4.97: *VATES-Q2826004J*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC USUARIOS G2*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Mon Dec 16 11:54:50 CET 2024*

Valid to: *Tue Dec 13 11:54:49 CET 2039*

Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:8C:14:C4:E1:84:05:B2:06:33:D0:4F:1F:7D:15:80:8E:A1:DE:D4:3B:70:ED:95:80:F0:44:BE:F4:FA:96:BE:D1:06:85:D7:8E:56:DD:BA:34:E0:85:68:52:BC:B2:1A:05:71:13:DD:D8:AE:93:4B:3C:3A:89:3A:57:A9:60:7E:24*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *E2:29:99:47:2A:FF:5B:26:8A:C8:34:41:66:45:AF:52:3A:08:F1:80*

Authority Info Access *http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt
http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder*

Certificate Policies *Policy OID: 2.5.29.32.0*

Extended Key Usage *id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

CRL Distribution Points *http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl*

Subject Key Identifier *B8:E4:76:50:CD:AE:4E:C2:0E:E6:41:6D:B5:66:3E:1D:C1:20:46:6E*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *28:3A:9F:9F:E9:67:4F:67:EF:D6:E2:7B:B5:43:E0:EC:19:2C:BE:FF:20:FC:83:6C:22:43:65:47:44:C5:AF:89*

X509SubjectName

Subject CN: *AC USUARIOS G2*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject O: *FNMT-RCM*

Issuer CN: *AC RAIZ FNMT-RCM G2*
Issuer 2.5.4.97: *VATES-Q2826004J*
Issuer O: *FNMT-RCM*
Issuer C: *ES*
Subject CN: *AC REPRESENTACIÓN G2*
Subject 2.5.4.97: *VATES-Q2826004J*
Subject O: *FNMT-RCM*
Subject C: *ES*
Valid from: *Mon Dec 16 12:01:31 CET 2024*
Valid to: *Tue Dec 13 12:01:30 CET 2039*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:E3:C7:D1:27:5B:FF:19:EC:CC:AC:0E:AC:FF:B9:7A:43:5D:B0:55:05:46:3A:90:46:11:6C:EC:05:7E:41:30:B3:C7:FC:36:60:8D:BA:83:54:4F:F6:51:43:2E:00:AD:A7:2A:F4:9A:CS:BD:F5:16:10:FE:1C:FA:D0:3A:10:EA:D6*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *E2:29:99:47:2A:FF:5B:26:8A:C8:34:41:66:45:AF:52:3A:08:F1:80*
Authority Info Access *http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt*
http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder
Certificate Policies *Policy OID: 2.5.29.32.0*
Extended Key Usage *id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
CRL Distribution Points *http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl*
Subject Key Identifier *E2:37:CF:17:30:5F:A7:33:BD:97:D0:91:7B:D2:59:C1:49:29:CF:C9*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *0D:F2:88:3B:60:74:D5:B7:D7:94:0B:69:CA:65:8A:3A:9A:74:7A:8E:17:1F:65:3A:D4:CE:02:30:08:7D:9D:64*
X509SubjectName
Subject CN: *AC REPRESENTACIÓN G2*
Subject 2.5.4.97: *VATES-Q2826004J*

Subject O:	FNMT-RCM
Subject C:	ES
X509SKI	
X509 SK I	4jfPFzBfpzO9I9CRe9JZwUkpz8k=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined. [es] undefined.
Status Starting Time	2025-07-17T02:00:00Z

4.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation	
URI	[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

4.18 - Service (granted): Qualified certificates issued by AC ENTIDADES G2

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services. [es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
Service Name	
Name	[en] Qualified certificates issued by AC ENTIDADES G2
Name	[es] Certificados cualificados emitidos por AC ENTIDADES G2

Service digital identities

Certificate fields details

Version:	3
Serial Number:	141292681913566155608616841680497278942212804413

X509 Certificate	-----BEGIN CERTIFICATE----- MIIDUDCCATWgAwIBAgIUIGUjYcYF7YAXA/FbcFBwWfYgTz0wCgYIKoZIzj0EAwMwWDELMAKGA1UEBhMCRVMEETAPBgNVBAoMCEZOTY0CkNNMRgwFgDYQRhDA9WQVRfUy1RMgyNjAwNEoxHDAaBgNVBAMMEEDTAPBgNVBRIzSVNC1S000gR2wHhCMQwMDewMTAwNTU1WncNMzkxMDA3MTAwMTU0WjBU MQswCQYDVQOGewjFuzERMA8GA1UECgwIRk5NVCI1S000xGDAWBgNVBGEtMDZBVEVTLVEyODI2MDA0 SjEYMBYGA1UEAwwPQUUMgRU5USURBREVTIEcyMkFweW1HkoZlZj0CAQYIKoZIzj0DAQcDQgAE7piH FBEcp2E5gYjNLE++b2JefY+Yr788FMBgRgajwDcat++eTqS1JZUKCCORqngG1ZyP87K0Suge CEYfqQCAx8wggF7MBIGAlUdEwEBwQIMAYBA8CAQAwHwYDVR0JBgBwFoAU4imZRYrWYakYDRB ZkVWUjoi8YAwgZUGCcsGAQUFBwEBBGIgMIGFMDeGCSGAQUFBzACHSodHRwOi8vd3d3LmNlcnQu Zm50cSlicy9jZjZlcy9BQ1JBSVpG1UURUx13J0MEcGCCSQAQJFBA8BntodHRwOi8vd3d3LmNlcnQu cmFpemcyLmNlcnQuZm50cSlicy9vY3NwY2FyYWI6R2VtZ2NzFjI3BvbmRicjARBgNVHSAECIAI MAYGBFUDIAAwKgYDVR0BICMwIQYIKwYBBQUHAWIGCisGAQQBgicKAwwGCsGStb3LweB8TA+BgnV HREBNZALMDQpMAhVh1odHRwOi8vd3d3LmNlcnQuZm50cSlicy9jcmxmdGF5ZjEOTVR5ODI1HMSj cmwwHOYDVR0BOBBYFQU27eCYEpLafBu4ZdOmPBFYVswMA4GA1UdEwEBwQEAwIBBjAKBgqhkJQ PQODAwNpAD8mAjEAlu77gdf1oWZ7ueAareQ4hhz2BoKfH5thcw1JBySejKv808ya3ukhQDy/n WTDQAJEA+QHGXipstZGwSfHCPqGEnLFTgYUHGPDQ1oqJ0RdECG3S8MNNOCgqg8NKTTP -----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: *AC RAIZ FNMT-RCM G2*

Issuer 2.5.4.97: *VATES-Q2826004J*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AC ENTIDADES G2*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject O: *FNMT-RCM*

Subject C: *ES*

Valid from: *Thu Oct 10 12:01:55 CEST 2024*

Valid to: *Fri Oct 07 12:01:54 CEST 2039*

Public Key:
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:EE:92:07:14:11:02:A7:61:25:E6:92:58:34:BD:9E:F9:B6:49:79:FE:18:F9:7A:FB:F7:C1:57:31:BA:E0:7A:36:BF:C3:47:1E:97:E7:BB:AB:9D:49:65:49:02:08:64:6A:9E:71:83:67:23:FF:07:B2:B4:4A:E8:04:08:4C:9F:8E

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *E2:29:99:47:2A:FF:5B:26:8A:C8:34:41:66:45:AF:52:3A:08:F1:80*

Authority Info Access
http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt
http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder

Certificate Policies *Policy OID: 2.5.29.32.0*

Extended Key Usage *id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

CRL Distribution Points *http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl*

Subject Key Identifier *E5:36:ED:E0:98:12:92:DA:14:1B:AE:E1:97:50:98:FF:05:C9:5B:30*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EC:75:1E:45:28:20:21:D1:BC:AF:02:9C:49:7D:05:CD:DE:C1:E3:A7:63:29:AB:84:5A:FA:C3:5E:75:9C:24:DD*

X509SubjectName

Subject CN: *AC ENTIDADES G2*

Subject 2.5.4.97: VATES-Q2826004J

Subject O: FNMT-RCM

Subject C: ES

X509SKI

X509 SK I 5Tbt4JgSktoUG67hl1CY/wXJWzA=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-07-17T02:00:00Z

4.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

4.19 - Service (granted): Qualified certificates issued by AC SECTOR PÚBLICO G2

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified certificates issued by AC SECTOR PÚBLICO G2

Name [es] Certificados cualificados emitidos por AC SECTOR PÚBLICO G2

Service digital identities

Certificate fields details

Version: 3

Serial Number: 420050182499522489324051859282231330578481553274

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDVCCAtugAwIBAgIU5Z0znXmJXKMZm3mefv9PNYCH3owCgYIKoZIzj0EAwMwWDELMAKGA1UE
BhMCRVMxETAPBgNVBAoMCEZOTVQlUkNNMRgwFgYDVORhDA9WQVRFluY1RMgyNjAwNEoxHDAaBgNV
BAMMEQDFIFBSVGRKSNVCI1S000gRzIwHhNMjQwMEZMTA1ODExNjEzMTA1ODExYjB9
MCOwCOYDVQOCGEwIFuzERMA8GA1UECgwIRKSNVCI1S000xGDAWBgNVBGEEMD1ZBVEVTLVEyODZMDA0
SjEeMBwGA1UEAwVwQUUMgU0V0VE95SjFDDmKjMSUNPIECyMfKwEwYHkoZizj0CAQYIKoZIzj0DAQcD
QgAEQ04Z2WjKc9ajnamc0bqto3uWuzm8owUeIU7UpBKAyZnQ1a5b1j428NqoT74db4UzHv
7GvOny3uDan6QCAK8wqg7MBGAIUdEwEBwQIMAYBAI8CAQAwHwYV7R0jBBowF0Al4mZRYr/
WvakyDRBZKwVUjgI8YAwgZUGCCSGAOUFBwEBBIBIGIMGFMDoGCCSGAOUFBZACH5odHRwOi8vd3d3
LnNlcnQzZm5tdC5lc3ky9jZj0cy99Q1BSVpGTA1URzluY3J0MEcGCCSGAOUFBZABhIodHRwOi8v
b2NzcGhncmFpemcyLnNlcnQzZm5tdC5lc3ky9jZj0yY2FyYWI6RzlvT2NscFJlc3BvbmRicjARBgNV
HSAECAIMAYGBFUDIAAwKgYDVROlBCMwiQYIKwYBBQUHAWIGCCSGAQQBgicKAwGCCSgSiB3LwEB
BTA+BgNVHRSBEHZA1MDQgMaAvhIodHRwOi8vd3d3LnNlcnQzZm5tdC5lc3ky9jZj0yY2FyYWI6RzlvT2NscFJlc3BvbmRicjARBgNV
HQIHMISjcmwwHOYDVR0OBByEFYwknz0B/vrthWScsQleXW0/fnTMA4GA1UdDwEBwQEAwIBBIAK
BgqhkhjOPQODAwNoADBlAEAv+00paQ1k6KALP7yVsdCwBbh3esUk48MmgPTp8QmQWDRbs00RoEI
84DTpgpNNs38AjBZUMGVTPENSXPoziNhimTWo0Doe5psa9bjPg5zHjbejT3388Mm/kA0wo6TtGH5
LdQ=

```

-----END CERTIFICATE-----

Signature algorithm:	SHA384withECDSA
Issuer CN:	AC RAIZ FNMT-RCM G2
Issuer 2.5.4.97:	VATES-Q2826004J
Issuer O:	FNMT-RCM
Issuer C:	ES
Subject CN:	AC SECTOR PÚBLICO G2
Subject 2.5.4.97:	VATES-Q2826004J
Subject O:	FNMT-RCM
Subject C:	ES
Valid from:	Mon Dec 16 11:58:13 CET 2024
Valid to:	Tue Dec 13 11:58:12 CET 2039
Public Key:	30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:0D:2D:38:67:05:E3:29:CF:7F:68:99:9A:99:CA:1B:AA:9B:68:DE:E5:AE:CE:60:68:C1:47:A2:53:B5:29:04:A0:32:DA:BA:D0:87:56:B9:6F:58:38:67:C3:6A:A1:3A:FB:E1:D6:B8:53:31:EF:FD:81:AF:3A:7C:B7:B8:36:A2:C7
Basic Constraints	IsCA: true - Path length: 0
Authority Key Identifier	E2:29:99:47:2A:FF:5B:26:8A:C8:34:41:66:45:AF:52:3A:08:F1:80
Authority Info Access	http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder
Certificate Policies	Policy OID: 2.5.29.32.0
Extended Key Usage	id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12
CRL Distribution Points	http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl
Subject Key Identifier	9C:24:9F:3D:01:FE:FA:E1:85:64:9C:B1:08:9E:5D:6D:3F:15:F9:D3
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256

Thumbprint: 98:33:29:B0:0C:30:52:D7:EC:CD:46:BF:2C:F3:E2:9D:05:AE:93:D1:AA:14:6B:D5:07:8C:37:26:AE:82:71:FE

X509SubjectName

Subject CN: AC SECTOR PÚBLICO G2

Subject 2.5.4.97: VATES-Q2826004J

Subject O: FNMT-RCM

Subject C: ES

X509SKI

X509 SK I nCSfPQH++uGFZJyxCJ5dbT8V+dM=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2025-07-17T02:00:00Z

4.19.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

4.19.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.5734.3.23.1.1

Description

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.5734.3.23.3.1

Description

Policy Identifier:

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>	
Service type description	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name		
Name	[en]	Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM-TSU 2025
Name	[es]	Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM-TSU 2025

Certificate fields details

Version: 3

Serial Number: 667686980749011454590729379768938228586049670319

X509 Certificate

[illegible]

Signature algorithm: *SHA384withECDSA*

Issuer CN: AC TSA FNMT

Issuer 2.5.4.97: *VATES-028260041*

Issuer O: *FNMT-RCM*

Issuer C: *ES*

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM-TSU 2025*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject O: *FNMT-RCM*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Mon Dec 16 11:34:54 CET 2024*

Valid to: *Sat Dec 15 11:34:53 CET 2029*

Public Key:
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:71:41:C1:62:D2:C8:98:28:6F:6B:28:C0:BC:68:9A:6A:26:83:28:D8:CB:B1:05:D0:BE:1F:E6:95:44:BC:BA:D0:59:D7:D5:13:11:28:52:19:83:A2:08:EA:9E:BD:54:A7:3D:47:9C:1F:57:63:70:77:F6:6D:38:5D:FE:EF:5A:70

Basic Constraints *IsCA: false*

Authority Key Identifier *48:02:BE:75:74:31:DE:28:BF:6C:8B:89:8D:A2:D8:A5:67:E5:1D:64*

Authority Info Access
http://www.cert.fnmt.es/certs/ACTSAG2.crt
http://ocsptsag2.cert.fnmt.es/ocsptsag2/OcspResponder

Certificate Policies
Policy OID: 1.3.6.1.4.1.5734.3.28.1.0
CPS pointer: http://www.cert.fnmt/dpcs/
CPS text: [Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://www.cert.fnmt.es/crlsactsafnmtg2/CRL.crl*

Subject Key Identifier *93:C8:F7:02:84:73:1A:69:D3:F2:90:41:D0:A0:A7:3B:7B:85:07:DC*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint:
56:CA:B2:CD:97:7B:47:C1:4F:00:67:D3:04:B8:55:4A:0E:31:BA:1D:21:B0:F1:5B:D
F:7F:AA:81:9D:A0:31:76

X509SubjectName

Subject CN: *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM-TSU 2025*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject 0: *FNMT-RCM*

Subject L: *MADRID*

Subject C: ES

X509SKI

X509 SK I *k8j3AoRzGmnT8pBB0KCnO3uFB9w=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Service status description	[en]	undefined.

[es] undefined.

Status Starting Time 2025-07-17T02:00:00Z

4.21 - Service (granted): Qualified certificates issued by AC TSA CLIENTES

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified certificates issued by AC TSA CLIENTES

Name [es] *Certificados cualificados emitidos por AC TSA CLIENTES*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 530036330854435450328521346880634557618719955141

X509 Certificate -----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: AC RAIZ FNMT-RCM TSA

Issuer 2.5.4.97: *VATES-Q2826004I*

Issuer O: *FNMT-RCM*
Issuer C: *ES*
Subject CN: *AC TSA CLIENTES*
Subject 2.5.4.97: *VATES-Q2826004J*
Subject O: *FNMT-RCM*
Subject C: *ES*
Valid from: *Thu Oct 10 12:04:18 CEST 2024*
Valid to: *Fri Oct 07 12:04:17 CEST 2039*
Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:C7:F3:F5:08:AE:78:7C:66:F5:27:83:DA:69:0E:DF:C6:3C:08:52:10:96:ED:F1:BE:59:DF:F9:0A:1C:7D:CF:ED:64:83:92:82:D6:72:AF:78:FC:59:0D:09:8A:84:43:7D:93:2C:0B:34:F7:2D:60:45:E8:1E:FE:05:1C:49:E2:5F:84:1C:96:0E:91:FD:A6:81:7B:9B:51:CA:42:6A:FC:EF:E6:12:8D:E0:B8:B1:FD:00:36:A4:85:17:D8:5E:1A:38*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *8F:18:75:3B:80:43:DC:18:C1:6E:E3:B4:B6:6A:AC:F7:37:66:09:01*
Authority Info Access *http://www.cert.fnmt.es/certs/ACRAIZFNMTTSA.crt*
http://ocspraiztsa.cert.fnmt.es/ocspraiztsa/OcspResponder
Certificate Policies *Policy OID: 2.5.29.32.0*
Extended Key Usage *id_kp_timeStamping*
CRL Distribution Points *http://www.cert.fnmt.es/crls/ACRAIZFNMTTSA.crl*
Subject Key Identifier *F2:D4:61:F8:CA:96:BD:5C:3D:1E:A6:96:7E:E4:95:7D:49:E1:2A:6D*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *8E:6A:F1:E1:37:7A:DF:7E:F1:9A:89:79:6D:2C:3D:D7:2A:C0:9D:86:44:8A:47:C9:2C:2F:F9:1E:C3:D0:25:9E*

X509SubjectName

Subject CN: *AC TSA CLIENTES*
Subject 2.5.4.97: *VATES-Q2826004J*
Subject O: *FNMT-RCM*
Subject C: *ES*

X509SKI

X509 SK I *8tRh+MqWvVw9HqaWfuSVfUnhKm0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-07-17T02:00:00Z*

4.21.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5 - TSP: Consorci Administració Oberta de Catalunya - CAOC

TSP Name

Name [en] *Consorci Administració Oberta de Catalunya - CAOC*

Name [es] *Consorci Administració Oberta de Catalunya - CAOC*

TSP Trade Name

Name [en] *VATES-Q0801175A*

Name [en] *Consorci AOC (CATCert)*

Name [es] *Consorci AOC (CATCert)*

Name [en] *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Name [es] *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Name [en] *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

PostalAddress

Street Address [en] *Calle Salvador Espriu, 45-51*

Locality [en] *L'Hospitalet del Llobregat*

State Or Province [en] *Barcelona*

Postal Code [en] *08908*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Calle Salvador Espriu, 45-51*

Locality [es] *L'Hospitalet del Llobregat*

State Or Province [es] *Barcelona*

Postal Code [es] *08908*

Country Name [es] *ES*

ElectronicAddress

URI [en] *http://www.aoc.cat*

URI	[en]	http://www.aoc.cat

URI [es] *<http://www.aoc.cat>*

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	<i>[en]</i> A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	<i>[es]</i> Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[en]	Qualified certificates issued by CA IdCAT

Name [es] *Certificados Reconocidos emitidos por CA idCAT*

Version: 3

Serial Number: 149207157159073437715447019610265252046

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: EC-ACC

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu <https://www.catcert.net/verarrel> (c)03*

Issuer OU: *Serveis Publics de Certificacio*
Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Issuer C: *ES*
Subject CN: *EC-IDCat*
Subject OU: *Entitat publica de certificacio de ciutadans*
Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*
Subject OU: *Serveis Publics de Certificacio ECV-2*
Subject L: *Passatge de la Concepcio 11 08008 Barcelona*
Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C: *ES*
Valid from: *Fri Oct 31 11:40:39 CET 2003*
Valid to: *Thu Oct 31 11:40:39 CET 2019*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BB:DF:40:C3:D4:1C:11:79:22:CF:2A:54:B3:CD:F2:EB:B7:84:44:CD:4B:48:41:9E:01:47:80:D1:E1:80:60:31:69:C9:AE:ED:29:AE:A9:EF:AB:D7:60:ED:29:5D:C0:F2:74:85:79:57:56:4A:0B:33:EC:B5:52:56:34:10:4C:B6:B0:5C:CC:03:CB:5F:9F:69:D5:C6:C7:90:27:17:BF:F2:26:00:25:E3:4D:42:24:20:EA:69:CB:80:B6:8E:F4:00:F7:FD:0D:99:A8:3C:3E:04:82:9E:4F:B8:EE:68:0A:22:A9:DC:97:FA:7B:E1:F4:08:F2:4C:A8:B9:C8:C9:3C:5E:5F:7D:8B:C0:76:0A:D2:A0:B0:3A:18:31:88:1B:ED:26:68:DD:31:FB:27:43:54:CA:9F:A6:17:8E:EC:65:E7:BA:FF:45:00:B1:1B:65:F9:EC:7A:AE:C5:A6:4A:17:33:CD:F4:6D:49:67:C4:0E:B7:18:01:26:3D:F4:AC:D1:2D:49:11:6E:A5:86:4D:83:46:C3:EE:24:C5:F6:87:DF:57:C9:FF:A5:52:7A:43:CC:FE:88:35:67:ED:10:FE:20:D5:2D:2C:99:BE:89:1C:50:41:C5:32:2B:5C:8D:FA:51:02:64:6A:CE:61:7D:13:83:ED:78:42:9B:FD:96:AC:AB:EB:59:02:03:01:00:01*
Issuer Alternative Name *ec_acc@catcert.net*
Subject Alternative Name *ec_idcat@catcert.net*
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *CD:92:C0:45:46:34:76:0D:D2:F4:5B:A2:74:1D:AB:CF:6C:B6:0B:B9*
Authority Key Identifier *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*
Certificate Policies *Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*
CPS pointer: <https://www.catcert.net/verCIC-2>
CPS text: [Aquest certificat semet única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]
CRL Distribution Points *<http://epsd.catcert.net/crl/ec-acc.crl>*
<http://epsd2.catcert.net/crl/ec-acc.crl>
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*

Thumbprint: *95:4B:88:92:23:49:8A:ED:51:AA:7A:29:B6:2E:ED:24:BE:03:CD:48:1D:18:2E:03:EB:83:BA:E8:DD:7B:D7:1B*

X509SubjectName

Subject CN: *EC-IDCat*

Subject OU: *Entitat publica de certificacio de ciutadans*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

5.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

5.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] [Qualified certificates issued by CA IdCAT](#)*

Name *[es] [Certificados Reconocidos emitidos por CA idCAT](#)*

Service digital identities**X509SubjectName**

Subject CN: *EC-IDCat*

Subject OU: *Entitat publica de certificacio de ciutadans*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *zZLARUY0dg3S9FuidB2rz2y2C7k=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2016-06-30T22:00:00Z*

5.1.2.1 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

5.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service Name

Name *[en]* *Qualified certificates issued by CA IdCAT*

Name *[es]* *Certificados Reconocidos emitidos por CA idCAT*

Service digital identities**X509SubjectName**

Subject CN: *EC-IDCat*

Subject OU: *Entitat publica de certificacio de ciutadans*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *zZLARUY0dg3S9FuidB2rz2y2C7k=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2006-01-23T00:00:00Z*

5.2 - Service (withdrawn): Certificados Reconocidos emitidos por CA AL

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name [es] *Certificados Reconocidos emitidos por CA AL*

Name [en] *Qualified certificates issued by CA AL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *81871235804792199700514938710945526542*

Subject Key Identifier *4C:EC:8D:49:D4:2B:02:03:9A:D0:48:30:0A:4B:6B:BD:31:7A:A6:34*

Authority Key Identifier *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

Certificate Policies
Policy OID: 1.3.6.1.4.1.15096.1.3.1.12
CPS pointer: <https://www.catcert.net/verCIC-2>
CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]

CRL Distribution Points
<http://epsd.catcert.net/crl/ec-acc.crl>
<http://epsd2.catcert.net/crl/ec-acc.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *59:2C:50:8E:39:D7:66:5F:84:45:86:C3:B9:E7:65:AF:D5:D8:0B:BE:05:F9:28:9C:B0:DE:D5:71:1A:C9:C1:0A*

X509SubjectName

Subject CN: *EC-AL*

Subject OU: *Administracions Locals de Catalunya*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Service Status*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time*2018-03-15T01:00:00Z***Scheme Service Definition URI**

URI *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

5.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

5.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

5.2.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA AL

Name [en] Qualified certificates issued by CA AL

Service digital identities

X509SubjectName

Subject CN: EC-AL

Subject OU: Administracions Locals de Catalunya

Subject OU: Vegeu https://www.catcert.net/verCIC-2 (c)03

Subject OU: Serveis Publics de Certificacio ECV-2

Subject L: *Passatge de la Concepció 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados Reconocidos emitidos por CA AL*

Name [en] *Qualified certificates issued by CA AL*

Service digital identities**X509SubjectName**

Subject CN: *EC-AL*

Subject OU: *Administracions Locals de Catalunya*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

Policy Identifier:

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	<i>[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[es]	Certificados Reconocidos emitidos por CA SAFP
Name	[en]	Qualified certificates issued by CA SAFP

Certificate fields details

Version:	3
Serial Number:	148786221414740922626357724534625015094
X509 Certificate	-----BEGIN CERTIFICATE-----

[illegible]

Signature algorithm: *SHA1withRSA*

Issuer CN: *EC-GENCAT*

Issuer OU: *Generalitat de Catalunya*

Issuer OU: *Vegeu <https://www.catcert.net/verCIC-1> (c)03*

Issuer OU: *Serveis Publics de Certificacio ECV-1*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-SAFP*

Subject OU: *Secretaria d'Administracio i Funcio Publica*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Valid from: *Wed Jan 08 14:01:10 CET 2003*

Valid to: *Mon Jan 07 23:59:59 CET 2019*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:99:23:C6:CA:08:61:2E:FF:C1:86:64:64:D4:49:D7:58:9B:76:66:30:09:49:BA:AF:CD:E4:22:80:1F:2C:34:16:97:81:13:51:80:90:F8:D4:86:0E:21:F7:ED:8F:18:9E:8D:94:B3:FC:A0:5F:F4:08:09:4E:E3:9D:BE:27:F8:48:09:71:73:63:AF:FD:D4:AE:D2:0E:96:34:0A:04:C8:4E:7A:4A:F7:09:3E:C0:7F:FE:92:F9:23:DB:25:90:D1:BC:5B:F2:D1:99:38:9E:A6:84:FF:0A:54:B5:9A:5C:51:11:86:4B:30:91:16:FB:20:E4:28:6A:5F:DA:7E:61:09:39:F9:5F:A0:2D:4B:F7:5F:FD:F5:E3:39:15:38:0F:D2:11:3C:47:68:A7:B7:F8:9C:82:37:BB:C0:A5:AE:5C:70:9D:8A:37:4D:93:D7:51:DB:50:14:14:78:F7:F9:F7:C7:E0:B7:05:F1:7E:AA:23:37:37:55:E0:EB:63:46:50:C:E:09:3C:AE:43:26:40:C4:6E:7D:CE:9E:1F:AC:CE:28:56:E7:81:2C:AC:D5:53:30:40:58:61:95:16:C7:5A:A8:79:F4:2A:71:86:15:A8:1F:D2:46:13:6C:58:3A:6D:42:99:21:66:CE:13:13:80:8B:F9:BC:F2:89:A3:60:D6:18:86:89:02:03:01:00:01*

Issuer Alternative Name *ec_gencat@catcert.net*

Subject Alternative Name *ec_safp@catcert.net*

Basic Constraints *IsCA: true*

Subject Key Identifier *05:B7:ED:4F:16:52:DD:FA:E6:92:C0:A2:72:79:56:60:54:C2:24:13*

Authority Key Identifier *31:6A:5C:0A:46:4E:37:AF:42:E3:B0:60:2B:0C:0F:2D:2F:93:DF:14*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*
CPS pointer: <https://www.catcert.net/verCIC-2>
CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]

CRL Distribution Points *<http://epsd.catcert.net/crl/ec-gencat.crl>*
<http://epsd2.catcert.net/crl/ec-gencat.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: 20:7C:EC:E0:38:B9:82:6A:12:0A:91:9D:4B:41:BC:A8:F3:7F:2E:99:46:21:BF:5A:99:3A:04:08:7D:55:6D:C6

X509SubjectName

Subject CN: EC-SAFP

Subject OU: Secretaria d'Administracio i Funcio Publica

Subject OU: Vegeu <https://www.catcert.net/verCIC-2> (c)03

Subject OU: Serveis Publics de Certificacio ECV-2

Subject L: Passatge de la Concepcio 11 08008 Barcelona

Subject O: Agencia Catalana de Certificacio (NIF Q-0801176-I)

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2018-03-15T01:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados Reconocidos emitidos por CA SAFP*

Name [en] *Qualified certificates issued by CA SAFP*

Service digital identities**X509SubjectName**

Subject CN: *EC-SAFP*

Subject OU: *Secretaria d'Administracio i Funcio Publica*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *BbftTxZS3frmksCicnIWYFTCJBM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

5.3.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

5.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA SAFP

Name [en] Qualified certificates issued by CA SAFP

Service digital identities**X509SubjectName**

Subject CN: EC-SAFP

Subject OU: Secretaria d'Administracio i Funcio Publica

Subject OU: Vegeu https://www.catcert.net/verCIC-2 (c)03

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *BbftTxZS3frmksCicnIWYFTCJBM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] [es]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i> <i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.4 - Service (withdrawn): Certificados Reconocidos emitidos por CA PARLAMENT

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Name [es] *Certificados Reconocidos emitidos por CA PARLAMENT*

Name	[en]	Qualified certificates issued by CA PARLAMENT

Version: 3

Serial Number: 49921083824290425381953941137842983617

[illegible]

Signature algorithm: *SHA1withRSA*

Issuer CN: EC-ACC

Issuer OU: *Jerarquia Entitats de Certificacio Catalanes*

Issuer OU: *Vegeu <https://www.catcert.net/verarrel> (c)03*

Issuer OU: *Serveis Publics de Certificacio*

Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Issuer C: *ES*

Subject CN: *EC-PARLAMENT*

Subject OU: *Parlament de Catalunya*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepció 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Valid from: *Wed Jun 30 10:57:35 CEST 2004*

Valid to: *Mon Jun 29 23:59:59 CEST 2020*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:09:97:D7:07:DE:74:B6:A7:F4:5F:CF:9C:9E:71:95:22:62:97:2F:92:36:75:0C:9C:B6:9C:D8:11:EB:0A:A6:E5:EC:7B:A8:8D:75:F0:B5:89:7C:05:16:4C:8F:3F:60:89:D3:5D:E5:A6:D0:47:04:9A:A3:41:1A:C9:9E:82:ED:7E:5E:98:37:F1:C2:D6:88:A1:6D:BE:F4:EB:21:64:85:D7:CA:7C:2E:C4:92:C9:26:42:D0:09:24:1D:15:BA:2B:25:05:5C:4E:BE:88:1F:AA:28:1F:69:3B:8E:DF:2B:5C:B7:34:14:67:F3:DD:58:0A:FF:5C:BA:9B:BE:F8:5F:A5:44:FD:76:67:18:E8:18:04:29:8A:7F:2B:66:D7:8D:00:81:1D:6E:73:9E:4D:19:8A:DE:12:40:5A:78:0C:C2:C5:51:2C:89:30:BE:0F:D2:0D:C1:FB:3D:AF:26:5F:D5:D3:43:FB:1E:45:89:D3:59:F1:7F:D9:10:D7:83:5C:CF:C1:E7:9E:24:1C:2C:11:04:00:29:6C:21:68:3A:D6:B5:86:70:80:7B:8E:50:F9:22:61:98:FC:A7:1A:3E:38:E3:54:FB:3F:D0:5F:8F:B4:2F:44:04:6F:C4:2D:DC:38:96:5F:1D:0D:7B:51:A2:1B:EB:8E:AB:62:87:4E:A1:39:9A:EF:02:03:01:00:01*

Issuer Alternative Name *ec_acc@catcert.net*

Subject Alternative Name *ec-parlament@catcert.net*

Basic Constraints *IsCA: true*

Subject Key Identifier *1E:13:98:EA:C2:42:59:55:B6:DE:2F:3E:CA:9F:C9:EA:CB:2E:2C:14*

Authority Key Identifier *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*
CP5 pointer: <https://www.catcert.net/verCIC-2>
CP5 text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]

CRL Distribution Points *<http://epsd.catcert.net/crl/ec-acc.crl>*
<http://epsd2.catcert.net/crl/ec-acc.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *44:C5:0A:C8:0E:DB:E9:E5:52:E3:C9:6C:E5:BD:11:C8:37:C7:0F:56:A3:3A:CA:BC:F1:8D:8D:7A:9B:35:0E:07*

X509SubjectName

Subject CN: *EC-PARLAMENT*

Subject OU: *Parlament de Catalunya*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepció 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2018-03-15T01:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

5.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

Policy Identifier:

Identifier *[OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

Policy Identifier:

Identifier *[OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier *[OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

5.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA PARLAMENT*

Name *[en]* *Qualified certificates issued by CA PARLAMENT*

Service digital identities

X509SubjectName

Subject CN: *EC-PARLAMENT*

Subject OU: *Parlament de Catalunya*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

5.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

5.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Reconocidos emitidos por CA PARLAMENT*

Name [en] *Qualified certificates issued by CA PARLAMENT*

Service digital identities

X509SubjectName

Subject CN: *EC-PARLAMENT*

Subject OU: *Parlament de Catalunya*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2010-05-05T00:00:00Z*

5.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

5.5 - Service (withdrawn): Certificados Reconocidos emitidos por CA UR

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados Reconocidos emitidos por CA UR

Name [en] Qualified certificates issued by CA UR

Service digital identities

Certificate fields details

Version: 3

Serial Number: 8834028594214827114689084859419303276

Basic Constraints	<i>IsCA: true</i>
Subject Key Identifier	<i>48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B</i>
Authority Key Identifier	<i>A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.15096.1.3.1.12</i> <i>CPS pointer: https://www.catcert.net/verCIC-2</i> <i>CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu https://www.catcert.net/verCIC-2]</i>
CRL Distribution Points	<i>http://epsd.catcert.net/crl/ec-acc.crl</i> <i>http://epsd2.catcert.net/crl/ec-acc.crl</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>87:00:D0:47:E5:07:11:16:F6:75:51:A4:39:39:98:D6:29:E6:6F:02:C7:B5:2E:61:8E:F4:F9:49:6E:73:47:56</i>

X509SubjectName

Subject CN:	<i>EC-UR</i>
Subject OU:	<i>Universitats i Recerca</i>
Subject OU:	<i>Vegeu https://www.catcert.net/verCIC-2 (c)03</i>
Subject OU:	<i>Serveis Publics de Certificacio ECV-2</i>
Subject L:	<i>Passatge de la Concepcio 11 08008 Barcelona</i>
Subject O:	<i>Agencia Catalana de Certificacio (NIF Q-0801176-I)</i>
Subject C:	<i>ES</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time*2018-03-15T01:00:00Z***Scheme Service Definition URI**

URI	<i>[es]</i>	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI	<i>[en]</i>	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

5.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3

5.5.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

5.5.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA UR

Name [en] Qualified certificates issued by CA UR

Service digital identities**X509SubjectName**

Subject CN: EC-UR

Subject OU: Universitats i Recerca

Subject OU: Vegeu https://www.catcert.net/verCIC-2 (c)03

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *SJ+NhtHL8daKUnt/FaIKUfiX/gs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3*

5.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Reconocidos emitidos por CA UR*

Name *[en]* *Qualified certificates issued by CA UR*

Service digital identities

X509SubjectName

Subject CN: *EC-UR*

Subject OU: *Universitats i Recerca*

Subject OU: *Vegeu https://www.catcert.net/verCIC-2 (c)03*

Subject OU: *Serveis Publics de Certificacio ECV-2*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *SJ+NhtHL8daKUnt/FaIKUfiX/gS=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3*

Issuer OU: *Universitats i Recerca*
Issuer OU: *Vegeu <https://www.catcert.net/verCIC-2> (c)03*
Issuer OU: *Serveis Publics de Certificacio ECV-2*
Issuer L: *Passatge de la Concepcio 11 08008 Barcelona*
Issuer O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Issuer C: *ES*
Subject CN: *EC-URV*
Subject OU: *Universitat Rovira i Virgili*
Subject OU: *Vegeu <https://www.catcert.net/verCIC-3> (c)05*
Subject OU: *Serveis Publics de Certificacio*
Subject L: *Passatge de la Concepcio 11 08008 Barcelona*
Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C: *ES*
Valid from: *Fri Apr 17 11:47:19 CEST 2009*
Valid to: *Tue Apr 16 23:59:59 CEST 2019*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EB:9F:6A:FF:FA:42:3F:EF:A7:6F:D9:7C:92:42:2E:F3:CE:39:EB:13:D1:F5:11:38:00:80:DD:0E:66:02:9C:E1:F0:AF:03:58:2D:0D:B1:87:FC:2B:87:80:34:50:E2:30:27:3E:BA:BF:00:93:07:9A:A0:9D:D7:08:82:E6:13:D4:28:D9:7B:FC:7E:AE:F7:D3:6E:72:62:65:D9:42:A1:7F:BD:4A:F0:1D:15:D6:8D:F4:16:82:F0:0B:F5:66:76:43:16:94:8E:69:A7:9A:1B:F4:5B:BD:C8:99:25:D4:CD:EE:1B:A7:0C:1D:DC:85:33:15:30:ED:40:11:AC:2B:66:40:27:6B:00:7F:16:6E:B6:0A:08:BE:88:42:DD:6B:20:EA:3A:C3:AE:9A:58:D8:6D:82:BC:7B:1F:A8:3C:53:9D:CB:91:40:A9:EC:9D:AA:D6:90:BE:ED:12:28:E3:42:14:A3:E9:C0:FA:CC:4A:76:87:AA:6D:08:F7:37:8D:81:FF:BC:7A:1B:2F:31:3D:E6:0F:00:1C:FD:64:C0:67:00:31:6D:76:A9:3C:82:E7:E4:9A:51:6C:F9:29:60:82:8E:5C:0D:61:E2:54:4D:5F:31:C4:86:3D:6D:A3:0C:E5:2D:9B:CA:B9:8F:7C:A3:25:57:C4:84:A6:D6:46:AA:B2:2E:D5:E9:02:03:01:00:01*
Issuer Alternative Name *ec_ur@catcert.net*
Subject Alternative Name *ec-urv@catcert.net*
Basic Constraints *IsCA: true*
Subject Key Identifier *BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E*
Authority Key Identifier *48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*
Certificate Policies *Policy OID: 1.3.6.1.4.1.15096.1.3.1.13*
CPS pointer: <https://www.catcert.net/verCIC-3>
CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3. Vegeu <https://www.catcert.net/verCIC-3>]
CRL Distribution Points *<http://epsd.catcert.net/crl/ec-ur.crl>*
<http://epsd2.catcert.net/crl/ec-ur.crl>

Key Usage:*keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***A4:65:2E:D2:43:DA:CC:3F:EE:E1:F0:ED:7C:91:BD:B1:9A:9B:C2:25:E7:2A:5C:97:F
D:A4:F1:F0:01:25:BA:A3***Certificate fields details****Version:***3***Serial Number:***132441740454361425377162905070003236530***X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIHhDCCBgCgAwIBAgIQY6NZ9DJTvilCd0YS4IsusIANBqkqhkiG9w0BAQUFADCCARgx CzAlBgNV
BAYTAKVMTSswOQYDVQKKEzBZ2VuuY2JhIEhndGfsYw5hGRIENicnRzmljYWNpbyAoTkIGFET
BDgwMTESWlJkTEUMDGA1UEBXMwUGFzc2F0Z2UgZGUGbGEGQ29uY2VwY2VlDEIDAMDA4IEJh
cmNlGCUyTEUjKwCAIUeCzMIU2VydmlpbyB0dWJsaW5hZGRIENicnRzmljYWNpbyB0Y1YmE1
MDMGA1UECXM5MmVnZXUgaHR0CHM6Lm93d3cuY2F0Y2VydC5uZXQvdmlvY00DLTlgkGMPMDMxHzAd
BgNVBASTFVlvaXZicnNpdGF0cyB0fjY2VvY2E0AMBgNVBAMTBUDLVVSMBA4XDAlMDUwMzAs
MetyxP0X0TEzMDUwMzAsMetyxP0fowagZM0swCQYDVQGEwFUEzFMDkGA1UEChMyQWdlbmNpYSBD
YXRhbGZuY3BkZSBkZjI0aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxNDAYBgNVBACzK1Bhc3Nh
dGdlIGRIIGxhIEWbmlkGNDpYXMSAwODAwOCBCYXJlZmVwbnEkdambGnVBASTH1Nlc3ZlaXNp
UHVudGlicyBkZSBkZjI0aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IChndHBoO8v3d3LmNhdGNI
cnQubmV0L3ZickNjOy0zChjKTA1MSUwWwYDVQOLExxVbmlDZXJzaXRhdCB5b3ZpcmEgaSBWaxIn
aWxpMQ8wDQYDVQDEwZ2F0Y1VlUWggEiMA0GCSqGSIb3DQEBAAQUAA4IBDWAwwgEKAoIBAQQm2r/
+HJ76dv2Nys07TzpmE9HJEtpaANOOZpk4C4YAJgtDbc3Cu3sDR04JanpQAJHmfgc1Iwic
5hPUKNI7H6u99NucmJlZUKhf71K8B0V1o30FoLwC/VmdkMWI5pp5ob9f9ujkI1M3uG6cMHdyF
MxUw7UAR/CtmQCdrAH8WbtrKCL6Q11i0o6w66aWhtgrx7H6g8U53LkUCp7Jzq1pC+7Rlo40IU
o+nk++sk0e0pQ3JN4Z87x6Gv8PehfABzMB04Df0q8gurfimf++Sigso5cDWHVETfMCSG
PW2JDOUTm8a53vjVfEHkbWRgqyLXpAgMBAAGiggl-3MIICBzAcBqNVHRIETATgRFY191ckBj
YXRjZXJlLn5ldAdBgNVHREEFjAUGRjY1Y1cnZAY2F0Y2VydC5uZXQvdWYDVROTAAQHBAUWAweB
ZaOB9NVHQBABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROj
BIBKCCASSAFEifYbry/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkG
AlUEChMyQWdlbmNpY3BkZSBkZjI0aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkx
KDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1
IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjKTAzMTUwWwYDVQOLEyxKZXJhcnF1
aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EPMA0GA1UEAxMGRUMTQUJ0dGhAG
pV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwEENMIG+MCwGCcsGAQUF
BwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUHAgIwYAAfFx
dWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQBABE
BAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5pH2MhZMQswCQYDVQQGEWlueE7MDkGAlUEChMyQWdlbmNpY3BkZSBkZjI0
aWZpY2FjaW8gKE5jRiBRLTA4MDEuNzYtSSkxKDAmBgNVASTH1Nlc3ZlaXNpUHVudGlicyBkZSBkZjI0
aWZpY2FjaW8wNVAzZG9uVnVASTFZ2Z2V1IGh0dHBzO8v3d3LmNhdGNIcnQubmV0L3ZickNjOy0zChjK
TAzMTUwWwYDVQOLEyxKZXJhcnF1aWVgeWV5daxRhdHhMgZGUGQ2VydGImaWWhY2VlENhndGfsYw5lc2EP
MA0GA1UEAxMGRUMTQUJ0dGhAGpV88soCQYDVQSE5bZ1sMIHicBgNVHSAEgdwgdEwpc4CCysGAQQB9qBwE
ENMIG+MCwGCcsGAQUFBwIBFodHRwczovL3d3dy5jYXRjZXJ0Lm5ldG92ZXJlD0SUMtMzCBjQYIKwYBBQUH
AgIwYAAfFxdWVzOCBjZXJ0aWZpY2F0L0ZicG90Y2VydC5uZXQvdWYDVROTAAQHBAUWAweBZaOB9NVHQB
ABEBAIMCAQYwHQYDVRODBEFfLsuq54w1JwQC7X9pKTCFstRRI7k+MI8QYOVROjBIBKCCASSAFEifYbry
/HWij7fxWiCH4I/4LoYH5p
```

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*
Subject C: *ES*
Valid from: *Tue May 03 11:36:18 CEST 2005*
Valid to: *Fri May 03 11:36:18 CEST 2013*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EB:9F:6A:FF:FA:42:3F:EF:A7:6F:D9:7C:92:42:2E:F3:CE:39:E8:13:D1:F5:11:38:00:80:DD:0E:66:02:9C:E1:F0:AF:03:58:20:0D:B1:B7:FC:2B:87:80:34:50:E2:30:27:3E:BA:BF:00:93:07:9A:A0:9D:D7:08:82:E6:13:D4:28:D9:7B:FC:7E:AE:F7:D3:6E:72:62:65:D9:42:A1:7F:BD:4A:F0:1D:15:D6:8D:F4:16:82:F0:0B:F5:66:76:43:16:94:8E:69:A7:9A:1B:F4:5B:BD:C8:99:25:D4:CD:EE:1B:A7:0C:1D:DC:85:33:15:30:ED:40:11:AC:2B:66:40:27:68:00:7F:16:6E:B6:0A:08:BE:88:42:DD:6B:2D:EA:3A:C3:AE:9A:58:D8:6D:82:BC:7B:1F:A8:3C:53:9D:CB:91:40:A9:EC:9D:AA:D6:90:BE:ED:12:28:E3:42:14:A3:E9:C0:FA:CC:4A:76:87:AA:6D:08:F7:37:8D:81:FF:BC:7A:1B:2F:31:30:E6:DF:00:1C:FD:64:C0:67:00:31:6D:76:A9:3C:82:E7:E4:9A:51:6C:F9:29:60:82:8E:5C:0D:61:E2:54:4D:5F:31:C4:86:3D:6D:A3:0C:E5:2D:9B:CA:B9:8F:7C:A3:25:57:C4:84:A6:D6:46:AA:B2:2E:D5:E9:02:03:01:00:01*
Issuer Alternative Name *ec_ur@catcert.net*
Subject Alternative Name *ec-urv@catcert.net*
Basic Constraints *IsCA: true*
Subject Key Identifier *BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E*
Authority Key Identifier *48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*
Certificate Policies *Policy OID: 1.3.6.1.4.1.15096.1.3.1.13*
CPs pointer: <https://www.catcert.net/verCIC-3>
CPs text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3. Vegeu <https://www.catcert.net/verCIC-3>]
CRL Distribution Points *<http://epsd.catcert.net/crl/ec-ur.crl>*
<http://epsd2.catcert.net/crl/ec-ur.crl>
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *88:33:D0:A9:1F:26:45:EF:EF:C3:B4:E0:0F:B8:97:C5:20:65:7E:BC:88:EA:F7:3B:9E:F0:F1:9A:2C:7B:A1:53*
X509SubjectName
Subject CN: *EC-URV*
Subject OU: *Universitat Rovira i Virgili*
Subject OU: *Vegeu <https://www.catcert.net/verCIC-3> (c)05*
Subject OU: *Serveis Publics de Certificacio*
Subject L: *Passatge de la Concepcio 11 08008 Barcelona*
Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2018-03-15T01:00:00Z

Scheme Service Definition URI

URI [es] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [en] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

5.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

5.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

5.6.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Reconocidos emitidos por CA URV*

Name [en] *Qualified certificates issued by CA URV*

Service digital identities**X509SubjectName**

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu https://www.catcert.net/verCIC-3 (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *uy6pLjDUnBBztf2pd8I+w1GXuT4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.6.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5*

Policy Identifier:

Identifier [OIDsAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

Policy Identifier:

Identifier [OIDsAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

5.6.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados Reconocidos emitidos por CA URV*

Name [en] *Qualified certificates issued by CA URV*

Service digital identities**X509SubjectName**

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu https://www.catcert.net/verCIC-3 (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

X509SKI

X509 SK I *uy6pLjDUnBBztf2pd8I+w1GXuT4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-05-05T00:00:00Z*

5.6.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

5.7 - Service (granted): Qualified certificates issued by CA Ciudadania

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified certificates issued by CA Ciudadania
Name	[es]	Certificados Reconocidos emitidos por CA Ciudadania

Service digital identities

Certificate fields details

Version:	3
Serial Number:	154100517041182570311467181176543273551

Authority Info Access *http://ocsp.catcert.cat*

CRL Distribution Points *http://epsd.catcert.net/crl/ec-acc.crl*
http://epsd2.catcert.net/crl/ec-acc.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6*

X509SubjectName

Subject CN: *EC-Ciutadania*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

5.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.7.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by CA Ciutadania*

Name [es] *Certificados Reconocidos emitidos por CA Ciutadania*

Service digital identities

X509SubjectName

Subject CN: *EC-Ciutadania*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *C2hZPofloxUa4ECCII+fHbLFNxU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-11-17T23:00:00Z*

5.8 - Service (granted): Qualified certificates issued by CA SectorPublic

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified certificates issued by CA SectorPublic*

Name [es] *Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *151118660848720701053205649823964411794*

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIF4zCCBMugAwIBAgIQcbBIOXyOB9IUGpZ/dV3k3kANBgkqhkiG9w0BAQoFADCB8zELMAKGA1UE
BhMCRVXmQzA5BgNVBAQTMkFhZjW5aWVWegQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0w
ODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0
VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UE
CxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYD
MDEGA1UECgwQ09OU09S00kgOURNSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYD
VQOLCFTZjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwgYDVo
QLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwczov
L3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90
YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbm
EgZGUgQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3Mq
ZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2V
hcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOK
VSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0
wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOL
EwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVv
YXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYD
ZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2Xj
Z2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYX
ZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5l
U1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2
VlChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2Vl
MTUwMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDM
GA1UECxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0Ux
VtI0BMsowKAYDZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwg
YDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwcz
ovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90
YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbmEg
ZGUgQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5
pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2Vhcn
libCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSV
EEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0wO
DAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEV
wZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYX
JkdWlnIEVudG90YXN0aW90S0RUSU5lU1RSQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9
wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2VlChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2Wl
B1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTUwMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0
Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1UECxMsSmVvYXJkdWlnIEVudG90YXN0aW90S0RUSU5lU1R
SQUJlYTBOKVSVEEgREUgQ0F0U0UxVtI0BMsowKAYDZC9wQ2F0YVWxbmEgZGUgQ2VydGlnaWNhY2Vl
ChOSUYguS0wODAMTCZlUkpsSgwgYDVoQLEs9T2XjZ2WlB1YmtpY3MqZC5pQ2VydGlnaWNhY2VlMTU
wMmY0VQOLEVwZWRldG5odHRwczovL3Q3dy5YXRYXZjX0Jm5lCg9Z2VhcnlibCAtYkwMzE1MDMGA1U
E
-----END CERTIFICATE-----

```

Signature algorithm:*SHA256withRSA***Issuer CN:***EC-ACC***Issuer OU:***Jerarquia Entitats de Certificacio Catalanes***Issuer OU:***Vegeu <https://www.catcert.net/verarrel> (c)03***Issuer OU:***Serveis Publics de Certificacio***Issuer O:***Agencia Catalana de Certificacio (NIF Q-0801176-I)***Issuer C:***ES***Subject CN:***EC-SectorPublic***Subject OU:***Serveis Públics de Certificació***Subject O:***CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA***Subject C:***ES***Valid from:***Thu Sep 18 10:23:27 CEST 2014***Valid to:***Wed Sep 18 10:23:27 CEST 2030***Public Key:**

```

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:AE:4E:31:31:BC:F1:0B:11:F1:89:DC:C5:3D:47:39:D2:70:42:0B:F2:A4:C4
:4F:06:53:38:51:99:80:50:6F:46:81:80:24:15:77:41:C5:D2:5E:9F:7E:AF:98:7B:73:2A:B5:F4:32:8B:4E:2A:91:84:A9:A7:C1:20:DF:40:21:D8:86:FE:26:20:95:0C:F2:66:C4:64:24:70:43:67
:ED:D5:34:55:D5:81:85:9D:46:60:84:B8:77:D8:F8:D2:AE:39:5C:65:C4:C7:E6:80:1A:4B:CB:86:5D:D2:13:7F:80:26:9A:CF:70:6B:E0:31:EF:4E:57:14:27:79:DA:C8:E2:07:8A:94:26:DA:7A:
:84:C0:B8:10:20:87:8D:66:CB:C3:40:24:A7:8B:CF:88:F7:DB:84:80:31:83:8D:34:F3:AF:5E:88:CC:84:76:44:2C:41:8C:60:CF:2A:C4:13:D9:A8:34:54:55:EB:AC:87:8B:1F:1E:9E:FD:50:98:D
:F:CD:90:CA:9D:24:58:32:F3:A1:CF:D8:63:EB:40:EF:78:7C:E3:46:48:1D:A6:CF:FA:E2:E2:A7:C6:63:57:A8:AE:83:E7:9B:94:3C:22:25:AD:BD:F0:DA:04:A8:BF:0D:6E:63:FA:88:14:27:BF:86
:C3:A7:CC:01:85:52:C1:D6:A3:C3:02:03:01:00:01

```

Basic Constraints*IsCA: true - Path length: 0***Subject Key Identifier***47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73:DC:E2:D9***Authority Key Identifier***A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D***Certificate Policies***Policy OID: 2.5.29.32.0**CPS pointer: <https://www.aoc.cat/CATCert/Regulacio>**CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació. Vegeu <https://www.aoc.cat/CATCert/Regulacio>]*

Authority Info Access *http://ocsp.catcert.cat*

CRL Distribution Points *http://epsd.catcert.net/crl/ec-acc.crl*
http://epsd2.catcert.net/crl/ec-acc.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3*

X509SubjectName

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2022-06-29T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

5.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

5.8.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.8.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5.8.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by CA SectorPublic*

Name [es] *Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities**X509SubjectName**

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-03-15T01:00:00Z*

5.8.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

5.8.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

5.8.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

5.8.4.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

5.8.5 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by CA SectorPublic

Name [es] *Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities

X509SubjectName

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.8.5.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

5.8.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.8.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by CA SectorPublic*

Name *[es]* *Certificados Reconocidos emitidos por CA SectorPublic*

Service digital identities**X509SubjectName**

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-11-17T23:00:00Z*

5.8.6.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

Subject C: *ES*

Valid from: *Thu Mar 02 12:36:51 CET 2023*

Valid to: *Mon Jan 20 11:21:14 CET 2048*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:A7:60:5A:10:83:8D:D1:F5:A9:95:B4:46:DA:16:79:86:13:23:A9:62:D1:A7:B9:08:5D:4A:05:9F:38:BC:CB:E
D:8A:10:6E:6B:7A:09:87:E5:D1:CE:0A:77:1C:E0:82:C4:C3:17:5D:F0:11:8B:58:CF:A3:50:A9:82:CE:59:88:A5:2C:0C:4C:55:F2:94:24:33:C2:CF:9A:C2:50:97:C4:B4:69:30:80:37:AF:EB:26:
C7:13:5B:AE:AB:99:74:14:CB*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *49:23:96:09:1F:25:2C:BE:12:B6:E8:0F:03:F3:6B:9B:27:E5:9E:81*

Authority Info Access *http://epscd.aoc.cat/descarrega/caroot-a.crt
http://ocsp.aoc.cat*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://epscd.aoc.cat*

Extended Key Usage *id_kp_clientAuth - id_kp_smartcardlogon*

CRL Distribution Points *http://epscd.aoc.cat/crl/caroot-a.crl*

Subject Key Identifier *1D:FE:29:65:11:BF:3F:57:67:22:BB:97:D4:78:61:34:9B:76:53:E6*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2B:7B:39:0F:F6:52:AE:CA:8B:2F:35:23:25:AE:89:FB:15:3A:A9:94:40:AA:9F:E8:02:
57:B6:D7:98:87:A5:60*

X509SubjectName

Subject CN: *SubCA SECTOR PUBLIC Q (G3) A.1*

Subject 2.5.4.97: *VATES-Q0801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *Hf4pZRG/P1dnIruX1HhhNjt2U+Y=*

Service Status

Service status description *[en] undefined.
[es] undefined.*

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2024-10-16T00:00:00Z

Signature algorithm: *SHA384withECDSA*

Issuer CN: *CA CONSORCI AOC (G3) ROOT-A*

Issuer 2.5.4.97: *VATES-Q0801175A*

Issuer O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Issuer C: *ES*

Subject CN: *SubCA CIUTADANIA Q (G3) A.2*

Subject 2.5.4.97: *VATES-Q0801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Valid from: *Thu Feb 02 11:21:26 CET 2023*

Valid to: *Mon Jan 20 11:21:14 CET 2048*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:A5:E2:F0:B8:68:D6:72:FF:BE:AB:1B:11:06:E0:6B:6F:B9:72:35:08:D0:65:E8:28:32:5C:9C:EA:5D:81:E9:93:FA:6E:9E:5C:55:E5:7C:75:6F:2F:21:00:5D:74:67:45:C0:A5:A0:E1:25:3F:8C:5A:95:47:32:33:5B:47:9A:EA:45:A4:F6:83:26:B6:FE:BB:74:D4:46:36:F5:5E:66:89:EC:48:9F:F7:F5:E0:A5:AA:0C:44:5A:31:23:EE:FD:DC*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *49:23:96:09:1F:25:2C:BE:12:B6:E8:0F:03:F3:6B:9B:27:E5:9E:81*

Authority Info Access *http://epscd.aoc.cat/descarrega/caroot-a.crt*
http://ocsp.aoc.cat

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://epscd.aoc.cat

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://epscd.aoc.cat/crl/caroot-a.crl*

Subject Key Identifier *C2:FA:5A:12:28:46:17:61:A4:84:3E:7B:BA:E5:9A:70:CC:11:DD:38*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E6:DC:96:BB:0D:BC:B2:42:49:0F:DF:34:8C:B8:C9:EC:01:2E:9C:B9:59:FF:44:58:B
B:50:3E:5E:FB:1E:17:35*

X509SubjectName

Subject CN: *SubCA CIUTADANIA Q (G3) A.2*

Subject 2.5.4.97: VATES-Q0801175A

Subject O: CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA

Subject C: ES

X509SKI

X509 SK I *wvpaEihGF2GkhD57uuWacMwR3Tg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2024-10-16T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

5.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.11 - Service (granted): Qualified certificates issued by SubCA Q TSA (G3) A.5

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified certificates issued by SubCA Q TSA (G3) A.5*

Name [es] *Certificados Cualificados emitidos por SubCA Q TSA (G3) A.5*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 44496993247485484787890989451779687452

X509 Certificate

-----BEGIN CERTIFICATE-----

```
MIIDKjCCAXmgAwIBAgIQXnPlfcW+r9boC9Mj97EHDAKBggqhkiOPOQDazCBgIEMAKGAIUEBhMC
RVMMzAx8BqNVBAQmKkNPTINPlukNIEFETUIOSVNUKFD5U8gTOFUIRBIERFIENBVEFMVUSZOTey
MBYGA1UEYmVwPktFURVMUUT44MDExNzVBMSc2wgdVdVOQDDBDOSBDTOSTT1JOS5B8TOMpKEczKSBS
T09ULUEwhhcnMjMwMjAyMTAyNDE3WncNNdGwMTiWMTAyMTEOWB7MQswCOYDVOQGEWJFUEZEMDEG
A1UECgwQO9OU09SQUQgQUINUSU5J1R5OUNJTyBPOKSVSEegREUgQ00LQUxVTlBMRgwfYDVOORh
DA9WVURFUY1RMDgwMTE3NUEzHTAbBgNVBAMMFN1YkNBFegVFNBChHMygQS41hYWEAYHkoZi
zjQCAQYFK4EEACIDYgAEKtA4AahcyOoXVMWGC1J3PkL3tOeatq9g5TEK1owNBC+y8KPENyqC
ajbNf61umtSPZ7/URzg1UxV1I6TN5VCWBN5aQ98bOYPRJgXV0surZMISD50nj/jijqjInMo4IB
WDCcAYOwEgYDVR0TAQHBAgwgBgEB/wBADAfBgNVHSMEGDAWgBRj5YjYHvUsvK26A8D82ubj+We
gTBgBggrBgEFBQOCBAQRdMfswOAYIKwYBBQUHMAKGLGh0dHA6Ly9icHNjZC5hb2MuY2F0L2Ric2Nh
cnJlZ2YyZ2Fyb290LWUyY3U0MB8GCCSGAQUFBzABhNodHRwOi8vd2Nzc5b2MuY2F0MDYGA1Ud
IAQVMC0wKwYEVRRgADAJMECCEGCSGAQUFBzABhNodHRwczovL2Vwc2NkLnFvYy5jYXQwewYDVR0I
BAwwCgYIKwYBBQUHAWgwNgYDVR0RBC8wLTArCmg1YlaHR0CDovL2Vwc2NkLnFvYy5jYXQwewY3Js
L2Nhcm9vdC1hLmNyY2AdBgNVHQ4EFgQUaEFB03qTavZcwRcW5V5I4Yi09c0wDgYDVR0PAQH/BAQD
AgEgMAoGCCS3M49BAMDzCAmGOCGjRk00KypZtR5Gy6r0f0usutmoB24srKEvEtX
HvvoBxFM8JWb8mrVAiwD+yM8+b+mEcSL4d8laol/y9EGkxMDDH2P3JA+BuRUvaqVe30Nlorx
CfIlopyH
```

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: *CA CONSORCI AOC (G3) ROOT-A*

Issuer 2.5.4.97: *VATES-Q0801175A*

Issuer O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Issuer C: *ES*

Subject CN: *SubCA Q TSA (G3) A.5*

Subject 2.5.4.97: *VATES-Q0801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Valid from: *Thu Feb 02 11:24:17 CET 2023*

Valid to: *Mon Jan 20 11:21:14 CET 2048*

Public Key: 30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:28:B1:04:00:22:03:62:00:04:92:D0:38:01:A8:5C:63:4A:17:D1:53:16:18:88:F5:8F:73:E4:2F:7B:4E:79:A7:EA:8F:D8:39:B4:42:A2:D6:8C:0D:04:2F:B2:E8:A3:C4:37:2A:82:6A:36:CD:7F:AD:6E:9A:D4:8F:67:BF:D4:47:38:35:53:15:75:97:A4:CD:27:95:5C:58:13:79:69:0F:7C:6C:E6:0F:7D:4A:97:57:4B:2E:AD:93:25:B0:34:B4:9E:3F:E3:8E:5A:89:8A:39:CC

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *49:23:96:09:1F:25:2C:BE:12:B6:E8:0F:03:F3:6B:9B:27:E5:9E:81*

Authority Info Access *http://epsd.aoc.cat/descarrega/caroot-a.crt*
http://ocsp.aoc.cat

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://epsd.aoc.cat

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://epsd.aoc.cat/crl/caroot-a.crl*

Subject Key Identifier *68:47:C1:D3:7A:93:6A:F6:5C:C1:17:16:E5:5E:48:E1:88:B4:F5:CD*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *63:EB:5B:A0:DE:32:D4:AE:2D:BC:5F:2D:D1:59:DF:4E:7E:B2:4D:61:BA:53:70:78:4E:B0:72:39:86:50:C3:30*

X509SubjectName

Subject CN: *SubCA Q TSA (G3) A.5*

Subject 2.5.4.97: *VATES-Q0801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *aEfB03qTavZcwRcW5V5I4Yi09c0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2024-10-16T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

5.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5.12 - Service (granted): Qualified timestamps issued by CONSORCI AOC Q TSU 2024

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified timestamps issued by CONSORCI AOC Q TSU 2024*

Name *[es]*

Sellos de tiempo cualificados emitidos por CONSORCI AOC Q TSU 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 508956971944146919794102396865127229366413589491

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: *SubCA Q TSA (G3) A.5*

Issuer 2.5.4.97: VATES-Q0801175A

Issuer 0: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Issuer C: *ES*

Subject CN: *CONSORCI AOC Q TSU 2024*

Subject 2.5.4.97: *VATES-00801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

Valid from: *Mon Nov 04 12:46:49 CET 2024*

Valid to: Sat Nov 03 12:46:48 CET 2029

Public Key: 30:82:01:22:30:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C2:36:69:F5:C1:6C:37:6F:AA:FE:BC:FA:0A:47:5F:B9:FC:7C:3B:1F:65:48:03:34:50:58:07:A5:C7:84:FF:98:CE:FC:68:A5:E2:F4:59:31:25:7D:7C:46:28:CF:33:4F:21:F6:88:A5:28:2A:98:AE:5F:94:D9:58:05:E0:90:65:1C:3E:00:67:F5:0A:67:F3:4F:D8:07:1A:3B:38:D0:9F:12:3E:0D:37:C8:FF:98:CE:FC:68:80:1B:68:34:D1:26:A3:17:13:F3:17:50:AF:06:68:09:0A:58:1E:46:5D:C3:B1:CB:8B:91:C5:F8:2B:AF:49:6A:E1:0A:44:58:AE:4C:02:B2:78:81:56:1E:82:1A:0A:C5:FC:90:C7:88:69:48:76:F0:02:E4:A6:98:51:8D:B8:04:44:FF:BE:30:8D:0F:86:B8:01:02:44:47:93:48:2C:2B:8D:05:65:4F:A1:FE:0F:01:00:0A:CA:04:92:2B:48:7D:06:8E:D0:6E:34:77:10:CB:19:50:47:83:96:42:46:1B:F0:9D:5F:32:1D:5A:28:39:2D:44:36:52:73:45:43:53:FB:93:02:61:FA:5F:A6:28:04:1B:1A:11:8B:0A:CB:24:27:56:79:07:F2:D9:36:00:0A:6E:02:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier 68:47:C1:D3:7A:93:6A:F6:5C:C1:17:16:E5:5E:48:E1:88:B4:F5:CD

Authority Info Access <http://enscd.aoc.cat/descarrega/casub-a5.crt>

<http://ocsp.aoc.cat>

Certificate Policies*Policy OID: 1.3.6.1.4.1.15096.1.3.2.112**CPS pointer: <https://epsd.aoc.cat>**CPS text: [Certificat de Servei de Segell Qualificat de Temps]**Policy OID: 0.4.0.194112.1.1***Extended Key Usage***id_kp_timeStamping***QCStatements - crit. = false***id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15***CRL Distribution Points***<http://epsd.aoc.cat/crl/casub-a5.crl>***Subject Key Identifier***21:31:FA:C6:00:5E:55:EC:09:77:DF:C9:EC:E3:20:6B:8F:4D:C7:1F***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***65:F1:3E:10:2A:C8:B8:74:8F:0C:35:6B:23:8D:FE:63:09:B5:1E:A0:7F:57:57:4A:AA
:77:F5:9F:8F:B4:DD:AE***X509SubjectName****Subject CN:***CONSORCI AOC Q TSU 2024***Subject 2.5.4.97:***VATES-Q0801175A***Subject O:***CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA***Subject C:***ES***X509SKI****X509 SK I***ITH6xgBeVewJd9/J7OMga49Nxx8=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-08-06T00:00:00Z***5.13 - Service (granted): Qualified certificates issued by SubCA SECTOR PUBLIC R Q (G3)****A.3****Service Type Identifier***<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>***Service type description** [en]*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified certificates issued by SubCA SECTOR PUBLIC R Q (G3) A.3

Name [es] Certificados cualificados emitidos por SubCA SECTOR PUBLIC R Q (G3) A.3

Service digital identities

Certificate fields details

Version: 3

Serial Number: 18382583791552318563277984815242290027

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDDCAzgAwIBAgIQDdRbWwqmtic2jv45QjzAKBggqhkiOPOODAxCBgJELMAKGA1UEBhMC
RVVwMzAxBoNBAAQMKPTINPUBKJIEFETUIOSVNUUkFBSU8gTOIFURBIEFENBVEFNUVU2OTY
MBYGA1UEYwQwPVkFURVMTUTAA4MDExNzVBM5QwIgwYDQODDBRdOSBDTOSTT1JDS5B8TOMgKczK5B5
T09ULUEWHhcnMjMwMzAyMTEZODAZhcnNDQmDgWMTiWMTAyMTE0WjCBhZELMAKGA1UEBhMCRVVMkMzAx
BgNVBAQMKKPTINPUBKJIEFETUIOSVNUUkFBSU8gTOIFURBIEFENBVEFNUVU2OTYMBYGA1UE
YwQwPVkFURVMTUTAA4MDExNzVBM5QwIgwYDQODDBRdOSBDTOSTT1JgUUFCTEIDIFgUSAgRzMp
IEEuMzBzMBAGByqGSM49AgEGS5uBBAAIAZiABNaNuGM6Bnh063h5BHaz7h6jXWuriAIGuaq5bh9
07Lx4XZomsu39jupQj6+epihor3gQ4Rj6d4HvOYszgrOF3KQWz4H6HXq4H2CLBajUas
XJl3kUdT7DzWKQCAW8wqgFMBIGA1UdEwEB/wQIMAYBAQCAAwHwYDVROjBBgwFoAUS5SOWCR8I
LL45lugPA/NmyfIndeEwaQTIkwYBBQUHAEEXTBBMDgCcsGAQUFB2AChixodHRwOi8vZXB2L2Qw
YW9uLmNhdDA2BqNVHSAELZaIMCkGBFUDIAAwizAhBggrBgEFBQcCARYVaHR0cHM6Ly9lCHNlZCsh
b2MuY2F0MCoGA1UdQjMCEGCGCsGAQUFBwMCBggrBgEEAYI3PAICBgqhkiG9y8BAQUwNgYDVROF
BC9wLTArCmgl4YaHR0cDovL2VwczNkLmFyYy5lYXQv3jgl2NhcmlvdCJlNmNybDA4BqNVH0AE
FgOUzuN0qInqbatAS64B7/rMeInuhwwDgYDVROPAQH/BAQDAgEGMAoGCCqGSM49BAMDA2KAMGyc
MOCrym2utbQj6bDnL9Q0Tt00UeGQGS3hCldYLL5WbT2XJhhYAMKbsKkDCt5pn74LACMQDIPDck
5gBRPMQ4sTFm687Gf5slnMNQmy8X5n/Nnd3XO3ILrfvPyS8gq2URYYODGcs=

```

-----END CERTIFICATE-----

Signature algorithm: SHA384withECDSA

Issuer CN: CA CONSORCI AOC (G3) ROOT-A

Issuer 2.5.4.97: VATES-Q0801175A

Issuer O: CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA

Issuer C: ES

Subject CN: SubCA SECTOR PUBLIC R Q (G3) A.3

Subject 2.5.4.97: VATES-Q0801175A

Subject O: CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA

Subject C: ES

Valid from: Thu Mar 02 12:38:03 CET 2023

Valid to: Mon Jan 20 11:21:14 CET 2048

Public Key: 30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:28:81:04:00:22:03:62:00:04:D6:8D:B8:63:3A:06:71:E8:EB:78:79:04:76:B3:AE:1E:89:25:75:AE:50:35:1A:E6:AA:49:88:7D:D3:B2:F1:DB:85:F3:3A:6B:28:FF:7F:63:BB:FA:50:8F:AF:9E:A6:28:68:AF:78:10:8F:84:63:6F:A0:F8:B6:F0:D8:E7:38:2B:38:5D:CA:0D:6C:F8:24:7E:9F:5C:2A:78:AE:3D:82:2C:16:A3:89:46:92:5C:92:77:90:9B:83:4F:B0:F3:58

Basic Constraints: IsCA: true - Path length: 0

Authority Key Identifier: 49:23:96:09:1F:25:2C:BE:12:B6:E8:0F:03:F3:6B:9B:27:E5:9E:81

Authority Info Access *http://epscd.aoc.cat/descarrega/caroot-a.crt
http://ocsp.aoc.cat*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://epscd.aoc.cat*

Extended Key Usage *id_kp_clientAuth - id_kp_smartcardlogon*

CRL Distribution Points *http://epscd.aoc.cat/crl/caroot-a.crl*

Subject Key Identifier *CE:E3:74:A8:83:7F:A9:B6:AD:01:2E:B8:07:BF:EB:31:E2:27:BA:1C*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *78:3E:D4:7B:51:75:A9:02:88:D2:76:75:68:42:6E:8F:C5:FF:72:6F:A4:BC:0A:03:5F
:4B:BF:3A:93:86:A6:0F*

X509SubjectName

Subject CN: *SubCA SECTOR PUBLIC R Q (G3) A.3*

Subject 2.5.4.97: *VATES-Q0801175A*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

X509SKI

X509 SK I *zuN0qIN/qbatAS64B7/rMeInuhw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.
[es] undefined.*

Status Starting Time *2025-10-02T02:00:00Z*

5.13.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.13.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation**URI***[en]**<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

6 - TSP: ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

TSP Name

Name [en] ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

Name [es] ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

TSP Trade Name

Name [en] VATES-G63287510

Name [en] ANF AC

Name [es] ANF AC

Name [en] ANF Autoridad de Certificacion

PostalAddress

Street Address [en] Gran Vía de les Corts Catalanes, 996

Locality [en] Barcelona

State Or Province [en] Barcelona

Postal Code [en] 8018

Country Name [en] ES

PostalAddress

Street Address [es] Gran Vía de les Corts Catalanes, 996

Locality [es] Barcelona

State Or Province [es] Barcelona

Postal Code [es] 8018

Country Name [es] ES

ElectronicAddress

URI [en] http://www.anf.es

URI [en] mailto:info@anf.es

TSP Information URI

Issuer C: *ES*
Subject CN: *ANF Server CA*
Subject SERIAL NUMBER: *G-63287510*
Subject OU: *ANF Clase 1 CA*
Subject O: *ANF Autoridad de Certificacion*
Subject L: *Barcelona (see current address at <https://www.anf.es/address/>)*
Subject ST: *Barcelona*
Subject C: *ES*
Valid from: *Tue Apr 05 16:29:05 CEST 2005*
Valid to: *Fri Apr 03 16:29:05 CEST 2015*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BF:EA:4B:A7:9A:88:39:6B:2C:48:40:07:04:93:7C:F7:B8:2D:7E:A5:37:E2:61:D6:21:FC:90:37:C8:69:3E:5E:8B:37:DF:58:6F:3B:D8:B6:C3:88:40:90:F4:9D:0C:5C:10:52:B1:83:E5:5F:91:10:E6:FD:A8:80:14:5F:D3:8B:BD:5C:BD:0F:23:92:09:37:E3:72:D2:66:94:0B:5C:74:94:2F:5E:F2:4E:D8:03:C6:B3:CE:56:A5:1C:D9:7B:FD:4F:07:4C:D4:B7:DA:5F:29:4D:75:F2:1F:55:CF:32:23:1C:46:09:27:1D:45:EC:F1:8C:34:89:DE:7B:16:A7:43:5E:8A:2B:E9:94:43:1E:D7:3E:93:6D:6F:89:3D:BC:EE:B1:C8:B7:FF:C9:7D:E3:5F:0D:6F:77:78:F5:2A:2E:8D:C4:8B:98:97:30:B1:46:5A:0B:63:70:D4:78:C7:86:B3:7F:FF:27:42:AA:9F:8A:6E:6D:A1:94:CA:EC:87:02:1C:D6:54:4B:FD:BC:89:9B:A6:63:3B:66:8C:16:89:89:97:C3:50:E8:F6:42:01:A7:77:7D:10:19:92:03:E8:5D:45:C8:15:C5:87:1B:0D:91:F2:C6:39:9C:7B:F3:C0:0A:99:F8:EE:83:6F:7E:42:77:11:8E:C3:1F:1C:72:2F:3D:1B:02:03:01:00:01*
Subject Key Identifier *BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C*
Basic Constraints *IsCA: true*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.1.8*
CPS pointer: <https://www.anf.es/AC/documentos>
*CPS text: [Antes de aceptar este certificado, compruebe:
-Condiciones, limitaciones y usos autorizados segun CP a la que se somete.
-Estado de vigencia]*
Authority Key Identifier *BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *71:D9:41:36:C6:0F:F5:74:6E:8D:93:23:27:A9:AE:D5:BE:6A:31:F4:2C:7F:55:B0:5A:37:4F:9B:6F:4D:27:27*

X509SubjectName

Subject CN: *ANF Server CA*
Subject SERIAL NUMBER: *G-63287510*
Subject OU: *ANF Clase 1 CA*
Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <https://www.anf.es/address/>)*

Subject ST: *Barcelona*

Subject C: *ES*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

6.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18332.2.4*

6.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*
[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18332.2.4*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.18332.3.4*

6.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

6.1.4 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificate issued by ANF Server CA*

Name *[es]* *Certificado reconocido emitido por la CA ANF Server CA*

Service digital identities**X509SubjectName**

Subject CN: *ANF Server CA*

Subject SERIAL NUMBER: *G-63287510*

Subject OU: *ANF Clase 1 CA*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <https://www.anf.es/address/>)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *vjv2tDG3cyRIOcVXE5R1qp+BPYw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-05-11T00:00:00Z*

6.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) , identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.18332.2.4

6.1.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.18332.2.4

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.18332.3.4

6.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified certificate issued by ANF Server CA*

Name [es] *Certificado reconocido emitido por la CA ANF Server CA*

Service digital identities**X509SubjectName**

Subject CN: *ANF Server CA*

Subject SERIAL NUMBER: *G-63287510*

Subject OU: *ANF Clase 1 CA*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <https://www.anf.es/address/>)*

Subject ST: Barcelona

Subject C: ES

X509SKI

X509 SK I vjv2tDG3cyRIOcVXE5R1qp+BPYw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2004-11-25T00:00:00Z

6.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18332.2.4

6.1.5.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18332.2.4

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.18332.3.4

Issuer ST: *Barcelona*
Issuer C: *ES*
Subject CN: *ANF Assured ID CA1*
Subject SERIAL NUMBER: *G63287510*
Subject E: *info@anf.es*
Subject OU: *ANF Autoridad Intermedia de Identidad*
Subject O: *ANF Autoridad de Certificacion*
Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*
Subject ST: *Barcelona*
Subject C: *ES*
Valid from: *Mon Mar 03 12:17:23 CET 2014*
Valid to: *Thu Feb 29 12:17:23 CET 2024*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:7B:F4:89:6D:FC:7D:98:0C:EA:24:F9:EE:8C:AD:C4:E0:A7:EC:81:57:FA:0A:
95:4B:7E:7C:85:C7:44:49:E2:C9:DA:5A:34:14:41:E2:89:94:00:2D:68:20:52:5B:19:70:85:01:58:3E:64:47:EB:5F:3B:58:97:8D:9A:45:75:47:DC:C3:1E:57:80:51:15:99:0D:7B:5F:AC:16:A
4:72:A0:C6:C2:E5:37:BC:87:B7:FD:DE:F9:65:88:F0:8C:58:94:98:8E:10:46:D7:18:E7:FF:7B:CS:AD:95:8B:60:55:0E:B2:EE:73:E5:97:86:F0:FA:25:B6:C3:37:DD:CC:2A:38:8F:14:46:1A:08:
8B:40:5D:92:0D:7F:02:72:C1:1D:F6:FF:53:FA:E7:98:AF:1A:57:5B:70:82:84:EE:18:EE:56:D9:28:D1:47:54:00:44:DC:31:88:B9:E2:B4:CB:4E:B7:57:9F:59:47:35:B4:A0:1A:06:A2:18:7D:9
3:3D:E2:6C:FD:79:6F:23:C6:2B:A4:04:90:9A:9B:EB:E7:2E:2C:03:14:99:2B:E0:7B:4A:8C:C7:10:95:17:3B:DB:3B:03:E7:FF:E4:E0:C9:BA:E2:4A:26:ED:52:EB:A3:8E:19:C4:C2:42:04:C0:24:
81:46:2D:3C:5E:FA:D2:07:07:C4:87:D0:0D:F7:FD:5C:DD:90:F8:94:49:96:1B:D9:48:C3:2F:74:13:A0:F5:59:9A:98:3A:20:E1:28:35:F7:36:83:7D:60:E8:CB:71:81:39:B1:C2:39:28:BD:A4:2
1:74:A5:0F:F6:F6:F4:64:DB:0A:18:7A:5D:E0:2A:19:AC:1E:26:3A:E8:18:43:F3:92:93:9B:85:09:F7:46:D0:85:F2:22:C1:5E:0D:66:A7:DB:79:4C:2E:6F:BD:49:D7:AE:9B:78:93:B2:F0:76:EB:
C2:5A:72:8E:C3:FA:BA:DD:54:30:80:D0:E3:17:14:07:EB:FD:4B:AB:62:39:63:AB:44:F6:9E:9B:2A:A3:59:4B:AB:D2:07:6C:E2:9F:9A:9C:F8:4B:C9:04:41:84:7E:11:E3:74:46:EB:E4:D4:8E:A
3:E7:62:45:C4:DA:21:66:9F:46:2C:E1:8E:0A:84:09:D3:F5:5D:5A:F6:57:88:B1:A0:F7:39:1A:27:35:54:93:3C:48:B5:38:8C:BC:ED:43:DE:D5:E8:C0:95:E6:B0:BB:7F:9C:F6:9B:2D:1A:D1:1D
:87:1B:B5:6B:A2:6C:04:19:4C:3B:F6:9B:62:E6:F8:7E:B6:BB:A4:B1:34:BF:54:A4:09:E2:2C:2D:47:6F:FB:47:2A:36:B2:7C:CA:CE:86:24:A3:6F:39:62:D3:02:03:01:00:01

```

Subject Key Identifier *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Authority Key Identifier *87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17*
Basic Constraints *IsCA: true*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003 España. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]
CPS pointer: <https://www.anf.es/es/documentos>
CRL Distribution Points
https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl
https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl
ldap://ldap.anf.es:389/cn=ANF_Global_Root_CA_arl.crl,ou=ANF_Global_Root_CA,dc=anf
[DC=anf,CN=ANF_Global_Root_CA_arl.crl,OU=ANF_Global_Root_CA](#)
Authority Info Access *<http://ocsp.anf.es/spain/AV>*

Subject Alternative Name *http://www.anf.es*

info@anf.es

OU="Inscrita en el Ministerio del Interior de España con el numero nacional 171.443", SERIALNUMBER="G63287510", O=ANF Autoridad de Certificacion, L=Barcelona, STREET=Gran Via de les Corts Catalanes. 996. 08018

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FB:E0:EC:01:17:9E:8F:99:CC:58:BF:D2:53:8A:B1:1E:75:7D:18:C6:43:7A:8D:C9:65:19:10:F4:45:3C:D4:C5*

X509SubjectName

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

Subject ST: *Barcelona*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-02-05T00:00:00Z*

Scheme Service Definition URI

URI *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

6.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22

6.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.2.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.13

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.14

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.18332.2.5.1.15

Description**6.2.5 - History instance n.1 - Status: granted**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificate issued by ANF Assured ID CA1*

Name *[es]* *Certificado reconocido emitido por la CA ANF Assured ID CA1*

Service digital identities

X509SubjectName

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-10-28T01:00:00Z*

6.2.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

6.2.5.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.2.5.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.2.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.13

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.14

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.15

Description**6.2.6 - History instance n.2 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificate issued by ANF Assured ID CA1

Name	[es]	Certificado reconocido emitido por la CA ANF Assured ID CA1

Service digital identities**X509SubjectName**

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2018-03-15T01:00:00Z*

6.2.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDASURN]	<i>urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11</i>

Policy Identifier:

Identifier	[OIDASURN]	<i>urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22</i>

6.2.6.6 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

6.2.6.7 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.2.6.8 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22

Policy Identifier:

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.13

Policy Identifier:

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.14

Policy Identifier:

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.18332.2.5.1.15

Description**6.2.7 - History instance n.3 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificate issued by ANF Assured ID CA1

Name	[es]	Certificado reconocido emitido por la CA ANF Assured ID CA1

Service digital identities**X509SubjectName**

Subject CN:	ANF Assured ID CA1

Subject SERIAL NUMBER:	G63287510

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2016-06-30T22:00:00Z*

6.2.7.9 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22</i>

6.2.7.10 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

6.2.8 - History instance n.4 - Status: undersupervision

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service Name

Name [en] *Qualified certificate issued by ANF Assured ID CA1*

Name [es] *Certificado reconocido emitido por la CA ANF Assured ID CA1*

Service digital identities

X509SubjectName

Subject CN: *ANF Assured ID CA1*

Subject SERIAL NUMBER: *G63287510*

Subject E: *info@anf.es*

Subject OU: *ANF Autoridad Intermedia de Identidad*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

Subject ST: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2014-09-15T00:00:00Z*

6.2.8.11 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

Policy Identifier:

Subject OU: ANF Autoridad Intermedia PKde API
Subject C: ES
Subject CN: ANF High Assurance AP CA1
Subject SERIAL NUMBER: G63287510
Valid from: Fri May 20 17:08:29 CEST 2016
Valid to: Mon May 18 17:08:29 CEST 2026
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:84:93:2F:7E:53:18:FA:3D:F1:06:E2:CD:E7:F2:3B:02:C2:64:EE:E5:1E:B6:F8:
0D:8D:5B:85:9A:F4:0F:A3:D7:92:CD:5A:03:75:91:2F:0F:EF:50:85:80:2C:FE:7E:45:65:71:1C:16:AD:E6:F8:42:7A:19:99:C7:0E:0B:4A:89:5C:03:1A:0A:BE:DC:E6:62:82:94:3E:DD:4A:CE:A
B:81:FD:43:25:45:33:9C:04:65:4A:26:7E:9B:A1:2A:45:24:84:4E:D4:63:C8:45:FE:BD:80:8E:0C:DF:3E:F9:C7:E3:FF:6B:8A:F7:0A:90:EF:C1:7D:E9:E2:66:59:B2:85:AB:E9:A5:4F:A5:C2:AC:
E0:01:BB:4E:7D:9D:58:FB:A8:2D:0F:BD:64:DF:D4:43:68:98:D7:D4:01:BD:F1:55:E0:9B:C1:05:6A:8E:73:D2:F6:B3:42:37:9A:F5:86:43:A0:C4:F2:62:8E:9C:86:8D:14:44:E3:B6:F5:DE:0C:F
5:29:03:03:80:54:F9:5C:1A:1E:D6:AF:D0:2B:63:73:5E:8C:C9:88:66:A8:90:E0:CA:33:1F:4E:50:85:03:6E:A6:47:57:27:78:1F:31:83:8D:28:C9:33:30:00:87:10:9A:62:C5:48:E7:16:B4:2A:E
A:5B:37:42:CB:F4:13:CC:5F:C9:1A:E0:85:D1:EF:6A:6B:18:24:DE:21:95:A4:8D:10:C7:D0:D9:7C:5D:B3:93:F1:23:03:3D:4F:AD:5E:13:20:0A:C9:6C:5A:E9:5B:66:87:19:B3:84:39:97:97:3B
:1A:D9:21:C8:F8:F1:43:40:EC:D1:D1:8B:AF:AB:A5:DA:AF:C1:49:43:6C:2B:95:E9:1B:1C:7E:6D:BB:00:26:C3:AA:8C:AE:D6:58:3A:7B:6C:55:F2:5F:0F:20:F5:72:FA:74:39:77:22:77:E5:05:3
F:D7:72:D8:75:3E:36:67:BA:E5:49:FB:8C:E4:4D:8B:C1:42:6E:79:CD:07:A0:4D:02:3F:AB:77:ED:D4:C7:ED:01:01:69:58:39:30:A8:13:D9:8E:4A:68:4B:3E:4F:43:3B:20:5D:0B:F8:8E:77:D
B:8F:79:5A:36:56:59:0A:0C:B2:77:C9:35:A0:AD:D2:89:13:65:64:2B:E5:7D:29:51:D7:32:0C:25:C2:DA:15:CF:6D:6C:10:51:ED:82:CF:6E:F2:85:CE:A1:8C:FF:F8:FA:6D:AB:96:6C:03:9D:4E
:80:9D:9C:44:93:73:84:90:AD:04:71:B2:AB:C0:83:9C:1E:04:0C:1A:BA:22:D2:DC:C8:9E:0B:F3:FA:6F:EC:A1:83:5C:19:A6:CC:89:98:95:A1:D5:1B:8E:71:02:03:01:00:01

```

Subject Key Identifier 92:47:FD:D2:C3:61:2B:A9:C7:09:A7:3D:3E:35:27:51:31:08:6C:35
Authority Key Identifier 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17
Basic Constraints *IsCA: true*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]
CPS pointer: <http://www.anf.es/es/documentos>
CRL Distribution Points *https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl*
https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl
Authority Info Access *<http://ocsp.anf.es/spain/AV>*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 4D:C5:4F:4C:5B:DA:C1:95:57:06:6E:32:F6:2F:8C:48:6B:15:5B:00:F5:3D:10:2D:E7:8C:98:EE:61:A2:C3:17

X509SubjectName

Subject O: ANF Autoridad de Certificacion
Subject OU: ANF Autoridad Intermedia PKde API
Subject C: ES
Subject CN: ANF High Assurance AP CA1

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *kkf90sNhK6nHCac9PjUnUTEIbDU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2022-01-11T02:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by ANF High Assurance AP CA1*

Name *[es]* *Certificados cualificados emitidos por ANF High Assurance AP CA1*

Service digital identities

X509SubjectName

Subject O: *ANF Autoridad de Certificacion*

Subject OU: ANF Autoridad Intermedia PKde API

Subject C: ES

Subject CN: ANF High Assurance AP CA1

Subject SERIAL NUMBER: G63287510

X509SKI

X509 SKI kkf90sNhK6nHCac9PjUnUTEIbDU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-03-15T01:00:00Z

6.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.3.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

6.4 - Service (granted): Qualified certificates issued by ANF High Assurance EV CA1

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified certificates issued by ANF High Assurance EV CA1

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:45:34:9F:DE:D0:07:5E:6F:80:DA:46:B4:FA:F8:69:79:D9:33:E8:8C:E5:F2:CD:23:F7:4F:53:C2:10:8F:7A:09:34:5B:FE:50:31:C1:FA:08:A4:81:1F:81:08:DD:5D:C8:BA:FF:5E:F0:F3:3C:3A:9A:44:64:D9:7F:80:78:9E:83:1A:CC:F3:C8:B6:61:87:39:60:1D:30:04:DF:94:EF:B2:27:2F:D4:0B:F1:BE:74:68:86:69:5A:20:D8:A7:16:E8:E7:72:90:74:3E:38:25:B2:F8:29:4E:AA:84:E7:F5:D1:A5:56:9E:20:76:3D:2F:3A:7C:D5:76:4F:3A:21:D9:45:14:FC:57:DC:43:EE:EA:E7:67:48:56:7E:B6:17:2B:4C:7B:21:C5:C0:13:25:40:1D:01:92:1F:F8:CD:2C:B2:61:B2:7C:41:B7:85:E1:36:60:07:00:19:AC:74:28:45:6D:CS:77:1D:3F:53:9B:5E:01:61:2E:86:71:8D:07:2E:61:95:6B:8E:5D:39:91:EA:9F:15:AB:CA:9C:60:E2:7F:9C:A6:D3:7E:9B:CF:3D:83:EF:E3:3D:AB:89:88:71:8E:7D:06:A4:DC:60:E7:BF:3A:09:F9:D9:20:15:F4:27:24:89:68:10:53:66:86:E0:94:2D:F6:D6:51:A9:10:21:7D:CE:DA:44:07:56:EB:F3:5F:A9:64:B5:15:BA:8B:AE:F4:3E:08:3D:F0:FF:B9:CB:5C:A7:95:64:1B:74:4B:07:33:0A:FF:74:CF:B2:FB:0B:52:9B:60:49:52:BE:E7:24:54:30:4E:CC:6C:C3:A0:49:7E:C0:E6:13:8D:AF:3F:08:5B:AD:1C:D1:33:C8:2C:3B:CF:D2:62:81:C1:A6:45:04:61:84:42:A1:B2:64:C5:93:E8:58:D7:A6:FD:B8:76:FA:02:84:DB:6E:B8:80:3A:F8:88:47:71:4F:F1:58:80:EC:C9:8D:A6:5D:72:1E:26:04:06:2D:A4:64:EB:4A:9C:2E:FF:22:0E:44:8B:BA:3F:C1:04:95:E3:EC:B6:CE:64:D2:22:43:79:FF:C3:96:E2:42:AC:1D:F2:80:C0:32:DE:3E:24:91:D2:93:14:11:9B:58:59:9C:35:EC:0D:0D:8D:80:0F:EC:FB:4A:59:9B:C9:04:BA:97:2F:8F:46:8B:73:9F:A4:37:66:88:29:FA:6E:E3:0F:12:E1:FB:AE:D0:A1:48:10:8B:4D:EC:9F:85:F9:05:B5:8D:11:65:D8:CB:15:E7:D5:7F:FB:73:17:7F:42:90:55:85:3F:C3:58:D9:CF:2F:FB:81:3F:87:8D:2F:9C:8A:0D:6E:D3:3F:B5:61:BF:45:02:03:01:00:01

Subject Key Identifier

86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78

Authority Key Identifier

87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

Basic Constraints

IsCA: true

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]

CPS pointer: <http://www.anf.es/es/documentos>**CRL Distribution Points**http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crlhttp://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl**Authority Info Access**<http://ocsp.anf.es/spain/AV>http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer**Key Usage:**

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04

X509SubjectName**Subject O:**

ANF Autoridad de Certificacion

Subject OU:

ANF Autoridad Intermedia Tecnicos

Subject C:

ES

Subject CN:

ANF High Assurance EV CA1

Subject SERIAL NUMBER:

G63287510

X509SKI**X509 SK I**

hr7ji+ 7o/UsorZErpcBe4gslzng=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Service status description** [en]

undefined.

[es]

undefined.

Status Starting Time

2018-03-15T01:00:00Z

Issuer O: ANF Autoridad de Certificacion

Issuer OU: ANF Clase 1 CA

Issuer C: ES

Issuer CN: ANF Global Root CA

Issuer SERIAL NUMBER: G63287510

Subject O: ANF Autoridad de Certificacion

Subject OU: ANF Autoridad Intermedia Tecnicos

Subject C: ES

Subject CN: ANF High Assurance EV CA1

Subject SERIAL NUMBER: G63287510

Valid from: Fri May 20 16:48:24 CEST 2016

Valid to: Mon May 18 16:48:24 CEST 2026

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:45:34:9F:DE:D0:07:5E:6F:80:DA:46:84:FA:F8:69:79:D9:33:E8:8C:E5:F2:CD:23:FE:4F:53:C2:10:8F:7A:09:34:5B:FE:50:31:C1:FA:08:A4:81:1F:01:08:DD:5D:CB:BA:FF:5E:F0:F3:3C:3A:9A:4A:64:D9:7F:80:78:9E:83:1A:CC:F3:C8:B8:61:87:39:60:1D:30:04:DF:94:EF:B2:2F:D4:0B:F1:BE:74:68:86:69:5A:20:D8:A7:16:E8:E7:72:90:74:3E:38:25:B2:F8:29:4E:AA:84:E7:F5:D1:A5:56:9E:20:76:3D:2F:3A:7C:D5:76:4F:3A:21:D9:45:14:FC:57:DC:43:E:EA:E7:67:48:56:7E:B6:17:2B:4C:7B:21:C5:C0:13:25:40:1D:01:92:1F:F8:CD:2C:B2:61:B2:7C:41:B7:85:E1:36:60:07:00:19:AC:74:28:45:6D:C5:77:1D:3F:53:98:5E:01:61:2E:86:71:8D:07:2E:61:95:68:BE:5D:39:91:FA:9F:15:AB:CA:9C:60:E2:7F:9C:A6:D3:7E:98:CF:3D:83:EF:E3:3D:AB:89:88:71:8E:7D:06:A4:DC:60:E7:8F:3A:09:F9:D9:20:15:F4:27:24:89:68:10:53:66:86:E0:94:2D:F6:D6:51:A9:10:21:7D:CE:DA:44:07:56:EB:F3:5F:A9:64:B5:15:BA:88:AE:F4:3E:08:3D:F0:FF:B9:CB:5C:A7:95:64:1B:7A:48:07:33:0A:FF:74:CF:B2:FB:0B:52:98:60:49:52:BE:7:24:54:30:4E:CC:8C:3A:D0:49:7E:C0:E6:13:8D:AF:3F:08:58:AD:1C:D1:33:CB:2C:38:CF:D2:62:81:C1:A6:45:04:61:B4:42:A1:B2:64:C5:93:E8:58:D7:A6:FD:B8:76:FA:02:B4:DB:6E:B8:80:3A:F8:88:47:71:4F:F1:58:80:EC:C9:8D:A6:5D:72:1E:26:04:06:2D:A4:64:EB:4A:9C:2E:FF:22:0E:44:8B:8A:3F:C1:04:95:E3:EC:8B:CE:64:D2:22:43:79:FF:C3:96:E2:42:AC:1D:F2:60:C0:32:DE:3E:24:91:D2:93:14:11:9B:58:59:9C:35:EC:0D:0D:8D:80:0F:EC:F8:4A:59:9B:C9:D4:BA:97:2F:8F:46:88:73:9F:A4:37:66:88:29:FA:6E:E3:0F:12:E1:FB:AE:D0:A1:48:10:B8:4D:EC:9F:85:F9:05:B5:8D:11:65:D8:CB:15:E7:D5:7F:FB:73:17:7F:42:90:55:85:3F:C3:58:D9:CF:2F:FB:81:3F:F8:07:8D:2F:9C:8A:0D:6E:D3:3F:B5:61:BF:45:02:03:01:00:01

Subject Key Identifier 86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78

Authority Key Identifier 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]
CPS pointer: <http://www.anf.es/es/documentos>

CRL Distribution Points *http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl*
http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl

Authority Info Access *<http://ocsp.anf.es/spain/AV>*
http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04*

X509SubjectName

Subject O: *ANF Autoridad de Certificacion*

Subject OU: *ANF Autoridad Intermedia Tecnicos*

Subject C: *ES*

Subject CN: *ANF High Assurance EV CA1*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *hr7ji+7o/UsoRzErcpBe4gslzng=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2022-01-11T02:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF.aspx*

6.5.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by ANF High Assurance EV CA1*

Name *[es]* *Sellos de tiempo cualificados emitidos por ANF High Assurance EV CA1*

Service digital identities

X509SubjectName

Subject O: *ANF Autoridad de Certificacion*

Subject OU: *ANF Autoridad Intermedia Tecnicos*

Subject C: ES

Subject CN: ANF High Assurance EV CA1

Subject SERIAL NUMBER: G63287510

X509SKI

X509 SK I hr7ji+7o/UsoRzErcpBe4gslzng=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-03-15T01:00:00Z

6.6 - Service (withdrawn): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service type description [en] undefined.
[es] undefined.

Service Name

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION

Name [es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION

Service digital identities

Certificate fields details

Version: 3

Serial Number: 996613180148035949

Subject SURNAME: DIAZ VILCHES - 37271387W

Subject O: ANF AUTORIDAD DE CERTIFICACION ASOCIACION ANF AC

Subject T: PRESIDENTE

Subject 2.5.4.13: Cargo: PRESIDENTE .INSCRIPCIÓN: REG. ASOCIACIONES DEL MINISTERIO DEL INTERIOR. GRUPO 1º, SEC. 1ª, NUM. 171443. FECHA: 12.01.2004.

Subject OU: Certificado de Sello Electronico

Subject SERIAL NUMBER: TINESG63287510

Valid from: Mon Dec 24 11:03:11 CET 2018

Valid to: Wed Dec 23 11:03:11 CET 2020

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:A0:80:15:9E:4B:AC:20:27:FD:AD:F7:2C:3F:D8:A9:07:D9:B3:4B:C2:30:A6:3D:FE:4B:F2:33:51:B1:EC:8A:FE:D3:C3:08:CA:81:19:6D:01:1E:F6:5D:35:25:96:3A:50:07:FC:96:1F:7C:50:B5:A9:C9:48:4E:79:AD:0C:D6:F9:C2:46:83:73:0E:6C:98:08:9B:85:5A:55:E9:C A:F4:6E:AD:22:8D:67:2D:9B:59:6D:E7:DB:65:4A:C8:8B:A3:E3:38:13:EE:CL:A5:BD:77:A4:54:76:61:8B:35:A8:13:83:69:BF:13:6D:9C:82:EC:50:E9:93:ES:C8:5D:23:79:7E:15:F5:AC:00:AE AD:95:53:8B:D3:5F:A8:A7:C8:51:91:9A:DC:7A:4B:F1:3F:F5:A6:AF:15:87:C6:F2:99:AE:C1:9B:EB:9B:60:B3:01:5E:26:9B:20:D6:EC:12:63:C7:56:6D:E4:18:4C:94:71:26:F5:B4:AC:F4:D6:A E:46:BB:FD:ES:AC:A1:A9:4E:0E:1E:24:7C:88:7B:48:E6:45:C4:EA:C6:61:B6:9A:21:D2:71:19:E0:A4:2C:3C:A1:CF:17:72:EF:00:EA:1F:67:C0:71:3F:E9:E6:ED:0F:68:8B:65:7A:E7:D6:F4:5F: CC:09:BA:86:69:2F:E5:10:DB:4D:65:02:03:01:00:01

Basic Constraints IsCA: false

Authority Info Access
<http://ocsp.anf.es/spain/AV>
http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer

CRL Distribution Points https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl

Subject Directory Attributes
2.5.4.15 Private Organization
1.3.6.1.4.1.311.60.2.1.1 Madrid
1.3.6.1.4.1.311.60.2.1.2 Madrid
1.3.6.1.4.1.18332.600 ARMD v.3.5.1.70
1.3.6.1.4.1.18332.30.1 España
1.3.6.1.4.1.18332.10.10.1
https://tomcat2.anf.es/cliente_archivo_ws/poderes/119814498-89288764
2.5.4.9 PASEO DE LA CASTELLANA, 79
1.3.6.1.4.1.18332.40.1 CERTIFICADO CUALIFICADO
1.3.6.1.4.1.18332.41.1 1000
2.5.4.17 28046
1.3.6.1.4.1.18332.91.1 Asociación
2.5.4.42 FLORENCIO
2.5.4.4 DÍAZ VILCHES - 37271387W
1.3.6.1.4.1.18332.42.1 000-0000
2.5.4.9 PASEO DE LA CASTELLANA, 79

QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_RetentionPeriod: 15</i> <i>id_etsi_qcs_LimiteValue</i> <i>Value: 1000</i> <i>Currency: EUR</i>
Subject Alternative Name	<i>serviciotecnico@anf.es</i>
Subject Key Identifier	30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30: 82:01:0A:02:82:01:01:00:A8:A0:80:15:9E:4B:AC:20:27:FD:AD:F7:2C:3F:D8:A9:0 7:D9:B3:4B:C2:30:A6:3D:FE:4B:F2:33:51:B1:EC:8A:FE:D3:C3:08:CA:81:19:6D:01 :1E:F6:5D:35:25:96:3A:50:07:FC:96:1F:7C:50:B5:A9:C9:48:4E:79:AD:0C:D6:F9:C 2:46:83:73:0E:6C:98:08:9B:85:5A:55:E9:CA:F4:6E:AD:22:8D:67:2D:9B:59:6D:E7: DB:65:4A:C8:8B:A3:E3:38:13:EE:C1:A5:BD:77:A4:54:76:61:8B:35:A8:13:83:69:B F:13:6D:9C:82:EC:50:E9:93:E5:C8:5D:23:79:7E:15:F5:AC:00:AE:A0:95:53:B8:D3: 5F:A8:A7:C8:51:91:9A:DC:7A:48:F1:3F:F5:A6:AF:15:B7:C6:F2:99:AE:C1:9B:EB:9B :60:B3:91:5E:26:9B:20:D6:EC:12:63:C7:56:60:E4:18:4C:94:71:26:F5:B4:AC:F4:D 6:AE:46:BB:FD:E5:AC:A1:A9:4E:0E:1E:24:7C:88:7B:48:E6:45:C4:EA:C6:61:B6:9A: 21:D2:71:19:E0:A4:2C:3C:A1:CF:17:72:EF:00:EA:1F:67:C0:71:3F:E9:E6:ED:0F:6B :8B:65:7A:E7:D6:F4:5F:CC:09:BA:B6:69:2F:E5:10:DB:4D:65:02:03:01:00:01
Extended Key Usage	<i>id_kp_codeSigning - id_kp_clientAuth - id_kp_serverAuth</i>
Authority Key Identifier	<i>35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.18332.25.1.1.1</i> <i>CPS pointer: http://www.anf.es/documentos</i> <i>CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]</i> <i>Policy OID: 0.4.0.194112.1.1</i>
Key Usage:	<i>digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>B1:14:56:6D:66:73:7E:AC:6F:1C:A1:AA:16:C0:0F:51:89:69:A2:C4:4C:A6:D8:6D:8 F:4F:97:EE:A2:41:C8:E9</i>
X509SubjectName	
X509SKI	
X509 SK I	MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgKCAFZ5LrCAn/a33LD/Yq QfZs0vCMKY9/kvyM1Gx7lr+08MlyoEZbQEe9l01JZY6Uaf8lh98ULWpyUhOea0M1v nCR0NzDmyYCJuFWIXpyvRurSKNZy2bWW3n22VKyluj4zgT7sGlvXekVHZhizWoE4 NpvxNtnlLsUOmT5chdl3l+FfWsAK6glVO401+op8hRkZrcekjxP/WmrXW3xvKZrsG b65tgs5FeJpsg1uwSY8dWYOQYTJRxjvW0rPTWrka7/eWsoalODh4kflh7SOZFxorGY baaldJxGeCkLDyhzyxdy7wDqH2fAct/p5u0Pa4tleufW9F/MCbq2aS/IENtNZQIDAQAB
Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description	[en] undefined. [es] undefined.
Status Starting Time	<i>2021-01-26T01:00:00Z</i>

6.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.6.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.6.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Service Name

Name	[en]	Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION

Name	[es]	Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION

Service digital identities**X509SubjectName****X509SKI**

X509 SK I	MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgKCAFZ5LrCAn/a33LD/YqQfZs0vCMKY9/kvyM1Gx7Ir+08MlyoEZbQEe9l01JZY6Uaf8lh98ULWpyUhOea0M1vnCRoNzDmyYCJuFWIXpyvRurSKNZy2bWW3n22VKyluj4zgT7sGlvXekVHZhizWoE4NpvxNtnlLsUOmT5chdl3l+FfWsAK6glVO401+op8hRkZrcekjxP/WmrXW3xvKZrsGb65tgs5FeJpsg1uwSY8dWYOQYTJRxjvW0rPTWrka7/eWsoalODh4kflh7SOZFxorGYbaaldJxGeCkLDyhzxdy7wDqH2fAct/p5u0Pa4tleufW9F/MCbq2aS/IEntNZQIDAQAB

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2019-02-18T01:00:00Z

6.6.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.6.3.2 - Extension (critical): additionalServiceInformation

Subject CN: ANF High Assurance Server CA
Subject OU: ANF Autoridad intermedia tecnicos
Subject O: ANF Autoridad de Certificacion
Subject C: ES
Subject SERIAL NUMBER: G63287510
Valid from: Thu Sep 05 18:35:44 CEST 2019
Valid to: Sun Sep 02 18:35:44 CEST 2029
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DD:A8:CB:E2:42:F5:FD:04:9F:26:7A:93:C5:2E:94:00:88:38:A6:35:96:FD:D3:
B5:CA:77:F6:C3:6E:D1:00:54:3F:C8:4E:39:60:01:66:F6:B4:35:33:8F:4F:CA:99:5A:95:FE:AE:40:D6:96:CB:9B:74:C5:12:DA:A0:00:80:CB:BF:BC:D3:0E:92:20:F4:CF:F2:1C:E6:3A:83:24:13:
B2:8E:71:BC:12:9C:33:21:4D:05:CF:8B:F1:00:C8:45:DE:ED:89:99:41:F0:35:0F:19:28:6D:92:72:63:B2:9F:63:ED:A7:31:88:CC:E9:D8:1B:5B:18:8F:A4:95:76:1D:06:D5:D9:44:6A:AA:13:
C4:FC:F9:F8:4C:71:DD:90:89:1A:F2:D3:19:52:68:4E:8D:08:15:75:C7:30:D2:86:61:42:23:51:F3:6C:3D:0B:5F:5F:D4:6A:88:A5:E5:43:62:F6:92:85:92:8E:0F:80:CA:0D:00:57:DA:69:42:2F:
29:94:78:8D:38:A1:69:55:33:85:5F:18:75:68:03:1A:30:F4:25:80:10:09:E0:02:89:23:6A:D9:0E:94:FB:D5:88:C1:36:C3:E0:47:B1:55:98:C7:40:15:0A:FD:3C:57:95:EE:7A:71:40:1F:11:6
A:FC:99:2E:9C:4A:95:9E:F0:0D:4B:3D:B1:E7:AA:19:BC:8A:C2:24:F5:C3:78:13:E1:DD:C8:B2:17:DE:33:CB:BA:28:5D:25:6C:4B:0F:3B:1E:4F:D4:E3:C6:CC:8C:9E:6C:B1:43:85:7E:07:20:2
1:FC:10:2E:B3:78:09:3C:94:8C:EF:2F:4B:67:67:EB:11:42:4E:06:ED:EC:20:6F:A0:D9:C2:35:96:84:0A:63:AC:F6:E6:30:F5:ED:28:AD:47:E8:9F:5B:7F:67:99:84:97:06:F7:D5:8E:8A:E8:2D:8
C:0E:65:A2:18:03:69:70:67:91:59:D9:67:14:A6:F5:D1:B9:C6:AD:94:89:47:AA:5C:86:BD:5F:AB:CA:59:89:8B:3A:9B:5C:EC:06:AE:70:3C:80:DE:3F:18:ED:1C:33:3F:0F:A5:EB:E4:4B:47:29
23:D9:AB:20:CD:EF:68:A2:3D:E8:65:94:10:3E:F3:36:F6:B4:8E:73:76:5E:20:2F:C1:AE:0D:BF:CC:B1:27:49:60:7F:3E:E0:AB:58:0A:C8:6A:F7:7B:99:4B:D4:37:00:63:7B:B3:88:9D:19:C6:6
4:3F:88:DA:61:B4:37:C9:69:E2:E1:38:85:2B:81:E4:A2:3F:46:70:8D:0D:CD:BE:5E:A0:9A:16:39:DC:98:20:A3:8D:72:8B:3F:9F:51:29:5F:6A:15:47:CD:02:03:01:00:01

```

Authority Key Identifier 9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37
Subject Key Identifier 94:BA:FA:EE:22:FA:32:1C:CB:05:77:B7:19:AF:12:F0:9A:6C:47:AB
Extended Key Usage id_kp_clientAuth - id_kp_serverAuth
CRL Distribution Points <http://crl.anf.es/crl/ANFSecureServerRootCA-ar1.crl>
<http://www.anf.es/crl/ANFSecureServerRootCA-ar1.crl>
Certificate Policies Policy OID: 2.5.29.32.0
CPS pointer: <http://www.anf.es/es/documentos>
Authority Info Access <http://ocsp.anf.es/spain/AV>
<http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer>
Basic Constraints IsCA: true
Key Usage: digitalSignature - keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:B
A:05:3B:06:96:95:C1:74
X509SubjectName
Subject CN: ANF High Assurance Server CA
Subject OU: ANF Autoridad intermedia tecnicos
Subject O: ANF Autoridad de Certificacion

Subject C: *ES*

Subject SERIAL NUMBER: *G63287510*

X509SKI

X509 SK I *ILr67iL6MhzLBXe3Ga8S8JpsR6s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-03-17T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

6.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

6.7.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by ANF High Assurance Server CA*

Name *[es]* *Certificados cualificados emitidos por ANF High Assurance Server CA*

Service digital identities

X509SubjectName

Subject CN: *ANF High Assurance Server CA*

Subject OU: *ANF Autoridad intermedia tecnicos*

Subject O: *ANF Autoridad de Certificacion*

Subject C: ES

Subject SERIAL NUMBER: G63287510

X509SKI

X509 SKI ILr67iL6MhzLBXe3Ga8S8JpsR6s=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-11-25T01:00:00Z

6.7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

6.8 - Service (withdrawn): Qualified timestamps issued by ANF High Assurance Server CA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by ANF High Assurance Server CA

Name	[es]	Sellos de tiempo cualificados emitidos por ANF High Assurance Server CA

Service digital identities

Certificate fields details

Version: 3

Serial Number: 99659964253702882

Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.anf.es/es/documentos</i>
Authority Info Access	<i>http://ocsp.anf.es/spain/AV</i> <i>http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer</i>
Basic Constraints	<i>IsCA: true</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:B A:05:3B:06:96:95:C1:74</i>

X509SubjectName

Subject CN:	<i>ANF High Assurance Server CA</i>
Subject OU:	<i>ANF Autoridad intermedia tecnicos</i>
Subject O:	<i>ANF Autoridad de Certificacion</i>
Subject C:	<i>ES</i>
Subject SERIAL NUMBER:	<i>G63287510</i>

X509SKI

X509 SK I	<i>lLr67iL6MhzLBXe3Ga8S8JpsR6s=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2022-01-11T02:00:00Z</i>

Scheme Service Definition URI

URI	<i>[en]</i>	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI	<i>[es]</i>	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

6.8.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name	<i>[en]</i>	<i>Qualified timestamps issued by ANF High Assurance Server CA</i>
Name	<i>[es]</i>	<i>Sellos de tiempo cualificados emitidos por ANF High Assurance Server CA</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>ANF High Assurance Server CA</i>
Subject OU:	<i>ANF Autoridad intermedia tecnicos</i>
Subject O:	<i>ANF Autoridad de Certificacion</i>
Subject C:	<i>ES</i>
Subject SERIAL NUMBER:	<i>G63287510</i>

X509SKI

X509 SK I	<i>lLr67iL6MhzLBXe3Ga8S8JpsR6s=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time	<i>2019-11-25T01:00:00Z</i>

6.9 - Service (withdrawn): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q</i>

Service type description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

Service Name

Name	<i>[en]</i>	<i>Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación</i>
Name	<i>[es]</i>	<i>Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados por ANF AC Servicio de validación</i>

Service digital identities**Certificate fields details**

Version:	<i>3</i>

Valid to: *Sat Dec 03 17:00:57 CET 2022*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:8E:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8D:08:D9:4E:A0:BB:8C:10:0C:09:11:9B:5F:D8:1F:A3:E3:64:6A:4A:03:64:CE:7F:76:81:DE:7D:94:CD:F9:11:E3:46:E9:33:2C:10:C5:B7:CF:3B:89:E1:1D:C8:11:6C:C8:F7:49:17:5D:5C:B6:06:CF:6D:23:0C:A6:C3:C7:6D:52:AF:CE:EE:6D:5D:AA:0D:24:86:72:AA:33:38:FF:C8:66:6F:D4:A0:90:45:D2:48:F6:E0:AB:44:3E:19:AD:47:A3:DD:22:14:2F:D4:9D:1F:05:6D:79:8E:23:79:F8:80:05:0F:E3:42:74:11:31:4B:16:22:80:FB:82:68:2F:AB:82:68:12:4E:CA:65:F6:80:72:C5:B4:8F:07:DE:8D:31:3B:BE:D7:06:44:8B:4F:74:CC:99:8C:8A:9E:E6:3B:5E:A9:C4:61:0D:45:4C:C7:C3:07:A6:92:E8:5F:75:C1:23:CF:95:5B:0B:4C:B0:7F:2C:B4:4A:54:3F:B7:AD:F1:0B:9D:E8:8C:C8:42:AA:FC:F9:FB:A0:86:88:81:74:EA:8A:42:6E:36:74:12:DC:53:3E:02:01:06:E3:55:6E:E0:55:EC:51:FB:04:E7:3D:3C:13:CD:F1:63:A7:4C:E7:14:2B:99:84:5C:21:CA:FF:CE:93:ED:19:E0:B6:20:D2:AF:02:03:01:00:01*

Authority Key Identifier *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*

Subject Key Identifier *77:F8:48:FC:FA:22:DC:51:FD:89:73:E4:90:49:B5:B3:00:7F:26:0B*

Subject Alternative Name *soporte@anf.es*

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*

Certificate Policies
Policy OID: 1.3.6.1.4.1.18332.25.1.1.1
CPS pointer: https://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.1

Authority Info Access
http://ocsp.anf.es/spain/AV
http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8D:25:C0:1A:24:CB:58:33:E4:97:46:90:D1:11:36:0A:B1:2A:F0:72:21:FD:8C:0C:7D:41:22:D9:12:54:65:C7*

X509SubjectName

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *ANF AC Servicio de validación*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: ES

X509SKI

X509 SK I d/hl/Poi3FH9iXPkkEm1swB/Jgs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2023-02-15T00:00:00Z

6.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.9.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service Name

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación

Name [es] Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados por ANF AC Servicio de validación

Service digital identities

X509SubjectName

Subject 2.5.4.97: VATES-G63287510

Subject CN: ANF AC Servicio de validación

Subject E: soporte@anf.es

Subject OU: Certificado Cualificado de Sello Electronico

Subject O: ANF Autoridad de Certificacion

Subject L: Barcelona

Subject ST: Cataluña

Subject C: ES

X509SKI

X509 SK I d/hl/Poi3FH9iXPkkEm1swB/Jgs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-01-26T01:00:00Z

6.9.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.10 - Service (withdrawn): Qualified electronic registered delivery service ANF AC

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description [en] An electronic delivery service providing qualified electronic deliveries.
[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name [en] Qualified electronic registered delivery service ANF AC

Name [es] Servicio cualificado de entrega electrónica certificada de ANF AC

Service digital identities

Certificate fields details

Version: 3

Valid to: *Fri Dec 02 13:52:56 CET 2022*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:CC:A7:68:64:58:F8:9C:8B:09:3E:96:1C:DC:40:31:39:17:16:D7:37:FA:38:4F:A7:78:8D:BD:44:28:48:F8:26:81:33:C9:05:90:8F:12:1D:92:8F:86:A6:38:F8:91:A2:F6:FE:59:74:FE:81:B6:0E:DA:32:55:A1:46:B3:DA:D8:CA:B6:46:B9:8E:92:A3:4C:62:B8:9D:69:48:B3:4D:84:D1:E6:4E:37:9A:1B:E5:58:B2:30:BE:8A:E4:4E:FF:D5:5E:16:3A:45:82:85:26:0F:72:42:10:F9:9C:88:CA:04:98:5D:B7:00:A2:0E:76:32:D7:AA:4C:8D:4E:22:5F:27:1C:1C:55:36:50:CE:A0:22:27:D2:6E:53:92:91:2C:05:FF:D0:F7:B9:84:A4:AA:77:23:6C:93:E4:E5:8C:7A:AA:B7:95:2C:01:F4:BD:80:81:66:B1:59:78:22:CA:FC:95:66:45:42:94:53:5D:5A:55:F6:1A:FB:EC:2E:A4:52:38:45:83:0A:B8:89:3E:92:83:4E:28:0D:7D:F5:A8:73:02:1D:3E:01:1D:D2:1F:60:C9:ED:2B:C9:6C:EF:02:95:C0:91:62:04:51:8E:6A:D1:85:8D:17:F3:82:B6:A7:13:5E:02:9F:6B:FC:FA:A0:79:2F:BB:66:CE:58:25:19:6F:02:03:01:00:01*

Authority Key Identifier *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*

Subject Key Identifier *79:B2:EE:74:1D:EA:FD:EC:AD:AB:BB:AD:23:F2:A6:CD:D4:4B:5D:F2*

Subject Alternative Name *soporte@anf.es*

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*

Certificate Policies
Policy OID: 1.3.6.1.4.1.18332.25.1.1.1
CPS pointer: https://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.1

Authority Info Access
http://ocsp.anf.es/spain/AV
http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer

Basic Constraints *isCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *20:94:FB:22:EC:CD:E5:50:9C:B8:87:D5:B8:34:2D:84:0C:75:D0:5E:46:1D:B7:82:00:14:0D:18:22:B8:3C:94*

X509SubjectName

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *Sign to Sign Delivery Services*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: ES

X509SKI

X509 SK I ebLudB3q/eytq7utl/KmzdRLXfl=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2023-02-15T00:00:00Z

6.10.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [en] Qualified electronic registered delivery service ANF AC

Name [es] Servicio cualificado de entrega electrónica certificada de ANF AC

Service digital identities

X509SubjectName

Subject 2.5.4.97: VATES-G63287510

Subject CN: Sign to Sign Delivery Services

Subject E: soporte@anf.es

Subject OU: Certificado Cualificado de Sello Electronico

Subject O: ANF Autoridad de Certificacion

Subject L: Barcelona

Subject ST: Cataluña

Subject C: ES

X509SKI

X509 SK I ebLudB3q/eytq7utl/KmzdRLXfl=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-03-17T01:00:00Z

Page 286

Issuer ST: *Barcelona*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-G63287510*
Subject CN: *ANF AC Servicio de conservación*
Subject E: *soporte@anf.es*
Subject OU: *Certificado Cualificado de Sello Electronico*
Subject O: *ANF Autoridad de Certificacion*
Subject L: *Barcelona*
Subject ST: *Cataluña*
Subject C: *ES*
Valid from: *Thu Dec 03 11:01:00 CET 2020*
Valid to: *Sat Dec 03 11:01:00 CET 2022*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A5:3E:E0:35:E6:74:20:1D:4A:18:85:DF:3E:B1:50:DA:79:DA:78:19:B1:6D:E1:EC:04:7D:E3:E8:86:1A:D4:90:95:28:F6:94:5B:CF:8F:FB:13:41:08:0D:3D:0A:9D:3A:16:AA:B4:93:4C:2E:81:30:F7:FE:FF:52:3D:3C:8C:7A:02:EE:72:D9:4E:AE:4D:94:D6:82:D6:95:40:1C:51:1E:DD:A9:E9:61:44:8C:74:4F:2D:67:D7:5D:16:80:AF:18:20:22:9F:08:88:8F:82:26:E7:D1:C1:EA:E7:79:A5:D9:AD:B8:14:07:62:C5:96:B4:60:89:18:2B:3E:53:78:9F:39:A3:55:0A:8A:5:6:74:89:2E:9A:29:25:78:04:C9:8F:2B:A8:2B:4C:52:42:18:C3:69:6F:15:AC:A7:DF:59:3A:FA:EE:66:88:FF:CD:E2:A0:38:E0:EB:6E:4E:6A:3C:D8:E7:5E:DE:78:EC:FA:98:E2:3F:E3:09:9F:2D:82:76:69:85:CA:B0:80:E6:0E:4D:7E:04:1A:2B:AD:57:37:4C:3F:9F:3D:CB:30:FD:94:F3:1A:38:72:4D:C5:BE:9E:DE:55:10:CE:C8:23:8F:B9:10:89:FD:FA:AF:6D:83:9B:03:C7:4B:E8:08:56:15:DD:D1:46:21:65:C1:D4:F7:63:E5:5F:02:03:01:00:01*
Authority Key Identifier *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Subject Key Identifier *11:5E:8B:8B:62:23:EB:73:D1:95:0B:C6:F8:05:EE:A3:FB:16:92:53*
Subject Alternative Name *soporte@anf.es*
Extended Key Usage *id_kp_clientAuth*
CRL Distribution Points *https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*
Certificate Policies
Policy OID: 1.3.6.1.4.1.18332.25.1.1.1
CPS pointer: https://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.1
Authority Info Access
http://ocsp.anf.es/spain/AV
http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer
Basic Constraints *IsCA: false*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *54:AC:F8:77:4B:6F:AB:83:7B:AB:F5:47:3E:C7:8B:13:85:7E:5E:D1:D7:D5:9F:30:B3:5C:9C:EA:3E:9F:C8:62*

X509SubjectName

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *ANF AC Servicio de conservación*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: *ES*

X509SKI

X509 SK I *EV6Li2Ij63PRIQvG+AXuo/sWkIM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2023-02-15T00:00:00Z*

6.11.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.11.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.11.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service Name

Name *[en]* *Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC*

Name *[es]* *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados de ANF AC*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-G63287510*

Subject CN: *ANF AC Servicio de conservación*

Subject E: *soporte@anf.es*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject L: *Barcelona*

Subject ST: *Cataluña*

Subject C: *ES*

X509SKI

X509 SK I *EV6Li2lj63PRIQvG+AXuo/sWkIM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-03-17T01:00:00Z*

6.11.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.11.3.2 - Extension (critical): additionalServiceInformation

Subject CN: ANF Secure Server CA
Subject OU: ANF Autoridad intermedia tecnicos
Subject O: ANF Autoridad de Certificacion
Subject C: ES
Subject SERIAL NUMBER: G63287510
Valid from: Mon Nov 09 13:47:22 CET 2020
Valid to: Thu Nov 07 13:47:22 CET 2030
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E1:F4:4B:D5:B6:72:8F:A0:3E:08:40:64:7B:B6:7B:09:6A:1E:1E:49:1C:06:CF:
31:FF:B1:DC:1D:88:2C:47:C8:55:CD:3F:27:89:83:FD:9E:07:9C:7E:70:02:69:7E:34:AE:46:90:71:49:7C:A9:1F:82:39:07:0C:F5:23:EC:2E:37:E0:A3:B1:C2:02:F6:3A:66:2A:82:7B:E2:89:59:
DC:FD:91:C0:FF:8F:FD:09:84:10:40:57:7E:93:EC:13:8F:D3:E3:2B:A9:30:A1:B6:DF:E8:BE:BF:4E:57:EA:08:F2:57:C1:74:23:89:3F:0B:06:06:1F:F6:EF:00:5B:9A:6E:6B:18:82:5A:B0:05:88:
5F:C3:EF:00:8E:CC:C7:49:A1:AF:60:A7:FB:C2:47:25:FE:0F:5A:9D:36:67:17:5F:DE:3E:22:31:0D:D0:1B:BA:D2:67:F9:03:1D:F5:F7:D1:F5:46:8F:9E:B6:E4:CC:59:67:E5:13:79:7E:F3:A9:2A:
9A:2A:8D:8D:4B:2E:A6:DC:2B:C5:5B:5E:31:1A:CE:AC:23:F6:1F:F6:57:A1:A6:59:F3:D4:E1:21:87:94:9C:BC:B2:8F:51:4C:89:E8:6F:08:63:72:F5:B1:53:85:3C:00:26:D9:3F:E0:95:AF:23:A
1:A1:93:33:FD:64:CE:2F:BE:14:A6:E1:45:2E:7D:E2:A5:BD:58:DA:92:B5:F8:51:FF:17:F6:08:72:D8:3E:B6:72:B8:C7:A6:3C:F8:8C:D9:B9:12:F2:1A:C8:03:03:99:B9:AD:F5:0C:34:8E:19:E6:
46:04:91:63:D8:C7:B9:73:68:A8:53:BC:71:F8:17:B1:17:A3:04:53:3B:3F:2B:61:C5:A8:18:35:BC:C6:BD:E4:54:BF:19:3E:B8:30:56:85:B3:0F:24:35:A4:C1:A4:A8:98:2C:99:C1:61:15:6A:C
E:B8:C0:C1:61:96:FE:FC:25:C4:1A:A8:43:F0:04:26:64:9C:37:4E:58:07:6D:28:A3:1E:37:D9:75:CC:FC:15:88:4B:AA:F1:14:C7:70:6A:7B:25:B0:15:98:40:F9:C7:45:89:FC:28:A5:13:38:50:A
7:50:0A:94:9D:A5:8C:B1:8F:F6:B8:12:AC:82:1C:D8:DD:40:F3:F3:4C:14:4E:11:5D:ED:75:54:EC:72:86:09:9F:D5:18:CA:3F:8F:97:44:8F:8F:4D:9E:B1:8B:CF:CF:0A:6D:E9:C1:C2:BE:F2:14:
68:89:E3:9E:B6:88:38:A6:EE:A0:CB:06:F7:FD:67:55:63:33:3F:EA:1F:98:D9:48:E4:F7:5C:9D:CF:29:4D:3B:75:E1:62:7E:59:B9:11:80:16:8E:31:02:03:01:00:01

```

Authority Key Identifier 9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37
Subject Key Identifier 96:02:AD:E4:C9:F9:4F:B0:AD:38:0B:A4:FE:AE:6C:A6:6E:E4:7C:8A
Extended Key Usage id_kp_serverAuth
CRL Distribution Points
<http://crl.anf.es/crl/ANFSecureServerRootCA-ar1.crl>
<http://www.anf.es/crl/ANFSecureServerRootCA-ar1.crl>
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <http://www.anf.es/es/documentos>
Authority Info Access
<http://ocsp.anf.es/spain/AV>
<http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer>
Basic Constraints IsCA: true
Key Usage: digitalSignature - keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 30:6B:F8:09:96:36:A4:4F:FF:B5:EE:DC:E6:E3:0C:0F:36:C7:D4:3F:6C:CA:5A:2C:A3:AB:71:66:8F:35:33:20

X509SubjectName

Subject CN: ANF Secure Server CA
Subject OU: ANF Autoridad intermedia tecnicos
Subject O: ANF Autoridad de Certificacion

Subject C: ES

Subject SERIAL NUMBER: G63287510

X509SKI

X509 SK I IgKt5Mn5T7CtOAuk/q5spm7kflo=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2021-03-17T01:00:00Z

6.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

6.13 - Service (granted): Certificados electrónicos cualificados emitidos por «ANF AC Qualified Certificates for eSignature»

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados electrónicos cualificados emitidos por «ANF AC Qualified Certificates for eSignature»

Name [en] Qualified certificate issued by «ANF AC Qualified Certificates for eSignature»

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1012805015691284571405761703

Certificate Policies*Policy OID: 2.5.29.32.0**CPS pointer: <https://anf.es/repositorio-legal/>**CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]***Authority Info Access***<http://ocsp.anf.es/spain/AV>**http://crl.anf.es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer***Basic Constraints***IsCA: true***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***B7:CD:F2:3A:73:A2:DA:1B:51:5A:64:40:3E:90:A3:B9:0C:45:DD:FB:B2:55:8B:C1:C1:2F:B9:BC:FA:2E:5A:23***X509SubjectName****Subject CN:***ANF AC Qualified Certificates for eSignature***Subject OU:***Certificados Cualificados de Firma Electronica***Subject 2.5.4.97:***VATES-G63287510***Subject O:***ANF Autoridad de Certificacion***Subject C:***ES***X509SKI****X509 SK I***Ki8z/L1sf1gGUxhA4n72ubATi3A=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2023-01-31T00:00:00Z***Scheme Service Definition URI****URI** *[en]**<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI** *[es]**<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***6.13.1 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.13.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.18332.3.4.1.8.22

6.14 - Service (granted): Certificados electrónicos cualificados emitidos por «ANF AC Qualified Certificates for eSeal»

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[es]	Certificados electrónicos cualificados emitidos por «ANF AC Qualified Certificates for eSeal»
Name	[en]	Qualified certificate issued by «ANF AC Qualified Certificates for eSeal»

Service digital identities**Certificate fields details**

Version:	3
Serial Number:	1014815336566756646709811293

Certificate Policies*Policy OID: 2.5.29.32.0**CPS pointer: <https://anf.es/repositorio-legal/>**CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC]***Authority Info Access***<http://ocsp.anf.es/spain/AV>**http://crl.anf.es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer***Basic Constraints***IsCA: true***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***34:31:29:2A:66:FB:3E:A5:3F:8B:70:6E:A4:D9:80:38:1C:B8:65:DF:6C:99:F0:52:45:36:54:5B:58:CF:9F:FF***X509SubjectName****Subject CN:***ANF AC Qualified Certificates for eSeal***Subject OU:***Certificados Cualificados de Sello Electronico***Subject 2.5.4.97:***VATES-G63287510***Subject O:***ANF Autoridad de Certificacion***Subject C:***ES***X509SKI****X509 SK I***fNOsW6NNyfEwAnfdTrHVXWHkyow=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2023-01-31T00:00:00Z***Scheme Service Definition URI****URI** *[en]**<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI** *[es]**<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***6.14.1 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.14.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.18332.25.1.1.9

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.18332.25.1.1.11

6.15 - Service (withdrawn): Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de validación"

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Service type description	[en]	undefined.
	[es]	undefined.

Service Name

Name	[en]	Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de validación"

Name	[es]	Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados "ANF AC Servicio de validación"

Service digital identities**Certificate fields details**

Version:	3

Serial Number:	995616158423738526593418293

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.18332.10.4=G63287510

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A3:E8:60:F2:D9:A5:E7:B4:B2:63:4B:87:BC:AC:1E:0D:3D:F7:56:54:F8:90:2D:83:D*
A:16:60:A3:FD:D6:FD:92

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

X509SKI

X509 SK I *UtafUoOU5ofKm7IGQuP7aR+jgBs=*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] undefined.

[es] undefined.

Status Starting Time*2025-03-13T00:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

6.15.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.15.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.15.3 - History instance n.1 - Status: granted**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q***Service Name**

Name [en] *Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de validación"*

Name [es] *Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados "ANF AC Servicio de validación"*

Service digital identities**X509SubjectName**

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

X509SKI

X509 SK I *UtafUoOU5ofKm7lGQuP7aR+jgBs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-02-15T00:00:00Z*

6.15.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.15.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

6.16 - Service (withdrawn): Qualified electronic registered delivery service by "Sign to Sign Delivery Services"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en]* *An electronic delivery service providing qualified electronic deliveries.*
[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[en]* *Qualified electronic registered delivery service by "Sign to Sign Delivery Services"*

Name *[es]* *Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"*

Service digital identities

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:55:61:13:40:FD:38:89:52:2E:8A:50:5E:42:65:02:29:02:59:74:66:2B:17:3A:81:4B:F4:13:72:EB:E7:18:8B:56:B3:9A:72:3B:2C:D6:CA:5F:40:5F:6D:C6:3A:6B:75:09:75:FB:C0:A2:1E:3B:02:23:B3:92:6C:11:03:41:4B:1E:11:89:35:E8:5A:2D:5D:17:53:67:3D:CE:D0:A8:C2:FB:07:EB:DF:29:FA:46:DA:40:95:7F:B0:8C:09:8B:43:ED:6D:81:2F:56:72:C8:18:9E:1F:4D:7E:65:74:7D:A0:C2:19:71:36:3D:A3:18:1A:D4:3A:7A:C9:3C:A9:8A:65:35:2E:2E:9B:7A:84:38:74:CE:33:3A:3F:88:E5:8F:1E:8A:73:DD:20:DD:FA:F0:83:7F:31:1B:78:4E:0D:50:92:38:0C:A0:AB:96:DE:18:9E:AE:3D:83:20:EE:AD:0F:0C:8F:98:12:0B:89:D5:F9:8C:D4:52:89:BF:7D:F9:01:0D:35:3A:00:F6:29:18:BD:30:05:26:E7:91:38:98:52:75:22:E1:3F:33:52:30:06:7C:72:74:B0:15:0F:C1:52:A8:35:DD:76:EB:13:9F:41:9D:95:19:47:68:BB:5A:AC:BE:12:2F:DB:19:F6:C9:8A:A5:8E:5B:AD:78:04:DD:43:02:03:01:00:01

Authority Key Identifier

7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C

Subject Key Identifier

75:67:1B:D1:86:EB:46:D0:25:E3:97:A0:D4:63:03:3C:B0:F4:C5:CD

Subject Alternative Name

soporte@anf.es

OID.1.3.6.1.4.1.18332.10.4=G63287510

Extended Key Usage

id_kp_clientAuth

CRL Distribution Points

http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl

Certificate Policies

Policy OID: 1.3.6.1.4.1.18332.25.1.1.9

CPS pointer: <http://www.anf.es/documentos>

Policy OID: 0.4.0.194112.1.3

Authority Info Access

<http://ocsp.anf.es/spain/AV>

<http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer>

Basic Constraints

IsCA: false

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

id_etsi_qcs_QcSSCD

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

F6:91:23:12:D8:88:D3:BD:A4:E7:05:CE:BD:2A:E8:65:5B:15:05:E7:F3:AA:4B:23:F0:AA:20:7C:5D:0E:A1:A0

X509SubjectName**Subject L:**

BARCELONA

Subject ST:

BARCELONA

Subject 2.5.4.97:

VATES-G63287510

Subject OU:

Certificado Cualificado de Sello Electronico

Subject O:

ANF Autoridad de Certificacion

Subject CN:

Sign to Sign Delivery Services

Subject SERIAL NUMBER:

G63287510

Subject C: ES

X509SKI

X509 SK I dWcb0YbrRtAl45eg1GMDPLD0xc0=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-03-13T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

6.16.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [en] Qualified electronic registered delivery service by "Sign to Sign Delivery Services"

Name [es] Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"

Service digital identities

X509SubjectName

Subject L: BARCELONA

Subject ST: BARCELONA

Subject 2.5.4.97: VATES-G63287510

Subject OU: Certificado Cualificado de Sello Electronico

Subject O: ANF Autoridad de Certificacion

Subject CN: Sign to Sign Delivery Services

Subject SERIAL NUMBER: G63287510

Subject C: ES

Issuer 2.5.4.97: *VATES-G63287510*
Issuer O: *ANF Autoridad de Certificacion*
Issuer C: *ES*
Subject L: *BARCELONA*
Subject ST: *BARCELONA*
Subject 2.5.4.97: *VATES-G63287510*
Subject OU: *Certificado Cualificado de Sello Electronico*
Subject O: *ANF Autoridad de Certificacion*
Subject CN: *ANF AC Servicio de conservación*
Subject SERIAL NUMBER: *G63287510*
Subject C: *ES*
Valid from: *Wed Feb 01 17:06:59 CET 2023*
Valid to: *Fri Jan 31 17:06:59 CET 2025*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:96:EA:9D:03:79:47:EA:81:2D:F9:53:62:CE:9D:F7:65:4E:65:19:95:DE:6D:58:4E:FD:D8:84:21:30:45:C4:49:22:06:34:4F:6C:4D:7B:8B:07:DE:74:94:00:DC:AC:15:34:4A:A3:9F:DE:3B:F6:81:BA:4D:53:AF:13:8B:30:9A:DD:B3:32:93:01:37:60:82:35:3D:6A:0A:97:13:19:8C:91:66:B7:E3:3D:EE:C4:BF:3F:37:D7:DD:F2:71:B2:33:13:84:46:FB:A8:44:8F:B7:C3:31:DF:A1:7D:E6:C6:D7:11:A4:0C:B3:A8:2E:A5:80:21:1B:F9:38:E6:75:33:81:FF:C4:7B:7A:E5:D6:95:FB:0F:9F:E1:82:F3:FA:68:14:AD:BA:B6:1C:54:F1:72:58:0A:25:0B:B9:46:FE:8B:7F:A1:EE:17:3B:60:45:E4:96:9A:26:52:35:15:1E:22:7C:9D:BE:9D:81:06:97:8F:98:4B:50:06:BD:E3:6F:80:5D:FB:6A:5C:90:DD:8B:C8:E0:76:71:D6:43:F3:89:52:23:E3:66:B7:7B:3C:F6:DE:3D:E0:F2:1E:8E:29:60:2E:05:26:AA:CE:E6:C1:DD:5B:AE:C5:48:86:06:E0:5E:95:DB:5B:D1:AB:FE:69:C0:1A:B9:2A:6D:91:5D:6C:9B:04:A1:02:03:01:00:01*
Authority Key Identifier *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*
Subject Key Identifier *31:A0:3E:00:2E:C7:E3:95:6A:7D:CF:0E:3C:D0:34:FE:6B:B3:AC:39*
Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.18332.10.4=G63287510
Extended Key Usage *id_kp_clientAuth*
CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3
Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer
Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A9:F1:05:6A:B9:B3:F9:3C:0F:35:4A:C1:F4:00:6D:9E:ED:41:F8:95:95:29:4B:ED:2E:2E:4D:16:9E:F5:1F:D9*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *ANF AC Servicio de conservación*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

X509SKI

X509 SK I *MaA+AC7H45Vqfc8OPNA0/muzrDk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2025-03-13T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

6.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

6.17.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

6.17.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service Name

Name	[en]	Qualified preservation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de conservación"

Name	[es]	Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados "ANF AC Servicio de conservación"

Service digital identities**X509SubjectName**

Subject L:	BARCELONA
Subject ST:	BARCELONA
Subject 2.5.4.97:	VATES-G63287510
Subject OU:	Certificado Cualificado de Sello Electronico
Subject O:	ANF Autoridad de Certificacion
Subject CN:	ANF AC Servicio de conservación
Subject SERIAL NUMBER:	G63287510
Subject C:	ES

X509SKI

X509 SK I	MaA+AC7H45Vqfc8OPNA0/muzrDk=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2023-02-15T00:00:00Z

Signature algorithm: *SHA256withRSA*

Issuer CN: *ANF AC Qualified Certificates for eSeal*

Issuer OU: *Certificados Cualificados de Sello Electronico*

Issuer 2.5.4.97: *VATES-G63287510*

Issuer O: *ANF Autoridad de Certificacion*

Issuer C: *ES*

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

Valid from: *Wed Feb 05 11:15:23 CET 2025*

Valid to: *Wed Jan 30 11:15:23 CET 2030*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:81:0B:C9:51:18:68:15:95:F5:0C:32:C8:14:A3:14:72:DE:35:63:56:4B:8C:E8:B0:17:EF:89:C4:E2:76:22:95:5C:01:51:05:73:62:BC:E9:8E:94:80:C5:04:49:85:69:03:38:15:6A:2A:80:89:0A:93:1F:CA:E7:06:8B:30:9A:AF:85:CD:63:0D:00:9A:9D:CD:F3:FE:CF:8C:C4:95:A8:3D:9F:FF:0A:C3:CC:BD:E7:08:00:8C:95:4B:35:9B:35:7F:61:DC:F1:61:8A:24:EC:6C:02:7F:68:51:C6:99:4A:78:0A:BF:1D:C6:08:59:88:6A:F4:97:46:D3:48:57:FC:9F:53:77:88:CD:44:B3:18:5E:D1:F2:78:99:73:CE:FD:4B:C2:CB:40:4E:A3:03:12:27:75:A1:C0:5A:0D:A5:C6:B8:2E:D9:A4:56:92:DE:E4:21:0E:08:FF:95:58:85:FC:5D:93:61:95:BF:10:23:EC:4E:FC:53:B2:23:86:7E:C4:C6:FA:5D:6D:D2:D2:30:52:49:B0:61:76:6E:18:B2:5D:E7:F0:42:D0:9C:26:F7:1C:06:43:D2:3C:24:1F:DE:57:24:22:46:FE:49:63:20:30:D1:5C:88:AB:96:3E:82:7B:F4:84:1C:0F:D3:19:B4:99:26:FD:59:AC:24:A8:9F:02:03:01:00:01*

Authority Key Identifier *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*

Subject Key Identifier *63:8C:5B:1A:C0:6D:32:95:84:FE:95:CD:07:09:40:60:AA:5B:C3:74*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.18332.10.4=G63287510

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *98:93:B6:C2:60:31:C7:51:D1:28:B6:C7:A6:D4:63:E1:04:02:66:B6:00:1C:14:FA:45:9E:AE:D6:1E:B3:31:70*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

X509SKI

X509 SK I *Y4xbGsBtMpWE/pXNBwLAYKpbw3Q=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-03-13T00:00:00Z*

6.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.18.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.19 - Service (granted): Qualified electronic registered delivery service by Sign to Sign Delivery Services 2025

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q

Service type description	[en]	undefined.
	[es]	undefined.

Service Name

Name	[en]	Qualified electronic registered delivery service by Sign to Sign Delivery Services 2025

Name	[es]	Servicio cualificado de entrega electrónica certificada Sign to Sign Delivery Services 2025

Service digital identities

Certificate fields details

Version: 3

Serial Number: 998971279387218164748443963

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: ANF AC Qualified Certificates for eSeal

Issuer OU: *Certificados Cualificados de Sello Electronico*

Issuer 2.5.4.97: *VATES-G63287510*
Issuer O: *ANF Autoridad de Certificacion*
Issuer C: *ES*
Subject L: *BARCELONA*
Subject ST: *BARCELONA*
Subject 2.5.4.97: *VATES-G63287510*
Subject OU: *Certificado Cualificado de Sello Electronico*
Subject O: *ANF Autoridad de Certificacion*
Subject CN: *Sign to Sign Delivery Services*
Subject SERIAL NUMBER: *G63287510*
Subject C: *ES*
Valid from: *Wed Feb 05 11:15:23 CET 2025*
Valid to: *Wed Jan 30 11:15:23 CET 2030*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:1C:1A:6F:99:95:11:7A:69:80:75:FF:E6:32:54:2C:0A:13:D1:1B:F0:8E:12:1F:02:17:3D:F6:64:93:7E:B6:62:FA:F8:03:76:28:AF:81:92:5E:0B:ED:7E:34:D4:31:94:54:27:51:F3:7B:67:E5:62:C9:B5:F0:81:8A:45:A6:80:69:71:CC:6D:72:0C:EA:F2:79:99:EB:2B:52:88:08:D9:4D:E1:A1:4B:1F:51:D8:23:8C:B2:88:90:13:83:EE:C4:95:21:0D:DA:84:DD:21:22:3E:09:B5:E8:77:FF:36:89:2E:99:91:ED:97:75:41:06:2D:9F:3E:84:AE:AE:16:39:0F:E7:04:AF:CA:4:15:AE:6E:1F:34:25:BB:37:3E:AE:23:40:38:65:D6:3A:B8:B2:95:EE:28:CF:48:E8:92:51:67:BC:EE:E7:A1:8A:B5:18:1B:87:FC:D0:60:CB:03:E2:05:B5:74:6F:C0:22:64:61:12:21:EA:92:6B:8B:0C:83:F6:64:B8:91:DA:25:98:C1:D3:F0:6E:CE:D1:96:44:29:2A:6C:53:83:9D:4E:E1:B9:46:DC:03:E1:EE:68:70:A5:32:93:71:C9:66:61:D2:D5:34:89:8B:CF:C7:F0:87:6E:06:62:ED:08:82:27:98:19:2F:D2:A8:19:AB:C2:B1:02:03:01:00:01*
Authority Key Identifier *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*
Subject Key Identifier *29:C5:0B:77:31:30:1D:8D:25:7A:2A:21:C8:EA:F4:69:B1:3A:F7:3C*
Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.18332.10.4=G63287510
Extended Key Usage *id_kp_clientAuth*
CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3
Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer
Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *85:BD:21:36:DF:50:9E:04:98:4B:7F:BD:9C:66:5E:2C:26:E4:EC:E8:58:7A:CF:D5:5C:69:EE:FD:D6:07:93:C3*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Autoridad de Certificacion*

Subject CN: *Sign to Sign Delivery Services*

Subject SERIAL NUMBER: *G63287510*

Subject C: *ES*

X509SKI

X509 SK I *KcULdzEwHY0leiohyOr0abE69zw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-03-13T00:00:00Z*

6.20 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals ANF AC Servicio de conservación 2025

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service type description *[en] A preservation service for qualified electronic signatures.*
[es] Un servicio de la preservación de las firmas electrónicas reconocidas.

Service Name

Subject C: *ES*

Valid from: *Wed Feb 05 11:15:24 CET 2025*

Valid to: *Wed Jan 30 11:15:24 CET 2030*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A5:B1:6B:A8:76:6F:13:53:4D:61:98:D8:F1:08:9C:CA:65:51:87:68:A0:6B:C6:F1EF:7C:3E:C7:8F:A6:46:9A:D9:60:49:E8:B3:89:3D:E5:88:20:58:8A:E4:EB:4A:21:0E:32:2D:EE:F2:8A:DA:DF:58:DC:15:E6:32:F1:3F:7E:45:F1:5B:83:8F:83:13:39:1C:A6:8E:32:AD:CF:B2:E4:46:76:BF:5A:A9:49:01:04:61:80:D3:42:CB:51:EE:71:67:3A:85:97:5A:4D:EB:77:EA:32:6D:FE:2C:A0:4E:71:34:78:AD:32:05:9B:4A:A6:19:D4:EB:2F:C5:4B:22:4E:79:43:28:A2:8E:71:E CED:66:16:CD:52:10:B3:A1:61:E2:2C:A4:ED:B0:57:A3:FC:21:61:94:90:05:5D:1C:58:47:C3:4A:56:44:2F:E7:C2:4D:A4:B9:6F:B6:CA:3E:3E:36:9E:76:49:93:B7:14:31:F1:00:22:96:D5:65:73:1F:3D:39:9A:C8:B4:81:71:A4:48:5B:2E:09:18:FD:A0:47:1B:11:80:1D:70:D6:90:37:E0:75:A3:35:C8:47:82:CD:11:F8:32:C4:98:99:6D:98:75:0E:49:0E:47:B5:4E:48:05:91:16:46:23:F0:45:66:C9:84:FB:FB:7F:89:67:E3:02:03:01:00:01*

Authority Key Identifier *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*

Subject Key Identifier *44:90:25:D7:1A:AB:7F:41:22:7B:E6:AB:52:7B:6C:18:1B:6F:97:F1*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.18332.10.4=G63287510

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *18:49:D7:DA:C7:0F:7C:1C:AC:46:06:58:B2:18:E3:81:8E:68:95:B0:91:E0:E9:1A:89:27:2A:BF:78:00:2E:52*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-G63287510*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: ANF Autoridad de Certificación

Subject CN: ANF AC Servicio de conservación

Subject SERIAL NUMBER: G63287510

Subject C: ES

X509SKI

X509 SKI RJA1xqrf0Eie+arUntsGBtvI/E=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-03-13T00:00:00Z

6.20.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.20.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.21 - Service (granted): Qualified time stamps issued by ANF AC Qualified TSA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified time stamps issued by ANF AC Qualified TSA

Name [es] Servicio Sellos de tiempo cualificados emitidos por ANF AC Qualified TSA

Service digital identities

Certificate fields details

Version: 3

3

Serial Number: 998430095372259593600630501

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer O: *ANF Autoridad de Certificacion*

Issuer OU: *ANF Clase 1 CA*

Issuer C: *ES*

Issuer CN: ANF Global Root CA

Issuer SERIAL NUMBER: *G63287510*

Subject CN: *ANF AC Qualified TSA*

Subject OU: *Sellado de tiempo cualificado*

Subject 2.5.4.97: *VATES-G63287510*

Subject 0: *ANF Autoridad de Certificacion*

Subject C: *ES*

Valid from: Wed Nov 13 12:31:26 CET 2024

Valid to: *Sun Nov 11 12:31:26 CET 2035*

Public Key:

Authority Key Identifier 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

Subject Key Identifier *E8:BD:81:8C:52:84:3D:E6:47:D7:B8:98:42:4B:B7:39:AC:A9:4A:23*

CRL Distribution Points	<i>http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://anf.es/repositorio-legal/</i> <i>CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]</i>
Authority Info Access	<i>http://ocsp.anf.es/spain/AV</i> <i>http://crl.anf.es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer</i>
Basic Constraints	<i>IsCA: true</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>AF:BC:8E:2D:54:6C:A7:49:9D:8A:81:04:A7:65:B0:0D:2A:30:F3:B0:27:53:94:D6:7A:8D:60:C0:3D:01:63:B5</i>

X509SubjectName

Subject CN:	<i>ANF AC Qualified TSA</i>
Subject OU:	<i>Sellado de tiempo cualificado</i>
Subject 2.5.4.97:	<i>VATES-G63287510</i>
Subject O:	<i>ANF Autoridad de Certificacion</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>6L2BjFKEPeZH17iYQku3OaypSiM=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time*2025-03-27T00:00:00Z*

7 - TSP: Consejo General de la Abogacía Española

TSP Name

Name *[en]* *Consejo General de la Abogacía Española*

Name *[es]* *Consejo General de la Abogacía Española*

TSP Trade Name

Name *[en]* *VATES-Q2863006I*

Name *[en]* *AC ABOGACÍA*

Name *[es]* *AC ABOGACÍA*

Name *[en]* *Consejo General de la Abogacia NIF:Q-2863006I*

Name *[en]* *Consejo General de la Abogacia NIF Q2863006I*

Name *[en]* *Consejo General de la Abogacia*

Name *[en]* *CONSEJO GENERAL DE LA ABOGACIA*

PostalAddress

Street Address *[en]* *Paseo de Recoletos, 13*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28004*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Paseo de Recoletos, 13*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28004*

Country Name *[es]* *ES*

ElectronicAddress

URI [en] <http://www.acabogacia.org>

URI [en] <mailto:info@acabogacia.org>

TSP Information URI

URI [en] <http://www.acabogacia.org>

URI [es] <http://www.acabogacia.org>

7.1 - Service (withdrawn): Qualified certificate provided by AC Certificados Corporativos

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified certificate provided by AC Certificados Corporativos*

Name [es] *Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 161146793180004064011629729231987846242

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIF5TCCBM2gAwIBAgIQeTu+UkNX0v1C9JEjpsYjANBgkqhkiG9w0BAQUFADBSMQswCQYDVQOQ
EwFjU2E2MDQGA1UECmQ29uc2Vqb3BhZDZlcmFscGRllGxhIEFib2dhY2h1IE5JRjRlTlR4MmMw
MDZlMTIwMAYDVQQDEYlBdXRVcmkYlYQZGUGQ2VydGlnaWVhY2Vib2Z5b25BbYm9nYWNpYTAE
Fw0wNTA2MTUwNzI4MDRaFw0xNzA2MTUwMjAwMDBaMHQswCQYDVQGEWjUzEPMAAGAlUEBxMG
TWFkcmkMSAwqYlR0ZmVudGlnaWVhY2Vib2dhY2h1IE5JRjRlTlR4MmMwMDZlMTIwMAYDVQOQ
EwFjU2E2MDQGA1UECmQ29uc2Vqb3BhZDZlcmFscGRllGxhIEFib2dhY2h1IE5JRjRlTlR4MmMw
MDZlMTIwMAYDVQOQEwFjUzEPMAAGAlUEBxMGYlYQZGUGQ2VydGlnaWVhY2Vib2Z5b25BbYm9nYWNpYTAE
aWVhY2Vib2Z5b25BbYm9nYWNpYTAEaWVhY2Vib2Z5b25BbYm9nYWNpYTAEaWVhY2Vib2Z5b25BbYm9nYWNpYTAE
h6yKXZmNVdzEb12qtmppYMQioTnopby4NpWdrcr0HD92+zQjvIFRPjGMVhK11Vinh4teyQn
U3U9uwKjKt8DLToZGnersiCaxzGunsNlGjMcprMjHhOrpGc3MhOvKGIK0OlinkArteBE08
/q2zeG8ngpTsz5kxwz2m2f56b9bW8YleYVScplCLKq6n38m3nLZ0nm2ypvvyz2J8jh
BgVigIA0ZGo/MbUDKjCm9K3dcxOZYdFVqH040V46ptHgefKAHMK9u2wJnL1YhGdNCMG08+S
j25fQzG08yewKizAirh2ar9XxasCAwEAaOCAGkwgIFMDcGA1UdeGQwMc6BEWfjQGFjYlVjv
Z2FjaWEub3JnhhldHRwOi8vd3d3LmFjYlVjvZ2FjaWEub3JnMA8GA1UdeWFBwOFMAMBA8wDgYD
VR0PAQH/BAQDAgEGMBEGCWCsAGG+ElBAQOEAWlAB2AdBgNVHQ4EFgQUWnIMpQ28CBYswoVFTzkr
5yFf8b8whwYDVR0BBgqFolUjlnMj0EsCOQicmNn8F5pMTwgaGA1UdeIA5BzCBgQOCBoYl
KwYBAGBgRUKAEOwqZEWLQYIKwYBBQUHAgEWXVyaTpodrRwOi8vd3d3LmFjYlVjvZ2FjaWEub3Jn
L2RvzBgBgrBGEFBQCCAlBUIGIDb25zdWw0ZSBSY5BkZWNSYXh1Y2Vib2Z5b25BbYm9nYWNpYTAE
ZGUGY2VydGlnaWVhY2Vib2Z5b25BbYm9nYWNpYTAEZGUGY2VydGlnaWVhY2Vib2Z5b25BbYm9nYWNpYTAE
YKBeoFyGLGh0dHA6Ly93d3cuYWNhYm9nYWNpY5vcmcy3j3sL2FjYlVjvZ2FjaWEub3JnshixodHRw
Oi8v3j3sLmFjYlVjvZ2FjaWEub3JnL2Nybc9hY2Fib2dhY2h1LmNybDANBgkqhkiG9w0BAQUFAAOC
AQEAUvmcLaagCOK41RUNCFA2HyY7XQJFuwuwKKRY+wyK8z5PPMdmWjWRUgWixOwa5l0j
rYkzvpQWwLRHwvq+G5yYtjCYfie63uRa/nfIEL2Ef1DZfdTjLqmjksrV5gh94AM7ol8j3bgl
nAFGBUwblWqMUsB294+0MQV9p9HVxjzdcjhFLKj0V15b4Qa5lqPWSkt7lghfN40bRTWzaHTncO
B1yuv9vRQY9LZmz+vFe++uT8i5N0ETm1b5cCumGfOSGAB7Aic0ZU4e8H6LroebCmY1zTouwv6
KtWvBwNB8Ssnvm09j60U5A4j45VmbjYFvpljQGYgGA==
-----END CERTIFICATE-----
```

Signature algorithm: SHA1withRSA

Issuer CN: Autoridad de Certificación de la Abogacia

Issuer O: Consejo General de la Abogacia NIF:Q-28630061

Issuer C: ES

Subject CN: *ACA - Certificados Corporativos*
Subject OU: *Autoridad de Certificacion de la Abogacia*
Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*
Subject E: *ac@acabogacia.org*
Subject L: *Madrid*
Subject C: *ES*
Valid from: *Wed Jun 15 09:28:04 CEST 2005*
Valid to: *Wed Jun 14 00:00:00 CEST 2017*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:46:D0:14:0C:97:AC:8A:D1:76:66:35:57:73:11:BD:76:AA:D9:A9:A5:83:34:AA:2A:13:36:8A:5B:C8:83:69:58:39:5C:AF:41:C3:F7:6F:83:95:08:EF:D4:54:4F:8C:63:15:86:41:F5:D5:58:A7:86:CE:2D:7B:24:27:53:75:3D:BB:02:8D:8C:AB:7C:0C:B4:E8:64:69:DE:AE:C8:82:71:AC:71:CC:6B:A7:80:D2:E0:24:C1:1C:A6:65:C9:1E:14:2B:A4:67:37:32:1A:2F:44:69:25:2B:43:A2:96:29:E4:02:86:1E:04:4D:3C:FE:AD:B3:1B:C8:A7:82:04:EC:CD:9E:64:C3:0A:D9:9A:BD:AD:7D:2E:8D:F5:5C:01:61:47:98:FD:54:82:A4:97:08:08:A4:3A:02:75:FC:9A:49:DB:2D:C6:74:9E:7A:F6:CA:9B:ED:CA:FC:D3:DB:C2:61:06:05:62:83:F8:80:D1:91:A8:FC:C6:D4:0E:42:89:70:83:3D:2B:77:5C:C4:E6:58:74:52:15:A8:73:88:A1:5E:3A:A6:D1:C6:79:F2:80:1C:C2:BD:BB:6C:09:9C:BD:7F:CA:11:83:9C:23:06:3B:CF:92:8F:6E:45:43:3F:C6:3B:CC:9E:5A:49:73:02:2A:E5:9F:66:AB:97:DB:57:5D:AB:02:03:01:00:01*
Issuer Alternative Name *ac@acabogacia.org*
Subject Alternative Name *ac@acabogacia.org*
http://www.acabogacia.org
Basic Constraints *IsCA: true*
Subject Key Identifier *5A:79:4C:A1:0C:FC:08:16:2C:C2:85:45:4F:32:AB:E7:2B:45:C0:11*
Authority Key Identifier *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*
Certificate Policies *Policy OID: 1.3.6.1.4.1.16533.10.1.1*
CPS pointer: uri:http://www.acabogacia.org/doc
CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]
CRL Distribution Points *http://www.acabogacia.org/crl/acabogacia.crl*
http://crl.acabogacia.org/crl/acabogacia.crl
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *C3:2F:2C:6D:70:6F:AC:23:94:7D:2B:09:21:A4:B5:A6:98:0B:E7:96:BB:2D:D6:F2:11:8E:BA:6D:82:54:A8:FC*

X509SubjectName

Subject CN: *ACA - Certificados Corporativos*
Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject E: *ac@acabogacia.org*

Subject L: *Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2017-12-04T01:00:00Z*

7.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificate provided by AC Certificados Corporativos*

Name [es] *Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

Service digital identities

X509SubjectName

Subject CN: *ACA - Certificados Corporativos*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject E: *ac@acabogacia.org*

Subject L: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *WnlMoQz8CBYswoVFTzKr5ytFwBE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

7.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDA sURN]	<i>urn:oid:1.3.6.1.4.1.16533.10.5.1</i>

7.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

7.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	<i>Qualified certificate provided by AC Certificados Corporativos</i>

Name	[es]	<i>Certificados Reconocidos emitidos por CA AC Certificados Corporativos</i>

Service digital identities

X509SubjectName

Subject CN: *ACA - Certificados Corporativos*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject E: *ac@acabogacia.org*

Subject L: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *WnIMoQz8CBYswoVFTzKr5ytFwBE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-05-22T00:00:00Z*

7.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAURN]* *urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.2 - Service (withdrawn): Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Certificate fields details

Version: 3

Serial Number: 136

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm:	SHA1withRSA
Issuer E:	ca@firmaprofesional.com
Issuer CN:	Autoridad de Certificacion Firmaprofesional CIF A62634068
Issuer L:	C/ Muntaner 244 Barcelona
Issuer C:	ES
Subject CN:	Autoridad de Certificacion de la Abogacia
Subject O:	Consejo General de la Abogacia NIF Q2863006I
Subject OU:	Consulte http://www.acabogacia.org
Subject L:	Paseo de Recoletos 13 Madrid
Subject E:	ac@acabogacia.org
Subject C:	ES
Valid from:	Tue Mar 02 10:43:10 CET 2004
Valid to:	Tue Mar 26 00:00:00 CET 2013

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:30:1D:65:B4:B4:5B:2A:CF:0E:B9:CB:52:99:3A:50:18:A1:F1:2D:5F:D6:50:3A:1F:95:76:2E:99:D0:60:42:7F:38:22:03:7D:4F:D8:F0:F5:4A:9B:1F:BE:AD:58:A1:45:AE:BF:BC:F9:CE:B6:8E:24:B4:C2:27:25:DC:84:F2:D5:50:82:11:88:FD:61:77:96:E0:79:49:55:DC:53:79:71:7C:8B:7F:5C:72:81:EA:CA:A4:F1:EF:D8:D1:A9:E6:DD:EC:9A:67:8B:C6:8D:CC:51:06:62:28:7E:6E:3A:3E:71:8C:23:C7:9E:63:05:13:DE:EA:F7:C9:C2:08:7F:EE:67:80:D3:F6:E9:2D:E2:EB:25:88:CF:A8:E0:9A:ED:77:02:1A:7A:DF:13:12:E4:94:C9:0C:E3:A4:88:48:08:00:C3:84:63:C7:C4:D4:26:37:6C:25:59:8B:D0:33:4B:A3:C9:AD:53:3F:F3:18:56:93:60:B6:4E:C7:C1:5FAE:00:3F:3D:79:05:3A:E5:AF:5D:F3:1D:44:44:3A:47:1A:9E:57:9E:56:93:8A:03:08:25:2D:C2:46:D1:FC:D9:C0:03:27:CA:9D:1A:7E:DB:4A:00:2E:CD:94:CF:ED:16:25:F7:F6:00:01:27:67:DE:6C:D7:EC:A4:26:D7:39:F8:B1:2D:02:03:01:00:01

Issuer Alternative Name

<http://www.firmaprofesional.com>

Subject Alternative Name

<http://www.acabogacia.org>

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

22:BA:59:71:AC:73:A4:13:6D:3C:18:AF:F5:D0:82:E3:56:BD:93:B0

Authority Key Identifier

33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7

Certificate Policies

Policy OID: 1.3.6.1.4.1.13177.10.10.1

CPS pointer: <http://www.firmaprofesional.com/cps/cps.htm>

CRL Distribution Points

<http://crl.firmaprofesional.com/firmaprofesional.crl>

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

BC:85:94:4D:A4:E3:04:E9:B7:05:8A:19:B6:73:AF:95:F5:40:D0:0D:CD:A0:10:90:3A:00:9D:A2:FB:AC:AB:6E

X509SubjectName**Subject CN:**

Autoridad de Certificacion de la Abogacia

Subject O:

Consejo General de la Abogacia NIF Q2863006I

Subject OU:

Consulte <http://www.acabogacia.org>

Subject L:

Paseo de Recoletos 13 Madrid

Subject E:

ac@acabogacia.org

Subject C:

ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2016-06-30T22:00:00Z

7.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**7.2.2 - History instance n.1 - Status: supervisionceased****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name	[en]	Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía

Name	[es]	Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía

Service digital identities**X509SubjectName**

Subject CN:	Autoridad de Certificacion de la Abogacia

Subject O:	Consejo General de la Abogacia NIF Q28630061

Subject OU:	Consulte http://www.acabogacia.org

Subject L:	Paseo de Recoletos 13 Madrid

Subject E:	ac@acabogacia.org

Subject C:	ES

X509SKI

X509 SK I	IrpZcaxzpBNtPBiv9dCC41a9k7A=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time** 2007-05-21T22:00:00Z**7.2.3 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name	[en]	Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía

Name	[es]	Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía

Service digital identities**X509SubjectName**

Subject CN: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia NIF Q28630061*

Subject OU: *Consulte <http://www.acabogacia.org>*

Subject L: *Paseo de Recoletos 13 Madrid*

Subject E: *ac@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *IrpZcaxzpBNtPBiv9dCC41a9k7A=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2004-11-25T00:00:00Z*

7.3 - Service (withdrawn): Qualified Certificates issued by ACA Trusted

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by ACA Trusted*

Name [es] *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *45119609637205326338567747423576232129*

CRL Distribution Points
<http://www.acabogacia.org/crl/acabogacia.crl>
<http://crl.acabogacia.org/crl/acabogacia.crl>

Key Usage:
keyCertSign - cRLSign

Thumbprint algorithm:
SHA-256

Thumbprint:
68:07:A3:F3:7B:3C:6C:18:07:48:52:65:73:0B:BE:3F:6A:37:86:6F:34:8F:5E:F2:12:3C:E8:63:77:38:E0:FC

X509SubjectName

Subject CN:
ACA - Trusted Certificates

Subject O:
Consejo General de la Abogacia NIF:Q-2863006I

Subject OU:
Autoridad de Certificacion de la Abogacia

Subject E:
ca@acabogacia.org

Subject C:
ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] *undefined.*
 [es] *undefined.*

Status Starting Time *2017-12-04T01:00:00Z*

7.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
 [es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities

X509SubjectName

Subject CN: *ACA - Trusted Certificates*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject E: *ca@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *WvY0zpZ2Vrd86dzcHRNsed4PMHY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

7.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACA Trusted*

Name *[es]* *Certificados Reconocidos emitidos por CA ACA Trusted*

Service digital identities**X509SubjectName**

Subject CN: *ACA - Trusted Certificates*

Subject O: *Consejo General de la Abogacia NIF:Q-2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject E: *ca@acabogacia.org*

Subject C: *ES*

X509SKI

X509 SK I *WvY0zpZ2Vrd86dzcHRNsed4PMHY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-09-27T22:00:00Z*

7.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDAURN]* *urn:oid:1.3.6.1.4.1.16533.20.2.1*

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name [en]

Qualified certificate provided by AC Certificados Corporativos 2014

Name [es]

Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014

Certificate fields details

Version: 3

Serial Number: 50277584362934511984483198896977516751

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion de la Abogacia*

Issuer O: *Consejo General de la Abogacía NIF:O-28630061*

Issuer C: *ES*

Subject CN: *ACA - Certificados Corporativos - 2014*

Subject SERIAL NUMBER: 028630061

Subject OU: *Autoridad de Certificación de la Abogacía*

Subject 0: *Consejo General de la Abogacía*

Subject C: ES

Issuer C: *ES*
Subject CN: *ACA - Certificados Corporativos - 2014*
Subject SERIAL NUMBER: *Q2863006I*
Subject OU: *Autoridad de Certificacion de la Abogacia*
Subject O: *Consejo General de la Abogacia*
Subject C: *ES*
Valid from: *Wed Mar 05 17:57:30 CET 2014*
Valid to: *Tue Mar 05 17:57:30 CET 2030*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:80:FA:18:04:60:97:F8:EB:18:44:39:56:05:30:F3:8A:F1:4D:F1:BF:29:27:6C:82:EB:B5:E8:8E:56:54:E0:C8:EE:C8:E6:1E:B9:BF:A9:87:49:2C:08:83:C7:D1:F3:54:CD:A4:A6:74:49:0C:4C:D1:E5:B9:A2:80:12:86:2F:7C:30:7D:A2:CF:94:E6:02:D7:EE:97:AE:D7:48:72:33:03:94:9C:B6:C8:51:58:F6:98:7C:74:92:8A:95:C6:E5:1C:EB:26:8D:14:27:8D:B4:84:58:76:CD:9D:FD:37:4E:89:40:15:EC:70:C2:A9:4E:EF:47:D1:42:12:47:20:00:30:D5:FE:B3:CF:A7:03:EF:D6:5A:EF:7B:BE:02:AC:F4:4F:21:E7:BA:EF:3C:6D:72:A9:77:7D:B8:2A:B9:A2:70:DA:75:B7:FD:8C:3B:EF:4F:14:2E:91:B3:C8:7E:83:04:C0:9B:1B:75:A7:5B:EC:BC:BC:77:FA:EA:E4:C0:98:35:68:47:50:89:70:4A:EE:6A:66:69:F5:1B:3E:36:07:5C:83:E1:92:A7:B4:12:F9:18:D5:C6:B6:47:A0:1F:DE:2F:AE:A3:2A:D9:F5:EF:B9:19:C2:55:EC:F0:E4:CE:71:5A:9E:FC:38:3E:BB:9F:D0:AF:88:FD:15:EA:A0:CF:2A:39:02:03:01:00:01*
Basic Constraints *IsCA: true*
Subject Key Identifier *33:6D:D0:E9:CD:18:D7:B4:EB:4E:FC:F3:E3:CD:FB:3D:5B:C0:A3:9E*
Authority Key Identifier *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*
Certificate Policies *Policy OID: 1.3.6.1.4.1.16533.10.1.1*
CPS pointer: uri:http://www.acabogacia.org/doc
CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]
CRL Distribution Points *http://www.acabogacia.org/crl/acabogacia.crl*
http://crl.acabogacia.org/crl/acabogacia.crl
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *5C:DF:25:EE:A9:A1:49:42:F3:4B:38:B8:EA:17:24:2D:DC:53:F8:78:1D:25:A7:8A:98:18:9E:94:E1:69:72:91*

X509SubjectName

Subject CN: *ACA - Certificados Corporativos - 2014*
Subject SERIAL NUMBER: *Q2863006I*
Subject OU: *Autoridad de Certificacion de la Abogacia*
Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2017-12-04T01:00:00Z*

7.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.16533.10.5.1*

7.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified certificate provided by AC Certificados Corporativos 2014*

Name *[es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014*

Service digital identities

X509SubjectName

Subject CN: *ACA - Certificados Corporativos - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: ES

X509SKI

X509 SKI M23Q6c0Y17TrTvzz4837PVvAo54=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

7.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

7.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

7.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified certificate provided by AC Certificados Corporativos 2014

Name [es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014

Service digital identities

X509SubjectName

Subject CN: ACA - Certificados Corporativos - 2014

Subject SERIAL NUMBER: Q2863006I

Subject OU: Autoridad de Certificacion de la Abogacia

Subject O: Consejo General de la Abogacia

Subject C: ES

X509SKI

X509 SK I M23Q6c0Y17TrTvzz4837PVvAo54=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2014-06-04T22:00:00Z

7.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

7.5 - Service (withdrawn): Qualified Certificates issued by ACA Trusted 2014

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by ACA Trusted 2014

Name [es] Certificados Reconocidos emitidos por CA ACA Trusted 2014

Service digital identities

Certificate fields details

Version: 3

Serial Number: 124100380054207126185684841771003655184

Version: 3

Serial Number: 103184541973990179423004459516921083112

-----END CERTIFICATE-----

Subject Key Identifier *81:8F:D1:63:00:4A:CA:4D:20:97:A6:52:00:60:2E:D2:CC:36:8B:6D*

Authority Key Identifier *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*

Certificate Policies *Policy OID: 1.3.6.1.4.1.16533.10.1.1*
CPS pointer: uri:http://www.acabogacia.org/doc
CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]

CRL Distribution Points *http://www.acabogacia.org/crl/acabogacia.crl*
http://crl.acabogacia.org/crl/acabogacia.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BE:F7:3E:BA:EE:78:9B:5B:7A:FC:E3:87:04:2E:1D:E9:3F:B4:57:BD:3B:A7:DC:CE:5C:BB:9F:A9:9F:15:24:DD*

X509SubjectName

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2017-12-04T01:00:00Z***7.5.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDASURN] urn:oid:1.3.6.1.4.1.16533.20.2.1*

7.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

7.5.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by ACA Trusted 2014

Name	[es]	Certificados Reconocidos emitidos por CA ACA Trusted 2014

Service digital identities**X509SubjectName**

Subject CN:	ACA - Trusted Certificates - 2014
Subject SERIAL NUMBER:	Q2863006I
Subject OU:	Autoridad de Certificacion de la Abogacia
Subject O:	Consejo General de la Abogacia
Subject C:	ES

X509SKI

X509 SK I	gY/RYwBKyk0gl6ZSAGAu0sw2i20=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

7.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.20.2.1

7.5.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**7.5.4 - History instance n.2 - Status: undersupervision****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name

[en]

Qualified Certificates issued by ACA Trusted 2014

Name

[es]

Certificados Reconocidos emitidos por CA ACA Trusted 2014

Service digital identities**X509SubjectName**

Subject CN:

ACA - Trusted Certificates - 2014

Subject SERIAL NUMBER:

Q2863006I

Subject OU:

Autoridad de Certificacion de la Abogacia

Subject O:

Consejo General de la Abogacia

Subject C:

ES

X509SKI

X509 SK I

gY/RYwBKyk0gl6ZSAGAu0sw2i20=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2014-06-04T22:00:00Z

7.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Subject CN: ACA CA1
Subject O: CONSEJO GENERAL DE LA ABOGACIA
Subject OU: AUTORIDAD DE CERTIFICACION DE LA ABOGACIA
Subject 2.5.4.97: VATES-Q28630061
Subject C: ES
Valid from: Thu Jun 23 14:09:37 CEST 2016
Valid to: Sun Jun 23 14:09:37 CEST 2030
Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BA:F0:FF:97:4E:FA:06:8E:55:5C:B6:03:C5:24:4B:35:7D:97:68:E7:6A:9A:D2:4B:AB:8B:7A:83:AC:35:11:53:84:F0:1F:8C:F2:C2:81:04:AF:F9:78:51:0C:F4:CC:E8:8B:48:70:92:D4:BA:A9:13:06:66:6F:A9:73:87:5F:2E:C3:8B:ED:7B:F3:91:AF:38:92:6C:72:16:F7:5E:3C:14:A7:AC:3A:BA:FB:8F:22:A1:FB:04:A7:8A:E2:FA:A0:21:03:4A:76:8D:DD:C0:3E:C0:5B:C5:75:90:4B:C0:A6:74:08:62:A8:18:5A:4A:09:8E:3E:32:68:4D:51:7D:19:89:39:13:AA:19:06:8B:94:6D:89:E7:BE:80:30:1A:E0:62:5E:9A:26:34:DF:AC:54:A4:53:48:13:D2:19:D9:32:68:49:F2:8D:89:83:75:81:C1:36:F2:50:6F:E0:78:D8:2F:40:18:8F:27:9C:62:C3:EE:10:77:C9:48:98:84:94:A4:0E:83:22:F9:6C:37:64:0F:2E:23:27:70:55:19:04:81:07:7E:4F:F3:CF:77:E1:80:E0:38:60:83:88:DF:1E:4C:70:23:83:AD:24:8C:23:82:88:07:58:10:01:8C:70:EF:46:F3:69:FF:9F:57:5A:61:08:E3:C2:18:8F:7B:C4:89:5B:73:30:97:C4:E8:21:D6:C0:BB:C6:EE:3C:1C:90:99:38:42:90:A8:0C:90:DE:9A:3F:A7:2C:82:F0:5C:5E:83:C7:50:F5:10:47:9F:9F:F2:08:2F:55:F8:D5:5B:8C:36:21:2F:87:1F:48:82:E8:C4:9A:35:7A:02:16:A6:6F:EA:30:36:A3:26:39:CA:F5:59:21:F9:90:E8:28:EA:BB:8C:D1:A2:28:86:64:78:67:59:87:E6:30:8D:7F:8C:0C:D7:3F:D0:B7:55:5A:DA:06:A2:8C:A4:04:01:2D:0B:85:3C:EC:8E:E5:86:D8:82:CA:26:59:80:8B:03:8C:4E:F2:AC:5E:5B:55:28:86:D8:0B:72:E5:87:22:8C:26:37:58:43:16:46:6A:9D:C1:29:90:6D:CB:AE:E6:F4:3E:EB:16:32:89:17:1A:BD:94:DE:0A:A3:49:CC:2B:86:70:8B:A4:1D:9D:66:9A:AC:CF:68:CC:6B:15:BD:E7:3D:12:8F:4E:C7:D6:38:D5:56:27:95:DF:D6:1C:A1:7C:E8:E0:31:0B:19:F8:C8:84:1D:AA:58:0B:F4:46:8E:F0:03:D9:A1:49:F3:BC:FA:2F:B5:76:3D:60:B5:AD:E9:66:18:8C:11:84:39:81:EA:50:E6:32:FB:82:A8:EA:65:2A:71:3D:C7:2F:02:03:01:00:01
Basic Constraints *IsCA: true*
Extended Key Usage *id_kp_clientAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.acabogacia.org/doc>
Subject Key Identifier 72:A9:E7:D6:8E:02:67:A0:4A:4C:1A:67:31:BC:B7:FE:CB:84:B4:9B
Authority Info Access *<http://ocsp.redabogacia.org>*
http://www.acabogacia.org/certificados/aca_root.crt
Authority Key Identifier 1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD
CRL Distribution Points *http://www.acabogacia.org/crl/aca_arl.crl*
http://crl.acabogacia.org/crl/aca_arl.crl
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 70:5E:B3:A0:B1:F0:9D:ED:A3:ED:45:76:6B:BB:C0:21:97:70:0A:BB:1E:2D:1D:9E:28:62:AC:58:9D:C9:FD:77

X509SubjectName

Subject CN: ACA CA1
Subject O: CONSEJO GENERAL DE LA ABOGACIA
Subject OU: AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

Subject 2.5.4.97: *VATES-Q2863006I*

Subject C: *ES*

X509SKI

X509 SK I *cqnn1o4CZ6BKTbMby3/suEtJs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-11-02T00:00:00Z*

7.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.7 - Service (granted): Qualified certificates issued by ACA CA2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[en]* *Qualified certificates issued by ACA CA2*

Name *[es]* *Certificados cualificados emitidos por ACA CA2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *97911743187377240900748830157217551837*

Authority Info Access
<http://ocsp.redabogacia.org>
http://www.acabogacia.org/certificados/aca_root.crt

Authority Key Identifier
 1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD

CRL Distribution Points
http://www.acabogacia.org/crl/aca_arl.crl
http://crl.acabogacia.org/crl/aca_arl.crl

Key Usage:
 keyCertSign - cRLSign

Thumbprint algorithm:
 SHA-256

Thumbprint:
 7E:93:16:A5:CE:CF:B9:0A:53:AD:C3:C7:76:94:50:F4:2C:DC:3A:9B:85:DF:4C:75:77:B0:53:DC:BB:25:58:12

X509SubjectName

Subject CN:
 ACA CA2

Subject O:
 CONSEJO GENERAL DE LA ABOGACIA

Subject OU:
 AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

Subject 2.5.4.97:
 VATES-Q2863006I

Subject C:
 ES

X509SKI

X509 SK I
 ihUfr3TvHwEHcyqQKkEJfhtlOMA=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
 [es] undefined.

Status Starting Time
 2017-12-04T01:00:00Z

7.7.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

7.7.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**7.7.3 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified certificates issued by ACA CA2

Name

[es]

Certificados cualificados emitidos por ACA CA2

Service digital identities**X509SubjectName****Subject CN:**

ACA CA2

Subject O:

CONSEJO GENERAL DE LA ABOGACIA

Subject OU:

AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

Subject 2.5.4.97:

VATES-Q2863006I

Subject C:

ES

X509SKI**X509 SK I**

ihUfr3TvHwEHcyqQKkEJfhtlOMA=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2016-11-02T00:00:00Z

7.7.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**7.8 - Service (withdrawn): Qualified certificates issued by ACA CA3****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified certificates issued by ACA CA3
Name	[es]	Certificados cualificados emitidos por ACA CA3

Service digital identities

Certificate fields details

Version:	3
Serial Number:	114392107427724248384195985487754308843
X509 Certificate	-----BEGIN CERTIFICATE----- MIHJTCCBQ2gAwIBAgIQVg8eVqYwsNRXa8/pD7os6zANBgkqhkiG9w0BAQsFAADBDQswCOYDVQOG EwJFuzESMBAGAlUEBRMjUT14NjMwMDZlMScwQjQyDVQOKDB5DT05TRUpIEoFTkV5QUwgrREUgTEeG QUJPfR0fDSUEUEtAFB6NVBAAMCEDD5B5T09lJmB4XDTE2MDYyMzE5MDI0OVoXDTMwMDYyMzE5MDI0 OVoWgZYxCzAJBgNVBAYTARgVYTAkVTRgVfYV9VORhDA9W0VFRUy1RMjg2MzAwNkxkMjAwBgNVBAsMKUUV VE95SURBRCEBRSBDRVJUSUZlQ0FD5lU90lERFIExBIEFCT0dBQ00lBMScwQjQyDVQOKDB5DT05TRUpP IEoFTkV5QUwgrREUgTEeGQUJPfR0fDSUEUEtAFB6NVBAAMCEDD5B5T09lJmB4XDTE2MDYyMzE5MDI0 AQUA4ACDwAwggKAOiCAODCKMFRK6sNsbdt9NpYmYVxsajASl+Q+8Bveq9wUmr/gR+9HPg9Xi tShCutwks5BilcV+AUplbbDYmYc7XIXThBqu0/Of2DEKpglWl0h6Llh99Uaw90aKGQSeG3tBwOD yqAZk7aJlMyrcDD00qvc8B9ePduzfdlJhMfAnr9d9Dm/Cy4JCWQ+MMTTO3DZlVdgyLO6 Kf2JWvajzjJBzu/k6p+DUB9EGfa8Nk3v82dVc53cx8Ytsy8rq5Wzko/KHY0psdLOCbvp8apL2 5fhKtj4z9YD2Ebbj9P0xyK5+GUKEuEKCDt9gCFMcRncdPotAudsM1BIBHhpolbUOvWlcc5Z7tl grVibe9bga58b8h0drtAdexOryy0BTZ00MOPg442LePrOy9D011k8SS53660beypH0l8IGHf bgMKsz2TxcD71tSNRkxkAHe30REHsedUVBv3y1iXaZlCMx2X3vDoGqVW2BgruFkb5UliVbcl 690D13CaDoPms4ZNgK04Ug9sTm3nNGz5hvar6xMB7h47M+tLa2dLSWFCosjY5yxQpTLAG08NC1k 4N+8Bx04eZ9ymFwAeP4e4vat6FFHA1pUJIZQ+C4H1DDU21WHdsVRLDIDPStrHWAAXQ1111TQ aq3HkuYTCnFZUgpaekHYwIDAQABo4IbPTCCAaEwDwYDVDR0TAQHBAUwAwEB/2AOBqNVHQ8BAf8E BAMCAQYwhQYDVROlBBYwFAyIKwYBBQUHAWEGCCSGAQUBwMCMd4GA1UdiaQ3MDUwMwYEVROgADAR MCKGCCSGAQUBwBpT1odHrwOi8vd3d3LmFYWjvZ2FaWEub3jnL2RvY2d8B9NVHQ4EFQOLPjd AbrGKMVMtTnc8K3m1zWVty8weAYIKwYBBQUHAQEEDBqMCCcCSGAOUFB2ABhttdHrwOi8vd2Nz cC5yZWRhYm9nYWNPY55vcmcwPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYWVhYm9nYWNPY55vcmcv Y2YyYyGimaWVhZG95Z2F1YV9ybz90LmNyY2dA8B9NVHSMGDAW9b0aVeQVMeKmxHUIHFA01wkAW/ ZlB8B9NVHREXjBcMFggWKBWhilodHrwOi8vd3d3LmFYWjvZ2FaWEub3jnL2NybC9hY2FFYXJs LmNyblYpaHR0cDovL2NybC5hY2Fib2dhY2lHlM9yZy9jcmwvYWVhYm9nYWNPY55vcmcwDQY/KoZlhwcn AQELBOADgIBAJuInQjmgpDRE7V3bCTKMAg8Wkt3PqgYwvSmUafQYRP+/XdoOcrvAILR6 LRCGZERcjoQa4X1IPqH88PnsZku3Aq8XNyGIVg8lTPA4Vm5YcdpGRB55+KObRG3AKMMBghm WRRHUC+yMnkj5e9e1jC24NjNTs1jmbCv6xmpNZt0lB470go0CjOnjC3wh46t6wo9L0kQFM68 WkXGqQ5AcvKk9K3Kc0drNTAcWz0WkHpgAALKnJoc6kZBR7K7wBpP4EgH19f3WfXCt9a/e CVRIqW51ygSajp77YVsxj4PulONstCF6FermNCKtjeOYW5tsb5tZIGW+Oq2nC9pZdvbf9D 6CLYhBMZx4G+6ixFletyqrpdFulrghcP6M6DCYXW6GDl0l1PmidxWxypPkdQWfydxGbgafx xGL9ku/GLSjT3LmPukwRb+TrIaxihlyVDVsnO60zch80LHfPYSkde7emdg86HfaE0106a pYrbeCmEw/dtcQyTJtnkZagaV1nWvX2KChotyjn2GLNL6iM4ewkQAUlQvOzmOIF4k5g8bBCE PoPmw/Uis4Ya76+yRlooX4fdl0AcVdVz5Vjlv60TCAEeLDcQZnRAiYo/Ux+RGJHj/SSUv03 I6eDfLRGKjL -----END CERTIFICATE-----
Signature algorithm:	SHA256withRSA
Issuer CN:	ACA ROOT
Issuer O:	CONSEJO GENERAL DE LA ABOGACIA
Issuer SERIAL NUMBER:	Q2863006I
Issuer C:	ES
Subject CN:	ACA CA3
Subject O:	CONSEJO GENERAL DE LA ABOGACIA
Subject OU:	AUTORIDAD DE CERTIFICACION DE LA ABOGACIA
Subject 2.5.4.97:	VATES-Q2863006I
Subject C:	ES
Valid from:	Thu Jun 23 14:02:49 CEST 2016
Valid to:	Sun Jun 23 14:02:49 CEST 2030

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C2:88:A3:05:7C:AE:AC:36:C6:DD:B7:D3:69:62:66:22:57:1B:1A:8C:04:88:F9:0F:BC:06:F7:AA:F7:05:26:AF:F8:11:F8:D1:CF:83:D5:E2:7D:28:42:BA:DC:24:B1:20:62:95:C5:7E:01:4A:63:6D:80:D8:99:87:3B:C4:85:D3:84:1A:AE:D3:F3:9F:D9:D1:24:3D:C2:56:23:48:7A:2E:58:7D:F5:46:80:F7:46:8A:19:04:9E:0A:8D:ED:07:04:03:CA:00:19:93:88:09:31:1C:82:73:80:D0:D2:AB:F2:F1:C0:72:78:F0:EE:CE:47:E2:75:48:4C:AC:50:21:AF:F6:BD:74:FD:1D:A FFF:C6:CB:8F:E3:09:64:3E:30:CE:D3:43:70:D9:21:57:60:C8:B3:8A:90:FC:C9:5A:F6:A3:8F:32:09:07:3B:BF:92:3E:A9:F8:35:3C:F4:41:9F:68:CC:4D:93:7B:FC:D9:D5:5C:E7:77:31:F1:8B:6C:CB:CA:EA:E5:9C:E4:3B:F5:C7:63:4A:6C:74:B3:92:6E:FA:7C:6A:92:F6:E5:F8:4A:B7:F2:78:CF:D6:03:D8:46:C1:27:D3:F4:C7:22:89:F8:65:0A:12:E1:17:08:38:49:80:27:CC:71:19:DC:7 4FA:AD:03:F8:9D:80:CD:41:94:17:C7:A6:89:58:50:E5:56:95:C7:39:67:BB:65:82:B5:62:E9:EF:18:80:0E:51:6C:11:F4:76:B1:40:0D:E5:CE:7F:28:34:6D:36:6D:D3:43:0E:3E:00:38:D8:B7: 8F:AD:06:20:97:D0:FF:97:59:1B:4A:C4:B7:E8:A4:1B:13:2A:48:87:45:3C:94:61:DF:EA:03:0A:E7:3D:93:C5:C0:F8:D6:D4:8D:B5:19:31:00:77:B7:B8:A1:21:49:E7:54:55:F0:6B:BF:7C:B5:8 9:76:99:22:50:8C:C7:65:F7:BC:3A:06:A9:55:B6:06:07:EE:18:46:F9:52:58:95:95:B7:09:EB:D3:83:D7:70:9A:0E:83:E6:83:86:4D:80:A4:38:52:0F:6C:4E:6D:E7:34:6C:F9:86:F6:AB:EB:13: 01:EE:1E:3B:33:EB:4B:03:67:4B:49:61:42:A2:C2:58:E7:2C:50:A5:F4:CB:00:6D:3C:34:2D:64:E0:DF:81:6D:70:F6:79:9F:71:26:61:6F:03:13:C0:AF:8B:6F:6A:D6:FA:14:70:35:8E:75:07:65: 0F:8E:E0:7D:5D:0D:4D:B5:58:77:5A:55:12:C3:94:33:D2:AE:8A:C7:58:00:17:43:52:F5:D5:37:D0:6A:AD:C7:5E:E6:13:09:39:C5:65:48:29:69:E9:07:63:02:03:01:00:01

Basic Constraints*IsCA: true***Extended Key Usage***id_kp_serverAuth***Certificate Policies***Policy OID: 2.5.29.32.0**CPS pointer: <http://www.acabogacia.org/doc>***Subject Key Identifier***3D:D8:DD:01:BA:C6:28:C5:4C:B5:39:C2:F0:AD:E6:D7:35:95:4F:2F***Authority Info Access***<http://ocsp.redabogacia.org>**http://www.acabogacia.org/certificados/aca_root.crt***Authority Key Identifier***1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD***CRL Distribution Points***http://www.acabogacia.org/crl/aca_arl.crl**http://crl.acabogacia.org/crl/aca_arl.crl***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***AF:57:FD:80:5A:0E:F9:0E:97:57:65:C0:D5:D5:5E:3F:D2:4C:FC:49:B7:3A:A1:A4:9 E:19:79:01:8D:54:FC:26***X509SubjectName****Subject CN:***ACA CA3***Subject O:***CONSEJO GENERAL DE LA ABOGACIA***Subject OU:***AUTORIDAD DE CERTIFICACION DE LA ABOGACIA***Subject 2.5.4.97:***VATES-Q2863006I***Subject C:***ES***X509SKI****X509 SK I***PdjdAbrGKMVMtTnC8K3m1zWVTy8=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2023-09-14T00:00:00Z*

7.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication***7.8.2 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name***[en]**Qualified certificates issued by ACA CA3***Name***[es]**Certificados cualificados emitidos por ACA CA3***Service digital identities****X509SubjectName****Subject CN:***ACA CA3***Subject O:***CONSEJO GENERAL DE LA ABOGACIA***Subject OU:***AUTORIDAD DE CERTIFICACION DE LA ABOGACIA***Subject 2.5.4.97:***VATES-Q2863006I***Subject C:***ES***X509SKI****X509 SK I***PdjdAbrGKMVMtTnC8K3m1zWVTy8=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2017-12-04T01:00:00Z***7.8.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en]

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name [en]

[en]

Qualified certificates issued by ACA 1

Name [es]

[es]

Certificados cualificados emitidos por ACA 1

Certificate fields details

Version: 3

3

Serial Number: 475620442846804506607735566580566146960161737045

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withECDSA*

Issuer CN: ACA ROOT 2

Issuer O: *CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA*

Issuer 2.5.4.97: VATES-028630061

Issuer C: *ES*

Subject CN: ACA 1

Subject 0: *CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject C: ES

Valid from: Mon Mar 18 16:51:30 CET 2024

Valid to: *Fri Mar 18 16:51:30 CET 2044*

Public Key: *30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:01:CB:94:25:B5:F9:66:34:84:7B:88:BE:DE:C6:9B:F1:B0:24:BD:C4:2A:8D:33:02:3A:62:5F:EF:22:68:A2:2D:9D:43:6F:77:61:A1:06:6A:C3:1A:6F:03:AC:2F:4A:FE:89:2E:67:05:AB:84:0A:8F:A6:2A:4A:AC:41:08:03:2A:83:F4:01:44:D8:37:EC:D1:5B:56:69:0B:55:DA:72:BC:A1:CB:65:21:46:F1:EC:E4:FA:88:BF:03:BC:FE:F7:2D:07:E9:D5:8F:65:27:E9:22:5B:42:93:83:BC:1B:F8:80:1C:42:48:47:B8:2E:07:53:BA:5A:F7:3B:81:10:60:F4:79:3C:3A:90*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *5C:E7:DC:7B:92:2B:FA:71:F0:AD:19:1D:A1:36:8F:D4:76:18:B3:15*

Authority Info Access *http://acacert.acabogacia.org/aca_root2.crt
http://acaocsp.acabogacia.org/*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: http://www.acabogacia.org/doc*

CRL Distribution Points *http://acacrl.acabogacia.org/crl/ACA_root2_ARL.crl
https://acacrl.acabogacia.org/crl/ACA_root2_ARL.crl*

Subject Key Identifier *62:8E:68:88:32:5F:FF:9D:5B:2E:9F:3B:43:8A:03:05:F4:08:33:C2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C6:DF:AA:AC:E2:35:DA:93:E1:C8:7D:4E:C7:76:86:52:56:3D:54:C5:38:B3:1E:8C:B
D:06:80:E9:1D:B7:53:16*

X509SubjectName

Subject CN: *ACA 1*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject C: *ES*

X509SKI

X509 SK I *Yo5oiDJf/51bLp87Q4oDBfQIM8I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.
[es] undefined.*

Status Starting Time *2026-02-19T03:00:00Z*

7.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

7.9.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

7.9.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.1.2

Description**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.2.2

Description**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.3.2

Description**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.4.2

Description**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.5.2

Description**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.16533.50.6.2
Description		
Description		

7.9.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by ACA 1*

Name [es] *Certificados cualificados emitidos por ACA 1*

Service digital identities

X509SubjectName

Subject CN: *ACA 1*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject C: *ES*

X509SKI

X509 SK I *Yo5oiDJf/51bLp87Q4oDBfQIM8I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-07-24T00:00:00Z*

7.9.4.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.9.4.2 - Extension (critical): additionalServiceInformation

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject C: *ES*

Valid from: *Mon Mar 18 17:26:13 CET 2024*

Valid to: *Fri Mar 18 17:26:13 CET 2044*

Public Key:
*30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:00:F0:96:50:9D:E7:4B:41:8C:BE:5C:41:79:23:89:6B:A4:A0:8E:07:89:66:5C:D1:84:EE:05:1F:D3:D6
A3:3E:48:D2:E0:00:2B:47:86:A1:82:79:68:82:21:14:E3:28:31:DE:85:76:5C:58:C7:18:09:E9:A6:35:11:22:C2:41:15:91:00:C7:8E:1F:37:BB:19:8C:0A:46:17:BF:3C:08:28:41:21:34:10:3B
:37:68:DD:A5:54:C6:2C:B0:20:43:F2:4E:6B:88:67:2E:EE:B0:4C:B7:10:64:72:23:56:85:9E:66:AF:9F:15:47:3E:52:BF:93:5C:4E:93:E4:29:CF:72:56:62:E0*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *5C:E7:DC:7B:92:2B:FA:71:F0:AD:19:1D:A1:36:8F:D4:76:18:B3:15*

Authority Info Access *http://acacert.acabogacia.org/aca_root2.crt
http://acaocsp.acabogacia.org/*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: http://www.acabogacia.org/doc*

CRL Distribution Points *http://acacrl.acabogacia.org/crl/ACA_root2_ARL.crl
https://acacrl.acabogacia.org/crl/ACA_root2_ARL.crl*

Subject Key Identifier *57:5B:CC:BF:F1:01:4B:34:8A:E7:AE:03:72:CD:65:FD:07:AA:1F:8B*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DE:A1:D4:D5:42:2C:CE:C8:36:4A:58:A8:E6:D2:21:FD:BE:16:73:24:6B:33:54:38:6
7:1F:67:A8:60:17:EF:DC*

X509SubjectName

Subject CN: *ACA 2*

Subject O: *CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA*

Subject 2.5.4.97: *VATES-Q2863006I*

Subject OU: *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

Subject C: *ES*

X509SKI

X509 SK I *V1vMv/EBSzSK564Dcs1l/QeqH4s=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] undefined.

Status Starting Time 2026-02-19T03:00:00Z

7.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

7.10.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.16533.60.1.2

Description

Description

7.10.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified certificates issued by ACA 2

Name [es] Certificados cualificados emitidos por ACA 2

Service digital identities

X509SubjectName

Subject CN: ACA 2

Subject O: CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA

Subject 2.5.4.97: VATES-Q2863006I

Subject OU: AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

Subject C: ES

X509SKI

X509 SK I *V1vMv/EBSzSK564Dcs1l/QeqH4s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-07-24T00:00:00Z*

7.10.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8 - TSP: Colegio de Ingenieros de Caminos, Canales y Puertos

TSP Name

Name [en] *Colegio de Ingenieros de Caminos, Canales y Puertos*

Name [es] *Colegio de Ingenieros de Caminos, Canales y Puertos*

TSP Trade Name

Name [en] *CICCP*

Name [es] *CICCP*

Name [en] *VATES-Q2867009I*

Name [en] *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

PostalAddress

Street Address [es] *Almagro, 42*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Postal Code [es] *28010*

Country Name [es] *ES*

PostalAddress

Street Address [en] *Almagro, 42*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28010*

Country Name [en] *ES*

ElectronicAddress

URI [en] *mailto:informatica@ciccp.es*

URI [en] *http://www.ciccp.es*

TSP Information URI

Page 364

Issuer C: *ES*
Subject CN: *CA CICCIP Clase 3*
Subject OU: *CICCIP C.I.F. Q-2867009-I*
Subject O: *CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos*
Subject L: *Madrid*
Subject ST: *Madrid*
Subject C: *ES*
Subject E: *pki@ciccp.es*
Valid from: *Wed Oct 23 17:16:34 CEST 2002*
Valid to: *Mon Jan 23 16:26:34 CET 2006*
Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:3D:EB:1D:7A:92:21:88:BE:FD:48:99:B8:A1:9A:2E:34:98:21:15:DC:99:08:7A:C9:43:C4:9A:A7:DC:24:DD:68:27:41:A2:03:DE:B9:58:64:D6:54:15:EE:72:F9:08:E4:AA:0A:90:F8:58:BA:A2:7B:80:44:9B:80:2A:5A:F7:00:5A:4A:7F:99:90:7B:9A:1C:39:6D:FA:5D:63:4B:67:35:8D:A8:1F:4B:9B:B1:45:A0:9D:03:93:BB:A7:E2:EC:2E:E1:11:01:04:EE:40:39:97:C2:2D:90:9A:07:BE:58:5A:2B:7B:30:1A:8B:3C:AB:A6:DE:73:89:90:83:99:F1:14:98:86:87:29:64:03:A3:F5:86:52:34:3E:98:E9:60:9C:12:88:75:EB:18:F4:07:CB:2B:02:AC:0B:82:20:0F:CF:80:70:9C:18:C1:80:E4:F0:20:CD:84:76:C4:53:5A:09:C4:53:27:24:89:CC:23:99:3A:87:96:E0:50:AA:95:10:4E:07:17:07:66:80:74:FC:8D:BC:F1:9B:39:4B:42:87:C8:B5:D1:79:5F:19:8D:2F:50:42:B3:6E:07:91:7D:4D:09:6A:93:76:A0:7B:56:5D:3C:83:6C:35:2B:46:BC:1F:79:00:85:F2:B1:D1:BF:30:BC:8F:D9:3C:63:82:EB:02:03:01:00:01
Subject Key Identifier *EE:8E:43:4E:DC:53:F7:6D:24:01:3D:1C:44:46:36:1F:07:A2:BB:FB*
Basic Constraints *IsCA: true*
Authority Key Identifier *BA:DD:EB:7F:1D:55:12:D1:1F:B0:17:39:82:7C:1B:5A:66:B3:B0:8A*
CRL Distribution Points
http://pki.ciccp.es/pki/caciccp.crl
http://pkiback.ciccp.es/pki/caciccp.crl
Authority Info Access
http://pki.ciccp.es/pki/caciccp.crt
http://pkiback.ciccp.es/pki/caciccp.crt
Key Usage: *digitalSignature - nonRepudiation - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *DD:5A:AB:55:AB:2D:22:CC:CB:DB:C3:71:33:CC:FB:B3:E5:1A:D4:B9:C3:3C:EC:15:3F:AF:3B:48:B6:8C:58:C2*
X509SubjectName
Subject CN: *CA CICCIP Clase 3*
Subject OU: *CICCIP C.I.F. Q-2867009-I*
Subject O: *CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

8.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificate*

Name [es] *Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

Service digital identities

X509SubjectName

Subject CN: *CA CICCP Clase 3*

Subject OU: *CICCP C.I.F. Q-2867009-I*

Subject O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

X509SKI

X509 SK I *7o5DTtxT920kAT0cREY2Hweiu/s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2010-01-25T00:00:00Z*

8.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate*

Name *[es]* *Certificados Reconocidos emitidos por la CA CICCPC Clase 3 PKI anterior*

Service digital identities**X509SubjectName**

Subject CN: *CA CICCPC Clase 3*

Subject OU: *CICCPC C.I.F. Q-2867009-I*

Subject O: *CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

X509SKI

X509 SK I *7o5DTtxT920kAT0cREY2Hweiu/s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2005-03-03T00:00:00Z*

8.2 - Service (withdrawn): Qualified Certificate

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
Service Name		
Name	[en]	Qualified Certificate
	[es]	Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3
Service digital identities		
Certificate fields details		
Version:	3	
Serial Number:	135031685893278259059350935028450579902	
X509 Certificate	-----BEGIN CERTIFICATE----- MIIGeCCBGogAwIBAgIQZyH3oF77FcwRIZuXVvjaNBgkqhkiG9w0BAQUFADCBzzEhMBkGCSqG SIlb3DQGEIARYMcGtpQGnpY2NwLmVzM0swCQYDVQGEW/FUZEPMA0GA1UECBMGWfKcmkMQ8wDQYD VQOHewZNYWYyaW0xOzBBBgNVBAAgT0kNMQ0NMQ0GQ29sZWdpbW8kbmdlbmlcm9zIGRIENh bWluu3MgO2FuYXkcyb5IFB1ZAB03MmTAfBgNVBAsTGENJQ0N0JEMuSS5SLBRLT14NlcwMDk1 STZEMBCGA1UEAxMQ00EgO0ID01AgQ2xhc2UgMzAeFw0wOTA4MTcxMDI1MjhaFw0xOTA4MTcxMDM1 MjZaMHpMRswGQYJKoZIhvcNAQkBFgwa2IAyZjly3AuZXMxMzA2BgNVBAYTAkVMTQ8wDQYDVQOQI EwZNYWYyaW0xOzBBBgNVBAAgT0kNMQ0NMQ0GQ29sZWdpbW8kbmdlbmlcm9zIGRIENh Z2ZVusWVyb3MgZGUgO2FtaW5vcyBDYW5hbGvZiHkgUHVicnRvczEhMB8GA1UECxMY00ID01AgQy5j LkYulFEtMjZzAw0S1JMRkwfWYDVQQDEXBQSD5UNDUCBDbGZzZSAzMlIjANBgkqhkiG9w0B AQEFAAOCBgAMICCGKCAAgEA0HL0+2AHSicUThv40eycdWg990CC24KngbK354dRoQ+arg+NpKt gWZ0Hj2xvKEOWHFsele7YjGikWUjp6Xe+9YtaG1SLkMFF5h0GAVDujatXH2Z2TyWLSce8ngWUD btkhV5A04cvFHismHiddHmVD54E0cwj9Xret3rayPcc74Cz9uxlITY+4fXCL5VBWit6T4EC6DuQP vd+9uAyu19INQIMZn81ugH0wJcgsg0a3KPPX+3nREYNESjRPS6atWFTLmuQmVzE02TBHke9Gx eCBV9oSSUXZ49nseek187IKYIRmK7PrER8zNXdtZuY100fMP78v+nw18fmuO14zmRXUSeWY7j Wh0jKdi0F04VIDXjwRbJly5cR71ote3MMvOyEhv+14vN6Y+3jo2ndKAHFL00R7ArK+ksn59dl q43xZigXT9atg7QkE1730kZn1Y9bV6at0UjTuM1cnmTE5C53D+scmcg6n8vjZc0S7yZ1 1oBYUjNB88kqDNz3/Z2I7+GGn9heX4XZ3P+Jrfs+Ls25Vu2or/Csd8bxfz2AXsRSGrG/Ofanr vtY/Q9OUNhDmgR80zP7jdi8wrQ/GorEyKcKuDrtsAtmPl2N6j4ZU38hnc76pN0zaOgaUyTIS wdrFT71Y+BSUJCWbQp5oe+8CAwEAaahRMEBwCwOVROPBAAQ0AgGCMABCA1UdEwEBwOFMAMBA8w HQYDVRO0BBYEFM+NapRP0kPUA3TdAgx6k7WWDSMBAAGCSGAQ0BgicVAQQDAGAMAAQCSG5Ib3 DQEBBQUAA4ICAQAEvolcVIGQOP17MvQOW5W2vPOBlnbGzUma2BZz1qsyhg0UisgC0YexhRXalhX ejaxWEIEj0z+4lq6QUQ3cs2s3EJZUjNnQ4aspE9N45f0bwn0oKwNhmkbPjKkwvCvNf948fm3 q+K+G0RroPm1bJly24U4K+7UjyH0wRjCBL1JPEwlt/Pwphg/aks8RE2plsjwajlNukRz5W57 qd14RdgVrQH2NC8vq1p34LhGjwUlkSebLZ447m/cn/Gn+sm7OmN+ackCE3O17XJlG19EMM 52FoR8Hluc4H0OECDOsag0y7ExEtrKvSpOCw2b5fpfYv69B/UlMTTICTvzkCS1GspkUIEOZ K2EgAr+LBSC3swD7gDev+SCiyULqujyysKUH7RDT1L6BCxrYE8lp+1dAXV0PYqbg/XJx02jmg K2TH3CIBQO25di2ysEg+9YGcGk6bKhU0eJbCH+bM7sg31g9nRGmjhUX2IPVnzapaUWcx2+2Vl 5Nnz4urMvCBFLPCU6f5sLk5nOSac1gw10SpAXDnNym5dPSQ5CvUj51zCUMlyJZAhuaqBT wwVxEbJisNx0XaVH5MatnSVFv37m12D2WskHEBcUdTvJG4vOeIR0LgqfRnSwf08eD19wvry6h24 dzh1mIMjEDIKw== -----END CERTIFICATE-----	
Signature algorithm:	SHA1withRSA	
Issuer CN:	CA CICCPC Clase 3	
Issuer OU:	CICCPC C.I.F. Q-2867009-I	
Issuer O:	CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos	
Issuer L:	Madrid	
Issuer ST:	Madrid	
Issuer C:	ES	
Issuer E:	pki@ciccp.es	
Subject CN:	CA CICCPC Clase 3	
Subject OU:	CICCPC C.I.F. Q-2867009-I	
Subject O:	CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos	

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Valid from: *Mon Aug 17 12:25:28 CEST 2009*

Valid to: *Sat Aug 17 12:35:26 CEST 2019*

Public Key:

```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D0:72:CE:FB:30:21:4A:27:14:4E:1C:78:D1:EC:9C:75:68:07:F7:40:82:DB:85:
E1:81:82:91:DF:9E:1D:46:84:3E:AA:88:3E:36:02:6D:81:6D:A8:1C:9D:B1:BE:41:10:38:71:6C:78:87:88:60:91:A5:91:65:09:A7:A5:DE:F8:D6:1F:68:6A:F5:48:B9:24:30:57:F9:9E:1D:06:0
2:F0:EE:25:AB:57:1D:9D:93:C9:62:D2:71:EF:27:81:65:03:6E:D2:A1:BF:90:34:E1:CB:C5:1E:2B:0C:1E:27:5D:1E:65:43:48:81:10:73:02:7D:5E:B7:AD:DE:B6:82:3D:C7:3B:E0:2C:FD:BB:1
5:13:63:EE:1F:5D:C2:F9:7D:50:56:22:DE:93:E0:40:8A:0E:E4:0F:BD:DF:8D:88:0C:AE:D7:D2:0D:D3:F3:08:66:1F:35:BA:A1:CE:C3:F8:28:82:CA:90:68:74:4A:3D:7F:B7:9D:11:18:9C:4E:6
3:44:FB:04:E9:AB:56:15:32:66:89:09:95:CC:44:36:4F:C1:E4:78:D1:B1:78:20:55:F6:84:92:51:76:78:F6:78:1E:78:AD:7C:EC:82:98:21:19:A5:2B:83:EB:11:1F:33:35:77:62:85:98:98:D7:
43:9F:30:FE:FC:BF:E9:F0:4F:C7:E7:B8:ED:78:23:39:91:5D:4E:5E:59:8E:E3:5A:1D:09:29:D8:B4:17:4E:15:20:35:E3:68:04:5B:27:FC:92:71:1E:F5:A2:D7:B7:30:CB:C8:38:21:21:BF:EB:78:
BC:DE:98:FB:78:E8:DA:77:57:02:11:4B:43:44:7B:AC:09:2B:FA:4B:27:4B:D7:48:AB:82:37:C5:92:20:5D:3F:5A:B6:01:50:93:32:08:EF:72:87:66:D9:C8:63:DA:95:EA:AB:74:52:38:93:B8:C
D:73:72:73:2D:13:90:B3:4B:70:FE:B1:C9:9C:83:A9:FC:CE:3B:D9:73:44:AD:EF:2C:D3:D6:80:38:52:33:41:07:C2:AA:0C:DC:F7:9D:A2:EF:E1:86:9F:D8:5E:5C:3E:17:67:73:FE:26:87:C9:
B3:E2:EC:DB:95:6E:DA:8A:FF:09:27:7C:6F:17:F1:CF:60:17:B1:14:86:AC:6F:CE:7D:A9:EB:BE:D6:3F:43:D3:94:36:10:E6:81:1F:0E:CC:FE:E3:76:2F:30:AC:E8:C6:A2:B1:32:91:80:A4:B8:3
A:ED:80:0B:66:40:F9:76:37:A8:89:E1:95:37:F2:19:C2:EF:AA:4D:D3:36:90:82:AB:BF:C9:38:B9:C1:DA:C5:ED:FD:55:FB:C4:94:60:25:8D:A8:3E:68:7B:EF:02:03:01:00:01
```

Basic Constraints *IsCA: true*

Subject Key Identifier *CF:8D:6A:94:4F:AB:4A:E4:3D:40:37:4D:D0:06:C7:A9:3B:59:60:D2*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AE:6B:A1:14:86:B5:17:CD:68:88:7F:55:86:68:49:67:DD:C9:EB:46:F6:7A:9D:BF:59:3E:31:D2:D2:4E:95:37*

X509SubjectName

Subject CN: *CA CICCP Clase 3*

Subject OU: *CICCP C.I.F. Q-2867009-I*

Subject O: *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

8.2.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Key Usage	[digitalSignature]	true
Key Usage	[nonRepudiation]	true
Key Usage	[keyEncipherment]	true
Key Usage	[dataEncipherment]	true
Key Usage	[keyAgreement]	false
Key Usage	[keyCertSign]	false
Key Usage	[crlSign]	false
Key Usage	[encipherOnly]	false
Key Usage	[decipherOnly]	false

8.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

8.2.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificate

Name [es] Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3

Service digital identities

X509SubjectName

Subject CN: CA CICCIP Clase 3

Subject OU: CICCIP C.I.F. Q-2867009-I

Subject O: CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos

Subject L: Madrid

Subject ST: Madrid

Subject C: ES

Subject E: pki@ciccp.es

X509SKI

X509 SK I z41qlE+rSuQ9QDdN0AbHqTtZYNI=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2015-03-19T23:00:00Z

8.2.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Key Usage	[digitalSignature]	true
Key Usage	[nonRepudiation]	true
Key Usage	[keyEncipherment]	true
Key Usage	[dataEncipherment]	true
Key Usage	[keyAgreement]	false
Key Usage	[keyCertSign]	false
Key Usage	[crlSign]	false

Key Usage [encipherOnly] false

Key Usage [decipherOnly] false

8.2.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificate*

Name [es] *Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3*

Service digital identities

X509SubjectName

Subject CN: *CA CICCPC Clase 3*

Subject OU: *CICCPC C.I.F. Q-2867009-I*

Subject O: *CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos*

Subject L: *Madrid*

Subject ST: *Madrid*

Subject C: *ES*

Subject E: *pki@ciccp.es*

X509SKI

X509 SK I *z41qlE+rSuQ9QDdN0AbHqTtZYNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2013-07-07T00:00:00Z*

8.2.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Key Usage	[digitalSignature]	true
Key Usage	[nonRepudiation]	true
Key Usage	[keyEncipherment]	true
Key Usage	[dataEncipherment]	true
Key Usage	[keyAgreement]	false
Key Usage	[keyCertSign]	false
Key Usage	[crlSign]	false
Key Usage	[encipherOnly]	false
Key Usage	[decipherOnly]	false

8.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificate

Name [es] Certificados Reconocidos emitidos por la CA CA CICCIP Clase 3

Service digital identities

X509SubjectName

Subject CN: CA CICCIP Clase 3

Subject OU: CICCIP C.I.F. Q-2867009-I

Subject O: CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos

Subject L: Madrid

Subject ST: Madrid

Subject C: *ES*

Subject E: *pki@ciccp.es*

X509SKI

X509 SK I *z41qlE+rSuQ9QDdN0AbHqTtZYNI=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2010-01-25T00:00:00Z*

9 - TSP: HEALTHSIGN, S.L.

TSP Name

Name [en] *HEALTHSIGN, S.L.*

Name [es] *HEALTHSIGN, S.L.*

TSP Trade Name

Name [en] *VATES-B17944554*

Name [en] *HEALTHSIGN, S.L.*

Name [es] *HEALTHSIGN, S.L.*

Name [en] *Col·legi Oficial de Infermeria de Lleida*

Name [es] *Col·legi Oficial de Infermeria de Lleida*

Name [en] *Col·legi Oficial de Infermeria de Girona*

Name [es] *Col·legi Oficial de Infermeria de Girona*

Name [en] *Col·legi Oficial de Infermeria de Tarragona*

Name [es] *Col·legi Oficial de Infermeria de Tarragona*

Name [en] *Col·legi Oficial de Metges de Lleida*

Name [es] *Col·legi Oficial de Metges de Lleida*

Name [en] *Col·legi Oficial de Metges de Girona*

Name [es] *Col·legi Oficial de Metges de Girona*

Name [en] *Col·legi Oficial de Metges de Tarragona*

Name [es] *Col·legi Oficial de Metges de Tarragona*

Name [en] *Col·legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Name [en] *Col·legi Oficial de Infermeria de Tarragona – CIF Q4366005I*

Name [en] *Col·legi Oficial de Metges de Lleida – CIF Q2566001J*

Name [en] *Col·legi Oficial de Infermeria de Girona – CIF Q1766003F*

Name [en] *Col·legi Oficial de Metges de Girona – CIF Q1766001J*

Name [en] *Col·legi Oficial de Metges de Tarragona – CIF Q4366001H*

PostalAddress

Street Address [en] *C/Albereda, 3-5, ático*

Locality [en] *Girona*

State Or Province [en] *Gerona*

Postal Code [en] *17004*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/Albereda, 3-5, ático*

Locality [es] *Girona*

State Or Province [es] *Gerona*

Postal Code [es] *17004*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:healthsign@healthsign.org*

URI [en] *http://www.healthsign.org*

TSP Information URI

URI [en] *http://www.healthsign.org/pub/eng*

URI [es] *http://www.healthsign.org*

9.1 - Service (withdrawn): Certificado de Colegiado Reconocido emitido por CA CODILL CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name [en] *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 458154954257264109682702

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: AC HEALTHSIGN

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: HEALTHSIGN SL - CIF B17944554

Issuer C: *ES*

Subject CN: CODILL CA

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject 0: *Col·legi Oficial de Infermeria de Lleida - CIF Q-2566003-F*

Subject C: ES

Valid from: Wed Jul 22 10:09:02 CEST 2009

Valid to: Mon Jul 22 10:19:02 CEST 2024

[illegible]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *B0:58:E7:04:D5:20:5E:84:D6:48:4B:1A:6D:D1:19:73:BD:52:EF:6C*

Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.28537.1.1</i> <i>CPS pointer: http://www.healthsign.org/repository/</i> <i>Policy OID: 2.5.29.32.0</i>
Authority Key Identifier	<i>0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79</i>
CRL Distribution Points	<i>http://www.healthsign.org/repository/hesica.crl</i>
Authority Info Access	<i>http://www.healthsign.org/repository/hesica.crt</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>C7:F6:82:27:03:47:4B:47:1C:14:4F:B8:B8:13:B3:9C:D9:69:53:7F:AD:59:5B:56:C8:06:B4:C5:3C:D1:A0:43</i>

X509SubjectName

Subject CN:	<i>CODILL CA</i>
Subject OU:	<i>Paer Casanovas 37 - altell 25008 - LLEIDA</i>
Subject O:	<i>Col-legi Oficial de Infermeria de Lleida - CIF Q-2566003-F</i>
Subject C:	<i>ES</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en]	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI [es]	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

9.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

9.1.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name *[en]* *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

X509SubjectName

Subject CN: *CODILL CA*

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject O: *Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Subject C: *ES*

X509SKI

X509 SK I *sFjnBNUGxOTWSEsabdEZc71S72w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2015-11-30T23:00:00Z*

9.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificado de Colegiado Reconocido emitido por CA CODILL CA*

Name *[en]* *Qualified Member Certificate issued by CA CODILL CA*

Service digital identities

X509SubjectName

Subject CN: *CODILL CA*

Subject OU: *Paer Casanovas 37 - altell 25008 - LLEIDA*

Subject O: *Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

Subject C: *ES*

Subject OU: *Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*
Subject O: *Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Subject C: *ES*
Valid from: *Thu Apr 26 13:07:08 CEST 2007*
Valid to: *Tue Apr 26 13:17:08 CEST 2022*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:6F:2E:58:FB:F7:62:6B:73:F2:7B:B9:DC:BB:22:AD:22:E7:6F:44:44:5A:8D:57:F4:77:24:07:CD:13:25:69:FD:9B:C4:46:D8:A1:C2:C7:DE:39:A9:10:6A:9E:91:AE:B3:EF:87:D7:FF:25:0E:C4:08:28:9C:8C:6F:4D:9D:5E:01:27:1E:AC:CA:3C:98:F8:23:ED:04:15:CE:F9:44:37:FA:56:BB:A5:43:A7:8C:1B:67:15:CA:2E:20:30:3A:1B:A2:A2:FD:48:3C:38:73:94:B1:C5:B6:CC:EF:05:2C:64:54:07:02:7F:03:5E:10:10:F1:E7:98:93:7E:F2:05:7D:2C:54:EC:91:A1:99:D6:4B:C0:92:54:31:8F:20:BD:8F:87:E8:91:26:08:49:07:81:9B:D9:2F:33:F5:3A:C8:E9:2D:86:04:CE:8E:C2:C5:B6:3B:C8:B9:44:40:B6:ED:14:66:C0:1B:82:74:4F:A3:9F:3A:7A:C8:AF:EC:C3:64:AF:0C:B4:14:CA:69:66:AF:E9:76:44:5D:14:EF:65:7D:C2:DB:B5:36:A4:AF:4B:C4:59:AA:1B:CE:B2:67:72:00:B6:B3:AF:EE:11:DE:55:2E:09:DB:B0:FF:F2:86:4C:D7:48:AC:8C:EF:F7:AE:43:C5:85:F6:2C:80:17:AA:8A:E3:B5:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *4B:7F:CC:2F:1E:1D:60:2A:E7:1D:49:2E:C2:74:7B:41:12:32:B1:44*
Certificate Policies *Policy OID: 1.3.6.1.4.1.28537.1.1*
CPS pointer: <http://www.healthsign.org/repository/>
Policy OID: 2.5.29.32.0
Authority Key Identifier *0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*
CRL Distribution Points *<http://www.healthsign.org/repository/hesica.crl>*
Authority Info Access *<http://www.healthsign.org/repository/hesica.crt>*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *F8:07:01:AE:DC:23:5D:23:71:03:C1:08:61:7D:94:46:5D:41:3C:40:37:17:0B:59:9E:AB:DD:64:8D:33:56:5E*

X509SubjectName

Subject CN: *CODITA CA*
Subject OU: *Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*
Subject O: *Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I*
Subject C: *ES*

Service Status

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI	[en]	https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

9.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

9.2.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified Member Certificate issued by CA CODITA CA
Name	[es]	Certificado de Colegiado Reconocido emitido por CA CODITA CA

Service digital identities**X509SubjectName**

Subject CN:	CODITA CA
Subject OU:	Avda. Pau Casals. 13-5e. 43003 - TARRAGONA
Subject O:	Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I
Subject C:	ES

X509SKI

X509 SK I	S3/MLx4dYCrnHUKuwnR7QRlysUQ=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2015-11-30T23:00:00Z

9.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified Member Certificate issued by CA CODITA CA
Name	[es]	Certificado de Colegiado Reconocido emitido por CA CODITA CA

Service digital identities**X509SubjectName**

Subject CN:	CODITA CA
Subject OU:	Avda. Pau Casals. 13-5e. 43003 - TARRAGONA
Subject O:	Col-legi Oficial de Infermeria de Tarragona – CIF Q4366005I
Subject C:	ES

X509SKI

X509 SK I	S3/MLx4dYCrnHUKuwnR7QRlysUQ=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2009-09-09T00:00:00Z

9.3 - Service (withdrawn): Qualified Member Certificate issued by CA COMLL CA

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Member Certificate issued by CA COMLL CA
Name	[es]	Certificado de Colegiado Reconocido emitido por CA COMLL CA

Service digital identities**Certificate fields details**

Version:	3
Serial Number:	86355775820241070718986

Thumbprint algorithm: *SHA-256*

Thumbprint: *80:D0:B3:C8:B8:C3:1C:D3:3E:36:0E:1A:DA:20:8A:37:12:EF:FE:09:1B:B2:84:40:52:A7:35:F7:B4:5C:CC:42*

X509SubjectName

Subject CN: *COMLL CA*

Subject OU: *Rambla Arago 14. pral. 25002 - LLEIDA*

Subject O: *Col-legi Oficial de Metges de Lleida - CIF Q2566001J*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

9.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.3.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Member Certificate issued by CA COMLL CA*

Name [es] *Certificado de Colegiado Reconocido emitido por CA COMLL CA*

Service digital identities

X509SubjectName

Subject CN: COMLL CA

Subject OU: Rambla Arago 14. pral. 25002 - LLEIDA

Subject O: Col-legi Oficial de Metges de Lleida – CIF Q2566001J

Subject C: ES

X509SKI

X509 SK I VNY3KgJCiR2H21XB3HXoW/8AmuE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2015-11-30T23:00:00Z

9.3.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Member Certificate issued by CA COMLL CA

Name [es] Certificado de Colegiado Reconocido emitido por CA COMLL CA

Service digital identities

X509SubjectName

Subject CN: COMLL CA

Subject OU: Rambla Arago 14. pral. 25002 - LLEIDA

Subject O: Col-legi Oficial de Metges de Lleida – CIF Q2566001J

Subject C: ES

X509SKI

X509 SK I VNY3KgJCiR2H21XB3HXoW/8AmuE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-09-09T00:00:00Z

9.4 - Service (withdrawn): Qualified Member Certificate issued by CA CODIGI CA

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:55:DC:C5:5B:D9:19:FA:B5:5C:7E:06:7A:BF:64:FC:EF:24:87:7D:3D:AB:88:4C:78:51:AC:89:03:75:88:39:AB:6E:4B:0A:29:27:3A:DA:AD:47:FD:86:C5:B9:C3:83:E7:CC:97:6F:00:E7:07:DB:C5:85:FC:CD:1D:E6:6C:70:DC:09:8D:3B:12:27:E2:99:89:45:29:14:8D:27:8B:22:CB:94:D9:68:EA:A1:05:13:88:E6:5C:94:49:42:2B:3D:16:C2:48:4E:88:9F:49:04:81:F3:5E:02:06:DA:06:5D:70:7E:A3:43:2F:02:D0:0E:2A:CE:5E:D5:59:54:5E:CB:5E:2F:70:8E:0E:73:A7:5C:6B:C5:FD:79:D4:71:50:9F:37:15:3F:AE:89:63:11:9A:44:16:88:04:56:94:5B:19:98:59:3D:A7:CA:E4:E2:0A:79:0C:63:D0:2E:85:F6:56:88:4F:C8:32:19:82:A3:4C:CD:0C:CB:6A:4F:11:EE:3C:2D:74:F4:2F:55:51:67:E7:29:CE:0A:AC:6D:B8:35:FB:3F:8D:62:F3:04:84:CE:73:C7:EF:34:20:8F:40:A5:9B:47:05:94:8E:DF:92:E0:36:E3:15:4B:D8:79:D1:C2:D7:B5:37:EC:52:65:E6:EE:29:7C:AD:D7:1E:37:A4:07:47:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

E6:81:F5:66:F5:F5:D7:9D:DB:BF:94:6B:99:6E:49:37:20:22:F1:54

Certificate Policies

Policy OID: 1.3.6.1.4.1.28537.1.1

CPS pointer: <http://www.healthsign.org/repository/>

Policy OID: 2.5.29.32.0

Authority Key Identifier

0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

CRL Distribution Points

<http://www.healthsign.org/repository/hesica.crl>

Authority Info Access

<http://www.healthsign.org/repository/hesica.crt>

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

E2:2F:28:CC:4C:F2:3F:D3:2B:9B:C1:93:04:A9:91:82:00:8A:BF:69:65:4D:CA:42:BA:65:CC:9B:FA:10:D9:D4

X509SubjectName**Subject CN:**

CODIGI CA

Subject OU:

Albereda. 3-5. 3a. 17004 - GIRONA

Subject O:

Col-legi Oficial de Infermeria de Girona - CIF Q1766003F

Subject C:

ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI**URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

9.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

9.4.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Member Certificate issued by CA CODIGI CA

Name	[es]	Certificado de Colegiado Reconocido emitido por CA CODIGI CA

Service digital identities**X509SubjectName**

Subject CN:	CODIGI CA

Subject OU:	Albereda. 3-5. 3a. 17004 - GIRONA

Subject O:	Col-legi Oficial de Infermeria de Girona – CIF Q1766003F

Subject C:	ES

X509SKI

X509 SK I	5oH1ZvX1153bv5RrmW5JNyAi8VQ=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time	2015-11-30T23:00:00Z

9.4.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Member Certificate issued by CA CODIGI CA

Name	[es]	Certificado de Colegiado Reconocido emitido por CA CODIGI CA

Service digital identities**X509SubjectName**

Subject CN: CODIGI CA

Subject OU: Albereda. 3-5. 3a. 17004 - GIRONA

Subject O: Col-legi Oficial de Infermeria de Girona - CIF Q1766003F

Subject C: ES

X509SKI

X509 SK I 5oH1ZvX1153bv5RrmW5JNyAi8VQ=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-09-09T00:00:00Z

9.5 - Service (withdrawn): Qualified Member Certificate issued by CA COMG CA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Member Certificate issued by CA COMG CA

Name [es] Certificado de Colegiado Reconocido emitido por CA COMG CA

Service digital identities

Certificate fields details

Version: 3

Serial Number: 458579612176927755862027

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIFDCCA/WgAwIBAgIKYRumjQAAAAACZANBgkqhkiG9w0BAQIADCBgTELMAKGA1UEBHMCRVMx
KDAmBgNVBAsMA0h0FQUUSFNR0dglU0wgd4oCTENjRkCMTCSNDQINTQMDAUBgNVBAStJ0F5YmVy
ZWRhIG51bS4gMy01LlBBdGJlIAxNzAwNCAiEjUk9OOTEWMBOGA1UEAxMNQUUMgSEVBTFRlU0IH
TJAeFw0wNzA0MjcwNzMDMTdaFw0yMjA0MjcwNzMDMTdaMIGNMQswCjYDVQOGEwIjFuzE/MDUQA1UE
Cgw2O29s1WwZ2xtZ2p22lhbCBKZSBNZ2RnZXNpZG9uZ29hbnR0dG9uZ29hbnR0dG9uZ29hbnR0dG9u
MSswQjYDVQOLEyBjBjIGJlcmVkaS5AaZlUUEF0aWwudE3MDA0IC0gR0IST05BMRAwDgYDVQOGEwdD
T01HIEBMBjBjIGJlcmVkaS5w0BAQEAQCAQ8AMIBGcgKCAQEArdDAJ0ZjBq7LLXkEi6OKH
wShuAJoyZHR0F1O2TxZ29u5n6R0VS70cb3ZqCR4yUBPeyMnx84CzXqmG2c7m3zmng9
VRfYTOY6kGLM62NngOPbHAN6H7wDcDc2vOxcgHw0MvY5+ajZwf3vZwtjPEZMBILFeuTGIPmP
1L5hDfTRVHVNUeOLH3VWFTcm0LgHhJLFPx7DW8wW5CwPQ7SHtk0mkmxSoiqKpVvU2fCZXWf
1b6UWWhysm+K0ILUCUDD0pGnU1BT1yOZ8U1Xa28ywc91UGrsU18K5DQCNKcXCRWw
JkY2p8Te45wIDAQAB04IBdzCCAXMwEgYDVR0TAQH/BAQwBgEB/wIBADAdBgNVHQ4EFgQUIGVEO
B9DrtdgBHZ2W7n0OFTLL+owCwYDVR0PBAQDAgGMBAGCcsGAQOBgcVAQODAgEAMFQCA1UdIARN
MScwQjYKwYBACB3n8A1A2MDDECCSGAQU1F5wBFRVodHRwOi8vd3d3LnhtbW0aHnZ24ub3Jn
L3JlIG92aXRvcnkYAYGBFUDIAAwGQYIKwYBBAGCNxQCBawecgBTAHUAUAYgBDAEEwHwYDVR0jBBgw
FoAUC26TY3lamDAKB+6s6974dNysKwQAYDVR0BDkwnZAI0dOgMYTvaHR0CDovL3d3y5oZWfS
dGhzaWduLm5yZy9yZ2Rwcz00b3J5L2hlcj01Sj51cmwwSwYIKwYBBQILHAQEPBAQMDGcCCSGAQU1F
BzCh9odHRwOi8vd3d3LnhtbW0aHnZ24ub3JnL3JlIG92aXRvcnkvaGVzWNLmNydDANBgk
kiG9w0BAQIUAQCAQEABo31Ga434wmzv0a25HmJ0ncAge4fSg1LKEVj42cV00BoL609TCZ
NpN7VR0YeyxZvH0SKXp7RtcZ++H+zl0nn0ic2A+J4vTC08PWLkaX9cag0PRscollgCX
mZcikkj6YKRpikgM5iVosDEQWR+ilPlRsyhgrUpwDIXR4XRF5HWYOPR0t9Y95g7Qsa0gI8Y
x+WIWSpluqhp7JOMp5q3i0ZK+4N2H/7P02PSUJN0XV0SGf8hnceztIvC7f0gEIRGNjzR0Jky
qUEZSKdVIB7sqMh134Gn3f6vGLG50SwVx8TU8zDTY3BtwMboiYKA==

```

-----END CERTIFICATE-----

Signature algorithm: SHA1withRSA

Issuer CN: AC HEALTHSIGN

Issuer OU: *Albereda num. 3-5. Atic. 17004 - GIRONA*

Issuer O: *HEALTHSIGN SL - CIF B17944554*

Issuer C: *ES*

Subject CN: *COMG CA*

Subject OU: *Albereda 3-5. Atic. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Metges de Girona - CIF Q1766001J*

Subject C: *ES*

Valid from: *Fri Apr 27 09:34:17 CEST 2007*

Valid to: *Wed Apr 27 09:44:17 CEST 2022*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:30:C0:25:FD:19:27:CA:BB:D4:BC:4A:84:48:BA:FC:E9:07:C2:24:A1:B8:09:49:A3:26:73:47:C2:10:17:5D:36:4F:FC:59:4E:0B:A8:E6:7E:91:8D:54:8B:D1:C0:60:DE:26:6A:71:1E:32:50:13:DE:BE:33:27:C4:1E:02:C5:95:EA:98:6D:9C:EE:6D:F3:9A:61:BD:55:11:72:7D:33:98:EA:41:88:33:AD:8D:9E:03:8F:6C:70:0D:E8:77:FB:CD:37:03:73:68:D0:5D:C8:07:C3:43:2D:57:2E:7E:6A:56:70:7F:7B:D9:C2:D2:4F:13:33:01:20:B7:C4:B9:31:A2:3C:F9:8F:D4:82:F9:84:31:53:45:51:D5:35:47:8E:2C:7D:D5:58:54:C2:98:42:E0:1C:72:4B:B4:FC:45:0D:6F:30:5A:C0:BF:C0:F4:3B:48:7B:65:93:49:AB:2A:65:D2:A2:2A:8A:3E:95:6E:D8:57:19:5D:F5:9F:2D:8E:94:E9:65:87:CA:C9:8E:90:6F:DF:53:97:02:50:35:74:FD:C2:0F:80:8C:67:53:74:F5:C8:E6:5D:F1:45:E5:6B:3F:32:C0:28:E0:D5:41:AB:82:ED:7C:29:DE:5D:CD:01:8D:5D:C5:C2:45:62:F0:26:B2:A5:61:9A:7C:B1:37:B8:E7:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *19:51:0E:6F:D0:EB:96:D8:1D:04:76:76:59:89:CE:39:F4:CB:D7:EA*

Certificate Policies *Policy OID: 1.3.6.1.4.1.28537.1.1*
CPS pointer: <http://www.healthsign.org/repository/>
Policy OID: 2.5.29.32.0

Authority Key Identifier *0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*

CRL Distribution Points *<http://www.healthsign.org/repository/hesica.crl>*

Authority Info Access *<http://www.healthsign.org/repository/hesica.crt>*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *98:1F:E6:9D:F6:31:4B:83:0B:F9:94:91:FF:81:29:AC:D7:C0:AA:30:53:59:4E:1C:31:07:56:15:3B:C8:E0:60*

X509SubjectName

Subject CN: *COMG CA*

Subject OU: *Albereda 3-5. Atic. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Metges de Girona - CIF Q1766001J*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

9.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.5.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Member Certificate issued by CA COMG CA*

Name *[es] Certificado de Colegiado Reconocido emitido por CA COMG CA*

Service digital identities

X509SubjectName

Subject CN: *COMG CA*

Subject OU: *Albereda 3-5. Atic. 17004 - GIRONA*

Subject O: *Col-legi Oficial de Metges de Girona - CIF Q1766001J*

Subject C: *ES*

X509SKI

X509 SK I *GVEOb9DrItgdBHZ2WYnOOFTL1+o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time 2015-11-30T23:00:00Z

9.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Member Certificate issued by CA COMG CA

Name [es] Certificado de Colegiado Reconocido emitido por CA COMG CA

Service digital identities

X509SubjectName

Subject CN: COMG CA

Subject OU: Albereda 3-5. Atic. 17004 - GIRONA

Subject O: Col-legi Oficial de Metges de Girona - CIF Q1766001J

Subject C: ES

X509SKI

X509 SK I GVEOb9DrItgdBHZZWYnOOFTL1+o=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-09-09T00:00:00Z

9.6 - Service (withdrawn): Qualified Member Certificate issued by CA COMT CA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Member Certificate issued by CA COMT CA

Name [es] Certificado de Colegiado Reconocido emitido por CA COMT CA

Service digital identities

CRL Distribution Points *http://www.healthsign.org/repository/hesica.crl*

Authority Info Access *http://www.healthsign.org/repository/hesica.crt*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FC:6F:34:24:8C:BB:7D:A5:73:06:E6:0C:4A:4F:92:4A:39:2D:7F:F6:FC:23:E6:04:27:08:3D:E7:72:7C:9E:A9*

X509SubjectName

Subject CN: *COMT CA*

Subject OU: *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

Subject O: *Col-legi Oficial de Metges de Tarragona - CIF Q4366001H*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

9.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.6.2 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Member Certificate issued by CA COMT CA*

Name [es] *Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities

X509SubjectName

Subject CN: *COMT CA*

Subject OU: *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

Subject O: *Col-legi Oficial de Metges de Tarragona - CIF Q4366001H*

Subject C: *ES*

X509SKI

X509 SK I *p2b1KSwPwwOQpZhyKZYFsEUMW5M=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>*

Status Starting Time *2015-11-30T23:00:00Z*

9.6.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service Name

Name [en] *Qualified Member Certificate issued by CA COMT CA*

Name [es] *Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities

X509SubjectName

Subject CN: *COMT CA*

Subject OU: *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

Subject O: *Col-legi Oficial de Metges de Tarragona - CIF Q4366001H*

Subject C: *ES*

X509SKI

X509 SK I *p2b1KSwPwwOQpZhyKZYFsEUMW5M=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time

2009-09-09T00:00:00Z

10 - TSP: Infraestructuras y Servicios de Telecomunicaciones y Certificación SA

TSP Name

Name	[en]	Infraestructuras y Servicios de Telecomunicaciones y Certificación SA
Name	[es]	Infraestructuras y Servicios de Telecomunicaciones y Certificación SA
Name	[ca]	Infraestructures i Serveis de Telecomunicacions i Certificació
Name	[en]	Instituto Valenciano de Finanzas

TSP Trade Name

Name	[en]	Agencia de Tecnología y Certificación Electrónica - ACCV
Name	[es]	Agencia de Tecnología y Certificación Electrónica - ACCV
Name	[en]	ACCV
Name	[es]	ACCV
Name	[en]	Generalitat Valenciana
Name	[es]	Generalitat Valenciana
Name	[en]	Institut Valencià de Finances - IVF
Name	[es]	Institut Valencià de Finances - IVF
Name	[en]	ISTEC
Name	[es]	ISTEC
Name	[en]	Instituto Valenciano de Finanzas
Name	[en]	VATES-A40573396

PostalAddress

Street Address	[en]	Pista de Ademuz S/N
Locality	[en]	Burjassot
State Or Province	[en]	Valencia
Postal Code	[en]	46100
Country Name	[en]	ES

PostalAddress

Street Address	[es]	<i>Pista de Ademuz S/N</i>
Locality	[es]	<i>Burjassot</i>
State Or Province	[es]	<i>Valencia</i>
Postal Code	[es]	<i>46100</i>
Country Name	[es]	<i>ES</i>

ElectronicAddress

URI	[en]	<i>mailto:accv@accv.es</i>
URI	[en]	<i>http://www.accv.es</i>

TSP Information URI

URI	[en]	<i>http://www.accv.es/quienes-somos/who-are-we</i>
URI	[es]	<i>http://www.accv.es</i>

10.1 - Service (withdrawn): Certificados Reconocidos emitidos por CA ACCV-CA2**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[es]	<i>Certificados Reconocidos emitidos por CA ACCV-CA2</i>
Name	[en]	<i>Qualified Certificates issued by ACCV-CA2</i>

Service digital identities**Certificate fields details**

Version:	<i>3</i>
Serial Number:	<i>1146754895</i>

Thumbprint algorithm: *SHA-256*

Thumbprint: *AF:2A:96:31:00:E0:AB:38:18:E0:AD:5A:D4:38:22:1D:0C:B1:E8:6C:65:5E:5E:5A:9D:D3:1C:87:57:56:43:2C*

X509SubjectName

Subject C: *ES*

Subject O: *Generalitat Valenciana*

Subject OU: *PKIGVA*

Subject CN: *ACCV-CA2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

10.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.16.2.0*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.17.2.0*

10.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

10.1.4 - History instance n.1 - Status: supervisionceased

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Reconocidos emitidos por CA ACCV-CA2

Name [en] Qualified Certificates issued by ACCV-CA2

Service digital identities

X509SubjectName

Subject C: ES

Subject O: Generalitat Valenciana

Subject OU: PKIGVA

Subject CN: ACCV-CA2

X509SKI

X509 SKI s3jtBaV5QTrC9MBSKP9jQz+/44E=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2016-05-01T00:00:00Z

10.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

10.1.4.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.8149.3.6.4.0
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.8149.3.6.5.0
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	Certificados Reconocidos emitidos por CA ACCV-CA2
Name	[en]	Qualified Certificates issued by ACCV-CA2

Service digital identities

X509SubjectName

Subject C:	ES
Subject O:	Generalitat Valenciana
Subject OU:	PKIGVA
Subject CN:	ACCV-CA2

X509SKI

X509 SK I	s3jtBaV5QTrC9MBSKP9jQz+/44E=

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-03-16T00:00:00Z*

10.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

10.1.5.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en]

it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

10.2 - Service (withdrawn): Qualified Certificates issued by CA GVA

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en]

Qualified Certificates issued by CA GVA

Name

[es]

Certificados Reconocidos emitidos por CA GVA

Service digital identities

Certificate fields details

Version:

3

Serial Number:

999621763

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer CN:

Root CA Generalitat Valenciana

Issuer OU:

PKIGVA

Issuer O:

Generalitat Valenciana

Issuer C:

ES

Subject CN:

CAGVA

Subject OU:

PKIGVA

Subject O:

Generalitat Valenciana

Subject C:

FS

Valid from:

Tue Sep 04 18:42:43 CEST 2001

Valid to:

Fri Sep 02 18:42:43 CEST 2011

Public Key:[illegible]

Basic Constraints	<i>IsCA: true - Path length: 0</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.8149.2.1.0</i> <i>CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana. La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de Certificación se encuentra en la dirección web http://www.pki.gva.es/cps]</i> <i>CPS pointer: http://www.pki.gva.es/cps</i>
Authority Info Access	<i>http://ocsp.pki.gva.es</i>
Authority Key Identifier	<i>7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC</i>
Subject Key Identifier	<i>71:4C:03:54:F2:72:6B:5C:8D:1E:71:D4:58:82:0D:D7:1F:57:B7:DD</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>9D:AE:71:05:BD:9A:45:07:D2:78:21:01:FD:23:19:10:88:3E:22:27:26:47:0E:2D:98:33:3B:68:7F:9A:4F:63</i>

X509SubjectName

Subject CN:	<i>CAGVA</i>
Subject OU:	<i>PKIGVA</i>
Subject O:	<i>Generalitat Valenciana</i>
Subject C:	<i>ES</i>

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time*2016-06-30T22:00:00Z***Scheme Service Definition URI**

URI	<i>[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI	<i>[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

10.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**10.2.2 - History instance n.1 - Status: supervisionceased****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified Certificates issued by CA GVA

Name

[es]

Certificados Reconocidos emitidos por CA GVA

Service digital identities**X509SubjectName****Subject CN:**

CAGVA

Subject OU:

PKIGVA

Subject O:

Generalitat Valenciana

Subject C:

ES

X509SKI**X509 SK I**

cUwDVPJya1yNHnHUWIIN1x9Xt90=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time**

2012-04-15T22:00:00Z

10.2.3 - History instance n.2 - Status: undersupervision**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified Certificates issued by CA GVA

Name

[es]

Certificados Reconocidos emitidos por CA GVA

Service digital identities**X509SubjectName****Subject CN:**

CAGVA

Issuer OU: *PKIGVA*
Issuer O: *Generalitat Valenciana*
Issuer C: *ES*
Subject C: *ES*
Subject O: *Generalitat Valenciana*
Subject OU: *PKIGVA*
Subject CN: *ACCV-CA1*
Valid from: *Thu May 04 14:26:56 CEST 2006*
Valid to: *Sun May 01 14:26:56 CEST 2016*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:07:0A:03:EF:D6:3D:0E:DC:02:87:AF:02:EC:CC:5F:F4:C1:7A:71:F5:65:8B:D9:38:69:B2:E8:80:6C:E2:4D:37:06:84:99:5E:08:28:2C:8D:86:6D:A2:85:6E:90:5F:E2:9F:F3:07:CF:0C:E1:04:88:AD:0A:79:9F:6D:41:24:1F:87:6A:9D:AB:81:2D:FF:26:E9:24:6E:CD:77:1A:8E:B2:2A:16:B2:BA:98:FF:C6:09:26:37:88:CF:8E:88:D5:34:6C:44:EF:C9:72:AB:D2:52:23:DC:AD:D8:7B:9B:C3:60:36:47:5D:74:21:82:99:2C:79:48:37:BA:53:75:CA:22:D7:34:85:F6:AA:5A:A2:8F:2E:BF:05:D7:0D:7B:46:65:57:9A:67:1D:A8:A2:85:8D:16:A4:F9:BB:43:4C:17:DC:88:DF:FF:D0:F0:11:45:31:75:5D:15:51:27:BB:28:02:FE:C9:EE:C8:F3:FB:69:D6:BF:EE:E5:90:30:98:E1:FC:89:84:3E:D6:3C:D1:1E:E6:D6:88:AB:18:E7:32:E9:8C:A9:28:FE:C0:E2:1D:4D:20:02:63:BA:04:01:99:0F:CC:C5:91:E1:4E:19:4F:D7:64:BB:43:DD:6E:87:BD:9F:2D:E5:7E:44:18:2C:91:14:59:E8:90:DF:85:CC:BA:71:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Certificate Policies *Policy OID: 1.3.6.1.4.1.8149.2.1.0*
CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana. La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de Certificación se encuentra en la dirección web http://www.pki.gva.es/cps]
CPS pointer: http://www.pki.gva.es/cps
Authority Key Identifier *7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC*
Subject Key Identifier *1B:90:85:EB:CC:C2:5D:36:64:9B:EA:C6:24:74:41:30:C9:CA:24:52*
Thumbprint algorithm: *SHA-256*
Thumbprint: *C7:D8:33:48:A3:0A:A6:7A:79:C7:20:38:D1:EF:E5:33:18:89:E6:4D:A1:47:E2:7A:1D:8F:FE:47:AE:8C:BE:29*
X509SubjectName
Subject C: *ES*
Subject O: *Generalitat Valenciana*
Subject OU: *PKIGVA*
Subject CN: *ACCV-CA1*
Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Service status description *[en] undefined.*

[es] undefined.

Status Starting Time 2016-06-30T22:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

10.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

10.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

10.3.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by ACCV-CA1

Name [es] Certificados Reconocidos emitidos por ACCV-CA1

Service digital identities

X509SubjectName

Subject C: ES

Subject O: Generalitat Valenciana

Subject OU: PKIGVA

Subject CN: ACCV-CA1

X509SKI

X509 SKI G5CF68zCXTZkm+rGJHRBMMnKJFI=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2016-05-01T00:00:00Z

10.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

10.3.3.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

10.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by ACCV-CA1

Name [es] Certificados Reconocidos emitidos por ACCV-CA1

Service digital identities

X509SubjectName

Subject C: ES

Subject O: Generalitat Valenciana

Subject OU: PKIGVA

Subject CN: ACCV-CA1

X509SKI

X509 SK I G5CF68zCXTZkm+rGJHRBMMnKJFI=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2007-03-16T00:00:00Z

10.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

10.3.4.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Subject C: *ES*
Subject O: *ACCV*
Subject OU: *PKIACCV*
Subject CN: *ACCVCA-110*
Valid from: *Thu Oct 13 13:22:04 CEST 2011*
Valid to: *Fri Jan 01 00:59:00 CET 2027*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A0:75:4B:CB:2F:A6:88:2D:BD:BF:FB:10:65:F8:D0:2C:89:2B:DE:01:07:23:57
:00:EC:4B:F4:98:99:0E:8F:1E:63:92:99:38:C6:9E:CD:6D:13:83:FC:43:39:55:5C:59:56:2F:A6:A3:C5:AD:92:97:3C:43:3A:E0:98:85:D0:35:A2:74:21:A2:38:2C:2F:1F:E1:8A:22:C7:49:88:3
4:3D:33:0A:72:06:37:18:62:D7:99:CF:E0:78:AA:67:B9:3D:BB:E6:24:CA:52:F9:31:7E:55:35:B5:A5:FD:38:0C:8F:15:07:CD:A3:91:60:A3:DB:48:C4:65:01:04:9D:D5:BE:CE:53:43:CD:6B:8
A:7E:5A:81:76:5E:A6:D4:CC:C7:51:D2:AC:34:DE:08:32:06:F8:D1:5E:04:C5:90:82:A2:8F:31:C3:03:97:1E:98:37:F1:75:93:4F:EE:DE:88:3B:1B:B4:27:12:83:22:A8:2F:30:51:FC:F0:5A:9D:
78:97:7C:B9:85:56:A4:1A:68:84:89:59:D0:68:78:AF:72:8D:6F:A8:CD:CE:E5:40:B5:69:64:97:87:01:CB:0D:67:E7:09:8C:4A:0C:4F:C5:7E:81:B5:0A:C5:52:8B:E2:96:88:1D:CC:37:3F:F1:B
E:08:06:A1:73:20:D8:D7:FC:FF:67:12:B2:5D:77:86:90:B2:7E:B6:B8:4A:26:67:C3:D4:C2:74:3A:C6:19:0C:4A:A1:63:28:3A:AA:29:42:A3:97:90:AF:F8:F4:28:04:0E:B4:58:02:21:82:8C:64:
C0:2D:48:62:2E:55:D2:E7:22:00:56:A6:B3:C6:09:88:75:34:FD:93:6D:B5:1E:20:F8:95:25:3E:39:FB:55:BA:22:F0:E8:B9:60:AC:B1:7A:7B:50:FA:40:D1:37:A8:02:41:CF:0E:CA:CC:7C:34:9
D:30:66:7C:AD:F0:C1:73:8F:FE:0E:97:3B:0E:DE:F8:D2:97:C4:04:93:D1:74:40:5F:7E:DE:27:26:17:3E:9D:04:B6:10:82:C6:43:0F:22:86:F0:39:09:6C:88:F0:84:37:AF:07:44:B6:42:B6:9B:
33:7B:31:C8:A0:48:98:6E:EB:34:C9:8B:67:2C:69:BD:7F:6F:3D:7C:F5:78:68:31:84:9F:E9:4C:26:4C:05:ED:BF:CA:01:51:2E:3A:07:10:98:64:48:90:A2:A2:80:85:96:E5:1C:72:D6:25:3E:A
D:4F:BA:0C:15:78:8C:E9:65:93:95:66:FC:0F:57:44:8A:02:55:7E:4D:D7:6F:65:55:B4:8C:5E:F3:88:C1:28:54:9A:56:F7:3E:C1:88:3D:C6:BA:6C:59:49:C9:02:03:01:00:01

```

Authority Info Access *http://ocsp.accv.es*
Subject Key Identifier *92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E*
Basic Constraints *isCA: true*
Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]
CPS pointer: http://www.accv.es/legislacion_c.htm
CRL Distribution Points *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *13:45:C2:D3:9A:E4:B6:5C:CA:71:E8:8E:9A:2B:29:C7:1D:C9:13:F9:52:E9:35:A8:12:B0:04:DB:A7:AE:79:57*

Certificate fields details

Version: *3*
Serial Number: *3707946637220933198*

Certificate Policies*Policy OID: 2.5.29.32.0**CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en <http://www.accv.es>]**CPS pointer: http://www.accv.es/legislacion_c.htm***CRL Distribution Points***http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl***Subject Alternative Name***accv@accv.es***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11***X509SubjectName****Subject C:***ES***Subject O:***ACCV***Subject OU:***PKIACCV***Subject CN:***ACCVCA-110***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2024-11-08T02:00:00Z***Scheme Service Definition URI****URI**

[en]

*<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI**

[es]

*<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***10.4.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description** [en]*undefined.*

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[OIDsURN]

urn:oid:1.3.6.1.4.1.8149.3.10.2.0

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.8149.3.22.1.0

10.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

10.4.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by ACCVCA-110

Name [es] Certificados Reconocidos emitidos por ACCVCA-110

Service digital identities**X509SubjectName**

Subject C: ES

Subject O: ACCV

Subject OU: PKIACCV

Subject CN: ACCVCA-110

X509SKI

X509 SK I kIKuRm1bvb6FwbNhR6j/t9mTwA4=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2018-01-16T01:00:00Z

10.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

10.4.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.4.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by ACCVCA-110*

Name [es] *Certificados Reconocidos emitidos por ACCVCA-110*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-110*

X509SKI

X509 SK I *kIKuRm1bvb6FwbNhR6j/t9mTwA4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

10.4.4.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.8149.3.10.2.0

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.8149.3.22.1.0

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.8149.3.10.3.0

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.8149.3.22.2.0

10.4.4.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

10.4.5 - History instance n.3 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by ACCVCA-110

Name	[es]	Certificados Reconocidos emitidos por ACCVCA-110

Service digital identities**X509SubjectName**

Subject C:	ES

Subject O:	ACCV

Subject OU:	PKIACCV

Subject CN:	ACCVCA-110

X509SKI

X509 SK I

kIKuRm1bvb6FwbNhR6j/t9mTwA4=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2012-04-15T22:00:00Z

10.4.5.5 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.10.2.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.22.1.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.10.3.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.22.2.0

10.4.5.6 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in "Service digital identity" and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Issuer CN: ACCVRAIZ1
Subject C: ES
Subject O: ACCV
Subject OU: PKIACCV
Subject CN: ACCVCA-120
Valid from: Thu Oct 13 16:55:04 CEST 2011
Valid to: Fri Jan 01 00:59:00 CET 2027
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9B:06:23:17:1E:D2:66:66:AB:2E:3D:3E:EC:3A:9D:26:7E:AA:87:91:30:3E:98:
17:C6:71:33:CC:57:CE:49:04:02:9B:AC:A5:82:50:01:8D:54:C4:CE:79:7D:08:99:8F:C9:D3:4D:C6:08:15:18:A3:40:FA:13:4C:14:26:40:15:2E:4F:EA:72:7C:6D:9E:12:65:82:08:A5:9E:9E:8
1:4A:17:0D:5F:FE:23:2D:05:81:6E:EC:24:B3:CF:87:7D:B7:D8:EB:5E:BF:14:A2:C0:61:3C:8A:98:C9:05:56:55:3F:EA:98:30:51:29:79:D9:08:44:8D:87:CC:5D:17:56:89:92:F5:87:D6:38:32:
BB:CA:1D:BE:77:80:AA:3C:27:D7:D5:6D:1A:19:E0:4A:D8:58:24:00:15:C4:5D:E4:60:64:3A:F5:53:99:26:2D:16:40:A0:6E:4D:64:1E:97:3D:C5:5D:B9:D0:6F:95:ED:F3:38:69:C5:3E:56:1E:
0C:CB:11:48:E0:45:C1:04:74:2F:8B:5C:11:9D:50:43:68:BF:8A:1A:B7:51:F2:46:7A:C5:AD:82:19:FF:FF:FB:10:0C:2F:0A:ED:35:FD:C2:19:51:93:0E:90:C7:95:7C:4D:C3:89:C5:03:49:68:1
0:50:9E:C3:41:C3:8D:53:05:7E:2C:82:5C:33:17:9D:30:7C:0D:97:9F:43:D2:E0:68:53:D2:68:3F:8A:37:AA:22:1D:59:3F:B7:81:29:CE:29:B0:C3:49:66:DC:E1:8D:D5:02:78:AF:96:6D:94:43
:A8:AE:FC:1A:FF:4A:F7:DE:68:C4:51:03:99:1F:4A:C9:BE:63:0C:78:06:57:CA:91:76:2B:A9:E6:0D:22:6A:73:12:83:68:94:E5:1C:46:CE:3B:DD:19:42:C3:80:09:AF:27:F7:C1:88:23:2F:D7:9
A:CB:83:3F:1C:E3:36:31:34:36:CD:1D:17:C4:4F:44:E5:C4:46:6D:2C:AD:70:18:BD:E5:AD:78:17:00:05:CB:15:64:90:CD:3C:39:12:00:70:B9:ED:96:31:90:C8:96:F8:68:C7:5E:48:79:7E:4
6:ED:07:2B:2A:B4:12:F0:30:9D:5A:11:A5:84:35:15:24:E7:01:92:42:C9:86:54:63:2A:2B:66:62:24:C8:A1:18:85:69:1B:78:48:8F:88:FB:4D:38:AC:79:5C:6E:BF:44:73:BE:87:6D:29:81:62:
C9:AE:21:FA:E4:F2:74:8F:0C:69:EF:D0:B3:A8:AC:C8:5A:5D:D7:27:E9:CE:51:66:91:F4:D3:C9:6F:E9:F3:79:C2:92:DE:12:44:2E:CC:68:C0:4C:B4:C5:6E:8F:02:03:01:00:01

```

Authority Info Access <http://ocsp.accv.es>
Subject Key Identifier E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5
Basic Constraints *IsCA: true*
Authority Key Identifier D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]
CPS pointer: http://www.accv.es/legislacion_c.htm
CRL Distribution Points http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl
Subject Alternative Name accv@accv.es
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 3B:C5:18:56:04:0A:D7:FF:66:83:AA:85:A0:D3:4F:9E:A6:80:CD:23:C3:7C:B8:A0:42:3B:0F:89:A2:44:05:B9

Certificate fields details

Version: 3
Serial Number: 4753158885672534199

Certificate Policies*Policy OID: 2.5.29.32.0**CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en <http://www.accv.es>]**CPS pointer: http://www.accv.es/legislacion_c.htm***CRL Distribution Points***http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl***Subject Alternative Name***accv@accv.es***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2***X509SubjectName****Subject C:***ES***Subject O:***ACCV***Subject OU:***PKIACCV***Subject CN:***ACCVCA-120***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2026-01-22T02:00:00Z***Scheme Service Definition URI****URI**

[en]

*<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI**

[es]

*<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***10.5.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description** [en]*undefined.*

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[OIDsURN]

urn:oid:1.3.6.1.4.1.8149.3.16.3.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.14.3.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.15.3.0

10.5.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.5.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.6.0

10.5.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

10.5.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by ACCVCA-120

Name [es] *Certificados Reconocidos emitidos por ACCVCA-120*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-120*

X509SKI

X509 SK I *6ECbjvtmP8FE2KHf1EqBQggXy+U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-01-16T01:00:00Z*

10.5.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.8149.3.16.3.0*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.8149.3.17.3.0*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.8149.3.14.3.0*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.8149.3.15.3.0*

10.5.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	<i>[en]</i>	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	<i>[es]</i>	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.8149.3.7.5.0*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.8149.3.6.6.0*

10.5.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.5.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.5.4.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

10.5.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ACCVCA-120*

Name *[es]* *Certificados Reconocidos emitidos por ACCVCA-120*

Service digital identities**X509SubjectName**

Subject C: ES

Subject O: ACCV

Subject OU: PKIACCV

Subject CN: ACCVCA-120

X509SKI

X509 SK I 6ECbjvtmP8FE2KHf1EqBQggXy+U=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

10.5.5.6 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.16.3.0

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

10.5.5.7 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.5.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.6.0

10.5.5.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

10.5.6 - History instance n.3 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by ACCVCA-120

Name [es] Certificados Reconocidos emitidos por ACCVCA-120

Service digital identities

X509SubjectName

Subject C: ES

Subject O: ACCV

Subject OU: PKIACCV

Subject CN: ACCVCA-120

X509SKI

X509 SK I 6ECbjvtmP8FE2KHf1EqBQggXy+U=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2012-04-15T22:00:00Z

10.5.6.9 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.16.3.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

10.5.6.10 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en]

it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.7.5.0

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.8149.3.6.6.0

10.6 - Service (withdrawn): Qualified Certificate issued by ACCVCA-130

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificate issued by ACCVCA-130

Name [es] ACCVCA-130

Service digital identities

Certificate fields details

Version:

3

Serial Number:

6022689390316330646

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIHkKCCBgAgwIBAgIIU5TkF0ZRnpYwDOYKozIhvcNAQELBQAwQIESMBAGA1UEAwwJQUINDVJB
SVoxMRAwGgYDVQQLDAAQ0S0IBQNDWMW0wYwYDVQQDAQBARQNDWMW0wYwYDVQGEwIFU2Aefw0xNTAx
MTUxMDIzMjRfAw0YJjE5MzEyMzU0MDBAZMEMxZARBgNVBAMMCKFDQ1ZDQ0S0xMzAxZEA0BQNVBAsM
I1BL5UFDO1YxDTALBqNVB4oMBEFDQ1YxZzAjbG9NVBAYTAKVIMiCjANBgkqhkiG9w0BAQoFAAOC
AgBAMiCCkCAgeAo5Kruh7jPEBxpdCBPFS0NBvPFR9B0CWZynbjLBxv6MTjAhehTqL1X90ECEQ
pWapNpygo6fNg8fMGYWhCsP5DvEmq5Um1xBnLjH8jMSiP7VCIMV59KdVu+nF8PpZno8hecsf
F4ylZLpMDIwiskh5Zp9e6cVBJsskRjDY4gWITWRYODe1ZQ5mu+2+YkvZ2RpOPo6k4eGlsFG
29jZ2VilhasDf4ZLv19F515DNXFFYmnnjMfTfLkuaIB7jBdGgRn5YhmGuNsP05gH5DF5YK
Lqg6A83KmyqslgYzN7ZYWfYnzB6ZzF0HPM9GX3PuSKKXyFpUxYL0nHWH7B3Se4F5m+mmFk9GM
vJvuUvkt0O2ysFPE3pytI1jIjrvGBK5cmZHKQbqBw52ooSEJNbmvtzshUxVEFTDRq+BavleaZFN
v5hSh5Q4c7Yv5nu80AMHjp06bwA+7B591eIdOdoMuedhyvE3lGqYku25a3uIK9j0z+qg1
0hZH5eNrexjWV20DIF6kgZqo6CZp0zm5eTfbaZ16oVZrpmTeG95datQzghDqXP684el67G275IQ
Nok2Wu5wT9oKAM6xomNp6zsr0Uy9KOBqMP8BTPIB98rwp9xmQH4Ss/r1zZK3xt+mYypB01QR5V
vKEEs1bnV3LjMCAwEAAQCAoKwggKMFCCGCCSGAAUfBwEBBCMwIFABg9yBgEFBQcwAYTtaHR0
CDoVLT9jc3AuYWNjdj51c2AzdG9NVHQ4EFgQU55f9DF3YMFtV4Yt+1YDI6fxblwDwYDR0TAQH/
BAUwAwEB/zAFBgNVHSMEDGDAWgBTSh7Tj3zcnk1X2VuqB5TbMB4N/TCCAxBGA1UdIASCAxYwggFy
MIIB9yEVR0uADCCAWQwwEuBg9BgEFBQcCAiCASAaggEAEAAQ0B0AGBACgBpACQAY0BKACAA
ZABIACAQwBIAHIAgABpAglYABGjAGEAYWpAPMAbAgAqAEABgB0AGUAq9BtACIAZABpAGEAIBK
AGUAIABsAGEAIBBAEMAQwBWAACAABABAgcAZ0BuAGMAAQ0BACAAZABIACAAABAIAgMBgBvAGwA
bwb8ACQAY0AGUAAB0AGUAq9B0AGUAZ0BAGAY0BAGABWBUACAAARQBSAGUAYWBoAHIAHwBu
AGKAYWBAcWAlIABDAEAKAgAgAFEAIAAA2ADAAMQAxADUANgBFACkALgAgAEMAUABTACAAZ0BuACAA
aAB0AHQAcAAAGAC8ALwB3AHcadwAuAGEAYWBJAHYALgBIAHMMWMayIKwYBBQUHAgEwJGh0dHA6Ly93
d3cuYWVudj51c2AzdG9cZm91c2Zpdm91cnR0B9NVHRBETjBMMEqS8KbRodfRw0bvd3d3
LmFiY3Y3YXZMvZm5szWfKbWUldFyY2hpd9m9ZLNicnRpmjYWRvcy9yYWI6YWNjdjFfZG9yLmN5
dAA0BgNVH0BBAfEBAMCAQYwFwYDVRORBBAwDoEMYYWJdkbhy2N2LmVMA0GCCSgSlb3DQEBcWUA
A4ICAQAs1+0b+uvsV35X0zHeesc2RlZiGz8yRiGpZTzBt94fAw6bTyWELZHHKw+DxIz
j4EvgI+U8Cbbwm9CVGUNA5e0l1byyWjgd/y2V8gGX+zmTX8mowih1zPIN6Zsodc2abCNXjilRL
WeGKnOlizYj+Jxtv6bWu7229ZUr2+vSSb0wJASUaEn1zn+OkqzKvTBk408xcgB5CqRj9XZFWS
oHx+w0pZuZuZxYrm4FLXbp+1HczE1wKrb8bBOMNMCPDFIH8fKvOrjKpsV8bvrvc01D9
lwIcP9YVY4Rsq4Qesuspshyr1HyLr+IoyqsdKLjUQo67o7ITWHh04mW5wz0KREn/siqR+chyZ2
RpIO7Hgw647fBYuIWxdQavqDKMehJLKjVosYwK4X9fjnP+5+wFSAM+0zINDbezBAIMlp0s5DV
9KQz9T9EPxTl60uWmjrBtp6PRvuvr++ivsZGLWj58pKsseKqfUJ52s2B84L10+UjMO+q
LWVohAyGyNkyv5eVS3Lrn3NzgVb5QZfHs14lcpHUPayMW1YkN0l+egCXVgTNVFGJup4Tjel
2gw1Yi4Z7FadKT9c9JZSuYN4Zb+qtM8ysaB1bg7UfU+dArY8nfXuHeo4MhiF6cx7HxobOy2p7r
ligccw==

```

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer C:

ES

Issuer O:

ACCV

Issuer OU:

PKIACCV

Issuer CN:

ACCVRAIZ1

Subject C:

ES

Subject O:

ACCV

Subject OU:

PKIACCV

Subject CN:

ACCVCA-130

Valid from:

Thu Jan 15 11:23:24 CET 2015

Valid to:

Fri Jan 01 00:59:00 CET 2027

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A3:92:89:AE:E8:78:24:F1:01:C6:97:42:F0:F7:F7:A8:DF:2F:7C:F4:7D:F1:00:
96:67:29:D8:8C:00:57:8F:A3:13:8F:00:22:7A:14:EA:D5:7F:0E:CC:44:0D:AE:A5:AA:A4:DA:72:82:8E:BF:6D:D8:1F:F0:53:20:61:68:42:80:F4:83:8C:49:A0:E5:49:85:C4:10:CB:8C:70:49:3
1:22:0F:ED:50:A5:31:54:BD:2A:27:55:BB:E9:C5:F0:FA:59:9E:8F:21:79:CB:1F:17:8C:89:CC:BA:7F:30:3F:E5:C0:8B:23:92:1E:59:A7:D7:BA:71:50:49:81:29:11:24:36:38:81:69:53:59:16:0
E:FF:47:B5:65:04:AB:BB:ED:BE:60:AC:86:65:1A:4E:3E:8E:A4:E1:E1:A5:22:C1:46:CF:DC:88:CD:58:A2:D2:16:AC:0D:FE:37:2E:FD:7D:17:9D:79:B4:D1:97:14:86:26:36:72:E3:30:59:5F:FC
:B2:AE:02:5F:3B:D0:89:46:A9:19:F9:CA:13:06:B8:93:6C:3F:4E:6D:1F:9D:FE:17:96:24:2E:A8:3A:03:CD:CA:9B:28:2C:22:CB:18:CC:DE:FE:61:68:85:00:DC:C1:E9:9C:CS:D0:73:CC:F4:85:F
7:3E:E4:A4:28:A5:F2:16:95:31:60:BD:27:1D:61:FB:07:74:9E:E0:5E:66:FA:69:85:93:D1:8C:BC:95:6E:A1:4B:E4:B4:E3:86:CA:C1:4F:13:7A:58:B6:5D:62:26:3A:D5:18:19:39:72:66:47:29:
06:FA:07:0E:59:A2:84:84:24:D6:E6:BE:DC:EC:85:4C:55:10:54:C3:46:0F:BC:6A:F9:5E:69:91:4D:BE:5E:61:8A:54:90:E1:CE:D8:96:F4:A7:BB:CD:00:31:F8:49:FE:90:FA:6F:00:3E:EC:11:B
D:05:E9:50:75:CA:0C:80:F7:47:CA:F1:37:94:64:9B:C6:68:76:E5:AD:EE:FF:F2:8D:EE:3A:33:FA:AA:85:D2:16:47:E5:E3:6B:13:18:D6:57:6D:03:94:5E:A4:81:9A:A8:E8:2F:F6:A7:4C:E6:E5:
E4:DF:6D:A6:75:EA:85:59:AE:99:93:78:6F:79:75:A6:D0:CE:01:C3:75:73:FA:07:87:A5:EB:81:B6:EF:98:D0:36:89:36:5A:EE:70:4F:DA:0A:00:CE:B1:A2:63:69:EB:3B:2B:D2:E6:08:F6:44:0
1:A8:3C:FC:05:33:E5:88:17:FC:AF:08:3D:C6:64:07:E1:2B:3F:AF:5C:D9:2B:7C:6D:FA:66:32:A4:1A:35:39:1E:55:BC:A1:04:AA:CD:58:9D:57:F7:2E:33:02:03:01:00:01

```

Authority Info Access

http://ocsp.accv.es

Subject Key Identifier

E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2

Basic Constraints

IsCA: true

Authority Key Identifier *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]
CPS pointer: http://www.accv.es/legislacion_c.htm

CRL Distribution Points *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl*

Subject Alternative Name *accv@accv.es*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *57:2B:F8:99:FD:77:43:62:DC:19:21:96:25:EC:C1:57:BB:55:43:4E:A5:16:6D:57:58:DC:4B:4F:89:0D:66:53*

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2026-01-22T02:00:00Z***Scheme Service Definition URI**

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

10.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.6.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate issued by ACCVCA-130*

Name *[es]* *ACCVCA-130*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

X509SKI

X509 SK I *5Sf9DFi3YMFTV4Yt+1YDi/6fxbl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

10.6.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.6.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificate issued by ACCVCA-130*

Name *[es]* *ACCVCA-130*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *ACCV*

Subject OU: *PKIACCV*

Subject CN: *ACCVCA-130*

X509SKI

X509 SK I *55f9DFi3YMFTV4Yt+1YDi/6fxbl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-23T22:00:00Z*

10.7 - Service (granted): Qualified timestamps issued by 'TSA1 ACCV 2016'

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by 'TSA1 ACCV 2016'*

Name *[es]* *Sellos cualificados de tiempo emitidos por 'TSA1 ACCV 2016'*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *969592673683204365*

Certificate Policies*Policy OID: 1.3.6.1.4.1.8149.3.100.2.0**CPS text: [Servidor de Sellado de Tiempo de la Agencia de Tecnología y Certificación Electrónica IVF (Pl. de Napoles y Sicilia 6, CP 46003 CIF Q9650010C). CPS y CP en <http://www.accv.es>]**CPS pointer: http://www.accv.es/legislacion_c.htm***CRL Distribution Points***http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl***Extended Key Usage***id_kp_timeStamping***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***2C:8D:42:33:F9:BC:80:93:4E:46:6F:0C:9F:76:41:1F:65:A5:C1:78:98:30:16:0B:66:68:59:EF:93:DE:25:66***X509SubjectName****Subject C:***ES***Subject ST:***Valencia***Subject L:***Valencia***Subject O:***Agencia de Tecnología y Certificación Electrónica - ACCV***Subject OU:***PKIACCV***Subject CN:***TSA1 ACCV 2016***X509SKI****X509 SK I***xsTYQMhIj2dS1HD+k7VDIRilZQ=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2019-12-23T02:00:00Z***Scheme Service Definition URI****URI***[en]**<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI***[es]**<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

Valid from: *Tue Jul 25 14:09:25 CEST 2023*

Valid to: *Fri Jul 19 14:09:24 CEST 2047*

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BC:E7:A1:A4:E5:99:5C:CF:72:BD:73:9F:64:1B:C4:08:F0:66:2D:56:FF:73:5A:
78:1E:58:98:F4:C2:08:81:02:50:A1:77:5D:00:32:3F:08:CF:73:12:93:C8:88:1E:0A:5E:73:59:9F:87:61:83:7E:46:25:CC:4F:84:A0:D4:C9:84:F7:C3:E5:1D:A3:8A:8F:93:18:70:F8:E5:87:83:
BB:FB:C2:8C:20:D8:FF:F9:6C:A4:E8:28:62:24:6C:D2:64:E4:21:C5:53:1E:5F:6C:01:15:90:2B:C5:16:5D:AD:46:DA:6B:9F:57:02:E4:08:EA:72:46:2D:01:DC:C2:17:07:36:0F:6E:7F:7E:57:6
7:98:16:11:55:CF:BC:F6:7D:FD:E9:68:3D:DB:5D:DD:5C:4D:B2:3C:ED:CA:2B:38:BE:89:1A:07:6F:6B:E5:DC:9E:44:11:51:E4:22:C5:DE:63:59:59:85:C5:B4:AC:A2:2C:E6:69:7D:01:E2:52:8
4:E7:0F:A6:D8:A5:9A:8E:37:6D:82:1E:B1:E2:34:E7:70:8F:A9:C5:88:BE:F7:6F:20:58:06:88:53:0F:E1:57:58:CD:A5:0E:DC:AE:D9:5A:8D:1C:FA:67:C4:46:C7:83:F8:EE:C2:29:1F:DF:3D:37:
A6:74:98:57:A9:BB:DD:39:31:8D:67:0C:4C:C3:D3:68:58:04:EC:34:A6:C2:89:1F:CD:1D:DD:3F:75:5D:BA:C7:D6:D1:E1:D0:BB:7F:9F:92:AD:D2:1A:48:3D:E0:77:28:59:9A:15:F8:91:C5:45
:47:D2:91:45:2F:A4:69:55:F0:43:9D:6F:11:6B:4E:56:1F:B3:43:6F:6D:6E:9D:34:2E:84:95:7E:42:6D:17:87:64:C2:D2:1F:A0:F7:C3:33:FE:E2:FA:97:54:08:81:43:69:FF:BD:5F:EF:9E:6B:5E:
E5:82:85:43:78:E5:22:EC:7D:01:84:88:83:42:34:62:CC:A2:FC:8F:A6:DE:65:74:E2:99:54:24:56:C3:12:95:24:88:02:86:80:47:DA:DB:BB:13:55:54:68:A3:DC:5A:A0:87:EF:F1:FC:16:00:
2:A9:68:00:85:FD:B9:CA:27:8E:06:96:B4:1A:14:85:3D:88:10:C6:20:51:C9:49:F1:50:9F:35:54:1D:91:E0:41:46:33:56:98:33:1C:96:BF:75:F2:16:54:6B:80:40:C8:1F:C9:FF:6C:FE:13:F4:F
B:27:DA:A0:8D:8A:85:16:51:A7:4A:2D:D2:98:70:14:7A:A0:09:C5:60:7D:34:E5:58:67:7C:8A:22:87:1C:86:E8:92:FB:78:BF:9A:88:47:9E:B9:18:78:51:02:03:01:00:01

```

Basic Constraints *IsCA: true*

Authority Key Identifier *19:5A:13:3A:A1:9D:27:F7:A6:38:49:7B:54:59:5A:6E:A6:6A:A4:BB*

Authority Info Access
http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt
<http://ocsp.accv.es>

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points
http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl
CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES

Subject Key Identifier *0D:F8:F0:62:B7:5F:36:D3:39:85:FC:67:E0:D3:C1:9E:19:98:B3:53*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A6:6B:48:56:45:A5:D6:6A:57:14:A3:60:E0:2D:DF:3A:B7:18:75:E7:7D:B1:98:BA:32:1A:8F:62:FF:01:D7:E1*

X509SubjectName

Subject CN: *ACCV RSA1 CLIENTE*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *DfjwYrdfNtM5hfxn4NPBnhmYs1M=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

10.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.9 - Service (granted): Certificados cualificados emitidos por ACCV RSA1 PROFESIONALES

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados cualificados emitidos por ACCV RSA1 PROFESIONALES*

Name [en] *Qualified Certificates issued by ACCV RSA1 PROFESIONALES*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *241479089205114716505435207289017673985767729586*

Authority Info Access	<i>http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt</i> <i>http://ocsp.accv.es</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
CRL Distribution Points	<i>http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl</i> <i>CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES</i>
Subject Key Identifier	<i>C0:3E:7C:2D:92:B6:55:A8:56:7D:76:CE:E8:AC:34:64:B1:77:02:96</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>60:AD:C7:42:48:A4:5F:7D:F9:68:58:7F:38:11:9F:50:E9:9B:4E:06:D1:A6:24:1D:C6:B8:F6:D1:9C:D2:A3:8A</i>

X509SubjectName

Subject CN:	<i>ACCV RSA1 PROFESIONALES</i>
Subject 2.5.4.97:	<i>VATES-A40573396</i>
Subject O:	<i>ISTEC</i>
Subject L:	<i>BURJASSOT</i>
Subject ST:	<i>VALENCIA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>wD58LZK2VahWfXbO6Kw0ZLF3ApY=</i>

Service Status

Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2023-12-21T00:00:00Z</i>

Scheme Service Definition URI

URI	<i>[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

Issuer L:	BURJASSOT
Issuer ST:	VALENCIA
Issuer C:	ES
Subject CN:	ACCV RSA1 COMPONENTES
Subject 2.5.4.97:	VATES-A40573396
Subject O:	ISTEC
Subject L:	BURJASSOT
Subject ST:	VALENCIA
Subject C:	ES
Valid from:	Tue Jul 25 14:20:01 CEST 2023
Valid to:	Fri Jul 19 14:20:00 CEST 2047
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EC:A5:7A:92:24:D5:51:F9:A1:B2:84:08:81:6C:A1:B6:D2:47:8F:13:AB:63:91: B6:87:C4:97:63:69:2B:63:29:0B:C3:ED:E0:6B:24:CA:23:6E:56:4B:36:0A:F0:8E:9A:B3:3F:62:D4:EA:95:79:BE:5D:D7:96:93:01:2A:B6:D8:85:2E:0C:FF:68:5F:AF:C5:10:78:47:31:74:00:5 7:43:91:29:B8:4D:1F:81:40:B8:45:02:2E:7A:F1:55:83:AE:B8:AA:C6:1E:32:56:C7:4E:6A:30:13:79:49:AA:FA:F0:0D:CB:99:EC:2B:A9:AE:22:09:7B:F2:F1:79:AD:C9:0C:57:1B:A5:D9:EB:7C: 22:07:38:11:EA:52:28:41:E0:93:85:FB:9A:19:23:69:D8:0C:D9:30:87:C0:95:91:93:32:72:38:B3:7E:42:3D:23:0E:0A:EA:C7:B5:3E:7A:F2:D0:D2:4F:9D:BC:2D:E2:BC:22:06:19:41:4F:5F:8 3:F2:E2:02:F1:C0:4C:58:35:5F:05:9D:5A:75:57:50:9F:82:10:F9:A8:76:61:94:3F:18:8B:E4:6F:52:0C:86:99:29:FA:B5:42:93:D8:68:9F:01:91:B8:7A:B0:4E:6C:E8:73:6F:50:1A:73:17:D0:F A:38:EF:67:6F:86:DC:0E:1C:DD:88:55:E3:5D:65:C6:4F:06:9E:6A:EF:8C:87:F3:E9:CD:4A:50:53:C3:2D:F8:BA:4D:50:E5:93:BE:3B:3C:E7:F7:4E:28:42:22:78:FA:D7:74:DF:2C:86:4F:6A:12: 0F:71:85:A8:AA:8F:2F:64:3D:07:CE:5F:2F:5A:6A:7F:7B:96:ED:6A:F4:7A:1F:13:30:4A:F5:BD:C2:CD:CC:BA:73:6D:DA:EC:F2:98:B5:1B:4E:FF:81:58:CC:72:A8:A3:90:05:77:5D:ES:F1:21:C 7:72:A5:24:20:1E:28:2D:F8:62:27:01:5D:FE:1A:4E:D8:66:63:DA:88:D6:FD:9F:A0:11:90:C5:1E:87:E4:FC:2A:72:F5:4B:23:D0:F7:F6:2C:35:1B:8A:5A:81:6E:5B:D3:01:F7:77:BF:1B:D6:16: 88:E3:C0:CE:B6:D6:74:7B:61:85:CB:17:63:A8:9F:71:23:74:EB:B3:A1:68:71:5D:D2:1A:9C:78:2A:66:DD:55:6B:0C:EB:3D:63:40:8E:E1:49:45:97:A1:90:84:94:21:40:1E:68:09:26:EE:C6:C C:3A:87:7F:64:84:E2:97:63:C8:52:4F:58:74:24:AE:B9:0F:65:52:F6:90:3C:61:1E:23:26:98:70:20:F9:73:DC:47:80:62:B2:DA:80:33:66:C8:E4:53:41:02:03:01:00:01 </pre>
Basic Constraints	IsCA: true
Authority Key Identifier	19:5A:13:3A:A1:9D:27:F7:A6:38:49:7B:54:59:5A:6E:A6:6A:A4:BB
Authority Info Access	http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt http://ocsp.accv.es
Certificate Policies	Policy OID: 2.5.29.32.0 CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]
Extended Key Usage	id_kp_clientAuth
CRL Distribution Points	http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
Subject Key Identifier	A9:48:0F:4C:E0:8C:43:E6:7E:D5:82:94:18:49:B2:45:26:D7:01:D5
Key Usage:	digitalSignature - keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	50:D5:74:8D:83:1C:28:64:45:9B:23:D8:B9:9D:F5:3D:BA:43:BB:BB:2B:C4:BF:CD:DB:57:31:B5:2B:56:B6:9E

X509SubjectName

Subject CN: *ACCV RSA1 COMPONENTES*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *qUgPTOCMQ+Z+1YKUGEmyRSbXAdU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

10.10.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.11 - Service (granted): Certificados cualificados emitidos por ACCV ECC1 CLIENTE**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados cualificados emitidos por ACCV ECC1 CLIENTE*

Name [en] *Qualified Certificates issued by ACCV ECC1 CLIENTE*

Authority Key Identifier	<i>9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15</i>
Authority Info Access	<i>http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crt</i> <i>http://ocsp.accv.es</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
CRL Distribution Points	<i>http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crl</i> <i>CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES</i>
Subject Key Identifier	<i>37:C4:94:3D:38:EB:EB:86:F5:8E:31:CC:5C:DB:8C:78:C3:D1:96:C1</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>5C:AF:44:B2:92:3B:14:6C:B5:75:AB:2A:B9:A0:A2:93:A1:34:60:23:35:D9:7E:57:9C:44:49:35:32:F4:84:96</i>

X509SubjectName

Subject CN:	<i>ACCV ECC1 CLIENTE</i>
Subject 2.5.4.97:	<i>VATES-A40573396</i>
Subject O:	<i>ISTEC</i>
Subject L:	<i>BURJASSOT</i>
Subject ST:	<i>VALENCIA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>N8SUPTjr64b1jjHMXNuMeMPRISE=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2023-12-21T00:00:00Z</i>

Scheme Service Definition URI

AdditionalServiceInformation

10.12 - Service (granted): Certificados cualificados emitidos por ACCV ECC1 PROFESIONALES

<http://uri.etsi.org/TrstSvc/Svctype/CA/OC>

Service Name

Name [es] *Certificados cualificados emitidos por ACCV ECC1 PROFESIONALES*

Name	[en]	Qualified Certificates issued by ACCV ECC1 PROFESIONALES

Service digital identities

Certificate fields details

Version: 3

Serial Number: 542714709950611360586364493036685225291506674687

X509 Certificate

Signature algorithm:	SHA512withECDSA
Issuer CN:	ACCV ROOT ECC EIDAS 2023
Issuer 2.5.4.97:	VATES-A40573396
Issuer O:	ISTEC

Issuer L: *BURJASSOT*
Issuer ST: *VALENCIA*
Issuer C: *ES*
Subject CN: *ACCV ECC1 PROFESIONALES*
Subject 2.5.4.97: *VATES-A40573396*
Subject O: *ISTEC*
Subject L: *BURJASSOT*
Subject ST: *VALENCIA*
Subject C: *ES*
Valid from: *Tue Jul 25 14:18:11 CEST 2023*
Valid to: *Fri Jul 19 14:18:10 CEST 2047*
Public Key: *30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:01:61:32:58:8F:93:98:C3:F2:F4:EF:8C:26:C5:CE:DC:8C:87:AF:16:59:92:0D:B3:FD:83:3D:AF:37:1D:6A:D1:72:87:56:F2:42:60:26:DA:EF:D3:DE:65:76:62:58:ED:87:48:E9:EF:33:F3:21:80:ED:DA:17:E6:D4:56:F8:09:D2:4E:00:32:87:52:39:79:42:C1:A1:81:D5:43:14:1D:E1:B2:AA:AS:7E:8B:C7:BE:80:7A:16:8A:82:24:2C:8C:D8:6E:0D:5A:AA:12:6B:25:B1:37:46:27:F8:33:37:40:2E:33:18:39:0C:B7:C1:37:7A:C2:2D:55:77:F6:9A:14:AC:A3:FD:B6*
Basic Constraints *IsCA: true*
Authority Key Identifier *9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15*
Authority Info Access *http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crt*
http://ocsp.accv.es
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]
Extended Key Usage *id_kp_clientAuth*
CRL Distribution Points *http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crl*
CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
Subject Key Identifier *31:DE:C0:D5:C6:B8:47:F5:94:0B:31:A3:A4:87:FF:C6:9F:98:88:1C*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *34:FD:B6:F3:D2:D1:07:0D:D8:42:8B:CE:11:D6:22:94:E1:FF:2C:49:E8:B1:28:B6:11:60:D7:48:C7:A5:37:AA*

X509SubjectName

Subject CN: *ACCV ECC1 PROFESIONALES*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *Md7A1ca4R/WUCzGjplf/xp+YiBw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2023-12-21T00:00:00Z

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

10.12.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.13 - Service (granted): Certificados cualificados emitidos por ACCV ECC1 COMPONENTES**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados cualificados emitidos por ACCV ECC1 COMPONENTES*

Certificate fields details

Version: 3

Serial Number: 288384503797355422930025878200965719802385314764

[illegible]

Signature algorithm: *SHA512withECDSA*

Issuer CN: *ACCV ROOT ECC EIDAS 2023*

Issuer 2.5.4.97: VATES-A40573396

Issuer 0: *ISTEC*

Issuer L: *BURIASSOT*

Issuer ST: VALENCIA

Issuer C: *ES*

Subject CN: *ACCV ECC1 COMPONENTES*

Subject 2.5.4.97: *VATES-A40573396*

Subject 0: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *FS*

Valid from: Tue Jul 25 14:20:39 CEST 2023

Valid to: *Fri Jul 19 14:20:38 CEST 2047*

Public Key:

Basic Constraints	<i>IsCA: true</i>
Authority Key Identifier	<i>9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15</i>
Authority Info Access	<i>http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crt</i> <i>http://ocsp.accv.es</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
CRL Distribution Points	<i>http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crl</i> <i>CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES</i>
Subject Key Identifier	<i>EC:57:F3:2F:01:10:3A:FB:61:47:D2:3B:68:96:33:F5:15:68:53:7E</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>D2:6E:70:2D:03:9A:57:13:DD:AB:F7:10:E4:71:93:73:4E:55:50:71:17:63:78:50:51:78:8D:0F:D2:D7:F4:EA</i>

X509SubjectName

Subject CN:	<i>ACCV ECC1 COMPONENTES</i>
Subject 2.5.4.97:	<i>VATES-A40573396</i>
Subject O:	<i>ISTEC</i>
Subject L:	<i>BURJASSOT</i>
Subject ST:	<i>VALENCIA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>7FfzLwEQOvthR9I7ajYz9RVoU34=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time*2023-12-21T00:00:00Z*

Issuer O: *ISTEC*
Issuer L: *BURJASSOT*
Issuer ST: *VALENCIA*
Issuer C: *ES*
Subject CN: *ACCV RSA1 TSA*
Subject 2.5.4.97: *VATES-A40573396*
Subject O: *ISTEC*
Subject L: *BURJASSOT*
Subject ST: *VALENCIA*
Subject C: *ES*
Valid from: *Tue Feb 27 15:20:58 CET 2024*
Valid to: *Fri Feb 21 15:20:57 CET 2048*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:02:02:01:00:CB:DF:38:28:90:29:78:23:23:F3:9F:0A:AB:49:F9:DA:A2:F5:D0:15:8A:17:9F:
7F:9C:67:4B:8B:D5:7C:9E:78:FF:0F:89:81:7D:1A:25:12:9B:AD:4F:23:40:62:A5:9F:86:46:86:D7:2E:6C:87:93:A3:83:F6:71:F1:2C:9F:4E:FA:24:6F:4B:A6:3F:2C:82:45:D7:CF:C2:A9:F4:F4:
9A:F2:A9:2D:15:73:F3:62:DE:07:01:F8:69:17:7B:4D:B2:27:0A:02:C3:B6:15:02:5D:B9:83:62:47:C2:D8:33:74:28:E0:6C:7B:6A:40:36:CF:A9:3E:69:F8:8E:90:6C:B2:A3:8E:BF:E8:B9:1C:0F:
7D:8B:93:DC:03:20:D2:01:CA:69:50:CB:81:29:46:8B:9A:2F:35:AE:F1:DD:A6:CI:EL:63:03:DC:04:32:CF:7C:5A:CE:38:6E:FA:99:B5:42:B8:67:43:C4:0B:2C:48:EA:5E:E0:27:40:52:B8:D4:
7C:87:6E:CB:71:58:A0:F6:38:36:09:37:F0:AB:0A:FD:6C:0B:04:DD:2E:21:30:A6:27:70:5A:EB:E4:7B:7B:51:84:B5:0C:88:66:8D:01:A9:3D:78:CC:78:49:CB:C4:6C:57:E9:DD:6A:26:A8:AF:
95:4D:35:0A:85:BE:A9:67:59:2F:86:A9:23:65:11:7D:FD:5E:F0:E9:9D:E8:65:DE:D3:63:E7:00:80:C1:21:08:E8:F3:3B:24:55:CE:55:CC:DC:92:E6:24:E4:F0:82:FD:00:46:2F:63:64:4A:1F:F2:
BB:87:AD:58:D1:B6:62:FF:1B:45:C9:18:4F:EB:6F:69:4F:50:08:1F:40:0B:59:07:5F:AD:92:96:9F:DA:ED:33:0A:C0:C7:93:D4:E7:71:35:0F:23:CC:A7:80:54:9C:D4:2A:A7:02:B3:23:FE:A1:7
1:43:35:AD:89:2C:6E:85:F3:5A:59:66:70:4B:FE:E9:E6:DE:CA:F5:11:6A:EB:AE:3F:98:72:AA:62:8A:3B:24:25:B8:E1:2A:59:4F:65:FF:66:0A:59:01:88:72:40:E2:BE:15:57:C5:26:C1:8D:B1:9
FA7:C2:95:73:45:9C:D5:4E:92:8D:2A:F9:68:9F:56:99:EB:02:E:EC:9C:F3:5E:28:13:7A:CD:C3:C3:B8:08:B2:3B:46:9B:39:3F:40:7A:0B:77:88:74:16:E9:53:AD:DB:6C:54:AB:48:97:28:C6:
8C:EB:97:36:CB:60:6B:60:61:4D:21:CE:9A:50:9D:DE:A6:8D:38:53:A1:7C:4A:F4:B2:FF:3E:4B:4E:A9:B1:FC:64:47:B2:E4:DD:2C:72:84:2D:3B:78:7D:02:03:01:00:01

```

Basic Constraints *IsCA: true*
Authority Key Identifier *C9:9E:61:22:B2:91:3C:77:7E:21:DA:A9:8F:9A:81:1F:30:54:1A:AB*
Authority Info Access *http://www.accv.es/gestcert/accv_root_rsa_eidas_tsa_2024.crt*
http://ocsp.accv.es
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.accv.es/legislacion_c.htm
Extended Key Usage *id_kp_timeStamping*
CRL Distribution Points *http://www.accv.es/gestcert/accv_root_rsa_eidas_tsa_2024.crl*
Subject Key Identifier *E1:EF:00:25:CA:9D:7B:42:3B:46:A5:AD:CF:86:D1:DC:E9:8A:AC:AC*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *FD:D5:AA:DD:52:B5:99:5E:F4:B4:A9:33:A7:89:74:6D:45:59:DA:F2:F1:A1:5A:59:4B:D1:51:AA:18:D9:99:39*

X509SubjectName

Subject CN: *ACCV RSA1 TSA*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *4e8Ajqcde0I7RqWtz4bR3OmKrKw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2025-05-06T00:00:00Z

Scheme Service Definition URI

URI [en] *https://avance.digital.gob.es/en-us/servicios/firmaelectronica/paginas/tsu_infraestructurasstc.aspx*

URI [es] *https://avance.digital.gob.es/es/Servicios/FirmaElectronica/Paginas/TSU_InfraestructurasSTC.aspx*

10.15 - Service (granted): Qualified time stamps issued by "ACCV ECC1 TSA"**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified time stamps issued by "ACCV ECC1 TSA"*

Name [es] *Servicio de expedición de sellos electrónicos cualificados de tiempo por "ACCV ECC1 TSA"*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: 55719492625506493394786418733599518029587307684

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIEEjCCASgAwIBAgIUCCkMAeoraH+Q9JfDQbF0yKSXKQwCgYIKoZlZjOEAwQwYUxCzAIBgNV
BAYTAkVMTREwDwYDVQOQIDAhWQXFTKjNjOTESMBAGAlUEBwwjOIVS5kFTU09UMQ4wDAYDVQQKDAVJ
U1RfQ2EYMBIjGAUEYQWVFRVFRMjQwNTczMzZMSUwWYDVQQDDbB00WfjPT1QgRUNDIFRT
Q5BF5URBUyayMDI0MB4XDTI0MDIyNzE0MjE0NVVoXDQ04MDIyMTE0MjE0NFowdGJELMAkGA1UEBhMC
RVNMEtAPBqNVBAgMCFZ8TEVQOQIBMRiweAYDVQOHDAICVjKQVNTT1QxDjAMBqNVBAoMBUITVEVD
MR9wFjYDQVRhDAQWQVRfUy1BNDA1NzE0MjE0NVVhYU8gNVBAMMDUFDO1YgRUNDMSB1UEEwZSwEAYH
Kozj0CAQYFK4EEACMDgYYABAA0KLvwFn3EOPAFBm6OWSpQrwA0n7zVIGAJtjGPyWeL+Vx70Rg
u76gLeR7gej06lmYEQRCBtpoVOKLMS21JlYAwAcS956BT6vmdZaAXT9XtWdPfec+4b3mHrTpS8
1COL0xvUWkmzGhFxfjg9t92+qSGUwK5W95ph3ujhTWZK5qOCATswggGHMA8GAlUdeWcBjwOF
MAMBAF8wHwYDVR0jBBgwFoAUwPPnqxRWg/5aOvTolJZs2O2QeQweQYIKwYBBQUHAQEEdTBMEgG
CcsGAQUFBzAChxodHRwOi8vd3d3LmFjY3Y3YUZXNvZ2VzdGNCcnQvYWNjdj9yb290X2VY19laWRh
c190c2FmYjNC5jcnQwHwYKwYBBQUHMAEGZ3d3LmFjY3Y3YUZXNvZ2VzdGNCcnQvYWNjdj9yb290X2VY19laWRh
PDA6BgRVHSAAMDliwMAYIKwYBBQUHAgEwGh0dHA6Ly93d3cuYWNjdj9yb290X2VY19laWRh
Lmh0bTATBgNVHSUEDDAKBggrBgEFBQcDCDBNBgNVHR8ERBEMEKgQKA+hixodHRwOi8vd3d3LmFj
Y3Y3YUZXNvZ2VzdGNCcnQvYWNjdj9yb290X2VY19laWRhcn190c2FmYjNC5jcmwwHwYDVR0OB8YE
FK1NGwZjT4WQsdG3RNFxzAU3rxMA4GA1UdDwEB/wQEAwIBBjAKBgqgqHkOPQODBAOBiAwgYcc
OXuo3minle6VjMuZS5FieF0z3FS0a2YPdHxknteWMEHLh4v+VbAvGbu9qt16WTSUIOHUXRjV/+
G8IOWT0uswAA4IBBhCHUdJp+0gd7xRlqPsetjHG28Q+n61iiQHVXaVHg+ZBEW4znRaxqc6ydl
yftVtVMTESBxLbZBMGA9rttCA=

-----END CERTIFICATE-----

Signature algorithm: SHA512withECDSA

Issuer CN: ACCV ROOT ECC TSA EIDAS 2024

Issuer 2.5.4.97: VATES-A40573396

Issuer O: ISTECS

Issuer L: BURJASSOT

Issuer ST: VALENCIA

Issuer C: ES

Subject CN: ACCV ECC1 TSA

Subject 2.5.4.97: VATES-A40573396

Subject O: ISTECS

Subject L: BURJASSOT

Subject ST: VALENCIA

Subject C: ES

Valid from: Tue Feb 27 15:21:45 CET 2024

Valid to: Fri Feb 21 15:21:44 CET 2048

Public Key: 30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:00:34:28:BB:F0:16:7D:C4:38:F0:05:06:6E:8E:59:2A:50:AF:00:34:9F:BC:D5:20:60:09:84:98:C6:3D:85:9E:2F:E5:71:EF:44:60:BB:8E:AA:2D:E4:7B:81:E8:E8:E8:89:98:11:04:42:06:DA:68:55:F3:8A:2C:C4:B6:D6:32:18:03:00:1C:B3:DE:7A:05:3E:AF:99:D6:5A:01:74:FD:5E:D5:9D:3E:D1:5E:73:EE:1B:DE:61:EB:4E:94:81:D4:2D:0B:D3:1A:EF:51:62:A6:CC:61:F1:17:17:E3:B6:A8:21:F7:3F:AA:20:65:30:2B:95:BD:4A:98:6D:DE:E8:E1:4D:6D:A4:E6

Basic Constraints IsCA: true

Authority Key Identifier FF:03:CF:9E:AC:51:5A:0F:EC:68:EB:D3:A0:92:76:B3:3D:36:41:E4

Authority Info Access http://www.accv.es/gestcert/accv_root_ecc_eidas_tsa_2024.crt
http://ocsp.accv.es

Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.accv.es/legislacion_c.htm</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	<i>http://www.accv.es/gestcert/accv_root_ecc_eidas_tsa_2024.crl</i>
Subject Key Identifier	<i>AD:4D:88:6C:19:26:34:F8:59:0B:1D:1B:74:4D:17:1C:C0:53:7A:F1</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>67:7C:8F:5F:17:69:6D:CC:96:F5:92:C8:B0:2E:B5:0A:E2:1A:7A:1C:97:09:97:D4:A7:FE:B9:3D:09:4E:99:57</i>

X509SubjectName

Subject CN:	<i>ACCV ECC1 TSA</i>
Subject 2.5.4.97:	<i>VATES-A40573396</i>
Subject O:	<i>ISTEC</i>
Subject L:	<i>BURJASSOT</i>
Subject ST:	<i>VALENCIA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>rU2lbBkmNPhZCx0bdE0XHMBTevE=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time*2025-05-06T00:00:00Z***Scheme Service Definition URI**

URI <i>[en]</i>	<i>https://avance.digital.gob.es/en-us/servicios/firmaelectronica/paginas/tsu_infraestructurasstc.aspx</i>
URI <i>[es]</i>	<i>https://avance.digital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_InfraestructurasSTC.aspx</i>

10.16 - Service (granted): Qualified certificates issued by "ACCV RSA1 TLS"

Subject L:	BURJASSOT
Subject ST:	VALENCIA
Subject C:	ES
Valid from:	Tue Feb 27 15:18:56 CET 2024
Valid to:	Wed Feb 23 15:18:55 CET 2039
Public Key:	<pre>30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DB:11:B7:FD:DE:59:EA:9E:14:9D:09:4A:D3:70:48:11:FA:3B:93:8B:0E:8A:08 :F9:49:01:75:AE:DC:C3:BF:E3:8D:A9:40:AE:5F:33:81:AE:46:5C:4C:1A:FF:7D:CC:07:78:FA:A3:67:FC:43:2D:C7:D0:C9:EC:78:45:86:B1:8B:A3:F4:EB:E6:E7:AB:81:CE:39:C7:25:A4:1D:93: 34:28:6D:6D:FC:10:E4:80:64:6E:B7:82:59:EB:AE:45:6F:42:AB:00:7A:5A:25:46:D6:E6:F8:96:C1:8C:52:9C:12:A3:DA:49:05:62:A6:02:72:09:AA:C4:A8:F6:A0:83:77:D7:56:ED:F8:BF:5C:8 5:1A:52:E2:15:5B:8E:EF:05:D6:62:D3:29:DC:01:9B:48:07:49:62:20:A0:71:54:70:3F:23:D6:C9:DA:B5:5C:A3:D8:EB:B6:E1:98:0D:8D:8A:67:9A:2E:8F:A4:DD:D7:34:44:31:91:A8:8E:CA:E 5:37:D7:01:3C:14:92:21:99:AC:89:DD:92:F4:7E:7E:34:BF:18:EE:50:2B:4B:6C:35:14:D4:8B:FD:A1:58:A0:FA:EC:67:12:8B:2B:81:09:80:6B:36:CB:3F:30:9E:15:11:C4:5C:43:3E:18:9E:2E: A3:8B:83:46:C3:15:BF:A6:02:A1:E8:4A:CF:F9:B1:EF:24:12:D0:83:0D:2B:DC:29:60:E5:00:F8:07:E3:F7:3B:93:86:46:0D:92:5A:40:2A:70:8D:90:1A:8B:DC:E9:35:C2:CF:63:E8:23:47:23:5 EF2:E8:33:EB:55:E0:FC:10:21:B5:FC:21:AE:05:F6:46:34:5A:69:C4:DD:DD:40:7A:80:42:17:8B:97:7B:78:3C:34:F3:A7:2C:5C:5A:8A:3C:AA:A9:89:EB:13:49:D4:DB:F8:B2:13:2C:97:1F:7F: 3D:3E:A2:FF:9B:C2:FF:8E:B5:E1:89:2E:6E:E2:7E:E9:CA:F7:04:6A:8B:24:A5:04:22:3B:F6:F3:8B:08:63:8A:60:8A:A7:3F:E2:89:D7:0A:03:2D:91:FE:F5:5C:9C:66:62:58:80:5D:32:53:51:D9: 92:03:D5:A2:DE:B2:50:88:C4:EB:59:25:F0:8A:1E:45:5C:04:D6:44:13:6D:99:D0:CO:AA:75:A0:DF:F6:92:4E:69:58:FE:B0:71:7C:1A:8B:31:9E:16:A3:EE:7D:A1:50:46:00:8E:EF:C3:2A:F5:8 7:00:C3:AC:B1:8C:1B:92:06:4C:D3:DC:DE:C2:1E:F0:C8:C7:3C:63:55:0F:42:0E:4F:97:EF:44:9D:F8:AF:F3:64:D6:8D:E7:5A:8A:F9:EF:8B:C6:9A:12:6F:DD:02:03:01:00:01</pre>
Basic Constraints	IsCA: true
Authority Key Identifier	0B:3F:A4:1D:11:E0:BD:C1:8A:C4:08:B7:5E:7F:76:B2:F3:AC:BB:0D
Authority Info Access	http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crt http://ocsp.accv.es
Certificate Policies	Policy OID: 2.5.29.32.0 CPS pointer: http://www.accv.es/legislacion_c.htm
Extended Key Usage	id_kp_serverAuth
CRL Distribution Points	http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crl
Subject Key Identifier	2F:2E:03:35:56:31:F3:02:43:49:96:8D:B1:F0:F0:42:04:CF:B4:FA
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	34:64:40:CF:76:74:A5:29:30:55:45:56:33:22:FC:FB:38:F5:A4:B3:F1:E7:E8:52:DF:F8:A4:B7:A5:EF:72:D1
X509SubjectName	
Subject CN:	ACCV RSA1 TLS
Subject 2.5.4.97:	VATES-A40573396
Subject O:	ISTEC
Subject L:	BURJASSOT
Subject ST:	VALENCIA
Subject C:	ES

Issuer CN: *ACCV ROOT ECC TLS 2024*

Issuer 2.5.4.97: *VATES-A40573396*

Issuer O: *ISTEC*

Issuer L: *BURJASSOT*

Issuer ST: *VALENCIA*

Issuer C: *ES*

Subject CN: *ACCV ECC1 TLS*

Subject 2.5.4.97: *VATES-A40573396*

Subject O: *ISTEC*

Subject L: *BURJASSOT*

Subject ST: *VALENCIA*

Subject C: *ES*

Valid from: *Tue Feb 27 15:20:09 CET 2024*

Valid to: *Wed Feb 23 15:20:08 CET 2039*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:1A:32:61:13:B0:E1:6A:13:A2:C3:61:78:9C:FD:68:33:44:03:04:D1:CF:F7:4F:E2:77:3C:D1:9E:72:87:21:61:8D:2A:27:10:3C:D3:70:9D:86:0D:4C:E3:38:19:ED:6B:10:E1:3F:55:8F:94:75:90:7C:D8:27:6D:99:9E:DB:21:B4:26:20:07:6F:67:78:A3:50:1E:39:F2:AE:DD:EF:90:AE:74:F4:99:BD:A3:6F:16:A2:A8:E6:64:A8:EA:E7:89*

Basic Constraints *IsCA: true*

Authority Key Identifier *CE:FC:70:C7:87:A4:25:5C:9E:52:92:AA:5F:C3:26:52:26:6E:1F:EA*

Authority Info Access *http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crt*
http://ocsp.accv.es

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.accv.es/legislacion_c.htm

Extended Key Usage *id_kp_serverAuth*

CRL Distribution Points *http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crl*

Subject Key Identifier *A3:ED:C8:AD:A9:AE:0E:6E:36:32:96:04:B2:27:18:D4:F0:51:A6:4D*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: 93:C0:87:AB:93:31:B7:4C:0F:CC:CE:11:BC:61:FB:9F:A6:D4:32:07:7D:8F:10:18:19:4F:A4:CC:A6:64:D7:81

X509SubjectName

Subject CN: ACCV ECC1 TLS

Subject 2.5.4.97: VATES-A40573396

Subject O: ISTECH

Subject L: BURJASSOT

Subject ST: VALENCIA

Subject C: ES

X509SKI

X509 SK I o+3IramuDm42MpYEsicY1PBRpk0=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2025-05-06T00:00:00Z

10.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

11 - TSP: AC Camerfirma, S.A.

TSP Name

Name [en] AC Camerfirma, S.A.

Name [es] AC Camerfirma, S.A.

TSP Trade Name

Name [en] VATES-A82743287

Name [en] Camerfirma

Name [es] Camerfirma

Name [en] AC Camerfirma S.A.

Name [en] AC Camerfirma SA

Name [en] AC CAMERFIRMA S.A.

Name [en] AC CAMERFIRMA SA

PostalAddress

Street Address [en] C/ Rodríguez Marín nº 88

Locality [en] Madrid

State Or Province [en] Madrid

Postal Code [en] 28016

Country Name [en] ES

PostalAddress

Street Address [es] C/ Rodríguez Marín nº 88

Locality [es] Madrid

State Or Province [es] Madrid

Postal Code [es] 28016

Country Name [es] ES

ElectronicAddress

URI	[en]	http://www.camerfirma.com
URI	[es]	http://www.camerfirma.com

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificates issued by CA AC Racer-2009

Name [es] *Certificados Reconocidos emitidos por la CA Racer - 2009*

Version: 3

Serial Number: 3

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: AC Camerfirma - 2009

Issuer L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Issuer SERIAL NUMBER: A82743287
Issuer O: AC Camerfirma S.A.
Issuer C: ES
Subject CN: RACER - 2009
Subject L: Madrid (see current address at <https://www.camerfirma.com/address>)
Subject SERIAL NUMBER: A82743287
Subject O: AC Camerfirma S.A.
Subject C: ES
Valid from: Wed Mar 25 11:47:09 CET 2009
Valid to: Sat Mar 23 11:47:09 CET 2019
Public Key:
30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D8:E4:54:88:62:77:2F:89:25:72:7F:FB:0C:E5:EB:93:83:1A:3E:53:2E:BB:CB:E5:23:0C:F3:17:79:32:58:7F:51:1A:03:F2:3F:39:56:5D:3C:8F:1E:07:6C:62:ED:0C:4A:A6:93:20:CF:FA:1B:E1:85:E2:FF:F6:CB:00:ED:BE:19:9D:63:31:88:94:42:E2:7F:F2:12:85:FC:29:B9:A9:41:6F:41:1E:C1:FC:DC:C0:74:28:0F:2E:22:BE:3F:46:F6:78:C3:53:C6:A0:5B:80:4D:0A:E0:3B:A3:3C:9E:72:90:56:F8:6A:AD:E0:07:AE:AB:5F:66:A8:00:11:CD:07:35:99:09:94:06:EF:1F:B2:F7:43:75:B7:91:00:B3:2C:83:8F:1E:C9:D6:64:99:F4:78:29:D2:BA:6E:6D:D8:55:92:96:54:95:2A:89:7A:96:AE:EF:CF:C3:D7:AB:47:DD:5F:00:48:0F:48:1F:6E:0F:A1:69:5A:E7:72:B7:8D:EF:7A:13:A3:11:DA:0A:E0:EE:72:F9:94:00:C7:D8:78:20:B2:DB:26:81:C4:EB:1D:CF:ED:90:9E:A1:0E:13:0D:9A:57:19:4C:F8:E6:13:08:7D:34:C1:F5:67:CC:B3:67:32:A4:F8:06:6F:3B:7C:25:79:25:EC:87:9A:25:A9:11:45:5F:EE:CB:63:E3:FF:53:E5:44:7B:67:26:EB:E3:29:66:92:4F:2A:AA:5C:56:A5:73:F9:A2:FC:CA:E9:80:16:F2:E9:8D:71:08:EF:2A:EF:FF:7C:5F:B2:6E:B6:CA:47:2D:AD:22:20:47:00:E3:8D:A3:92:52:63:3C:92:BB:49:03:0D:C3:37:02:86:91:60:DA:55:59:9F:85:1B:AE:09:E7:94:C7:D7:E7:63:EC:06:3F:9D:10:3E:0B:AC:27:1E:67:FB:4A:2E:06:7D:6F:AC:DE:56:02:4A:7C:5A:BF:BE:20:41:DA:90:D5:61:00:E9:F9:AB:5C:81:FE:3A:DF:3B:AB:64:AC:13:1C:F9:40:AE:2C:AD:29:5C:E9:82:40:D7:E0:D2:C5:FF:5F:B2:31:CA:A9:85:84:02:FF:41:33:69:6A:CB:9C:2D:00:1B:D1:C4:B4:97:57:36:7F:5D:74:00:3E:BD:F7:13:A8:19:F0:B7:9E:B2:53:88:3A:63:BA:A8:24:48:BA:E3:28:E4:80:16:85:EC:C3:6E:BA:C4:D5:30:D9:C1:9B:A1:CB:4F:73:D4:A5:53:72:7B:C9:44:FC:AB:85:0C:2A:F1:8E:7B:DB:FF:1A:C9:6C:53:EB:80:50:93:88:5D:B9:2E:22:15:94:46:0D:91:EA:F7:BA:48:4C:CF:75:02:03:01:00:01
Basic Constraints *IsCA: true - Path length: 1*
Subject Key Identifier AC:16:D7:10:D1:6F:75:F6:84:88:68:E6:44:25:11:72:CA:B3:1B:80
Authority Key Identifier C8:00:0F:FC:C6:52:FC:9F:DB:3B:64:2E:32:B9:6E:2E:71:F3:65:79
Authority Info Access http://www.camerfirma.com/certs/ac_camerfirma-2009.crt
<http://ocsp.camerfirma.com>
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://policy.camerfirma.com>
CRL Distribution Points http://crl.camerfirma.com/ac_camerfirma-2009.crl
http://crl1.camerfirma.com/ac_camerfirma-2009.crl
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 47:CF:DE:E3:76:09:72:5C:FF:03:7B:56:A0:71:C4:3A:A0:58:69:A8:44:28:A5:D8:61:FF:92:B9:45:02:92:AA
X509SubjectName
Subject CN: RACER - 2009

Subject L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject C: *ES*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2017-07-21T00:00:00Z*

11.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

11.1.3 - History instance n.1 - Status: granted

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service Name

Name	[en]	Qualified Certificates issued by CA AC Racer-2009
Name	[es]	Certificados Reconocidos emitidos por la CA Racer - 2009

Service digital identities**X509SubjectName**

Subject CN:	RACER - 2009
Subject L:	Madrid (see current address at https://www.camerfirma.com/address)
Subject SERIAL NUMBER:	A82743287
Subject O:	AC Camerfirma S.A.
Subject C:	ES

X509SKI

X509 SK I	rBbXENFvdfaEiGjmRCURcsqzG4A=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time

2016-06-30T22:00:00Z

11.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.1.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA AC Racer-2009

Name	[es]	Certificados Reconocidos emitidos por la CA Racer - 2009

Service digital identities**X509SubjectName**

Subject CN:	RACER - 2009
Subject L:	Madrid (see current address at https://www.camerfirma.com/address)
Subject SERIAL NUMBER:	A82743287
Subject O:	AC Camerfirma S.A.
Subject C:	ES

X509SKI

X509 SK I	rBbXENFvdFaEiGjmRCURcsqzG4A=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2010-07-02T00:00:00Z

11.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.2 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Camerales - 2009

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Camerales - 2009

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009

Service digital identities

Certificate fields details

Version: 3

Serial Number: 2

Authority Info Access	<i>http://www.camerfirma.com/certs/root_chambers-2008.crt</i> <i>http://ocsp.camerfirma.com</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://policy.camerfirma.com</i>
CRL Distribution Points	<i>http://crl.camerfirma.com/chambersroot-2008.crl</i> <i>http://crl1.camerfirma.com/chambersroot-2008.crl</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>2F:2B:32:E7:8F:C6:9D:2F:FC:64:5E:B6:06:8E:07:4E:74:97:74:49:5F:DC:25:10:93:B0:EE:E0:4E:FA:FD:17</i>

X509SubjectName

Subject CN:	<i>Camerfirma Certificados Camerales - 2009</i>
Subject L:	<i>Madrid (see current address at https://www.camerfirma.com/address)</i>
Subject SERIAL NUMBER:	<i>A82743287</i>
Subject O:	<i>AC Camerfirma S.A.</i>
Subject C:	<i>ES</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time *2017-07-21T00:00:00Z*

11.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

11.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by the CA Camerfirma Camerales - 2009*

Name [es] *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

Service digital identities**X509SubjectName**

Subject CN: *Camerfirma Certificados Camerales - 2009*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject C: *ES*

X509SKI

X509 SK I *HsRaioRvEZBYs+IJ1xbm6sMk5o0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.2.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Camerales - 2009

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009

Service digital identities**X509SubjectName**

Subject CN: Camerfirma Certificados Camerales - 2009

Subject L: Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject C: ES

X509SKI

X509 SK I HsRaioRvEZBYs+IJ1xbm6sMk5o0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2010-07-02T00:00:00Z

11.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.3 - Service (withdrawn): Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

Name	[en]	Qualified Certificates issued by CA AC Camerfirma Certificados Camerales
Name	[es]	Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales

Certificate fields details

[illegible]

Valid to: Thu Feb 09 16:42:47 CET 2034

Public Key:

30:82:01:20:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0D:00:30:82:01:08:02:82:01:01:00:A3:C6:7B:EF:8F:4D:5F:DF:A9:60:1A:18:A1:45:85:5F:D5:F0:0F:11:7B:13:24:AA:08:E1:A2:D0:70:45:12:87:9B:33:64:4E:D5:4E:D1:A2:C8:C4:CC:73:68:82:9A:76:97:69:F8:D8:1C:AF:0B:82:6C:BA:4F:DC:71:18:46:79:39:2E:31:EA:88:2D:8B:FC:82:D7:70:0F:B6:ED:D7:DD:8D:A4:3D:52:EE:ED:93:30:E4:7A:10:0B:AE:30:06:3E:98:72:7C:53:9C:1C:26:55:6D:39:0E:3C:D1:5E:9E:8E:C8:12:04:28:46:80:07:D8:EF:DA:A1:25:7E:1F:D8:D8:7E:05:18:A5:9D:FE:EB:75:83:44:9C:45:90:28:FB:A0:92:30:D4:31:69:8F:AB:C9:72:83:D7:58:96:93:35:97:25:AF:54:64:E6:AC:1B:BC:F8:B8:FA:9C:1A:BE:3F:1F:3D:BF:09:32:C3:4E:0A:74:C6:43:09:62:EC:CE:CE:DA:54:BC:E0:02:AF:19:64:4B:6B:AD:29:4C:15:94:08:A4:26:76:E8:37:07:FF:7A:7F:78:45:B1:CD:CE:42:9C:E6:DD:12:01:BC:C2:7F:9E:EE:79:AC:1B:CF:14:9D:3D:AF:92:00:2D:B9:14:DB:AB:EB:81:4A:91:F7:6A:E4:F3:E3:02:01:03

Basic Constraints

IsCA: true - Path length: 11

CRL Distribution Points

http://crl.chambersign.org/chambersroot.crl

Subject Key Identifier

B6:1F:4E:9D:1C:68:91:2E:37:72:60:E1:46:8F:5A:A5:2A:31:31:B9

Authority Key Identifier

E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A

Subject Alternative Name

ac_camerfirma_cc@camerfirma.com

Issuer Alternative Name

chambersroot@chambersign.org

Certificate Policies

Policy OID: 1.3.6.1.4.1.17326.10.9.1

CPS pointer: http://cps.camerfirma.com/cps/ac_camerfirma_cc.html

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

C7:D8:43:81:E1:1F:7C:57:46:77:1A:F5:B0:50:DC:51:FC:6F:DA:D6:F6:F3:5B:B5:3A:3D:E9:13:82:2E:A0:9E

X509SubjectName**Subject CN:**

AC Camerfirma Certificados Camerales

Subject O:

AC Camerfirma SA

Subject SERIAL NUMBER:

A82743287

Subject L:

Madrid (see current address at www.camerfirma.com/address)

Subject E:

ac_camerfirma_cc@camerfirma.com

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2022-09-06T00:00:00Z

11.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en]

undefined.

[es]

undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

11.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

Name [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

Service digital identities**X509SubjectName**

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: ES

X509SKI

X509 SKI th9OnRxokS43cmDhRo9apSoxMbk=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2020-06-09T00:00:00Z

11.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

11.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

11.3.4 - History instance n.2 - Status: withdrawn

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

Name [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

Service digital identities

X509SubjectName

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: *ES*

X509SKI

X509 SK I *th9OnRxokS43cmDhRo9apSoxMbk=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Status Starting Time *2017-07-21T00:00:00Z*

11.3.4.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

11.3.4.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.3.5 - History instance n.3 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

Name	[es]	Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales

Service digital identities**X509SubjectName**

Subject CN:	AC Camerfirma Certificados Camerales
Subject O:	AC Camerfirma SA
Subject SERIAL NUMBER:	A82743287
Subject L:	Madrid (see current address at www.camerfirma.com/address)
Subject E:	ac_camerfirma_cc@camerfirma.com
Subject C:	ES

X509SKI

X509 SK I	th9OnRxokS43cmDhRo9apSoxMbk=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

11.3.5.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

11.3.5.6 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.3.6 - History instance n.4 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

Name [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

Service digital identities**X509SubjectName**

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *ac_camerfirma_cc@camerfirma.com*

Subject C: *ES*

X509SKI**X509 SK I***th9OnRxokS43cmDhRo9apSoxMbk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision***Status Starting Time***2004-11-25T00:00:00Z***11.3.6.7 - Extension (not critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1</i>

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2</i>

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1</i>

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2</i>

11.4 - Service (withdrawn): Qualified Certificates issued by CA AC Racer**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	<i>[en]</i>	<i>Qualified Certificates issued by CA AC Racer</i>

Certificate fields details

Version: 3

Serial Number: 1

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: AC Camerfirma

Issuer O: *AC Camerfirma SA*

Issuer L: *Madrid (see current address at www.camerfirma.com/address)*

Issuer SERIAL NUMBER: *A82743287*

Issuer E: *ac camerfirma@camerfirma.com*

Issuer C: *ES*

Subject CN: *RACER*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *caracer@camerfirma.com*

Subject C: *ES*

Valid from: *Thu Dec 04 18:26:41 CET 2003*

Valid to: *Mon Dec 04 18:26:41 CET 2023*

Public Key:

30:82:01:1F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0C:00:30:82:01:07:02:82:01:00:7B:4D:F2:CB:51:D9:C6:0B:5D:83:56:F6:36:87:17:AA:D3:3B:DF:1E:BD:F7:69:20:F5:F7:9E:70:40:ED:DF:A3:40:75:89:82:FA:88:7A:30:AA:03:DC:22:10:46:21:CB:9B:EF:D1:CB:2B:9D:0F:AA:34:0F:42:CD:78:6A:D1:62:97:05:C3:BC:CA:39:85:FF:98:C1:93:21:72:8B:3E:4B:8B:05:DA:02:BE:0C:B1:E1:A9:B2:06:28:19:57:A0:23:1A:7E:3E:C4:8C:D0:CB:99:63:3B:25:65:9D:F1:5F:23:8F:5A:C2:47:D7:D3:E0:4D:BF:9A:96:2A:9B:21:83:ES:A7:14:E5:B5:19:DD:0C:25:73:07:EA:E3:6C:8B:6F:C7:76:A4:A0:B2:F5:10:D5:D4:0D:7A:52:B1:CF:E1:1B:4D:F8:AE:C3:E1:F0:81:06:E9:7F:F9:EC:7B:8A:06:BF:47:2A:D2:90:3C:E6:07:44:A0:EF:9F:2C:EC:11:67:C0:EE:7C:06:95:60:04:E7:A9:F4:EF:61:EC:70:61:87:10:EC:D5:83:C4:25:F4:E6:25:6C:E7:5A:DB:87:94:2B:C0:8A:BF:4A:DE:CB:FF:AC:50:77:EF:B4:9A:57:C0:26:80:BB:4C:5E:42:6A:CA:1:DA:E4:89:29:23:20:23:D5:8F:C3:02:01:03

Basic Constraints

IsCA: true - Path length: 10

CRL Distribution Points

http://crl.camerfirma.com/racer.crl

Subject Key Identifier

BE:BC:08:D4:2E:BA:00:4C:80:DC:26:67:B4:A5:D8:DD:C3:4A:1A:F9

Authority Key Identifier

70:C1:95:FA:5D:A5:16:BE:62:E8:A4:7D:E3:D4:64:5F:C4:E1:3E:9D

Authority Info Access

http://www.camerfirma.com/certs/ac_camerfirma.crt

Subject Alternative Name

caracer@camerfirma.com

Issuer Alternative Name

ac_camerfirma@camerfirma.com

Certificate Policies

Policy OID: 1.3.6.1.4.1.17326.10.8.1

CPS pointer: http://cps.camerfirma.com/cps/racer.html

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

F1:71:21:77:93:5D:BA:40:BD:BD:99:C5:F7:53:31:9C:F6:29:35:49:B7:28:47:41:E4:39:16:AD:3B:FB:DD:75

X509SubjectName**Subject CN:**

RACER

Subject O:

AC Camerfirma SA

Subject SERIAL NUMBER:

A82743287

Subject L:

Madrid (see current address at www.camerfirma.com/address)

Subject E:

caracer@camerfirma.com

Subject C:

ES

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2017-07-21T00:00:00Z

11.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en]

undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.4.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA AC Racer

Name	[es]	Certificados Reconocidos emitidos por la CA Racer

Service digital identities**X509SubjectName**

Subject CN:	RACER

Subject O:	AC Camerfirma SA

Subject SERIAL NUMBER:	A82743287

Subject L:	Madrid (see current address at www.camerfirma.com/address)

Subject E:	caracer@camerfirma.com

Subject C: ES

X509SKI

X509 SKI *vrwl1C66AEyA3CZntKXY3cNKGvk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

11.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA AC Racer*

Name [es] *Certificados Reconocidos emitidos por la CA Racer*

Service digital identities

X509SubjectName

Subject CN: *RACER*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at www.camerfirma.com/address)*

Subject E: *caracer@camerfirma.com*

Subject C: *ES*

X509SKI

X509 SK I *vrwl1C66AEyA3CZntKXY3cNKGvk=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2010-07-02T00:00:00Z*

11.4.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA*

Subject L: *MADRID (Ver en <https://www.camerfirma.com/address>)*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

Valid from: *Tue Feb 23 09:46:37 CET 2010*

Valid to: *Sun Feb 20 09:46:37 CET 2022*

Public Key:
30:82:01:20:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0D:00:30:82:01:08:02:82:01:01:00:DC:36:AE:43:33:75:F4:0D:47:9A:8B:D2:AC:EE:56:3A:8A:29:A1:20:ED:EF:89
F9:A2:9E:B0:DD:94:29:28:A2:63:21:16:AE:E8:13:D4:3A:5F:99:64:A3:DE:7E:9A:90:A5:46:6F:E7:0F:55:EA:04:E4:DA:D3:85:80:63:2B:DC:AC:85:D1:1F:41:7A:BC:42:29:F3:A7:B0:DC:8F
02:2D:4B:56:75:E1:86:E7:99:B6:C5:C0:9C:48:A3:AB:78:60:DD:71:DF:F3:F9:4B:20:75:AB:9E:AE:1B:DB:24:6D:42:99:B0:2B:D6:85:A5:99:50:AF:DC:CD:D8:5A:E7:F4:DB:E4:17:F7:AC
A5:FF:13:2A:40:00:5C:7F:33:6B:9C:AE:0B:68:B9:99:35:C7:E8:85:B1:4C:29:B4:DE:47:E8:54:94:69:53:7D:BD:25:D3:51:44:81:A3:86:08:FE:C9:31:EA:8A:0E:74:4C:36:7D:4A:7B:B7:C8:A
9:FF:B3:E2:80:A8:AF:65:F8:05:07:21:6A:A0:3A:61:20:86:B6:13:8F:35:C2:18:4A:4F:BF:64:F2:10:05:CE:86:CC:D7:DE:FC:CD:C1:28:60:7F:C4:A5:CF:D7:78:1F:54:DF:12:C5:21:D3:66:E6
5D:B6:DE:F0:6E:54:8B:26:CD:63:4B:CD:02:01:03

Basic Constraints *IsCA: true - Path length: 2*

CRL Distribution Points
*<http://crl.camerfirma.com/chambersroot.crl>
<http://crl1.camerfirma.com/chambersroot.crl>*

Subject Key Identifier *E5:46:50:E8:43:A0:B2:F7:1C:E4:B6:FF:D8:00:04:20:F7:1F:A4:0B*

Authority Key Identifier *E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A*

Authority Info Access
*<http://www.camerfirma.com/certs/ROOT-CHAMBERS.crt>
<http://ocsp.camerfirma.com>*

Subject Alternative Name *[]*

Issuer Alternative Name *chambersroot@chamberssign.org*

Certificate Policies
*Policy OID: 1.3.6.1.4.1.17326.1.3.1
CPS pointer: <https://policy.camerfirma.com>
CPS text: [Certificado raíz. Consulte las condiciones de uso en <https://policy.camerfirma.com>]*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *83:90:E7:03:57:E9:B5:73:CA:3D:D2:9D:BD:DC:23:7E:CA:F9:36:78:2C:A3:38:9C:7
9:43:FB:C2:B7:FA:A0:B6*

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP*

Subject SERIAL NUMBER: *A82743287*

Subject OU: AC CAMERFIRMA

Subject L: MADRID (Ver en <https://www.camerfirma.com/address>)

Subject O: AC CAMERFIRMA S.A.

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2017-07-21T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

11.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

11.5.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name *[en]* *Qualified Certificates issued by the CA Camerfirma Public Administration*

Name *[es]* *Certificados Reconocidos emitidos por la CA Camerfirma AAPP*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA*

Subject L: *MADRID (Ver en <https://www.camerfirma.com/address>)*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

X509SKI

X509 SK I *5UZQ6EOgsvcc5Lb/2AAEIPcfpAs=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2016-06-30T22:00:00Z*

11.5.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

11.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

11.5.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by the CA Camerfirma Public Administration*

Name *[es]* *Certificados Reconocidos emitidos por la CA Camerfirma AAPP*

Service digital identities**X509SubjectName**

Subject CN: *AC CAMERFIRMA AAPP*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA*

Subject L: *MADRID (Ver en https://www.camerfirma.com/address)*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

X509SKI

X509 SK I *5UZQ6EOgsvcc5Lb/2AAEIpcfpAs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-22T00:00:00Z*

11.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

Issuer C: *EU*

Subject CN: *Camerfirma AAPP II - 2014*

Subject L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

Valid from: *Tue Dec 16 12:59:01 CET 2014*

Valid to: *Tue Dec 15 12:59:01 CET 2037*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:F8:63:F6:EB:C4:3A:19:BA:EC:7F:E7:4D:2B:D0:19:23:B9:EF:10:7B:3A:31:2B:34:91:B3:DC:42:DE:22:FE:9B:16:D6:B6:A1:CC:DC:1D:7E:C8:EE:27:36:3B:9F:A9:11:7B:47:76:0E:45:E0:A3:CE:78:B0:DB:7E:1B:46:F4:67:2C:BA:83:1F:BE:36:AA:6D:47:01:03:C2:0F:C2:47:6D:78:D9:DF:53:56:99:56:64:0D:0A:84:30:C1:46:E3:84:74:3C:D4:DF:FE:6F:86:D2:ED:3B:C7:31:F9:A6:2D:F9:62:79:AA:D5:1A:34:C7:58:7B:B3:0A:D4:26:89:28:50:96:6D:7E:BD:25:D3:4F:51:AD:2C:69:98:84:61:28:A3:0F:49:7D:24:25:34:F6:13:76:71:58:9D:5B:F6:6C:0D:54:79:F9:99:F3:EB:3F:A2:40:55:DF:CD:2C:11:79:B4:F6:B8:41:43:73:54:8D:88:1E:23:67:4F:67:F3:70:80:2D:42:D9:3D:69:85:25:F5:06:61:C7:A2:FA:74:0D:D9:92:99:65:26:60:9A:6A:B0:74:D4:56:A0:B6:27:35:71:90:26:F1:63:CB:D6:17:20:22:13:BC:24:57:54:B7:D4:F0:44:F0:08:C3:60:EA:A2:D1:F4:4F:C1:63:9F:77:E1:BC:AA:9D:16:A3:DA:1F:30:40:59:BF:0F:C3:12:43:81:CF:5B:CB:CE:8E:BD:94:E2:A5:C5:0C:8F:6D:D6:D1:52:F9:1F:BC:E4:28:88:CD:29:86:CB:1B:1F:71:FF:82:A6:21:83:B5:EB:30:34:DE:64:A5:CD:5F:50:2C:06:07:FD:DB:62:96:45:66:CF:43:59:F8:48:75:16:4E:6C:58:7F:92:82:48:05:69:04:EB:C8:F7:2C:6E:E7:34:6A:94:CD:3E:FF:90:1E:20:1C:0B:A8:8C:5D:B1:E6:59:51:63:48:61:B5:E6:72:21:E6:13:38:5B:CD:E0:F6:58:82:E6:32:3B:89:42:21:97:CF:47:0D:94:89:2A:5F:1A:82:1E:1B:51:FA:1B:F7:8A:9B:44:71:D3:B5:85:51:C1:E6:1F:D2:9D:F0:2F:37:BC:CD:46:5E:B2:65:E4:39:6F:0A:10:1B:8B:3C:0C:F8:57:0B:03:49:00:3F:75:15:30:AA:DA:CA:2F:8E:97:A8:31:08:40:08:1B:D3:24:DC:BD:BA:19:31:23:1C:3B:78:41:C9:CD:26:CF:AF:5D:A2:CC:0B:5C:26:BD:D0:6C:68:B0:7D:96:89:06:4E:0C:46:1F:C7:39:2B:36:7D:E1:39:F0:F7:2E:92:F3:F3:EE:EB:5D:F7:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *5D:A1:55:A4:DC:4A:AC:83:11:F9:AA:38:E5:F7:68:4A:FE:15:15:4C*

Authority Key Identifier *F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*

Authority Info Access
http://www.camerfirma.com/certs/root_chambers-2008.crt
<http://ocsp.camerfirma.com>

Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://policy.camerfirma.com>

CRL Distribution Points
<http://crl.camerfirma.com/chambersroot-2008.crl>
<http://crl1.camerfirma.com/chambersroot-2008.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *72:39:D2:F7:70:FA:FF:3B:1C:F8:BE:2A:05:EC:03:ED:EA:AC:05:3B:55:4F:90:D3:69:21:15:5B:A8:05:19:81*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time 2017-07-21T00:00:00Z

Scheme Service Definition URI

URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

11.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.6.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014
Name	[es]	Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014

Service digital identities

X509SubjectName

Subject CN:	Camerfirma AAPP II - 2014
Subject L:	Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SKI XaFVpNxKrIMR+ao45fdoSv4VFUw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

11.6.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

11.6.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

Name [es] Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014

Service digital identities

X509SubjectName

Subject CN: Camerfirma AAPP II - 2014

Subject L: Madrid (see current address at <https://www.camerfirma.com/address>)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SK I XaFVpNxKrIMR+ao45fdoSv4VFUw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2015-07-07T00:00:00Z

11.6.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

11.7 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016

Subject CN: *AC CAMERFIRMA AAPP - 2016*
Subject O: *AC CAMERFIRMA S.A.*
Subject SERIAL NUMBER: *A82743287*
Subject OU: *AC CAMERFIRMA AAPP - 2016*
Subject OU: *see current address at <https://www.camerfirma.com/address>*
Subject ST: *MADRID*
Subject L: *MADRID*
Subject C: *ES*
Valid from: *Thu Feb 18 11:42:46 CET 2016*
Valid to: *Fri Jan 13 11:42:46 CET 2040*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B0:13:83:13:08:A8:86:EA:12:C0:3C:CE:C7:2C:8A:5D:17:E5:B4:AC:F5:56:BB
 BF:A1:FC:E9:C5:61:F7:98:91:3A:6E:73:E3:8F:88:50:93:88:59:A1:2C:63:FC:02:39:B9:94:A2:E5:C5:A9:83:4D:8D:59:02:E0:88:81:AA:00:8E:65:37:3C:6A:4D:9B:E6:71:2F:7A:CC:68:F1:6
 1:B3:BF:51:56:5C:B2:D0:C7:B3:E3:04:5B:90:9F:25:6C:7E:9E:6A:31:ED:33:11:35:18:7F:8C:4A:A0:35:38:D7:D3:DA:66:E9:8F:EC:0A:D5:3D:F8:B0:D7:4D:2A:7C:73:E6:43:7B:32:53:6D:D
 A:97:90:93:23:D5:43:CA:7F:AE:68:CE:F6:89:A7:7C:18:32:16:56:87:A2:DD:07:AC:0C:0D:01:A8:7F:86:BB:C4:C8:FA:8E:10:50:C9:86:DA:73:6C:D0:1A:16:C6:3C:79:7A:17:38:83:45:A3:F4
 35:80:53:EA:54:E4:66:17:89:12:DE:B1:E3:EA:58:E3:2A:9E:2D:5E:92:38:E3:75:28:FC:A5:8F:D3:21:86:6A:AE:87:A3:C1:50:EE:C7:D2:AB:FE:B7:D4:63:D2:A2:C9:34:32:67:8A:A2:B1:EC:8
 B:FD:E0:AF:E2:45:1E:44:06:15:1F:3A:DE:3C:57:2C:3E:DD:2B:1C:8B:7A:0E:C0:FF:1F:6D:6E:25:08:78:68:85:92:59:B9:65:4D:40:8B:AF:89:A9:06:A8:70:CB:C0:CF:F1:8E:CE:6F:5A:89:72:
 2E:66:4A:F0:4E:8D:2B:43:6F:81:63:3F:C3:FB:6C:16:AD:9D:FE:7A:18:C7:1F:44:0F:EE:05:36:0C:FB:C2:03:C3:55:EE:0E:12:CE:40:0E:64:AB:FC:E6:04:6A:CF:51:C3:E1:BF:CA:12:62:FD:32:
 5B:37:FD:F8:5C:7D:7E:5B:D1:F8:43:3F:62:9A:9C:12:EE:7B:C8:BE:1A:F9:C4:82:49:7B:B2:9D:67:45:AC:9C:1D:81:A7:DD:8B:E3:26:CF:F5:A2:84:BE:BF:C2:0B:6F:E4:74:5D:0D:8C:B7:5B:A
 A:1F:95:76:0D:FD:F8:8C:1F:59:47:6B:3E:72:88:56:93:94:08:8D:FA:12:2A:E4:16:73:8B:D5:DE:73:68:97:B2:56:43:D7:AD:E0:85:A4:11:21:84:5B:E4:CC:47:A1:A8:31:79:31:12:11:2C:89:
 E7:7B:55:EC:85:3A:9E:A9:0D:A9:1D:CB:86:7C:87:8D:1D:02:8E:F1:86:B1:03:47:DF:B0:31:18:C5:32:E7:EB:A4:75:A6:7B:D9:48:52:7F:B9:5A:24:FE:11:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 2*
Subject Key Identifier *8E:B6:48:04:67:95:0E:4F:99:1F:CA:25:32:C8:86:21:32:51:9A:1F*
Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*
Authority Info Access *<http://www.camerfirma.com/certs/chambersofcommerceroor-2016.crt>
<http://ocsp.camerfirma.com>*
Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0
 CPS pointer: <https://policy.camerfirma.com>*
CRL Distribution Points *<http://crl.camerfirma.com/chambersofcommerceroor-2016.crl>
<http://crl1.camerfirma.com/chambersofcommerceroor-2016.crl>*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *B9:CC:D2:5E:63:36:48:F4:56:21:53:16:31:8B:6C:F4:52:C8:E0:76:DB:C6:F2:B1:32
 :1F:D8:39:2A:91:72:66*
X509SubjectName

Subject CN: AC CAMERFIRMA AAPP - 2016

Subject O: AC CAMERFIRMA S.A.

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA AAPP - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject ST: MADRID

Subject L: MADRID

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2017-07-21T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

11.7.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

11.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**11.7.3 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

*Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016***Name**

[es]

*Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016***Service digital identities****X509SubjectName****Subject CN:***AC CAMERFIRMA AAPP - 2016***Subject O:***AC CAMERFIRMA S.A.***Subject SERIAL NUMBER:***A82743287***Subject OU:***AC CAMERFIRMA AAPP - 2016***Subject OU:***see current address at <https://www.camerfirma.com/address>***Subject ST:***MADRID***Subject L:***MADRID***Subject C:***ES***X509SKI****X509 SK I***jrZIBGeVDk+ZH8oIMsiGITJRmh8=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time***2016-06-30T22:00:00Z***11.7.3.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description**

[en]

undefined.

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.1.3.3.1*

11.7.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.7.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016*

Name [es] *Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA AAPP - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA AAPP - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *jrZIBGeVDk+ZH8oIMsiGITJRmh8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time

2016-04-01T00:00:00Z

11.7.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

11.8 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Camerales - 2016

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by the CA Camerfirma Camerales - 2016
Name	[es]	Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016

Service digital identities**Certificate fields details**

Version:	3
Serial Number:	5368777926801035574

Valid to: *Fri Jan 13 12:02:18 CET 2040*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B7:E2:80:96:86:06:48:4F:D7:22:38:34:80:03:7A:4D:B5:DB:46:ED:80:1E:1E:11:DE:00:74:F0:58:02:F8:DB:8A:1F:43:D5:97:B4:20:8E:0D:A0:53:E2:D0:7F:23:77:95:E9:D9:BA:A8:66:9D:25:21:14:7D:E9:DC:EB:01:1A:61:72:89:3C:A5:5A:2C:C8:1E:6A:6E:96:13:F7:4A:21:4F:6A:87:8F:67:96:06:1F:D7:94:CE:6D:CB:3A:ED:82:62:D0:75:8D:9B:29:30:8C:59:EA:AC:1F:65:64:46:D6:45:38:81:8A:5B:F0:A7:A6:3C:98:04:A4:5D:8A:FC:98:02:37:F0:5D:0B:CD:1F:F5:0D:E7:F1:BC:9D:55:5E:06:CD:47:6E:7C:8F:3E:1E:A3:9D:F5:05:B8:AB:0E:6E:33:AB:80:14:8B:25:E6:F5:66:F6:E0:94:E7:F9:5B:1D:CA:8F:5D:F2:B2:BB:8F:22:B9:4D:00:1F:46:98:30:47:10:68:5A:C9:F7:94:86:E8:16:48:AD:9D:E9:1C:9D:EC:63:D4:28:DF:C0:60:78:77:83:7A:A5:19:F8:E6:79:13:E6:4F:88:EE:01:38:84:E4:90:5C:C6:08:1A:AB:AC:65:DA:8F:69:D3:A4:BD:83:46:99:F9:EA:4C:91:07:10:ED:7B:44:69:99:AA:F2:B4:82:83:8F:F5:AB:A4:AF:32:25:4D:F5:91:8E:D8:B3:4D:A6:75:FE:52:88:A2:91:15:21:18:0C:D9:47:AC:25:61:AE:88:41:15:EB:A4:71:0C:DF:AB:FC:CB:37:D2:22:F2:23:14:04:F8:3D:83:D9:CD:3C:81:CB:95:DA:12:95:FD:F8:CE:68:CD:05:A5:93:CD:88:11:59:2B:6E:49:93:09:D6:E5:9C:75:45:86:1D:88:55:FC:EE:E4:EE:25:E7:F2:D3:03:AA:04:CB:C9:F4:15:CB:2D:3E:7D:C5:58:1F:61:78:92:0C:86:F7:40:39:06:96:78:19:73:C1:73:84:24:7D:B7:2F:C8:C8:24:F8:3B:03:6E:E9:A1:33:70:40:68:C8:56:86:CB:6F:2A:11:2A:74:C1:2F:19:A4:1C:0C:C9:88:3E:BE:4E:75:0B:B4:2C:52:96:0B:6C:BB:ED:AF:AF:90:9B:3B:A3:45:D0:48:CF:FE:CE:AC:B7:6A:70:47:62:2C:19:B2:D1:53:9B:56:EB:BB:78:7C:CC:4B:4D:2A:E4:BA:63:D6:09:42:EB:CF:34:02:2F:02:0C:26:2F:AD:50:E9:20:AF:F7:E5:30:0E:E7:C8:51:CF:5F:BD:2F:2E:8E:BB:BE:3C:9E:EC:68:52:4B:23:09:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *97:A3:58:24:76:6C:09:9F:1A:E4:9F:AE:26:29:77:34:D3:84:D4:EF*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access *http://www.camerfirma.com/certs/chambersofcommercerooot-2016.crt*
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points *http://crl.camerfirma.com/chambersofcommercerooot-2016.crl*
http://crl1.camerfirma.com/chambersofcommercerooot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *42:38:89:2F:E2:D3:34:A1:18:40:86:55:D6:9B:9F:A5:5D:81:A2:53:B1:28:D5:22:54:89:46:F9:DB:0A:F6:69*

X509SubjectName

Subject CN: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] undefined.

Status Starting Time 2017-07-21T00:00:00Z

11.8.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.8.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by the CA Camerfirma Camerales - 2016

Name [es] Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

Subject O: AC CAMERFIRMA S.A.

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I I6NYJHZsCZ8a5J+ujil3NNOE1O8=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

11.8.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.8.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**11.8.4 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [en] *Qualified Certificates issued by the CA Camerfirma Camerales - 2016***Name** [es] *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016***Service digital identities****X509SubjectName****Subject CN:** *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016***Subject O:** *AC CAMERFIRMA S.A.***Subject SERIAL NUMBER:** *A82743287***Subject OU:** *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016***Subject OU:** *see current address at <https://www.camerfirma.com/address>***Subject L:** *MADRID***Subject ST:** *MADRID***Subject C:** *ES***X509SKI****X509 SK I** *I6NYJHZsCZ8a5J+ujil3NNOE1O8=***Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time** *2016-04-01T00:00:00Z***11.8.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

11.9 - Service (withdrawn): Qualified Certificates issued by CA AC Racer-2016

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en]

Qualified Certificates issued by CA AC Racer-2016

Name [es]

Certificados Reconocidos emitidos por la CA Racer-2016

Service digital identities

Certificate fields details

Version: 3

Serial Number: 9748782597291380995

Valid to: *Wed Dec 14 17:10:18 CET 2039*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A4:81:41:D5:39:E7:61:BA:4E:1C:8C:EC:4E:8C:C6:0B:C7:87:92:B3:04:47:1D:28:FE:6E:5D:F2:1E:45:88:45:9F:9F:EC:68:B1:29:EC:8B:28:9A:63:FE:48:DC:34:0C:93:84:00:51:49:55:AB:D4:09:9D:EE:D2:FA:46:4A:8B:FF:70:68:DF:3F:EA:28:12:88:2B:8A:49:47:F3:B7:1B:A3:5A:8C:FD:27:D9:58:6A:DF:28:9E:BA:EB:95:D9:4D:43:08:5E:DF:9A:2A:DC:B5:56:F9:28:BB:D3:9B:5E:A0:73:72:75:32:C9:82:3A:4B:AE:EA:8C:52:16:50:56:8C:71:4C:37:6E:C1:E3:FC:D5:4C:51:D2:14:43:82:24:AB:9C:F5:F9:55:F5:DA:C9:89:E8:AB:04:16:0A:B5:94:33:7F:60:EA:2F:D6:A3:5E:F7:A3:7F:5F:1C:03:53:54:4F:7A:6E:59:FD:16:12:5C:81:1D:4D:17:3F:90:7B:61:2E:26:A9:FC:DB:66:5E:43:A7:5C:51:60:4C:ED:67:7D:14:A7:EB:66:08:9C:0F:1D:46:83:A6:F7:4A:14:A3:66:48:63:30:FD:01:3F:C1:F1:A6:06:E3:9F:79:03:A9:8C:60:AC:41:7E:71:15:84:BE:70:34:E3:80:27:70:D2:B9:6F:66:4E:07:36:FA:62:58:21:F3:10:8C:2E:A5:9F:DB:23:65:E1:A4:5F:2E:D8:18:43:63:5D:2A:C9:A4:F2:27:D5:47:D5:85:CE:38:C3:D7:38:D5:DB:62:57:25:66:92:33:E4:3D:50:D4:6E:4A:66:96:A4:CC:B4:E3:62:3C:FA:7C:81:B1:7B:86:28:14:F4:DF:50:C5:7E:60:10:E5:5C:A5:71:96:9D:55:CD:72:98:50:3A:78:3F:53:86:F1:9B:A6:1A:CF:D5:C8:7D:24:82:7A:9E:6E:0A:97:02:12:CB:75:3A:E7:60:DA:D9:DA:EF:69:D2:E3:E6:DF:7C:09:AF:DB:38:D3:95:B7:8D:BE:E7:37:BA:E8:D4:D1:56:5F:0D:55:FF:4D:24:A4:2E:19:19:DB:23:96:B2:AD:B3:42:34:65:76:AB:B7:F3:3D:F6:6F:49:15:43:EA:7A:12:C5:8F:AD:E2:9C:70:90:65:98:B4:69:58:7D:43:67:F9:63:3C:96:D6:2C:4F:0A:13:CB:A4:1D:7A:6C:C5:58:91:1A:F6:EB:08:EC:C0:12:5E:47:E8:86:67:41:C6:49:F4:15:E7:1F:10:28:C4:52:C4:EA:BE:8E:8B:C4:59:5A:5A:C4:F2:D9:C4:58:C8:E2:BC:F2:3B:18:85:3A:CD:45:2C:9F:1F:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 1*

Subject Key Identifier *BB:71:68:C8:7B:3F:A5:63:BC:06:E5:0A:AA:5B:3A:46:6A:62:68:4C*

Authority Key Identifier *08:28:6E:C7:17:02:0D:DF:4D:EF:C9:A2:77:AD:59:68:2D:5D:DF:45*

Authority Info Access
http://www.camerfirma.com/certs/ac_camerfirma-2016.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/ac_camerfirma-2016.crl
http://crl1.camerfirma.com/ac_camerfirma-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A7:9D:0E:26:DB:A2:4A:A6:FC:B0:A4:7C:44:C7:CA:F6:F4:F5:DD:DE:F0:34:11:59:2D:4B:21:07:E1:0A:C7:2B*

X509SubjectName

Subject CN: *RACER - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *RACER - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] undefined.

Status Starting Time 2017-07-21T00:00:00Z

11.9.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.9.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA AC Racer-2016

Name [es] Certificados Reconocidos emitidos por la CA Racer-2016

Service digital identities

X509SubjectName

Subject CN: RACER - 2016

Subject O: AC CAMERFIRMA S.A.

Subject SERIAL NUMBER: A82743287

Subject OU: RACER - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I u3FoyHs/pWO8BuUKqls6RmpiaEw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

11.9.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**11.9.4 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [en] *Qualified Certificates issued by CA AC Racer-2016***Name** [es] *Certificados Reconocidos emitidos por la CA Racer-2016***Service digital identities****X509SubjectName****Subject CN:** *RACER - 2016***Subject O:** *AC CAMERFIRMA S.A.***Subject SERIAL NUMBER:** *A82743287***Subject OU:** *RACER - 2016***Subject OU:** *see current address at <https://www.camerfirma.com/address>***Subject L:** *MADRID***Subject ST:** *MADRID***Subject C:** *ES***X509SKI****X509 SK I** *u3FoyHs/pWO8BuUKqls6RmpiaEw=***Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time** *2016-04-01T00:00:00Z***11.9.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

11.10 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Name [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Service digital identities

Certificate fields details

Version: 3

Serial Number: 5859548927499719925

Subject C: *ES*

Valid from: *Thu Apr 14 10:48:09 CEST 2016*

Valid to: *Fri Mar 09 09:48:09 CET 2040*

Public Key:

```

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:72:2B:E5:7E:D8:38:34:88:1C:45:C9:22:EF:B9:1C:9D:9D:80:93:99:1E:15
C8:C0:B7:16:0B:09:1B:19:47:24:CD:7B:89:09:02:8B:8B:CB:A0:EE:77:27:23:6D:73:E1:42:F7:A2:1A:D6:1B:FF:DA:E8:5C:AB:35:2A:06:AD:16:EA:3C:B2:4F:79:C7:24:50:89:8B:5E:6C:70:
DA:3F:D1:D1:95:51:D0:03:10:9D:5C:47:72:5A:5B:E6:23:34:8B:2B:E4:04:D6:A3:D0:B6:AC:A6:FF:26:32:86:2D:E4:C9:3A:63:05:7D:7C:4D:47:8C:AF:78:4B:90:C0:B1:C7:E8:E4:D9:74:09:
46:B6:CF:23:83:8B:DF:DF:CE:75:F8:75:D2:75:9A:B7:21:DD:13:84:F0:EF:44:20:1B:66:B9:C4:E5:35:8A:CB:F3:E2:01:C5:DC:39:C8:A9:2D:13:D1:40:B2:6D:97:C1:71:09:5A:A2:30:81:33:0
6:08:F8:66:62:26:FC:93:5C:08:A8:C7:1C:28:73:CD:DD:15:98:75:D3:D4:3C:4E:D3:20:97:3E:58:37:17:8D:F9:8D:72:85:D8:75:8E:82:C2:CC:1D:39:C9:7A:7B:00:04:56:15:E6:68:2A:F8:A
5:8B:83:C4:AD:C6:E4:67:7A:3A:DE:E9:D0:26:88:87:04:2A:84:81:90:D2:CF:54:24:DF:49:3F:2E:7E:CB:4A:CA:95:64:E2:EF:17:02:D8:4D:44:12:52:B7:6F:7A:2A:F9:C2:5E:30:F5:EC:CC
79:0F:10:93:8E:F2:56:10:17:C1:C8:1A:A4:53:78:5A:BE:F9:FE:6A:6C:8E:C7:0D:30:C3:E8:9F:C5:E0:4B:18:81:B9:07:C0:25:F6:03:F4:72:5C:28:0C:29:B8:6F:E8:9D:38:57:82:AF:64:43:5F:
20:E3:04:7B:7B:0A:DF:05:91:F9:C2:89:40:E9:04:88:78:5E:38:B3:72:19:01:C3:58:B9:26:24:56:0F:1C:74:35:7E:CB:4F:C4:BF:54:83:62:66:FE:2E:33:A4:D5:26:F6:52:D7:AE:0E:5A:98:CD
2B:CF:BF:C6:3A:4F:A2:7D:74:44:A8:31:14:AE:B6:2E:85:18:DA:62:CB:B8:78:56:CA:3E:47:59:D2:CE:78:6E:D1:3D:88:76:C7:1B:25:AA:69:9E:C0:7B:A2:A1:70:BA:21:CE:9A:75:D3:30:AF:
82:16:07:34:24:18:35:D3:12:E7:3B:01:6F:E4:EA:72:7E:70:EC:DD:0A:24:37:AC:30:99:C2:7D:1F:31:2B:36:16:47:DE:1A:E5:DD:15:92:A6:34:61:2C:3C:19:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *70:B8:F8:24:C7:51:CA:CE:22:80:92:08:C9:C0:68:2F:C1:47:58:51*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access
http://www.camerfirma.com/certs/chambersofcommercerooot-2016.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/chambersofcommercerooot-2016.crl
http://crl1.camerfirma.com/chambersofcommercerooot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EE:DD:45:7A:F1:35:3D:76:F4:8E:7C:61:23:F3:91:40:E5:F9:A0:69:CA:51:B4:3E:EA:86:15:C9:CE:C0:D4:BB*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

11.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.10.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.17326.99.18.1*

Description

11.10.3 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Name *[es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject ST: MADRID

Subject L: MADRID

Subject C: ES

X509SKI

X509 SK I cLj4JMdRys4igJllycBoL8FHWFE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2016-06-23T22:00:00Z

11.11 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Name [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Service digital identities

Certificate fields details

Version: 3

Serial Number: 6102780882998024770

Subject C: *ES*

Valid from: *Thu Apr 14 10:33:07 CEST 2016*

Valid to: *Fri Mar 09 09:33:07 CET 2040*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CE:58:D7:7F:64:52:80:6E:00:7E:66:1B:02:C8:D8:A0:37:EA:FB:83:F9:C2:0C:73:81:F3:CC:54:FC:E4:67:A1:18:4E:8F:22:83:4C:D2:1A:D2:87:F5:E1:17:EA:22:01:EA:32:CE:41:AD:68:08:67:68:66:19:9A:56:D6:FF:FA:71:8D:DE:B1:EC:31:D9:CA:AB:89:A9:F0:F8:F5:A3:EC:13:02:DF:7A:95:9E:78:56:D2:6C:9E:2D:30:14:36:97:6A:52:9B:13:E3:35:8A:00:79:EB:30:F2:17:21:4E:06:4D:CE:0F:A3:5A:FD:1C:2F:F1:F9:06:FF:5C:CD:51:51:29:93:80:CE:E4:8D:0A:A9:F3:DD:D8:C6:5B:4E:01:04:15:68:64:DD:7D:6E:DB:8F:69:07:5F:82:19:72:29:31:82:9F:27:17:A0:BE:08:E4:D4:59:11:49:BE:29:BB:84:61:D7:F2:68:64:38:A3:48:8B:6E:68:71:64:75:DD:F8:8F:89:15:9D:F0:C3:83:84:03:4E:CA:D4:53:72:21:91:E8:49:13:D8:69:27:44:F7:B7:49:5C:93:2A:F4:8D:AE:CD:C4:0F:AA:4D:4A:24:EA:F1:10:B4:EC:4F:45:09:50:ED:1E:A6:7C:10:7A:57:95:4D:5E:29:7F:7D:DA:F5:CB:97:73:B1:D1:8D:41:80:68:93:2D:85:35:84:52:14:81:83:E2:10:79:A3:1E:81:5A:32:C4:09:52:2D:24:56:87:EA:1F:E4:62:84:03:95:F2:79:53:39:80:8D:B9:56:1B:61:59:5F:6F:5F:73:5D:94:40:64:92:73:70:57:1E:08:54:17:E9:86:F0:6E:48:CE:88:A7:9F:EC:4B:80:ED:1E:FE:7C:CC:18:52:03:86:9C:23:1C:D3:CC:A5:7D:B2:F2:39:80:DD:A0:18:53:4F:62:FF:25:01:C5:A0:35:B9:16:A6:9A:91:05:4D:C4:0E:B2:4C:F8:19:84:1A:C8:E8:FD:5C:F6:28:8A:22:46:81:87:65:1F:2F:D3:24:81:F8:12:A0:96:84:DD:53:6F:EE:13:00:53:28:C D:31:93:B8:1E:BD:AC:7C:10:81:9A:81:DA:4A:9F:66:CE:9C:02:BC:B2:EC:37:E9:5E:BD:E6:D5:10:B0:F1:8A:51:E7:97:41:3C:10:51:96:B1:4C:78:AA:CA:79:58:65:55:C6:DE:42:CD:62:B2:82:D1:9B:86:AC:36:6D:86:E6:14:DA:91:22:41:6C:48:42:44:F2:3D:AD:1F:02:39:28:01:B0:35:2D:4E:2B:82:45:AE:9E:B5:2A:1A:45:55:74:00:71:85:9A:17:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access
http://www.camerfirma.com/certs/chambersofcommercerooroot-2016.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/chambersofcommercerooroot-2016.crl
http://crl1.camerfirma.com/chambersofcommercerooroot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *3A:80:66:26:6D:28:BD:28:CC:D0:F5:64:C8:FB:C1:21:9B:4F:FA:E4:03:E0:1E:50:39:D3:0F:24:00:F0:EB:09*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject ST: *MADRID*

Subject L: MADRID

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2018-03-15T01:00:00Z

11.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

11.11.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.17326.99.18.1

Description

11.11.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Name [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Subject O: AC CAMERFIRMA S.A.

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at <https://www.camerfirma.com/address>*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2017-07-21T00:00:00Z*

11.11.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

11.11.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

11.11.4 - History instance n.2 - Status: granted

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

Service Name

Name *[en]* *Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Name *[es]* *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at <https://www.camerfirma.com/address>*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2016-06-30T22:00:00Z*

11.11.4.3 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2</i>

11.11.4.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.11.5 - History instance n.3 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Name	[es]	Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Service digital identities**X509SubjectName**

Subject CN:	AC CAMERFIRMA FOR LEGAL PERSONS - 2016
Subject O:	AC CAMERFIRMA S.A.
Subject 2.5.4.97:	VATES-A82743287
Subject SERIAL NUMBER:	A82743287
Subject OU:	AC CAMERFIRMA FOR LEGAL PERSONS - 2016
Subject OU:	see current address at https://www.camerfirma.com/address
Subject ST:	MADRID
Subject L:	MADRID
Subject C:	ES

X509SKI

X509 SK I	wyeFk9cvlsUbrHYz2YaiSn1oFEI=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2016-06-23T22:00:00Z

11.11.5.5 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.12 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	<i>[en]</i>	<i>Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016</i>
Name	<i>[es]</i>	<i>Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016</i>

Service digital identities**Certificate fields details**

Version: 3

Subject ST: MADRID
Subject C: ES
Valid from: Thu Apr 14 17:13:34 CEST 2016
Valid to: Wed Feb 08 16:13:34 CET 2040
Public Key: 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AB:33:6D:B8:55:EB:1E:FE:4E:AD:37:DB:E5:C8:87:F1:78:6E:F6:93:0A:2B:0E:93:4C:C8:06:95:C3:26:FA:9A:0A:08:4A:C2:B3:AE:5B:C2:3B:F1:30:6D:1B:6C:54:1E:14:86:AE:B5:07:19:BD:79:B9:CE:CA:89:63:D7:6A:33:C3:5F:60:A2:A7:76:96:A3:D8:72:14:43:D2:EC:85:64:4B:6B:A6:8C:EE:E2:7D:91:CF:F4:69:88:64:1F:1D:D2:C2:91:4B:37:3E:8F:38:54:37:32:00:DB:6B:1C:C7:D0:95:37:53:CE:A4:F6:F8:E6:87:80:41:6D:21:90:2D:5D:10:55:4A:35:1D:16:D3:E4:0E:C2:27:1A:BC:D8:7E:29:F2:FD:80:13:EB:93:2C:58:64:1C:EE:6D:AS:BA:AF:6F:AC:3F:38:6E:33:6A:56:AF:66:E9:C6:EE:S1:60:46:0A:D5:FE:DE:99:DF:C4:FD:C6:C4:E2:DD:F5:00:4B:14:39:BE:98:8B:E9:CB:91:93:31:99:67:8E:34:2E:F6:DE:7A:43:43:30:75:9B:E6:E0:AD:FD:96:60:04:5E:38:D2:91:0F:89:35:88:80:9A:DA:F8:58:27:3D:22:C1:12:65:C8:53:CB:D5:C F:90:81:B9:B4:EE:9C:69:8C:29:98:E8:9D:23:8E:9D:6E:7A:3D:A1:B3:77:DD:89:FA:CD:62:CF:1E:B9:38:44:FE:95:75:E7:84:EA:14:72:1D:64:E6:AE:69:8E:BB:AD:DA:07:E4:68:E5:4D:C1:F0:24:4A:24:56:39:22:50:39:C5:B6:82:BE:50:4C:28:C5:ED:D3:4D:3A:2D:3F:65:0D:77:07:A0:3D:11:A9:86:6D:DA:DB:5E:40:1D:B5:8B:A0:9F:F7:52:71:A5:54:49:B7:73:D6:13:FD:5A:9F:5A:0D:C8:6D:BA:12:C0:C1:06:21:70:E0:3A:EA:51:70:29:07:9D:9E:C5:04:25:88:82:F1:B6:27:7C:DC:1F:8E:5C:43:F1:A3:54:CD:1D:A2:E2:07:04:4A:68:60:1F:7B:35:51:0C:66:3A:BE:91:E 4:9D:2C:D6:8B:D2:1C:22:AE:3A:A7:B0:0E:86:39:1C:5C:BD:3A:82:CD:DB:82:9B:4E:47:13:C0:A4:14:CF:ED:82:E7:0B:EB:DD:79:7C:5E:EC:26:63:B5:9B:2E:8F:B0:13:42:39:07:53:9D:B7:6 5:10:19:3C:ED:6B:58:E7:01:64:EA:A1:4B:A7:BF:B3:C9:32:3D:F8:56:D6:19:3F:D6:46:DE:C6:65:1F:13:59:1B:DC:B9:08:5B:B8:93:1C:A7:D4:DD:59:38:F6:8D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 1*
Subject Key Identifier *4E:36:56:A8:58:CE:1B:83:85:60:4C:D4:1B:A1:DF:72:3D:AF:7B:5F*
Authority Key Identifier *D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84*
Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma-2016.crt
http://ocsp.camerfirma.com*
Extended Key Usage *id_kp_clientAuth*
Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com*
CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma-2016.crl
http://crl1.camerfirma.com/ac_camerfirma-2016.crl*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *EF:41:1C:83:7A:C3:30:41:85:E5:39:13:FE:36:9B:F8:FF:65:98:C2:A5:2B:DB:1B:6E:2D:EA:B5:DC:C7:F0:6F*

X509SubjectName
Subject CN: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject O: *AC CAMERFIRMA S.A.*
Subject 2.5.4.97: *VATES-A82743287*
Subject SERIAL NUMBER: *A82743287*
Subject OU: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*
Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.12.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Name [es] *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *TjZWqFjOG4OFYEzUG6Hfcj2ve18=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

11.12.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	<i>Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016</i>

Name	[es]	<i>Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016</i>

Service digital identities

X509SubjectName

Subject CN: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Issuer CN: AC CAMERFIRMA - 2016
Issuer O: AC CAMERFIRMA S.A.
Issuer 2.5.4.97: VATES-A82743287
Issuer SERIAL NUMBER: A82743287
Issuer OU: AC CAMERFIRMA - 2016
Issuer OU: see current address at <https://www.camerfirma.com/address>
Issuer L: MADRID
Issuer ST: MADRID
Issuer C: ES
Subject CN: AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016
Subject O: AC CAMERFIRMA S.A.
Subject 2.5.4.97: VATES-A82743287
Subject SERIAL NUMBER: A82743287
Subject OU: AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016
Subject OU: see current address at <https://www.camerfirma.com/address>
Subject L: MADRID
Subject ST: MADRID
Subject C: ES
Valid from: Thu Apr 14 16:58:36 CEST 2016
Valid to: Wed Feb 08 15:58:36 CET 2040
Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C4:29:BB:37:DD:77:A9:84:03:83:0A:DE:86:B5:60:42:E9:E8:86:ED:C9:68:B9:20:34:4E:26:0E:A1:33:18:1F:E8:4C:54:A0:E5:34:44:68:B2:D4:E2:C9:C3:2C:F9:95:01:54:D5:1A:7A:23:6D:87:95:8D:63:C7:7C:8C:38:74:18:0A:3C:8D:95:3F:46:56:0C:98:53:B4:48:A0:DE:1A:EC:CB:3E:F3:C0:43:86:F5:19:D2:74:84:3C:6D:54:CB:AB:B2:AB:0E:AD:67:3B:C9:82:2F:24:3F:83:F9:E9:F4:F6:C5:68:A6:3A:FD:6D:46:65:DC:38:83:56:B1:B3:0F:F1:9C:41:EA:8C:D6:D8:3F:C2:FD:8A:D4:F8:C5:00:0E:7D:32:C8:5E:83:F5:11:2F:B9:13:56:0E:97:4B:D5:DD:98:E8:1F:BD:26:20:17:45:69:65:24:1D:80:99:EF:54:34:0C:CA:DF:37:C3:42:43:32:83:96:71:30:54:81:E9:82:A5:0C:00:53:02:98:87:36:9C:4C:0C:3F:E7:BA:B3:1B:E2:30:28:09:C1:E0:C9:76:8E:58:98:3E:2C:FD:FF:62:3A:A0:F1:58:07:03:5F:55:C7:F9:0A:AD:8E:FC:34:DC:59:0F:87:67:0B:51:F9:B1:19:44:9E:AA:F7:47:D2:F1:CB:40:F3:C3:53:F0:30:64:D8:C0:8D:F7:93:66:89:8F:92:D9:52:47:67:4D:96:2E:0D:54:CC:61:38:2F:A3:49:4D:AC:66:6D:0E:5E:91:E1:F1:8A:B3:F0:1C:7A:C6:57:37:AF:DA:35:AC:82:2A:D9:92:96:31:8D:BD:D0:FB:64:D0:12:E0:8B:BC:99:30:67:3A:FB:98:4C:26:44:63:0C:95:9D:63:1D:31:C8:6B:E2:44:14:40:A7:6F:4D:0B:B3:E6:1A:75:52:EE:91:E4:71:EB:07:83:58:40:9A:97:DD:51:6C:8C:93:C6:67:1C:9C:0F:C9:E3:CD:CF:43:0D:0C:5A:8A:9E:05:8B:2B:98:46:5C:0E:2B:AC:58:93:04:C8:86:38:1F:ED:C1:44:C4:E2:0F:DC:C9:EF:56:9F:6C:6B:BF:59:7C:92:A9:21:76:D9:5F:92:10:3D:EA:21:35:D2:1E:38:E0:1C:85:C7:7E:F6:88:E6:92:D:5A:83:EE:B8:AF:33:DF:48:19:62:61:E8:81:30:E3:9A:E0:18:D9:3D:BF:9E:77:32:F8:99:43:70:62:B4:D8:FA:0C:CB:DB:1D:D2:5E:0A:06:B8:EF:D5:7E:AA:81:59:CD:C2:0F:3C:09:86:75:67:69:D5:D7:E7:E2:91:6F:9A:80:04:CD:02:03:01:00:01
Basic Constraints IsCA: true - Path length: 1
Subject Key Identifier 80:21:DF:71:F1:EF:D4:6B:DA:33:86:D1:0F:BE:C5:DD:65:4C:84:5E
Authority Key Identifier D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84

Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma-2016.crt
http://ocsp.camerfirma.com*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com*

CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma-2016.crl
http://crl1.camerfirma.com/ac_camerfirma-2016.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4D:20:C9:51:E1:34:89:3B:C5:90:1B:FA:F8:E2:40:A5:BE:7D:00:59:6D:D3:1C:40:42:92:52:F2:E0:4F:8B:46*

X509SubjectName

Subject CN: *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.
[es] undefined.*

Status Starting Time *2017-07-21T00:00:00Z*

11.13.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.
[es] undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

11.13.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Name [es] *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Service digital identities**X509SubjectName**

Subject CN: *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SKI *gCHfcfHv1GvaM4bRD77F3WVMhF4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.13.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

11.13.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Name *[es] Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Service digital identities**X509SubjectName**

Subject CN: *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I gCHfcfHv1GvaM4bRD77F3WVMhF4=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2016-06-23T22:00:00Z

11.13.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2

11.14 - Service (withdrawn): Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

Subject C: *ES*

Valid from: *Thu Jan 15 10:21:16 CET 2015*

Valid to: *Tue Dec 15 10:21:16 CET 2037*

Public Key:
 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:87:9D:D2:8D:A4:58:9F:56:AF:6F:F8:5E:5D:46:84:FD:A1:59:20:C0:47:C3:76:C3:F0:D0:BC:B4:47:E7:8C:E4:C3:A4:DF:9C:C4:8A:5F:FE:96:A1:0C:6D:09:9C:BE:08:00:87:A2:3C:88:08:24:91:76:AC:AA:1F:92:31:83:08:8E:F5:D8:0F:23:48:2D:E1:B3:82:83:F4:BB:3D:B:84:73:3B:A0:DD:F2:1D:70:E1:85:DD:4D:18:DA:1C:3F:9E:16:7A:17:8D:F9:11:37:58:FD:32:10:4A:3E:0F:66:26:33:05:07:BA:FE:0A:89:7B:6F:7A:23:E4:B2:FF:97:92:4C:F9:6A:EA:A9:A4:F3:1A:62:50:FA:CB:8F:40:12:C1:98:DB:33:84:50:8F:0F:3B:8F:AD:3B:15:0A:86:F8:22:32:E5:9C:D7:BB:C7:DD:57:66:33:03:A3:45:ED:12:75:80:22:60:B4:08:8B:2A:89:18:D7:44:A3:7B:8E:7F:0F:14:5F:16:89:49:15:E1:98:5F:A3:32:7E:A3:80:DC:D6:58:D0:31:C7:00:0A:CB:DE:44:5E:5A:48:42:CC:7F:EE:DD:96:DA:7B:68:10:83:C7:18:99:38:57:EF:F2:03:47:76:A2:52:C4:A8:10:03:91:1B:4F:D8:78:82:D3:09:72:F8:3A:7B:38:69:A3:B5:F8:DB:A8:BA:D5:9E:6A:3F:98:B3:F7:CE:99:98:6E:95:2D:B9:BA:C7:89:8D:2B:95:6E:80:A3:91:59:2D:C4:D4:BD:C0:31:16:3C:4B:59:52:04:2C:F8:E7:4D:E6:CE:88:7B:E8:25:36:FD:EE:B8:40:D4:EA:AA:C2:8A:B9:15:62:47:14:8F:62:77:35:F3:14:B3:B4:2D:7F:F8:BA:02:3D:2D:95:B1:9A:F5:96:D0:EE:02:78:F8:67:86:9D:1A:34:4F:C6:80:0C:3A:94:CC:7B:6E:36:5E:0D:7C:71:42:75:03:10:4F:E6:02:A3:87:45:40:A7:8D:15:12:29:56:EE:04:11:34:A3:3E:5F:CF:79:D4:C1:C5:95:56:0A:E6:FE:39:20:A9:35:F8:12:A9:D9:7B:EC:81:98:A5:7A:84:51:18:57:ED:68:56:1E:E4:CC:D3:78:1E:0E:E7:CC:68:81:C9:2E:DC:0A:E0:44:C1:42:C5:85:F5:23:6B:50:6E:F4:4A:A0:9D:D2:77:09:5D:17:09:62:00:5D:58:49:9C:F3:4F:8B:AC:B8:5B:5D:63:2C:9E:D7:48:64:B3:DE:C0:A1:DB:58:34:1A:98:22:DA:95:C7:18:30:7A:E4:97:3F:40:91:D9:E5:96:87:0A:BC:C5:9F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34:65*

Authority Key Identifier *F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*

Authority Info Access
http://www.camerfirma.com/certs/root_chambers-2008.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/chambersroot-2008.crl
http://crl1.camerfirma.com/chambersroot-2008.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *66:EA:E2:70:9B:54:CD:D1:69:31:77:B1:33:2F:F0:36:CD:D0:F7:23:DB:30:39:ED:31:15:55:A6:CB:F5:FF:3E*

X509SubjectName

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time 2021-11-16T02:00:00Z

11.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

11.14.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Name	[es]	Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015

Service digital identities

X509SubjectName

Subject CN:	Camerfirma Corporate Server II - 2015

Subject L:	Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER:	A82743287

Subject O:	AC Camerfirma S.A.

Subject OU:	AC CAMERFIRMA

Subject C:	ES

X509SKI

X509 SK I	Y+nw8FYAaGWwIWwOXNcZCJ0INGU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2017-08-16T01:00:00Z

11.14.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation**URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication***11.14.3 - History instance n.2 - Status: withdrawn****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name***[en]**Qualified Certificates issued by Camerfirma Corporate Server II - 2015***Name***[es]**Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015***Service digital identities****X509SubjectName****Subject CN:***Camerfirma Corporate Server II - 2015***Subject L:***Madrid (see current address at <https://www.camerfirma.com/address>)***Subject SERIAL NUMBER:***A82743287***Subject O:***AC Camerfirma S.A.***Subject OU:***AC CAMERFIRMA***Subject C:***ES***X509SKI****X509 SK I***Y+nw8FYAaGWwIWwOXNcZCJ0INGU=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Status Starting Time***2017-07-21T00:00:00Z***11.14.3.2 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description***[en]**undefined.**[es]**undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier***[OIDsURN]**urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

11.14.3.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.14.4 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

Name [es] *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

Service digital identities**X509SubjectName**

Subject CN: *Camerfirma Corporate Server II - 2015*

Subject L: *Madrid (see current address at https://www.camerfirma.com/address)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject OU: *AC CAMERFIRMA*

Subject C: *ES*

X509SKI

X509 SK I *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.14.4.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es]

undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

11.14.4.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.14.5 - History instance n.4 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Name [es] Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015

Service digital identities**X509SubjectName**

Subject CN: Camerfirma Corporate Server II - 2015

Subject L: Madrid (see current address at https://www.camerfirma.com/address)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

X509SKI

X509 SK I Y+nw8FYAaGWwIWwOXNcZCJ0INGU=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2016-06-23T22:00:00Z

11.14.5.6 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

11.15 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016

Name	[es]	Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES - 2016

Service digital identities**Certificate fields details**

Version:	3

Serial Number:	2579987068168128523

Subject C: *ES*

Valid from: *Mon Apr 18 17:43:54 CEST 2016*

Valid to: *Tue Mar 13 16:43:54 CET 2040*

Public Key:
30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D3:35:56:9F:5D:AE:7A:67:3F:D4:0F:B4:57:B5:3E:68:F0:D6:8B:CB:E8:C2:6C:C0:68:0F:6F:A9:E1:19:CD:57:41:36:F6:49:DF:84:AB:68:D9:70:80:0C:92:26:52:00:5C:F3:96:09:7F:D8:1E:22:70:7C:CB:DD:BA:58:72:23:95:4E:1B:C3:BB:31:E3:A0:8A:0E:97:3F:8A:79:3F:61:69:C9:18:08:78:60:7F:4A:65:A7:6C:70:EB:27:31:4D:D8:74:FB:16:C8:8F:7E:26:E0:9F:D4:E6:19:2A:53:1D:F1:22:EA:F9:0E:E4:29:CE:DB:35:48:F4:2F:AA:31:A4:0A:4A:A3:E4:32:8B:2D:4A:F3:E7:4B:FE:48:0E:1E:68:A5:8C:49:27:4A:3E:EE:BE:7A:E7:12:A7:15:5C:4F:89:42:40:23:19:A2:CE:4F:F8:15:8D:AA:08:7A:CA:1D:4E:12:68:30:A7:C4:D2:B4:87:2C:3C:D0:0D:62:8A:EF:00:6E:AE:54:D0:08:45:21:59:28:97:0F:87:53:A1:46:CB:8E:4C:69:DD:80:89:07:CB:9E:8E:13:0D:27:FF:A8:EC:3E:B5:CC:2D:46:AE:FE:58:04:94:3B:88:82:AC:6A:4B:E6:18:D8:24:D8:84:8E:55:78:43:3A:A6:1E:05:46:2F:C4:E5:75:88:B7:59:1A:BE:EC:68:0A:25:9D:0F:EF:6E:91:F1:7B:52:31:38:90:D9:36:8C:77:39:31:BC:08:06:04:06:9F:3C:F3:8B:28:1E:D9:2E:99:86:49:39:98:F3:4B:1A:F6:22:5D:49:51:60:2F:49:3E:08:42:08:02:D3:DE:99:58:A8:A2:CC:43:5D:8D:F2:0A:76:45:13:93:0C:5A:82:75:E7:10:EA:21:FC:97:ED:8E:2F:58:EF:43:D2:EA:F9:2E:4A:07:F0:99:E7:C6:07:E2:11:67:17:51:CC:8D:0F:13:C5:55:8F:90:FC:BE:20:61:74:84:47:D2:25:4B:E9:50:5C:89:A8:1C:8C:99:BD:49:D2:92:A7:D5:A7:F3:EF:39:73:8C:D9:E1:18:1D:F1:5A:27:03:45:F7:31:92:38:E9:61:58:22:74:97:F1:87:FE:D7:1D:C3:1A:A6:09:04:86:E5:15:A6:A5:12:CD:C2:60:C9:BF:7C:21:42:AF:F2:76:45:E9:8A:A8:0A:CE:C3:2E:38:49:72:C0:70:C8:64:08:B4:28:A7:62:F2:F9:F1:3A:85:ED:76:1F:12:A2:BD:F2:9B:0E:0F:C0:7C:66:82:52:2A:01:2D:0D:E9:7D:F0:5F:54:CD:A9:61:6D:35:14:61:F2:39:F2:F1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *EC:95:33:3B:71:C0:D2:B1:9C:58:23:0B:36:41:BC:54:9E:2C:92:1D*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access
http://www.camerfirma.com/certs/chambersofcommercerooot-2016.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_serverAuth*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/chambersofcommercerooot-2016.crl
http://crl1.camerfirma.com/chambersofcommercerooot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *93:7D:7D:5D:0B:7F:B7:DB:03:93:99:BC:0B:67:0C:C2:03:C7:AB:4E:33:2F:AE:45:3C:C3:8E:C1:88:DD:EA:2B*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I 7JUzO3HA0rGcWCMLNkG8VJ4skh0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2021-11-16T02:00:00Z

11.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

11.15.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016

Name [es] Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES - 2016

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA FOR WEBSITES - 2016

Subject O: AC CAMERFIRMA S.A.

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA FOR WEBSITES - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *7JUzO3HA0rGcWCMLNkG8VJ4skh0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-03-15T01:00:00Z*

11.15.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

11.16 - Service (withdrawn): Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name	[en]	<i>Qualified timestamps issued by AC CAMERFIRMA TSA - 2016</i>

Name	[es]	<i>Sellos de tiempo cualificados emitidos por AC CAMERFIRMA TSA - 2016</i>

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1564901409084605058*

Subject C: *ES*

Valid from: *Thu Apr 14 12:42:09 CEST 2016*

Valid to: *Fri Mar 09 11:42:09 CET 2040*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:CC:BF:25:18:57:8E:09:63:C0:94:89:2E:36:3D:4F:B3:E3:B1:BD:69:1D:6F:7B:C5:CF:02:26:47:87:A5:EC:C8:D7:B3:11:10:44:9F:59:8D:84:10:49:D2:6A:63:B7:5E:B2:1B:C3:0E:22:32:EB:D7:54:92:35:4F:6C:35:F9:B4:08:4F:C3:F8:B6:61:83:8C:A9:11:1C:2E:A8:1C:44:05:9F:59:9C:13:75:6F:C5:43:5B:8D:B5:0F:AE:43:DD:E7:BA:DA:19:86:3F:E9:A4:FB:76:EA:C0:38:04:55:03:A5:E4:59:02:9C:04:84:FD:20:FA:4D:AF:0F:F2:23:53:BF:1C:DA:D4:DB:73:E0:44:49:FD:8E:01:38:A7:8F:12:21:9D:A4:BE:4B:AD:04:6F:1B:03:C2:64:0D:A0:D8:A0:15:E2:7E:DA:87:37:7C:76:60:B2:69:3C:2A:34:C2:95:D9:1A:48:4F:B9:82:C0:77:56:9C:A2:A6:06:4F:30:41:3D:01:1B:16:35:FA:1F:66:3A:BA:99:B4:DC:93:85:6E:62:32:2B:AE:A9:E3:21:AA:E7:38:37:EA:77:61:57:5C:8B:03:78:62:6A:BC:C9:E8:83:F5:41:63:F0:3E:7C:CC:89:6D:24:49:18:F1:8B:9F:4D:F1:13:A9:A5:FC:D7:D7:78:C9:EC:A1:CF:17:F3:DF:DA:5D:53:3F:F7:20:5C:EE:B2:1B:10:E1:EC:15:09:0D:05:C0:61:1B:02:6C:5B:3C:5A:2D:C1:5E:9F:0A:12:8D:51:EA:6C:89:87:89:E6:19:25:6A:F2:6E:2C:2B:EB:A8:06:E3:FB:7F:68:27:68:C2:F0:86:80:B0:09:9C:01:83:76:1E:36:C9:EB:DB:14:D4:72:80:14:B8:9C:CD:9E:4A:CD:D6:CE:A6:65:CE:A0:AC:99:ED:B7:25:AC:2F:78:C4:EE:FF:70:CE:DF:BC:94:55:37:D0:58:87:02:CC:CA:30:34:4B:DE:83:39:B4:AB:53:B4:B8:F7:55:21:78:36:3B:1F:4A:66:12:9A:F3:69:87:F6:34:DF:C4:FB:13:B8:3C:C2:20:30:F8:D7:38:FA:8E:75:17:1A:A4:85:AA:9B:A2:CD:09:69:2E:53:87:CF:7B:E9:AD:BF:7F:25:D9:BB:0A:E2:D4:24:8F:A9:91:2C:5F:62:97:AB:32:DF:13:5E:CA:99:34:99:2D:E7:D5:87:E7:5E:74:33:BE:33:7D:5C:22:18:DF:FE:A3:1E:C8:E6:2E:08:D7:B9:A8:87:E0:72:3E:74:10:91:5E:A9:C1:D8:22:82:EE:E6:36:57:26:DF:68:A6:7B:F9:37:71:1B:4B:F1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*

Authority Key Identifier *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

Authority Info Access
http://www.camerfirma.com/certs/chambersofcommercerooot-2016.crt
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_timeStamping*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points
http://crl.camerfirma.com/chambersofcommercerooot-2016.crl
http://crl1.camerfirma.com/chambersofcommercerooot-2016.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BA:AE:2C:63:38:85:7D:50:20:0F:6F:73:DD:45:E6:5A:A2:D8:95:BE:D4:67:5B:6E:39:6B:72:22:E0:18:A9:B8*

X509SubjectName

Subject CN: *AC CAMERFIRMA TSA - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA TSA - 2016*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I Hm21xj/vkIVeN/rb/RCqutk7Tiw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2023-10-24T00:00:00Z

Scheme Service Definition URI

URI [en] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx

URI [es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx

11.16.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [en] Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

Name [es] Sellos de tiempo cualificados emitidos por AC CAMERFIRMA TSA - 2016

Service digital identities

X509SubjectName

Subject CN: AC CAMERFIRMA TSA - 2016

Subject O: AC CAMERFIRMA S.A.

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA TSA - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *Hm21xj/vklVeN/rb/RCqutk7Tiw=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time *2018-03-15T01:00:00Z*

11.17 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018

Name	[es]	Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES 2018

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1787353533750921228

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CHAMBERS OF COMMERCE ROOT 2018*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *CHAMBERS OF COMMERCE ROOT 2018*

Issuer OU: *see current address at www.camerfirma.com/address*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject OU: *see current address at <https://www.camerfirma.com/address>*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Valid from: *Thu Oct 04 11:00:23 CEST 2018*

Valid to: *Thu Aug 28 11:00:23 CEST 2042*

Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:16:72:15:4B:7F:47:CB:1B:DA:2F:17:2A:B8:42:B9:CA:8C:C8:DA:BB:C2:C5:C7:05:09:53:58:8E:00:73:FF:9D:DC:80:57:0C:CF:2C:91:DE:35:76:97:8B:C4:9C:E3:ED:53:06:16:D8:0D:AF:43:DC:7D:F1:6E:3B:E5:6A:70:29:DC:80:BC:66:8C:8E:30:FD:27:F3:0C:F8:6F:9E:40:DD:5D:BD:CB:2A:13:A4:2C:F5:F9:E9:B5:5D:43:8D:CA:53:2B:F0:C5:CF:7A:1B:83:38:9D:85:9B:38:3D:88:04:8A:5B:7D:DA:1C:0A:91:BD:82:3C:2E:D9:18:67:B9:41:99:34:16:E7:57:CA:8D:DB:CB:80:59:BD:FE:B1:B8:22:C0:03:5E:33:3E:ES:C3:69:84:E0:6F:8B:07:1E:4F:8B:88:38:6D:C9:F9:D7:B9:0A:92:7F:F3:F0:7D:05:D4:EA:60:93:11:68:49:47:E3:F2:D1:5F:71:B8:F8:6C:7A:2C:CA:FF:AD:78:CC:6A:12:76:AE:4D:61:14:56:A8:36:F7:4D:88:42:1B:33:05:02:95:44:8F:D1:CE:7B:2D:6F:23:61:5B:38:5A:EB:CA:CB:61:42:37:87:47:CC:59:7B:40:1F:DA:5C:10:EB:15:81:0D:B6:3E:E3:AE:E4:3A:A7:A9:57:C7:79:05:C9:3C:2D:D1:97:54:40:34:B8:41:58:A8:0D:28:CD:87:9D:4B:B4:2C:43:5D:F4:42:87:99:D0:11:6E:F1:5A:59:D5:EC:20:AE:85:EF:10:79:A7:F7:06:F7:57:01:64:6F:DC:B6:D8:FF:6C:EA:BD:88:03:AA:FC:8E:2F:E9:7A:A3:17:07:2E:BE:AD:9B:77:31:18:01:51:79:F7:38:F9:71:3D:43:6D:D1:15:C1:52:BF:A2:A1:8F:83:FE:5B:87:E3:24:87:A5:AF:BD:C0:0D:5C:35:52:B6:6A:3E:89:44:46:1D:CF:E7:DA:96:29:09:4B:5C:FB:20:86:F8:46:F7:CB:D9:D4:16:CC:52:A6:7A:FE:D6:77:AD:E9:DA:C2:4C:48:17:D1:89:81:94:20:4B:03:08:08:1F:FC:37:85:B5:BF:06:AF:D5:05:DA:83:4C:C5:BB:80:76:90:6F:13:18:6A:CB:91:78:55:5E:4B:2C:6D:E0:C1:54:AB:70:07:C9:47:71:D9:C6:93:62:37:68:9F:3D:D7:13:1A:F0:0C:AB:18:D3:3C:5E:D4:FF:25:74:D5:33:1D:61:B4:D4:0F:35:CB:8C:73:C9:EA:69:F3:25:2E:7F:0D:4C:4B:F8:2A:E8:C2:C5:94:20:BB:6C:F6:38:0F:E1:49:48:2D:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 2*

Subject Key Identifier *50:47:5C:2F:BA:12:7B:5F:74:38:1B:07:12:31:FB:68:4C:A8:EF:DE*

Authority Key Identifier *B5:2E:59:20:B2:AF:43:BB:95:3D:C2:51:99:E3:75:55:34:48:B0:1C*

Authority Info Access *http://www.camerfirma.com/certs/chambersofcommercerooot2018.crt*
http://ocsp.camerfirma.com

Extended Key Usage *id_kp_serverAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://policy.camerfirma.com

CRL Distribution Points *http://crl.camerfirma.com/chambersofcommercerooot2018.crl*
http://crl1.camerfirma.com/chambersofcommercerooot2018.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BF:0F:44:91:F3:71:48:9D:F2:EB:18:7B:DC:B4:B2:ED:D9:AB:2D:A0:16:CC:64:08:4C:AC:45:19:5E:F3:59:0D*

X509SubjectName

Subject CN: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject O: *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA FOR WEBSITES 2018*

Subject OU: *see current address at https://www.camerfirma.com/address*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *UEdcL7oSe190OBsHEjH7aEyo794=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-04-28T00:00:00Z*

11.17.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI***[en]**<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>***11.17.2 - History instance n.1 - Status: granted****Service Type Identifier***<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>***Service Name****Name***[en]**Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018***Name***[es]**Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES 2018***Service digital identities****X509SubjectName****Subject CN:***AC CAMERFIRMA FOR WEBSITES 2018***Subject O:***AC CAMERFIRMA S.A.***Subject 2.5.4.97:***VATES-A82743287***Subject SERIAL NUMBER:***A82743287***Subject OU:***AC CAMERFIRMA FOR WEBSITES 2018***Subject OU:***see current address at <https://www.camerfirma.com/address>***Subject L:***MADRID***Subject ST:***MADRID***Subject C:***ES***X509SKI****X509 SK I***UEdcL7oSe190OBsHEjH7aEyo794=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Status Starting Time***2019-09-15T22:00:00Z***11.17.2.1 - Extension (critical): additionalServiceInformation**

Issuer L: MADRID
Issuer ST: MADRID
Issuer C: ES
Subject CN: AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021
Subject 2.5.4.97: VATES-A82743287
Subject SERIAL NUMBER: A82743287
Subject OU: PKI SERVICES
Subject O: AC CAMERFIRMA S.A.
Subject L: MADRID
Subject ST: MADRID
Subject C: ES
Valid from: Wed Oct 20 17:12:16 CEST 2021
Valid to: Fri Oct 16 17:12:16 CEST 2037
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EF:56:15:D8:53:6F:9E:F1:5D:6B:02:22:3D:FC:7A:E0:CE:A1:64:41:88:21:C0:
E5:41:14:4D:62:FE:11:67:67:75:74:8A:D8:F3:3A:8A:50:8A:E4:5A:60:A3:8A:15:57:79:0C:C4:5E:72:69:65:36:DA:66:20:C3:78:AF:EA:EF:CC:1B:81:6A:A6:A4:00:F9:41:AB:95:3A:F1:43:E7
A7:C3:D8:78:12:44:4A:16:52:A9:7D:2A:EA:F4:55:1B:C3:55:E6:80:34:55:8B:F3:EB:16:19:E8:69:88:55:A6:C6:5B:A9:02:03:6F:6C:DD:CB:80:FA:32:10:14:76:9A:A4:22:6D:0E:93:79:1F:0
9:42:46:2A:B1:54:BD:D5:10:E9:70:55:9D:9A:25:1D:B8:6D:CA:27:4B:EC:22:68:25:4C:CF:31:E4:F5:B6:51:92:D1:54:CA:D7:CE:8C:9B:A9:FD:4C:74:B0:41:28:11:F2:8D:F4:8B:25:83:5C:E
7:AE:40:3B:06:A5:A3:6F:98:22:AF:6E:F2:BB:AB:E0:F9:8E:FE:DD:63:C1:16:F9:C6:7B:CE:DE:5D:90:E7:E8:5D:AB:5B:29:96:B2:08:22:BE:68:50:A2:94:EF:EA:3A:B7:B9:CA:7A:21:5D:CD:A
F:5F:52:CE:00:34:3A:C6:C7:39:4D:50:DF:70:65:0C:E0:D6:CF:A8:8B:7F:54:ED:09:A2:40:03:34:35:D2:55:BA:6C:DC:F5:9A:53:98:3D:E9:CB:57:74:38:2E:5F:6F:D5:C9:1A:68:5C:42:77:4E:
E6:37:6C:5E:22:F2:DC:2A:CC:5B:1C:85:1D:AF:50:7A:A4:8A:CE:8A:9D:CF:83:F9:C3:7E:02:C3:54:F8:0E:2E:3E:E9:B7:9E:25:EE:5F:E7:3D:69:AE:41:AF:40:5C:72:B7:E9:FD:F8:49:62:F8:00
2F:17:AE:6D:46:3C:7E:5D:6E:7A:B5:D4:CE:8B:F3:1A:6A:D9:84:0E:83:90:ED:7B:98:47:17:DA:B9:AC:FE:B4:51:20:2D:39:57:32:6C:93:76:10:D3:4F:23:2F:D8:FC:93:76:3A:93:35:D8:7B:
C0:21:B8:A8:A3:0E:64:9E:A7:86:D1:DA:BB:F4:88:12:6E:E0:E6:A9:29:A8:70:F1:03:5E:82:26:5D:49:3B:10:26:22:53:C0:C3:3E:60:23:18:A9:89:F8:93:CA:41:53:90:C7:4E:C0:9C:C1:28:5
4:A5:B7:0E:0B:2A:FB:DA:C6:84:9A:41:79:80:9A:EC:89:F1:03:F1:37:2D:2B:9A:38:F1:89:A1:AB:15:7A:4E:B6:DF:2F:C2:9C:92:1B:5C:16:69:11:04:08:5D:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier C7:6F:2D:C4:10:8A:6E:DD:F3:11:65:69:C6:4A:43:7B:C3:0F:68:14
Authority Key Identifier 51:11:32:7A:10:D0:D8:8C:4C:09:84:97:B1:A9:3E:B2:54:BA:87:C9
Authority Info Access <http://ca.camerfirma.com/certs/camerfirmaroot2021.crt>
<http://ocsp2021.camerfirma.com>
Extended Key Usage *id_kp_clientAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://policy2021.camerfirma.com
CRL Distribution Points <http://crl.ca.camerfirma.com/camerfirmaroot2021.crl>
<http://crl1.ca.camerfirma.com/camerfirmaroot2021.crl>
Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4D:18:7D:4E:5B:BA:7B:BA:D4:22:B7:5B:EF:B4:DC:B2:17:9D:1C:CD:11:5A:18:D2:C8:35:0F:FF:AC:31:6B:34*

X509SubjectName

Subject CN: *AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *PKI SERVICES*

Subject O: *AC CAMERFIRMA S.A.*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *x28txBCKbt3zEWVpxkpDe8MPaBQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-01-31T00:00:00Z*

11.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.18.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.17326.10.21.1.2.3*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.3.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.4.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.5.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.6.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.7.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.8.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.1.3

11.18.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Cualificados emitidos por AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021*

Name [en] *Qualified Certificates issued by AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021*

Service digital identities**X509SubjectName**

Subject CN: *AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021*

Subject 2.5.4.97: *VATES-A82743287*

Subject SERIAL NUMBER: *A82743287*

Subject OU: PKI SERVICES

Subject O: AC CAMERFIRMA S.A.

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I x28txBCKbt3zEWVpxkpDe8MPaBQ=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2022-09-06T00:00:00Z

11.18.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.18.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.17326.10.21.1.2.3

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.17326.10.21.1.3.3

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.17326.10.21.1.4.3

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.17326.10.21.1.5.3

Policy Identifier:

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>
Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>
Service Name		
Name	<i>[es]</i>	<i>Sellos de tiempo cualificados emitidos por “AC CAMERFIRMA QUALIFIED TSU - 2022”</i>
	<i>[en]</i>	<i>Qualified timestamps issued by “AC CAMERFIRMA QUALIFIED TSU - 2022”</i>

[illegible]

Issuer L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Issuer SERIAL NUMBER: *A82743287*

Issuer O: *AC Camerfirma S.A.*

Issuer OU: *AC CAMERFIRMA*

Issuer C: *ES*

Subject CN: *AC CAMERFIRMA QUALIFIED TSU - 2022*

Subject 2.5.4.97: *VATES-A82743287*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

Valid from: *Thu Jun 09 14:13:07 CEST 2022*

Valid to: *Wed Jun 07 14:13:07 CEST 2028*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:89:45:52:F5:30:56:B8:74:3A:3F:67:A4:DB:5F:05:1D:77:62:34:28:E4:44:87:62:4A:9E:AC:37:A2:E6:D9:97:2F:FA:36:12:A7:E8:61:18:C9:39:73:14:D6:37:2A:96:1D:A6:F1:0F:20:05:EB:E7:C0:28:45:ED:50:72:D4:44:31:5D:06:F3:B3:33:F8:04:64:4E:9B:65:73:EF:FA:2D:B7:AC:7B:85:3A:27:50:BC:59:78:34:9D:70:DB:28:98:33:2C:A3:BA:55:17:CB:BA:EB:98:F3:66:36:D9:46:0C:B0:5F:43:04:35:A2:95:19:06:76:9E:4B:F7:DB:E6:75:02:DD:8D:35:BA:97:CE:92:4B:85:49:E6:45:19:31:98:EA:C2:5E:83:C7:41:C6:A6:AD:40:8E:AD:35:56:2A:F4:F3:87:19:39:2E:67:1F:74:E3:DD:81:59:EB:D6:D4:E2:E9:EE:75:66:E6:A2:45:14:C4:4A:B7:59:EF:82:54:7F:2A:8D:83:55:11:36:64:D8:90:10:ED:C3:D8:F7:20:7F:21:7B:2D:51:08:A0:84:9F:DB:8D:7E:03:28:A0:F5:BD:B7:27:CC:9C:AA:A2:CE:7F:80:1D:D3:D2:DD:88:72:E1:AA:D8:83:1A:C D:53:B3:16:3A:87:BE:FE:89:31:13:C1:02:03:01:00:01

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *64:40:E1:6F:F9:CC:F3:CA:B2:3D:84:D0:3E:74:8C:C5:F0:A2:86:80*

Authority Info Access
http://www.camerfirma.com/certs/camerfirma_tsaii-2014.crt
<http://ocsp.camerfirma.com>

Authority Key Identifier *17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4*

CRL Distribution Points
http://crl.camerfirma.com/camerfirma_tsaii-2014.crl
http://crl1.camerfirma.com/camerfirma_tsaii-2014.crl

Certificate Policies
Policy OID: 1.3.6.1.4.1.17326.10.13.1.3
CPS pointer: <https://policy.camerfirma.com>

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4A:98:A7:75:E6:1B:2F:8A:A7:6B:EB:D4:64:3B:E0:53:F3:E5:A8:5D:4D:D7:06:2D:02:80:5B:C7:DB:2C:18:92*

X509SubjectName

X509 SK I *ZEDhb/nM88qyPYTOPnSMxfCih0A=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time 2022-10-10T00:00:00Z

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/OC</i>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified certificates issued by INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES 2024

Name [es] *Certificados cualificados emitidos por INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES 2024*

Certificate fields details

Version: 3

Serial Number: 353760978990492450419320879269297097507640382546

[illegible]

Signature algorithm: *SHA384withECDSA*

Issuer CN: *INFOCERT-CAMERFIRMA CERTIFICATES 2024*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer C: *ES*

Subject CN: *INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024*

Subject 2.5.4.97: *VATES-A82743287*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

Valid from: *Fri Feb 16 12:55:23 CET 2024*

Valid to: *Thu Feb 16 12:55:23 CET 2040*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:B8:D3:0C:B2:AC:2E:82:7C:C0:30:A4:C5:27:FD:66:38:77:5F:C2:E7:9C:22:63:71:93:BF:83:6B:74:62:74:72
A5:7B:17:88:E4:9B:32:4C:79:34:52:F2:3F:01:30:77:6E:32:71:EA:B7:A7:36:B7:35:4F:0F:2F:CC:BE:EA:AF:DE:5A:E9:8B:0E:45:63:21:97:1C:52:2D:7A:9D:7D:D1:27:54:74:70:DD:95:48:8
D:4B:AF:2F:DE:94:7B:A6:6B*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *A9:D8:FB:35:5A:A4:AA:49:2F:72:3C:55:00:69:80:24:2F:CE:20:CF*

Authority Key Identifier *16:A8:FF:F5:19:05:E9:47:AA:D2:56:1C:10:08:F0:4D:F6:9A:73:59*

Authority Info Access *http://ca.camerfirma.com/certs/root_certificates_2024.crt
http://ocsp.camerfirma.com*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://policy.camerfirma.com*

CRL Distribution Points *http://crl.ca.camerfirma.com/root_certificates_2024.crl
http://crl1.ca.camerfirma.com/root_certificates_2024.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:58:31:18:E6:C5:E5:D2:10:DF:34:DD:35:97:F1:13:6A:5B:16:48:22:18:FC:C2:D
D:3B:85:F7:A5:C8:1C:FF*

X509SubjectName

Subject CN:	INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024
Subject 2.5.4.97:	VATES-A82743287
Subject O:	AC CAMERFIRMA S.A.
Subject C:	ES
X509SKI	
X509 SK I	qdj7NVqkqkkvcjxVAGmAjC/OIM8=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2024-10-16T00:00:00Z

11.20.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

11.20.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

11.21 - Service (granted): Qualified certificates issued by INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
Service Name	
Name	[en] Qualified certificates issued by INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024
Name	[es] Certificados cualificados emitidos por INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Certificate Policies	Policy OID: 2.5.29.32.0 CPS pointer: https://policy.camerfirma.com
CRL Distribution Points	http://crl.ca.camerfirma.com/root_timestamp_2024.crl http://crl1.ca.camerfirma.com/root_timestamp_2024.crl
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	B4:CE:3F:04:8F:90:AE:BE:5E:16:8E:7B:87:81:35:48:44:52:5B:BC:DE:F8:78:E2:42:1C:BB:3F:46:71:18:DD
X509SubjectName	
Subject CN:	INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024
Subject 2.5.4.97:	VATES-A82743287
Subject O:	AC CAMERFIRMA S.A.
Subject C:	ES
X509SKI	
X509 SK I	jZQyG0FVBFRCOiFx6RGd9TSAq14=
Service Status	
Service status description	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
[en]	undefined.
[es]	undefined.
Status Starting Time	2024-10-16T00:00:00Z

11.21.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

11.22 - Service (granted): Qualified timestamps issued by AC CAMERFIRMA QUALIFIED TSU RSA 2024

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST
Service type description	[en] A time-stamping generation service creating and signing qualified time-stamps tokens. [es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.
Service Name	

Certificate fields details

Version: 3

Serial Number: 1854613904021888061663

[illegible]

Signature algorithm:	SHA256withRSA
Issuer CN:	Camerfirma TSA II - 2014
Issuer L:	Madrid (see current address at https://www.camerfirma.com/address)
Issuer SERIAL NUMBER:	A82743287
Issuer O:	AC Camerfirma S.A.
Issuer OU:	AC CAMERFIRMA
Issuer C:	ES
Subject CN:	AC CAMERFIRMA QUALIFIED TSU RSA - 2024
Subject 2.5.4.97:	VATES-A82743287
Subject O:	AC CAMERFIRMA SA
Subject C:	ES
Valid from:	Thu Apr 11 17:46:32 CEST 2024
Valid to:	Wed Apr 10 17:46:32 CEST 2030

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C4:89:0A:3A:0B:1C:85:F1:8F:B3:0D:FD:4D:A3:FD:57:66:A6:80:DA:9C:D4:8
3:0F:BF:96:B8:C9:CE:F0:19:44:F0:89:52:72:36:08:86:EE:14:37:DA:2E:61:EC:F7:62:9D:A9:84:96:14:CC:07:D0:F4:5A:D6:82:0F:20:71:65:FF:E3:D5:5F:AF:E3:21:79:76:AB:C2:7B:75:38:
74:AE:76:91:95:27:86:E6:DF:0A:F8:9E:63:52:D0:39:39:96:57:48:0D:54:1A:63:4D:4F:BF:41:88:E1:7C:EE:48:F3:DB:51:5C:76:90:CE:3A:CF:99:BD:21:80:FB:14:8A:44:89:F3:5F:12:CB:36
:3C:7F:20:75:7C:D1:55:25:09:31:09:55:1F:50:EF:FC:39:A1:24:66:B4:6B:07:30:12:21:87:6C:14:C5:77:46:88:9C:98:43:61:04:36:5B:34:51:6D:BB:B6:F7:2A:AC:DE:12:6F:21:69:1F:2A:04
:CA:EF:EF:D2:1B:70:96:21:97:EF:5E:7C:50:AA:10:00:34:39:6F:54:5C:3B:CC:2F:0E:C2:A6:88:3A:5B:4E:1A:DB:FB:A1:CC:0E:CB:32:E1:6A:7A:DE:7B:09:22:20:81:79:33:1C:0F:6A:46:97:7
1:1E:73:96:12:83:CC:49:92:FA:05:A2:A0:EA:77:EA:BD:29:5A:AF:71:D2:5B:E4:99:52:B5:FB:34:2F:FF:5A:65:19:52:F9:AC:8D:9D:5C:78:ED:69:7C:73:1A:17:01:02:80:36:9F:C3:0D:3A:F0:
5D:66:21:C9:C2:05:12:41:0D:70:30:08:89:F0:C2:BC:83:A8:E6:E4:FC:93:7A:5A:DD:94:DB:6C:24:60:82:9A:4F:C4:E9:BF:6B:C0:79:A9:E6:D3:7F:F0:23:30:36:90:D8:1E:03:22:E5:DA:B3:5
B:AA:80:6E:0F:AC:94:BE:E6:B5:9D:18:55:70:E1:83:59:01:BD:0D:20:ED:16:6B:A6:88:1B:37:3A:40:AE:50:57:75:57:43:13:A0:F0:CD:1A:DD:54:24:19:80:48:27:E0:0C:4F:A8:D7:31:16:F8
:0B:11:C9:42:EF:26:8A:89:CB:08:0E:06:5D:2B:5D:FB:D2:DB:A2:58:EE:6B:12:3B:8B:D6:DB:85:C3:74:1C:40:05:68:90:E7:48:43:EB:B4:3C:A9:1E:76:CD:7F:D2:E7:FB:6C:7C:B1:71:DA:70
:14:9B:44:4F:7D:48:75:82:A5:C7:18:0D:E3:0F:5F:97:48:A5:B5:D7:2D:E6:09:E3:DF:75:C0:62:6A:2C:01:2B:03:CB:12:8E:8B:A2:C4:C2:DF:23:88:6A:63:02:03:01:00:01

Basic Constraints*IsCA: false***Extended Key Usage***id_kp_timeStamping***Subject Key Identifier***97:64:A9:01:34:F3:EC:36:7D:95:49:99:C1:1C:8F:E8:EA:BF:37:D7***Authority Info Access***http://www.camerfirma.com/certs/camerfirma_tsaii-2014.crt**http://ocsp.camerfirma.com***Authority Key Identifier***17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4***CRL Distribution Points***http://crl.camerfirma.com/camerfirma_tsaii-2014.crl**http://crl1.camerfirma.com/camerfirma_tsaii-2014.crl***Certificate Policies***Policy OID: 1.3.6.1.4.1.17326.10.13.1.3**CPS pointer: https://policy.camerfirma.com***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***37:56:0C:6E:0F:4B:77:A4:4F:31:FC:84:38:EC:05:20:1C:90:05:CF:54:BD:8D:80:B7
:4D:A8:19:F3:D1:86:80***X509SubjectName****Subject CN:***AC CAMERFIRMA QUALIFIED TSU RSA - 2024***Subject 2.5.4.97:***VATES-A82743287***Subject O:***AC CAMERFIRMA SA***Subject C:***ES***X509SKI****X509 SK I***I2SpATTz7DZ9IUmZwRyP6Oq/N9c=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2025-02-05T00:00:00Z*

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified timestamps issued by "AC CAMERFIRMA QUALIFIED TSU - 2024"

Name	[es]	Stamps of time qualified issued by "AC CAMERFIRMA QUALIFIED TSU - 2024"

Version: 3

Serial Number: 627269352927850834846

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Camerfirma TSA II - 2014*

Issuer L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Issuer SERIAL NUMBER: *A82743287*

Issuer O: *AC Camerfirma S.A.*

Issuer OU: *AC CAMERFIRMA*

Issuer C: *FS*

Subject CN: AC CAMERFIRMA QUALIFIED TSU - 2024

Subject 2.5.4.97: *VATES-A82743287*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

Valid from: *Mon Nov 25 13:30:48 CET 2024*

Valid to: *Sun Nov 24 13:30:48 CET 2030*

Public Key:
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:B7:1C:41:C7:FC:A4:74:3F:95:12:90:50:49:B5:72:15:97:EF:97:15:8C:81:9E:5A:12:D8:E0:21:EE:CB:F4:6D:2B:85:56:F6:7A:CB:F4:61:F5:0F:21:2D:54:4C:4C:01:10:4E:72:3A:F0:73:86:01:D1:D9:86:F8:4D:1B:A2:4B:28:89:04:26:DF:3B:4A:CD:4D:3E:53:2C:25:F4:02:D1:63:BA:85:B2:FC:9E:51:83:A6:18:71:F8:2A:D6:8F:7A:0A:21:9B:C8:BD:1A:CD:0C:F3:97:43:99:96:0A:A0:B6:85:9F:73:2E:38:F0:4E:48:C4:66:8A:3E:8E:AF:CD:CA:19:90:98:23:58:2C:69:9E:6F:E6:F1:89:88:81:B5:7C:00:67:37:01:F9:5D:69:F8:BA:47:FF:B7:44:CC:84:75:F9:A1:A9:E8:EE:38:B4:62:0E:1E:77:0F:5C:08:64:28:31:5F:AE:65:53:87:E8:A5:44:F2:80:03:2C:D9:C6:C9:1E:38:52:97:6A:86:59:5A:14:3D:A3:40:86:52:8A:D8:AD:0D:4C:46:A0:7C:32:59:38:48:84:A4:D9:0F:EF:7C:86:13:5D:94:BC:03:42:03:02:A4:F7:14:46:65:80:C2:95:6C:93:CF:B2:64:94:52:2A:1D:E9:0D:50:EC:CD:48:41:79:3F:76:FD:CF:AE:C1:BD:08:55:B9:63:F1:10:0A:F9:9A:4F:F7:9A:22:09:A8:11:40:16:28:E5:BB:62:03:3C:42:76:90:BF:79:62:46:E0:D0:37:A9:71:1E:8A:D0:0C:5A:E5:06:FA:32:6C:40:DD:3F:8D:60:45:2F:CE:28:C7:10:91:AC:47:B1:36:4A:1E:75:F7:9E:C1:0C:6E:CA:00:50:A4:9E:4B:C5:5D:F9:7D:4B:13:A8:62:C5:B8:C9:33:48:97:07:3E:1B:48:9E:78:CC:68:69:02:E4:79:ED:A8:58:04:13:4F:2F:B0:37:2E:7B:C2:EC:E3:C9:AA:7F:02:03:01:00:01

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *27:B9:1B:6B:E0:71:52:27:11:3E:F8:C6:C0:DA:14:FD:85:A8:A6:0B*

Authority Info Access
http://www.camerfirma.com/certs/camerfirma_tsaii-2014.crt
http://ocsp.camerfirma.com

Authority Key Identifier *17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4*

CRL Distribution Points
http://crl.camerfirma.com/camerfirma_tsaii-2014.crl
http://crl1.camerfirma.com/camerfirma_tsaii-2014.crl

Certificate Policies
Policy OID: 1.3.6.1.4.1.17326.10.13.1.3
CPS pointer: https://policy.camerfirma.com

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E3:6C:91:99:7C:25:3A:91:D2:CC:52:81:C9:65:BE:97:75:F0:85:5B:BF:70:88:AE:F1:62:F8:CA:F4:A0:02:23*

X509SubjectName

Subject CN: *AC CAMERFIRMA QUALIFIED TSU - 2024*

Subject 2.5.4.97: *VATES-A82743287*

Subject O: *AC CAMERFIRMA S.A.*

Subject C: *ES*

X509SKI

X509 SK I *J7kba+BxUicRPvjGwNoU/YWopgs=*

Service Status		<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time		<i>2025-05-21T00:00:00Z</i>

12 - TSP: COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

TSP Name

Name	[en]	COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA
Name	[es]	COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

TSP Trade Name

Name	[en]	VATES-Q2863012G
Name	[en]	REGISTRADORES DE ESPAÑA
Name	[es]	REGISTRADORES DE ESPAÑA
Name	[en]	Colegio de Registradores de la Propiedad y Mercantiles de España
Name	[en]	Colegio de Registradores de la Propiedad y Mercantiles

PostalAddress

Street Address	[en]	Calle Príncipe de Vergara, nº 70
Locality	[en]	Madrid
State Or Province	[en]	Madrid
Postal Code	[en]	28006
Country Name	[en]	ES

PostalAddress

Street Address	[es]	Calle Príncipe de Vergara, nº 70
Locality	[es]	Madrid
State Or Province	[es]	Madrid
Postal Code	[es]	28006
Country Name	[es]	ES

ElectronicAddress

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificate issued by internal CA
Name	[es]	Certificado reconocido emitido por la CA certificados internos

Version:	3
Serial Number:	75338451500473229499040475996576529077
X509 Certificate	-----BEGIN CERTIFICATE-----

[illegible]

Signature algorithm:	SHA1withRSA
Issuer CN:	Registradores de España - CA Raíz
Issuer OU:	Certificado Propio

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Issuer C: *ES*

Subject CN: *Registradores de España - CA Interna*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

Valid from: *Wed Jan 31 11:03:38 CET 2007*

Valid to: *Thu Jan 31 09:31:10 CET 2019*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:09:91:DE:03:DD:79:81:88:E0:3F:82:71:73:2F:50:BD:6A:3A:A6:B7:3C:DB
AC:B2:C8:0F:0C:F2:2C:AE:DB:83:7C:B7:64:AE:98:78:9F:7D:28:06:B9:1E:2D:65:39:A7:59:78:85:E1:58:F3:74:8C:C0:C2:FA:86:9C:2E:80:49:41:6D:1D:40:46:F3:11:10:50:43:AF:BA:47:F
2:FE:F1:2C:8B:E0:84:13:6E:C4:8D:CB:7D:C3:F8:ED:0F:FE:0A:C7:8C:8A:F6:24:8B:02:B0:80:7D:3B:EA:C8:FD:59:08:0D:80:12:88:A9:43:62:30:64:F8:B4:8F:49:43:D4:F8:87:F6:A2:F6:D0:
64:9C:95:A2:EC:A5:3C:2A:7A:9A:C4:98:0D:2C:28:7D:B7:2B:46:02:25:DE:6F:DC:8C:F5:62:7F:B2:69:D6:F4:F6:B8:6A:58:D8:1A:EC:E6:3A:88:22:B6:58:B4:A1:24:E2:E1:4E:AD:AF:E9:73:6
3:6B:19:A6:5E:AB:97:FF:27:1C:D8:CA:CE:5F:18:38:76:CF:0E:66:3B:06:70:17:38:28:B8:67:94:C6:BC:F3:F2:05:DE:6F:2E:38:41:64:71:57:E1:2E:CC:8A:AA:45:2A:E4:85:72:66:49:D2:69:F
7:87:F6:7D:FC:D5:B9:3A:5F:75:78:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *8E:F0:63:77:74:70:20:BE:CB:94:84:95:31:15:2A:D9:0D:E5:9D:0B*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://pki.registradores.org/normativa/index.htm>
CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]

Authority Info Access *http://pki.registradores.org/certificados/ca_raiz_scr.crt*

Authority Key Identifier *1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5*

CRL Distribution Points *http://pki.registradores.org/crls/arl_scr.crl*
<ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *3A:50:ED:C2:11:47:D8:67:37:75:C7:07:D3:2F:19:7D:DC:BE:34:75:BF:07:41:50:31:9E:11:61:DD:77:19:59*

X509SubjectName

Subject CN: *Registradores de España - CA Interna*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2018-02-06T01:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

12.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Certificate issued by internal CA*

Name *[es] Certificado reconocido emitido por la CA certificados internos*

Service digital identities

X509SubjectName

Subject CN: *Registradores de España - CA Interna*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

X509SKI

X509 SK I *jvBjd3RwIL7LIISVMRUq2Q3lnQs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time 2016-06-30T22:00:00Z

12.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

12.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificate issued by internal CA

Name [es] Certificado reconocido emitido por la CA certificados internos

Service digital identities

X509SubjectName

Subject CN: Registradores de España - CA Interna

Subject OU: Certificado Propio

Subject O: Colegio de Registradores de la Propiedad y Mercantiles de España

Subject C: ES

X509SKI

X509 SK I jvBjd3RwIL7LIISVMRUq2Q3lnQs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-02-13T00:00:00Z

12.2 - Service (withdrawn): Qualified Certificate issued by external CA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Subject Key Identifier *73:8A:03:F5:F4:B3:63:91:BC:4B:35:58:EA:A2:89:F3:19:1C:D3:94*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://pki.registradores.org/normativa/index.htm>
CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]

Authority Info Access *http://pki.registradores.org/certificados/ca_raiz_scr.crt*

Authority Key Identifier *1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5*

CRL Distribution Points *http://pki.registradores.org/crls/arl_scr.crl*
<ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *13:51:F3:92:83:7A:73:9D:D8:53:D7:F8:E2:FE:FF:39:12:77:18:79:82:1F:A4:76:14:DB:87:A3:AF:03:5C:E6*

X509SubjectName

Subject CN: *Registradores de España - CA Externa*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

Service Status*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2018-02-06T01:00:00Z***Scheme Service Definition URI**

URI *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

12.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

12.2.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified Certificate issued by external CA*

Name [es] *Certificado reconocido emitido por la CA certificados externos*

Service digital identities

X509SubjectName

Subject CN: *Registradores de España - CA Externa*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

X509SKI

X509 SK I *c4oD9fSzY5G8SzVY6qKJ8xkc05Q=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

12.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

12.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified Certificate issued by external CA*

Name [es] *Certificado reconocido emitido por la CA certificados externos*

Service digital identities**X509SubjectName**

Subject CN: *Registradores de España - CA Externa*

Subject OU: *Certificado Propio*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles de España*

Subject C: *ES*

X509SKI

X509 SK I *c4oD9fSzY5G8SzVY6qKJ8xkc05Q=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-02-13T00:00:00Z*

12.3 - Service (granted): Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[en] Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna*

Name *[es] Certificados cualificados emitidos por Autoridad de Certificación de los Registradores - AC Interna*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *33250107883580613301075761566452252203*

Authority Key Identifier *DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

CRL Distribution Points *http://pki.registradores.org/crls/arl_psc_corpme.crl*
ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

X509SubjectName

Subject CN: *Autoridad de Certificación de los Registradores - AC Interna*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *2LBZoZQFEituoRdXKNMRAVuvvgQ0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-07-17T02:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

12.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

12.3.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna

Name	[es]	Certificados cualificados emitidos por Autoridad de Certificación de los Registradores - AC Interna

Service digital identities**X509SubjectName**

Subject CN:	Autoridad de Certificación de los Registradores - AC Interna

Subject O:	Colegio de Registradores de la Propiedad y Mercantiles

Subject 2.5.4.97:	VATES-Q2863012G

Subject C:	ES

X509SKI

X509 SK I	2LBZoZQFEituoRdXKNMRAVuvvgQ0=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2017-02-22T00:00:00Z

12.3.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

12.4 - Service (granted): Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Externa

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Name	[en]	Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Externa

Version: 3

Serial Number: 20396695907009046247205297166071772756

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer CN: *Autoridad de Certificación Raíz de los Registradores*

Issuer O: *Colegio de Registradores de la Propiedad y Mercantiles*

Issuer 2.5.4.97: VATES-Q2863012G

Issuer C: *ES*

Subject CN: *Autoridad de Certificación de los Registradores - AC Externa*

Subject 0: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: ES

Valid from: *Mon Jun 06 17:06:11 CEST 2016*

Valid to: *Tue Jun 06 17:06:11 CEST 2028*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:A5:8D:12:C2:C8:97:88:02:67:EA:05:70:B2:D4:A7:8E:EF:E5:82:E2:05:98:EB:F3:CF:43:80:87:FD:07:F8:E0:A4:40:FB:99:20:2C:E6:55:F0:1A:02:EA:AF:73:82:D9:5F:4B:B7:D1:F2:1D:51:CD:DA:64:F2:87:07:AC:19:E3:CE:6C:5C:37:60:BF:DF:80:C4:21:68:B9:9A:0B:4D:7B:A4:43:93:68:0B:37:68:21:FC:50:78:63:9B:95:12:DC:F9:0D:C4:2D:8B:C3:B7:DC:0B:42:D8:93:5B:6E:04:83:73:DB:83:45:65:18:95:20:5F:0A:63:22:8A:FE:88:4D:F5:6E:8B:05:49:D4:40:11:84:00:80:07:53:22:AF:CB:53:47:6D:69:85:CE:0D:3A:0B:70:92:C2:46:FA:42:59:D5:2D:76:6B:3C:6C:4E:4A:A7:27:3C:76:CF:CD:D2:45:A8:A3:E1:6E:D6:93:E8:C8:DD:5C:93:52:93:44:0D:10:8B:09:55:8C:9F:EA:3E:ED:12:01:6A:55:45:37:86:11:27:F4:2A:C3:03:46:70:21:DF:8A:3C:9E:0C:9B:9C:7A:00:56:64:87:4B:15:87:40:8B:9D:9E:70:2A:2E:90:3E:B1:9A:73:C6:EB:AD:59:EA:5A:67:C3:5B:F7:27:5A:3A:70:A1:CA:77:C9:C4:7A:16:D8:DC:E3:95:46:97:07:55:7E:62:7A:74:54:00:84:33:19:88:6D:CA:03:35:FC:2B:01:18:9D:60:4D:96:F5:AB:F6:69:52:86:BC:4C:B3:3D:F2:6C:58:62:07:56:7D:17:4C:56:08:A4:8E:0C:3B:FC:74:F6:06:A4:B2:4D:ED:35:C3:03:0C:76:1D:48:11:C6:D2:87:1E:77:A6:0B:DA:D5:3D:DC:61:28:F7:D0:55:0E:40:1B:56:2C:32:AD:CF:17:57:AE:60:A3:6B:33:92:9F:36:C3:8C:84:88:F1:B5:ED:81:8B:27:1D:7B:28:CB:86:07:20:BC:D4:36:BF:C6:57:12:C7:87:BA:39:1F:11:06:A3:A4:5C:4A:0D:72:A8:42:DD:3A:99:C8:47:A9:37:DE:27:03:A9:A6:FC:75:64:6A:AB:FC:13:D6:39:50:47:96:89:61:DE:5E:97:CE:2D:C8:93:84:B2:FC:8D:7B:99:0D:7D:54:A7:64:1E:A8:27:3A:6A:A2:2B:F5:D5:74:62:F8:A8:86:F2:EF:84:02:13:83:C1:C5:33:8F:79:5A:5E:C0:61:C7:C6:05:38:7C:44:BF:12:1D:BC:69:AC:80:FA:DE:97:DF:F6:13:33:51:55:0E:16:F3:FA:A6:83:9F:A3:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *35:B8:65:CD:35:A0:A2:0F:9A:AF:E2:75:FE:DB:0C:48:52:3D:03:40*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://pki.registradores.org/normativa/index.htm>
CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access *http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt*

Authority Key Identifier *DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

CRL Distribution Points *http://pki.registradores.org/crls/arl_psc_corpme.crl*
<ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributi onPoint>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FB:7E:80:1D:60:D0:40:92:30:59:BD:31:CC:04:FA:49:C5:20:86:05:A0:09:C5:CB:D0:17:39:00:67:E6:57:17*

X509SubjectName

Subject CN: *Autoridad de Certificación de los Registradores - AC Externa*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *NbhlzTWgog+ar+J1/tsMSFI9A0A=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time 2017-02-22T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

12.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

12.5 - Service (withdrawn): Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01

Name [es] Sellos de tiempo cualificados emitidos por Autoridad de Certificación de los Registradores - TSA - 01

Service digital identities

Certificate fields details

Version: 3

Serial Number: 21558290793992193382977497126169320943

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIH3zCCBceqAwIBAQIOEDf5zKb6wodZQruatCGd7zANBqkghiG9w0BAQSFADCBsDELMakGA1UE
BHMCRVMxGDAwBgNVBGEtMDE2BzE5VjE5ODYzMDY5RzE5MDQGA1UECgwzQ285ZWdpbyBkZS85S2Wdp
c3RyYWRvcnVzIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRl
YVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQz
GUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGU
DTE3MDYxNTE2NTQwMfOxdT4MDYwNjE0MzQ0fOwga4kCzABgNVBAYTAkVTRmRwFgYDVQRhDA9W
OVRUfUyIRmRwFgYDVQREBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS
cm9waWVxYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGUO2YyYVQzGUGU
w7NuIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRl
DwAwggEKAQIBAQIRf6K8l9P8WjgWHEZDp+youJgiTLRnos+4AdcKbZvKadJRDceRsKt6T6C
E9JDCpYLEsWKouuyKlgVg1vIwauJDeo53e++LhkW6LlGHIe73jVd2bHYGOzGSKVsmxjgTUAUZ
W77LzK7oxjRNAC024mtgHReutWtO2uVl6yPr2LyIHRTa2qd9++c8rXhpkutu3aAISTVultrILWv
nKksZz9DdZtWjgRnuuDe+0ex3fUskys26ZzcbUgRlFayGT3gw36HgOP1fs+AhEt++u
YgRmxxbrRhtCwd5yqrsGdpECRLQj1oBRVxL7cSOpMhdznrmHEaQMBAAAggdlzMIIC7zAOB8qNV
HGB8AFBEAMCBsAwfYDVR0IAQHBAwwCgYIKwYBBQUHAgwWHQYDVR0BBYEFMTIOUzVuvSEyhW1
tUss1lbrDRpMIBBAyDVR0BgiHmH5Mh2BgwBgEEA1GGAABGQewgeUwPAyIKwYBBQUHAgEw
MGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlc3VmcjVmb3VybW0aXzh1ZiUzGV4Lhnh0bTcBpAYIKwYB
BQUHAgIwZCZGZDZlODAwZDZlFkbyBzdWp0dG8yS8yS8yS8yS8yS8yS8yS8yS8yS8yS8yS8yS8yS8y
aWNNcyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85
iFbYb3BpZWRhZC85IE1cmNhbW9pbG9zIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRlIGRl
AQR7MHkKwYIKwYBBQUHAGGhmh0dHA6Ly9vY3NwLnJlZzIzdHJhZG9yZXNub3JlLnZBLBgrBgEF
BQOCARyARhR0cDovLzB855ZjWdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2WdpbyBkZS85S2
Y19lb3JwbWUyY3J0MB8GA1UdlwOYMBAAfNiwwGUBRirbqeXVjITEQFBr4ENMHyBgNVHR8Egeow
gecweSgeSgeGggd6GOGh0dHA6Ly9wa2kucmVnaXN0cmFkb3Jlc3VmcjV3Jscj9jcmxftaW50X3Bz
Y19lb3JwbWUyY3JshoChbGRhcnR0d2akYXAucmVnaXN0cmFkb3Jlc3VmcjV049QUIMBjIRF
UK5BLE89Q29sZWdpbyUyMGRlITWUmVnaXN0cmFkb3Jlc3VmcjV049QUIMBjIRF
ZXI0aWZpY2F2ZjVldm91YXRpb25MaXN0P2Jhc2Uub2JqZWNOY2xhc3M9YjIjMRGldHJpYnV0aW9u
UC9pbW9wODYkZG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90dG90
GKMMRWCzRkq6RqkxIAshRiggkmyEH48WBT+9RqU0rTEC4d8g85T5s66TIE5Cs58ITNhuYg
9i7gUYzVjgUdHtUOT49ol+s4hiEmuM0ucT4Mxg3FD6OimLUvWBzA5hgsOljX40jLXXVds
7ogKWBgKrfyglw++d6hQjYnVdowW0H3PAPlwUEV0mg2vkryfOS9r78UBGRCCjZzj7KtM4
509oxyHnSx89VdSVeCncZpmRcstvmkg9b8Afc9aufjJhMhmbWjdfFpMHHgBkyZVEECzhr25
uLEP20eJ4ndXpFS7GzT2ZNRhnlVxBrKs1ZPT9PW0A8Lyv2nL2RK9bO2WMM4++sknmBThSzs
jWtILM1gldOP37B805qKedAAq74+128Cq91DAkE1LJAhrctU899VGSU5R6p1ty2p8C
0ym7U9HF1DqmAtSRZEwzKR5nrtE6DMxpBG7lqYnWNXHdk52vdeOrZFaxNgRp+KM780+80eX9g
b3YPZnvKAsrC7dxjphgOZVDMv09HfrcjdBewIWGZvupqkrhgNo3vmk02jRcLIZtawhOp3mL0eG
byj9g9V0X9Dpz1KYUZxkAHM41Qj0vi

```

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

Autoridad de Certificación de los Registradores - AC Interna

Issuer O:

Colegio de Registradores de la Propiedad y Mercantiles

Issuer 2.5.4.97:

VATES-Q2863012G

Issuer C:

ES

Subject CN:

Autoridad de Certificación de los Registradores - TSA - 01

Subject O:

Colegio de Registradores de la Propiedad y Mercantiles

Subject 2.5.4.97:

VATES-Q2863012G

Subject C:

ES

Valid from:

Thu Jun 15 18:54:00 CEST 2017

Valid to:

Tue Jun 06 16:38:48 CEST 2028

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D1:20:7A:FA:28:12:27:F4:FF:16:8E:0C:21:11:90:E9:FA:3A:2E:D6:08:93:2D:19:EB:83:EA:F8:15:02:98:63:83:19:28:8A:56:D8:26:C4:98:13:52:45:19:5B:8E:CB:CC:AE:E8:C6:34:4D:01:CD:36:E2:6B:60:1D:17:AE:B5:6B:4E:DA:E5:65:B7:AC:8F:C5:1D:8B:CA:51:C1:4D:AD:A0:77:0F:9C:F2:B5:C7:A6:29:2D:BB:76:80:89:24:D5:B8:9B:6B:94:B5:AF:9C:C2:AC:C5:9A:7D:0D:DC:43:CE:D5:98:27:CF:51:BA:E6:FA:F8:47:B1:DC:55:2C:F2:4B:FF:B3:3E:A2:0A:27:01:FD:4A:09:44:71:5A:60:6A:F7:AB:0D:FA:E4:40:AF:51:6C:CA:08:44:22:DF:AE:62:0A:C1:9B:1C:5B:46:1B:42:C1:D4:B2:A8:74:86:76:91:02:AC:BA:09:D6:80:51:57:12:FB:73:F4:8E:A4:C1:DD:CE:7A:EE:98:71:29:02:03:01:00:01

Extended Key Usage

id_kp_timeStamping

Subject Key Identifier

C4:C8:39:4C:D5:BA:FE:44:CA:15:B5:B5:4B:2C:D4:86:EB:0F:F4:69

Certificate Policies

Policy OID: 1.3.6.1.4.1.17276.0.1.10.1

CPS pointer: <http://pki.registradores.org/normativa/index.htm>

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access

<http://ocsp.registradores.org/>http://pki.registradores.org/certificados/ac_int_psc_corpme.crt

Authority Key Identifier

D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D

CRL Distribution Points*http://pki.registradores.org/crls/crl_int_psc_corpme.crl**ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registra
dores%20-%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributi
onPoint***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***33:5A:CB:56:33:A7:34:AB:EA:D2:34:93:AD:91:0E:FC:C9:D7:EB:C3:43:06:E1:E4:8
C:7B:AF:07:0C:11:2D:57***X509SubjectName****Subject CN:***Autoridad de Certificación de los Registradores - TSA - 01***Subject O:***Colegio de Registradores de la Propiedad y Mercantiles***Subject 2.5.4.97:***VATES-Q2863012G***Subject C:***ES***X509SKI****X509 SK I***xMg5TNW6/kTKFbW1SyzUhusP9Gk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-07-17T02:00:00Z***Scheme Service Definition URI****URI** [en]*https://avancedigital.mineco.gob.es/en-
us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx***URI** [es]*https://avancedigital.mineco.gob.es/es-
es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx***12.5.1 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST***Service Name****Name** [en]*Qualified timestamps issued by Autoridad de Certificación de los
Registradores - TSA - 01***Name** [es]*Sellos de tiempo cualificados emitidos por Autoridad de Certificación de los
Registradores - TSA - 01*

Service digital identities**X509SubjectName**

Subject CN: *Autoridad de Certificación de los Registradores - TSA - 01*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *xMg5TNW6/kTKFbW1SyzUhusP9Gk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-02-06T01:00:00Z*

12.6 - Service (granted): OCSP Responses issued by Autoridad de Certificación de los Registradores - VA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en] A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

[es] A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.

Service Name

Name *[en] OCSP Responses issued by Autoridad de Certificación de los Registradores - VA*

Name *[es] Respuestas OCSP emitidas por Autoridad de Certificación de los Registradores - VA*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *33250107883580613301075761566452252203*

Authority Key Identifier *DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

CRL Distribution Points *http://pki.registradores.org/crls/arl_psc_corpme.crl*
ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

X509SubjectName

Subject CN: *Autoridad de Certificación de los Registradores - AC Interna*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

X509SKI

X509 SK I *2LBZoZQFEituoRdXKNMRAVuvvgQ0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2018-02-06T01:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[en] http://pki.registradores.org/certificados/ac_va_psc_corpme.crt*

URI *[es] http://pki.registradores.org/certificados/ac_va_psc_corpme.crt*

12.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C: *ES*

Valid from: *Mon Mar 31 09:16:45 CEST 2025*

Valid to: *Fri Mar 31 09:16:45 CEST 2028*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:1E:4D:94:70:F8:FD:8F:68:98:70:E7:B1:7C:E6:00:45:21:92:00:4A:54:96:43:1D:CB:05:91:B1:9D:15:06:A2:72:56:33:A4:39:19:F3:84:09:64:9F:C0:BF:6A:6D:71:26:23:0A:62:16:4C:8C:93:2E:08:7D:1F:89:38:15:B1:F7:0D:FD:08:EC:36:BA:73:8C:BA:BE:8C:B0:C9:7F:99:1B:1F:AB:8B:95:87:67:C6:F5:80:42:82:9E:A6:FA:10:BA:C8:CD:03:B8:E0:9E:7E:C3:8C:F5:F2:69:58:8C:E5:F9:3A:1A:C3:FC:96:56:B1:CB:25:8C:B1:28:00:84:19:3F:4B:4E:30:03:06:0F:D2:E7:18:0F:FC:2B:C9:A4:FE:A4:CB:B3:D8:6D:35:49:1D:5F:1C:27:23:82:12:C2:D2:F6:2B:86:5C:97:F8:E3:DE:BC:C6:84:0A:27:89:02:A0:2C:69:0C:13:35:B9:72:5D:0A:63:8B:8D:BF:DB:D5:08:19:C4:10:D7:45:06:16:D2:9F:F0:4D:ED:29:C0:DF:AF:5F:27:CC:8F:86:6D:8E:CE:A8:C9:94:10:30:DE:1D:A3:93:63:2C:70:CB:0D:3F:13:A4:BC:19:FC:3B:B6:84:FA:36:E9:34:20:07:8D:87:46:1A:04:98:99:4D:6C:A3:02:03:01:00:01

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_QcSSCD

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *C6:19:88:3D:04:16:14:0C:7B:0A:92:06:BD:E6:80:CB:AE:36:C8:8A*

Certificate Policies *Policy OID: 1.3.6.1.4.1.17276.0.1.10.1*

CPS pointer: <http://pki.registradores.org/normativa/index.htm>

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

Authority Info Access *<http://ocsp.registradores.org/>*
http://pki.registradores.org/certificados/ac_int_psc_corpme.crt

Authority Key Identifier *D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D*

CRL Distribution Points *http://pki.registradores.org/crls/crl_int_psc_corpme.crl*
<ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint>

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F1:21:62:D2:57:EA:0F:19:5E:1D:19:06:82:6D:EB:13:21:B7:A1:9B:A9:8D:85:29:C7:DB:54:2D:50:1D:E2:21*

X509SubjectName

Subject CN: *Autoridad de Certificación de los Registradores - TSA - 01*

Subject O: *Colegio de Registradores de la Propiedad y Mercantiles*

Subject 2.5.4.97: *VATES-Q2863012G*

Subject C:	ES
X509SKI	
X509 SK I	xhmIPQQWFax7CplGveaAy642ylo=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2025-07-17T02:00:00Z

13 - TSP: Banco Español de Crédito, S.A

TSP Name

Name [en] Banco Español de Crédito, S.A

Name [es] Banco Español de Crédito, S.A

TSP Trade Name

Name [en] VATES-A28000032

Name [en] Banesto CA

Name [es] Banesto CA

Name [en] Banesto S.A. - C.I.F. A28000032

Name [es] Banesto S.A. - C.I.F. A28000032

PostalAddress

Street Address [es] Avda. Gran Vía de Hortaleza, 3

Locality [es] Madrid

State Or Province [es] Madrid

Postal Code [es] 28043

Country Name [es] ES

PostalAddress

Street Address [en] Avda. Gran Vía de Hortaleza, 3

Locality [en] Madrid

State Or Province [en] Madrid

Postal Code [en] 28043

Country Name [en] ES

ElectronicAddress

URI [en] http://ca.banesto.es

URI [en] mailto:correo@banesto.es

TSP Information URI

URI	[en]	http://ca.banesto.es
URI	[es]	http://ca.banesto.es

13.1 - Service (withdrawn): Banesto Qualified Certificates of previous CA PSC Banesto Clientes

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
Service Name		
Name	[en]	Banesto Qualified Certificates of previous CA PSC Banesto Clientes
Name	[es]	Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior

Service digital identities

Certificate fields details

Version:	3
Serial Number:	133541311365006312211899543605729653832
X509 Certificate	-----BEGIN CERTIFICATE----- MIIF7jCCBNagAwIBAgIQZHce/EjphIQ8keTNT+I0SDANBgkqhkiG9w0BAQUFADB1M0swCOYDVQOG EwJFuzEhMB8GA1UEBxMYTlVWZzW5hIDGwDI4MDMzIC0gTWkcmkM5gwgYDVQOKE9CYW5lc3Rv IFMuQ54glSBDLkkuR4gQTI4MDAwMDMyMRkwfwYDVQDEx8QU0MgQmFuzXN0byB5b290MB4XD TAYMDMANTYyMTA1MT1xODUyMDMkNDIhDAwMfoweTELMAIGAE1UEBhMCVRVMTAFBgNVBACGE1ic2V ySA4MCAyODAzMyAtIE1hZHp2DEoMCA1UEChMFQmFuzXN0byBTLkEuIC0gOy5lKkYyUEEYODAw MDA2MjEjEDM8sGA1UEAxMjUjFNDIEjhmVzdG8gQ2xpZW50ZXMwgwEIMA0GC5qG5lb3DQEBQAUA4IB DIAwaggEKAolBAQCDYURIRkHdNHSUArsh9Q7Zod25MIA3GghdsACBc+4mdV6h1102u2nCkuyMb QdRcreH01vRmVhvYhYKvdxWlapp1HCTDLsxMjCys6Pa9nCuzD3P2wXC8wYikgHFpOb+SxAl6W5 oBK4jSxSajG1HWkkgEHXTm0LNYX6PYlqJuzFg9KcvOaWekwcLbjrZh4+2FKL5RQKuz1HwGdR3qg kV9H11PYnylgoXs4iKm7Vh0AaP2A+igm9Ibjuu0oGsaBy9W1TasdtudQ2izalt3ljwoQ3F71 r8puM2KlMnYmGV0tthCHB8ceM+4085LkV0lvZrBFXc15sqzjAgMBAAAggg0MIICDAYBgNV HRIETAPgQ1YUBiYV5lc3RvLnVzMB8GA1UdEQRMA+BDWNhQjhmVzdG8uZXNwDwYDVR0TAQH/ BAUwAwEBIzAObgNVH8BAI8BEMCAQwwHQYDVR0BBYEFCEtGvck7KcrSaO3Q2TeQuwOIMGu BgNVHSMEgaYwgaOAF0o6FjOVLsaV54PEYOrpF8qK5ujoXmkdzB1M0swCOYDVQOGewJFuzEhMB8G A1UEBxMYTlVWZzW5hIDGwDI4MDMzIC0gTWkcmkM5gwgYDVQOKE9CYW5lc3RvIFMuQ54glSBD LkkuR4gQTI4MDAwMDMyMRkwfwYDVQDEx8QU0MgQmFuzXN0byB5b290ghcdeLyZBhVseetpKvkk Z8Y4MIBCOYDVR0gBIBADCB/TCB+gYIKwYBBAHWAEBMIHsMDEGCCsGAQUFBGFIWodHRwOi8v Y2EuYmFuzXN0by5lc3R5S2Bvc2l0b3ljbY9EUEMvMIG2BggrBgEFBQcAICBqRgBpKvZdGyY2V dGimaWNhZG8gaGeg2ikybilib0aWRvH8vciB0U0MgQmFuzXN0byB5b290Ihgkc2UgZW5jaWVu dHJlHjI23VsYWRvH8vciB5YXN0Y29uZGJlaW9uZXN0Y2VuzXN0byB5b290Ihgkc2UgZW5jaWVu dSBEZWNSYXhY2lviBkZSB0cmfjdGJlYXN0Y2VuzXN0byB5b290Ihgkc2UgZW5jaWVu oc+gLYYraH8vciB5YXN0Y29uZGJlaW9uZXN0Y2VuzXN0byB5b290Ihgkc2UgZW5jaWVu 9w0BAQUFAAOCAQEAJCsMAMhm5SHI007V0o3Hoc/UmsUjRlQ9B/LiaBGFsjjWwzB6wxBl+v/ UNatED9Ob0H4H1utPicwgMTxKipoQ7h+cRja0zVaAtNalqIB/Re/V7b6LGRVj0+vgGng+ACGP9 YEjgspj3Kx3NpklM2F0S0+eyohcG0eQA/W7BS0ZcrrfBEvsYEpLEdtpgljSSEC7n0RmWj3 47p5SS+7oDN98xpggNg8AYAJ55ZjAPpFnDp4Q5Jh75aZpYyzXnglbl/m9H8a08Is0/mYqGwad bsvPp5SR+RHdINOLCvHTG6wwsBNznKosHvRwnkV57IAv+9sN9YXZA== -----END CERTIFICATE-----
Signature algorithm:	SHA1withRSA
Issuer CN:	PSC Banesto Root
Issuer O:	Banesto S.A. - C.I.F. A28000032
Issuer L:	Mesena 80 28033 - Madrid
Issuer C:	ES
Subject CN:	PSC Banesto Clientes

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

Valid from: *Fri Mar 15 13:10:53 CET 2002*

Valid to: *Thu Mar 15 00:00:00 CET 2012*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8D:61:44:45:89:19:07:74:D1:D2:50:0A:ED:B2:1F:50:ED:9A:1D:DB:93:08:88:0D:C6:AA:17:5D:00:20:46:F8:89:83:55:5E:B7:D5:00:AE:DA:70:97:BB:23:1B:41:04:5C:AD:E1:F4:D6:F4:66:BE:1B:D8:86:56:24:BD:DC:56:21:AA:69:D4:70:93:0C:BB:31:30:9E:9C:62:CE:8F:68:D9:C2:BB:30:F7:3F:6C:17:08:CC:18:8E:48:07:16:93:9B:F9:2C:40:23:A5:92:A0:12:88:8D:2C:52:6A:38:06:D4:75:A4:92:01:07:5D:39:B4:2C:D6:17:E8:F6:35:AA:3B:B3:16:0F:4A:72:F3:9A:59:E9:30:70:B6:E3:AD:98:78:F8:61:64:20:8E:51:40:AB:99:D4:75:9D:47:7A:A0:92:55:7D:1F:5B:4F:62:7C:88:82:85:DA:E7:88:8A:9B:BB:C7:38:08:8F:CC:0F:A2:AA:6F:5F:8D:BB:EE:89:0A:06:80:06:F2:F5:6D:53:AA:C7:6D:89:D4:36:8B:36:A5:B7:72:48:C2:84:37:17:B1:75:AF:CA:6E:33:68:4A:94:C9:D8:98:65:74:B6:D1:C2:1C:1F:1C:78:CF:B8:43:CE:48:92:F2:34:22:F6:68:04:5B:57:73:5E:6C:AB:38:A3:02:03:01:00:01*

Issuer Alternative Name *ca@banesto.es*

Subject Alternative Name *ca@banesto.es*

Basic Constraints *IsCA: true*

Subject Key Identifier *23:44:4C:6B:ED:72:4E:E4:71:1B:00:3B:74:23:D9:37:90:BB:03:A5*

Authority Key Identifier *EA:3A:16:3A:10:54:BB:1A:55:2E:0F:11:83:AB:A4:50:6A:2B:9B:89*

Certificate Policies *Policy OID: 1.3.6.1.4.1.11076.1.1*

CPS pointer: <http://ca.banesto.es/Repositorio/DPC/>

CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]

CRL Distribution Points *<http://ca.banesto.es/CRL/PSCRootBanesto.crl>*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *53:99:01:61:F9:3C:B7:9E:6E:75:13:06:74:A4:53:DE:7E:2D:22:C8:1B:51:10:40:68:8B:66:7E:3F:65:35:30*

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time 2016-06-30T22:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

13.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

other Criteria List
assert=at Least One
Identifier 1.3.6.1.4.1.18838.1.1

13.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

13.1.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Banesto Qualified Certificates of previous CA PSC Banesto Clientes

Name [es] Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior

Service digital identities

X509SubjectName

Subject CN: PSC Banesto Clientes

Subject O: Banesto S.A. - C.I.F. A28000032

Subject L: Mesena 80 28033 - Madrid

Subject C: ES

X509SKI**X509 SK I***I0RMa+1yTuRxGwA7dCPZN5C7A6U=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased***Status Starting Time***2013-05-23T22:00:00Z***13.1.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]****Qualifier type description** [en]*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es]

*está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.***Criteria list assert=atLeastOne****other Criteria List
assert=at Least One
Identifier***1.3.6.1.4.1.18838.1.1***13.1.4 - History instance n.2 - Status: supervisionincessation****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name**

[en]

*Banesto Qualified Certificates of previous CA PSC Banesto Clientes***Name**

[es]

*Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior***Service digital identities****X509SubjectName****Subject CN:***PSC Banesto Clientes***Subject O:***Banesto S.A. - C.I.F. A28000032***Subject L:***Mesena 80 28033 - Madrid***Subject C:***ES***X509SKI****X509 SK I***I0RMa+1yTuRxGwA7dCPZN5C7A6U=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

Status Starting Time 2009-10-16T00:00:00Z

13.1.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

**other Criteria List
assert=at Least One
Identifier** 1.3.6.1.4.1.18838.1.1

13.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name *[en]* Banesto Qualified Certificates of previous CA PSC Banesto Clientes

Name *[es]* Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior

Service digital identities

X509SubjectName

Subject CN: PSC Banesto Clientes

Subject O: Banesto S.A. - C.I.F. A28000032

Subject L: Mesena 80 28033 - Madrid

Subject C: ES

X509SKI

X509 SK I I0RMa+1yTuRxGwA7dCPZN5C7A6U=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2004-11-25T00:00:00Z

Issuer CN: *PSC Banesto Root*
Issuer O: *Banesto S.A. - C.I.F. A28000032*
Issuer L: *Mesena 80 28033 - Madrid*
Issuer C: *ES*
Subject CN: *PSC Banesto Clientes*
Subject O: *Banesto S.A. - C.I.F. A28000032*
Subject L: *Mesena 80 28033 - Madrid*
Subject C: *ES*
Valid from: *Wed Nov 26 19:50:00 CET 2008*
Valid to: *Mon Dec 30 23:49:59 CET 2030*
Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AC:3B:90:F4:FB:3C:4C:FF:F8:71:71:86:F2:0A:8A:5D:0C:E7:BD:9A:58:E3:4C:04:59:04:63:CC:65:01:64:85:2F:9A:84:8E:D4:35:3C:D0:FE:3D:47:07:02:13:EE:C2:71:19:E2:93:FA:CC:61:8B:41:8A:32:C5:F2:BC:7F:02:1B:8E:83:19:10:BE:96:3D:FD:12:ED:5F:43:7F:94:01:51:36:DA:39:B7:4F:27:C2:EE:7A:48:85:23:ED:B0:87:5E:98:00:82:D8:E4:CC:FB:A3:42:DD:E5:C1:FC:A0:82:CD:85:64:4B:15:32:3D:65:47:51:68:0B:68:66:5D:D7:9D:95:32:52:0C:2B:EE:5C:9C:79:03:02:DC:8E:2C:ED:0C:7D:43:85:54:EF:85:6E:85:17:33:6F:9D:45:B1:15:32:9F:3C:5B:F4:9C:F3:53:57:7E:AD:2E:21:96:1B:9C:A6:03:B0:3D:E8:99:A6:05:B9:85:85:F9:44:1F:94:31:C6:D8:10:72:44:34:79:F0:BE:DA:69:9C:FA:48:66:80:E3:BE:73:0D:76:55:5F:2D:5A:5C:62:83:24:93:EE:78:0E:57:5E:00:0A:C1:77:99:9A:6B:BA:33:AF:94:BD:FC:14:54:C8:A7:34:33:32:10:11:2F:95:7E:DB:4A:2B:F6:C0:D9:81:77:38:0E:57:CF:82:DF:01:99:80:BA:24:2B:59:11:A3:05:8B:A1:59:FF:01:80:19:16:59:AB:94:48:2A:B8:EF:9B:A5:9E:96:B3:31:73:52:2C:53:C5:4F:18:30:C3:72:60:43:7F:90:F8:55:2E:2B:96:66:87:88:D9:7E:17:71:C2:C3:8F:43:A9:B5:BA:C7:30:B2:D3:12:52:E1:D8:43:2C:30:72:5A:4C:02:31:7C:D6:48:4A:8D:33:6E:D6:AF:D C:78:FF:54:3D:19:15:78:1D:E3:39:5D:A1:3D:AD:37:C0:3C:9F:9B:66:11:5F:0B:79:DB:76:15:92:82:91:9B:34:7B:EF:CF:3D:14:9B:00:4B:C4:69:82:2CF5:01:F8:0F:79:32:C4:6D:3E:E6:5C:32:81:4C:96:05:A6:41:72:9D:EF:AD:23:F3:41:90:4A:78:8C:80:17:2A:D4:A1:4E:30:74:96:70:06:6C:67:1A:9E:94:8C:49:43:6A:98:57:76:83:0E:D2:68:C7:2C:8D:6F:5D:E6:1C:99:78:68:3 F:64:CB:9E:9B:DA:C1:66:DE:24:0C:EA:83:79:16:9C:02:39:D1:FC:13:E1:AF:E7:C4:00:A5:77:58:A9:AC:44:19:37:17:DF:18:39:CB:2C:FD:19:34:10:E7:02:03:01:00:01
Issuer Alternative Name *ca@banesto.es*
Subject Alternative Name *ca@banesto.es*
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *53:77:C9:90:55:A7:3A:34:65:97:14:7D:97:3E:F2:FC:02:2E:0E:AC*
Authority Key Identifier *5A:BD:29:5D:C8:17:96:57:CD:6F:29:D3:E1:A2:F5:D4:4E:C4:CC:F2*
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <http://ca.banesto.es/Repositorio/DPC/>
CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]
CRL Distribution Points *<http://ca.banesto.es/CRL/PSCRootBanesto.crl>*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *46:6C:9A:9D:76:A6:A4:04:68:F9:18:BE:BD:9D:9F:10:41:78:A7:60:03:78:45:94:FF:94:3B:F7:8D:73:29:B9*

X509SubjectName

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI [en] *https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

13.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

other Criteria List
assert=at Least One
Identifier *1.3.6.1.4.1.18838.1.1*

13.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.2.3 - History Instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Banesto Qualified Certificates of CA PSC Banesto Clientes*

Name [es] *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

Service digital identities**X509SubjectName**

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

X509SKI

X509 SK I *U3fjkFWnOjRIlxR9Iz7y/AluDqw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

Status Starting Time *2013-05-23T22:00:00Z*

13.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List
assert=at Least One
Identifier *1.3.6.1.4.1.18838.1.1*

13.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Banesto Qualified Certificates of CA PSC Banesto Clientes*

Name [es] *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

Service digital identities**X509SubjectName**

Subject CN: *PSC Banesto Clientes*

Subject O: *Banesto S.A. - C.I.F. A28000032*

Subject L: *Mesena 80 28033 - Madrid*

Subject C: *ES*

X509SKI

X509 SK I *U3fjkFWnOjRIlxR9Iz7y/AluDqw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-10-16T00:00:00Z*

13.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier	<i>1.3.6.1.4.1.18838.1.1</i>

14 - TSP: EDICOM CAPITAL, S.L.

TSP Name

Name [en] *EDICOM CAPITAL, S.L.*

Name [es] *EDICOM CAPITAL, S.L.*

TSP Trade Name

Name [en] *VATES-B96490867*

Name [en] *EDICOM*

Name [es] *EDICOM*

Name [es] *INTERCAMBIO ELECTRONICO DE DATOS Y COMUNICACIONES SL*

Name [es] *EDICOM CAPITAL SL*

PostalAddress

Street Address [en] *Calle Charles Robert Darwin, número 8*

Locality [en] *Paterna*

State Or Province [en] *Valencia*

Postal Code [en] *46980*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Calle Charles Robert Darwin, número 8*

Locality [es] *Paterna*

State Or Province [es] *Valencia*

Postal Code [es] *46980*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:acedicom@edicomgroup.com*

URI [en] *http://acedicom.edicomgroup.com*

Subject O: *EDICOM*

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

Valid from: *Fri Apr 18 18:24:22 CEST 2008*

Valid to: *Thu Apr 13 18:24:22 CEST 2028*

Public Key:

```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:FF:92:95:E1:68:06:76:B4:2C:C8:58:48:CA:FD:80:54:29:55:63:24:FF:90:65:9
B:10:75:7B:C3:6A:D8:62:02:01:F2:18:86:B5:7C:5A:38:B1:E4:58:B9:F8:D3:D8:2D:9F:BD:32:37:BF:2C:15:6D:BE:B5:F4:21:D2:13:91:D9:07:AD:01:05:D6:F3:BD:77:CE:5F:42:81:0A:F9:6
A:E3:83:00:A8:2B:2E:55:13:63:81:CA:47:1C:7B:5C:16:57:7A:1B:83:60:04:3A:3E:65:C3:CD:01:DE:DE:A4:D6:0C:BA:8E:DE:D9:04:EE:17:56:22:9B:8F:63:FD:4D:16:0B:B7:7B:77:8C:F9:25
:B5:D1:6D:99:12:2E:4F:1A:88:E6:EA:04:92:AE:3D:11:89:51:42:3D:87:B0:31:85:AF:79:5A:9C:FE:E7:4E:5E:92:4F:43:FC:AB:3A:AD:A5:12:26:66:B9:E2:0C:D7:98:CE:D4:58:A5:95:40:0A:
B7:44:9D:13:74:36:C2:A5:EB:22:15:98:10:D8:8B:C5:04:9F:1D:8F:60:E5:06:1B:98:CF:B9:79:A0:3D:A2:23:3F:42:3F:6B:FA:1C:03:7B:30:8D:CE:6C:C0:BF:E6:1B:5F:8F:67:8B:84:19:D5:1
5:EF:7B:CB:90:36:31:62:C9:BC:02:AB:46:5F:9B:FE:1A:68:94:34:3D:90:8E:AD:F6:E4:1D:09:7F:4A:88:38:3F:BE:67:FD:34:96:F5:1D:BC:30:74:CB:38:EE:D5:6C:AB:D4:FC:F4:00:B7:00:5B:
85:32:16:76:33:E9:D8:A3:99:9D:05:00:AA:16:E6:F3:81:7D:6F:7D:AA:86:6D:AD:15:74:D3:C4:A2:71:AA:F4:14:7D:E7:32:B8:1F:BC:D5:F1:4E:BD:6F:17:02:39:D7:0E:95:42:3A:C7:00:3E:E
9:26:63:11:EA:0B:D1:4A:FF:18:9D:82:D7:7B:2F:3A:D9:96:F8:E8:1E:92:AE:13:55:C8:D9:27:F6:DC:48:1B:80:24:C1:85:E3:77:9D:9A:A4:F3:0C:11:1D:0D:C8:B4:14:EE:85:82:57:09:BF:2D
:58:7F:2F:22:23:D8:70:CB:79:6C:C9:4B:F2:A9:2A:C8:FC:87:2B:D7:1A:50:F8:27:E8:2F:43:E3:3A:BD:D8:57:71:FD:CE:A6:52:5B:F9:DD:4D:ED:E5:F6:6F:89:ED:8B:93:9C:76:21:75:F0:92:4
C:29:F7:2F:9C:01:2E:FE:50:46:9E:64:0C:14:B3:07:5B:C5:C2:73:6C:F1:07:5C:45:24:14:35:AE:83:F1:6A:4D:89:7A:FA:B3:D8:2D:66:F0:36:87:F5:2B:53:02:03:01:00:01
```

Basic Constraints *IsCA: true*

Authority Key Identifier *A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50*

Subject Key Identifier *A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://acedicom.edicomgroup.com/doc>

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *03:95:0F:B4:9A:53:1F:3E:19:91:94:23:98:DF:A9:E0:EA:32:D7:BA:1C:DD:9B:C8:5D:B5:7E:D9:40:0B:43:4A*

X509SubjectName

Subject C: *ES*

Subject O: *EDICOM*

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2017-12-01T01:00:00Z*

Scheme Service Definition URI

URI *[en] <http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt>*

URI	[es]	http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt
URI	[en]	http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt
URI	[es]	http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt

14.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC

14.1.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier	1.3.6.1.4.1.30051.3.1.1

14.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.1.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified certificates issued by the AC ACEDICOM Root
Name	[es]	Certificados Reconocidos emitidos por la CA ACEDICOM Root

Service digital identities

X509SubjectName

Subject C:	ES
Subject O:	EDICOM

Subject OU: *PKI*

Subject CN: *ACEDICOM Root*

X509SKI

X509 SK I *prPhKytJttdzoaqU9QHnc2VMrFA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

14.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</i>

14.1.4.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	<i>undefined.</i>
	[es]	<i>undefined.</i>

Criteria list assert=*atLeastOne*

other Criteria List assert= <i>at Least One</i> Identifier	<i>1.3.6.1.4.1.30051.3.1.1</i>

14.1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

14.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	<i>Qualified certificates issued by the AC ACEDICOM Root</i>

Name	[es]	<i>Certificados Reconocidos emitidos por la CA ACEDICOM Root</i>

Service digital identities

X509SubjectName

Subject C: ES

Subject O: EDICOM

Subject OU: PKI

Subject CN: ACEDICOM Root

X509SKI

X509 SK I prPhKytJtttdzoaqU9QHnc2VMrFA=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2008-11-07T00:00:00Z

14.1.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

14.1.5.5 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

other Criteria List
assert=at Least One
Identifier 1.3.6.1.4.1.30051.3.1.1

14.2 - Service (withdrawn): Qualified certificates issued by the CAEDICOM01

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Authority Info Access	<i>http://acedicom.edicomgroup.com/certs/caedicomroot.cer</i> <i>http://ocsp.acedicom.edicomgroup.com/caedicomroot</i>
Subject Key Identifier	<i>6D:6A:88:F8:2E:EA:7F:2F:CD:C0:F4:76:77:93:E6:45:32:EF:8B:05</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Authority Key Identifier	<i>14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.30051.2.3.1.1</i> <i>CPS text: [Certification Practice Statement]</i> <i>CPS pointer: http://acedicom.edicomgroup.com</i>
CRL Distribution Points	<i>http://acedicom.edicomgroup.com/caedicomroot.crl</i>
Subject Alternative Name	<i>acedicom@edicomgroup.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>33:9D:15:B1:65:CA:81:61:E4:D3:79:26:18:C6:FD:E8:4E:49:04:D0:46:69:54:1C:E E:6B:D3:33:BC:D5:B5:F4</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Calle Charles Robert Darwin 8 - 46980 - Paterna</i>
Subject O:	<i>EDICOM</i>
Subject SERIAL NUMBER:	<i>B96490867</i>
Subject CN:	<i>CAEDICOM01</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time*2024-09-30T00:00:00Z***Scheme Service Definition URI**

URI	<i>[en]</i>	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI	<i>[es]</i>	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

14.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.6

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.4

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.5

14.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.2.4 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates issued by the CAEDICOM01

Name	[es]	Certificados Reconocidos emitidos por la CA CAEDICOM01

Service digital identities

X509SubjectName

Subject C:	ES

Subject L: *Calle Charles Robert Darwin 8 - 46980 - Paterna*

Subject O: *EDICOM*

Subject SERIAL NUMBER: *B96490867*

Subject CN: *CAEDICOM01*

X509SKI

X509 SK I *bWqI+C7qfy/NwPR2d5PmRTLviwU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-12-01T01:00:00Z*

14.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.30051.2.3.2.6</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.30051.2.3.2.4</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.30051.2.3.2.5</i>

14.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

14.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</i>

14.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified certificates issued by the CAEDICOM01*

Name *[es]* *Certificados Reconocidos emitidos por la CA CAEDICOM01*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject L: *Calle Charles Robert Darwin 8 - 46980 - Paterna*

Subject O: *EDICOM*

Subject SERIAL NUMBER: *B96490867*

Subject CN: *CAEDICOM01*

X509SKI

X509 SK I *bWql+C7qfy/NwPR2d5PmRTLviwU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

14.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.6*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.30051.2.3.2.4*

Policy Identifier:

Identifier [OIdAsURN] urn:oid:1.3.6.1.4.1.30051.2.3.2.5

14.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by the CAEDICOM01

Name [es] Certificados Reconocidos emitidos por la CA CAEDICOM01

Service digital identities

X509SubjectName

Subject C: ES

Subject L: Calle Charles Robert Darwin 8 - 46980 - Paterna

Subject O: EDICOM

Subject SERIAL NUMBER: B96490867

Subject CN: CAEDICOM01

X509SKI

X509 SK I bWql+C7qfy/NwPR2d5PmRTLviwU=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2014-12-31T23:00:00Z

14.2.6.6 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.30051.2.3.2.6

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.30051.2.3.2.4

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.30051.2.3.2.5

14.3 - Service (withdrawn): Sellos cualificados de tiempo emitidos por EDICOM

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en]

A time-stamping generation service creating and signing qualified time-stamps tokens.

[es]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [es]

Sellos cualificados de tiempo emitidos por EDICOM

Name [en]

Qualified timestamps issued by EDICOM

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2019-12-10T01:00:00Z

Scheme Service Definition URI

URI [en]

<https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es]

<https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

14.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por EDICOM*

Name *[en]* *Qualified timestamps issued by EDICOM*

Service digital identities

X509SubjectName

X509SKI

X509 SK I *ziAzKLt9C4McA/Uq1OAj6qYXaGY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-12-01T01:00:00Z*

14.4 - Service (withdrawn): Conservación de sellos electrónicos cualificados proporcionado por EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service type description *[en]* *A preservation service for qualified electronic signatures.*
[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name *[es]* *Conservación de sellos electrónicos cualificados proporcionado por EDICOM*

Name *[en]* *Preservation of qualified electronic seals provided by EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

14.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.4.2 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service Name

Name	[es]	Conservación de sellos electrónicos cualificados proporcionado por EDICOM

Name	[en]	Preservation of qualified electronic seals provided by EDICOM

Service digital identities**X509SubjectName****X509SKI**

X509 SK I	f5On7ZPIbFzYVwO/qd9aELFd72Y=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2017-12-01T01:00:00Z

14.4.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.5 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada EDICOM

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service type description	[en]	An electronic delivery service providing qualified electronic deliveries.
	[es]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name	[es]	Servicio cualificado de entrega electrónica certificada EDICOM

Name [en] *Qualified electronic registered delivery service EDICOM*

Service digital identities

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2022-10-20T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

14.5.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada EDICOM*

Name [en] *Qualified electronic registered delivery service EDICOM*

Service digital identities

X509SubjectName

X509SKI

X509 SK I *f5On7ZPlbFzYVwO/qd9aELFd72Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-02-28T01:00:00Z*

14.6 - Service (withdrawn): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service type description [en] *undefined.*
[es] *undefined.*

Service Name

Name	[es]	<i>Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM</i>
Name	[en]	<i>Qualified validation service for qualified electronic signatures and qualified electronic seals by EDICOM</i>

Service digital identities

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>	
Service status description	[en]	<i>undefined.</i>
	[es]	<i>undefined.</i>

Status Starting Time *2022-06-29T00:00:00Z*

Scheme Service Definition URI

URI	[en]	<i>https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI	[es]	<i>https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

14.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

14.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</i>

14.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service Name

Name	[es]	<i>Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM</i>
Name	[en]	<i>Qualified validation service for qualified electronic signatures and qualified electronic seals by EDICOM</i>

Service digital identities

X509SubjectName

X509SKI

X509 SKI *f5On7ZPlbFzYVwO/qd9aELFd72Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-02-28T01:00:00Z*

14.6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

14.7 - Service (withdrawn): Sellos cualificados de tiempo emitidos por TSA EDICOM

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por TSA EDICOM*

Name *[en]* *Qualified timestamps issued by TSA EDICOM*

Service digital identities

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2024-06-05T00:00:00Z*

14.7.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Signature algorithm:	<i>SHA256withRSA</i>
Issuer C:	<i>ES</i>
Issuer O:	<i>EDICOM</i>
Issuer CN:	<i>CAEDICOM Root</i>
Subject C:	<i>ES</i>
Subject L:	<i>PATERNA</i>
Subject O:	<i>EDICOM CAPITAL SL</i>
Subject 2.5.4.97:	<i>VATES-B96490867</i>
Subject SERIAL NUMBER:	<i>B96490867</i>
Subject CN:	<i>CAEDICOM04</i>
Valid from:	<i>Thu Sep 23 15:50:20 CEST 2021</i>
Valid to:	<i>Sun May 21 12:20:00 CEST 2034</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:90:90:8C:72:B5:32:B5:90:F9:86:03:A4:51:A0:DD:8E:AB:0E:7F:53:EF:8E:4B: 58:42:79:92:03:77:22:9C:4F:A4:8B:C3:40:31:38:6E:46:59:AE:1A:12:33:C4:49:F2:DC:75:27:A1:DC:AB:D7:23:57:A2:A6:48:A2:3C:F1:EB:C8:05:61:18:D3:2E:63:4B:03:8C:70:E2:FC:21:A 9:53:63:32:88:90:2C:B5:B6:76:8B:0D:A4:4E:01:56:68:F0:9B:2D:21:6F:92:D7:60:61:B2:D4:32:CC:1C:09:5F:4E:85:74:3B:3C:FE:F9:B9:A8:22:83:D1:54:FC:46:7E:C6:47:17:11:FB:37:84: D1:1A:C6:78:FC:FA:C4:2D:8B:68:60:73:50:4C:B7:88:3A:7C:04:9B:DF:27:5B:A4:46:A7:B9:3E:13:F0:6C:B1:31:DA:66:88:09:94:11:77:D7:61:26:76:3A:4F:58:90:2B:74:6C:85:99:93:0 9:E2:A2:4C:E5:9B:3C:AE:C4:6E:BE:C0:F0:20:8D:F0:35:C6:2B:8B:6C:3F:DB:13:E6:7A:E9:79:23:B7:8B:02:67:F2:DE:CE:12:00:1F:68:37:2A:F0:05:66:66:E8:AF:5B:1C:45:CAE:1B:75:73: 6C:EF:46:A4:40:52:42:23:45:C9:C3:1C:73:61:EB:BF:12:36:5D:F1:F5:52:D7:CE:54:AC:AD:E2:D1:EA:C5:5C:6C:31:F8:CF:98:16:24:B2:98:4D:45:D5:E8:57:8E:87:CD:07:5E:F8:A6:5C:3D:B 4:6D:45:BF:CA:8E:09:02:1E:92:25:F5:DF:D2:C4:64:4F:B6:7C:58:2E:80:BA:1C:ED:1C:21:B7:EC:96:C1:B1:ED:AF:29:05:A3:1A:45:92:18:56:8B:41:A0:A3:B1:C1:BC:53:0E:CA:D3:C3:E0:3F D2:33:72:C3:20:11:6C:55:41:26:74:10:DE:C5:D1:F7:A0:C7:68:02:02:41:2A:79:F4:7A:19:F7:F6:42:18:A1:43:11:DE:11:E4:4E:F5:85:96:AE:E7:2B:16:15:BB:D6:77:C8:B9:60:B2:EA:95:B 3:D3:9E:55:88:F1:5C:A3:9F:40:A8:4A:92:85:3C:F3:7E:8B:8E:D4:96:7B:54:D6:00:EF:3F:47:5A:5D:CF:C4:F7:59:9E:B7:84:C6:D1:9F:59:54:A5:81:5D:27:31:8A:A6:0A:38:C5:7D:0A:14:06: EE:7A:02:D7:A8:31:76:88:66:EE:14:80:CB:92:F2:66:44:E9:63:C1:93:C9:1D:21:14:FC:60:23:BE:6F:F4:47:5E:F7:B2:A3:08:C0:27:72:71:58:2E:23:1F:02:03:01:00:01 </pre>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Authority Key Identifier	<i>14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB</i>
Authority Info Access	<i>http://acedicom.edicomgroup.com/certs/caedicomroot.cer</i> <i>http://ocsp.acedicom.edicomgroup.com/caedicomroot</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.30051.2.3.1.1</i> <i>CPS text: [Certification Practice Statement]</i> <i>CPS pointer: http://acedicom.edicomgroup.com</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
CRL Distribution Points	<i>http://acedicom.edicomgroup.com/caedicomroot.crl</i>
Subject Key Identifier	<i>06:CE:5F:AA:B1:96:26:CD:B5:3F:AD:8E:61:9A:F5:47:21:A7:F9:05</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>

Thumbprint:

B2:11:C4:8C:2B:D4:50:66:DD:DC:3C:62:65:8B:13:5D:85:FE:13:05:89:6F:E3:2F:A
A:2B:E7:0B:A4:AA:07:73

X509SubjectName**Subject C:**

ES

Subject L:

PATERNA

Subject O:

EDICOM CAPITAL SL

Subject 2.5.4.97:

VATES-B96490867

Subject SERIAL NUMBER:

B96490867

Subject CN:

CAEDICOM04

X509SKI**X509 SK I**

Bs5fqrGWjs21P62OYZr1RyGn+QU=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2025-12-18T00:00:00Z

14.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

14.8.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

14.8.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en]

undefined.

[es]

undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.26
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.23
Description		

14.8.4 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service Name		
Name	[en]	Qualified certificates issued by the CAEDICOM04
Name	[es]	Certificados cualificados emitidos por CAEDICOM04
Service digital identities		
Certificate fields details		
Version:	3	
Serial Number:	281263316054875990527557336648097697286431660675	
X509 Certificate	-----BEGIN CERTIFICATE----- MIH0JCBSqgAwIBAgIUUMURhpcFr40+VU3q0ADqeGFnW6MwDOYKozZlhcNAQELBQAwNjEWMBOG A1UEAwNQOFFREIDT00gUm9vdDEPMADGA1UECgwGRURJQ09NMQswCOYDVOQGEWJFUzAeFw0yMTA5 MjMxMzUwMjBafw0zNDAlMjEwMDIwMDBaMH4eZARBgNVBAMTCKNBURJQ09NMDOXqEJAQBgNVBAUT CUI5NQSMQDg2N2EYMBYGA1UEYmMPVXVURVMOXk2NDkwODY3MlR0wGAYDVQKEAFFREIDT00gOQFO SVRBTCBTTDEQMA4GA1UEBxMHUEFURVJQOTELMAKGA1UEBhMCRVMwggglMA0GCsgGSib3DOEBAQUA A4ICDwAggkKAOICAOQCKixyTK1kPmGA6RRon2Ogw5JU++OS1hceZlDdyKcT657wDAxO25GWA4a EJPESLcdseh3KvX1leikiiPPhrywVhGNMuY0v1VHDjCCgU2MynjAestbZ2uw2kTqVWpCblFv ktgYbLUMswcCV90hXQ7PP75uagig9FU/EZ+xcXEFs3hNEaxnj8/PRELbhoTHNQTLeOnwEm98n W6RGp7k+E/BssTHaZogI8F31ZEmdipWJArDgyFmZMj4qIM52gbrsRuvsD9l3wNcYruGw/2xPm eu5I7e70mly3s4S0890NyrwBWZmk615cRcm11czurqRAUKjPcnDHHNhe78SN3s9VLx2i5s relResVcbDH7z5gWJLYTUXV6Fduh80HXvmXD20bUWJyo4JAh65jPKf0sRk77Z8WC6AuhztHCg3 7Jb8se2vKOWjGKWSGFaLQaCjsg8Uw7K08PgP9lzc5MgEWxVQ5Z0EN7F0legx7gC0kEqeFR6Gf72 OhnhXHeER09YWWuucFhW71nfrUWC6pW2055VpPCs39AqEgShTzfoU01JZVNYA7zSHW3P xPdzNreExtGRVWslgV0nMYqmCjFQOUbu56AteoMxaiZu4UsMu58mZE6WPB8kdIR8YCO+b/RH XueyowvA3jxWC4JHwIDAQABo4IBjCCAfowEgYDVROTAQH/BAGwBgEB/wiBADAfBgNVH5MEGDAW gbQUlSp2GOGYrRn0u2H4FAdesjzCbkWYKwYBBQUHQAQEEgY1wqYmWQqYKwYBBQUHMAKGNmho dHA6Ly9hY2VkaWV5bW55ZGZlbnNcm91c35ib20vY2VydHMvY2FIZGJlb21y6290LmNlcjA9Bggg BgEgFBQcAwY1xaHR0cDovL29jc3AUYWNlZGJlb20uZWRRPy29tZ3JvdXAuY29tL2NhZWRRPy29cm9v dDcBbmVYDVR0BICFMIGOMGMBgwBgEgEAHqYwIDAQEWBDB0ggrBgEFBQDCCAJBCHk4AQAIAHIA dABPAGYAAQBAQAGEAdABpAG8AbgAgAFAcBgAGMADABoBAGMAZQAgAFMAQABhAQAZQBAGUAbgB0 MCSGCCsGAQUFBwIBFh9odHRwOi8vYWNlZGJlb20uZWRRPy29tZ3JvdXAuY29tL2NhZWRRPy29cm9v dDcBbmVYDVR0BICFMIGOMGMBgwBgEgEAHqYwIDAQEWBDB0ggrBgEFBQDCCAJBCHk4AQAIAHIA dABPAGYAAQBAQAGEAdABpAG8AbgAgAFAcBgAGMADABoBAGMAZQAgAFMAQABhAQAZQBAGUAbgB0 Y29tZ3JvdXAuY29tL2NhZWRRPy29tcm9vZC5jcmmwHOYDVR00OB9YEFABOX6xlibNET+tmGa9Uch pKFM4AGAludDwEBwQEAWiBhANBgkqhkiG9w0BAQsFAAOCAQEA8sbDULP5QhmsJ307a4hmiXk YmDKSrnB6Cg3k8xNbnvXr0e3Tb4Hkxw6iEN6Nj14dcifkggz3leB9b9Wggs0KRLXoc6KGI77PY 4JYL2ly0sokG0EXCpuduG/HK+BkfuxejYv7b6nfrFJMPYOBEGbO7LHCgmV4lt0sX4R9ReuR+8e rtuAp8BU9hg5shih6EPigQ1MHSQIMu4f+RMCN39v8f2PYTKVDpOV+U85o0sr76i5ZAtvrtApEbD NyZu/ee558BIR655SOL6Hvar1yden1z0qm5a1Cpmog4P2fPz3PfZRAUULVQTEqH /nctfjWUjHOTYrqP1BcauMADz3A3uNVB6N7AZngRrRDZcx53qx08PwabLQ3P7LoRoy2ibnVoy CWcr065khjI651Vul62Y05fS2rWYonCev8Gkl1hXwGZxP3B/YdZpncjL5rohZd43v95lk D8dtVr+do5tAAK4K0Y9fLuu1MkOYV2B05B6mVnTAZL122mVb0Q12nVPLX865NkxMgAe +wQU1ti+cy439nPbu1GkDzwdW7B8K8A8mjrBcI/Z33VUShvuz/K45MeaX69hwnk6fOub+7gzOL soco5Ct36k4eK49U6rQtxmpN0122mk090N8rd60ckMNVn+73c= -----END CERTIFICATE-----	
Signature algorithm:	SHA256withRSA	
Issuer C:	ES	
Issuer O:	EDICOM	
Issuer CN:	CAEDICOM Root	
Subject C:	ES	
Subject L:	PATERNA	

Subject O: *EDICOM CAPITAL SL*

Subject 2.5.4.97: *VATES-B96490867*

Subject SERIAL NUMBER: *B96490867*

Subject CN: *CAEDICOM04*

Valid from: *Thu Sep 23 15:50:20 CEST 2021*

Valid to: *Sun May 21 12:20:00 CEST 2034*

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:90:90:8C:72:B5:32:B5:90:F9:86:03:A4:51:A0:DD:8E:AB:0E:7F:53:EF:8E:4B:
58:42:79:92:03:77:22:9C:4F:A4:8B:C3:40:31:38:6E:46:59:AE:1A:12:33:C4:49:F2:DC:75:27:A1:DC:AB:D7:23:57:A2:A6:48:A2:3C:F1:EB:C8:05:61:18:D3:2E:63:4B:03:8C:70:E2:FC:21:A
9:53:63:32:88:90:2C:B5:B6:76:8B:0D:A4:4E:01:56:68:F0:9B:2D:21:6F:92:D7:60:61:B2:D4:32:CC:1C:09:5F:4E:85:74:3B:3C:FE:F9:B9:A8:22:83:D1:54:FC:46:7E:C6:47:17:11:FB:37:84:
D1:1A:C6:78:FC:FA:C4:2D:88:68:60:73:50:4C:B7:88:3A:7C:04:9B:DF:27:5B:A4:46:A7:B9:3E:13:F0:6C:B1:31:DA:66:88:09:94:11:77:D7:61:26:76:3A:4F:58:90:2B:74:6C:85:99:93:0
9:E2:A2:4C:E5:98:3C:AE:C4:6E:BE:C0:F0:20:8D:F0:35:C6:2B:8B:6C:3F:0B:13:E6:7A:E9:79:23:B7:8B:02:67:F2:DE:CE:12:D0:1F:68:37:2A:F0:05:66:66:E8:AF:F5:B1:C4:5C:AE:18:75:73:
6C:EF:46:A4:40:52:42:23:45:C9:C3:1C:73:61:E8:BF:12:36:5D:F1:F5:52:D7:CE:54:AC:AD:E2:D1:EA:C5:5C:6C:31:FB:CF:98:16:24:B2:98:4D:45:D5:E8:57:6E:67:CD:07:5E:F8:A6:5C:3D:B
4:6D:45:BF:CA:8E:09:02:1E:92:25:F5:DF:D2:C4:64:4F:B6:7C:58:2E:80:BA:1C:ED:1C:21:B7:EC:96:C1:B1:ED:AF:29:05:A3:1A:45:92:18:56:8B:41:A0:A3:B1:C1:BC:53:0E:CA:D3:C3:E0:3F
4:D2:33:72:C3:20:11:6C:55:41:26:74:10:DE:C5:D1:F7:A0:C7:8B:02:02:41:2A:79:F4:7A:19:F7:F6:42:18:A1:43:11:DE:11:E4:4E:F5:85:96:AE:E7:2B:16:15:BB:D6:77:C8:B9:60:B2:EA:95:B
3:D3:9E:55:88:F1:5C:A3:9F:40:A8:4A:92:85:3C:F3:7E:8B:8E:D4:96:7B:54:D6:00:EF:3F:47:5A:5D:CF:C4:F7:59:9E:B7:84:C6:D1:9F:59:54:A5:81:5D:27:31:8A:A6:0A:38:C5:7D:0A:14:06:
EE:7A:02:D7:A8:31:76:88:66:EE:14:80:CB:92:F2:66:44:E9:63:C1:93:C9:1D:21:14:FC:60:23:8E:6F:F4:47:5E:F7:B2:A3:08:C0:27:72:71:58:2E:23:1F:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB*

Authority Info Access
http://acedicom.edicomgroup.com/certs/caedicomroot.cer
http://ocsp.acedicom.edicomgroup.com/caedicomroot

Certificate Policies
Policy OID: 1.3.6.1.4.1.30051.2.3.1.1
CPS text: [Certification Practice Statement]
CPS pointer: http://acedicom.edicomgroup.com

Extended Key Usage *id_kp_serverAuth*

CRL Distribution Points *http://acedicom.edicomgroup.com/caedicomroot.crl*

Subject Key Identifier *06:CE:5F:AA:B1:96:26:CD:B5:3F:AD:8E:61:9A:F5:47:21:A7:F9:05*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B2:11:C4:8C:2B:D4:50:66:DD:DC:3C:62:65:8B:13:5D:85:FE:13:05:89:6F:E3:2F:A
A:2B:E7:0B:A4:AA:07:73*

X509SubjectName

Subject C: *ES*

Subject L: *PATERNA*

Subject O: *EDICOM CAPITAL SL*

Subject 2.5.4.97: *VATES-B96490867*

Subject SERIAL NUMBER: B96490867

Subject CN: CAEDICOM04

X509SKI

X509 SK I Bs5fqrGWjs21P62OYZr1RyGn+QU=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2024-06-05T00:00:00Z

14.8.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.8.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.8.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.30051.2.3.2.26

Description

14.8.5 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by the CAEDICOM04

Name [es] Certificados cualificados emitidos por CAEDICOM04

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject L: *PATERNA*

Subject O: *EDICOM CAPITAL SL*

Subject 2.5.4.97: *VATES-B96490867*

Subject SERIAL NUMBER: *B96490867*

Subject CN: *CAEDICOM04*

X509SKI

X509 SK I *Bs5fqrGWJs21P62OYZr1RyGn+QU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-01-11T02:00:00Z*

14.8.5.4 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

14.8.5.5 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

14.9 - Service (granted): Servicio cualificado de conservación de sellos electrónicos cualificados 2022

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service type description *[en]* *A preservation service for qualified electronic signatures.*
[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name *[es]* *Servicio cualificado de conservación de sellos electrónicos cualificados 2022*

Name [en] Preservation of qualified electronic seals 2022

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2022-05-31T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

14.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

14.10 - Service (granted): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados emitido por CAEDICOM04

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service type description [en] undefined.
[es] undefined.

Service Name

Name [es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados emitido por CAEDICOM04

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals by CAEDICOM04

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2022-06-29T00:00:00Z

14.10.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.10.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.11 - Service (granted): Servicio cualificado de entrega electrónica certificada EDICOM (2022)**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description	[en]	An electronic delivery service providing qualified electronic deliveries.
	[es]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name	[es]	Servicio cualificado de entrega electrónica certificada EDICOM (2022)

Name	[en]	Qualified electronic registered delivery service EDICOM (2022)

Service digital identities**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time

2022-10-20T00:00:00Z

14.12 - Service (granted): Sellos cualificados de tiempo emitidos por TSA EDICOM 2024**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[es]	Sellos cualificados de tiempo emitidos por TSA EDICOM 2024

Name	[en]	Qualified timestamps issued by TSA EDICOM 2024

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2024-06-10T00:00:00Z

14.13 - Service (granted): Servicio cualificado de entrega electrónica certificada EDICOM 2024

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description [en] An electronic delivery service providing qualified electronic deliveries.

[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name [es] Servicio cualificado de entrega electrónica certificada EDICOM 2024

Name [en] Qualified electronic registered delivery service EDICOM 2024

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2024-06-05T00:00:00Z

14.14 - Service (granted): Servicio cualificado de conservación de sellos electrónicos cualificados 2024

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

Service type description [en] A preservation service for qualified electronic signatures.

[es] Un servicio de la preservación de las firmas electrónicas reconocidas.

Service Name

Name [es] Servicio cualificado de conservación de sellos electrónicos cualificados 2024

Name [en] Preservation of qualified electronic seals 2024

Service digital identities

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2024-06-05T00:00:00Z

14.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

14.15 - Service (granted): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados 2024

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Service type description [en] undefined.
[es] undefined.

Service Name

Name [es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados 2024

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals 2024

Service digital identities

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2024-06-05T00:00:00Z

14.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

14.15.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

15 - TSP: Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

TSP Name

Name	[en]	Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)
Name	[es]	Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

TSP Trade Name

Name	[en]	Ministerio de Defensa de España
Name	[es]	Ministerio de Defensa de España
Name	[en]	MDEF
Name	[es]	MDEF
Name	[en]	VATES-S2800231I
Name	[en]	MINISTERIO DE DEFENSA
Name	[es]	MINISTERIO DE DEFENSA

PostalAddress

Street Address	[en]	C/ Arturo Soria, 289
Locality	[en]	Madrid
State Or Province	[en]	Madrid
Postal Code	[en]	28071
Country Name	[en]	ES

PostalAddress

Street Address	[es]	C/ Arturo Soria, 289
Locality	[es]	Madrid
State Or Province	[es]	Madrid

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name		
Name	[en]	Qualified Certificates issued by Ministerio de Defensa de España
Name	[es]	Certificados reconocidos emitidos por CA MINISDEF-EC-WPG

Certificate fields details

Version:	3
Serial Number:	111762255326584813916284623438012473554
X509 Certificate	-----BEGIN CERTIFICATE-----

Page 636

Signature algorithm: *SHA1withRSA*

Issuer CN: *MINISDEF-EC-RAIZ*

Issuer OU: *PKI*

Issuer O: *MDEF*

Issuer C: *ES*

Subject CN: *MINISDEF-EC-WPG*

Subject OU: *PKI*

Subject O: *MDEF*

Subject C: *ES*

Valid from: *Wed Sep 15 10:27:21 CEST 2010*

Valid to: *Wed Sep 15 10:27:21 CEST 2021*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:56:5B:53:DB:70:07:EC:21:86:8B:08:EC:44:CE:24:6B:41:8C:4F:4B:F3:CD:F7:1D:5F:66:8C:89:BF:CE:CD:87:88:93:91:3F:8C:79:27:D2:94:F0:C7:7C:8F:5A:27:FC:8D:36:18:43:C7:7D:9C:CD:27:D0:1E:2D:3F:8A:3B:4E:D2:4E:B1:5F:85:A1:96:6F:A7:FB:C8:1C:90:B3:A0:E4:FF:DF:A4:6D:DD:15:A2:53:C4:C2:06:83:95:07:85:85:65:35:E0:AD:34:27:AC:6C:95:71:17:2A:7E:06:8B:B2:E8:74:AF:24:59:C2:99:C7:6E:F5:B3:D8:FF:20:D1:AC:41:A8:12:DE:92:31:BF:45:40:74:9B:D4:3F:30:C4:75:7E:03:88:21:46:9D:72:04:CF:85:13:AF:25:38:2B:5D:5A:2A:66:39:1D:BF:EC:C6:D2:C3:BC:94:78:FD:D4:6F:2A:C2:AA:27:37:BC:2C:89:4A:25:B5:A4:7C:88:09:A7:14:65:AD:41:57:1E:69:61:9A:9C:AD:85:5F:E2:EC:90:8F:A1:FA:12:A8:B2:75:FA:34:9F:94:4C:4C:70:82:CD:67:69:FF:93:51:2E:76:8F:FA:2B:83:CB:F9:D8:CE:57:DB:CF:71:F2:72:C8:F5:F6:BC:F1:F3:66:01:5C:8B:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*

Authority Key Identifier *8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*

Certificate Policies
Policy OID: 2.16.724.1.1.1.1.1
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
Policy OID: 2.16.724.1.1.1.1.2
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
Policy OID: 2.16.724.1.1.1.1.3
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
Policy OID: 2.16.724.1.1.1.1.4
CPS pointer: <http://pki.mdef.es/cps/cps.htm>

Subject Alternative Name *CN=Entidad de Certificacion Subordinada WPG, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES*

CRL Distribution Points
Idap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
Idap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
<http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl>

Subject Key Identifier	AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2
Authority Key Identifier	8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D
Certificate Policies	Policy OID: 2.16.724.1.1.1.1.2 CPS pointer: http://pki.mdef.es/cps/cps.htm Policy OID: 2.16.724.1.1.1.1.3 CPS pointer: http://pki.mdef.es/cps/cps.htm Policy OID: 2.16.724.1.1.1.1.4 CPS pointer: http://pki.mdef.es/cps/cps.htm
CRL Distribution Points	Idap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,D C=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint Idap://Idap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	4E:27:9E:AE:24:E4:76:CA:89:50:7D:E8:F5:07:54:EE:57:CB:55:C0:39:4C:AC:7F:9C:A3:4E:C7:6D:47:0E:13
Signature fields details	
Version:	3
Serial Number:	53763582439856554449625523294782906924
X509 Certificate	-----BEGIN CERTIFICATE----- MIIG7jCCBNagAwIBAgIQH9RPudvzRFERgbZohILDANBghkhiG9w0BAQUFADBFMOswCOYDVOQG EwJfUzENMAsGA1UEChMETURFRjEMMAoGA1UECxDUUEtjMRkwFwYDQ0ExBNSU5jU0RFRi1Foy15 QlUaMB4XDTA2MDkyMDEwMTc1MioXDTYyMDkyMDEwMTc1MiowRDELMAkGA1UEBnMCRVmxkDTALBgNV BAAQTBElRUxYDDAKBgNVBAsTA1BLSTYEMBYGA1UEAxMTUOSVNERURyUmxv1BHMIIIBjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvZbU9twB+whhos17ETOjGtBjE9L8BD3HV9mjllvsz2H iJORP4x5j9KUBM8j1on/lo2GEPHfzNj9AeLT+K0075ToFtaGWb6f7yByds6Dk9+k1N0VgIPe wgaDIOqfNWU14K0j06sxKXK4dG7Lo4B8KwK2x27159jNCS0ag53a1xv0VAgjvLp2EoK4D iCFcnXIE24UTrY4K11akmY5Hb/sxtLDvjR4/dRvKsKajze8LIJpWkfjZpkRlRUFXhmlhmpyt hV7i7CiofoSquL+jsfExMcILNznk1Eudo6K4PL+dv0V9vPcfjyYPx2vPHzgzFcuwIDAQAB o4ICZTCCAAtUwDwYDVROTAQHBAUwwAwEBAAQBgNVH0SBABEBAMCAQYWHYOYDV00BBYEFKvjU5GA Wlp2D8dG27CbiatascqyMhwGA1UdIwR1MHOAFiwwVD3uHMA/CRU8N2hB3QAKExO9oUmkRzBFMOsw COYDVOQGEwJfUzENMAsGA1UEChMETURFRjEMMAoGA1UECxDUUEtjMRkwFwYDQ0ExBNSU5jU0RFR i1Foy15QlUaBghAAnHtp3b0G5Gcz3lied5MG8BgNVH5ABAFBgEwga4wOAYYIVUAQEBAGW LDAqBggrBgEFBQCCARyEaHR0cDovL3Bra5StZGVmlmVzL2Nwcy9jcmuaHRtMDgCGCGFVAEBAQED MCwKqY7KwYBBOUHAqEWHmh0dHA6Ly9wa2kubWRLZi5icy9jcmVvY3B2Lmh0bTA4BghghVQBAQEB BDA5MCoGCCCAQUFEBwIBF5odhRwOibvGtpLn1kZWYyZXNvY3B2L2Nwcy5odG0wagFUBgNVHRBE ggFLMIIBR2CCAUIOggGE/oiBO4aBuGxkYXA6Ly8vQ049TUOSVNERURyUmxv1BHMIIIBjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvZbU9twB+whhos17ETOjGtBjE9L8BD3HV9mjllvsz2H iJORP4x5j9KUBM8j1on/lo2GEPHfzNj9AeLT+K0075ToFtaGWb6f7yByds6Dk9+k1N0VgIPe wgaDIOqfNWU14K0j06sxKXK4dG7Lo4B8KwK2x27159jNCS0ag53a1xv0VAgjvLp2EoK4D iCFcnXIE24UTrY4K11akmY5Hb/sxtLDvjR4/dRvKsKajze8LIJpWkfjZpkRlRUFXhmlhmpyt hV7i7CiofoSquL+jsfExMcILNznk1Eudo6K4PL+dv0V9vPcfjyYPx2vPHzgzFcuwIDAQAB o4ICZTCCAAtUwDwYDVROTAQHBAUwwAwEBAAQBgNVH0SBABEBAMCAQYWHYOYDV00BBYEFKvjU5GA Wlp2D8dG27CbiatascqyMhwGA1UdIwR1MHOAFiwwVD3uHMA/CRU8N2hB3QAKExO9oUmkRzBFMOsw COYDVOQGEwJfUzENMAsGA1UEChMETURFRjEMMAoGA1UECxDUUEtjMRkwFwYDQ0ExBNSU5jU0RFR i1Foy15QlUaBghAAnHtp3b0G5Gcz3lied5MG8BgNVH5ABAFBgEwga4wOAYYIVUAQEBAGW LDAqBggrBgEFBQCCARyEaHR0cDovL3Bra5StZGVmlmVzL2Nwcy9jcmuaHRtMDgCGCGFVAEBAQED MCwKqY7KwYBBOUHAqEWHmh0dHA6Ly9wa2kubWRLZi5icy9jcmVvY3B2Lmh0bTA4BghghVQBAQEB BDA5MCoGCCCAQUFEBwIBF5odhRwOibvGtpLn1kZWYyZXNvY3B2L2Nwcy5odG0wagFUBgNVHRBE ggFLMIIBR2CCAUIOggGE/oiBO4aBuGxkYXA6Ly8vQ049TUOSVNERURyUmxv1BHMIIIBjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvZbU9twB+whhos17ETOjGtBjE9L8BD3HV9mjllvsz2H iJORP4x5j9KUBM8j1on/lo2GEPHfzNj9AeLT+K0075ToFtaGWb6f7yByds6Dk9+k1N0VgIPe wgaDIOqfNWU14K0j06sxKXK4dG7Lo4B8KwK2x27159jNCS0ag53a1xv0VAgjvLp2EoK4D iCFcnXIE24UTrY4K11akmY5Hb/sxtLDvjR4/dRvKsKajze8LIJpWkfjZpkRlRUFXhmlhmpyt hV7i7CiofoSquL+jsfExMcILNznk1Eudo6K4PL+dv0V9vPcfjyYPx2vPHzgzFcuwIDAQAB o4ICZTCCAAtUwDwYDVROTAQHBAUwwAwEBAAQBgNVH0SBABEBAMCAQYWHYOYDV00BBYEFKvjU5GA Wlp2D8dG27CbiatascqyMhwGA1UdIwR1MHOAFiwwVD3uHMA/CRU8N2hB3QAKExO9oUmkRzBFMOsw COYDVOQGEwJfUzENMAsGA1UEChMETURFRjEMMAoGA1UECxDUUEtjMRkwFwYDQ0ExBNSU5jU0RFR i1Foy15QlUaBghAAnHtp3b0G5Gcz3lied5MG8BgNVH5ABAFBgEwga4wOAYYIVUAQEBAGW LDAqBggrBgEFBQCCARyEaHR0cDovL3Bra5StZGVmlmVzL2Nwcy9jcmuaHRtMDgCGCGFVAEBAQED MCwKqY7KwYBBOUHAqEWHmh0dHA6Ly9wa2kubWRLZi5icy9jcmVvY3B2Lmh0bTA4BghghVQBAQEB BDA5MCoGCCCAQUFEBwIBF5odhRwOibvGtpLn1kZWYyZXNvY3B2L2Nwcy5odG0wagFUBgNVHRBE ggFLMIIBR2CCAUIOggGE/oiBO4aBuGxkYXA6Ly8vQ049TUOSVNERURyUmxv1BHMIIIBjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvZbU9twB+whhos17ETOjGtBjE9L8BD3HV9mjllvsz2H iJORP4x5j9KUBM8j1on/lo2GEPHfzNj9AeLT+K0075ToFtaGWb6f7yByds6Dk9+k1N0VgIPe wgaDIOqfNWU14K0j06sxKXK4dG7Lo4B8KwK2x27159jNCS0ag53a1xv0VAgjvLp2EoK4D iCFcnXIE24UTrY4K11akmY5Hb/sxtLDvjR4/dRvKsKajze8LIJpWkfjZpkRlRUFXhmlhmpyt hV7i7CiofoSquL+jsfExMcILNznk1Eudo6K4PL+dv0V9vPcfjyYPx2vPHzgzFcuwIDAQAB o4ICZTCCAAtUwDwYDVROTAQHBAUwwAwEBAAQBgNVH0SBABEBAMCAQYWHYOYDV00BBYEFKvjU5GA Wlp2D8dG27CbiatascqyMhwGA1UdIwR1MHOAFiwwVD3uHMA/CRU8N2hB3QAKExO9oUmkRzBFMOsw COYDVOQGEwJfUzENMAsGA1UEChMETURFRjEMMAoGA1UECxDUUEtjMRkwFwYDQ0ExBNSU5jU0RFR i1Foy15QlUaBghAAnHtp3b0G5Gcz3lied5MG8BgNVH5ABAFBgEwga4wOAYYIVUAQEBAGW LDAqBggrBgEFBQCCARyEaHR0cDovL3Bra5StZGVmlmVzL2Nwcy9jcmuaHRtMDgCGCGFVAEBAQED MCwKqY7KwYBBOUHAqEWHmh0dHA6Ly9wa2kubWRLZi5icy9jcmVvY3B2Lmh0bTA4BghghVQBAQEB BDA5MCoGCCCAQUFEBwIBF5odhRwOibvGtpLn1kZWYyZXNvY3B2L2Nwcy5odG0wagFUBgNVHRBE ggFLMIIBR2CCAUIOggGE/oiBO4aBuGxkYXA6Ly8vQ049TUOSVNERURyUmxv1BHMIIIBjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvZbU9twB+whhos17ETOjGtBjE9L8BD3HV9mjllvsz2H iJORP4x5j9KUBM8j1on/lo2GEPHfzNj9AeLT+K0075ToFtaGWb6f7yByds6Dk9+k1N0VgIPe wgaDIOqfNWU14K0j06sxKXK4dG7Lo4B8KwK2x27159jNCS0ag53a1xv0VAgjvLp2EoK4D iCFcnXIE24UTrY4K11akmY5Hb/sxtLDvjR4/dRvKsKajze8LIJpWkfjZpkRlRUFXhmlhmpyt hV7i7CiofoSquL+jsfExMcILNznk1Eudo6K4PL+dv0V9vPcfjyYPx2vPHzgzFcuwIDAQAB o4ICZTCCAAtUwDwYDVROTAQHBAUwwAwEBAAQBgNVH0SBABEBAMCAQYWHYOYDV00BBYEFKvjU

Issuer C: *ES*
Subject CN: *MINISDEF-EC-WPG*
Subject OU: *PKI*
Subject O: *MDEF*
Subject C: *ES*
Valid from: *Wed Sep 20 12:17:52 CEST 2006*
Valid to: *Thu Sep 20 12:17:52 CEST 2012*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:56:5B:53:D8:70:07:EC:21:86:8B:08:EC:44:CE:24:68:41:8C:4F:4B:F3:CD:F7:1D:5F:66:8C:89:8F:CE:CD:87:88:93:91:3F:8C:79:27:D2:94:F0:C7:7C:8F:5A:27:FC:8D:36:18:43:C7:7D:9C:CD:27:D0:1E:2D:3F:8A:3B:4E:D2:4E:81:5F:B5:A1:96:6F:A7:FB:C8:1C:90:B3:A0:E4:FF:DF:A4:60:DD:15:A2:53:C4:C2:06:83:95:07:85:85:65:35:E0:AD:34:27:AC:6C:95:71:17:2A:7E:06:8B:B2:E8:74:AF:24:59:C2:99:C7:6E:F5:B3:D8:FF:20:D1:AC:41:A8:12:DE:92:31:BF:45:40:74:9B:D4:3F:30:C4:75:7E:03:88:21:46:9D:72:04:CF:85:13:AF:25:38:2B:5D:5A:2A:66:39:1D:BF:EC:C6:D2:C3:BC:94:78:FD:D4:6F:2A:C2:AA:27:37:BC:2C:89:4A:25:B5:A4:7C:88:09:A7:14:65:AD:41:57:1E:69:61:9A:9C:AD:85:5F:E2:EC:90:8F:A1:FA:12:A8:B2:75:FA:34:9F:94:4C:4C:70:82:CD:67:69:FF:93:51:2E:76:8F:FA:2B:83:CB:F9:D8:CE:57:DB:CF:71:F2:72:C8:F5:F6:BC:F1:F3:66:01:5C:BB:02:03:01:00:01*
Basic Constraints *IsCA: true*
Subject Key Identifier *AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*
Authority Key Identifier *8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*
Certificate Policies *Policy OID: 2.16.724.1.1.1.1.2*
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
Policy OID: 2.16.724.1.1.1.1.3
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
Policy OID: 2.16.724.1.1.1.1.4
CPS pointer: <http://pki.mdef.es/cps/cps.htm>
CRL Distribution Points *ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,D C=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*
ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *49:D2:25:4C:1C:9F:02:F1:E6:B5:CC:DE:9C:2E:B7:79:CD:0D:A3:D9:93:90:8F:6D:8D:43:7B:57:C9:A2:D4:A7*

X509SubjectName

Subject CN: *MINISDEF-EC-WPG*
Subject OU: *PKI*

Subject O: *MDEF*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

15.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.1.1.1.1.2.14*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.1.1.1.1.3.14*

15.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by Ministerio de Defensa de España*

Name [es] *Certificados reconocidos emitidos por CA MINISDEF-EC-WPG*

Service digital identities**X509SubjectName**Subject CN: *MINISDEF-EC-WPG*Subject OU: *PKI*Subject O: *MDEF*Subject C: *ES***X509SKI**X509 SK I *q+O5IYBb+nYPx0bbsJulC1qxyrl=***Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time** *2016-06-30T22:00:00Z*15.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**Identifier *[OIDA sURN]* *urn:oid:2.16.724.1.1.1.1.2.14***Policy Identifier:**Identifier *[OIDA sURN]* *urn:oid:2.16.724.1.1.1.1.3.14*15.1.3.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformationURI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*15.1.4 - History instance n.2 - Status: undersupervision**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name**

Name [en] Qualified Certificates issued by Ministerio de Defensa de España

Name [es] Certificados reconocidos emitidos por CA MINISDEF-EC-WPG

Service digital identities

X509SubjectName

Subject CN: MINISDEF-EC-WPG

Subject OU: PKI

Subject O: MDEF

Subject C: ES

X509SKI

X509 SK I q+O5IYBb+nYPx0bbsJlC1qxyrl=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-04-30T00:00:00Z

15.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:2.16.724.1.1.1.1.2.14

Policy Identifier:

Identifier [OIDASURN] urn:oid:2.16.724.1.1.1.1.3.14

15.2 - Service (granted): Qualified Certificates issued by Ministerio de Defensa de España 2016

Subject C: *ES*

Valid from: *Thu Sep 08 09:51:27 CEST 2016*

Valid to: *Wed Sep 08 09:51:27 CEST 2027*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9A:8F:DA:E8:27:E9:F6:FF:BB:62:AD:D5:AA:9D:66:C5:21:EF:36:2E:B9:3B:AE:04:08:49:1D:36:40:69:88:9C:4F:77:62:98:84:3F:72:64:97:FD:E2:4D:AF:11:49:58:03:5E:E8:A9:3C:2A:1A:ED:F8:85:25:26:9F:D2:AE:9D:55:D6:09:4D:B3:16:71:37:1B:4C:02:89:F0:85:F8:D3:00:D6:74:DE:48:AF:C9:CF:DD:47:30:8F:7D:91:F3:48:5F:C1:55:F4:F6:EC:2B:F8:73:41:72:E6:F8:4E:9E:C7:AB:D5:0F:E2:CB:39:C2:13:02:DF:54:35:8E:95:FA:58:02:9A:93:9B:5F:CF:89:08:10:E1:82:56:27:CB:6A:82:A7:AA:0A:DB:42:50:17:93:ED:7A:6F:A2:13:CD:35:C0:19:6D:F1:24:76:66:11:B7:36:5D:1F:43:FE:D7:44:A4:18:AB:B5:5A:95:42:DD:F8:B3:26:80:20:44:C2:21:A7:2D:C6:DE:7E:1C:34:1D:C3:77:97:8F:0F:DC:31:CB:FD:03:A9:5B:0E:6E:42:29:FF:0F:D2:CA:38:48:16:56:2C:FE:3A:2F:96:0A:F3:09:6C:3F:0E:8F:C5:84:50:15:23:46:29:87:15:39:A:C5:C9:E0:4D:35:18:A2:42:4C:D3:B8:F2:84:B3:BD:12:94:DF:8D:08:38:58:05:C2:8A:43:05:08:4B:85:98:C6:82:4D:5D:19:53:2C:7F:10:2A:A4:C0:C6:85:93:B3:D7:ED:3D:E9:21:95:F9:A:6:8C:D8:1E:22:87:E7:68:18:55:0F:8E:BC:32:74:A6:6F:17:F8:2B:04:D4:FA:D3:24:D9:1C:0C:22:A4:E0:93:EB:6F:F3:27:4A:06:4A:71:C2:47:FA:F1:0C:91:C5:1A:69:CF:2F:3B:80:D9:FF:01:02:1F:61:36:5C:9F:3E:B6:9D:D0:36:6A:E8:6D:4B:4C:5C:20:E8:EE:CC:4A:08:9F:B1:59:8A:EA:30:0E:30:E6:F1:2E:32:A2:99:41:16:06:76:6E:F2:D0:2D:88:C5:2D:EE:67:C5:F4:D0:B3:98:11:D6:02:35:0F:29:2A:B6:70:5C:95:09:F7:26:1D:55:62:93:EC:93:C8:39:AF:F0:28:7C:E7:76:A8:EB:E9:07:D8:FA:16:72:9C:E0:DB:08:F6:D4:A7:01:37:B1:8E:6E:04:A5:5D:99:DE:B5:AA:8F:76:33:E4:60:C9:6D:A1:09:84:46:61:9B:E7:53:EB:6A:1A:BC:14:4C:E2:2D:FF:34:1A:CD:26:16:DA:1D:66:AD:19:39:F1:7B:1D:55:F0:EF:CD:9E:BD:05:41:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *91:54:98:88:CF:3E:55:96:34:8E:E5:77:BF:17:74:0F:EE:EA:08:D2*

Authority Key Identifier *8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://pki.mde.es/dpc/
CPS text: [Certificado de la Entidad de Certificacion Subordinada WPG2016 del Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).]

Subject Alternative Name *mail: agpmd@oc.mde.es*
CN=Entidad de Certificacion Subordinada WPG2016, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES

CRL Distribution Points *http://pki.mde.es/crl/DEFENSA-CRL-EC-RAIZ.crl*
ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *81:44:06:33:1B:97:9F:B1:4E:87:D1:CB:38:ED:0E:F2:BB:5B:EE:0A:1E:72:89:37:D6:BD:D5:D4:94:FC:D5:E6*

X509SubjectName

Subject CN: *DEFENSA-EC-WPG2016*

Subject 2.5.4.97: *VATES-S2800231I*

Subject OU: *PKI*

Subject O: *MINISTERIO DE DEFENSA*

Subject C: *ES*

X509SKI

X509 SK I*kVSYiM8+VZY0juV3vxd0D+7qCNI=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time*2018-10-08T01:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

15.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

15.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

15.2.4 - History instance n.1 - Status: withdrawn**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name**

Name [en] *Qualified Certificates issued by Ministerio de Defensa de España 2016*

Name [es] *Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

Service digital identities

X509SubjectName

Subject CN: *DEFENSA-EC-WPG2016*

Subject 2.5.4.97: *VATES-S2800231I*

Subject OU: *PKI*

Subject O: *MINISTERIO DE DEFENSA*

Subject C: *ES*

X509SKI

X509 SK I *kVSYiM8+VZY0juV3vxd0D+7qCNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Status Starting Time *2017-07-01T22:00:00Z*

15.2.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by Ministerio de Defensa de España 2016*

Name *[es]* *Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

Service digital identities**X509SubjectName**

Subject CN: *DEFENSA-EC-WPG2016*

Subject 2.5.4.97: *VATES-S2800231I*

Subject OU: *PKI*

Subject O: *MINISTERIO DE DEFENSA*

Subject C: *ES*

X509SKI

X509 SK I *kVSYiM8+VZY0juV3vxd0D+7qCNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-05-10T00:00:00Z*

15.2.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16 - TSP: Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.

TSP Name

Name	[en]	<i>Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.</i>
Name	[es]	<i>Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.</i>

TSP Trade Name

Name	[en]	<i>Izenpe, S.A</i>
Name	[es]	<i>Izenpe, S.A</i>
Name	[en]	<i>IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8</i>
Name	[es]	<i>IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8</i>
Name	[en]	<i>VATES-A01337260</i>
Name	[en]	<i>IZENPE S.A.</i>

PostalAddress

Street Address	[en]	<i>Avenida del Mediterráneo, 14</i>
Locality	[en]	<i>Vitoria-Gasteiz</i>
State Or Province	[en]	<i>Álava</i>
Postal Code	[en]	<i>1010</i>
Country Name	[en]	<i>ES</i>

PostalAddress

Street Address	[es]	<i>Avenida del Mediterráneo, 14</i>
Locality	[es]	<i>Vitoria-Gasteiz</i>
State Or Province	[es]	<i>Álava</i>
Postal Code	[es]	<i>1010</i>
Country Name	[es]	<i>ES</i>

Signature algorithm: *SHA1withRSA*

Issuer CN: *Izenpe.com*

Issuer O: *IZENPE S.A.*

Issuer C: *ES*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Valid from: *Tue Feb 24 09:05:46 CET 2009*

Valid to: *Sun Dec 13 00:00:00 CET 2037*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:A7:7E:89:81:F3:9B:E2:C2:83:A3:2E:94:FC:82:10:62:59:42:56:26:14:68:1B:31:0D:EB:2C:FF:E8:ED:19:2B:D6:C7:AD:B4:5D:49:C5:CB:72:55:00:FD:39:C8:77:6B:4A:F0:3D:96:5F:82:DA:70:D4:31:15:AA:7E:64:D9:57:57:23:91:0C:4E:A5:A8:36:3F:DD:64:20:E8:8D:B2:3C:68:DE:0A:D9:C9:52:8D:E0:19:4A:9E:E8:92:E0:1E:A0:CF:4D:E9:9D:6E:DC:EE:DC:80:98:7E:06:10:E3:74:85:33:F3:4D:41:16:DE:06:E2:67:EB:CA:E4:21:3C:6C:8F:FC:7A:D2:53:EC:17:00:98:2C:38:9E:4E:A8:CI:65:27:55:4C:EB:E3:38:5A:CE:F3:E2:67:56:C7:67:8D:6F:6B:AE:94:A2:89:86:35:0D:B7:AB:FD:D9:D6:9E:D0:A0:FC:25:92:66:0F:01:5E:17:40:58:C3:7F:7A:D6:7C:82:E3:93:C2:72:98:39:30:4D:3B:8B:B6:95:6D:EB:EC:9B:2A:85:0C:55:88:39:01:95:90:88:46:77:0F:7E:7F:28:43:33:4B:3E:93:94:35:84:0C:D4:7B:80:9E:81:2E:4F:C8:BD:C4:AD:57:36:82:55:FD:6F:45:2A:5E:F1:48:D2:57:CA:B3:8F:82:CB:46:77:AB:30:5D:C9:EC:30:2B:9F:9E:77:17:52:50:5C:2C:FF:F9:5C:D7:85:5F:5B:33:62:5F:5B:5C:F3:A3:84:52:E1:44:04:14:CD:7B:C6:63:BD:80:08:C5:15:F2:9E:B7:83:9C:F4:A5:31:E9:34:25:66:24:50:D1:EA:2A:27:28:4B:54:D3:3B:EA:01:F6:07:74:BB:A8:03:EC:33:69:42:46:B2:CD:D3:C2:D0:E0:1E:C4:D3:61:15:8E:5F:E3:E3:FF:65:96:8A:05:8B:FA:C6:22:4B:E4:D8:4D:1C:66:AF:15:DE:F1:6C:51:B1:22:8D:8B:3F:B3:8A:AE:11:73:01:78:F3:85:90:E4:B4:99:C2:8C:F1:8F:9D:72:29:C5:FF:60:79:FF:7E:17:7F:3D:99:AF:2D:80:F7:51:F3:2B:91:7B:0A:8B:C3:79:54:0F:AF:79:8E:89:51:F7:85:FC:DD:F9:03:19:83:CA:B0:DE:95:47:B9:BE:3B:06:3A:A0:BA:33:F2:EF:80:BA:06:20:84:6A:28:ED:AF:DB:E0:BE:C7:8F:68:2D:EC:1B:56:72:64:AD:08:48:16:D6:66:4B:E0:96:F5:DC:C9:0A:02:C4:D0:13:D8:6B:81:53:8A:C6:C8:CE:9E:5C:32:57:0E:8F:39:02:03:01:00:01

Subject Alternative Name *http://www.izenpe.com*
info@izenpe.com
STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *A4:17:1D:4E:65:D7:EF:87:95:2E:7F:8E:B8:75:CB:05:8B:D3:8C:7D*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *26:26:B1:95:63:BC:78:D9:B1:44:2B:93:CE:98:D1:4A:1E:4B:74:26:4A:CC:90:22:2F:1F:3C:23:85:C2:73:37*

Certificate fields details

Version:

3

Serial Number:

44226866073358392262219520495746478787

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIH0TCCBSugAwIBAgIQIUXI2bFUAS5MvqVCVTRYwzALBqkqhkiG9w0BAQswODELMakGA1UEBHMCRV
MxMFA5B8NvBAQMcOlaRUSQR58TlkeUMRMwEYOYDVQDDAplemVucGUuY29tMB4XDTewMTAyMDA4
MTYwMioxOTM3MTU1MjZMDAwMFMowagCAzABgNvBAYTAkVTRH0wEgY0Y0Q0A4WkVVOEUuY29t
LjE6MDEGGA1UECwwwTlpaIfppdXJ0YVdpdmkgCHVibGlr2EglSBDZXI0aWZpY2FkbyBwdWlsawNl
IFNDSTFGMEQGA1UEAw9SGVycml0YXlqZXRhIEVYwWt1bmrUZW4gODEglSBDOSBkZSBdaXVxYWRh
bm92hkgRlW50aWRhZGVzCg0KTCACAlwDQYKZGZlbnCAQEBBQAQDggPADCcAggIBAA+nfomB
85vwoQJLPT8sh8WUJWJHr0GzHd6yZ600ZK9bHrRdScLclUA/Tn0Ztk8D2WX4LaCNQxFap+
ZNIxVYORDE6lqDY3WQg8I2yPgicCtnUo3GUGe6lGtHqDPtemdbtz3ICVfyQ43FSM/NNQRbe
Buln6bItasix80Psf++CLDg+Tq6ZSdvTovj0J1r08+JNVsdnjW9p7subY1DberdnWntCg
/CSWZq8BXhdaW8N/etZ8su0TwnKpOTBN0lu2JWD7tqtQxViDkBlZCIRnffn8oZNLpOUnBQM
1HiwnoEuT89xkLXNoJlVW9FKI7xSNjKyrOPstGd6swXcnsMCufnncXUIBcLP5XNeFX1szY9b
XPQJFLHRAQJzXjGTZwCMUv8p6SgZ0pThpKCMYjFD6R6onKEU0zvaAfZnLuoA+weaUJGss0n
08t4B7E02EVjUj4/9lloofuR/Gikik200Czq8V3VfUdeUvbs/s4quEXMBePOFKO50mckMBb+d
cinfZ85/38Xf2Zry3w91HzK3F7CovDeVQPr3mOlVH3tfd+QMZg8gw3pVHub47BggujPy74C6
BicEajtr9yvspePaC3sG1ZyXK05BOWZkvivKxyOoCNAZ2GuB0r9yM6eXDJ085AgMBAAQ
ggZMIIB1TCBwwYDVR0RBIC/MIG8hhVodHRwOi8vd3d3LmI6Zm5wZ55jb2Z6D2Iuzm9AaxplbnBI
LmNvbasBKTCTBjFHMELUGA1UECgw+SVpFTlBFFMuQ54glSBD5UYgOTAxMzM3MjYwLjVlNjZlUjZp
dC9yewERZ2ZdcpeibUMTA1N5bGNjglZ3pQcZBBGwNvBAAMOKZ2GegZGvSiE1ZG0ZAJyW5j
byBF8G9ymikZWegMTQglSawMTaxMCBwaXRCvcmhLudhc3RlaXowDwYDVR0TAQH/BAUwAwEB/zAO
BgNVH08BAfEBAMCAQYwHQYDVR0OBBYEFKQXHU5J1++HIS5/rh1ywwL04x9MB8GA1UdlwQYMBAA
FBOCZQ6o8V7HjP5LGSr1V0GwFMDOGA1UdlAQMDEwLWYER0gADANACUGCsGAOUF8wBwBhlo
dHRwOi8vd3d3LmI6Zm5wZ55jb2V3Y3ZzMDcGCcsGAOUF8wEBBcswKTAAnBggrBgEFQcswAYYbaHR0
cDovL29jc3AuaXplbnBILmNvTo4MDk0MDMGA1UdhWQsMCowKKAmoCSGlmh0dHA6Ly9icmwwaXpl
bnBILmNvbs59Z2xkYmUuLjZyZDlwCwYKZGZlbnCAQELAAICAQA3p2M3S3G6P1Q1Yuv8eDx
KfCuxvqnfQ5Ddp+dRndsGKjN45emgOKUGO6Aap8V507060rPue0E2KsH9ryRu89shSEVPge
IC95ITxtkM7M39xcIQHtBxkqyhtooDjY3y5Ocby0AAqHfSRh0jJlDm/Q5MR0KvptT8Ohoq
LkThe1uDrZSaCaozmakGgMDSpipCqSdlNzdyXyEd1pDlIAjGv4pjhYXz0LDID40
ODQ4tqdpvtt6a1Ll6BHwoahjaF+5N+lgUINYVC5S0MCKBhvg2hmj0L/UaLxol63+D0YAqexCB
aI3me3/sYHL7WgWrgpKNmqYh+eak5Vnbm4YMcGtKbhwL1vLizLe4gk8TgKerzAIGC/MN42Hlvj
ELCZC/NPKuU6nwmLjEKRBS5E9LZis3300uJhcYrDMUjnz20BmGwJ24BtNL506IEsOYWhz
TxVIC6tRgZK9vvBQlqTKYduH8uLZ0p3lcrKRSYTxRvUeTj5ryX240KjIMpPohqvjpOZ5Ql
F0rY1GPPgumXOyfHb+7Ibc4855PB/YtoD5HEpuYjz5IPbXURKjyn1Ydarw2lrB300RqoK0KZyZ
Fari7jWexjIRvqXTJUXj1HpeCZap+ih1m1pH4kd7hx5bdhww==

```

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

Izenpe.com

Issuer O:

IZENPE S.A.

Issuer C:

ES

Subject CN:

Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)

Subject OU:

NZZ Ziurtagiri publikoa - Certificado publico SCI

Subject O:

IZENPE S.A.

Subject C:

ES

Valid from:

Wed Oct 20 10:16:02 CEST 2010

Valid to:

Sun Dec 13 00:00:00 CET 2037

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:8E:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:A7:7E:89:81:F3:98:E2:C2:83:A3:2E:94:FC:82:10:62:59:42:56:26:14:68:
1B:31:0D:EB:7C:FF:E8:ED:1B:2B:D6:C7:AD:B4:5D:49:C5:C8:72:55:00:FD:39:C8:77:6B:4A:FD:3D:96:5F:82:DA:70:04:31:15:AA:7E:64:D9:57:57:23:91:0C:4E:A5:A8:36:3F:DD:64:20:EB:
8D:B2:3C:68:DE:0A:D9:C9:52:8D:E0:19:4A:9E:E8:92:E0:1E:A0:CF:4D:E9:9D:6E:DC:EE:DC:80:98:7E:06:10:E3:74:85:33:F3:4D:41:16:DE:06:E2:67:EB:CA:E4:21:3C:6C:8F:FC:7A:D2:53:
EC:17:00:98:2C:38:3E:4E:A8:CI:65:27:55:4C:EB:E3:3B:5A:CE:F3:E2:67:56:C7:67:8D:6F:6B:AE:94:A2:89:B6:35:0D:B7:AB:FD:D9:D6:9E:D0:A0:FC:25:92:66:0F:01:5E:17:40:5B:C3:7F:7
A:D6:7C:82:E3:93:C2:72:0B:39:30:4D:3B:8B:B6:95:6D:EB:EC:9B:2A:85:0C:55:8B:39:01:95:90:88:46:77:DF:7E:7F:2B:43:33:4B:3E:93:94:35:84:0C:D4:7B:8D:9E:81:2E:4F:C8:BD:C4:AD
:57:3E:82:55:FD:6F:45:2A:5E:F1:48:D2:57:CA:B3:8F:82:CB:46:77:AB:30:5D:C9:EC:30:2B:9F:9E:77:17:52:50:5C:2C:FF:F9:5C:D7:85:5F:5B:33:62:5F:5B:9C:F3:A3:84:52:E1:44:04:14:CD
:7B:C6:63:BD:80:08:C5:15:F2:9E:B7:83:9C:F4:A5:31:E9:34:25:66:24:50:D1:EA:2A:27:28:4B:54:D3:3B:EA:01:F6:67:74:BB:AB:03:EC:33:69:42:46:B2:CD:27:D3:C2:D0:E0:1E:C4:D3:61:
15:0E:9F:E3:E3:FF:65:96:8A:05:BB:FA:C6:22:4B:E4:D8:4D:1C:66:AF:15:DE:F1:6E:51:B1:22:8D:BB:3F:83:84:AE:11:73:01:78:F3:85:80:E4:B4:99:C2:8C:F1:BF:9D:72:29:C5:FF:6D:79:FF
:7F:17:3D:99:AF:2D:80:F7:51:F3:2B:91:7B:0A:8B:C3:79:54:0F:AF:79:8E:89:51:F7:B5:FC:DD:F9:03:19:83:CA:8D:DE:95:47:B9:BE:3B:06:3A:A0:BA:33:F2:EF:80:BA:06:20:84:6A:28:ED
:AF:DB:E0:BE:C7:8F:68:2D:EC:1B:56:72:64:AD:08:48:16:D6:66:48:E0:96:F5:DC:09:0A:02:C4:D0:13:D8:68:81:53:8A:C6:C8:CE:9E:5C:32:57:0E:8F:39:02:03:01:00:01

```

Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints

IsCA: true

Subject Key Identifier

A4:17:1D:4E:65:D7:EF:87:95:2E:7F:8E:B8:75:CB:05:8B:D3:8C:7D

Authority Key Identifier

1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05

Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.izenpe.com/cps</i>
Authority Info Access	<i>http://ocsp.izenpe.com:8094</i>
CRL Distribution Points	<i>http://crl.izenpe.com/cgi-bin/arl2</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75</i>

X509SubjectName

Subject CN:	<i>Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)</i>
Subject OU:	<i>NZZ Ziurtagiri publikoa - Certificado publico SCI</i>
Subject O:	<i>IZENPE S.A.</i>
Subject C:	<i>ES</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time *2016-12-21T01:00:00Z*

Scheme Service Definition URI

URI [en]	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI [es]	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

16.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.7*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.9*

16.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*

Name [es] *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)*

Service digital identities

X509SubjectName

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *pBcdTmXX74eVLn+OuHXLBYvTjH0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time 2016-06-30T22:00:00Z

16.1.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.14777.2.7

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.14777.2.8

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.14777.2.9

16.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)

Name [es] Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)

Service digital identities

X509SubjectName

Subject CN: Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)

Subject OU: NZZ Ziurtagiri publikoa - Certificado publico SCI

Subject O: IZENPE S.A.

Subject C: ES

X509SKI

X509 SK I pBcdTmXX74eVLn+OuHXLBYvTjH0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-07-17T00:00:00Z

16.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.2.7

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.2.8

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.2.9

16.2 - Service (granted): Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

Basic Constraints	<i>IsCA: true</i>
Subject Key Identifier	<i>C6:AF:96:68:50:BE:6F:A1:E5:14:DC:B9:9D:97:3D:8D:73:E7:7E:9A</i>
Authority Key Identifier	<i>1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.izenpe.com/cps</i>
Authority Info Access	<i>http://ocsp.izenpe.com:8094</i>
CRL Distribution Points	<i>http://crl.izenpe.com/cgi-bin/arl2</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>1F:11:A6:55:5C:C6:F2:4D:43:E6:E4:E3:0E:E8:04:D4:16:45:84:7B:7F:D1:56:5A:19:18:63:34:5C:4E:25:6F</i>

Certificate fields details

Version:	3
Serial Number:	139873143337968509637750443090365398999
X509 Certificate	-----BEGIN CERTIFICATE-----

[illegible]

Signature algorithm:	SHA256withRSA
Issuer CN:	Izenpe.com
Issuer O:	IZENPE S.A.
Issuer C:	ES
Subject CN:	EAEko HAetako langileen CA - CA personal de AAPP vascas (2)
Subject OU:	AZZ Ziurtagiri publikoa - Certificado publico SCA
Subject O:	IZENPE S.A.

Subject C: *ES*

Valid from: *Wed Oct 20 10:22:40 CEST 2010*

Valid to: *Sun Dec 13 00:00:00 CET 2037*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D5:F0:7B:6E:B8:20:14:F2:C8:6B:15:91:C2:A8:F9:38:17:6C:D9:6E:3A:73:1E:17:53:26:3A:10:F9:51:C0:20:D7:A2:D7:06:06:99:39:9C:F7:47:A1:97:38:D0:2A:CC:86:BC:68:0B:4F:96:7A:7D:E2:69:C7:AF:5B:A7:A6:80:82:F3:16:FE:0B:ED:AE:4B:E0:C9:37:74:4D:02:67:FF:13:BA:F5:56:1C:53:0A:C2:AE:20:3E:CD:3E:10:65:D4:4A:7D:2E:E8:A7:D7:0E:FE:D9:F5:4A:6A:61:DC:8B:E5:2F:1C:9F:E4:C6:1C:0C:75:F2:8B:1E:4F:61:AC:43:7F:C8:F8:40:9F:00:78:0C:79:95:03:54:32:7E:AB:86:AE:6D:0B:C4:31:E3:82:03:8D:7E:8F:22:1A:B1:3E:4D:2D:5E:32:56:6D:51:56:5E:97:B0:44:33:61:2D:89:E7:CD:02:38:91:E0:D6:AB:E0:70:53:00:22:9F:48:F1:F0:19:25:22:8B:89:87:0A:43:4E:86:8C:56:EA:B3:7F:0B:7C:86:9D:7D:60:EA:3F:2F:3D:2F:7F:9E:44:F8:11:F8:0C:44:9D:7A:24:C3:91:7D:00:18:77:23:F7:8E:97:A8:9F:FC:DD:46:48:00:7C:8C:70:10:52:21:18:8E:45:A5:86:53:F8:98:CF:0A:73:37:32:4B:67:AC:A6:A8:77:E7:95:4B:F2:70:11:9A:CF:14:38:32:E7:F1:84:EB:7E:72:65:75:C5:C7:2B:63:D8:CD:18:BD:32:26:EE:23:46:07:3B:E3:32:82:05:FC:E8:E2:66:4E:86:53:DE:38:A6:DA:3A:EB:38:5F:AA:4A:AA:E5:5B:78:58:DD:E4:A8:35:F6:2C:B4:84:8A:18:02:F2:A0:CA:34:DD:91:F9:53:59:4A:D9:AE:4B:00:F1:DD:38:27:7C:F0:63:45:83:4F:1C:39:0A:72:8B:74:B7:AC:49:BA:C0:EE:E5:BC:CF:75:CD:70:D0:C2:31:C7:F0:46:28:42:36:97:CA:5F:00:68:FD:0F:AC:12:36:1F:32:41:18:D9:EF:69:18:0E:23:89:33:27:AE:F9:80:B2:2B:CB:A8:40:17:41:31:56:32:4F:F6:A2:86:21:26:67:C2:9C:32:9C:0C:65:AC:01:5B:E4:D9:4A:EA:1D:88:50:EE:C3:3C:EF:29:59:3D:5C:F0:2C:44:BB:D5:4E:A7:99:88:74:25:14:92:80:DF:82:E4:5F:03:A8:64:52:6C:D4:E5:58:BD:8F:55:4F:A4:03:76:5F:BC:06:07:FE:02:7D:FC:AB:A9:C1:05:7B:CE:69:8E:81:2F:02:03:01:00:01

Subject Alternative Name *http://www.izenpe.com*
info@izenpe.com
STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *C6:AF:96:68:50:BE:6F:A1:E5:14:DC:B9:9D:97:3D:8D:73:E7:7E:9A*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8*

X509SubjectName

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2026-05-20T03:00:00Z*

Scheme Service Definition URI

URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

16.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.4.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.4.4

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.14777.4.5

16.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

16.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

16.2.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

Name *[es]* *Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Service digital identities

X509SubjectName

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *xq+WaFC+b6HIFNy5nZc9jXPnfpo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

16.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.14777.4.3*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.14777.4.4*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.14777.4.5*

16.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.2.5 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Name [es] *Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)*

Service digital identities**X509SubjectName**

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *xq+WaFC+b6HIFNy5nZc9jXPnfpo=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2009-07-17T00:00:00Z*

16.2.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.14777.4.3*

Policy Identifier:

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)
Name	[es]	Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

[illegible]

Page 663

Issuer C: *ES*

Subject E: *Info@izenpe.com*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Valid from: *Tue Feb 04 18:46:25 CET 2003*

Valid to: *Mon Feb 04 00:00:00 CET 2013*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DB:00:67:D9:BC:0C:26:DA:0A:12:C8:85:25:C4:81:F0:47:BF:3D:83:C0:C8:A5:CB:17:8A:E8:EC:6E:6D:E2:BC:80:58:C9:94:82:5C:9A:C2:C3:51:BC:4F:44:0A:4E:2C:5F:BE:5D:41:12:39:DB:C7:7C:8F:1D:9A:32:8E:84:F3:81:35:7E:3D:D4:C1:45:1E:A3:AF:F6:1A:22:3B:EA:76:BA:CB:EF:40:37:81:C1:26:7B:38:E3:48:D9:A0:8D:98:CE:25:AE:E9:A6:88:9D:F8:81:4D:B6:D0:A8:5F:2F:D6:AA:FA:4A:15:53:5F:77:0C:68:AE:DA:AF:8B:1C:A0:B6:8B:26:83:47:C3:A9:48:31:54:E3:8D:8E:D4:00:93:E8:AE:8B:A4:C5:AB:C9:23:7C:31:FF:3E:68:A1:B8:7C:02:ED:6D:37:42:8C:2F:3F:AD:7B:08:69:41:0D:40:45:F5:45:42:A3:25:43:5F:25:25:37:78:6D:C1:F9:8B:7E:4A:93:F5:C2:9F:3F:1C:22:71:77:A5:90:1E:91:99:38:70:88:51:3B:E0:68:4F:98:87:EB:DF:4C:12:8A:21:9E:82:97:28:FE:43:AA:28:AE:59:81:8E:A4:DB:16:16:08:36:2F:5D:CA:A1:F2:1F:65:48:04:F3:B1:52:41:7F:4C:FD:02:03:01:00:01*

Subject Alternative Name *http://www.izenpe.com*

Basic Constraints *IsCA: true*

Subject Key Identifier *D5:3D:B6:B8:27:6D:84:3A:A8:25:07:4C:D0:D3:4E:EB:36:DB:95:B2*

Authority Key Identifier *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*

CRL Distribution Points *http://www.izenpe.com/cgi-bin/ar1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5C:68:F4:98:B2:38:B3:B2:AD:F8:A7:04:74:CF:24:F6:32:67:58:1B:ED:47:96:9F:B1:8B:5E:1B:4A:AB:80:A9*

X509SubjectName

Subject E: *Info@izenpe.com*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] undefined.

[es] undefined.

Status Starting Time*2016-06-30T22:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.9*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.14777.2.7*

16.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.3.3 - History instance n.1 - Status: supervisionceased**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name**

Name [en] *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

Name [es] *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

Service digital identities

X509SubjectName

Subject E: *Info@izenpe.com*

Subject CN: *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

Subject OU: *NZZ Ziurtagiri publikoa - Certificado publico SCI*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

X509SKI

X509 SK I *1T22uCdthDqoJQdM0NNO6zbbIbl=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>*

Status Starting Time *2009-07-17T00:00:00Z*

16.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] [es]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i> <i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.14777.2.8*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.14777.2.9*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.14777.2.7*

16.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service Name	
Name	<i>[en] Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)</i>
Name	<i>[es] Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)</i>

Service digital identities**X509SubjectName**

Subject E:	<i>Info@izenpe.com</i>
Subject CN:	<i>Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades</i>
Subject OU:	<i>NZZ Ziurtagiri publikoa - Certificado publico SCI</i>
Subject L:	<i>Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz</i>
Subject O:	<i>IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>1T22uCdthDqoJQdM0NNO6zbbbl=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</i>

Status Starting Time	<i>2005-03-03T00:00:00Z</i>

16.3.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	<i>[en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es] está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>
Service Name		
Name	<i>[en]</i>	<i>Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)</i>
	<i>[es]</i>	<i>Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)</i>

Certificate fields details

Serial Number: 20

Signature algorithm:	SHA1withRSA
Issuer E:	Info@izenpe.com
Issuer CN:	izenpe.com

Issuer L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*
Issuer O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Issuer C: *ES*
Subject E: *Info@izenpe.com*
Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas*
Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*
Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*
Subject C: *ES*
Valid from: *Tue Apr 08 15:27:21 CEST 2003*
Valid to: *Mon Apr 08 00:00:00 CEST 2013*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:97:15:85:53:CB:06:4F:B4:F1:54:21:DB:0C:6A:51:6D:76:0A:37:74:7F:1D:F4:EB:CE:DD:ED:CF:1D:E3:DE:5F:86:EE:36:A8:3D:F4:DF:56:A1:CA:33:63:4C:00:E4:1F:CD:8B:47:DE:93:83:94:8E:92:0F:23:13:45:7A:D7:B7:85:10:68:74:94:E1:86:59:3F:CS:DC:E1:7C:54:4B:82:70:D7:FF:0F:5F:47:55:0D:9E:EE:8F:F2:C1:BF:7C:D2:6D:9D:D1:D0:F2:A9:7C:59:CF:34:AF:5F:EC:30:DC:A4:E0:29:4C:3B:37:92:97:29:42:8E:D1:00:A3:63:D4:81:28:36:55:32:0F:FC:26:2F:6B:6E:25:55:C2:C0:D6:88:F6:1E:DE:27:06:9F:50:3D:96:1B:93:2D:71:B2:E1:C3:01:18:2E:1C:30:18:EC:C7:7E:39:24:21:F2:9A:FC:54:62:11:DC:78:C6:7F:1D:66:EA:D3:61:2B:1A:88:8C:39:13:D0:8D:86:E0:0E:96:8D:1B:9A:4B:B4:41:89:5E:B4:D7:89:BD:67:F7:B0:A9:D4:18:ED:53:F0:6E:78:8C:B5:10:F3:59:A3:88:D4:3E:23:95:01:55:E7:BF:8E:C7:8F:E1:5F:EA:2C:62:E5:35:1F:20:69:8D:38:0E:18:F7:79:2D:88:BD:02:03:01:00:01*
Subject Alternative Name *http://www.izenpe.com*
Basic Constraints *IsCA: true*
Subject Key Identifier *A2:94:8F:B3:68:E8:5F:6D:C1:FB:5A:56:9B:2C:14:68:D8:23:27:CA*
Authority Key Identifier *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*
CRL Distribution Points *http://www.izenpe.com/cgi-bin/ar/*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *0A:07:55:F0:F8:78:EB:9C:D3:13:48:8B:6C:79:91:90:C0:4E:59:27:54:16:30:63:83:02:4D:E7:8A:F8:47:38*

X509SubjectName

Subject E: *Info@izenpe.com*
Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas*
Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*
Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.14777.4.3*

16.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.4.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Name *[es] Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

Service digital identities

X509SubjectName

Subject E: *Info@izenpe.com*

Subject CN: *EAEko HAetako langileen CA - CA personal de AAPP vascas*

Subject OU: *AZZ Ziurtagiri publikoa - Certificado publico SCA*

Subject L: *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

Subject O: *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

Subject C: *ES*

X509SKI

X509 SK I *opSPs2joX23B+1pWmywUaNgjj8o=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased

Status Starting Time

2009-07-17T00:00:00Z

16.4.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.14777.4.3*

16.4.4 - History instance n.2 - Status: undersupervision**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	<i>Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)</i>
Name	[es]	<i>Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)</i>

Service digital identities

X509SubjectName

Subject E: Info@izenpe.com

Subject CN: EAEko HAetako langileen CA - CA personal de AAPP vascas

Subject OU: AZZ Ziurtagiri publikoa - Certificado publico SCA

Subject L: Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz

Subject O: IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Subject C: ES

X509SKI

X509 SK I opSPs2joX23B+1pWmywUaNgjj8o=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2005-03-03T00:00:00Z

16.4.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.14777.4.3

16.5 - Service (withdrawn): Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Subject Alternative Name *http://www.izenpe.com*
info@izenpe.com
STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Basic Constraints *IsCA: true*

Subject Key Identifier *F1:A3:1E:55:8C:D5:A2:9B:5E:7C:5A:56:C4:87:6A:E7:00:1D:B9:A8*

Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.izenpe.com/cps

Authority Info Access *http://ocsp.izenpe.com:8094*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0B:C3:6A:9B:6E:42:DD:BF:07:4C:FE:38:83:4F:20:0C:D4:4C:1D:28:E2:35:29:CF:E6:29:BC:48:4B:98:98:B9*

X509SubjectName

Subject CN: *Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Subject OU: *Ziurtagiri publikoa - Certificado publico*

Subject O: *IZENPE S.A.*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2018-03-15T01:00:00Z***Scheme Service Definition URI**

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.5.2 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco

Name	[es]	Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco

Service digital identities**X509SubjectName**

Subject CN:	Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco

Subject OU:	Ziurtagiri publikoa - Certificado publico

Subject O:	IZENPE S.A.

Subject C:	ES

X509SKI

X509 SK I	8aMeVYzVoptefFpWxldq5wAduag=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

16.5.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.5.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] *Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Name [es] *Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Service digital identities

X509SubjectName

Subject CN: *Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

Subject OU: *Ziurtagiri publikoa - Certificado publico*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *8aMeVYzVoptefFpWxldq5wAduag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-07-30T00:00:00Z*

16.6 - Service (withdrawn): Qualified timestamps issued by tsa.izenpe.com

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified timestamps issued by tsa.izenpe.com*

Name [es] *Sellos de tiempo cualificados emitidos por tsa.izenpe.com*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *153937334957709364140310094114160524157*

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CD:77:0A:3B:A5:00:5B:AC:3F:6E:F2:9E:7F:A4:C7:BE:A1:EF:41:BE:52:12:53:56:D
A:0D:D1:8F:04:5C:92:19*

X509SubjectName

Subject CN: *tsa.izenpe.com*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *58dpM6kv0GEyfcjPQafDIWB4XY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2022-10-10T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.6.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by tsa.izenpe.com*

Name *[es]* *Sellos de tiempo cualificados emitidos por tsa.izenpe.com*

Service digital identities**X509SubjectName**

X509 SK I *58dpM6kv0GEyfnclPQafDIWB4XY=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time 2017-07-21T00:00:00Z

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en] [es]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services. Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[en]	Qualified certificates issued by CA de certificados SSL EV
Name	[es]	Certificados cualificados emitidos por CA de certificados SSL EV

Version: 3

Serial Number: 145477172158191020923658859389206702465

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: *Izenpe.com*
Issuer O: *IZENPE S.A.*
Issuer C: *ES*
Subject CN: *CA de Certificados SSL EV*
Subject OU: *BZ Ziurtagiri publikoa - Certificado publico EV*
Subject O: *IZENPE S.A.*
Subject C: *ES*
Valid from: *Wed Oct 20 10:28:56 CEST 2010*
Valid to: *Tue Oct 20 10:28:56 CEST 2020*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EB:B2:9D:4D:4A:FF:14:9F:D5:68:16:8B:D4:12:60:9A:6E:AE:F2:86:A8:12:59:
34:7A:C7:73:7A:87:F8:02:CB:0A:38:F7:57:CA:FA:DD:3D:63:D1:41:D2:36:3F:8F:C4:8F:68:3B:7F:4C:A7:7B:48:E5:34:9A:5B:03:0D:35:76:85:22:01:A7:A6:A1:D9:54:A1:52:E6:07:CB:D3:
81:6C:C0:C7:B6:9E:4D:18:11:CC:C7:E7:62:E1:35:7F:76:C1:F8:C7:D1:6D:C0:7F:45:75:D1:43:5E:DB:95:5D:A5:29:42:94:15:B6:EB:18:C2:09:27:EB:35:31:E4:E1:FB:28:18:0D:A2:8E:C6:0
B:85:6D:F8:C0:1C:2E:B3:71:22:43:2E:2A:32:95:91:07:D9:6A:05:FE:CD:C2:41:B2:D5:57:C1:5B:C9:AC:E1:8F:89:D9:EB:1B:9D:B7:22:EE:10:37:D2:AF:74:D0:8E:01:4B:4E:37:81:75:53:57
92:EB:27:46:7A:E0:D4:AD:08:A2:6C:26:13:3D:69:3B:7A:7F:80:93:9E:D8:AA:38:A4:8A:0D:83:61:75:A3:D7:D9:3C:59:35:E3:F4:0C:40:8B:35:E9:66:05:E0:BF:81:7F:47:2D:C8:F9:8B:7E:0
E:AB:0F:15:51:FB:EB:70:F9:DB:DC:14:F7:34:36:CD:8F:9C:93:2E:3D:78:61:BF:1C:01:A0:85:71:5E:AC:A5:28:10:9D:0C:E7:83:7D:B6:70:94:0C:54:88:02:1E:BB:4F:48:80:7F:4B:15:77:2A:
2E:81:48:6D:3F:17:83:7E:3E:A6:3E:5A:F6:DF:F8:9C:1E:92:4C:71:1A:DF:3D:F6:35:2B:8B:95:DB:AE:A1:92:DF:5F:80:48:44:6D:4D:FF:0D:B3:10:E8:E9:09:F3:1A:25:A0:33:1B:2C:C1:C1:28
1C:BC:92:3D:6D:4C:5D:6D:EB:26:85:74:61:FE:FE:E9:E0:24:A2:2C:33:9D:29:21:66:F3:66:EF:35:E0:8D:98:A1:58:04:B4:D2:5C:BC:29:96:75:BF:00:BC:95:0B:0C:EE:88:A0:6B:34:BF:82:1
D:2D:09:A9:85:8F:D1:FF:B5:4A:15:D6:BF:4B:C5:E0:E7:63:58:EB:83:7E:21:07:4F:4D:B9:A9:37:16:2A:70:93:0C:E2:D0:BF:3A:73:83:5A:FF:85:49:D0:45:A3:C8:1B:CC:92:15:DE:97:45:38:
A0:9E:60:45:F5:42:8A:47:88:14:2E:71:A0:5A:8C:5B:73:37:88:26:8F:B6:19:E9:F2:D0:C3:A5:95:D0:90:43:AF:98:50:0C:3C:EF:72:D1:D8:52:33:F6:C5:02:03:01:00:01

```

Subject Alternative Name *http://www.izenpe.com*
info@izenpe.com
STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Basic Constraints *IsCA: true*
Subject Key Identifier *A6:CE:69:69:2E:A6:21:35:3B:3A:CF:0A:F1:2E:3F:15:AC:19:90:27*
Authority Key Identifier *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.izenpe.com/cps
Authority Info Access *http://ocsp.izenpe.com*
CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *B0:8C:19:6A:2E:D1:E8:4F:98:92:DB:1B:61:21:9C:EB:64:28:82:47:8F:39:B0:87:19:60:3D:07:35:FA:03:D1*
X509SubjectName
Subject CN: *CA de Certificados SSL EV*

Subject OU: BZ Ziurtagiri publikoa - Certificado publico EV

Subject O: IZENPE S.A.

Subject C: ES

X509SKI

X509 SK I ps5paS6mITU7Os8K8S4/FawZkCc=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2022-10-10T00:00:00Z

Scheme Service Definition URI

URI [en] <https://advancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://advancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

16.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

16.7.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified certificates issued by CA de certificados SSL EV

Name [es] Certificados cualificados emitidos por CA de certificados SSL EV

Service digital identities

X509SubjectName

Subject CN: CA de Certificados SSL EV

Subject OU: BZ Ziurtagiri publikoa - Certificado publico EV

Subject O: IZENPE S.A.

Subject C: ES

X509SKI

X509 SK I ps5paS6mITU7Os8K8S4/FawZkCc=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-03-15T01:00:00Z

16.7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

16.8 - Service (granted): Qualified certificates issued by CA de certificados SSL EV (new)

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified certificates issued by CA de certificados SSL EV (new)

Name	[es]	Certificados cualificados emitidos por CA de certificados SSL EV (nueva)

Service digital identities

Certificate fields details

Version: 3

Serial Number: 138892462179354702629058714957455292581

CRL Distribution Points *http://crl.izenpe.com/cgi-bin/arl2*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37*

X509SubjectName

Subject CN: *CA de Certificados SSL EV*

Subject OU: *BZ Ziurtagiri publikoa - Certificado publico EV*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *xu3+d/tRVk38q9XjsQwTo79U45s=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2019-07-15T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

16.9 - Service (withdrawn): Qualified Certificates issued by SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Public Key:

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AE:93:1D:C6:83:00:B5:D4:FE:FD:EF:DF:96:AF:3A:9E:49:7A:1F:8D:1D:A2:75:07:A0:BA:BF:93:A7:9D:1C:15:77:23:92:98:16:A7:85:90:08:C8:F4:75:88:77:FF:6A:49:E4:69:56:80:E9:67:46:BC:19:65:46:A9:E0:4E:F8:51:E2:A1:0E:41:F1:84:5D:BC:98:6C:BD:8D:E2:25:A2:91:19:14:51:87:ES:CB:EC:F4:C5:6C:97:0F:61:6D:9F:24:2B:98:E2:0F:C5:FD:BB:36:CA:FE:F6:5D:C3:12:D1:DE:5A:37:06:52:58:C7:4E:F0:D2:51:7E:32:0E:33:4C:42:29:93:58:95:45:96:05:1E:9C:24:1C:7A:8D:A5:09:9F:A6:F2:D5:00:84:0C:AF:C5:BC:39:54:72:76:89:EC:C5:92:3E:FC:80:FC:EF:A1:AF:CE:83:72:3A:80:6C:77:A1:B5:BD:00:DD:20:A8:D2:0C:38:EE:A7:8A:19:34:97:3E:CA:22:62:2F:27:83:59:10:E1:15:0F:67:A3:33:F0:D2:65:8B:E8:C9:39:C7:E4:4B:D1:58:B7:F1:D8:9A:A1:62:C2:47:98:57:0C:49:6C:26:E9:0F:C5:0D:FA:18:31:02:34:E8:46:AC:28:AB:D2:F1:D1:1D:77:24:22:28:25:03:78:05:58:79:80:E1:DE:87:8F:2C:D8:89:19:65:0D:3D:F9:F0:EC:19:1E:4D:D8:34:AA:CA:BE:F7:BB:D4:73:CA:07:5E:6B:9D:F9:12:32:2D:56:89:91:B6:9D:5D:A1:DF:84:77:08:7D:0E:87:32:45:D4:FC:8F:12:51:FF:44:AC:2E:12:99:28:1F:B3:E6:29:42:5B:76:35:DE:07:35:63:D0:45:4A:6F:5A:B3:AF:B7:2A:D7:0C:E7:CA:7E:50:44:96:BC:A2:F1:C2:04:F3:F2:38:CD:74:EF:46:DC:16:09:E7:BA:AD:15:45:E8:18:CB:46:98:42:F1:67:F2:3B:95:61:0D:86:1E:52:59:00:49:2A:9D:F5:8F:30:FE:9B:99:CC:14:13:16:5F:A6:56:3B:7A:26:23:28:23:8C:78:65:9D:2A:0C:C1:30:E3:D6:55:57:91:2D:72:73:EE:3C:DB:F9:68:86:77:41:6F:10:66:61:25:5C:9E:4E:1E:E9:B9:1B:A2:01:28:14:76:ED:21:2B:A7:02:BF:1D:88:90:90:B2:3D:76:1E:9A:78:67:87:53:84:1D:8E:B5:3E:C7:03:EA:46:6D:59:7F:66:A8:04:D6:87:B8:C8:B5:AC:5D:3B:C8:F4:46:EB:05:13:84:14:75:96:B4:73:2F:07:73:02:03:01:00:01

Authority Key Identifier

A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97

Subject Key Identifier

D3:E1:D0:00:10:E4:37:DB:20:C0:6E:CD:92:F5:9C:7F:0A:6B:2E:40

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: <https://www.izenpe.eus/cps>**Authority Info Access**http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt**Basic Constraints**

IsCA: true - Path length: 0

CRL Distribution Points<http://crl.izenpe.eus/cgi-bin/izrootqc>**Key Usage:**

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1A:48:85:AC:77:F5:55:9B:29:BF:AE:13:C4:86:FF:09:31:21:FA:C2:68:A8:EC:BB:2B:AB:30:3F:5D:A9:42:F9

X509SubjectName**Subject CN:**

SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

Subject 2.5.4.97:

VATES-A01337260

Subject O:

IZENPE S.A.

Subject C:

ES

X509SKI**X509 SK I**

0+HQABDkN9sgwG7NkvWcfwprLkA=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description** [en]

undefined.

[es]

undefined.

Status Starting Time

2026-05-20T03:00:00Z

Scheme Service Definition URI**URI** [en]<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**URI** [es]<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

16.9.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

16.9.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

16.9.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA
Name	[es]	Certificados cualificados de firma y de sello expedidos por SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

Service digital identities**X509SubjectName**

Subject CN:	SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA
Subject 2.5.4.97:	VATES-A01337260
Subject O:	IZENPE S.A.
Subject C:	ES

X509SKI

X509 SK I	0+HQABDkN9sgwG7NkvWcfwprLkA=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2021-04-21T00:00:00Z

16.9.3.1 - Extension (critical): additionalServiceInformation

Issuer O:	<i>IZENPE S.A.</i>
Issuer C:	<i>ES</i>
Subject CN:	<i>SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA</i>
Subject 2.5.4.97:	<i>VATES-A01337260</i>
Subject O:	<i>IZENPE S.A.</i>
Subject C:	<i>ES</i>
Valid from:	<i>Wed Sep 23 13:28:41 CEST 2020</i>
Valid to:	<i>Sat Sep 23 12:57:18 CEST 2045</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B9:46:3C:43:D7:1D:21:83:DE:34:96:48:5E:05:53:32:A7:18:66:A6:93:97:69: 93:AC:02:71:A6:70:60:DE:94:7B:06:FD:5B:F9:01:94:F8:09:EE:17:9A:AD:71:F4:AE:AE:27:EC:CF:C9:1A:A4:9D:7D:05:30:D8:38:82:D4:C2:3E:EC:E4:87:80:6B:66:D1:F0:96:C8:2E:08:DD: D3:9C:12:A6:30:89:A8:00:61:77:D2:FE:88:0C:F0:41:91:79:9A:BD:A7:BC:9D:AC:A6:FE:6C:24:32:9B:E6:BC:96:A2:D1:E8:6D:03:D3:BC:9B:20:E1:CD:F9:4D:BF:3F:9F:E4:1F:B1:FD:DA:65: 85:86:53:F2:C8:82:DF:A4:C4:D9:55:EA:F8:1C:A1:9E:5B:18:CC:34:AD:9B:80:40:23:74:2D:A0:6A:98:AC:68:9C:AD:37:AA:5B:65:BC:63:59:A8:32:AD:8D:09:6A:4A:8C:38:62:DC:07:A0:BF: 0D:D2:17:46:3B:20:44:51:E3:53:1C:01:85:FA:03:8B:9C:18:F5:0E:A3:C6:7B:8E:DF:D9:00:3A:5C:AF:F7:3C:DF:0D:61:89:7F:6A:1E:07:04:29:A2:66:2B:3E:98:06:C9:51:2E:26:DF:09:19:1 D:C2:09:07:8A:47:0D:7B:82:CC:6D:5A:0D:F1:18:80:3B:A9:E8:42:F4:7B:DF:1F:5C:F9:AE:92:47:59:8A:76:BE:B7:25:D6:29:22:01:00:E2:6F:5A:8A:D1:AF:A4:79:97:E4:D7:15:B1:02:74:87: 19:88:49:3D:7B:E8:49:C1:9E:24:35:05:F8:17:27:66:01:A5:3C:31:5C:FF:43:2B:D3:79:23:A3:10:C6:46:1D:F1:5D:84:BE:20:28:80:DD:9F:34:C3:0B:74:5C:E3:7D:E1:7E:D1:7A:35:E1:08:1 D:73:D1:A1:B3:1A:94:8B:8B:87:15:00:02:3D:84:5B:04:C7:8A:D3:DF:D2:91:B1:C9:88:7F:3C:51:34:BA:D2:83:39:B8:AA:7D:8F:CD:8B:A6:E3:98:A2:12:24:87:00:55:7E:CB:1A:46:00:8B:F 0:0A:DB:28:20:13:15:E5:45:A9:04:73:5D:F8:0F:CC:53:31:A9:4D:4C:61:E1:7F:AA:86:B2:61:A8:94:A3:15:6C:F7:E0:36:C5:93:B4:39:7C:C7:38:AA:5C:0A:25:F0:52:3E:F4:D8:D7:C7:54:C5: 77:9E:F9:66:09:C5:F3:40:2F:F2:DE:43:A3:D9:48:EB:1B:DF:A4:F9:A6:05:15:CD:A8:FA:8A:B2:E3:5E:1D:44:91:3A:84:7D:48:F9:06:99:AD:DB:B2:06:AF:D5:FD:02:03:01:00:01 </pre>
Authority Key Identifier	<i>A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97</i>
Subject Key Identifier	<i>61:AA:C8:2F:82:E4:8F:B1:D6:3C:50:D3:01:A0:44:0A:46:DE:1A:A4</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://www.izenpe.eus/cps</i>
Authority Info Access	<i>http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
CRL Distribution Points	<i>http://crl.izenpe.eus/cgi-bin/izrootqc</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>5C:29:9D:31:59:49:42:41:38:14:5E:5E:E1:DA:67:7D:93:4F:09:5D:8A:5B:F7:86:C7:AB:B8:CB:4F:C6:D6:5A</i>
X509SubjectName	
Subject CN:	<i>SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA</i>
Subject 2.5.4.97:	<i>VATES-A01337260</i>
Subject O:	<i>IZENPE S.A.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I *YarIL4Lkj7HWPFDTAaBECKbeGqQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-06-10T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

16.10.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.10.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.10.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified certificates issued by SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Name *[es] Certificados cualificados de firma y sello expedidos por SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Service digital identities**X509SubjectName**

Subject CN: *SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *YarIL4Lkj7HWPFDTAaBECKbeGqQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-04-21T00:00:00Z*

16.10.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.10.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.11 - Service (withdrawn): Qualified TimeStamp issued by SUBCA QC IZENPE - TSA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified TimeStamp issued by SUBCA QC IZENPE - TSA*

Name *[es]* *Sellos de tiempo cualificados emitidos por SUBCA QC IZENPE-TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *28904314925970312305335547853608733463*

-----END CERTIFICATE-----

SHA256withRSA

SUBCA QC IZENPE - TSA

VATES-A01337260

IZENPE S.A.

ES

tsa.izenpe.com

VATES-A01337260

IZENPE S.A.

ES

Fri Oct 30 14:54:16 CET 2020

Thu Oct 30 14:54:16 CET 2025

[illegible]

id kp timeStamping

6E:72:03:7C:9F:66:79:AD:E9:6B:5A:3B:B8:71:3F:8D:6F:BC:ED:CC

EA:84:45:BA:7F:5C:49:FB:15:0B:A3:0F:0E:8D:9C:E4:3F:AB:A2:C1

Policy OID: 1.3.6.1.4.1.14777.10.1

CPS pointer: <http://www.izenpe.eus/cps>

CPS text: [Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado]

Authority Info Access	<i>http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SUBCA_QC_TSA.crt</i>
CRL Distribution Points	<i>http://crl.izenpe.eus/cgi-bin/izenpeTSA</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>D0:96:8A:07:3A:C6:46:F6:86:AC:CD:A8:44:BB:A6:CE:83:0C:D0:E1:A2:F4:E2:28:DB:A6:73:47:C9:F3:61:7C</i>

X509SubjectName

Subject CN:	<i>tsa.izenpe.com</i>
Subject 2.5.4.97:	<i>VATES-A01337260</i>
Subject O:	<i>IZENPE S.A.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>bnIDfj9mea3pa1o7uHE/jW+87cw=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time	<i>2026-05-20T03:00:00Z</i>

Scheme Service Definition URI

URI [en]	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI [es]	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

16.11.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name [en]	<i>Qualified TimeStamp issued by SUBCA QC IZENPE - TSA</i>
Name [es]	<i>Sellos de tiempo cualificados emitidos por SUBCA QC IZENPE-TSA</i>

Service digital identities**X509SubjectName**

Subject CN: *tsa.izenpe.com*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *bnIDfj9mea3pa1o7uHE/jW+87cw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-04-21T00:00:00Z*

16.12 - Service (granted): Qualified TimeStamp issued by "tsa.izenpe.com 2025"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified TimeStamp issued by "tsa.izenpe.com 2025"*

Name *[es]* *Servicio de sello de tiempo cualificado emitido por "tsa.izenpe.com 2025"*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *159915055240229027990070856082539688926*

Authority Info Access	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SUBCA_QC_TSA.crt
CRL Distribution Points	http://crl.izenpe.eus/cgi-bin/izenpeTSA
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>FD:EE:56:8A:28:BF:EF:94:BD:19:AC:3F:89:1D:B8:3E:72:6B:0B:AB:18:84:BF:90:B0:FC:91:9C:84:18:62:6C</i>

X509SubjectName

Subject CN:	<i>tsa.izenpe.com</i>
Subject 2.5.4.97:	<i>VATES-A01337260</i>
Subject O:	<i>ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE S.A.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>mcgDWuKVAOKScNFukhmsxnVT58g=</i>

Service Status

	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2025-04-08T02:00:00Z</i>

16.13 - Service (granted): Qualified certificates issued by SUBCA SSL 2024**Service Type Identifier**

	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	<i>[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	<i>[en] Qualified certificates issued by SUBCA SSL 2024</i>
Name	<i>[es] Certificados cualificados emitidos por SUBCA SSL 2024</i>

Service digital identities**Certificate fields details**

[illegible]

Thumbprint algorithm: *SHA-256*

Thumbprint: *B8:7F:2C:A5:AD:30:25:9F:F3:E5:58:8D:E1:31:C3:62:6D:57:27:CA:E2:4F:9B:C9:B0:07:02:6D:BC:C2:D6:52*

X509SubjectName

Subject CN: *SUBCA SSL 2024*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *VzBZnKM9oGjss9vP1VXIqsdAKk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2026-05-20T03:00:00Z*

16.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

16.14 - Service (granted): Qualified certificates issued by CA HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA 2025

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified certificates issued by CA HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA 2025*

Name *[es]* *Certificados cualificados emitidos por CA HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA 2025*

Service digital identities

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D8:52:49:0E:D9:18:38:B0:6F:68:85:E1:71:53:73:8D:EB:FE:9A:5F:F9:DD:B9:6B:A0:E3:6E:5D:45:72:EF:EE*

X509SubjectName

Subject CN: *CA HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA 2025*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *U3ahslYPBaJimu16qcr1ENNAbh0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2026-05-20T03:00:00Z*

16.14.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.14.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

16.15 - Service (granted): Qualified certificates issued by CA ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA 2025**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Extended Key Usage *id_kp_clientAuth - id_kp_smartcardlogin - Unknown ExtendedKeyUsage OID: 1.3.6.1.5.5.7.3.36*

CRL Distribution Points *http://crl.izenpe.eus/crls/izqcroot.crl*

Authority Key Identifier *B7:17:A1:8A:5C:A4:D5:62:96:7B:FB:57:30:AE:A9:52:F2:A8:D9:0D*

Subject Key Identifier *B2:27:76:1E:C2:B3:BD:57:BB:F2:8A:84:A5:E5:9D:50:05:A0:C6:E6*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7E:4E:55:11:52:F0:6C:51:DB:57:62:36:16:25:14:BA:FD:7A:BC:E1:A3:A4:14:1A:1A:79:49:BD:CF:E1:A4:32*

X509SubjectName

Subject CN: *CA ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA 2025*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: *IZENPE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *sid2HsKzvVe78oqEpeWdUAWgxuY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-05-20T03:00:00Z*

16.15.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

16.15.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

[en] A time-stamping generation service creating and signing qualified time-stamps tokens.

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Name [en]

Qualified electronic timestamps issued by IZENPE TSU - 2025

Name [es]

Sellos cualificados de tiempo electrónicos emitidos por IZENPE TSU - 2025

Certificate fields details

Version: 3

Serial Number: 211786871781899083465841286308466043139

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: CA OC IZENPE - TSA 2025

Issuer 2.5.4.97: VATES-A01337260

Issuer O: IZENPF S A

Issuer C: *ES*

Subject CN: *IZENPE TSU - 2025*

Subject 2.5.4.97: *VATES-A01337260*

Subject O: IZENPE S A

Subject C: FS

Valid from: *Thu Oct 16 09:55:08 CEST 2025*

Valid to: *Wed Oct 16 09:55:08 CEST 2030*

Public Key:

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:5E:43:FB:EF:E5:7F:B4:18:9A:91:0E:61:A6:E7:25:74:AB:6E:D0:91:AA:E0:26:5B:98:AC:CB:78:52:E2:6D:55:27:24:C2:8B:0C:10:A8:23:58:34:8A:53:52:82:5D:D0:69:12:B5:59:77:BD:8C:5D:65:74:24:AD:38:7A:A1:CD

Extended Key Usage

id_kp_timeStamping

Certificate Policies

Policy OID: 1.3.6.1.4.1.14777.53.1.3

CPS pointer: <http://www.izenpe.eus/cps>

CPS text: [Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado]

Authority Info Access

http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/TSA2025.crt

CRL Distribution Points

<http://crl.izenpe.eus/crls/crltsa.crl>

Authority Key Identifier

6A:08:D5:EC:FA:B7:1D:43:8D:C2:E1:41:20:CC:38:67:73:32:B7:1B

Subject Key Identifier

59:2C:AF:D0:7B:4A:49:0E:D8:11:EA:94:69:80:7D:9B:94:54:66:E8

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

3E:DC:28:C0:17:47:50:2B:35:A9:69:A2:83:D2:E6:A6:5B:8B:65:9A:E8:87:A0:19:EB:2D:9B:2D:21:4B:08:FC

X509SubjectName**Subject CN:**

IZENPE TSU - 2025

Subject 2.5.4.97:

VATES-A01337260

Subject O:

IZENPE S.A.

Subject C:

ES

X509SKI**X509 SK I**

WSyv0HtKSQ7YEeqUaYB9m5RUZug=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2026-05-20T03:00:00Z

17 - TSP: Firmaprofesional, S.A.**TSP Name**

Name [en] *Firmaprofesional, S.A.*

Name [es] *Firmaprofesional, S.A.*

TSP Trade Name

Name [en] *Firmaprofesional, S.A.*

Name [es] *Firmaprofesional, S.A.*

Name [en] *VATES-A62634068*

Name [en] *Firmaprofesional S.A. NIF A-62634068*

Name [en] *Firmaprofesional SA*

Name [en] *Firmaprofesional S.A.*

PostalAddress

Street Address [en] *Paseo de la Bonanova, 47*

Locality [en] *Barcelona*

State Or Province [en] *Barcelona*

Postal Code [en] *8017*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Paseo de la Bonanova, 47*

Locality [es] *Barcelona*

State Or Province [es] *Barcelona*

Postal Code [es] *8017*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:info@firmaprofesional.com*

Subject OU:	Jerarquia de Certificacion Firmaprofesional
Subject OU:	Consulte http://www.firmaprofesional.com
Subject L:	C/ Muntaner 244 Barcelona
Subject E:	ca1@firmaprofesional.com
Subject C:	ES
Valid from:	Tue Aug 25 12:05:54 CEST 2009
Valid to:	Sun Jun 16 12:05:54 CEST 2030
Public Key:	30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:A8:9E:30:93:63:6F:A8:BA:B5:DC:6A:F1:A9:3A:05:66:E3:95:9D:B7:8C:41:5A:A5:0C:86:75:82:E8:95:00:18:F7:8C:A2:3D:A5:FF:8B:75:C4:24:4A:9A:9F:DA:A5:7C:6E:B7:A2:47:3F:3D:64:65:FE:57:8C:43:A4:21:25:54:CD:47:8C:8E:69:5C:5B:18:5B:C5:F6:72:24:F5:3E:F8:D8:96:02:86:04:A8:4E:ED:13:FE:9F:22:53:A2:2D:64:9F:1B:C9:94:87:8A:E6:67:C9:C3:8D:10:55:59:E9:43:17:F4:2C:AF:27:FB:CD:84:23:16:D6:25:D3:8B:02:88:72:45:37:09:24:90:3C:72:98:10:4D:26:DA:53:21:6C:0A:D6:6B:36:C8:D1:E1:64:F3:FF:55:1C:57:FD:9C:82:C9:A4:E1:64:4C:84:F8:E1:6C:DA:2F:2B:ED:F0:03:B1:DE:F0:CD:E1:71:4A:36:A3:56:88:85:3A:73:AD:8B:46:14:57:AB:E9:97:88:42:70:DA:AC:37:8D:39:4E:EA:51:09:FB:4F:C7:D9:79:AF:87:4E:82:E0:89:2C:D0:6A:E8:91:0F:7A:36:FB:DE:C1:54:DC:71:6F:89:74:DC:56:95:61:5D:4C:69:2D:0C:CE:7F:AC:4D:64:3D:1B:53:02:03:01:00:01
Basic Constraints	IsCA: true - Path length: 0
Authority Key Identifier	65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F
CRL Distribution Points	http://crl.firmaprofesional.com/fproot.crl
Subject Key Identifier	8B:50:57:5A:C1:BD:92:00:A6:B7:E5:85:5D:C3:DD:B6:B5:86:90:D2
Certificate Policies	Policy OID: 1.3.6.1.4.1.1377.10.10.1 CPS pointer: http://www.firmaprofesional.com/cps
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	0E:BB:DF:14:6E:63:F7:0F:AA:59:27:EE:8E:53:46:E9:C9:6C:5F:0D:9B:DD:32:12:B0:4E:D6:68:71:79:87:4D

Certificate fields details

[illegible]

Signature algorithm: *SHA1withRSA*

Issuer E: *ca@firmaprofesional.com*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer L: *C/ Muntaner 244 Barcelona*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - CA1*

Subject O: *Firmaprofesional S.A. NIF A-62634068*

Subject OU: *Jerarquia de Certificacion Firmaprofesional*

Subject OU: *Consulte <http://www.firmaprofesional.com>*

Subject L: *C/ Muntaner 244 Barcelona*

Subject E: *ca1@firmaprofesional.com*

Subject C: *ES*

Valid from: *Thu Mar 27 12:51:38 CET 2003*

Valid to: *Tue Mar 26 00:00:00 CET 2013*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:AB:9E:30:93:63:6F:A8:BA:B5:DC:6A:F1:A9:3A:05:66:E3:95:9D:B7:8C:41:5A:A5:0C:86:75:82:E8:95:00:18:F7:8C:A2:3D:A5:FF:8B:75:C4:24:4A:9A:9F:0A:A5:7C:6E:B7:A2:47:3F:3D:64:65:FE:57:8C:43:A4:21:25:54:CD:47:8C:8E:69:5C:5B:18:5B:C5:F6:72:24:F5:3E:F8:D8:96:02:86:0A:A8:AE:ED:13:FE:8F:22:53:A2:2D:64:9F:1B:C9:94:87:8A:E6:67:C9:C3:B0:10:55:59:E9:E4:17:F4:2C:AF:27:FB:CD:84:23:16:D6:25:D3:B9:02:88:72:45:37:09:24:80:3C:72:98:10:4D:26:D4:53:21:6C:0A:D6:6B:36:C8:D1:E1:64:F3:FF:55:1C:57:FD:FD:9C:B2:C9:A4:E1:64:4C:84:F8:E1:6C:DA:2F:2B:ED:F0:03:B1:DE:F0:CD:E1:71:4A:36:A3:56:8B:85:3A:73:AD:8B:46:14:57:AB:E9:97:88:42:70:DA:AC:37:80:39:4E:EA:51:09:FB:4F:C7:D9:79:AF:87:4E:82:E0:89:2C:D0:6A:E8:91:0F:7A:36:FB:DE:C1:54:DC:71:6F:89:74:DC:56:95:61:5D:4C:69:2D:0C:CE:7F:AC:4D:64:3D:1B:53:02:03:01:00:01

Issuer Alternative Name *<http://www.firmaprofesional.com>*

Subject Alternative Name *<http://www.firmaprofesional.com>*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *8B:50:57:5A:C1:BD:92:00:A6:B7:E5:85:5D:C3:DD:B6:B5:86:90:D2*

Authority Key Identifier *33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7*

Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.10.1*
CPS pointer: <http://www.firmaprofesional.com/cps/cps.htm>

CRL Distribution Points *<http://crl.firmaprofesional.com/firmaprofesional.crl>*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint:

65:BA:8F:C0:CE:3C:43:41:64:DC:40:81:5A:6C:A6:FB:44:C7:27:20:46:FC:D3:03:A
2:9D:A8:F4:1C:A2:07:5D

X509SubjectName

Subject CN: AC Firmaprofesional - CA1

Subject O: Firmaprofesional S.A. NIF A-62634068

Subject OU: Jerarquia de Certificacion Firmaprofesional

Subject OU: Consulte <http://www.firmaprofesional.com>

Subject L: C/ Muntaner 244 Barcelona

Subject E: ca1@firmaprofesional.com

Subject C: ES

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time

2017-11-16T00:00:00Z

17.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.2

17.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

17.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by "AC Firmaprofesional - CA1"*

Name *[es]* *Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

Service digital identities

X509SubjectName

Subject CN: *AC Firmaprofesional - CA1*

Subject O: *Firmaprofesional S.A. NIF A-62634068*

Subject OU: *Jerarquia de Certificacion Firmaprofesional*

Subject OU: *Consulte <http://www.firmaprofesional.com>*

Subject L: *C/ Muntaner 244 Barcelona*

Subject E: *ca1@firmaprofesional.com*

Subject C: *ES*

X509SKI

X509 SK I *i1BXWsG9kgCmt+WFxcPdtrWGkNI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

17.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.2*

17.1.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by "AC Firmaprofesional - CA1"
Name	[es]	Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"

Service digital identities**X509SubjectName**

Subject CN:	AC Firmaprofesional - CA1
Subject O:	Firmaprofesional S.A. NIF A-62634068
Subject OU:	Jerarquia de Certificacion Firmaprofesional
Subject OU:	Consulte http://www.firmaprofesional.com
Subject L:	C/ Muntaner 244 Barcelona
Subject E:	ca1@firmaprofesional.com
Subject C:	ES

X509SKI

X509 SK I	i1BXWsG9kgCmt+WFxcPdtrWGkNI=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2004-11-25T00:00:00Z

17.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*
Issuer C: *ES*
Subject CN: *AC Firmaprofesional - AAPP*
Subject SERIAL NUMBER: *A62634068*
Subject OU: *Certificados Digitales para la Administracion Publica*
Subject O: *Firmaprofesional SA*
Subject C: *ES*
Valid from: *Wed Jul 07 11:35:43 CEST 2010*
Valid to: *Thu Jul 07 11:35:43 CEST 2022*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:96:E9:0E:D5:3D:6E:40:F3:B2:08:1E:FA:09:2F:89:C7:C6:37:68:39:6F:B1:55:55:C0:F7:2E:21:01:A8:A5:F9:F7:74:4B:44:DF:EA:B9:83:77:49:4F:50:A9:FB:A4:5F:40:8D:CE:7F:7F:24:5C:BC:C2:07:6E:B9:2E:3E:2E:A7:52:F7:0A:65:59:EF:92:AA:7A:0F:C6:AA:63:AD:96:03:35:B1:99:C0:18:84:22:5E:9A:15:B7:E0:25:A1:0A:35:5E:1A:91:85:E9:F8:50:3A:87:FB:C9:34:5F:CA:47:65:CE:01:5E:AA:0A:60:B8:8F:5E:B8:E7:0B:AF:1B:8C:AD:59:09:8C:B5:14:A6:C6:50:45:D4:2C:AC:ED:E2:B6:FD:5F:36:5A:C3:6E:C0:24:5B:A7:57:D4:8A:A5:15:1E:03:64:03:0D:04:6F:11:9A:A7:56:AE:F0:71:3C:25:90:D2:28:44:B9:51:FC:DA:63:5F:14:10:74:6A:00:F2:61:68:54:CA:4A:33:22:39:3F:C4:67:69:87:04:24:02:A9:75:3C:E7:34:27:F1:3C:31:D6:04:CA:0E:ED:4E:19:D7:C3:C3:F1:49:FF:40:D8:F8:A5:78:56:A5:35:7B:F5:F0:67:66:42:D2:D6:E4:44:08:84:14:64:BD:84:FA:69:05:02:03:01:00:01*
Authority Info Access *http://servicios.firmaprofesional.com/ocsp*
Subject Key Identifier *A6:2E:EA:4D:25:2B:25:BA:A4:B5:DA:20:D2:1D:AE:E7:96:FD:99:F7*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.10.1*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CRL Distribution Points *https://crl.firmaprofesional.com/fpoot.crl*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *83:F6:F0:17:C2:53:6D:74:54:B7:B9:84:86:74:F3:64:01:29:CF:55:5D:D0:7D:83:D3:62:A1:7C:81:B7:52:5F*

Certificate fields details

Version: *3*
Serial Number: *7893570382112079418*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *63:65:B2:5E:92:99:B5:F3:82:EB:00:66:85:06:29:08:8E:BC:D9:BC:B3:98:F2:86:22:10:76:03:C3:C1:C2:7E*

X509SubjectName

Subject CN: *AC Firmaprofesional - AAPP*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Digitales para la Administracion Publica*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

17.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

17.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

17.2.4 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Emisión de certificados reconocidos (AAPP)

Name	[en]	Qualified Certificates Issuance (AAPP)

Service digital identities**X509SubjectName**

Subject CN:	AC Firmaprofesional - AAPP
Subject SERIAL NUMBER:	A62634068
Subject OU:	Certificados Digitales para la Administracion Publica
Subject O:	Firmaprofesional SA
Subject C:	ES

X509SKI

X509 SK I	pi7qTSUrJbqktdog0h2u55b9mfc=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2017-11-16T00:00:00Z

17.2.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

17.2.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.2.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

17.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Emisión de certificados reconocidos (AAPP)*

Name [en] *Qualified Certificates Issuance (AAPP)*

Service digital identities**X509SubjectName**

Subject CN: *AC Firmaprofesional - AAPP*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Digitales para la Administracion Publica*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

X509SKI

X509 SKI *pi7qTSUrJbqktdog0h2u55b9mfc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

17.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

17.2.5.5 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

17.2.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es] Emisión de certificados reconocidos (AAPP)*

Name [en] Qualified Certificates Issuance (AAPP)

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - AAPP

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Digitales para la Administracion Publica

Subject O: Firmaprofesional SA

Subject C: ES

X509SKI

X509 SK I pi7qTSUrJbqktdog0h2u55b9mfc=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2011-04-28T00:00:00Z

17.2.6.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es] está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2

17.3 - Service (granted): Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Cualificados*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Fri Dec 14 11:13:23 CET 2018*

Valid to: *Tue Dec 31 05:02:00 CET 2030*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:70:89:54:09:A0:9E:D7:68:0C:9C:5B:15:15:E3:DE:F5:9E:76:CE:F7:9B:3F:F2:77:D1:4A:E1:34:7D:07:E2:F9:F2:E9:54:8B:A1:53:90:F9:A3:10:BE:FA:96:F4:99:93:A0:82:00:D6:2E:F6:8E:9F:13:9D:63:47:AB:44:4D:95:03:33:8D:DF:AE:42:47:95:48:83:AB:A2:14:87:31:E8:DA:87:4C:B1:F8:25:2E:B2:85:83:49:73:9D:84:A5:7E:08:28:CD:FA:7B:DC:08:35:31:25:6F:A3:9A:23:7F:51:56:64:1F:34:11:2B:73:34:71:B4:11:19:13:40:0D:E2:8F:82:B5:2B:07:4D:36:F0:E8:41:83:23:CE:C4:CE:92:C7:70:48:C5:7C:FC:AF:69:97:5E:D9:45:92:48:2D:55:83:AD:53:CC:F2:4F:83:8C:F9:CE:A6:3C:49:A7:58:BF:AE:1E:9B:8B:E0:C9:73:BD:9F:F5:46:B3:BE:CA:7C:AE:6B:9E:21:1A:48:78:8A:28:ED:D5:AD:CF:79:C8:1D:63:BD:BA:F4:57:E1:96:C2:16:31:29:D7:BC:A3:9E:63:AB:BA:F8:5F:82:92:4C:70:AA:24:4E:E3:1B:C2:11:55:D8:D4:E6:C8:1C:F8:17:38:DD:D5:61:62:33:2F:1B:E5:02:03:01:00:01

Authority Info Access *http://crl.firmaprofesional.com/caroot.crt*
http://ocsp.firmaprofesional.com

Subject Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4C:CF:17:C0:C8:C1:C1:0D:58:76:EC:5E:32:80:FE:8D:13:4D:F3:6A:ED:D8:44:42:89:B9:90:BC:37:41:E7:4F*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-04-20T00:00:00Z*

17.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

17.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

17.3.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.13.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.22.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.21.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.1.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.11.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.2.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.12.3>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.40.3>

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.10.3

17.3.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Name [es] Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - CUALIFICADOS

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Cualificados

Subject O: Firmaprofesional S.A.

Subject C: ES

X509SKI

X509 SK I jHhMkwdv0dWGah2CokHZTAL4II0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2022-09-13T00:00:00Z

17.3.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

17.3.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

17.3.4.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.13.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.22.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.21.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.1.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.11.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.2.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.12.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.13177.10.1.40.3

17.3.5 - History instance n.2 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Name	[es]	Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"

Service digital identities**X509SubjectName**

Subject CN: *AC Firmaprofesional - CUALIFICADOS*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Certificados Cualificados*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *jHHMkwdv0dWGaH2COkHZTAL4II0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-10-28T01:00:00Z*

17.3.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.13.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.1.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.11.3*

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.13177.10.1.2.3

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.13177.10.1.12.3

17.3.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.3.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

17.3.6 - History instance n.3 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Name [es] Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - CUALIFICADOS

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Cualificados

Subject O: Firmaprofesional S.A.

Subject C: ES

X509SKI

X509 SK I jHhMkwdv0dWGah2CokHZTAL4II0=

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2017-11-16T00:00:00Z***17.3.6.7 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.13.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.1.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.11.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.2.3*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.12.3*

17.3.6.8 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

17.3.6.9 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

17.3.7 - History instance n.4 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Name	[es]	Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"

Service digital identities**X509SubjectName**

Subject CN:	AC Firmaprofesional - CUALIFICADOS

Subject SERIAL NUMBER:	A62634068

Subject OU:	Certificados Cualificados

Subject O:	Firmaprofesional S.A.

Subject C:	ES

X509SKI

X509 SK I	jHhMkwdv0dWGah2COkHZTAL4II0=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

17.3.7.10 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.13177.10.1.10.2

17.3.7.11 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.11.3

17.3.7.12 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

17.3.8 - History instance n.5 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by "AC Firmaprofesional - CUALIFICADOS"

Name [es] Certificados reconocidos emitidos por la "AC Firmaprofesional - CUALIFICADOS"

Service digital identities**X509SubjectName**

Subject CN: AC Firmaprofesional - CUALIFICADOS

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Cualificados

Subject O: Firmaprofesional S.A.

Subject C: ES

X509SKI

X509 SK I

jHMMkwdv0dWGaH2COkHZTAL4II0=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2015-07-26T22:00:00Z

17.3.8.13 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[OIDsURN]

urn:oid:1.3.6.1.4.1.13177.10.1.10.2

17.4 - Service (withdrawn): AC Firmaprofesional – CLOUD QUALIFIED TSA

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en]

A time-stamping generation service creating and signing qualified time-stamps tokens.

[es]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en]

AC Firmaprofesional – CLOUD QUALIFIED TSA

Name [es]

AC Firmaprofesional – CLOUD QUALIFIED TSA

Service digital identities

Certificate fields details

Version:

3

Serial Number:

6161211743113377719

-----END CERTIFICATE-----

SHA256withRSA

AC Firmaprofesional - INFRAESTRUCTURA

A62634068

Security Services

Firmaprofesional S.A.

ES

FIRMAPROFESIONAL CLOUD QUALIFIED TSU

VATES-A62634068

Firmaprofesional S.A.

ES

Mon Feb 27 14:19:33 CET 2017

Sun Feb 26 14:19:33 CET 2023

[illegible]

<http://crl.firmaprofesional.com/infraestructura.crt>

<http://ocsp.firmaprofesional.com>

F0:4D:42:4A:5E:32:C1:02:FE:61:82:AD:EC:25:50:86:07:0D:FB:B1

IsCA: false

62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79

Policy OID: 1.3.6.1.4.1.13177.10.1.4.1

CPS pointer: <http://www.firmaprofesional.com/cps>

CPS text: [Certificado de Servicio Seguro TSA]

CRL Distribution Points *http://crl.firmaprofesional.com/infraestructura.crl*
http://crl2.firmaprofesional.com/infraestructura.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *85:AF:F8:9B:8E:90:39:70:02:70:BB:83:6C:F5:35:8E:B8:85:A9:4F:FA:B4:6E:0E:94:15:F1:6C:5D:21:62:89*

X509SubjectName

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *8E1CSl4ywQL+YYKt7CVQhgcN+7E=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-12-21T00:00:00Z*

17.4.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] AC Firmaprofesional – CLOUD QUALIFIED TSA*

Name *[es] AC Firmaprofesional – CLOUD QUALIFIED TSA*

Service digital identities**X509SubjectName**

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Subject 2.5.4.97: *VATES-A62634068*

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	AC Firmaprofesional -INFRAESTRUCTURA
Name	[es]	AC Firmaprofesional -INFRAESTRUCTURA

```
Version: 3
Serial Number: 3137071291384231299
X509 Certificate -----BEGIN CERTIFICATE-----
```

Signature algorithm:	SHA256withRSA
Issuer CN:	Autoridad de Certificacion Firmaprofesional CIF A62634068
Issuer C:	ES

Subject CN: *AC Firmaprofesional - INFRAESTRUCTURA*
Subject SERIAL NUMBER: *A62634068*
Subject OU: *Security Services*
Subject O: *Firmaprofesional S.A.*
Subject C: *ES*
Valid from: *Wed Jul 29 13:25:09 CEST 2015*
Valid to: *Tue Dec 31 05:02:55 CET 2030*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:A5:FB:57:D4:4F:1E:66:7F:4A:91:A5:85:74:9F:44:41:2D:3A:28:91:4B:C4:9D:24:2D:50:88:E0:76:11:82:E2:14:47:8B:D9:01:59:1C:84:4F:E0:70:66:F8:26:C8:67:B8:6C:F8:62:C3:E5:73:86:59:AF:38:43:D0:60:44:8D:87:5C:5E:04:F4:F7:82:42:1F:9E:8E:D9:E7:A4:34:50:97:1F:DC:22:45:F9:CE:DE:F9:D3:15:DF:8C:0A:E2:7D:54:88:21:41:D1:7E:2C:9F:66:63:6E:CA:7D:EA:A8:1E:4E:FE:7C:F5:2B:F6:1E:94:A4:99:B5:88:DC:D3:4A:A5:C1:75:38:B1:FA:D9:44:52:60:9B:43:C3:EA:8C:49:A8:BA:14:F1:55:44:8C:1C:DD:6D:55:AC:1B:D2:84:73:DD:60:1B:4B:89:50:96:72:2D:61:89:3F:67:FB:23:FC:EB:92:2D:96:39:FF:52:3D:FA:C0:D3:5B:E2:63:0D:8F:49:EF:FC:D5:9E:CE:84:00:CA:C8:4E:FA:37:A6:7C:93:2E:07:69:2D:5A:36:CA:B1:C7:F2:D3:CA:55:21:FB:D3:B4:71:C1:8A:49:04:A9:3B:CE:CB:15:BA:CA:36:29:46:BC:84:50:63:3A:E3:22:D5:1A:C0:68:05:D0:A8:94:13:02:03:01:00:01*
Authority Info Access *http://crl.firmaprofesional.com/caroot.crt*
http://ocsp.firmaprofesional.com
Subject Key Identifier *62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps
CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*
Extended Key Usage *id_kp_clientAuth - id_kp_serverAuth - id_kp_OCSPSigning - id_kp_timeStamping*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *CD:74:19:8D:4C:23:E4:70:1D:EA:57:98:92:32:1B:9E:4F:47:A0:8B:D8:37:47:10:B8:99:AA:D1:49:5A:4B:35*

Certificate fields details

Version: *3*
Serial Number: *1069733489479276534*

Extended Key Usage *id_kp_serverAuth - id_kp_timeStamping*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *84:8C:03:AB:64:7D:5B:D7:E0:D0:C4:3C:0B:5D:67:4C:C9:89:3F:83:6A:B8:63:AF:8F:3F:13:84:B5:44:D8:33*

X509SubjectName

Subject CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Security Services*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *YhWrtbMleaWH/oDZlvCO/I8R/Xk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-01-26T01:00:00Z*

17.5.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.5.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *AC Firmaprofesional -INFRAESTRUCTURA*

Name *[es]* *AC Firmaprofesional -INFRAESTRUCTURA*

Service digital identities**X509SubjectName**

Subject CN: *AC Firmaprofesional - INFRAESTRUCTURA*

Subject SERIAL NUMBER: *A62634068*

Subject OU: *Security Services*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *YhWrtbMleaWH/oDZlvCO/l8R/Xk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-11-16T00:00:00Z*

17.5.2.1 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.6 - Service (withdrawn): Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Name *[en]* *Qualified timestamps issued by FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

Service digital identities**Certificate fields details**

Version: *3*

Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	<i>http://crl.firmaprofesional.com/infraestructura.crl</i> <i>http://crl2.firmaprofesional.com/infraestructura.crl</i>
Subject Key Identifier	<i>69:19:6D:E5:29:00:95:AC:6D:E8:48:A6:B7:9A:8C:59:82:9D:A7:73</i>
Key Usage:	<i>digitalSignature - nonRepudiation</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>CC:93:E2:7B:3D:2B:C8:FF:4E:4D:0E:65:2F:A2:18:7F:E3:AB:5D:FA:65:28:72:5C:FE:E3:70:E0:79:9C:E1:4A</i>

X509SubjectName

Subject CN:	<i>FIRMAPROFESIONAL CLOUD QUALIFIED TSU</i>
Subject 2.5.4.97:	<i>VATES-A62634068</i>
Subject O:	<i>Firmaprofesional S.A.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>aRlt5SkAlaxt6Eimt5qMWYKdp3M=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2024-12-03T00:00:00Z</i>

17.6.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name <i>[es]</i>	<i>Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU</i>
Name <i>[en]</i>	<i>Qualified timestamps issued by FIRMAPROFESIONAL CLOUD QUALIFIED TSU</i>

Service digital identities**X509SubjectName**

Subject CN:	<i>FIRMAPROFESIONAL CLOUD QUALIFIED TSU</i>

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - Secure Web 2020*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Thu Jul 30 10:58:14 CEST 2020*

Valid to: *Sun Jul 30 10:58:14 CEST 2023*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8E:1E:6E:D0:7D:E5:23:7E:4B:62:FF:34:E3:77:8A:4F:91:76:8E:42:BC:4B:00:70:8D:5E:B9:7E:9E:75:85:3D:0D:F0:51:2E:FF:92:32:59:47:92:0C:E5:A7:5C:94:96:81:6E:22:99:AA:4E:A6:3D:BD:92:4B:03:62:01:2C:8E:55:D5:78:8F:93:96:EB:5E:C2:90:66:DA:14:D7:5C:B7:7C:8E:BD:60:A7:10:20:A7:20:E4:15:36:3F:0F:B3:E4:19:A6:C3:D3:11:04:DA:0E:2C:68:CC:A6:95:C2:21:AA:7E:FA:4E:BF:35:3D:8C:19:90:D9:16:27:40:08:99:A8:D4:30:18:AB:AC:E4:25:7D:14:8E:79:38:36:5B:40:33:6A:FC:E2:DB:53:9C:F4:7C:83:CC:C8:48:B5:49:6D:28:EC:9B:88:30:15:CB:B4:9D:BC:3F:C9:C6:D2:A1:5B:68:18:66:59:7F:7E:2E:67:A4:BB:7D:14:5C:67:7F:99:E5:4D:D6:EE:65:FF:94:D1:1A:FB:05:3A:C0:F3:BA:CF:36:34:21:E0:AA:A6:BA:F6:41:74:76:6A:CB:35:C3:7E:A0:74:69:6D:13:C4:E5:0F:A5:41:91:87:96:CE:BF:91:A7:E5:B9:C0:D1:5B:97:51:0E:85:63:59:69:5F:95:30:33:02:03:01:00:01

Authority Info Access
<http://crl.firmaprofesional.com/caroot.crt>
<http://ocsp.firmaprofesional.com>

Subject Key Identifier *BD:97:0E:67:88:68:ED:29:1B:9B:AB:6A:0A:8A:36:8A:8D:2E:16:29*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *93:3B:80:F7:B9:72:55:DF:5C:F1:D9:5A:12:3E:90:17:22:DD:B3:0B:48:1A:F3:AA:83:54:82:01:11:9E:D3:03*

X509SubjectName

Subject CN: *AC Firmaprofesional - Secure Web 2020*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *vZcOZ4ho7Skbm6tqCoo2io0uFik=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-02-06T00:00:00Z*

17.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.7.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020*

Name [es] *Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2020*

Service digital identities

X509SubjectName

Subject CN: *AC Firmaprofesional - Secure Web 2020*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Issuer CN: *AC Firmaprofesional - CUALIFICADOS*

Issuer SERIAL NUMBER: *A62634068*

Issuer OU: *Certificados Cualificados*

Issuer O: *Firmaprofesional S.A.*

Issuer C: *ES*

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Thu Aug 06 13:39:33 CEST 2020*

Valid to: *Wed Aug 05 13:39:33 CEST 2026*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A1:01:28:28:61:4D:30:23:D7:13:AD:E7:E9:BA:6F:78:7A:22:98:39:33:14:62:A7:18:5D:57:74:26:2A:00:01:6E:AA:45:63:7D:33:64:86:1F:17:22:A2:2D:9D:80:BC:70:06:5A:5B:9F:EE:9A:FC:E5:77:80:73:40:CB:EE:5D:1C:C9:CB:A1:71:81:1C:35:17:A7:CE:D6:ED:F4:B7:F7:1A:A7:92:AE:AD:8A:27:FB:CD:E4:35:3F:04:0D:37:4C:AE:21:43:D8:75:AC:B4:EB:52:C0:80:11:58:36:48:B9:66:60:62:29:98:5D:F9:08:30:62:E9:31:61:7E:11:4F:4D:09:2C:02:5E:69:D2:45:56:C6:42:40:AC:2F:0C:D5:5B:4A:BA:95:08:85:38:DE:6E:18:67:E6:28:99:68:76:D1:1C:91:07:44:75:F4:43:52:24:DE:99:52:28:E9:79:32:A6:0C:FF:A4:0E:AA:15:C2:F2:0E:42:54:CB:97:87:16:1C:7D:0D:16:C0:8E:95:E6:8B:56:99:7C:45:8E:0B:D7:94:3A:B6:7B:32:7A:D4:8B:0F:BE:7E:87:34:4C:D9:45:C9:1E:20:E6:C3:3A:A2:C2:77:42:20:35:DD:56:63:46:CC:AD:7A:F7:5F:8C:5E:4A:19:0F:BA:30:93:0E:69:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Authority Info Access
http://crl.firmaprofesional.com/cualificados.crt
http://ocsp.firmaprofesional.com

Certificate Policies
Policy OID: 1.3.6.1.4.1.13177.10.1.4.1
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Certificado de Servicio Seguro de TSA cualificada]

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*

Subject Key Identifier *FD:7B:45:0E:E9:80:02:FD:3E:EB:55:8A:AA:C8:E1:9B:DD:3F:55:56*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E9:F0:94:3D:FC:4D:49:33:39:62:8A:18:3B:1F:89:09:B4:FD:B8:7B:C1:D9:1B:0C:B
C:D1:7B:F3:83:3C:20:22*

X509SubjectName

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I */XtFDumAAv0+61WKqsjhm90/VVY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2024-12-03T00:00:00Z*

17.8.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name [en] *AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

Name [es] *AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

Service digital identities

X509SubjectName

Subject CN: *FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I */XtFDumAAv0+61WKqsjhm90/VVY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-10-05T00:00:00Z*

Valid from: *Fri Mar 05 11:43:35 CET 2021*

Valid to: *Mon Mar 04 11:43:35 CET 2024*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A2:96:E0:B1:C5:4C:F9:6D:EF:B8:2F:9E:B0:D0:C2:28:1E:06:13:CF:71:86:8C:C5:F0:A4:EC:47:59:45:08:97:0D:0E:F7:82:76:D8:F0:48:5D:78:EC:26:36:DF:2E:08:67:47:32:75:F4:2F:26:6B:83:61:9A:16:53:0F:01:E4:03:F6:6A:23:58:E0:61:77:C4:33:04:4C:2F:CB:9B:D8:93:B1:49:F0:17:24:52:6C:D4:53:68:68:2B:5F:DD:D8:71:71:BA:DC:3E:EF:E9:8F:48:D2:6C:5E:97:A1:9A:C3:2E:19:DC:6C:BE:23:AA:A0:BB:2F:9F:78:06:D6:7C:41:F2:89:EC:98:D0:13:1A:CE:47:F4:6B:53:F7:57:84:68:99:B8:8C:4B:9A:19:2F:4A:A8:B5:1C:26:8D:8F:07:23:7C:00:FD:B7:66:E5:EF:70:D8:7A:26:AA:23:9D:8A:64:A7:EE:5C:F5:06:50:58:ED:4E:68:81:DD:8A:83:A3:C6:D5:72:21:72:48:06:36:37:C1:86:AB:37:FB:97:C3:40:72:34:72:EA:1A:4D:BD:F1:C1:C0:29:56:F8:E1:4D:6C:67:1E:4F:A0:18:75:58:9B:77:49:93:D5:11:69:77:D8:BA:F8:37:6F:A7:33:00:01:D8:B2:0F:FC:49:78:F3:57:02:03:01:00:01*

Authority Info Access *http://crl.firmaprofesional.com/caroot.crt*
http://ocsp.firmaprofesional.com

Subject Key Identifier *0B:6A:EC:EB:B2:A8:20:6B:3A:D7:B7:59:6E:4A:2A:2D:CD:DE:7C:6F*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPs text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPs pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *59:22:85:35:D1:14:E8:D2:9F:9B:92:D4:22:51:8B:C6:3D:DC:B5:70:97:42:8D:8C:C9:87:77:D9:07:C6:EE:FE*

X509SubjectName

Subject CN: *AC Firmaprofesional - Secure Web 2021*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *C2rs67KoIGs617dZbkoqLc3efG8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time 2024-05-13T00:00:00Z

17.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

17.9.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2021

Name [es] Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2021

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - Secure Web 2021

Subject OU: Security Services

Subject 2.5.4.97: VATES-A62634068

Subject O: Firmaprofesional S.A.

Subject C: ES

X509SKI

X509 SK I C2rs67KoIGs617dZbkoqLc3efG8=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-03-17T01:00:00Z

17.9.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Tue Apr 13 11:32:20 CEST 2021*

Valid to: *Tue Dec 31 05:02:00 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CD:08:9C:C3:85:94:6D:7F:D1:6D:39:00:46:1E:DF:28:44:BA:55:56:52:AC:20:80:08:32:EA:E3:F4:8A:AD:D6:0F:6E:32:0C:1C:F6:9A:26:7D:AE:C8:83:8B:F5:B9:CC:DE:50:C0:78:78:AA:5F:FD:E2:AD:3C:85:32:89:C1:BE:9A:EB:44:11:2B:11:C4:9B:1B:C6:BE:F0:26:A0:26:EF:AA:C8:D8:F8:42:C6:39:52:80:19:AC:D0:CA:E8:23:18:E1:2A:F7:B7:7A:0E:0D:F7:B9:6E:62:71:12:5A:B4:BD:49:EB:78:77:82:6A:DA:55:C6:A4:48:C2:2F:3C:5F:74:08:3C:26:FB:C7:77:6E:71:5A:92:33:D9:8E:EF:3C:80:B5:D3:C0:E7:40:A0:DC:04:2E:C4:11:75:04:35:BE:23:44:72:2B:77:BC:0B:8E:0C:C6:CE:B7:DC:DD:22:33:9B:BC:D7:3C:EB:25:49:16:27:7F:78:0E:86:16:F0:5B:9A:0F:4E:AB:D9:81:C2:7F:4F:04:B4:93:C3:16:DE:A6:5D:77:C2:B3:4F:91:7F:F2:74:10:A8:F3:42:5F:CE:F6:45:96:77:C9:3E:9E:F2:7F:85:F8:25:43:D0:98:0E:AC:5A:2D:F4:89:6A:98:47:80:54:2F:D0:E5:E8:48:00:4F:1C:D8:29:B1:29:F4:36:66:A1:1E:F6:90:0F:52:60:7B:FE:F4:CE:EB:E9:C5:D4:03:66:29:C1:D6:BD:2F:14:52:EB:3C:CB:07:90:18:4F:C9:CF:B6:8D:45:72:8E:C5:C0:D3:F6:11:2A:93:87:75:36:59:94:F7:5C:24:C8:B8:CC:43:E9:E9:F8:4D:05:80:3E:A5:FE:EE:C9:16:46:FE:93:53:69:A9:E1:79:36:58:99:95:9F:C2:93:05:29:69:48:EE:BB:42:00:8B:4C:9E:37:88:67:01:15:5A:19:01:D4:E0:C4:82:FD:02:6A:D9:10:65:CC:82:FA:62:F7:C3:68:BD:F1:A7:51:80:91:A1:6A:52:99:9E:AF:C6:1B:83:4A:05:4D:B2:E7:D9:88:32:21:D9:5E:FB:97:87:07:6A:B7:A0:B3:8D:35:08:58:23:9C:46:81:B1:0B:C7:52:9E:E0:81:2B:3E:98:D0:FD:AA:D7:4F:18:F7:10:19:2C:74:4A:21:80:C3:C5:48:EE:C6:B8:51:E0:D7:BC:B8:DD:F3:F5:63:F0:99:A0:E4:8E:FB:21:91:53:2E:90:78:DE:8F:C4:D5:58:57:7D:B6:CC:99:2F:72:09:88:1C:D9:23:8B:80:F6:E7:44:EF:A9:2A:C8:BA:7E:48:91:C1:10:64:46:28:0F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Authority Info Access
http://crl.firmaprofesional.com/caroot.crt
http://ocsp.firmaprofesional.com

Certificate Policies
Policy OID: 2.5.29.32.0
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Subject Key Identifier *16:A6:B4:B1:6C:C4:DB:DF:38:47:4C:1A:C0:46:36:58:DE:2C:EB:62*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *75:B1:4D:4D:63:80:6F:30:F5:38:06:0F:2E:B6:5C:13:65:BF:C0:CD:7F:3E:CD:C6:C0:07:02:18:B6:E4:67:59*

X509SubjectName

Subject CN: *AC Firmaprofesional - Timestamp 2021*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - Secure Web 2022*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: *Fri Mar 04 12:03:58 CET 2022*

Valid to: *Mon Mar 03 12:03:58 CET 2025*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A7:19:72:31:B6:22:62:4D:7A:50:57:95:D7:CD:A9:4E:D0:F2:19:8B:CF:8C:1D
F6:56:46:AC:BA:28:40:E0:A7:8C:5D:AD:12:EC:08:00:13:C9:0F:D2:09:36:7C:8E:88:AB:C9:E7:4B:EC:28:A0:EE:57:92:98:90:6F:08:5C:F4:81:2C:89:95:A0:AC:46:8A:5B:07:0D:84:E1:8E:9
E:C9:78:02:87:A5:B8:67:21:3F:4F:76:EA:37:AA:65:96:29:5F:32:20:AE:1C:DD:E6:3E:C4:34:FB:ES:8F:D0:FB:C8:29:79:EA:E8:88:97:7B:CA:ED:95:95:C3:DC:31:37:3A:F7:75:89:2B:56:0E:
47:E7:7E:E1:9E:3D:95:58:7D:DF:83:7C:6E:F3:70:72:58:69:19:ED:0C:56:4E:53:20:06:41:DA:B5:6E:5D:F1:E2:DE:B0:41:01:CB:DF:61:97:EF:44:FA:50:0E:29:61:2D:E3:69:2A:F7:A4:44:6B
3B:33:36:37:87:72:1E:8C:3E:64:90:D1:7C:3F:40:ED:8D:77:70:7B:3F:96:39:1B:89:5B:06:29:F8:7E:4D:1C:6C:7B:C9:B6:DE:68:B5:D2:51:8C:92:40:5A:5C:9D:F0:D3:8F:75:E7:11:D9:9
5:3D:7A:AA:18:EA:A0:AB:0C:5A:D7:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Authority Info Access
http://crl.firmaprofesional.com/caroot.crt
http://ocsp.firmaprofesional.com

Certificate Policies
Policy OID: 2.5.29.32.0
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps

Extended Key Usage *id_kp_serverAuth*

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Subject Key Identifier *9B:8D:B1:FE:46:22:0F:35:90:50:3B:24:41:F9:F3:3A:EC:EC:BC:F1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C0:68:D7:76:78:42:55:77:2B:BC:6A:E9:F7:0A:53:6A:41:0A:D6:88:A5:0D:DE:AF:B
F:66:BC:C5:25:47:96:F6*

X509SubjectName

Subject CN: AC Firmaprofesional - Secure Web 2022

Subject OU: Security Services

Subject 2.5.4.97: VATES-A62634068

Subject O: Firmaprofesional S.A.

Subject C: ES

X509SKI

X509 SK I m42x/kYiDzWQUDskQfnzOuzsvPE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2025-10-02T02:00:00Z

17.11.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

17.11.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2022

Name [en] Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2022

Service digital identities

X509SubjectName

Subject CN: AC Firmaprofesional - Secure Web 2022

Subject OU: Security Services

Subject 2.5.4.97: VATES-A62634068

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *m42x/kYiDzWQUDskQfnzOuzsvPE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-07-26T00:00:00Z*

17.11.2.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

17.12 - Service (granted): Qualified certificates issued by "AC FIRMAPROFESIONAL ICA B01 QUALIFIED 2022"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	<i>Qualified certificates issued by "AC FIRMAPROFESIONAL ICA B01 QUALIFIED 2022"</i>
Name	[es]	<i>Certificados cualificados emitidos por la "AC FIRMAPROFESIONAL ICA B01 QUALIFIED 2022"</i>

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *46921626131428221768086730976013821699*

Thumbprint: 4A:86:F3:33:7C:EC:89:A6:78:96:B8:A6:CB:BA:DA:84:AC:18:1E:B0:09:67:9E:15:04:15:6C:34:BC:9F:8A:A1

X509SubjectName

Subject CN: FIRMAPROFESIONAL ICA B01 QUALIFIED 2022

Subject 2.5.4.97: VATES-A62634068

Subject O: Firmaprofesional SA

Subject C: ES

X509SKI

X509 SK I S8252hMmVqqMfoh4gIR+zomSk4A=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2022-11-24T00:00:00Z

17.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

17.12.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

17.12.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.13.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.11.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.12.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.13177.10.1.40.3

17.13 - Service (granted): Qualified website authentication certificates issued by "AC FIRMAPROFESIONAL ICA A01 QWAC 2022"

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified website authentication certificates issued by "AC FIRMAPROFESIONAL ICA A01 QWAC 2022"

Name [es] Certificados cualificados de autenticación de sitio web emitidos por la "AC FIRMAPROFESIONAL ICA A01 QWAC 2022"

Service digital identities

Certificate fields details

Version: 3

Serial Number: 14462178535983271458309355633629699398

[illegible]

-----END CERTIFICATE-----

SHA384withECDSA

FIRMAPROFESIONAL CA ROOT-A WEB

VATES-A62634068

Firmaprofesional SA

ES

FIRMAPROFESIONAL ICA A01 OWAC 2022

VATES-A62634068

Firmaprofesional SA

ES

Tue Jul 19 14:16:44 CEST 2022

Sun Jul 18 14:16:44 CEST 2027

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:BE:EB:85:18:51:6B:F9:5C:56:F1:EA:1E:BD:38:2D:82:EE:6C:EF:2D:DF:EA:51:11:86:28:C7:72:4D:FA:19:11:18:0A:F8:CC:48:46:D3:6A:82:75:BD:A5:37:1E:BA:27:9F:13:26:02:EA:C5:F8:3D:8A:BB:88:DE:06:64:C3:F2:CA:78:96:F7:DA:1F:43:A7:2B:D7:9F:CD:D6:7A:37:32:67:F6:F7:5F:41:98:0B:7A:BC:9A:94:C9:77:DE:BC:DE

IsCA: true - Path length: 0

93:E1:43:63:5C:3C:9D:D6:27:F3:52:EC:17:B2:A9:AF:2C:F7:76:F8

http://crl.firmaprofesional.com/caroot-a_web.crt
http://ocsp.firmaprofesional.com

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <http://www.firmaprofesional.com/cps>]

```
id kp serverAuth
```

http://crl.firmaprofesional.com/caroot-a_web.crl

FD:3C:A7:E7:A2:68:D6:28:1A:3A:CF:7D:16:10:C4:FE:42:01:5B:C3

keyCertSign - cRLSign

Thumbprint algorithm: *SHA-256*

Thumbprint: *CC:1B:9F:9E:43:70:FB:68:14:1D:28:A1:15:EA:A8:63:F8:EA:DB:7A:04:E2:BD:23:B3:C6:2F:9D:9F:17:C2:63*

X509SubjectName

Subject CN: *FIRMAPROFESIONAL ICA A01 QWAC 2022*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

X509SKI

X509 SK I */Tyn56Jo1igaOs99FhDE/kIBW8M=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time

2022-11-24T00:00:00Z

17.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.14 - Service (granted): Sellos cualificados de tiempo emitidos por "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.*

Service Name

Name [es] *Sellos cualificados de tiempo emitidos por "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"*

Name [en] *Qualified timestamps issued by "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"*

Service digital identities

CRL Distribution Points *http://crl.firmaprofesional.com/caroot-b_gp.crl*

Subject Key Identifier *62:86:15:B9:E8:FD:95:F4:49:13:F6:7F:0F:AD:06:B3:55:A1:1F:BB*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1F:3F:44:97:DF:9B:AC:9D:72:F9:99:75:B3:7D:ED:7D:5D:B9:30:05:B1:BF:80:E0:71:02:76:6F:3A:E4:05:B9*

X509SubjectName

Subject CN: *FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional SA*

Subject C: *ES*

X509SKI

X509 SK I *YoYVuej9IfRJE/Z/D60Gs1WhH7s=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2022-11-24T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Firmaprofesional.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Firmaprofesional.aspx*

17.15 - Service (withdrawn): Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2024

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Certificate fields details

Version: 3

Serial Number: 54936302946284401254096794889344300539

X509 Certificate

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: AC Firmaprofesional - Secure Web 2024

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject 0: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: Wed Feb 14 12:20:46 CET 2024

Valid to: Sat Feb 13 12:20:46 CET 2027

[illegible]

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Authority Info Access
<http://crl.firmaprofesional.com/caroot.crt>
<http://ocsp.firmaprofesional.com>

Certificate Policies
 Policy OID: 2.5.29.32.0
 CPS pointer: <http://www.firmaprofesional.com/cps>

Extended Key Usage
 id_kp_serverAuth

CRL Distribution Points
<http://crl.firmaprofesional.com/fproot.crl>

Subject Key Identifier
 E8:8C:2C:05:7F:A7:04:D9:D7:8E:F9:31:D0:87:B0:A3:50:86:40:4C

Key Usage:
 keyCertSign - cRLSign

Thumbprint algorithm:
 SHA-256

Thumbprint:
 C3:F5:32:65:37:DB:64:77:C4:D7:BF:83:0F:F5:B4:01:A7:AD:B2:97:07:70:2A:DD:98:E6:24:61:F9:EE:67:C7

X509SubjectName

Subject CN:
 AC Firmaprofesional - Secure Web 2024

Subject OU:
 Security Services

Subject 2.5.4.97:
 VATES-A62634068

Subject O:
 Firmaprofesional S.A.

Subject C:
 ES

X509SKI

X509 SK I
 6lwsBX+nBNnXjvkx0Iewo1CGQEw=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
 [es] undefined.

Status Starting Time
 2026-05-20T03:00:00Z

17.15.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

17.15.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2024*

Name *[en]* *Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2024*

Service digital identities**X509SubjectName**

Subject CN: *AC Firmaprofesional - Secure Web 2024*

Subject OU: *Security Services*

Subject 2.5.4.97: *VATES-A62634068*

Subject O: *Firmaprofesional S.A.*

Subject C: *ES*

X509SKI

X509 SK I *6lwsBX+nBNnXjvkx0Iewo1CGQEw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-05-13T00:00:00Z*

17.15.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

17.16 - Service (granted): Issuance of qualified electronic certificates for website authentication issued by AC Firmaprofesional Secure Web 2025

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	[en]	Issuance of qualified electronic certificates for website authentication issued by AC Firmaprofesional Secure Web 2025

Name [es] Expedición de certificados electrónicos cualificados de autenticación de sitios web emitidos por AC Firmaprofesional Secure Web 2025

Service digital identities

Certificate fields details

Version: 3

Serial Number: 9593914973816114120304278634608082044

X509 Certificate

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autoridad de Certificacion Firmaprofesional CIF A62634068*

Issuer C: *ES*

Subject CN: *AC Firmaprofesional - Secure Web 2025*

Subject 2.5.4.97: *VATES-A62634068*

Subject 0: *Firmaprofesional S.A.*

Subject C: *ES*

Valid from: Tue Feb 25 13:35:39 CET 2025

Valid to: *Fri Feb 25 13:35:39 CET 2028*

Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EC:9F:3F:EE:F8:87:22:94:53:19:31:52:21:DD:18:DA:5A:4D:4A:3B:AF:0B:E3:A1:02:7C:B2:3D:42:AA:3C:B0:D9:BE:1C:EA:DA:9C:5A:84:0E:EC:4F:E4:3C:44:74:4C:F1:57:90:AE:4C:69:8A:7C:43:93:FA:8B:19:AF:5B:E7:E3:27:5F:8A:65:69:8C:30:AA:5D:4F:00:8D:06:C6:62:C2:8E:2D:2F:1E:65:8E:0D:2F:BA:A6:F8:A9:D3:B6:D8:68:6F:F1:F0:C2:21:15:4F:82:D7:6A:42:77:89:3A:A9:0A:02:66:74:62:79:4C:21:37:DB:D1:CF:50:80:4D:10:C9:33:40:98:01:EA:F7:2D:98:76:D2:0D:79:90:92:9C:9C:CE:A1:B8:71:97:94:9A:3D:0A:2B:0B:55:1A:53:38:E7:ED:5E:1E:73:11:86:51:31:C1:04:72:52:74:EB:9A:8D:58:2D:2B:2C:EC:4A:50:6D:62:DE:96:6D:4F:4E:D7:0A:67:7F:59:3F:66:9A:4D:42:0C:54:DD:03:FA:2A:85:35:7A:85:7C:01:EF:8E:02:91:31:C1:04:72:52:74:EB:9A:8D:58:2D:2B:2C:9B:5A:78:78:5C:D9:51:02:27:0A:B1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier 65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

Authority Info Access
<http://crl.firmaprofesional.com/caroot.crt>
<http://ocsp.firmaprofesional.com>

Certificate Policies
 Policy OID: 2.5.29.32.0

Extended Key Usage
 id_kp_serverAuth

CRL Distribution Points
<http://crl.firmaprofesional.com/fproot.crl>

Subject Key Identifier
 2A:A5:5B:FC:C6:0D:BB:25:3A:EF:87:8F:F5:1E:79:00:36:49:66:F5

Key Usage:
 keyCertSign - cRLSign

Thumbprint algorithm:
 SHA-256

Thumbprint:
 B7:8C:7F:63:E2:45:83:C7:D4:0C:1D:33:D8:DB:E1:16:B3:82:B4:BE:B9:EB:C4:1A:1A:06:8D:51:9B:AF:4B:AD

X509SubjectName

Subject CN:
 AC Firmaprofesional - Secure Web 2025

Subject 2.5.4.97:
 VATES-A62634068

Subject O:
 Firmaprofesional S.A.

Subject C:
 ES

X509SKI

X509 SK I
 KqVb/MYNuyU674eP9R55ADZJZvU=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
 [es] undefined.

Status Starting Time
 2025-10-02T02:00:00Z

17.16.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

18 - TSP: Tesorería General de la Seguridad Social

TSP Name

Name [en] *Tesorería General de la Seguridad Social*

Name [es] *Tesorería General de la Seguridad Social*

TSP Trade Name

Name [en] *Gerencia de Informática de la Seguridad Social*

Name [es] *Gerencia de Informática de la Seguridad Social*

Name [en] *Tesoreria General de la Seguridad Social*

Name [es] *Tesoreria General de la Seguridad Social*

Name [en] *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Name [en] *VATES-Q2827003A*

Name [en] *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

Name [es] *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

Name [en] *Seg-social*

Name [es] *Seg-social*

PostalAddress

Street Address [en] *Calle Doctor Tolosa Latour*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28041*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Calle Doctor Tolosa Latour*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[en]	Qualified certificates issued by GISS
Name	[es]	Certificados reconocidos emitido por GISS

Version: 3

Serial Number: 1045226008

Signature algorithm:	<i>SHA1withRSA</i>
Issuer OU:	<i>SGL</i>
Issuer O:	<i>Seq-social</i>

Issuer C: *ES*
Subject OU: *SGI*
Subject O: *Seg-social*
Subject C: *ES*
Valid from: *Fri Feb 14 13:03:28 CET 2003*
Valid to: *Tue Feb 14 13:33:28 CET 2023*
Public Key: *30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:A6:C8:9F:29:79:9A:2E:08:A8:52:D2:9F:9A:07:E1:02:21:35:F3:81:15:1A:CF:20:8F:9F:06:4D:48:F7:DA:25:59:7F:07:FD:41:1C:DA:8D:FD:77:85:AE:56:97:33:AF:DF:D7:B3:79:5D:9D:4E:7A:22:95:5B:62:1A:03:11:14:88:5A:C6:01:2C:36:2B:63:E1:99:D8:C5:61:D8:A7:9F:65:45:1D:DC:83:29:24:3E:11:FC:9E:4F:0D:67:3A:FC:5C:8A:37:7C:F6:36:0B:2A:76:5C:94:9D:02:BA:D4:CC:FA:9C:06:BA:D2:64:2B:25:89:E1:4E:5B:36:1C:CF:7D:02:03:01:00:01*
CRL Distribution Points *C=ES,O=Seg-social,OU=SGI,CN=CRL1*
Authority Key Identifier *71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*
Subject Key Identifier *71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*
Basic Constraints *IsCA: true*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *F8:00:14:4F:1B:0F:26:83:42:3F:3D:03:3A:4E:5B:B8:A4:67:59:9C:BB:06:36:2C:4C:19:C1:A9:D8:C2:51:B9*

X509SubjectName

Subject OU: *SGI*
Subject O: *Seg-social*
Subject C: *ES*

Service Status

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2018-05-03T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*
URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

18.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.1.4.2.1.3

18.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

18.1.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified certificates issued by GISS
Name	[es]	Certificados reconocidos emitido por GISS

Service digital identities

X509SubjectName

Subject OU:	SGL
Subject O:	Seg-social
Subject C:	ES

X509SKI

X509 SK I cXR36Dwip1KGUghdwGVkvPM02fg=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

18.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:2.16.724.1.4.2.1.3

18.1.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

18.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by GISS

Name [es] Certificados reconocidos emitido por GISS

Service digital identities**X509SubjectName**

Subject OU: SGI

Subject O: Seg-social

Subject C: ES

X509SKI

X509 SK I cXR36Dwip1KGUghdwGVkvPM02fg=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time 2010-04-20T00:00:00Z

18.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[OIDA_sURN]

urn:oid:2.16.724.1.4.2.1.3

18.2 - Service (withdrawn): Qualified certificates issued by SUBCA GISS01

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/OC>

Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en l

Qualified certificates issued by SUBCA GISS01

Name

[es]

Certificados reconocidos emitido por SUBCA GISS01

Service digital identities

Certificate fields details

Version:

3

Serial Number:

1466067264

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

RAIZ ACG/SSv2

Issuer SERIAL NUMBER: Q2827003A
Issuer OU: GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL
Issuer O: TESORERIA GENERAL DE LA SEGURIDAD SOCIAL
Issuer L: MADRID
Issuer C: ES
Subject CN: SUBCA GISS01
Subject SERIAL NUMBER: Q2827003A
Subject OU: GISS01
Subject OU: GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL
Subject O: TESORERIA GENERAL DE LA SEGURIDAD SOCIAL
Subject L: MADRID
Subject C: ES
Valid from: Thu Jun 16 11:51:17 CEST 2016
Valid to: Mon Jun 16 12:21:17 CEST 2031
Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:A3:10:C5:DC:E3:C9:EA:D6:43:47:3C:7D:17:32:2E:2B:E5:3D:53:07:C0:57:65:7E:00:3C:C6:95:90:6D:66:F6:47:7F:49:C3:83:E3:93:C4:E8:FE:7F:81:09:1A:D0:89:5F:61:46:04:2D:09:B9:AF:F4:00:1F:3B:BC:07:80:94:0B:CF:27:61:82:E8:45:3C:20:09:C6:81:88:6E:26:C9:81:34:31:D8:CE:C7:8F:85:FD:82:06:8C:97:6B:7A:2D:B2:77:CE:07:4B:E2:74:65:4F:55:99:CA:44:BC:9B:3E:37:21:C0:72:2B:88:13:FD:D3:E7:A3:A5:47:48:DF:5C:03:BB:C8:C3:60:2C:D5:15:62:A6:3C:59:B3:2C:AD:A7:E2:83:2A:71:80:E3:85:E6:A5:AB:07:AB:C7:80:2B:36:D1:58:8B:98:A8:64:69:36:72:F1:D4:CC:24:93:BE:BC:1A:21:EF:59:0A:21:E7:B4:0A:7F:8A:A7:51:E4:A2:C7:CD:3B:4A:E0:72:D9:56:5F:4E:02:0E:95:63:CA:21:BF:DF:35:A6:5F:D1:45:5B:1A:F4:95:8D:6D:8E:6D:18:89:91:09:EE:7B:85:34:8E:AC:C4:79:4C:BD:FF:ED:A7:AF:2C:A2:C0:3C:7E:FE:3A:74:F4:DB:2C:E9:2C:DB:AB:6E:AA:2D:1D:89:2D:04:A2:33:A1:B3:99:BF:FB:ED:68:55:2E:CE:29:64:38:3F:A1:0A:C4:AF:BB:3D:A8:71:05:82:E8:13:D9:55:22:4B:DD:A9:19:08:CD:7F:DB:E9:70:EF:1C:94:BB:76:E0:0F:B1:64:C6:24:F9:CE:C4:BB:3D:C8:9D:E9:CA:14:BF:02:A5:ED:4E:DB:C0:2C:7E:C2:A1:06:DC:F0:02:E2:58:96:7D:12:81:8F:2F:49:39:64:2C:A7:F3:3C:8A:EA:16:B4:F7:9F:DD:0E:2D:49:53:82:08:EE:12:84:40:DD:AD:E0:03:46:D7:87:AC:66:CC:A9:58:E0:6E:99:4B:F9:72:1F:C4:56:55:95:B3:DB:6E:A9:5B:71:27:9C:AE:4B:11:23:F2:2A:7C:40:8B:E2:20:F7:FC:13:2E:F3:AD:39:DC:96:29:E5:F9:66:A5:BD:6B:A0:95:52:5F:20:B4:3E:CB:1F:8F:51:62:02:D8:B5:2A:A0:42:BA:42:DF:02:4A:E1:A5:6A:A5:39:A1:BA:0F:EC:7C:E8:AB:FC:12:BA:DF:CF:DD:AE:C1:15:73:F9:6F:5C:66:CC:C0:09:75:46:8F:9B:46:EB:A6:0A:F2:BF:F8:F7:29:AD:87:A9:9E:6B:93:B0:75:3F:66:C4:59:7D:84:79:F6:D3:02:03:01:00:01
Basic Constraints *IsCA: true*
Certificate Policies *Policy OID: 2.16.724.1.4.2.2.1*
CPS pointer: <http://www.seg-social.es/ACGISS>
CPS text: [Certificado de la CA Subordinada GISS01 de ACGISSv2.Consulte las condiciones de uso en <http://www.seg-social.es/ACGISS>]
Authority Info Access *<http://ocsp.seg-social.gob.es/>*
http://www.seg-social.es/ACGISS/Certs/RAIZ_ACGISS_V2
CRL Distribution Points *<http://crl.seg-social.gob.es/ar1.crl>*
C=ES,L=MADRID,O=TESORERIA GENERAL DE LA SEGURIDAD SOCIAL,OU=GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL,SERIALNUMBER=Q2827003A,CN=RAIZ ACGISSv2,CN=CRL1
Authority Key Identifier *E3:78:D3:90:56:28:1E:D2:EF:2C:14:E4:62:5E:62:D3:47:3B:E6:4D*
Subject Key Identifier *8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A9:20:D6:61:E8:D9:0D:A3:07:AB:B1:1C:AC:5E:00:FF:93:02:26:AE:B0:FE:B6:A8:81:49:C6:55:95:5B:03:E1*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-10-26T01:00:00Z*

18.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

18.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:2.16.724.1.4.2.2.1.1.2*

Description

18.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified certificates issued by SUBCA GISS01*

Name [es] *Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities

X509SubjectName

Subject CN: *SUBCA GISS01*

Subject SERIAL NUMBER: *Q2827003A*

Subject OU: *GISS01*

Subject OU: *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

Subject O: *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-03T00:00:00Z*

18.2.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

18.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDAURN] urn:oid:2.16.724.1.4.2.2.1.1.2

Description**18.2.5 - History instance n.2 - Status: granted**

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified certificates issued by SUBCA GISS01

Name [es] Certificados reconocidos emitido por SUBCA GISS01

Service digital identities**X509SubjectName**

Subject CN: SUBCA GISS01

Subject SERIAL NUMBER: Q2827003A

Subject OU: GISS01

Subject OU: GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL

Subject O: TESORERIA GENERAL DE LA SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

X509SKI

X509 SK I jUrV/XKSPwcaEV/NgKrWGhp/9tM=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

18.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:2.16.724.1.4.2.2.1.1.2*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:2.16.724.1.4.2.2.1.1.1*

18.2.5.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

18.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by SUBCA GISS01*

Name [es] *Certificados reconocidos emitido por SUBCA GISS01*

Service digital identities**X509SubjectName**

Subject CN: *SUBCA GISS01*

Subject SERIAL NUMBER: *Q2827003A*

Subject OU: *GISS01*

Subject OU: *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

Subject O: *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time 2016-06-23T22:00:00Z

18.2.6.6 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.1.4.2.2.1.1.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.1.4.2.2.1.1.1

18.3 - Service (withdrawn): Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

Name [es] Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1466133214

Certificate Policies*Policy OID: 2.16.724.1.4.2.2.1.3.1**CPS pointer: <http://www.seg-social.es/ACGISS>**CPS text: [Certificado de sellado de tiempo. Consulte las condiciones de uso en <http://www.seg-social.es/ACGISS>]***Issuer Alternative Name***rfc822Name=acgiss.soporte.giss@seg-social.es***CRL Distribution Points***http://crl.seg-social.gob.es/ac_sub.crl***Authority Key Identifier***8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3***Subject Key Identifier***AA:26:8A:14:04:12:83:80:5A:6F:72:54:CE:53:AE:71:3B:1B:BC:5F***Basic Constraints***IsCA: false***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***EB:A2:BD:4B:A5:BD:CA:E7:73:A4:BA:EF:9E:59:74:83:AA:97:20:C2:5D:7C:AF:C7:4A:22:C4:DA:9A:76:02:09***X509SubjectName****Subject SERIAL NUMBER:***S2819001E+2.5.4.97***Subject OU:***SERVICIOS DE CONFIANZA***Subject O:***SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL***Subject C:***ES***X509SKI****X509 SK I***qiaKFAQSg4Bab3JUzIOucTsbvF8=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2021-10-26T01:00:00Z***Scheme Service Definition URI****URI**

[en]

*<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI**

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

18.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

Name *[es]* *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

Service digital identities**X509SubjectName**

Subject SERIAL NUMBER: *S2819001E+2.5.4.97*

Subject OU: *SERVICIOS DE CONFIANZA*

Subject O: *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

Subject C: *ES*

X509SKI

X509 SK I *qiaKFAQSg4Bab3JUzlOucTsbvF8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-03T00:00:00Z*

19 - TSP: Ministerio de Empleo y Seguridad Social

TSP Name

Name *[en]* *Ministerio de Empleo y Seguridad Social*

Name *[es]* *Ministerio de Empleo y Seguridad Social*

TSP Trade Name

Name *[en]* *Ministerio de Empleo y Seguridad Social*

Name *[es]* *Ministerio de Empleo y Seguridad Social*

Name *[en]* *Ministerio de Trabajo e Inmigracion*

Name *[es]* *Ministerio de Trabajo e Inmigracion*

Name *[en]* *VATES-S2819001E*

Name *[en]* *MINISTERIO DE TRABAJO E INMIGRACION*

Name *[en]* *MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

PostalAddress

Street Address *[en]* *Paseo de la Castellana, 63*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28071*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Paseo de la Castellana, 63*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28071*

Country Name *[es]* *ES*

ElectronicAddress

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	[en] <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es] <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[es]	Certificados Reconocidos emitidos por la AC1 RAIZ MTIN
Name	[en]	Qualified Certificates issued by AC1 RAIZ MTIN

Version:	3
Serial Number:	1304969050763335590
X509 Certificate	-----BEGIN CERTIFICATE-----

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: MADRID
Issuer O: MINISTERIO DE TRABAJO E INMIGRACION
Issuer OU: SUBDIRECCION GENERAL DE PROCESO DE DATOS
Issuer OU: PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
Issuer SERIAL NUMBER: S2819001E
Issuer CN: AC1 RAIZ MTIN
Subject C: ES
Subject L: MADRID
Subject O: MINISTERIO DE TRABAJO E INMIGRACION
Subject OU: SUBDIRECCION GENERAL DE PROCESO DE DATOS
Subject OU: PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
Subject SERIAL NUMBER: S2819001E
Subject CN: AC1 RAIZ MTIN
Valid from: Thu Nov 05 17:17:45 CET 2009
Valid to: Sun Nov 03 17:17:45 CET 2019
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DC:CD:CD:B1:8F:DE:25:F5:FF:1C:33:73:99:3C:1B:A1:6D:F5:A0:C4:7D:9B:3
8:66:8D:09:DF:03:6C:57:35:04:13:A1:FE:E3:5F:E6:22:04:58:18:09:4E:69:33:04:3F:95:C7:D9:4E:FF:33:34:A7:32:40:32:93:57:FE:81:AF:25:43:5C:10:FD:7B:57:0B:62:08:67:67:62:B4:E
3:E5:58:25:80:E6:AA:86:62:40:E7:4F:10:61:29:49:26:AB:4D:7C:A1:AB:5B:61:31:81:06:6A:64:94:4D:27:F8:4B:1E:D1:D5:43:E2:D7:B1:6D:F6:F6:FF:B4:70:55:F6:08:99:B7:74:01:E0:F3:9
E:B5:7C:E4:04:88:08:50:59:78:1F:1A:94:DB:EF:C8:C9:89:D3:37:B8:F3:3D:86:D1:19:C8:83:5A:10:07:08:4F:99:74:02:07:F0:32:51:C8:F8:E6:D0:3C:26:76:7D:72:7E:AC:76:37:C1:8A:75:
20:5C:40:DC:B4:3F:0D:49:7C:4D:67:AE:39:EF:E4:CE:80:E1:CA:9D:E6:2D:AB:E6:12:95:0A:F9:FB:DF:E3:E2:8C:3D:87:FB:45:6E:44:AB:F6:78:92:27:14:A1:5D:68:4F:70:7B:57:73:EF:F
9:5D:A8:0F:75:9F:EF:11:60:19:84:B0:64:40:EE:D8:A9:86:FA:A5:D7:45:F4:11:6F:F1:86:C8:34:5B:88:48:CE:BA:DD:CD:9B:DD:88:E3:01:36:E8:AC:6A:E8:12:0B:B0:E0:7B:90:1E:85:0B:49:
89:01:F6:FF:82:DF:58:65:22:83:48:D6:07:D0:1C:66:FC:66:28:3A:C4:C3:E5:F8:99:65:27:52:58:F3:6B:F1:6F:02:44:84:75:D0:A4:E3:68:53:61:72:EF:F6:2F:A9:B3:AC:F5:F4:F6:D0:5C:DC:
69:4C:CC:79:D2:A4:1B:C6:73:06:34:74:B4:F1:6A:CA:29:28:C7:34:84:5B:23:08:BA:00:8C:CC:09:C1:C7:6F:5D:04:AB:87:4F:26:77:A9:35:CF:2D:D6:B3:FF:31:69:D0:34:FB:25:EC:68:96:0
A:A2:DD:83:1F:CA:3C:8F:74:36:25:54:EF:F5:18:7B:C2:24:31:D1:FB:82:04:AE:04:82:D6:F5:02:29:71:E1:92:71:74:8E:DB:AA:71:1D:C4:3B:C6:62:26:6C:86:3C:23:55:EB:29:D1:1F:AB:CA:
1E:63:E7:B3:73:B4:A7:88:2A:3A:F6:1F:FB:87:65:88:FC:F3:9F:FE:BF:EB:D5:1D:B6:A8:03:E9:65:83:19:8C:E0:18:ED:17:D8:1C:0D:3D:9C:8A:58:7F:02:03:01:00:01

```

Basic Constraints *IsCA: true*
Subject Key Identifier 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83
Authority Info Access *http://ca.mtin.es/mtin/ocsp*
CRL Distribution Points *http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz*
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz
Certificate Policies *Policy OID: 1.3.6.1.4.1.27781.2.4.1*
CPS pointer: http://ca.mtin.es/mtin/DPCyPoliticass
CPS text: [Certificado raíz. Consulte las condiciones de uso en
http://ca.mtin.es/mtin/DPCyPoliticass]
Authority Key Identifier 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83

Version:	3
Serial Number:	5545899491963
X509 Certificate	-----BEGIN CERTIFICATE-----

Signature algorithm:	SHA1withRSA
Issuer C:	ES
Issuer L:	MADRID
Issuer O:	MINISTERIO DE TRABAJO E INMIGRACION
Issuer OU:	SUBDIRECCION GENERAL DE PROCESO DE DATOS
Issuer OU:	PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
Issuer SERIAL NUMBER:	S2819001E
Issuer CN:	AC1 RAIZ MTIN
Subject C:	ES
Subject L:	MADRID

Subject O: MINISTERIO DE TRABAJO E INMIGRACION
Subject OU: SUBDIRECCION GENERAL DE PROCESO DE DATOS
Subject OU: PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
Subject SERIAL NUMBER: S2819001E
Subject CN: AC1 RAZ MTIN
Valid from: Thu Nov 05 17:17:45 CET 2009
Valid to: Sun Nov 03 17:17:45 CET 2019
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DC:CD:CD:B1:8F:DE:25:F5:FF:1C:33:73:99:3C:1B:A1:6D:F5:A0:C4:7D:98:3
8:66:8D:09:DF:03:6C:57:95:B4:13:41:FE:E3:5F:E6:22:04:58:18:89:4E:69:33:04:3F:95:C7:D9:4E:FF:33:34:A7:32:40:32:93:57:FE:81:AF:25:43:5C:1D:F0:7B:57:08:62:08:67:62:84:E
3:E5:58:25:80:E6:AA:86:62:40:E7:4F:10:61:29:49:26:A8:4D:7C:A1:AB:5B:61:31:81:06:6A:64:94:4D:27:F8:48:1E:D1:D5:43:E2:D7:B1:6D:F6:F6:FF:B4:70:55:F6:08:99:B7:74:01:E0:F3:9
E:B5:7C:E4:04:88:08:50:59:78:1F:1A:94:DB:EF:C8:C9:89:D3:37:B8:F3:3D:86:D1:19:C8:83:5A:10:07:08:4F:99:74:02:07:F0:32:51:C8:F8:E6:D0:3C:26:76:7D:72:7E:AC:76:37:C1:8A:75:
20:5C:40:DC:84:3F:D0:49:7C:4D:67:AE:39:EF:E4:CE:80:E1:CA:9D:E6:2D:A8:2E:E6:12:95:DA:F9:FB:DF:E3:E2:8C:3D:87:FB:45:6E:44:A8:F6:78:92:27:14:A1:50:66:4F:70:78:57:73:EF:F
9:5D:A8:0F:75:9F:EF:11:60:19:84:80:64:40:EE:D8:A9:86:FA:A5:D7:45:F4:11:6F:F1:86:C8:34:58:88:48:CE:BA:DD:CD:9B:DD:88:E3:01:36:E8:AC:6A:E8:12:08:80:E0:7B:90:1E:85:0B:49:
89:01:F6:FF:82:DF:58:65:22:83:48:D6:07:D0:1C:66:FC:66:28:3A:C4:C3:E5:F8:99:65:27:52:58:F3:6B:F1:6F:02:44:84:75:D0:A4:E3:68:53:61:72:EF:F6:2F:A9:83:AC:F5:F4:F6:D0:5C:DC:
69:4C:CC:79:D2:A4:1B:C8:73:06:34:74:B4:F1:6A:CA:29:28:C7:34:84:5B:23:D8:8A:00:9C:09:C1:C7:6F:5D:04:A8:B7:4F:26:77:A9:35:CF:2D:D6:B3:FF:31:69:D0:34:F8:25:EC:68:96:0
A:A2:DD:83:1F:CA:3C:8F:74:36:25:54:EFF5:18:7B:C2:24:31:D1:FB:82:04:AE:04:82:D6:F5:02:29:71:E1:92:71:74:8E:DB:AA:71:1D:C4:38:C6:62:26:6C:86:3C:23:55:EB:29:D1:1F:AB:CA:
1E:63:E7:B3:73:B4:A7:B8:2A:3A:F6:1F:FB:87:65:88:FC:F3:9F:FE:BF:EB:D5:1D:B6:A8:03:E9:65:83:19:8C:E0:18:ED:17:D8:1C:0D:3D:9C:8A:58:7F:02:03:01:00:01

```

Authority Info Access <http://ca.mtin.es/mtin/ocsp>
Subject Alternative Name admin_ca@mtin.es
Issuer Alternative Name admin_ca@mtin.es
Basic Constraints *IsCA: true*
CRL Distribution Points
<http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz>
<http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz>
Certificate Policies
Policy OID: 1.3.6.1.4.1.27781.2.4.1
CPS pointer: <http://ca.mtin.es/mtin/DPCyPoliticass>
CPS text: [Certificado raíz. Consulte las condiciones de uso en <http://ca.mtin.es/mtin/DPCyPoliticass>]
Subject Key Identifier 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83
Authority Key Identifier 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: SHA-256
Thumbprint: 5B:1D:9D:24:DE:0A:FE:A8:B3:5B:A0:4A:1C:3E:25:D0:81:2C:DF:7C:46:25:DE:0A:89:AF:9F:E4:BB:D1:BB:15
X509SubjectName
Subject C: ES
Subject L: MADRID

Subject O: MINISTERIO DE TRABAJO E INMIGRACION

Subject OU: SUBDIRECCION GENERAL DE PROCESO DE DATOS

Subject OU: PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN

Subject SERIAL NUMBER: S2819001E

Subject CN: AC1 RAIZ MTIN

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2018-05-07T00:00:00Z

Scheme Service Definition URI

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

19.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3

19.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

19.1.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Reconocidos emitidos por la AC1 RAIZ MTIN*

Name [en] *Qualified Certificates issued by AC1 RAIZ MTIN*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject L: *MADRID*

Subject O: *MINISTERIO DE TRABAJO E INMIGRACION*

Subject OU: *SUBDIRECCION GENERAL DE PROCESO DE DATOS*

Subject OU: *PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*

Subject SERIAL NUMBER: *S2819001E*

Subject CN: *AC1 RAIZ MTIN*

X509SKI

X509 SK I *M0MYs8RLHcsf+fBO/N9K5BVgyIM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

19.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

19.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

19.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Reconocidos emitidos por la AC1 RAIZ MTIN

Name	[en]	Qualified Certificates issued by AC1 RAIZ MTIN

Service digital identities**X509SubjectName**

Subject C:	ES
Subject L:	MADRID
Subject O:	MINISTERIO DE TRABAJO E INMIGRACION
Subject OU:	SUBDIRECCION GENERAL DE PROCESO DE DATOS
Subject OU:	PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
Subject SERIAL NUMBER:	S2819001E
Subject CN:	AC1 RAIZ MTIN

X509SKI

X509 SK I	M0MYs8RLHcsf+fBO/N9K5BVgyIM=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time	2010-12-21T00:00:00Z

19.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3

19.2 - Service (withdrawn): SUBCA1 MEYSS

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] SUBCA1 MEYSS

Name [es] SUBCA1 MEYSS

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1480675521

Valid to:	<i>Tue Dec 02 12:56:29 CET 2036</i>
Public Key:	<i>30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:30:CF:7E:14:83:18:57:E9:FA:17:8D:36:A0:8F:D4:17:98:F6:E5:0E:A7:33:D4:72:8A:52:3F:C8:A6:E1:00:64:7F:FA:98:2A:61:39:63:5E:26:20:72:DC:7E:14:2C:7C:BD:EF:96:65:23:EE:EF:4F:05:18:02:59:F3:25:9B:D4:9F:31:18:43:ED:78:E7:FC:BC:43:90:F0:7A:10:57:B7:71:18:53:70:93:6D:C3:58:C6:22:68:2B:C4:79:E0:8E:04:63:C2:9E:96:3D:07:5A:1B:30:F0:5F:ED:FF:7A:19:CC:DC:2E:82:AC:33:D0:48:12:25:1F:6D:A3:25:D9:D6:BD:23:43:8B:8D:63:7D:8F:8D:DA:B7:26:FA:F6:51:CB:15:8B:4D:5E:C6:99:D8:98:FD:8C:05:21:AC:52:A6:B8:30:66:55:4A:61:76:90:7E:9C:3E:1A:A4:AF:D3:7B:4B:89:5C:CA:A0:A4:B4:70:98:B4:D5:CE:11:50:2F:62:60:7B:D8:F9:1E:0D:74:16:47:39:CE:89:75:27:DA:48:8F:59:C5:2C:5D:0B:E5:7C:CF:F4:6A:0B:1E:FC:2A:16:2A:00:71:00:38:18:0E:A5:80:7A:0E:BB:EE:81:E0:64:89:94:8D:03:7D:4A:81:C9:F6:B0:EF:4B:46:BF:05:3B:5D:99:8F:A1:65:FB:75:07:DC:48:9E:39:76:AA:46:01:15:0C:19:E9:23:72:EF:47:EE:6B:64:DF:AD:62:D8:7B:F0:33:C6:C8:2E:A3:69:FC:AC:8C:AF:7B:95:4C:B6:7A:F3:2F:16:94:73:B8:C1:1A:57:B3:DE:C8:66:D2:EF:AE:90:BC:D1:D5:39:DC:2A:4E:5C:F1:53:85:96:3F:86:81:57:1E:D2:7F:CB:95:4E:BE:7A:15:84:D1:A3:96:FC:A3:6C:FC:F4:37:A9:E3:86:6A:5A:D9:47:CE:BE:05:1D:8E:32:A1:4D:4E:A4:6D:DC:F4:9F:33:23:02:D4:F8:38:17:D4:78:31:AB:04:73:2C:E3:2F:15:82:A5:8E:A4:09:0D:DF:9D:A2:3E:10:3A:E9:5C:49:06:F4:98:DB:0E:5D:05:E3:75:0D:0F:51:93:D0:67:91:54:A3:0C:8F:1D:5C:BA:CF:66:4E:EC:CB:56:18:00:8B:9A:D9:C2:A1:2F:63:AB:49:CE:A8:FE:F6:48:F9:DF:6F:7B:1F:99:18:F9:2D:4D:76:B6:13:26:63:FA:D4:A3:7C:44:70:01:B2:F2:53:5A:22:7A:CE:EA:59:EB:97:70:01:A8:87:A3:51:CA:84:D1:DE:35:84:00:A7:B7:7A:B9:22:2F:4F:86:9F:03:0D:75:02:03:01:00:01</i>
Basic Constraints	<i>IsCA: true</i>
Authority Info Access	<i>http://ca.empleo.gob.es/meyss/ocsp http://ca.empleo.gob.es/meyss/certificados</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.27781.2.5.1.1 CPS pointer: http://ca.empleo.gob.es/meyss/DPCyPolíticas CPS text: [Certificado de AC Subordinada SUBCA1 MEYSS. Consulte las condiciones de uso en http://ca.empleo.gob.es/meyss/DPCyPolíticas]</i>
CRL Distribution Points	<i>http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1</i>
Authority Key Identifier	<i>7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71</i>
Subject Key Identifier	<i>9E:8B:1D:B3:FA:07:2B:81:D7:EA:59:E8:B9:69:F7:9D:B5:48:02:E2</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>24:E0:BA:DA:DA:29:05:5C:66:22:CA:23:74:A2:28:A4:71:A4:D2:4C:2D:54:71:88:E3:8F:07:1A:9D:14:60:88</i>
X509SubjectName	
Subject CN:	<i>SUBCA1 MEYSS</i>
Subject 2.5.4.97:	<i>VATES-S2819001E</i>
Subject SERIAL NUMBER:	<i>S2819001E</i>
Subject OU:	<i>PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS</i>
Subject OU:	<i>S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES</i>
Subject O:	<i>MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL</i>
Subject L:	<i>MADRID</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I *nosds/oHK4HX6lnouWn3nbVIAul=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-03-28T00:00:00Z*

19.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

19.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] SUBCA1 MEYSS*

Name *[es] SUBCA1 MEYSS*

Service digital identities

X509SubjectName

Subject CN: *SUBCA1 MEYSS*

Subject 2.5.4.97: *VATES-S2819001E*

Subject SERIAL NUMBER: *S2819001E*

Subject OU: *PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*

Subject OU: *S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*

Subject O: *MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *nosds/oHK4HX6lnouWn3nbVIAul=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-07T00:00:00Z*

19.2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

19.2.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *SUBCA1 MEYSS*

Name *[es]* *SUBCA1 MEYSS*

Service digital identities

X509SubjectName

Subject CN: *SUBCA1 MEYSS*

Subject 2.5.4.97: *VATES-S2819001E*

Subject SERIAL NUMBER: *S2819001E*

Subject OU: *PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*

Subject OU: S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Subject O: MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

X509SKI

X509 SK I nosds/oHK4HX6lnouWn3nbVIAul=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2017-04-11T00:00:00Z

19.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

19.3 - Service (withdrawn): SUBCA2 MEYSS

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	SUBCA2 MEYSS

Name	[es]	SUBCA2 MEYSS

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1480675522

Valid to:	Tue Dec 02 13:22:49 CET 2036
Public Key:	<pre> 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:26:65:6A:15:BD:46:DC:EE:AA:D0:1A:0C:EE:D9:21:20:DA:B6:28:18:9E:9 4:20:67:60:7D:5E:77:3E:CF:4E:8E:9B:28:2A:E1:70:41:2C:A7:7D:C2:C0:FA:A7:1A:51:81:64:5A:53:8B:0A:94:89:E4:C0:7C:36:CB:B8:F3:7B:01:1A:51:F4:F2:20:AF:E5:C7:E2:8B:08:12: EE:AE:7C:BB:07:1B:70:41:67:B5:F6:EB:DA:B5:27:74:94:46:50:48:C0:55:AC:43:AD:8E:24:62:8A:90:42:C5:06:D4:EF:53:17:32:0F:12:F6:66:95:94:42:41:E5:2C:44:9D:D1:75:47:01:FE:E1 :C6:09:73:1B:F0:D4:E5:2C:00:CD:AB:8C:5C:D2:D9:F1:06:51:15:62:33:A8:18:4E:65:D6:19:19:EC:E3:CB:2F:D5:F6:05:5B:39:90:C4:DC:0E:5F:04:8C:5C:86:DF:5B:3F:4A:C0:67:11:E3:D3: 06:90:0D:53:94:48:E6:95:CE:29:AC:FD:05:B3:10:F9:54:F7:41:DE:44:75:5A:C8:11:AC:5C:47:68:79:07:27:5C:40:4E:CD:0E:82:0F:97:12:2E:49:D7:9C:2A:02:9A:AE:25:1F:24:04:6E:52:A 7:17:C5:60:C8:8C:32:38:2E:91:69:82:74:AB:2E:40:BC:4E:76:15:09:50:94:A9:19:51:16:08:48:9A:94:2A:95:67:CD:F2:95:8D:28:D6:D3:CA:BA:DE:22:24:02:C0:5D:C3:B6:E2:16:82:6F:D5 :80:D7:56:BD:67:E9:1B:0D:A4:60:07:18:0E:36:06:21:52:29:45:A9:D0:7E:B2:20:8F:A7:48:BA:1C:F0:B9:55:B6:7F:18:95:89:5A:D5:8B:A2:36:E4:EC:F7:30:92:B9:27:48:5F:30:36:00:F3:A D:8E:1A:81:84:EA:E4:E8:99:58:05:9C:92:24:1B:39:0A:E8:8B:7B:1D:74:79:E4:82:1F:11:28:48:78:C8:77:A2:8A:83:66:F0:A9:23:D2:FF:20:9A:93:BC:F5:A3:D5:40:04:0A:30:2B:17:27:59: 99:19:F6:1E:6B:EA:0D:57:AD:17:F2:43:F0:50:17:D5:1E:28:05:8A:04:A9:4D:34:C4:9C:11:93:4F:5F:5F:24:76:B4:6A:C9:D8:AA:15:B1:EF:CB:B1:1D:25:EF:86:A1:BC:4D:E5:D9:FC:21:8 D:8B:DA:4C:58:68:30:85:48:76:A5:7D:9F:CA:72:D9:F3:81:D4:32:D6:07:E2:1D:17:9C:3E:10:E7:A6:20:C1:82:EA:62:A7:E2:93:4B:74:06:44:57:D1:14:E9:02:03:01:00:01 </pre>
Basic Constraints	IsCA: true
Authority Info Access	http://ca.empleo.gob.es/meyss/ocsp http://ca.empleo.gob.es/meyss/certificados
Certificate Policies	Policy OID: 1.3.6.1.4.1.27781.2.5.1.2 CPS pointer: http://ca.empleo.gob.es/meyss/DPCyPolíticas CPS text: [Certificado de AC Subordinada SUBCA2 MEYSS. Consulte las condiciones de uso en http://ca.empleo.gob.es/meyss/DPCyPolíticas]
CRL Distribution Points	http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1
Authority Key Identifier	7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71
Subject Key Identifier	72:2D:90:3D:45:86:98:6C:9D:E3:89:F6:E0:E4:3D:77:CC:FD:96:02
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	18:70:4F:60:CC:F3:59:4C:89:9A:DA:8B:E4:D4:D3:D3:7D:AA:8F:38:A5:FC:B0:61:F A:D8:D6:B1:A9:F5:6E:0B
X509SubjectName	
Subject CN:	SUBCA2 MEYSS
Subject 2.5.4.97:	VATES-S2819001E
Subject SERIAL NUMBER:	S2819001E
Subject OU:	PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS
Subject OU:	S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Subject O:	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Subject L:	MADRID
Subject C:	ES

X509SKI

X509 SKI *ci2QPUWGmGyd44n24OQ9d8z9lgl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-03-28T00:00:00Z*

19.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

19.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *SUBCA2 MEYSS*

Name *[es]* *SUBCA2 MEYSS*

Service digital identities

X509SubjectName

Subject CN: *SUBCA2 MEYSS*

Subject 2.5.4.97: *VATES-S2819001E*

Subject SERIAL NUMBER: *S2819001E*

Subject OU: *PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*

Subject OU: *S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*

Subject O: *MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *ci2QPUWGmGyd44n24OQ9d8z9lgl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-05-07T00:00:00Z*

19.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

19.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

19.3.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *SUBCA2 MEYSS*

Name *[es]* *SUBCA2 MEYSS*

Service digital identities

X509SubjectName

Subject CN: *SUBCA2 MEYSS*

Subject 2.5.4.97: *VATES-S2819001E*

Subject SERIAL NUMBER: *S2819001E*

Subject OU: *PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS*

Subject OU: *S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES*

Subject O: *MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *ci2QPUWGmGyd44n24OQ9d8z9Igl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-04-11T00:00:00Z*

19.3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

20 - TSP: Consejo General de Colegios Oficiales de Médicos

TSP Name

Name	[en]	Consejo General de Colegios Oficiales de Médicos
Name	[es]	Consejo General de Colegios Oficiales de Médicos de España (CGCOM)

TSP Trade Name

Name	[en]	Entidad de Certificación de la Organización Médica Colegial (EC-OMC)
Name	[es]	Entidad de Certificación de la Organización Médica Colegial (EC-OMC)
Name	[en]	Organizacion Medica Colegial
Name	[es]	Organizacion Medica Colegial
Name	[en]	VATES-Q2866017C
Name	[en]	ORGANIZACION MEDICA COLEGIAL
Name	[en]	CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

PostalAddress

Street Address	[es]	Plaza de las Cortes, 11
Locality	[es]	Madrid
State Or Province	[es]	Madrid
Postal Code	[es]	28014
Country Name	[es]	ES

PostalAddress

Street Address	[en]	Plaza de las Cortes, 11
Locality	[en]	Madrid
State Or Province	[en]	Madrid
Postal Code	[en]	28014
Country Name	[en]	ES

ElectronicAddress

Issuer O: *VeriSign, Inc.*
Issuer C: *US*
Subject CN: *OMC*
Subject OU: *Class 2 Managed PKI Individual Subscriber CA*
Subject OU: *Entidad de Certificacion*
Subject OU: *VeriSign Trust Network*
Subject O: *Organizacion Medica Colegial*
Subject C: *ES*
Valid from: *Fri Jan 26 01:00:00 CET 2007*
Valid to: *Thu Jan 26 00:59:59 CET 2017*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:7C:2B:1A:62:69:49:19:FE:FE:76:21:D5:D6:3E:38:03:76:96:DF:EE:F0:BF:C5:14:80:7F:14:F7:58:21:48:1A:6F:32:39:24:6C:DC:F7:89:06:A0:49:41:A7:57:A0:1C:E2:D0:C3:6E:46:90:63:82:D7:0B:68:18:58:82:74:24:C6:25:71:28:67:F1:5F:30:72:78:70:03:C5:10:89:A4:DF:28:D3:9D:DE:35:FE:18:61:B2:68:4F:33:28:48:A5:A7:97:18:F4:27:80:BF:42:22:2A:39:62:85:AA:2A:1F:18:CD:2E:09:87:EC:F7:BF:48:56:15:25:80:E1:6B:7D:C5:57:03:7B:4B:26:79:68:E4:D1:34:9F:96:AE:DA:1C:C9:86:39:D8:D1:09:CE:E9:FA:D8:3E:03:DB:3E:78:6C:CE:02:5F:12:38:74:14:AF:C1:27:7C:A8:18:08:75:7E:36:75:4E:73:73:99:34:FC:44:7D:18:23:E2:99:DE:19:50:0D:80:82:92:1B:55:14:E5:A5:20:DC:98:FB:C4:F8:35:83:43:54:EE:65:48:4D:5F:7A:78:50:77:0E:6F:BF:89:61:18:45:D0:71:A2:4F:4A:08:24:7F:F5:6E:92:BF:B1:9C:48:E0:21:A2:AA:74:26:83:40:08:0D:BA:AF:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Certificate Policies *Policy OID: 2.16.840.1.113733.1.7.23.2*
CPS pointer: https://www.verisign.com/rpa
CRL Distribution Points *http://crl.verisign.com/pca2-g2.crl*
Subject Alternative Name *CN=PrivateLabel4-2048-4*
Subject Key Identifier *D3:58:FC:F2:2F:B6:F5:BC:D0:DC:27:19:3E:AA:3C:69:29:88:99:76*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *A4:8A:6D:DD:5D:D5:5C:AF:68:CC:AA:E0:A5:98:97:9C:AE:35:BF:D3:AC:6E:20:B5:11:FA:A7:87:4F:BF:B6:92*

Certificate fields details

Version: *3*
Serial Number: *35019734869110279053858484427741191449*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:15:6A:E6:9A:C3:76:29:C4:4B:A2:66:57:AE:ED:3B:7D:FE:E9:5F:F3:61:51:6D:97:55:A9:55:6B:CE:4F:52*

X509SubjectName

Subject CN: *OMC*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Entidad de Certificacion*

Subject OU: *VeriSign Trust Network*

Subject O: *Organizacion Medica Colegial*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2018-07-16T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

20.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***20.1.3 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name***[en]**Qualified Certificates issued by AC EC-OMC***Name***[es]**Certificados Reconocidos emitidos por AC EC-OMC***Service digital identities****X509SubjectName****Subject CN:***OMC***Subject OU:***Class 2 Managed PKI Individual Subscriber CA***Subject OU:***Entidad de Certificacion***Subject OU:***VeriSign Trust Network***Subject O:***Organizacion Medica Colegial***Subject C:***ES***X509SKI****X509 SK I***01j88i+29bzQ3CcZPqo8aSmImXY=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2016-06-30T22:00:00Z***20.1.3.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description***[en]**undefined.**[es]**undefined.***Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.1.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC EC-OMC*

Name [es] *Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities

X509SubjectName

Subject CN: *OMC*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Entidad de Certificacion*

Subject OU: *VeriSign Trust Network*

Subject O: *Organizacion Medica Colegial*

Subject C: *ES*

X509SKI

X509 SK I *01j88i+29bzQ3CcZPqo8aSmlmXY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2016-03-31T22:00:00Z*

20.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDAURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDAURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.5*

20.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC EC-OMC*

Name *[es]* *Certificados Reconocidos emitidos por AC EC-OMC*

Service digital identities**X509SubjectName**

Subject CN: *OMC*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Entidad de Certificacion*

Subject OU: *VeriSign Trust Network*

Subject O: *Organizacion Medica Colegial*

Subject C: *ES*

X509SKI

X509 SK I *01j88i+29bzQ3CcZPqo8aSmImXY=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2011-01-27T00:00:00Z

20.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.5

20.2 - Service (withdrawn): Qualified Certificates issued by AC OMC (new CA)

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by AC OMC (new CA)*

Name [es] *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 484251359877222014

Extended Key Usage	<i>id_kp_clientAuth - id_kp_OCSPSigning</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://policy.camerfirma.com</i>
CRL Distribution Points	<i>http://crl.camerfirma.com/ac_camerfirma-2009.crl</i> <i>http://crl1.camerfirma.com/ac_camerfirma-2009.crl</i>
Subject Alternative Name	<i>certificacion@cgcom.es</i> <i>CN=CONSEJO GENERAL DE COLEGIOS DE MÃDICOS DE ESPAÑA, SERIALNUMBER=Q2866017C, STREET=PLAZA DE LAS CORTES 11, OID.2.5.4.17=28014, L=MADRID, ST=MADRID, C=ES</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>C1:76:11:DB:7B:31:13:61:E2:0D:7B:82:31:AA:DF:47:8B:CB:7F:FA:0B:E5:85:C0:6D:E2:30:92:23:C2:EF:8A</i>

X509SubjectName

Subject CN:	<i>OMC</i>
Subject OU:	<i>ENTIDAD DE CERTIFICACION</i>
Subject O:	<i>ORGANIZACION MEDICA COLEGIAL</i>
Subject C:	<i>ES</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time *2021-01-26T01:00:00Z*

Scheme Service Definition URI

URI [en]	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
URI [es]	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>

20.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by AC OMC (new CA)*

Name [es] *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities**X509SubjectName**

Subject CN: *OMC*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject O: *ORGANIZACION MEDICA COLEGIAL*

Subject C: *ES*

X509SKI

X509 SK I *52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-07-16T00:00:00Z*

20.2.4.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.2.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Certificates issued by AC OMC (new CA)*

Name [es] *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities

X509SubjectName

Subject CN: *OMC*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject O: *ORGANIZACION MEDICA COLEGIAL*

Subject C: *ES*

X509SKI

X509 SK I *52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

20.2.5.4 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.26852.1.1.5*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

20.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.2.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by AC OMC (new CA)*

Name *[es]* *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

Service digital identities**X509SubjectName**

Subject CN: *OMC*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject O: *ORGANIZACION MEDICA COLEGIAL*

Subject C: *ES*

X509SKI

X509 SK I *52QVZL6nNb73Ok7PLT4HC7dePys=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-03-31T22:00:00Z*

20.2.6.6 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.3*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.26852.1.1.5*

Issuer C: ES
Subject CN: CGCOM QUALIFIED 2020
Subject O: CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
Subject OU: ENTIDAD DE CERTIFICACION
Subject 2.5.4.97: VATES-Q2866017C
Subject L: MADRID
Subject ST: MADRID
Subject C: ES
Valid from: Mon Mar 02 11:41:18 CET 2020
Valid to: Wed Mar 02 11:41:18 CET 2033
Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A4:EE:FB:A9:0A:E7:0B:51:CD:12:AD:4B:4A:EB:10:43:2C:E1:37:F4:F9:3D:33:
2B:67:9E:7B:BF:03:66:01:82:BA:31:87:4F:03:DE:4A:AF:E7:4B:7E:F1:20:13:27:72:88:DB:83:AB:83:18:09:04:C2:C5:A7:3C:07:AD:76:3B:66:0B:99:7B:80:10:27:80:9A:CC:ES:EA:30:02:F
D:93:29:86:41:12:62:65:42:FA:06:60:AA:BA:13:77:4B:04:2B:CD:AF:2F:C6:52:94:09:F3:70:B3:2A:85:F0:C2:28:BB:93:68:5D:15:84:44:FB:9F:98:70:EB:86:1D:24:7C:B6:84:72:72:1E:59:
9D:D6:80:26:59:68:0C:01:5A:AF:09:C3:D1:B7:88:77:21:51:FA:72:D0:C3:42:8B:20:18:05:48:12:E0:3D:AF:A9:C7:C4:2F:B6:97:9C:EA:01:CD:56:26:2E:21:0F:D5:CB:09:88:97:EC:84:4F:5
0:FE:3E:DB:02:E0:E6:30:B5:74:9F:BB:6A:6F:70:FB:FE:00:92:ES:02:23:EC:BC:D9:06:7D:14:D3:DE:65:5F:27:2B:3B:2E:11:CF:2D:C0:15:EB:AA:0C:44:ED:F0:D7:F6:C5:BA:FB:33:AE:EC:83
:ED:44:D2:17:80:34:16:F4:01:DE:6D:0A:AF:0C:0B:08:86:98:5E:30:D0:DB:9C:8E:92:63:28:A5:00:1F:B1:3B:D4:55:4D:AE:DF:39:FB:84:A4:FB:E7:78:0E:F0:87:C7:8E:6F:CD:6E:CD:42:9B:
7E:7D:B3:4F:24:BB:6E:9E:67:86:AB:EB:21:CC:BF:D7:62:5B:C1:7B:2B:D0:67:80:D1:4B:1B:A6:22:52:75:D4:58:F6:63:1F:4F:FE:C7:40:6C:62:4D:8E:31:A9:3A:8B:EB:A7:CE:34:31:5C:CA:8
E:CF:06:98:A6:25:5D:2B:21:A3:3E:01:85:E4:5F:3D:F1:8F:E9:4E:00:4E:3C:59:5E:5C:70:66:85:2A:25:5E:A6:C5:E3:50:C5:08:D7:78:26:CC:18:F1:53:02:45:8F:2B:66:86:F1:6D:7E:15:23:9
2:97:86:F9:3F:32:37:0E:B9:2B:1B:72:16:46:A6:DA:65:48:4D:19:1F:4E:CF:AF:D4:A7:6A:93:06:EA:D5:63:59:03:F9:12:79:0C:C9:2F:1F:DD:3A:9E:B6:58:48:F3:C9:91:F0:99:29:FF:40:4
9:74:3C:67:27:65:6C:62:9A:8F:A8:70:32:ED:32:E0:2A:15:CA:3C:BC:CA:34:01:8B:E6:15:59:A7:BF:DC:35:26:2D:BF:6D:12:8B:D0:8D:B4:C4:0A:10:CF:02:03:01:00:01

Authority Key Identifier D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0
Subject Key Identifier 32:41:64:94:D4:2D:41:3A:CD:EB:2B:72:09:EB:AB:8D:88:3A:D1:CF
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://policy.vincasign.net>
CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]
Subject Alternative Name info@vincasign.net
CRL Distribution Points
<http://crl3.vincasign.net/casub.crl>
<http://crl4.vincasign.net/casub.crl>
Authority Info Access <http://www.vincasign.net/publickeys/caqualified.cer>
Basic Constraints IsCA: true - Path length: 1
Key Usage: keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 6E:8A:B9:A7:28:5D:70:EF:22:FC:7D:23:75:83:8D:65:3B:64:87:48:81:7A:80:63:4B:0C:1A:F1:04:3C:D3:66
X509SubjectName

Subject CN: CGCOM QUALIFIED 2020

Subject O: CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Subject OU: ENTIDAD DE CERTIFICACION

Subject 2.5.4.97: VATES-Q2866017C

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I MkFkINQtQTrN6ytyCeurjYg60c8=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2025-02-05T00:00:00Z

20.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

20.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

20.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.26852.1.1.1.4

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.6*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.12*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.26852.1.1.10.2*

Description**20.3.4 - History instance n.1 - Status: granted**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CGCOM QUALIFIED 2020*

Name [es] *Certificados cualificados emitidos por CGCOM QUALIFIED 2020*

Service digital identities**X509SubjectName**

Subject CN: *CGCOM QUALIFIED 2020*

Subject O: *CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject 2.5.4.97: *VATES-Q2866017C*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *MkFkINQtQTrN6ytyCeurjYg60c8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-09-07T01:00:00Z*

20.3.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

20.3.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

20.3.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.26852.1.1.1.4

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.26852.1.1.6

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.26852.1.1.12

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.26852.1.1.10.2

Description**20.4 - Service (withdrawn): Certificados cualificados emitidos por CGCOM QUALIFIED 2023**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Subject CN: *CGCOM QUALIFIED 2023*

Valid from: *Wed May 24 12:25:19 CEST 2023*

Valid to: *Sat May 21 12:25:18 CEST 2023*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:88:3C:FC:58:C5:1C:1C:8E:6E:43:88:9F:5D:34:EA:1A:25:49:36:7F:F9:58:30:71:EE:F2:78:C3:89:40:09:A6:8B:7C:81:F8:B1:72:7F:F2:EE:F8:B7:02:36:AE:D9:A2:C2:EC:12:F5:D1:D9:E1:FF:86:33:A9:E0:83:FC:A2:60:4F:88:6F:7C:42:A1:A9:75:38:86:7A:5D:C9:27:A8:3B:DF:AD:1A:DD:C6:D0:7B:91:45:46:88:2D:BE:E2:0C:71:5E:DD:92:4D:AF:7A:41:BA:16:C2:4F:30:C9:51:3D:5B:D8:02:74:AE:46:2A:39:67:02:C3:0C:B0:8C:DF:FD:FC:56:DD:80:11:B6:7F:6C:86:B7:47:12:33:00:46:A2:E8:D1:80:66:34:EE:5F:50:E9:55:45:1D:81:98:6E:D1:80:E4:F1:15:EA:E5:66:45:4C:39:84:58:D3:68:D5:78:47:B1:7B:56:64:5A:8C:C6:60:77:52:DD:0E:82:91:70:D4:67:AC:D1:F7:EF:90:28:AB:AB:94:D4:28:FA:A9:86:57:F3:A1:58:56:FC:67:93:32:63:D6:4B:D3:ED:3A:3E:62:15:75:48:C7:03:E7:FD:24:57:78:66:01:10:99:88:F7:D4:87:E6:81:A4:A3:0F:05:E2:25:E3:25:69:42:20:B4:23:8C:10:E8:F3:8E:6F:44:5B:E2:CA:77:C0:8D:0B:A5:8B:FA:E2:42:68:34:A8:02:68:05:A9:6E:BA:0A:3D:BB:A9:3B:4B:98:5A:79:ED:AB:BF:BC:AC:11:E5:69:FC:EC:A4:39:DE:F9:D7:74:34:DF:E8:F3:D3:62:48:C9:E2:1F:FB:CC:74:30:57:F2:EE:A3:A9:28:4C:AD:60:68:DC:4D:5D:E3:65:83:8E:0D:93:19:29:B7:34:18:97:C5:23:68:71:77:39:0A:11:C2:59:81:9A:F0:70:67:DF:8B:AD:B4:19:EE:A2:1A:F9:E3:AA:1C:68:A6:7F:DF:15:58:F3:7A:FE:16:16:2F:7C:2D:3A:71:E8:95:73:DC:25:DC:30:1A:A5:C9:54:BC:27:8E:C6:44:81:71:AB:91:2B:F8:E6:FA:3E:CC:5F:DA:73:D2:2E:8A:F5:31:CC:SD:A1:10:6F:2B:45:C9:60:48:D4:CC:3D:2B:12:0B:4F:A8:D9:79:E7:F2:09:11:C8:F8:66:F0:D2:94:13:A9:F2:77:4F:BC:82:E3:F4:D2:A9:90:76:EA:C9:34:37:07:82:5D:4A:EE:8B:8F:33:FD:FE:C0:2E:E7:F2:39:D0:6A:AA:30:21:8E:1A:40:5C:94:DE:06:61:51:24:0D:87:D8:9E:7C:66:8B:6F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 1*

Authority Key Identifier *FB:70:16:61:37:9E:DB:E7:32:97:40:3B:44:76:A2:7C:14:E3:B1:24*

Authority Info Access *http://www.vincasign.net/publickeys/cavintegris.cer*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.vincasign.net

CRL Distribution Points
http://crl1.vincasign.net/cavintegris.crl
http://crl2.vincasign.net/cavintegris.crl

Subject Key Identifier *34:44:02:DE:15:70:B6:FF:4D:FA:47:E3:5A:8D:9B:60:51:80:FC:AB*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *87:03:3F:EE:AB:43:12:15:50:5C:DD:79:AE:AF:56:93:36:7D:8B:84:CF:85:34:00:35:A6:A8:B6:92:62:8A:C9*

X509SubjectName

Subject C: *ES*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject O: *CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*

Subject 2.5.4.97: *VATES-Q2866017C*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject CN: *CGCOM QUALIFIED 2023*

X509SKI

X509 SK I *NEQC3hVwtv9N+kfjWo2bYFGA/Ks=*

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2025-02-05T00:00:00Z

20.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

20.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

20.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] <urn:oid:1.3.6.1.4.1.26852.1.1.1.4>

Policy Identifier:

Identifier [OIDA sURN] <urn:oid:1.3.6.1.4.1.26852.1.1.6>

Policy Identifier:

Identifier [OIDA sURN] <urn:oid:1.3.6.1.4.1.26852.1.1.12>

Policy Identifier:

Identifier [OIDA sURN] <urn:oid:1.3.6.1.4.1.26852.1.1.10.2>

Description**20.4.4 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados cualificados emitidos por CGCOM QUALIFIED 2023*

Name [en] *Qualified Certificates issued by CGCOM QUALIFIED 2023*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *MADRID*

Subject L: *MADRID*

Subject O: *CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS*

Subject 2.5.4.97: *VATES-Q2866017C*

Subject OU: *ENTIDAD DE CERTIFICACION*

Subject CN: *CGCOM QUALIFIED 2023*

X509SKI

X509 SK I *NEQC3hVwtv9N+kfjWo2bYFGA/Ks=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-12-11T01:00:00Z*

20.4.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

20.4.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

20.4.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.1.4

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.12

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.26852.1.1.10.2

Description

21 - TSP: BANCO DE ESPAÑA

TSP Name

Name [en] BANCO DE ESPAÑA

Name [es] BANCO DE ESPAÑA

TSP Trade Name

Name [en] BANCO DE ESPAÑA

Name [es] BANCO DE ESPAÑA

Name [en] EUROPEAN SYSTEM OF CENTRAL BANKS

Name [es] EUROPEAN SYSTEM OF CENTRAL BANKS

Name [en] VATES-V28000024

PostalAddress

Street Address [en] C/Alcalá, 48

Locality [en] Madrid

State Or Province [en] Madrid

Postal Code [en] 28014

Country Name [en] ES

PostalAddress

Street Address [es] C/Alcalá, 48

Locality [es] Madrid

State Or Province [es] Madrid

Postal Code [es] 28014

Country Name [es] ES

ElectronicAddress

URI [en] http://www.bde.es

URI [en] mailto:escb-pki@pki.escb.eu

URI	[en]	http://pki.bde.es

URI	[es]	http://pki.bde.es

URI	[en]	http://pki.escb.eu

URI	[es]	http://pki.escb.eu

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name [es] *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

Name	[en]	Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA

Certificate fields details

Version: 3

Serial Number: 72330364548887177642751079379801700075

X509 Certificate

[illegible]

Signature algorithm: *SHA1withRSA*

Issuer CN: *BANCO DE ESPAÑA-AC RAIZ*

Issuer O: *BANCO DE ESPAÑA*

Issuer C: *ES*

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

Valid from: *Thu Jul 29 09:03:28 CEST 2004*

Valid to: *Mon Jul 29 09:03:28 CEST 2019*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8B:BC:9B:01:0D:BD:80:34:D2:17:22:53:4E:4C:A3:0E:7D:0C:F9:0F:AF:54:40
:E5:21:92:C1:7E:6D:01:35:05:7C:F5:6D:12:A3:47:26:59:BA:C7:75:85:DA:DD:69:6C:F9:F9:30:23:FC:6E:23:F0:94:75:1C:82:F2:58:AB:1D:F0:BE:28:B3:F7:92:26:F8:1E:13:FD:15:09:A4:F6
:A6:E1:98:32:7E:9E:C3:99:68:56:8B:D0:A0:C0:FD:72:9A:A0:D7:4D:2D:0E:3B:16:08:44:A1:41:64:2C:FA:95:BF:43:91:62:7E:61:A0:0C:54:EB:42:76:D1:4B:E5:05:CE:D9:B7:6C:47:E4:29:0
D:79:AE:FF:4E:E1:C3:29:87:48:5F:D9:2C:EB:B7:C8:12:7A:6D:88:4A:70:F0:F3:EB:92:27:FF:85:8C:46:1C:3F:87:D1:C0:87:42:B2:FD:5A:63:F3:EB:ED:B5:58:C1:20:5E:A3:59:C8:F3:A7:6C:
7B:6B:32:C1:82:6A:49:AF:3D:C1:6A:5F:AA:29:10:1A:46:21:11:0A:B2:AB:6A:92:1F:A0:D7:96:74:35:0E:69:4A:AE:16:22:1D:B5:6C:B2:07:76:A7:4D:07:E2:1C:6E:E5:23:87:7E:1A:EA:04:8
2:8D:BE:D9:3E:91:1D:B7:80:F1:57:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *C2:45:2B:F4:F9:92:EE:33:59:98:E1:82:75:6B:8C:BC:D0:B6:E5:C1*

Authority Key Identifier *57:5E:6F:71:9E:36:73:9C:56:1C:3A:D5:08:F8:F2:2E:3D:08:64:EC*

Certificate Policies *Policy OID: 1.3.6.1.4.1.19484.2.2.1*
CPS pointer: <http://pki.bde.es/politicas>
*CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España.
@2004 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]*

Authority Info Access *<http://pkiva.bde.es>*

CRL Distribution Points *ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=SNTPKI01,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*
ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=Internas,CN=PKI,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint
<http://pki.bde.es/crls/ACraiz.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FF:2C:7C:52:66:D4:84:DB:63:87:C9:9A:0F:EB:F0:60:38:91:76:C4:9D:27:28:79:44:85:85:F1:9F:EC:13:0F*

X509SubjectName

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA*

Subject O: *BANCO DE ESPAÑA*

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2017-07-01T22:00:00Z

21.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

21.1.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

Name [en] *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

Service digital identities

X509SubjectName

Subject CN: BANCO DE ESPAÑA-AC CORPORATIVA

Subject O: BANCO DE ESPAÑA

Subject C: ES

X509SKI

X509 SK I *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

21.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**21.1.3 - History instance n.2 - Status: supervisionincessation****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [es] *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA***Name** [en] *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA***Service digital identities****X509SubjectName****Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA***Subject O:** *BANCO DE ESPAÑA***Subject C:** *ES***X509SKI****X509 SK I** *wkUr9PmS7jNZmOGCdWuMvNC25cE=***Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>**Status Starting Time** *2015-11-01T00:00:00Z***21.1.4 - History instance n.3 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [es] *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA***Name** [en] *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA***Service digital identities****X509SubjectName****Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA***Subject O:** *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</i>

Status Starting Time	2011-09-26T00:00:00Z

21.2 - Service (withdrawn): Qualified Certificates issued by ESCB-PKI ONLINE CA

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by ESCB-PKI ONLINE CA

Name	[es]	ESCB-PKI ONLINE CA

Service digital identities

Certificate fields details

Version: 3

Serial Number: 58589260405155732905307225959413577116

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: ESCB-PKI ROOT CA

Issuer O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Issuer C:	<i>EU</i>
Subject CN:	<i>ESCB-PKI ONLINE CA</i>
Subject O:	<i>EUROPEAN SYSTEM OF CENTRAL BANKS</i>
Subject C:	<i>EU</i>
Valid from:	<i>Fri Jul 22 12:46:35 CEST 2011</i>
Valid to:	<i>Wed Jul 22 12:46:35 CEST 2026</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:6F:CB:86:42:B3:41:27:CE:25:DA:85:A6:19:E6:03:F9:A3:DF:3B:B2:F1:E6: 7C:2E:FA:F8:56:09:8F:1D:5D:29:4A:2B:D6:68:20:98:D0:A2:08:5D:D8:49:4C:5E:EC:F6:92:6F:18:87:1A:41:32:5E:18:80:F8:8A:7B:A9:CF:07:3F:8A:5B:2A:F7:81:97:73:84:06:4B:C6:8C: C5:CD:5E:57:E4:EF:95:8C:6A:94:E1:76:D1:A4:3C:12:3B:5E:92:3C:6E:E5:65:AD:DC:8F:38:C1:0D:E7:53:D1:BE:22:6A:BF:8B:E3:E9:AC:2F:E8:28:94:1B:24:97:4F:EF:14:78:9C:A7:39:0F:C 3:98:B7:26:27:C3:5E:55:A3:C2:99:49:F3:01:37:36:58:8B:58:1A:32:F7:B1:28:6E:C4:AC:C6:40:DC:27:5C:5C:06:61:21:AC:9A:91:F6:F5:CD:C4:F1:47:27:E1:DC:6C:D7:98:81:11:CB:78:25: F6:27:5B:A4:C7:58:CA:0A:7D:70:D8:47:88:C4:54:C6:93:10:01:F5:18:E2:52:99:83:04:7E:60:DC:2F:12:EC:DE:4F:19:96:7C:13:C1:01:89:8F:80:42:F7:CE:4B:2A:CC:E7:51:18:8B:42:53:F9: 5F:A6:15:31:A7:7D:FB:6F:D4:64:8D:11:88:D4:E2:BA:0F:5C:5A:25:A3:36:F2:08:E7:10:79:F5:7A:C1:4A:D1:05:6F:85:FD:89:98:A0:0B:68:4E:60:3F:1B:45:EF:13:3D:D8:4F:6E:11:EA:B0:D E:8A:97:0A:E9:0A:98:7D:F2:DF:51:86:68:2E:52:84:FA:45:28:38:E8:76:19:98:E6:AA:06:A7:F6:1E:B1:03:BE:4A:BB:93:BA:69:E7:D7:66:70:FA:CE:F2:49:09:4B:B9:83:D4:6D:01:FC:85:90: EB:63:AA:A4:BE:80:48:80:96:F9:49:8A:12:2C:54:71:13:95:FE:A3:C5:7A:66:F7:40:A7:B1:74:1C:7A:F1:AC:57:7B:1B:94:A1:D8:69:8C:6E:4F:4A:59:1E:07:DE:67:5E:88:91:95:ED:D4:E9:4A: 5E:4D:EB:78:C2:27:CC:9B:64:44:75:1D:78:31:0F:D2:7C:CB:95:07:43:0E:9E:C8:8E:49:69:32:FF:14:9C:71:51:73:E6:0D:88:AD:18:BE:11:74:B1:67:C9:68:DF:60:35:1E:D5:B1:C5:1F:26: 8B:6B:FD:2E:CA:1D:B1:FE:B4:3E:AF:9B:A7:DA:DD:E5:F5:9E:A6:A6:DB:10:0D:41:56:CE:D5:0D:F1:40:E6:92:4F:44:6A:44:03:02:17:64:BB:DC:6F:B9:02:03:01:00:01 </pre>
Basic Constraints	<i>IsCA: true</i>
Subject Key Identifier	<i>E4:59:DE:44:24:B6:A4:3C:83:43:37:28:B0:C8:A4:AE:26:2D:3D:03</i>
Authority Key Identifier	<i>D5:85:1D:69:63:97:28:C9:59:E6:D1:67:07:CD:54:BC:DC:02:7E:EA</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://pki.escb.eu/policies</i>
Authority Info Access	<i>http://pki.escb.eu/certs/rootCA.crt</i>
CRL Distribution Points	<i>http://pki.escb.eu/crls/rootCA.crl</i> <i>ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20Root%20CA,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint</i> <i>http://iam-crl.escb.eu/escb/rootCA.crl</i> <i>http://escbpki/crls/rootCA.crl</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>4B:18:76:44:BF:79:4F:83:D0:00:99:9D:79:27:43:3F:75:F3:CF:B1:64:3A:6D:0F:8A:25:94:35:BE:86:1B:7A</i>
Certificate fields details	
Version:	<i>3</i>
Serial Number:	<i>135646708379632619634537957133020884269</i>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *13:35:26:DC:99:E9:CC:36:62:F8:F5:FA:20:06:30:05:BA:90:E6:63:2B:F3:4F:18:A8:4B:A3:9B:5F:AA:57:00*

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2017-07-01T22:00:00Z*

21.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

Name *[es]* *ESCB-PKI ONLINE CA*

Service digital identities

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

X509SKI

X509 SK I *5FneRCS2pDyDQzcosMikriYtPQM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

21.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.2.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

Name *[es]* *ESCB-PKI ONLINE CA*

Service digital identities

X509SubjectName

Subject CN: *ESCB-PKI ONLINE CA*

Subject O: *EUROPEAN SYSTEM OF CENTRAL BANKS*

Subject C: *EU*

X509SKI

X509 SK I *5FneRCS2pDyDQzcosMikriYtPQM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-02-24T23:00:00Z*

21.3 - Service (withdrawn): Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name

[en]

Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Name

[es]

Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Service digital identities

Certificate fields details

Version:

3

Serial Number:

33025408625715663557967398552839070848

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

BANCO DE ESPAÑA-AC RAIZ V2

Issuer O:

BANCO DE ESPAÑA

Issuer C:

ES

Subject CN:

BANCO DE ESPAÑA-AC CORPORATIVA V2

Subject O:

BANCO DE ESPAÑA

Subject C:

ES

Valid from:

Mon May 04 18:00:00 CEST 2015

Valid to:

Sat May 04 18:00:00 CEST 2030

Public Key:

30:82:02.22.00.06:29.A4:66:48:26:56:F7:0D:01:05:00:03:82:02.0f.00:30:82:02.04.0A:82:02.01.01.06:74:28:3F:1E:D3:9C:AB:88:39:3B:DF:C7:E1:00:10:78:39:64:85:EC:42:47:AC:C3:6E:11:26:76:18:1B:31:AD:03:03:3C:CB:FE:AF:4D:2C:97:88:72:00:64:77:B4:3F:34:71:F7:B2:64:25:5B:08:15:8D:32:86:FD:A0:81:64:62:54:5:5:FF:2B:B8:04:62:AD:4B:D9:78:78:43:43:02:68:66:AB:AD:67:3E:1D:60:64:67:20:67:89:A5:AE:D5:55:93:EB:96:93:45:45:D8:81:72:75:48:AF:FF:0C:C8:74:21:70:2D:D1:46:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42:95:35:35:7F:2E:4C:0A:60:93:34:56:3C:6D:04:3C:5C:CB:F9:20:64:92:70:EA:87:47:84:02:CE:2E:BA:4C:88:94:40:AD:61:6F:87:66:98:93:02:90:F3:BC:D1:4C:CB:81:49:9:5:5:FF:28:99:78:32:9D:87:B4:80:3C:40:BA:8D:D5:AE:F3:F3:5E:28:0B:23:CA:C9:88:74:82:02:74:3A:39:34:ED:B4:68:87:4F:85:41:65:25:5D:05:00:20:66:84:99:1C:67:AC:CB:87:1:42

Basic Constraints	<i>IsCA: true - Path length: 0</i>
Subject Key Identifier	<i>31:ED:F3:61:80:C8:49:DC:D6:CC:3D:0C:E6:28:E2:5C:60:53:DD:58</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.19484.2.2.1</i> <i>CPS pointer: http://pki.bde.es/políticas</i> <i>CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España.</i> <i>@2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]</i>
Authority Key Identifier	<i>4B:CC:E3:6B:D3:6C:39:34:4F:4D:C3:DE:60:C2:06:19:90:6D:6E:BF</i>
CRL Distribution Points	<i>ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint</i> <i>http://pki.bde.es/crls/ACraizv2.crl</i> <i>http://pki.redbde.es/crls/ACraizv2.crl</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>64:4B:79:C4:7D:87:C2:9B:31:6A:5C:D7:99:4C:F1:CF:CA:3E:1F:C0:78:55:21:87:56:5F:22:ED:83:25:03:95</i>
Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description	[en] undefined. [es] undefined.
Status Starting Time	<i>2017-07-01T22:00:00Z</i>

21.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

21.3.2 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service Name

Name	[en]	<i>Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2</i>
Name	[es]	<i>Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2</i>

Service digital identities**X509SubjectName**

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA V2*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2016-06-30T22:00:00Z

21.3.2.1 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

21.3.3 - History instance n.2 - Status: undersupervision**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Name *[es]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

Service digital identities**X509SubjectName**

Subject CN: *BANCO DE ESPAÑA-AC CORPORATIVA V2*

Subject O: *BANCO DE ESPAÑA*

Subject C: *ES*

X509SKI

X509 SK I *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2015-07-12T22:00:00Z

22 - TSP: Servicio de Salud de Castilla-La Mancha (SESCAM)

TSP Name

Name *[en]* *Servicio de Salud de Castilla-La Mancha (SESCAM)*

Name *[es]* *Servicio de Salud de Castilla-La Mancha (SESCAM)*

TSP Trade Name

Name *[en]* *Servicio de Salud de Castilla-La Mancha (SESCAM)*

Name *[es]* *Servicio de Salud de Castilla-La Mancha (SESCAM)*

Name *[en]* *JCCM*

Name *[es]* *JCCM*

Name *[en]* *SESCAM (NIF Q-4500146H)*

Name *[es]* *SESCAM (NIF Q-4500146H)*

Name *[en]* *VATES-Q4500146H*

PostalAddress

Street Address *[en]* *Avenida Río Guadiana*

Locality *[en]* *Toledo*

State Or Province *[en]* *Toledo*

Postal Code *[en]* *45007*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Avenida Río Guadiana*

Locality *[es]* *Toledo*

State Or Province *[es]* *Toledo*

Postal Code *[es]* *45007*

Country Name *[es]* *ES*

ElectronicAddress

Service Type Identifier

Service type description	<i>[en]</i> A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	<i>[es]</i> Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by CA SESCOAM CA Entidades Finales

Name	[es]	Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales

Service digital identities

Certificate fields details

Version: 3

Serial Number: 70907445827100184588831300374429509823

X509 Certificate

--BEGIN CERTIFICATE--

```
MIIFOzCgAgOgAiBQIwNjGm7n1WMTAA55VDUoVw2bAnGkhqG5wBOAQUFADBMSSQzVOQOg
EwE1UwEEMASGALUEUECHSNAIDTFRM0GALUECwNADUOT007ME8SRBRLT0IMdAYz2TcXMSUjG
ALUEAAwUOT007QFM1PbV3QgOeUWHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOg
COYDVOGQeWfUzENMASGALUECwNADUOT007ME8B4GALUECwNADUOT007HCHVUj500NTAMTQ2
GALUEAAwUOT007QFM1PbV3QgOeUWHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOg
BQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQ
o9BFE067yUjOxJ5SiXsmYU8r+g+BFK1Snp;+wS+gWYPIWPIX0X18hEUD9W6KcX4u94fA
EwE1UwEEMASGALUEUECHSNAIDTFRM0GALUECwNADUOT007ME8SRBRLT0IMdAYz2TcXMSUjG
63G8iH53uLnlvYdR07KpCgEFCN0B2iXscYsmgAd45W1+whYtTWN1XbEUD9W6KcX4u94fA
9UjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s
4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCge
BAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOxJ5SiX
smYU8r+g+BFK1Snp;+wS+gWYPIWPIX0X18hEUD9W6KcX4u94fA+1iNUORZzRtPvy20V9w
Q4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwsht
UjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMT
MTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07
FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW
5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00
W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1ayk
zLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234
cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOg
BQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9B
FE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09
R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPAD
CCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjO
VB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s434
3UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBA
EN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHRE
YD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhN
MTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUOR
ZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOX
PKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTW
MTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20
V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbk
wshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHz
CNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrU
WFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCb
kXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTw
MTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNN
H1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G
6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjY
BKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqk
UgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cAC
wAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQA
QgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE0
67yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/C
B82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCC
AgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5
w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343
UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBA
EN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHRE
YD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHh
NMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNU
ORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MO
XPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMT
WMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy
20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwK
MbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5
WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4Z
rUWFKR07FHNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUj
CbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTM
TwMTA00W5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07F
HNNH1aykzLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5
Ff9G6U1234cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W
5SjYBKMCOgBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1ayk
zLqkUgQo9BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U123
4cACwAAa09R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCO
gBQAQgEFPADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9
BFE067yUjOVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa0
9R/CB82s4343UWfUwHhNMTAXtMTWMTA00T5WHzCNnMTMTwMTA00W5SjYBKMCOgBQAQgEP
ADCCAgCgeBAEN+1iNUORZzRtPvy20V9wQ4ZrUWFKR07FHNNH1aykzLqkUgQo9BFE067yUj
OVB5w/WRHREYD9A+MOXPKDpBwKMbkwshtUjCbkXMSW5Ff9G6U1234cACwAAa09R/CB82s4
3
```

Signature algorithm: *SHA1withRSA*

Issuer CN: *SESCAM Root CA*

Issuer O: *SESCAM(NIF O-4500146H)*

Issuer O: ICCM

Issuer C: *ES*

Subject CN: *SESCAM CA Entidades Finales*

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

Valid from: *Tue Nov 30 11:49:29 CET 2010*

Valid to: *Fri Nov 30 11:49:29 CET 2035*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D2:3E:9F:58:97:A1:14:59:CD:A8:6D:3F:2B:F2:D9:0B:E5:F7:04:38:CE:B5:15:FC:59:11:D3:8A:7C:1D:55:65:D6:AC:A4:CC:A4:88:26:12:86:A2:AF:7C:10:5D:3A:81:3C:9A:8C:E5:D7:E6:3E:5C:31:4F:18:B9:FF:2A:FA:B0:45:20:A9:79:FE:7B:29:FA:18:2C:F2:FA:BF:39:63:C8:35:73:97:D7:C8:A2:7A:50:FD:5A:81:0A:75:C5:F1:F7:87:DA:F4:24:F4:5F:D0:8D:10:88:C6:FE:68:CB:0C:A8:A0:7F:D5:F1:B0:AF:EA:E5:A4:29:35:EE:62:83:47:FE:DF:F7:56:F7:05:BF:82:65:86:FC:F5:69:2A:17:66:EB:61:54:25:CF:A0:B2:6E:57:54:A4:DF:EB:71:BF:8A:2F:39:BB:79:CB:BE:F1:F1:83:4A:D8:70:AA:46:79:C1:71:FC:D4:1B:D9:0B:22:C5:2B:E6:A8:0D:2C:5B:F6:3E:C2:16:18:4F:3C:21:63:A1:84:51:4B:8E:C5:A1:96:20:66:5C:6E:DF:0B:F6:F5:0E:BF:CC:7F:5A:B4:49:F0:4C:F2:03:E3:10:5C:A3:DD:D8:A9:8C:6C:AC:2C:85:3B:8F:88:26:FD:74:A3:12:58:52:18:17:A1:A5:F7:5D:B7:B3:87:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *B5:C3:BB:5E:44:E9:E4:2E:34:04:E4:37:E3:1D:EA:51:FA:D2:07:FD*

Authority Key Identifier *E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D*

Certificate Policies *Policy OID: 2.5.29.32.0*
CP5 pointer: http://sescam.jccm.es/pki/dpc/dpcv2.html

CRL Distribution Points *http://sescam.jccm.es/pki/crls/sescam_root_ca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7B:14:45:2A:70:9D:F3:C6:8C:8E:EB:75:2F:88:78:C0:F5:21:C7:18:8C:23:81:11:DE:1D:DF:82:91:C4:17:2B*

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2017-07-01T22:00:00Z*

Scheme Service Definition URI

URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

22.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

22.1.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by CA SESCOAM CA Entidades Finales

Name [es] Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales

Service digital identities**X509SubjectName**

Subject CN: SESCOAM CA Entidades Finales

Subject O: SESCOAM (NIF Q-4500146H)

Subject O: JCCM

Subject C: ES

X509SKI

X509 SKI tc07XkTp5C40BOQ34x3qUfrSB/0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

22.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

22.1.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by CA SESCOAM CA Entidades Finales

Name [es] Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales

Service digital identities

X509SubjectName

Subject CN: SESCOAM CA Entidades Finales

Subject O: *SESCAM (NIF Q-4500146H)*

Subject O: *JCCM*

Subject C: *ES*

X509SKI

X509 SK I *tcO7XkTp5C40BOQ34x3qUfrSB/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

Status Starting Time *2012-06-08T00:00:00Z*

22.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SESCAM CA Entidades Finales*

Name [es] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

Service digital identities

X509SubjectName

Subject CN: SESCAM CA Entidades Finales

Subject O: SESCAM (NIF Q-4500146H)

Subject O: JCCM

Subject C: ES

X509SKI

X509 SK I tcO7XkTp5C40BOQ34x3qUfrSB/0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2011-09-16T00:00:00Z

22.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.2 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

Subject Key Identifier *B3:92:9C:69:4A:88:47:40:C4:85:46:DB:DE:19:68:80:29:8B:55:48*

Authority Key Identifier *E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <http://sescam.jccm.es/pki/dpc/dpcv2.html>
CPS text: [Los certificados emitidos bajo esta política son emitidos por el SESCAM para ACs subordinadas de la AC raíz del SESCAM]
CPS text: [Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA]

Authority Info Access *<http://sescam.jccm.es/va>*

CRL Distribution Points *http://sescam.jccm.es/pki/crls/sescam_root_ca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6F:C2:32:D6:10:27:6E:1B:95:B2:84:8A:E0:B2:60:36:23:C7:80:86:98:C8:97:56:42:AD:40:D2:8F:4B:D2:84*

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

Service Status*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2017-07-01T22:00:00Z***Scheme Service Definition URI**

URI *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

22.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

22.2.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA SESCOAM CA Entidades Finales - 2012

Name [es] Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales - 2012

Service digital identities

X509SubjectName

Subject CN: SESCOAM CA Entidades Finales

Subject SERIAL NUMBER: Q4500146H

Subject O: JCCM

Subject OU: SESCOAM

Subject C: ES

X509SKI

X509 SK I s5KcaUqIR0DEhUbb3hlogCmLVUg=

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

22.2.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.2.4 - History instance n.2 - Status: supervisionincessation

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SESCOAM CA Entidades Finales - 2012*

Name [es] *Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales - 2012*

Service digital identities

X509SubjectName

Subject CN: *SESCAM CA Entidades Finales*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: ES

X509SKI

X509 SKI s5KcaUqIR0DEhUbb3hlogCmLVUg=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

Status Starting Time 2016-06-26T22:00:00Z

22.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by CA SESCOAM CA Entidades Finales - 2012

Name [es] Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales - 2012

Service digital identities

X509SubjectName

Subject CN: SESCOAM CA Entidades Finales

Subject SERIAL NUMBER: Q4500146H

Subject O: JCCM

Subject OU: SESCOAM

Subject C: ES

X509SKI

X509 SK I s5KcaUqIR0DEhUbb3hlogCmLVUg=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2012-06-08T00:00:00Z

22.2.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.3 - Service (withdrawn): Qualified Certificates issued by CA SESCOAM CA Entidades Finales v2

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by CA SESCOAM CA Entidades Finales v2

Name [es] Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales v2

Certificate Policies*Policy OID: 2.5.29.32.0**CPS pointer: <http://sescam.jccm.es/pki/dpc>**CPS text: [Los certificados emitidos bajo esta política son emitidos por el SESCAM para CAs subordinadas de la CA Raíz del SESCAM]**CPS text: [Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA]***Authority Info Access***<http://sescam.jccm.es/va>***CRL Distribution Points***http://sescam.jccm.es/pki/crls/sescam_root_ca_v2.crl***Key Usage:***keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***CE:9F:E1:F8:BC:D8:9C:47:69:57:C7:82:17:F4:C4:6F:F5:02:2E:B9:06:63:12:36:2F:61:01:6F:62:9E:79:C4***X509SubjectName****Subject CN:***SESCAM CA Entidades Finales v2***Subject SERIAL NUMBER:***Q4500146H***Subject O:***JCCM***Subject OU:***SESCAM***Subject C:***ES***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2017-07-01T22:00:00Z***Scheme Service Definition URI****URI**

[en]

*<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***URI**

[es]

*<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>***22.3.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description** [en]*undefined.*

[es]

*undefined.***Criteria list assert=atLeastOne**

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

22.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

22.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SESCOAM CA Entidades Finales v2*

Name [es] *Certificados reconocidos emitidos por CA SESCOAM CA Entidades Finales v2*

Service digital identities**X509SubjectName**

Subject CN: *SESCAM CA Entidades Finales v2*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

X509SKI

X509 SK I *ieoqRDcPTF7MtM4a7omkbeilxa0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

22.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

22.3.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

22.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales v2

Name [es] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2

Service digital identities**X509SubjectName**

Subject CN: SESCAM CA Entidades Finales v2

Subject SERIAL NUMBER: Q4500146H

Subject O: JCCM

Subject OU: SESCAM

Subject C: ES

X509SKI

X509 SK I ie0qRDcPTF7MtM4a7omkbeilxa0=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2016-06-26T22:00:00Z

22.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**Qualifier type description** [en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne**Policy Identifier:****Identifier**

[OIDsURN]

urn:oid:2.16.724.4.8.10.60.10.3.2.1

Policy Identifier:**Identifier**

[OIDsURN]

urn:oid:2.16.724.4.8.10.60.10.3.2.2

23 - TSP: SIGNE S.A.**TSP Name**

Name *[en]* *SIGNE S.A.*

Name *[es]* *SIGNE S.A.*

TSP Trade Name

Name *[en]* *SIGNE Autoridad de Certificación*

Name *[es]* *SIGNE Autoridad de Certificación*

Name *[en]* *VATES-A11029279*

Name *[en]* *Signe S.A.*

PostalAddress

Street Address *[es]* *Avenida de la Industria, 18*

Locality *[es]* *Tres Cantos*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28760*

Country Name *[es]* *ES*

PostalAddress

Street Address *[en]* *Avenida de la Industria, 18*

Locality *[en]* *Tres Cantos*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28760*

Country Name *[en]* *ES*

ElectronicAddress

URI *[en]* *mailto:signe-ac@signe.com*

URI *[en]* *http://www.signe.es/signe-ac*

TSP Information URI

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service digital identities

Version:	3
Serial Number:	2445720188065766261
X509 Certificate	-----BEGIN CERTIFICATE-----

Signature algorithm:	SHA256withRSA
Issuer CN:	Autoridad de Certificacion Firmaprofesional CIF A62634068
Issuer C:	ES
Subject CN:	SIGNE Autoridad de Certificacion
Subject SERIAL NUMBER:	A11029279
Subject O:	SIGNE S.A.

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

Valid from: *Wed Jul 29 13:22:23 CEST 2015*

Valid to: *Tue Dec 31 05:02:55 CET 2030*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:97:AD:27:C9:B8:10:76:D3:A1:68:5B:E2:3F:23:D1:DB:5B:85:53:A2:28:3E:22:A9:64:39:98:58:E7:31:6A:BB:64:B1:60:7F:C6:2C:5B:08:DD:A5:70:CD:BB:7A:5D:89:3F:BA:48:49:80:0F:96:EC:EB:A7:8C:D3:A6:1C:35:BE:D0:41:9A:B9:E5:9D:40:D1:CD:CE:0B:84:07:A4:8F:98:AA:8C:7A:7A:1D:1A:B3:D6:00:12:69:23:D2:5D:CB:CE:B8:3B:EA:E2:3A:A0:FF:E8:38:99:60:0E:07:2F:6F:B1:7E:83:02:11:28:B1:78:D8:8E:EB:B5:F0:FF:B6:26:71:DC:2A:AE:47:22:6C:99:9F:40:65:14:04:A6:C4:E3:CC:B2:82:1A:E4:7A:10:D7:7E:F8:01:78:5D:82:3A:A8:0C:75:7B:2F:61:D0:31:5C:3D:77:C1:9A:8C:06:49:99:21:84:D8:49:3C:45:EF:CF:0B:2B:71:EC:D8:7D:6A:DE:72:2B:23:E6:F3:3B:6B:5F:51:3B:F7:0B:45:FD:03:A9:1E:ED:0E:A6:7A:FD:61:67:D2:03:7A:95:B6:0C:F6:BB:A2:6D:26:76:7B:20:CD:74:97:05:03:FF:42:E9:7F:09:C1:85:9B:17:F9:2A:8F:20:2E:AE:85:F6:E9:4F:E7:05:02:03:01:00:01

Authority Info Access
http://crl.firmaprofesional.com/caroot.crt
http://ocsp.firmaprofesional.com

Subject Key Identifier *90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]
CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points *http://crl.firmaprofesional.com/fproot.crl*

Extended Key Usage *id_kp_clientAuth - id_kp_OCSPSigning - id_kp_smartcardlogon*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1C:B4:70:72:8C:F5:6F:30:20:03:BB:0E:4E:B0:62:41:4F:A1:1D:4F:97:E3:F0:61:17:0C:96:C8:80:71:D7:11*

Certificate fields details

Version: *3*

Serial Number: *3624911463653416953*

Extended Key Usage *id_kp_clientAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C4:2C:E0:22:D0:A3:45:7B:6B:D6:97:87:11:CE:7B:C7:43:85:C4:B3:4E:11:EB:C8:B
A:EE:8B:1D:1B:83:27:99*

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion*

Subject SERIAL NUMBER: *A11029279*

Subject O: *SIGNE S.A.*

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2021-04-21T00:00:00Z*

23.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.36035.1.3.2*

23.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.1.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

23.1.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.2.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.10.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.5.3

Description**23.1.5 - History instance n.1 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name	[en]	Qualified certificates issued by SIGNE- Certification Authority

Service digital identities**X509SubjectName**

Subject CN:	SIGNE Autoridad de Certificacion

Subject SERIAL NUMBER:	A11029279

Subject O:	SIGNE S.A.

Subject L:	Avenida de la Industria 18. Tres Cantos 28760-Madrid

Subject C: ES

X509SKI

X509 SKI kK0aMf1HRW0yREMYhZdkxziubag=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-10-28T01:00:00Z

23.1.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.3.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.3.2

23.1.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

23.1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

23.1.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

Description**23.1.6 - History instance n.2 - Status: granted**

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name [en] Qualified certificates issued by SIGNE- Certification Authority

Service digital identities**X509SubjectName**

Subject CN: SIGNE Autoridad de Certificacion

Subject SERIAL NUMBER: A11029279

Subject O: SIGNE S.A.

Subject L: Avenida de la Industria 18. Tres Cantos 28760-Madrid

Subject C: ES

X509SKI

X509 SK I kK0aMf1HRW0yREMYhZdkxziubag=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2018-01-16T01:00:00Z

23.1.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.36035.1.3.1

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.36035.1.3.2

23.1.6.6 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

23.1.6.7 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

23.1.6.8 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

Description**23.1.7 - History instance n.3 - Status: granted**

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[es]* *Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación*

Name *[en]* *Qualified certificates issued by SIGNE- Certification Authority*

Service digital identities

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion*

Subject SERIAL NUMBER: *A11029279*

Subject O: *SIGNE S.A.*

Subject L: *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

Subject C: *ES*

X509SKI

X509 SK I *kK0aMf1HRW0yREMYhZdkxziubag=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

23.1.7.9 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.1*

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.36035.1.3.2*

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.1*

Policy Identifier:

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.2*

23.1.7.10 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**23.1.8 - History instance n.4 - Status: undersupervision****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name

[es]

Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name

[en]

Qualified certificates issued by SIGNE- Certification Authority

Service digital identities**X509SubjectName**

Subject CN:

SIGNE Autoridad de Certificacion

Subject SERIAL NUMBER:

A11029279

Subject O:

SIGNE S.A.

Subject L:

Avenida de la Industria 18. Tres Cantos 28760-Madrid

Subject C:

ES

X509SKI

X509 SK I

kK0aMf1HRW0yREMYhZdkxziubag=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2011-10-07T00:00:00Z

23.1.8.11 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description

[en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.3.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.3.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.10.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.36035.1.10.2

23.2 - Service (granted): Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020

Name [en] Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020

Service digital identities

Certificate fields details

Version: 3

Serial Number: 112294622129710941060350492154332911733

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B8:DF:38:4F:1F:CD:6E:CB:3F:4D:7D:D6:38:0E:54:D3:54:C6:12:56:56:0A:59:9D:80:45:32:47:D9:3A:F5:EA*

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *ljqC5qg/qePqI6Cr9o0ES0h7aMw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2024-12-03T00:00:00Z*

23.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

Name *[en]* *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

Service digital identities

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *ljqC5qg/qePqI6Cr9o0ES0h7aMw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-10-24T00:00:00Z*

23.2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.2.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.10.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.5.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.21.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.3.3
Description		

23.2.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [es] *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

Name [en] *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

Service digital identities

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *ljqC5qg/qePqI6Cr9o0ES0h7aMw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-10-20T00:00:00Z*

23.2.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.2.4.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.2.4.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.36035.1.2.3*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.36035.1.10.3*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.36035.1.5.3*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.36035.1.21.3*

Description

23.2.5 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

Name *[en]* *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

Service digital identities

X509SubjectName

Subject CN: *SIGNE Autoridad de Certificacion - 2020*

Subject OU: *Autoridad de Certificacion*

Subject 2.5.4.97: *VATES-A11029279*

Subject O: *SIGNE S.A.*

Subject C: *ES*

X509SKI

X509 SK I *ljqC5qg/qePqI6Cr9o0ES0h7aMw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-10-05T00:00:00Z*

23.2.5.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

23.2.5.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

23.2.5.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.10.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.36035.1.5.3
Description		

23.3 - Service (granted): Qualified electronic signature and seal certificates issued by
SIGNE SUBCA 2024

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name	
Name	[en] Qualified electronic signature and seal certificates issued by SIGNE SUBCA 2024
Name	[es] Certificados electrónicos cualificados de firma y sello emitidos por SIGNE SUBCA 2024

Service digital identities

Certificate fields details

Version:	3
Serial Number:	60692400370295334179024527137959826596
X509 Certificate	-----BEGIN CERTIFICATE----- MIIDCCAxqAwIBAgIQIajuxlaef4pvvIW7q8UpDAKBgggghkQPOQDABWMOswCOYDVOQGEWJF UzETMBEGA1UECgwKU2lnbmUuY5BLJEYMBYGA1UEYQwPvkFURVMQTEtMTkxNjAwWjBXMOSwCOYD DA9TSudORSBST09UdIwMjQwHhcnMjQwMjQwMTI1MzQzWncNNDkxMTI4MTkxNjAwWjBXMOSwCOYD VOQGEWJFUEtMBEGA1UECgwKU2lnbmUuY5BLJEYMBYGA1UEYQwPvkFURVMQTEtMTkxNjAwWjBXMOSwCOYD FWYDVOQDDBBTSUORSBTVUJQSAyMDI0MjQwHhcnMjQwMjQwMTI1MzQzWncNNDkxMTI4MTkxNjAwWjBXMOSwCOYD xz+M7lqOW5fZyCPI77cgaWRm3Tw3WtzcRo2Nha1wWSCoY3NsXRS6q502NvgEjgAhp4hx1p5JHx c1krWXA/ECNpODWPYqgittatWnXsALUthUokI5Aao4IBqCCAAyWegYDVR0TAQH/BAgwBgEB/wIB ADAHAgVHNSMEGDAWgBGAAsF47MH5yRZCX6iCjUe0z83Bgrg8gEFBQcBAQR/MGkw0wYkwyB BQUHMAKGL2h0dHA6Ly93d3cuc2lnbmUuZXNMc2lnbmUuY5BLJEYMBYGA1UEYQwPvkFURVMQTEtMTkxNjAwWjBXMOSwCOYD CCsGAQUFBzABhh5odHRwOi8vc2VydmJlaW9zLnNpZ251LnVzL29jc3AwgYQGA1UdIAR9MHsweQYE VR0gADBxMEEGCCsGAQUFBwIwMDUuMDI0MjQwHhcnMjQwMjQwMTI1MzQzWncNNDkxMTI4MTkxNjAwWjBXMOSwCOYD Y2FjacOzbiBkZSBTSudORTAsBggrBgEFBQcCARYgaHR0cDovL3d3d3ZzaWduZ55lcY9zaWduZ551h Yy9kcGMwQAYDVR0RBDkwNzA1ODQgMYYvaHR0cDovL3d3d3ZzaWduZ55lcY9zaWduZ551hYy9jcmwv C2lnbmUuY5BLJEYMBYGA1UEYQwPvkFURVMQTEtMTkxNjAwWjBXMOSwCOYDFAwIBBIAKBBgggghkQPOQDABWMOswCOYDVOQGEWJF UzETMBEGA1UECgwKU2lnbmUuY5BLJEYMBYGA1UEYQwPvkFURVMQTEtMTkxNjAwWjBXMOSwCOYD FWYDVOQDDBBTSUORSBTVUJQSAyMDI0MjQwHhcnMjQwMjQwMTI1MzQzWncNNDkxMTI4MTkxNjAwWjBXMOSwCOYD 3vjUAKW4s8= -----END CERTIFICATE-----
Signature algorithm:	SHA384withECDSA
Issuer CN:	SIGNE ROOT 2024
Issuer 2.5.4.97:	VATES-A11029279

Issuer O: *Signe S.A.*
Issuer C: *ES*
Subject CN: *SIGNE SUBCA 2024*
Subject 2.5.4.97: *VATES-A11029279*
Subject O: *Signe S.A.*
Subject C: *ES*
Valid from: *Wed Dec 04 13:53:43 CET 2024*
Valid to: *Sun Nov 28 13:16:00 CET 2049*
Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:33:E0:C7:83:7B:3F:C6:CC:2F:C7:3F:8C:EE:58:0E:5B:97:D9:C8:23:C8:EF:B7:20:69:64:66:DD:3C:37:5A:D7:33:46:86:4D:96:16:85:C1:64:82:A1:8D:CD:81:74:52:EA:AE:74:DA:B3:6F:80:48:EA:02:1A:78:87:1D:69:48:91:F1:73:59:2B:59:70:3F:10:23:5B:40:35:8F:CA:AD:20:96:D8:5A:5A:75:D2:68:85:13:1E:ED:24:97:90:1A*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *00:6C:5B:25:E4:5E:3B:30:7E:72:47:60:97:EA:20:A2:20:85:1E:D3*
Authority Info Access *http://www.signe.es/sign-ac/crl/sign-root.crt*
http://servicios.signe.es/ocsp
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de Autoridad de Certificación de SIGNE]
CPS pointer: http://www.signe.es/sign-ac/dpc
CRL Distribution Points *http://www.signe.es/sign-ac/crl/sign-root.crl*
Subject Key Identifier *4A:4F:AA:E9:4F:A8:7B:E0:17:EE:A2:3C:12:1E:AA:03:D4:25:EE:9F*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *24:41:66:24:09:47:C4:07:44:18:DF:26:06:FC:3E:BF:5A:76:5F:6B:96:92:18:5F:C0:91:EA:66:99:86:DA:35*

X509SubjectName

Subject CN: *SIGNE SUBCA 2024*
Subject 2.5.4.97: *VATES-A11029279*
Subject O: *Signe S.A.*
Subject C: *ES*

X509SKI

X509 SK I Sk+q6U+oe+AX7ql8Eh6qA9Ql7p8=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-10-02T02:00:00Z

23.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

23.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

23.4 - Service (granted): Qualified electronic timestamps issued by SIGNE TSA 2024

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified electronic timestamps issued by SIGNE TSA 2024

Name [es] Sellos cualificados de tiempo electrónico emitidos por SIGNE TSA 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 26506931831656710360878484361188294124

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDp2CCAY2gAwIBAgIQE/EMo9RjUfKYjs2fb097DAKBggqhkiOPOQDAzBWMQswCOYDVOQGEwIF
UzETMBEGA1UECgwKU2lnbmUySBLjEYMBYGA1UEYQwPVkFURVMTOTExMDI5Mjc5MRgwFgYDVQOD
DA9TSUORSBST09UdWwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQwMjQw
VOQGEwIFUzETMBEGA1UECgwKU2lnbmUySBLjEYMBYGA1UEYQwPVkFURVMTOTExMDI5Mjc5MRcw
FQYDVQODDASTSUIORSBUIUeGMAyND62MBAGBggGSM49AgEGBSuBBAIA2IABCWkVl/09pf5KnW7
Y2WKV+dBXSAMtSmt+WWp8B7Oeud2mKFFD6mQSManzNH89KPKxbnKTz+WWawQJz+qoSe9akWxVM
EgPc4k3FX+EdZ8VimrTHOfic5qHIA3P5EW36OCAB8wagG7MBIGAIUdEWEb/wQIMAYBARBCAQAw
HwYDVROjBBgwFoAUAGxbleReQzB+ckdpl+ogqICFHMwdwYKwY8BQUHAQEEa2BMDsGCCsGAQUF
B2ACI9odHRwOi8vd3d3LmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwz
BgEFBQcwAYYeaHR0cDovL3NlcnZpY2Vucy5zaWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwz
IAAwcTB8BggqBgEFBQcCAjA1DDNDZjI0aWZpY2FkbyBkZSBBdXRvcmlkYVwqZGUGO2VydGimaWNh
Y2N0S24gZGUGO2VydGimaWNhY2N0S24gZGUGO2VydGimaWNhY2N0S24gZGUGO2VydGimaWNh
ZHBjBMBMGA1UdJQQMMAoGCCsGAQUFBwMIMEAGAIUdHwQ5MDcwNaAzoDGL2h0dHA6Ly93d3cuZm
bmUuZmVuc2lnbmUyYWMvY3IsLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwzLmN5dWwz
UAEuBxq5DDA0BgNVHQ8BAf8EBAMCAQYwCgYIKoZIzj0EAwMDaAAwZQwSh+V4VajncUo50b68pV
fNb3jvhtcQ6RxiB0rWyyWeezd1smswkHDY5V7TLU8fKdAJEAUePEHXOed3gIuljPuPXMG63xfo
FM5UMVoUpruknCpJ8TZ5F35eEkmHob55qHcz

```

-----END CERTIFICATE-----

Signature algorithm:

SHA384withECDSA

Issuer CN:

SIGNE ROOT 2024

Issuer 2.5.4.97:

VATES-A11029279

Issuer O:

Signe S.A.

Issuer C:

ES

Subject CN:

SIGNE TSA 2024

Subject 2.5.4.97:

VATES-A11029279

Subject O:

Signe S.A.

Subject C:

ES

Valid from:

Wed Dec 04 13:57:24 CET 2024

Valid to:

Sun Nov 28 13:16:00 CET 2049

Public Key:

```

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:25:A4:55:FF:F4:F6:97:D2:2A:75:BB:63:65:8A:57:E7:41:5F:90:0C:85:29:88:F9:6C:29:F3:C2:13:39:EB:83:
DA:62:85:14:3E:A6:41:23:1A:9F:33:47:F3:D9:0F:2B:16:EB:34:A4:F3:F9:65:9A:C1:08:F6:FA:AA:12:EB:D6:A4:5B:15:4C:12:03:DC:E2:4D:C5:F5:E1:1D:67:C5:6D:8A:6A:D3:1C:E1:DF:8D:C
E:6A:85:F0:37:3E:C1:16:DF

```

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier

00:6C:5B:25:E4:5E:3B:30:7E:72:47:60:97:EA:20:A2:20:85:1E:D3

Authority Info Access

<http://www.signe.es/signe-ac/crl/signe-root.crt><http://servicios.signe.es/ocsp>

Certificate Policies

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación de SIGNE]

CPS pointer: <http://www.signe.es/signe-ac/dpc>

Extended Key Usage

id_kp_timeStamping

CRL Distribution Points

<http://www.signe.es/signe-ac/crl/signe-root.crl>

Subject Key Identifier

99:21:1D:AB:B6:3E:16:08:8E:42:DB:C1:3B:B8:01:2E:05:7A:B9:0C

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:	SHA-256
Thumbprint:	22:D9:B5:11:68:9F:F6:CB:79:7A:31:E7:73:24:DC:BC:0E:B3:C0:A3:5B:BC:DE:4F:8D:E7:7F:15:54:F8:76:03
X509SubjectName	
Subject CN:	SIGNE TSA 2024
Subject 2.5.4.97:	VATES-A11029279
Subject O:	Signe S.A.
Subject C:	ES
X509SKI	
X509 SK I	mSEdq7Y+FgiOQtvBO7gBLgV6uQw=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2025-10-02T02:00:00Z

24 - TSP: SISTEMAS INFORMATICOS ABIERTOS S.A.U.

TSP Name

Name [en] *SISTEMAS INFORMATICOS ABIERTOS S.A.U.*

Name [es] *SISTEMAS INFORMATICOS ABIERTOS S.A.U.*

TSP Trade Name

Name [en] *SIA*

Name [es] *SIA*

Name [en] *VATES-A82733262*

Name [en] *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Name [es] *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Name [en] *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Name [es] *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Name [en] *SISTEMAS INFORMATICOS ABIERTOS SAU*

PostalAddress

Street Address [en] *Avda. de Bruselas N.º 35*

Locality [en] *Alcobendas*

State Or Province [en] *Madrid*

Postal Code [en] *28108*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Avda. de Bruselas N.º 35*

Locality [es] *Alcobendas*

State Or Province [es] *Madrid*

Postal Code [es] *28108*

Country Name [es] *ES*

Issuer SERIAL NUMBER: A82733262

Issuer O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Issuer C: ES

Subject CN: SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

Valid from: Thu Jan 29 10:56:43 CET 2015

Valid to: Tue Jan 29 11:26:43 CET 2030

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:96:B7:EC:41:AA:6C:6A:DE:92:0A:D4:FF:04:C0:73:A5:75:FF:6F:FD:5D:AF:BC:78:32:3B:76:9F:82:81:F7:85:B3:2F:62:1C:61:9F:BF:2A:A1:C1:83:13:8C:02:CF:8A:4E:16:31:E0:59:55:A0:29:E6:87:A4:16:34:DF:F3:4C:DF:2E:E4:9C:95:40:88:08:0B:DC:3C:21:2C:3D:7B:56:19:D6:71:12:BC:16:83:34:48:99:5F:85:BC:97:89:FF:3B:39:E5:4A:52:C6:5D:74:AB:42:FC:A2:FC:D7:A2:6D:4F:71:60:89:ED:E0:D0:41:4B:3D:E1:57:BB:B1:9E:0F:27:FC:2E:D7:99:08:3F:E0:8B:2F:02:0C:41:F9:65:CB:D1:B1:86:E3:32:22:89:10:3B:A1:8E:2F:7B:5B:79:85:30:20:47:23:B8:D3:3B:FE:52:A0:56:11:98:06:96:CA:B8:BD:C7:1C:F5:83:14:F8:4A:CE:7D:11:86:F3:83:3F:89:EB:0E:08:E1:88:1F:99:EF:5A:05:3F:9C:76:82:7C:E3:8C:9C:6F:30:A0:7C:9C:DC:3E:08:BC:15:89:FE:5D:12:6E:47:59:21:F2:3F:DC:D1:95:64:07:3C:E6:EC:1F:67:34:F8:EC:F8:2B:3E:8F:56:19:6F:D8:D5:A0:15:DB:31:D1:58:9D:C3:D1:B1:AC:C4:60:FF:5C:6A:86:3E:B1:1C:1E:D9:A8:0C:7B:5D:18:46:C3:93:62:31:FD:8B:A8:64:39:DF:AA:34:33:A3:19:44:8C:76:81:D E:AD:74:23:AD:CA:BF:98:28:5F:F8:D5:5C:B3:0C:87:C9:E4:67:2B:38:4D:AC:8D:2E:99:F9:44:F8:19:0F:EC:95:C1:32:92:B0:75:70:AF:2C:61:54:64:37:8A:80:F5:8F:FC:02:EE:72:C8:71:62:2A:37:A5:F1:B4:53:20:36:EA:C5:E7:A5:51:22:20:F7:CE:12:FF:DA:85:69:3B:50:6F:88:FA:F1:76:A5:11:0C:89:2A:29:F5:82:08:9F:91:70:06:FF:FA:33:AC:8D:22:61:5E:24:A2:E7:E2:01:1A:01:88:61:E7:78:16:3E:85:DD:76:EF:F8:44:61:26:5C:65:3C:5D:33:81:9E:37:82:73:D4:31:27:AF:C3:00:36:25:40:62:90:DA:99:62:A8:5E:01:AB:C2:E5:86:CA:F9:4C:FC:80:A6:35:16:3B:B3:0C:3A:AD:A6:98:D8:9F:7D:DE:A0:95:90:3E:DE:2A:E9:6C:6C:37:59:0F:79:E9:4E:FA:08:A5:3B:E5:08:04:86:C4:72:D6:BE:69:37:54:7C:EC:C6:9F:98:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Info Access
https://psc.sia.es/ac_raiz.crt
<https://psc.sia.es/ocsp>

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://psc.sia.es>
CPS text: [Certificado de AC subordinada. Consulte las condiciones de uso en <https://psc.sia.es>]

CRL Distribution Points
<https://psc.sia.es/arl.crl>
C=ES,O=SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA,SERIALNUMBER=A82733262,CN=SIA ROOT,CN=CRL1

Authority Key Identifier 2E:E0:8D:C9:54:AE:A2:1B:73:C9:A6:A3:47:AB:99:63:C2:EE:D4:F0

Subject Key Identifier DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC

Key Usage: keyCertSign - cRLSign

Thumbprint algorithm: SHA-256

Thumbprint: 68:69:00:54:B9:17:C0:E4:A9:60:92:C4:B3:59:F7:41:80:98:B6:4E:F1:49:A7:0B:78:5A:38:9C:45:51:5D:10

X509SubjectName

Subject CN: SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2022-12-22T00:00:00Z

24.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

24.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

24.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] <urn:oid:1.3.6.1.4.1.39131.10.1.15>

Policy Identifier:

Identifier [OIDAURN] <urn:oid:1.3.6.1.4.1.39131.10.1.16>

Policy Identifier:

Identifier [OIDAURN] <urn:oid:1.3.6.1.4.1.39131.10.1.17>

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.18

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.13

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.13.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.13.2

Description**24.1.4 - History instance n.1 - Status: granted**

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by CA SIA SUB01

Name [es] Certificados Reconocidos emitidos por CA SIA SUB01

Service digital identities**X509SubjectName**

Subject CN: SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

X509SKI

X509 SKI *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-01-11T02:00:00Z*

24.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

24.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.15*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.16*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.17*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.18*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.20*

Policy Identifier:

Identifier *[OIDAURN]* *urn:oid:1.3.6.1.4.1.39131.10.1.13*

Description

24.1.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SIA SUB01*

Name *[es]* *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities**X509SubjectName**

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-01-16T01:00:00Z*

24.1.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

24.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.15

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.16

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.17

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.18

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.20

Description**24.1.6 - History instance n.3 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA SIA SUB01

Name	[es]	Certificados Reconocidos emitidos por CA SIA SUB01

Service digital identities**X509SubjectName**

Subject CN:	SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

X509SKI

X509 SK I 2mDRJzDSJoXNfkji9ul5H1owVaw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-10-28T01:00:00Z

24.1.6.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

24.1.6.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

24.1.6.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.15

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.16

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.17

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.39131.10.1.18*

Description**24.1.7 - History instance n.4 - Status: granted**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SIA SUB01*

Name [es] *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities**X509SubjectName**

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-08-02T00:00:00Z*

24.1.7.10 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.7.11 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

24.1.7.12 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.15

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.16

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.17

Policy Identifier:

Identifier	[OIDsAsURN]	urn:oid:1.3.6.1.4.1.39131.10.1.18

Description**24.1.8 - History instance n.5 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by CA SIA SUB01
Name	[es]	Certificados Reconocidos emitidos por CA SIA SUB01

Service digital identities**X509SubjectName**

Subject CN:	SIA SUB01
Subject SERIAL NUMBER:	A82733262
Subject OU:	QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

X509SKI

X509 SK I 2mDRJzDSJoXNfkji9ul5H1owVaw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-02-15T01:00:00Z

24.1.8.13 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

24.1.8.14 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

24.1.8.15 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.7

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.39131.10.1.18*

Description**24.1.9 - History instance n.6 - Status: granted**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by CA SIA SUB01*

Name [es] *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities**X509SubjectName**

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9ul5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

24.1.9.16 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.1.10 - History instance n.7 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by CA SIA SUB01*

Name *[es]* *Certificados Reconocidos emitidos por CA SIA SUB01*

Service digital identities

X509SubjectName

Subject CN: *SIA SUB01*

Subject SERIAL NUMBER: *A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *2mDRJzDSJoXNfkji9uI5H1owVaw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-07-06T00:00:00Z*

24.2 - Service (withdrawn): Qualified timestamps issued by TSAQC

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by TSAQC*

Name *[es]* *Sellos de tiempo cualificados emitidos por TSAQC*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1481140816*

Certificate Policies

Policy OID: 1.3.6.1.4.1.39131.10.1.14

CPS pointer: <https://psc.sia.es>CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: <https://psc.sia.es>]

Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false

*id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15*

Authority Key Identifier

DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

94:6B:BF:53:5A:21:D9:D7:32:E3:E5:70:B6:2E:79:3B:3A:09:22:21:35:7C:E1:B2:FA:61:C7:16:95:80:2D:38

Certificate fields details

Version:

3

Serial Number:

1481668284

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIG/DCCBQSAwIBAgIIEWFB2vDANBgkqhkiG9w0BAQsFADCBhQELMAkGA1UEBhMCVGVXODAzBGNV
BA0T1NlUURTRUFiEiQK9STUJFUSUNPjYBOKFURPjYBT0NVRURBQCBTt9OSU1BMRUwEwYD
VQQLExwRVUFMSUZRUQgO0ExEjAQBGNVBAUTCUE4MjczMzIzMEsMBAGA1UEAxMjU0BIFNVQjA
MB4XDThwMDkxNDExNTQwMVoXDTIzMDkxNDExMjQwMVoG9wG9gCzA1BgNVBAYTAkVTMTgwNgYDVOQK
Ej9TSVNURUU1BjYBjTKZPK1BVEIDT1MgQUJRVRVUT1MgU09DSUVEQUQgU0U5PTkiNOTEVMBGA1UE
CxMMUUVBTElGSUVEIENBMGRwFgYDVORHw9WQVRFljY1BODI3MzMyNjIxOjAMBGNVBAWMTBVRQVFD
MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1mSNqbsphXB3b4AW345hXSCZJEB3ns1p
yqs1BpNvUjLEjCccNvOnly9O9SCK113aRRMhcnstToGnHg3oeWwH95+J9NKKY+a8k4
ctXjez2tzfzrKH95WQ1n2EVIMbgmouk6UygcFePL4thW0MuQFipQ7YtagzXkiUdTV5vLyN
zVYORCAIM3esN9cQIVKgwGAT0vnnARQjboZduZHvo6lfdLuu5JAK1d5R006V9+y0EwoXbVrVQp
nRja121sL2KubyQ0Wab6WgtGZ+O6yqNFAI6M5poxmQF32Y7EHH9Jlhb2uZ266Ujh1qV7Yr
UyENIQIDAQAB04icbDCCAmgwDgYDVROPAQH/BAQDAgBAMBYGA1UdQEBwQMMaogCCcSAQUFBWMI
MGAGCCcSAQUFBWBBFQwUjA1BggrBgEFBQcwAYYXaHR0cHM6Ly9wcz2Muc2hlMmVzL29jc3AwkwyI
KwYBQQUHMAKGIH2h0dHBzOjBvcHNjLnNpY55ic9Yy19zdWwMSS5cnOwqfAGA1UdIAS66CB5CB
1wYLKwYBBAQCSvsKAQ4wgccwHgYKwYBQQUHAgEWEEmh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL
7EKBAIAIBgYEAISGAQIwITApRfVodirWcczovL3BzYy5zaWEuZXNwZWZATAmVUBMBG8gQAjYBBAj
BgCEA15GAQYCMewGA1UdHwRFMEwQaA1oD2GHGh0dHBzOjBvcHNjLnNpY55ic9CBpAYIKwYB
BQUHAgIwagZcMgZRDZjQdaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBzZWxs
b3MgZ2xwY3RyW7nuaWwcy6jWfSaWZpY2FkbyBkZSBzZ2JzaWwNpbyBkZSBleHBIZGiacOzbBkZSBz
c2BgeSBzW61hcyBkZSBzZ250YWN0byBibjogahR0cHM6Ly9wcz2Muc2hlMmVzMAKGBWQAI+xAQEw
egYKwYBQQUHAgMEbjBsmAgBgGQAjYBATALBgYEA15GAQMCAQ8wFQYIKwYBQQUHAgEwCQYHBAKL

```

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

Valid from: *Fri Sep 04 13:54:01 CEST 2020*

Valid to: *Mon Sep 04 14:24:01 CEST 2023*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:64:8D:A9:B4:A9:85:70:77:6F:80:16:DF:84:A1:5D:20:99:24:46:F7:9E:CD:69:CA:A8:35:06:93:55:6D:48:EC:2C:4F:C2:72:80:9F:36:80:E7:57:DC:4E:F7:CA:82:5C:82:35:C7:76:91:46:53:07:72:74:85:4C:EA:8D:86:AD:E8:12:FC:07:F7:9F:89:F5:03:4A:2A:FF:9A:F2:4B:F8:72:D9:17:8D:EC:D9:86:DF:F3:7E:B7:8A:1F:DE:56:43:59:F6:11:59:4C:6E:09:B4:BA:4E:94:CA:07:1D:15:E3:CB:E2:D8:56:D0:C8:90:7F:89:69:43:86:13:6A:09:F3:5E:42:14:75:35:79:BC:BC:8D:CD:56:34:44:20:22:33:77:AC:37:D7:10:21:52:86:C2:00:13:D2:F9:CD:01:F4:09:6C:E6:5D:B9:91:EF:A3:FE:88:7D:D2:EE:B9:22:40:2B:57:79:45:DD:3A:57:DF:B2:D0:4C:28:5F:F6:D5:AD:54:29:9D:12:54:88:6D:6C:8C:8D:8A:51:BC:9D:3B:FC:1A:E9:68:2D:75:9F:90:EA:0C:A0:34:50:16:E8:CE:69:C7:19:90:17:76:58:4F:F1:21:1D:FF:65:FC:98:74:88:67:59:DB:A0:54:86:1D:6A:57:86:2B:53:21:0D:95:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access
https://psc.sia.es/ocsp
https://psc.sia.es/ac_sub01.crt

Certificate Policies
Policy OID: 1.3.6.1.4.1.39131.10.1.14
CPS pointer: https://psc.sia.es
CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points
http://psc.sia.es/crlc10.crl
https://psc.sia.es/crlc10.crl

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *55:A4:10:9A:4E:AA:63:B6:46:1F:DB:B1:1E:1C:0B:AD:A6:E1:8C:DA:DB:45:4F:E5:63:A7:D3:6F:18:BF:57:1C*

X509SubjectName

Subject CN: *TSAQC*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *nrZ7bm nQvpA1gs5HCLWNwxsusSE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

24.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name [en] *Qualified timestamps issued by TSAQC*

Name [es] *Sellos de tiempo cualificados emitidos por TSAQC*

Service digital identities

X509SubjectName

Subject CN: *TSAQC*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

X509SKI

X509 SK I *nrZ7bm nQvpA1gs5HCLWNwxsusSE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-02-15T01:00:00Z*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Subject C: *ES*

Valid from: *Wed Nov 20 10:31:12 CET 2019*

Valid to: *Sun Nov 20 11:01:12 CET 2022*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A6:ED:2B:5A:EA:AE:05:F5:4A:4D:23:AB:BF:73:F7:91:FE:25:C2:85:77:DE:FC:A9:49:AC:16:08:68:C3:51:F7:33:D1:C1:3E:8E:6D:34:FC:5A:AE:BC:2E:1E:DD:B7:EA:AB:3A:2F:53:99:E2:E3:08:E4:51:0C:D1:A6:0B:81:84:71:1A:CF:B4:73:99:B7:BC:45:CC:CC:9E:CE:81:93:72:E6:1B:BC:4E:62:6D:D4:57:B4:08:23:88:66:CE:6D:59:EE:4D:AF:FE:CC:E5:8F:8B:2C:78:0B:AB:06:BB:DE:1F:39:DF:5B:6E:9C:59:E8:77:83:A1:E8:91:EE:6E:C1:68:FB:BB:19:33:D9:4A:AF:27:D4:BF:26:EE:53:D2:43:49:DC:84:8A:07:85:6D:5D:A2:EA:96:E2:BB:76:63:94:A5:4B:37:0A:10:BB:60:FD:15:4F:EC:8A:5C:EC:02:4D:F9:2F:A9:24:4B:17:64:64:E0:68:5F:DF:41:EA:7F:B0:49:AD:C3:81:E3:96:BC:56:90:3F:38:36:7F:75:D8:03:1D:B3:DA:09:BE:EE:B1:C5:40:D9:11:00:E9:03:6E:25:F3:15:03:AB:BC:0F:00:D4:D5:8E:36:64:1C:67:12:33:9A:9B:6A:FF:F4:4F:B2:E1:C2:13:4A:0F:8B:BD:2A:74:4B:02:03:01:00:01

Subject Alternative Name *OID.1.3.6.1.4.1.39131.10.2.7=A82733262,
 OID.1.3.6.1.4.1.39131.10.2.6=SISTEMAS INFORMATICOS ABIERTOS S.A.,
 OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE NIVEL MEDIO*

Extended Key Usage *id_kp_clientAuth*

Authority Info Access *https://psc.sia.es/ocsp
 https://psc.sia.es/ac_sub01.crt*

Certificate Policies *Policy OID: 1.3.6.1.4.1.39131.10.1.12
 CPS pointer: https://psc.sia.es
 CPS text: [Certificado cualificado de Sello Electrónico de nivel medio.
 Condiciones de uso y vías de contacto en: https://psc.sia.es]
 Policy OID: 0.4.0.194112.1.1
 Policy OID: 2.16.724.1.3.5.6.2*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance
 id_etsi_qcs_RetentionPeriod: 15*

CRL Distribution Points *http://psc.sia.es/crlc4.crl
 https://psc.sia.es/crlc4.crl*

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Subject Key Identifier *C3:93:A3:67:10:16:FC:2A:81:8B:8B:E5:3F:FA:81:EC:13:E8:20:8A*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B5:AA:55:A4:C5:50:58:F0:AE:92:63:96:18:EE:D9:F1:5D:63:F8:54:63:78:03:8A:9D
 :BD:92:9A:CB:4E:1B:52*

X509SubjectName

Subject CN: *SIAVAL*

Subject OU: SELLO ELECTRONICO

Subject 2.5.4.97: VATES-A82733262

Subject O: SISTEMAS INFORMATICOS ABIERTOS S.A.

Subject C: ES

X509SKI

X509 SK I w5OjZxAW/CqBi4vIP/qB7BPollo=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2022-12-22T00:00:00Z

24.3.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [es] Servicio cualificado de entrega electrónica certificada "SIAVAL"

Name [en] Qualified electronic registered delivery service "SIAVAL"

Service digital identities

X509SubjectName

Subject CN: SIAVAL

Subject OU: SELLO ELECTRONICO

Subject 2.5.4.97: VATES-A82733262

Subject O: SISTEMAS INFORMATICOS ABIERTOS S.A.

Subject C: ES

X509SKI

X509 SK I w5OjZxAW/CqBi4vIP/qB7BPollo=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-12-10T01:00:00Z

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name		
Name	[es]	Certificados electrónicos cualificados de autenticación de sitios web expedido por «SIA SSL SUB01 CA»
Name	[en]	Qualified Certificates for Web Site Authentication issued by «SIA SSL SUB01 CA»

Service digital identities

Certificate fields details	
Version:	3
Serial Number:	586069507734903019371865063389363923295135121821

[illegible]

Signature algorithm:	SHA256withRSA
Issuer CN:	SIA ROOT CA 2020
Issuer 2.5.4.97:	VATES-A82733262
Issuer O:	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA
Issuer C:	ES
Subject CN:	SIA SSL SUB01 CA
Subject 2.5.4.97:	VATES-A82733262

Subject OU: *QUALIFIED CA*
Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Subject C: *ES*
Valid from: *Fri Jul 23 12:54:36 CEST 2021*
Valid to: *Sat Jul 19 12:54:36 CEST 2036*
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:95:DF:85:EB:0A:08:FC:EB:56:FC:F2:8C:B3:5F:46:1F:78:24:B0:BA:42:56:
99:5C:7F:4C:68:C5:E9:29:A4:CE:66:B1:C4:58:BA:42:02:15:95:A8:B3:01:14:98:4A:88:42:BE:D4:F4:FD:88:40:BC:1F:85:A9:08:46:D9:1F:1A:2A:ED:2D:55:07:CF:D3:4D:5D:56:C9:A7:B4:
A9:1A:BA:68:D3:91:CF:41:59:30:03:14:08:03:72:73:97:22:5B:3E:02:53:79:4C:DC:EF:A0:AC:7D:88:85:8E:98:27:EB:F2:13:A8:78:0A:E9:3A:2D:6C:F4:12:9D:FF:4E:7F:BF:4F:3C:3E:97:97:
BA:E1:EA:91:8C:0F:6E:04:C8:8B:02:51:8A:44:95:E2:3C:22:17:F6:60:48:A5:46:C0:58:3A:8C:DD:AA:DE:E8:95:2B:C9:93:59:8F:85:AF:E3:8C:9E:5F:E2:5A:CC:63:6B:04:5E:77:23:7E:4F:A
8:2A:D6:AD:89:75:BC:2F:B7:1A:30:48:73:2B:57:25:1E:30:14:C0:CA:D4:0E:17:6D:58:30:30:16:D8:07:C5:69:78:F9:7F:15:77:C1:E5:29:6F:97:9D:86:C2:42:21:3F:F2:E8:4B:84:AB:E6:F7:
8C:02:95:C1:D3:D3:80:2F:8F:E2:34:84:78:88:C4:6A:03:74:F8:EC:44:47:1E:50:1E:42:F9:14:36:85:8D:FD:6B:EB:E2:19:8E:C5:59:3C:AF:72:D9:9D:08:9E:79:D6:BD:82:41:23:68:F9:7A:2
4:15:49:D2:A4:C6:C8:71:68:3F:3C:F5:84:21:68:FC:4D:5F:43:97:79:D0:72:11:34:DD:84:86:E2:EC:C2:50:70:1F:A2:C4:15:47:08:C6:10:46:4B:72:E6:21:5E:4E:60:10:D7:87:2C:62:59:46:
83:E0:94:A1:8E:37:43:BD:F4:AE:91:AD:69:68:95:1C:4B:EE:C1:E1:52:07:15:83:D7:3E:5D:D6:CB:AE:74:ED:AD:6C:C2:C5:71:3C:68:58:FC:53:75:A1:77:07:15:40:98:89:61:42:CD:F5:60:
00:AA:84:2F:A1:83:94:50:8B:91:5F:91:27:7D:72:D8:7D:AE:C6:D9:DF:6F:26:D4:F3:A7:9D:F9:52:5D:35:9E:EB:92:98:8B:A6:9E:76:55:56:01:9D:B0:AB:38:DF:21:3E:C9:CB:6A:92:AA:BE:F
E:EC:39:F1:EE:24:C6:F6:62:96:2C:52:3F:3A:00:43:81:BB:79:FC:DE:6D:20:D1:32:D1:E3:C4:0F:4F:F1:EB:8B:39:74:1E:1D:BA:B9:E0:0E:F8:11:31:CC:6B:02:03:01:00:01

```

Basic Constraints *IsCA: true*
Authority Key Identifier *95:1D:51:F9:FF:61:4D:DC:63:A1:8F:2E:C4:95:C7:22:56:33:72:53*
Authority Info Access *http://psc.sia.es/ac_raiz_2020.crt*
http://psc.sia.es/ocsp
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://psc.sia.es/
Extended Key Usage *id_kp_serverAuth*
CRL Distribution Points *http://psc.sia.es/arl2020.crl*
Subject Key Identifier *5B:58:D8:89:DC:DA:B8:55:32:64:4D:9B:B5:6C:27:9A:07:50:B9:6C*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *B1:02:3E:84:41:80:A7:25:4F:7C:0F:1A:D6:C6:5C:2D:CC:D5:9D:EF:38:80:01:C4:38:0B:CA:73:DB:F4:F3:38*

X509SubjectName

Subject CN: *SIA SSL SUB01 CA*
Subject 2.5.4.97: *VATES-A82733262*
Subject OU: *QUALIFIED CA*
Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*
Subject C: *ES*

X509SKI

X509 SK I*W1jYidzauFUyZE2btWwnmgdQuWw=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-09-03T02:00:00Z***24.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI**

[en]

*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication***24.4.2 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name**

[es]

*Certificados electrónicos cualificados de autenticación de sitios web expedido por «SIA SSL SUB01 CA»***Name**

[en]

*Qualified Certificates for Web Site Authentication issued by «SIA SSL SUB01 CA»***Service digital identities****X509SubjectName****Subject CN:***SIA SSL SUB01 CA***Subject 2.5.4.97:***VATES-A82733262***Subject OU:***QUALIFIED CA***Subject O:***SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA***Subject C:***ES***X509SKI****X509 SK I***W1jYidzauFUyZE2btWwnmgdQuWw=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2022-01-11T02:00:00Z*

Issuer C: *ES*

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Subject C: *ES*

Valid from: *Mon Sep 26 12:37:02 CEST 2022*

Valid to: *Fri Sep 26 13:07:02 CEST 2025*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:00:C7:33:C6:59:51:92:E4:9F:66:AF:D1:3A:67:D6:C6:46:D8:DD:59:9B:DD:89:9E:10:89:AE:BC:C3:18:51:92:EA:89:21:92:90:30:62:E4:C1:F0:12:82:99:AC:42:8C:1A:F3:F2:8E:AD:78:42:04:E8:2A:55:D0:27:8F:E6:CC:88:5D:7F:1E:70:E5:FB:D8:3E:AD:F1:1F:E2:DC:5D:6:3:2E:B0:90:42:4B:35:E7:46:58:DD:93:D7:16:97:7A:32:4F:11:1F:3D:55:FD:2B:10:94:AF:0F:3E:DE:63:5B:88:44:4D:20:CA:7F:36:B3:E0:A4:BB:BE:58:AB:C3:84:9B:87:5A:32:36:C0:EC:65:9A:41:89:AE:4D:04:1A:79:F8:58:DC:22:36:CD:95:00:23:9D:27:D7:A0:75:D3:9A:C9:0F:77:86:32:B7:39:A3:80:FB:28:CF:00:5F:EA:8E:C6:B1:5C:F5:AA:30:30:03:2A:38:C9:6C:F8:A4:FA:05:5E:A1:84:16:D6:6B:07:C1:89:C4:81:01:39:72:5F:2D:EA:71:F7:4B:00:CC:20:D9:B3:EA:3D:99:55:58:AB:CB:BE:34:F1:F6:23:DA:DC:AE:7E:10:90:63:05:33:18:4F:AS:25:9B:09:9F:AD:1C:31:82:7D:8B:E6:AA:04:0D:92:C2:0F:02:03:01:00:01*

Subject Alternative Name *OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE NIVEL MEDIO*

Extended Key Usage *id_kp_clientAuth*

Authority Info Access *https://psc.sia.es/ocsp*
https://psc.sia.es/ac_sub01.crt

Certificate Policies *Policy OID: 1.3.6.1.4.1.39131.10.1.12*
CPS pointer: https://psc.sia.es
CPS text: [Certificado cualificado de Sello Electrónico de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://psc.sia.es/crlc46.crl*
https://psc.sia.es/crlc46.crl

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Subject Key Identifier *A0:19:31:0A:1A:7D:CA:E3:54:60:E5:22:F6:D2:1B:F9:45:60:1E:30*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*

Thumbprint algorithm: *SHA-256*

Thumbprint: *68:17:1A:DD:9F:B5:E4:A8:DB:08:65:8D:17:8D:B1:1F:9A:17:C2:00:76:CF:7C:65:C
E:B7:37:C5:6C:E0:BA:7F*

X509SubjectName

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Subject C: *ES*

X509SKI

X509 SK I *oBkxChp9yuNUYOUi9tIb+UVgHjA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2025-10-02T02:00:00Z

24.5.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name [en] *Qualified electronic registered delivery service "SIAVAL 2022"*

Name [es] *Servicio cualificado de entrega electrónica certificada "SIAVAL 2022"*

Service digital identities**X509SubjectName**

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS S.A.*

Subject C: *ES*

X509SKI

X509 SK I *oBkxChp9yuNUYOUi9tIb+UVgHjA=*

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>	
Service type description	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name		
Name	[en]	Qualified timestamps issued by TSAQC 2022
Name	[es]	Sellos de tiempo cualificados emitidos por TSAQC 2022

Certificate fields details

Version:	3
Serial Number:	614817116171548320148179293635051900945888052447
X509 Certificate	-----BEGIN CERTIFICATE-----

Page 909

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Subject C: *ES*

Valid from: *Thu Nov 24 10:44:49 CET 2022*

Valid to: *Tue Jan 29 11:26:43 CET 2030*

Public Key:
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:AC:FF:8C:5B:EE:BE:FF:BF:E7:8A:24:0F:69:61:3B:0A:B7:01:EF:2A:A6:8D:94:E3:80:EC:CA:19:22:89:9F:8A:F2:18:C2:06:DE:A8:8B:53:52:55:34:4A:3A:5F:88:45:15:DA:04:A3:25:06:ED:4E:19:C2:E7:48:97:29:23:5D:CE:07:98:E3:79:7B:88:09:09:21:57:17:68:AE:6C:6E:F3:2A:29:C2:CC:A5:E0:30:4C:99:1E:40:DB:17:8F:8E:12:C1:BA:74:14:3B:E8:A8:88:08:68:70:34:27:1A:B4:C6:4E:95:18:B1:C8:50:3D:3D:A2:F5:99:63:7C:5C:22:43:44:D3:83:8D:C9:91:85:0D:CF:17:B2:2C:1C:97:86:78:DB:FB:57:00:D6:CE:2B:8A:7D:D5:57:45:E0:44:74:CC:5B:C4:26:94:B6:CB:49:34:58:4A:D2:91:1D:99:4C:0A:5A:FB:C7:09:FB:5C:CA:FC:58:5A:D1:C0:98:DF:D7:18:8F:EA:CD:06:CE:62:A0:4F:E5:68:EA:FA:0B:0D:62:43:34:61:69:BA:AC:E6:6D:67:3A:A1:00:AC:89:D8:44:13:37:91:82:8E:E2:C7:EB:37:26:EA:30:A2:EA:74:0F:78:C5:5B:C5:79:CE:A2:8A:87:63:4E:5B:74:4F:69:50:81:98:FC:B8:EC:8D:4F:84:3C:2E:8F:22:D0:42:9C:F5:98:C7:91:98:99:15:0C:4E:6E:62:4E:79:6F:7E:FC:42:04:83:35:AA:4F:AC:A5:67:F1:4D:56:5F:10:60:80:8F:54:DA:12:1E:5F:C7:D8:9D:7D:21:5F:C6:C2:14:61:7B:86:DE:26:32:33:0E:85:C8:2B:A7:B0:E8:6A:20:24:EF:BE:C8:56:95:61:7C:A2:59:2D:BD:85:95:34:F7:9C:BD:87:71:94:49:70:69:3A:C2:34:31:F4:7C:A4:46:42:A8:75:F7:7F:AA:20:66:AB:64:23:7F:63:47:51:93:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access
https://psc.sia.es/ocsp
https://psc.sia.es/ac_sub01.crt

Certificate Policies
Policy OID: 1.3.6.1.4.1.39131.10.1.25
CPS pointer: https://psc.sia.es
CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
http://psc.sia.es/crlc50.crl
https://psc.sia.es/crlc50.crl

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Subject Key Identifier *A8:CD:60:77:23:67:9B:2C:13:FE:FD:08:B9:36:A5:83:EE:90:C9:A8*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E8:F7:5A:D5:CE:08:97:D9:5A:FD:CA:AC:28:75:82:11:68:7E:A4:0D:3F:CE:D0:1C:80:6A:CA:08:5E:64:3D:1E*

X509SubjectName

Subject CN: *TSAQC 2022*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

X509 SK I *qM1gdyNnmywT/v0luTalg+6Qyag=*

Service status description	[en]	undefined.
	[es]	undefined.

24.7 - Service (granted): Qualified electronic registered delivery service SIAVAL 2025

Service type description	[en]	undefined.
	[es]	undefined.

Name	[en]	Qualified electronic registered delivery service SIAVAL 2025
Name	[es]	Servicio cualificado de entrega electrónica certificada SIAVAL 2025

Service digital identities

Certificate fields details

Version: 3

Serial Number: 394774150467396565075902420925279159915376419785

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: *SIA SUB01*

Issuer SERIAL NUMBER: *A82733262*

Issuer OU: *QUALIFIED CA*

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

Issuer C: *ES*

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Subject C: *ES*

Valid from: *Tue Jul 01 11:59:28 CEST 2025*

Valid to: *Sat Jul 01 11:59:28 CEST 2028*

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:D6:73:B9:FF:BA:09:88:BA:BA:CI:96:C0:0F:0A:9E:A0:E4:BE:48:5D:0D:60:97
:B0:56:B7:08:2D:C3:44:55:4A:98:7D:8A:34:47:D1:36:6D:6D:2B:1E:64:D4:84:EE:88:2B:88:8D:BC:CC:2C:ED:A5:1D:1C:7E:8B:8F:34:5C:6F:FC:A7:E2:3A:23:82:E8:06:8A:27:2E:CE:DA:B8
:FS:BC:FA:DF:F7:46:2D:E8:12:9E:2D:39:F2:D6:74:88:FF:B4:95:80:DF:39:35:0F:85:35:AB:DB:E1:59:40:08:43:22:97:D9:8F:BD:5C:A4:D2:C0:9A:E8:DF:E9:71:48:92:7B:64:F9:EF:D8:2C:C
D:6D:19:40:55:DE:7A:4B:87:CD:88:EF:E3:3A:AB:0E:4F:1D:09:87:23:70:79:C7:29:CA:1D:4C:CF:6C:AB:DF:7F:BC:B3:28:88:A8:31:E7:0D:83:85:C6:79:6F:FD:12:3E:5A:89:16:FF:A8:05:1B
:2D:56:17:98:8F:87:C3:4B:8B:9C:18:89:F0:0E:BF:7B:75:EB:1A:73:F7:FF:F6:52:A2:00:F0:E5:21:CC:85:30:DC:14:CE:8B:A5:A5:0B:FB:91:42:4E:61:89:23:59:90:F5:56:E2:94:DC:58:4C:A
2:5F:E6:07:E3:54:AD:FD:C2:C6:02:93:93:36:F3:92:11:86:AF:F7:37:58:64:41:5A:38:65:7B:55:4A:A2:D3:61:09:0E:86:F2:FB:0E:EE:F1:41:BB:F0:16:96:E4:25:AF:D1:25:D8:07:A0:D2:8B:
D2:11:C1:D9:EA:9E:D3:79:B1:F9:8F:63:0A:D6:E0:57:59:BA:99:20:57:70:09:78:F6:F5:CE:E3:90:A5:D8:A2:BF:DC:1C:C0:47:64:DE:18:3D:88:39:0A:23:5B:AC:A7:65:35:58:B8:9D:D1:D0:
1A:82:C3:04:61:C3:41:D5:19:77:2A:58:40:4F:56:82:FF:D8:AA:51:DC:E6:34:A8:47:CD:67:CC:45:02:03:01:00:01

Subject Alternative Name *OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE NIVEL MEDIO*

Extended Key Usage *id_kp_clientAuth*

Authority Info Access

https://psc.sia.es/ocsp

https://psc.sia.es/ac_sub01.crt

Certificate Policies

Policy OID: 1.3.6.1.4.1.39131.10.1.12

CPS pointer: https://psc.sia.es

CPS text: [Certificado cualificado de Sello Electrónico de nivel medio.

Condiciones de uso y vías de contacto en: https://psc.sia.es]

Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

http://psc.sia.es/crlc131.crl

https://psc.sia.es/crlc131.crl

Authority Key Identifier *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

Subject Key Identifier *FD:59:0B:9E:22:15:D7:53:BE:E0:3F:68:26:EF:20:9D:30:EF:62:4F*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5E:2E:97:AC:36:22:39:83:AC:0F:0C:74:97:54:C6:FC:0C:03:1A:86:2D:D3:1F:14:96:0E:F1:3B:06:DD:F8:75*

X509SubjectName

Subject CN: *SIAVAL*

Subject OU: *SELLO ELECTRONICO*

Subject 2.5.4.97: *VATES-A82733262*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Subject C: *ES*

X509SKI

X509 SK I */VkJnIlV11O+4D9oJu8gnTDvYk8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2025-10-02T02:00:00Z

24.8 - Service (granted): Qualified Certificates issued by SIA SUB01 2025**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by SIA SUB01 2025*

Name *[es]* *Certificados Cualificados emitidos por SIA SUB01 2025*

Service digital identities**Certificate fields details**

Version: *3*

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withECDSA*

Issuer CN: *SIA ROOT 2025*

Issuer 2.5.4.97: VATES-A82733262

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Issuer C: *ES*

Subject CN: *SIA SUB01 2025*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED*

Subject 0: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Subject C: *ES*

Valid from: *Fri Jun 06 12:36:43 CEST 2025*

Valid to: Thu Jun 01 12:36:43 CEST 2045

Public Key: 30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:B5:A1:EF:A9:15:78:3D:6D:F8:29:73:30:59:F6:29:DE:77:B1:84:09:2A:3D:BD:60:40:D9:0E:FC:F9:87:AF:41:49:8B:04:76:F7:69:CA:E4:D1:82:44:6C:F3:75:6C:CC:A9:A0:59:35:C3:79:33:BE:10:DA:2A:CA:EE:88:40:55:D9:3B:03:CF:68:5E:EA:E3:99:CF:DF:69:9A:26:5A:7A:4F:10:53:BF:FA:96:4A:D0:32:F6:ED:12:61:B1:51:6F

Basic Constraints *IsCA: true*

Authority Key Identifier 55:31:DE:31:B8:E5:65:AA:79:E8:50:A4:C0:98:6F:1B:6B:39:50:EE

Authority Info Access https://crl.sia.es/ac_root_2025.crt
<https://crl.sia.es/ocsp>

Certificate Policies *Policy OID: 2.5.29.32.0*
 CPS pointer: <https://psc.sia.es>

CRL Distribution Points http://crl.sia.es/arl_2025.crl
https://crl.sia.es/arl_2025.crl

Subject Key Identifier *C1:04:29:2D:D3:4F:A9:99:D7:61:FD:3B:03:15:D6:DD:6E:A8:CE:BF*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *59:B4:98:80:63:7B:4D:B1:99:07:7C:F0:E3:88:1B:35:43:56:40:6B:CA:19:14:71:E6:06:27:40:D8:D5:17:A2*

X509SubjectName

Subject CN: *SIA SUB01 2025*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Subject C: *ES*

X509SKI

X509 SK I *wQQpLdNPqZnXYf07AxXW3W6oz78=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-01-22T02:00:00Z*

24.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

24.8.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

24.8.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.18

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.13

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.39131.10.1.13.1

Description

Policy Identifier:

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>
Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>
Service Name		
Name	<i>[en]</i>	<i>Qualified electronic timestamps issued by TSAQC 2025</i>
	<i>[es]</i>	<i>Sellos cualificados de tiempo electrónicos emitidos por TSAQC 2025</i>

Certificate fields details

Version:	3
Serial Number:	385107211814017170181370972003920528646448171637
X509 Certificate	-----BEGIN CERTIFICATE-----

Signature algorithm:	SHA384withECDSA
Issuer CN:	SIA SUB01 2025
Issuer 2.5.4.97:	VATES-A82733262
Issuer OU:	QUALIFIED

Issuer O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Issuer C: *ES*

Subject CN: *TSAQC 2025*

Subject 2.5.4.97: *VATES-A82733262*

Subject OU: *QUALIFIED CA*

Subject O: *SISTEMAS INFORMATICOS ABIERTOS SAU*

Subject C: *ES*

Valid from: *Tue Jul 01 12:02:18 CEST 2025*

Valid to: *Fri Jun 29 12:02:18 CEST 2035*

Public Key:
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:F0:0B:9A:C0:88:B5:B5:32:8C:A2:E2:E7:A9:B4:1F:34:A1:5C:D6:F3:CF:15:F9:22:E0:FA:6D:6C:25:6A:F7:B5:1A:92:3C:F8:94:F1:9D:A6:AC:9B:78:90:8F:A7:02:07:D3:49:27:81:0E:1D:15:96:AC:16:A5:19:88:F5:94:23:82:11:4D:90:E7:EB:7C:73:7E:A1:1B:9B:94:D1:88:65:0E:27:CF:32:C3:73:4E:DC:FB:26:36:00:5D:E9:03:11:41:F6:CC:28:2A:AC:3E:A2:F3:1E:EC:B8:F6:63:C5:F7:9A:B7:BA:E9:32:81:2A:BE:4A:76:84:D9:2D:12:82:AB:21:58:BD:8F:CA:CF:86:16:C9:8A:03:AA:A7:FC:EB:85:F9:0D:67:C9:28:32:9F:98:67:A5:4D:14:EC:89:BB:A9:34:87:87:73:61:80:FA:CD:48:ED:11:8E:D7:54:F3:A9:A0:C4:7B:CC:03:5D:51:5C:8B:43:9E:7C:F8:51:28:12:9A:3D:77:BF:CC:55:F4:D1:8E:48:62:3F:F9:AD:18:02:1C:59:F5:56:0C:AF:AB:41:2A:8C:62:6F:D1:89:82:0C:60:49:6D:CF:6E:AA:E3:31:8B:15:19:61:6F:13:36:AA:8A:36:97:CA:81:E4:85:17:E4:91:DA:7C:5C:07:21:14:65:9C:D2:04:E5:0E:ED:76:89:8D:A7:96:F5:DD:9D:DD:10:35:A5:53:E6:73:30:FC:80:55:E8:49:DE:F8:1D:1D:D3:F6:86:F4:58:F6:98:AA:EF:83:C0:99:02:80:A6:4D:0A:DC:4B:91:AC:F6:1C:56:58:BA:4F:5E:38:4A:51:E2:54:6D:ED:7A:51:C4:90:B6:95:37:F3:30:80:09:F5:33:17:9A:C9:2D:87:45:F3:CF:93:F7:1F:2A:0D:20:2F:9D:26:02:34:1F:5D:A5:9B:69:06:79:06:E5:2F:60:2B:E4:43:7C:7D:BE:D5:8D:98:D4:AC:AF:EF:9B:DC:C9:FD:02:03:01:00:01

Authority Key Identifier *C1:04:29:2D:D3:4F:A9:99:D7:61:FD:3B:03:15:D6:DD:6E:A8:CF:BF*

Authority Info Access
https://crl.sia.es/ac_sub_2025.crt
https://crl.sia.es/ocsp

Certificate Policies
Policy OID: 1.3.6.1.4.1.39131.10.1.25
CPS pointer: https://psc.sia.es
CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es]
Policy OID: 0.4.0.2042.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points
http://crl.sia.es/crlc_2025_1.crl
https://crl.sia.es/crlc_2025_1.crl

Subject Key Identifier *2F:9F:B2:EB:E0:72:8B:EA:9E:1E:75:9C:3B:3A:6F:0B:76:EF:0C:D1*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E5:89:65:E4:48:95:83:D8:D6:9C:57:04:92:8E:16:04:6A:66:01:B4:4B:CE:DE:8C:31:3B:EA:70:7A:CD:6F:35*

X509SubjectName

Subject CN: TSAQC 2025

Subject 2.5.4.97: VATES-A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SAU

Subject C: ES

X509SKI

X509 SK I L5+y6+Byi+qeHnWcOzpvC3bvDNE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2026-05-20T03:00:00Z

25 - TSP: COLORIURIS, S.L

TSP Name

Name [en] *COLORIURIS, S.L*

Name [es] *COLORIURIS, S.L*

TSP Trade Name

Name [en] *Coloriuris, Prestador de Servicios de Confianza (CIPSC)*

Name [es] *Coloriuris, Prestador de Servicios de Confianza (CIPSC)*

Name [en] *VATES-B99091696*

Name [en] *Coloriuris S.L.*

PostalAddress

Street Address [en] *C/ Alfonso I nº 23, entresuelo centro*

Locality [en] *Zaragoza*

State Or Province [en] *Zaragoza*

Postal Code [en] *50003*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/ Alfonso I nº 23, entresuelo centro*

Locality [es] *Zaragoza*

State Or Province [es] *Zaragoza*

Postal Code [es] *50003*

Country Name [es] *ES*

ElectronicAddress

URI [en] *https://cipsc.coloriuris.net/*

URI [en] *mailto:info@coloriuris.net*

URI [es] *mailto:info@coloriuris.net*

URI	[en]	https://cipsc.coloriuris.net/

URI	[es]	https://cipsc.coloriuris.net/

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Name	[en]	Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física

Name [es] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Version: 3

Serial Number: 706445458326489759

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Zaragoza*
Issuer O: *Coloriuris S.L.*
Issuer OU: *Prestador de Servicios de Confianza*
Issuer SERIAL NUMBER: *B99091696*
Issuer CN: *CIPSC - Raíz de la Autoridad de Certificación*
Issuer E: *cipsc@coloriuris.net*
Subject C: *ES*
Subject L: *Zaragoza*
Subject O: *Coloriuris S.L.*
Subject OU: *Prestador de Servicios de Confianza*
Subject SERIAL NUMBER: *B99091696*
Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona física*
Subject E: *cipsc@coloriuris.net*
Valid from: *Tue Jul 14 12:15:10 CEST 2015*
Valid to: *Mon Jul 14 12:15:10 CEST 2025*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E3:3B:D0:77:B9:58:C8:80:54:90:5D:2E:AB:10:DB:DA:83:60:24:BA:D0:36:34:45:B1:A6:BA:5A:2B:D7:C1:85:1F:43:2A:13:70:C0:51:D3:00:E6:EC:09:FD:CC:BD:45:24:2A:26:90:C4:E7:AD:31:B3:DF:04:35:9C:98:9C:72:AB:75:B1:BA:FB:A2:1F:80:10:83:2E:CC:F8:13:54:1A:F7:27:AB:0A:0D:A6:C5:AB:47:B5:59:BA:E7:C3:53:37:41:ED:7A:59:39:43:FA:36:CD:88:16:4C:0E:99:A5:7F:32:05:6E:F9:70:F3:E4:C8:EA:23:D5:73:30:E3:67:8C:3B:44:1E:5E:0A:D9:47:F5:28:5D:1F:AC:98:EB:64:85:32:E3:E3:C7:02:10:88:D8:47:51:CB:D1:8F:9F:96:AF:5B:08:B1:41:3E:47:18:61:BA:52:05:DF:DA:CC:FB:F4:AD:BF:D8:63:6B:7B:42:08:C4:6C:A7:32:BB:62:99:94:4F:C4:19:54:F1:A4:08:93:C0:E4:39:60:4B:A4:C9:E7:63:C9:2F:93:12:40:E8:2D:B4:B5:90:26:78:5A:40:51:73:40:43:A5:96:8B:EE:F7:03:1C:3F:87:A5:7A:FD:A4:3B:90:45:90:21:C9:90:CF:65:88:43:22:F7:93:0D:55:02:03:01:00:01*
Authority Info Access *<https://cipsc.coloriuris.net/certificados/ac/raiz.crt>
<https://ocsp.coloriuris.net>*
Subject Key Identifier *02:E9:6A:2F:B2:05:D3:1B:63:FB:3C:C0:C5:92:6A:0B:FF:2D:83:29*
Basic Constraints *isCA: true*
Authority Key Identifier *79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6*
Certificate Policies *Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0*
CPS text: [SubAutoridad CIPSC para emisión de certificados de firma electrónica para persona física]
CPS pointer: <https://cipsc.coloriuris.net/politicas/>

CRL Distribution Points<https://cipsc.coloriuris.net/crl/ac/ac.crl>

CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de
Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de
Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

D8:23:77:C5:2B:28:D8:A9:39:40:35:B2:8B:71:3A:62:1C:C0:49:DA:5E:BC:D1:7F:F
9:A3:8C:5F:25:EA:1A:6D

X509SubjectName**Subject C:**

ES

Subject L:

Zaragoza

Subject O:

Coloriuris S.L.

Subject OU:

Prestador de Servicios de Confianza

Subject SERIAL NUMBER:

B99091696

Subject CN:

CIPSC - Subautoridad de emisión de certificados de persona física

Subject E:

cipsc@coloriuris.net

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2017-07-01T22:00:00Z

25.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**25.1.2 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name

[en]

Qualified Certificates issued by - CIPSC - Subautoridad de emisión de
certificados de persona física

Name [es] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona física*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SK I *AulqL7IF0xtj+zzAxZJqC/8tgyk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

25.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física*

Name [es] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona física*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SK I *AulqL7IF0xtj+zzAxZJqC/8tgyk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-10-19T22:00:00Z*

25.2 - Service (withdrawn): Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Name [es] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *3581065887593727996*

Authority Info Access	<i>https://cipsc.coloriuris.net/certificados/ac/raiz.crt</i> <i>https://ocsp.coloriuris.net</i>
Subject Key Identifier	<i>35:7F:37:8F:21:EE:4F:0A:68:00:7A:A7:A2:41:B1:E1:95:3A:D1:AE</i>
Basic Constraints	<i>IsCA: true</i>
Authority Key Identifier	<i>79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0</i> <i>CPS text: [SubAutoridad CIPSC para emisión de certificados para sello electrónico de persona jurídica]</i> <i>CPS pointer: https://cipsc.coloriuris.net/politicas/</i>
CRL Distribution Points	<i>https://cipsc.coloriuris.net/crl/ac/ac.crl</i> <i>CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>2B:03:88:BB:3A:37:32:FD:55:1B:21:BE:FE:2F:6D:6C:18:D0:FC:76:20:BD:31:EC:C3:4F:71:43:7F:DE:B2:E7</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Zaragoza</i>
Subject O:	<i>Coloriuris S.L.</i>
Subject OU:	<i>Prestador de Servicios de Confianza</i>
Subject SERIAL NUMBER:	<i>B99091696</i>
Subject CN:	<i>CIPSC - Subautoridad de emisión de certificados de persona jurídica</i>
Subject E:	<i>cipsc@coloriuris.net</i>

Service Status

Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time *2017-07-01T22:00:00Z*

25.2.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.1.2.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.1.2.2

25.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

25.2.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica

Name [es] Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica

Service digital identities

X509SubjectName

Subject C: ES

Subject L: Zaragoza

Subject O: Coloriuris S.L.

Subject OU: Prestador de Servicios de Confianza

Subject SERIAL NUMBER: B99091696

Subject CN: CIPSC - Subautoridad de emisión de certificados de persona jurídica

Subject E: cipsc@coloriuris.net

X509SKI**X509 SK I***NX83jyHuTwpoAHqnokGx4ZU60a4=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2016-06-30T22:00:00Z***25.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAsURN]	<i>urn:oid:1.3.6.1.4.1.37799.20.1.2.1</i>

Policy Identifier:

Identifier	[OIDAsURN]	<i>urn:oid:1.3.6.1.4.1.37799.20.1.2.2</i>

25.2.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

25.2.4 - History instance n.2 - Status: undersupervision**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name**

Name	[en]	<i>Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica</i>

Name	[es]	<i>Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica</i>

Service digital identities**X509SubjectName**

Subject C:	<i>ES</i>

Subject L:	<i>Zaragoza</i>

Subject O: *Coloriuris S.L.*

Subject OU: *Prestador de Servicios de Confianza*

Subject SERIAL NUMBER: *B99091696*

Subject CN: *CIPSC - Subautoridad de emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SK I *NX83jyHuTwpoAHqnokGx4ZU60a4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-10-19T22:00:00Z*

25.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.37799.20.1.2.1</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.37799.20.1.2.2</i>

25.3 - Service (withdrawn): Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Certificate fields details

```
Version: 3
Serial Number: 4580114715082243801
```

X509 Certificate

[illegible]

Signature algorithm:	SHA256withRSA
Issuer C:	ES
Issuer L:	Zaragoza
Issuer O:	Coloriuris S.L.
Issuer OU:	Prestador de Servicios de Confianza
Issuer 2.5.4.97:	VATES-B99091696
Issuer CN:	CIPSC - Raíz - Autoridad de Certificación
Issuer E:	cipsc@coloriuris.net
Subject C:	ES
Subject L:	Zaragoza
Subject O:	Coloriuris S.L.
Subject OU:	Prestador de Servicios de Confianza
Subject 2.5.4.97:	VATES-B99091696

Subject CN: *CIPSC - Emisión de certificados de persona jurídica*
Subject E: *cipsc@coloriuris.net*
Valid from: *Thu Sep 10 10:13:25 CEST 2015*
Valid to: *Wed Sep 10 10:13:25 CEST 2025*
Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:05:DD:CD:66:3F:EC:C7:90:32:CB:9E:73:C4:33:3D:80:0F:A1:7A:79:C4:31:23:4D:60:43:DA:A6:4B:C3:19:7E:E9:D8:7A:81:C2:10:83:D0:F3:9A:76:7E:80:13:E5:14:82:33:A2:8F:8C:52:C7:B3:6B:D7:55:87:FE:D4:B3:7F:AD:43:A0:F6:33:94:32:A5:57:53:7E:A7:CC:8D:C2:69:F5:8E:A6:A6:CB:80:5C:9A:04:EF:46:B1:5F:DC:E0:3A:93:B4:F5:A1:16:04:E9:14:80:7D:28:B9:2A:3D:46:79:24:9C:21:DC:BB:C3:64:C5:82:A0:68:42:EA:FE:0E:9B:55:17:BE:C7:D5:2D:08:27:0B:C4:BA:97:09:70:A9:29:3C:85:E9:09:3E:CD:AE:D5:08:CF:4C:50:F2:CF:F1:E2:F4:37:4A:40:9B:3C:25:35:DA:7B:45:DD:74:D6:54:06:CB:84:FC:F0:C7:79:29:F2:B6:AB:C5:9C:49:1C:5D:98:30:D6:48:CC:A0:08:C7:96:CE:FB:1F:7E:B9:8B:2B:2F:57:CD:A2:E6:FE:DB:3E:3B:89:10:E2:FE:70:A1:5A:91:6E:4D:6F:4D:8B:28:21:8C:74:98:1A:69:66:AB:50:E7:C8:1E:DA:A2:26:EF:E3:0D:23:9B:D4:19:E2:06:2A:D8:02:03:01:00:01
Authority Info Access
https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt
https://ocsp.coloriuris.net
Subject Key Identifier
7B:21:D2:FB:DA:8B:81:0D:06:3F:4F:8A:6B:7C:C9:A7:DE:5C:95:7B
Basic Constraints
IsCA: true - Path length: 2
Authority Key Identifier
56:0E:2D:3E:8C:F4:9F:C3:BF:7E:2B:E7:A7:BD:1B:53:14:01:28:EA
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://cipsc.coloriuris.net/politicas/
CRL Distribution Points
https://cipsc.coloriuris.net/crl/ac/ac-v3.crl
CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Certificación,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES
Key Usage:
keyCertSign - cRLSign
Thumbprint algorithm:
SHA-256
Thumbprint:
55:01:5F:B9:D2:CD:21:76:57:32:A2:34:0E:53:E4:18:4F:0C:0D:57:F7:6E:3B:4F:08:03:B6:C1:56:FF:BB:1E
X509SubjectName
Subject C: *ES*
Subject L: *Zaragoza*
Subject O: *Coloriuris S.L.*
Subject OU: *Prestador de Servicios de Confianza*
Subject 2.5.4.97: *VATES-B99091696*
Subject CN: *CIPSC - Emisión de certificados de persona jurídica*
Subject E: *cipsc@coloriuris.net*

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2017-07-01T22:00:00Z

25.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.2

25.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

25.3.3 - History instance n.1 - Status: granted**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name [en] Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica

Name [es] Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica

Service digital identities**X509SubjectName**

Subject C: ES

Subject L: Zaragoza

Subject O: Coloriuris S.L.

Subject OU: *Prestador de Servicios de Confianza*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - Emisión de certificados de persona jurídica*

Subject E: *cipsc@coloriuris.net*

X509SKI

X509 SKI *eyHS+9qLgQ0GP0+Ka3zJp95cIXs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

25.3.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.37799.20.2.2.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.37799.20.2.2.2*

25.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

25.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*

Name [es] *Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica*

Service digital identities

X509SubjectName

Subject C: ES

Subject L: Zaragoza

Subject O: Coloriuris S.L.

Subject OU: Prestador de Servicios de Confianza

Subject 2.5.4.97: VATES-B99091696

Subject CN: CIPSC - Emisión de certificados de persona jurídica

Subject E: cipsc@coloriuris.net

X509SKI

X509 SK I eyHS+9qLgQ0GP0+Ka3z/p95cIXs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2015-10-19T22:00:00Z

25.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.1

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.2

25.4 - Service (withdrawn): Qualified timestamps issued by Coloriuris (TSACI)

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3 - Emisor de sellos de tiempo de 2048*

Valid from: *Tue Jul 04 18:27:29 CEST 2017*

Valid to: *Sun Jul 04 18:27:29 CEST 2027*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AD:F1:21:3A:DC:B3:C4:12:81:19:79:CE:89:BA:74:9E:FC:EC:FC:99:02:39:90:37:EF:66:D6:54:5F:5D:82:CA:7D:13:08:6D:13:1C:38:64:32:1E:D2:E7:B6:17:A6:72:8F:D9:0F:7F:69:F8:68:8C:49:87:CD:E2:6D:88:2E:48:0D:62:8A:F0:C5:F2:2F:68:7A:CF:11:E5:D3:93:AC:09:45:E1:93:3D:12:C9:E5:44:85:AA:2A:C7:7D:8E:02:6C:91:3B:2C:E4:E8:6E:87:CC:DF:1F:D8:80:FC:5F:E4:02:DD:30:79:07:AA:E8:80:49:D8:03:EA:31:94:E5:35:33:DC:32:B7:B6:5D:C3:ED:67:17:FE:CE:1A:48:71:92:90:4B:AC:05:F7:5C:C4:6F:45:44:12:18:A8:91:32:7F:4B:60:A0:65:1E:6B:2E:64:18:9F:F1:75:D6:40:6D:7D:6C:3D:C7:F7:00:F9:F4:99:BE:F8:F8:77:BF:21:12:CF:5D:15:01:7F:18:34:17:32:FC:D5:57:21:27:64:76:9F:A2:33:58:EA:67:14:D8:0D:C3:42:77:F2:42:53:48:86:8E:B3:8A:F9:6C:4D:05:B3:00:28:13:33:46:00:5F:ED:3D:44:18:24:F3:4B:6D:F7:E4:4F:67:40:4F:4E:28:B9:D7:02:03:01:00:01*

Authority Info Access *https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt*
https://ocsp.coloriuris.net

Subject Key Identifier *60:62:82:B7:28:58:B6:EF:BA:9C:7B:7F:BA:73:08:34:81:88:01:CB*

Authority Key Identifier *67:FF:D4:BC:47:58:FF:3C:0A:89:AF:9D:B0:2A:EF:FC:02:5C:2A:5A*

Certificate Policies *Policy OID: 1.3.6.1.4.1.37799.20.5.1*
CPS text: [Certificado cualificado de emisión de sellos de tiempo electrónicos]
CPS pointer: https://cipsc.coloriuris.net/politicas/

CRL Distribution Points *http://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl*
CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D8:9C:1C:4E:94:77:B4:76:8B:1C:46:F7:E1:61:29:54:1C:CD:E1:99:51:A4:91:2A:F6:57:43:E7:BD:55:13:BE*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3 - Emisor de sellos de tiempo de 2048*

X509SKI

X509 SK I *YGK CtyhYtu+6nHt/unMINIGIAcs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-10-24T00:00:00Z*

25.4.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified timestamps issued by Coloriuris (TSACI)*

Name *[es] Sellos de tiempo cualificados emitidos por Coloriuris (TSACI)*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3 - Emisor de sellos de tiempo de 2048*

X509SKI

X509 SK I *YGK CtyhYtu+6nHt/unMINIGIAcs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-09-27T10:00:00Z*

25.5 - Service (granted): Qualified timestamps issued by Coloriuris (TSACI) v3.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by Coloriuris (TSACI) v3.1
Name	[es]	Sellos de tiempo cualificados emitidos por Coloriuris (TSACI) v3.1

Service digital identities

Certificate fields details

Version:	3
Serial Number:	7842311533657933281

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIVCCBJ+gAwIBAgILbNV8yh2hReEwDQYJKoZIhvcNAQENBQAwgeUxizAhBgkqhkiG9w0BCQEW
FGNpcHNjOGVubG9yaXVyaXMubmV0MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZGFK
IGRlRlNlGxhZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
A1UECwwuUHJlc3RhZG9yIGRlRlNlcnZpY2lcyBkZSBD625maWuemExGDAWBgNVBAoMD0NvbG9y
aXVyaXNjOGVubG9yaXVyaXMubmV0MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZGFK
WV0xOTI4MDQwITEuZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
ZWxs63MgZWx3Y3RyY25pY29kZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
YQwPvKfURVMTQjK5MDkxNjZMRGwFgYDVQODDA9D62xvcml1cmZlZmF1TC4xETAPBgNVBACMFph
cmFnb3p1h0wQwQYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZGFKIGRlRlNlGxhZG9uZG9u
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
SnrRQBM7HGlq8oz3qek8KaamJduYGUjGDMisukHnNy001DsPpm+iffpe/fdMLV/ZCHRunyIKom
ADcm634fPU4muExMbwxyFWDSh0l+O35vrtHPa70xPp+PxnCpHX0H0FmUv4zS21lqMvVBKdMYeY
SH8SLMcmB8RrS0A9vO6f0lprx+0uZsUe7XLNRotBIS06XmYdLcgcCtoz9BIMba03rtXtpV6
IREB0K9IRem1o4h79UUXKn7NrghJlQfwhngZqZc5NfrYhRRTWTU0e100c/9508VgwJNaVQha
TVkc6b7qHdHN0WkuTk2jRxf5zfe/wECaWEAAOCA0lwggM+M8BGA1UdlwQYMBaAFBG8NTz17Bmm
DmBdf1GgE4dJwFqMlCbggrBGFBOcCARYnaHR0cHM6Lg9aBzY55jb2xvcml1cmZlZmF1TC4xETAP
Y29s63JpdXJpcy5uZXVyaXVyaXMubmV0MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3Jp
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
hhdH0dHRwczovL29kZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
JXQFATC80DAcBggrBGFBOcCARYnaHR0cHM6Lg9aBzY55jb2xvcml1cmZlZmF1TC4xETAP
YXNjOGVubG9yaXVyaXMubmV0MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZGFK
a0BzAGkAbwBuAAcAAZABIAcAacwBIAgABwABwAHMAIAIAgAAZABIAcAacwBIAgABwABwAHMA
AGMA0BIAgABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABwABw
CgYIKwYBBQUHAwwgYQYIKwYBBQUHAQMEGTAXMBUCCGSAQUFBwCMAKGBwQAI+XIAQlwggE1BgNV
HR8EGGSMIBKDDCA5SgNKAyhBodHRwOiBvY2lwc2MuY29s63JpdXJpcy5uZXVyaXVyaXMubmV0
MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
IHYzLjEgGDAWBgNVBGEML2BVEYTLUI5OTA5MTY5NjEsMCoGA1UECwwuUHJlc3RhZG9yIGRlRlNl
cnZpY2lcyBkZSBD625maWuemExGDAWBgNVBAoMD0NvbG9yaXVyaXNjOGVubG9yaXVyaXMubmV0
MTtwOgYDVQODDDND5BTOyAtIFhw616lC0gQXV0b3JpZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
ZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9uZG9u
WmFyYWdvemExCzAIBGNVBAYTAKVTMB0GA1UdDgQWBRR+Wtse754TYIQ77CPV5qeyQCRDAOBgNV
HQ8BAfBEAMCBsAwDQYJKoZIhvcNAQENBQADggIBABgP5ZHyppPetPHCIK5YIYH5TxAJ+OmrZK
NpsoeEHE7q5W9w9wAFNwF8b9VdZx7nb+87YfMgic1DlNlVnQOLc2FAW3GDKyqZ53oAD8
XI46b7UESMYar3/n05va6Rdr5+EuxTQjg9bCx205mtMVL8ISNultBxEe3YDkjljhcV07d
uPTndqoCk/G+h5s5I9c18snBy16EADIMGlaUyX0follvkP3RzvOwU6LmPqyWjgkRemw57wE
j5RMT/+Ug034IRPZ23vDlJgDpQwAw3BU127vaR90CqllhlicCpwlfrfclU6OL59p:
hIHveL05bTh82Ch+UID5IW0vZTqkqzrqXqKNvhtG5H9Ant+17o/hKjuOsn7IAUZ7yIR4/8ZnocM
7y4HdLaRj++xZsRjILqoeNzzWYA+T+CVHT0oOKFuowKnNWUP0FNcxatYqzYEV268E19v2XRXdk
Vn7nKM9dITsrrLj5w6zoe2urBjCCRNpK66E/vLRLU6/GzCMGc5Klnubz424Zk96hTJUOS
01mcd/qDNDsNSKhdMz+V3B84gdepev1sja+I5Vjb25pk8XgMXgX03+oNqsU6nuhIOBzEU3dlqfiE
K81HlGJWqYW0B6zank+B24fZXyGeCe+1IKUsr9ma
-----END CERTIFICATE-----
```

Signature algorithm:	SHA512withRSA
Issuer C:	ES
Issuer L:	Zaragoza
Issuer O:	Coloriuris S.L.
Issuer OU:	Prestador de Servicios de Confianza
Issuer 2.5.4.97:	VATES-B99091696
Issuer CN:	CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1
Issuer E:	cipsc@coloriuris.net
Subject C:	ES
Subject L:	Zaragoza
Subject O:	Coloriuris S.L.
Subject 2.5.4.97:	VATES-B99091696

Subject CN: *CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048*

Valid from: *Fri Apr 06 13:35:35 CEST 2018*

Valid to: *Wed Apr 05 13:35:35 CEST 2028*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:C0:9A:9F:A6:4A:77:EB:40:13:3B:1C:68:AA:F2:8C:F7:A9:E9:3C:28:06:A6:8D:D8:98:19:48:E0:18:33:25:82:E2:87:9C:DC:B4:3B:50:EC:3E:99:BE:89:F1:69:78:F1:5D:7C:C2:D5:FD:97:07:46:E9:F2:94:A3:A6:00:30:A6:E8:7E:2B:3D:4E:26:B8:45:F1:31:BC:31:C8:55:B3:4A:1D:08:F8:ED:D2:BE:B1:C8:3D:AE:CE:C4:FA:7E:3F:19:C2:A4:75:F4:1F:41:62:9D:4B:F8:CD:26:65:D6:A3:2F:54:12:9D:31:8B:58:48:70:5E:48:83:06:98:1A:11:AD:22:1B:03:D8:CE:E9:F3:A5:A4:9A:F1:F8:47:59:B1:49:C4:ED:72:CD:46:8B:41:85:23:BA:5E:66:1D:2D:C8:1E:0A:D3:B3:80:19:4C:6D:A0:F7:07:14:71:4E:95:7A:95:11:3C:0C:AF:65:45:E9:B5:A3:88:7B:F5:45:17:2A:7E:CD:AE:A8:49:21:07:F0:AE:58:67:AB:F6:6A:65:CE:4D:21:FF:D8:85:14:53:59:35:34:7B:53:B4:73:FF:6C:D3:C5:46:C2:33:5A:55:08:5A:4D:59:1C:E9:BE:EA:1D:D1:CD:D1:62:AE:4E:4D:89:89:1C:5F:E7:37:DE:FF:01:02:03:01:00:01*

Authority Key Identifier *11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A*

Authority Info Access *https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt*
https://ocspv3.coloriuris.net

Certificate Policies *Policy OID: 1.3.6.1.4.1.37799.20.5.1*
CPS pointer: https://cipsc.coloriuris.net/politicas/
CPS text: [Certificado de emisión de sellos electrónicos cualificados de tiempo]

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl*
CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

Subject Key Identifier *7E:5A:DB:1E:ED:2E:13:B5:89:50:AC:5E:C2:3D:54:AA:7B:23:82:AC*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6C:17:A0:5F:0C:77:B9:6A:B0:39:A3:F8:50:58:73:1E:EB:02:F5:2F:B6:6D:87:D1:9B:93:D2:27:8D:82:64:99*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza*

Subject O: *Coloriuris S.L.*

Subject 2.5.4.97: *VATES-B99091696*

Subject CN: *CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048*

X509SKI

X509 SK I *flrbHu0uE7WJUKxewj1Uqnsjgqw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time	2018-05-24T00:00:00Z

26 - TSP: UANATACA, S.A

TSP Name

Name *[en]* *UANATACA, S.A*

Name *[es]* *UANATACA, S.A*

TSP Trade Name

Name *[en]* *UANATACA*

Name *[es]* *UANATACA*

Name *[en]* *UANATACA S.A.*

Name *[en]* *VATES-A66721499*

Name *[en]* *Uanataca S.A.*

PostalAddress

Street Address *[en]* *Avda. Meridiana núm 350 Planta 3*

Locality *[en]* *Barcelona*

State Or Province *[en]* *Barcelona*

Postal Code *[en]* *08027*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Avda. Meridiana núm 350 Planta 3*

Locality *[es]* *Barcelona*

State Or Province *[es]* *Barcelona*

Postal Code *[es]* *08027*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:info@uanataca.com*

URI *[en]* *http://www.uanataca.com*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

Valid from: *Fri Mar 11 11:35:33 CET 2016*

Valid to: *Sun Mar 11 11:35:33 CET 2029*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DF:FD:D8:93:CC:EF:C8:B1:26:D9:E7:1A:42:D9:F3:11:BB:08:41:CD:F4:E8:AB
C1:B1:71:CC:3F:04:66:96:05:6E:1B:C2:5A:09:1F:0F:6F:80:40:5D:63:86:BF:C8:B9:C8:DF:79:20:87:E9:89:22:BC:BC:DD:C6:26:6E:45:31:F8:FF:66:F4:06:C8:35:1F:D6:E1:05:BD:D0:B
3:AF:09:FD:7A:F1:1E:6F:DC:17:FC:22:42:91:8C:B3:5B:CC:6F:35:56:8E:00:B9:42:36:36:45:93:BC:1A:BF:F2:F3:54:45:E2:BC:1F:8F:D3:7B:1C:6A:B2:D0:D5:03:B6:8D:CD:1A:23:DB:39:93:
2C:F4:34:0A:DD:0E:4C:8B:AB:FF:36:5B:FA:F7:F5:89:9F:EF:41:45:1B:0A:CD:01:DB:1E:6E:76:7A:74:6B:09:A5:FC:3B:AD:C1:4A:1A:B3:ED:BC:70:61:E2:D7:3A:53:D8:E1:4E:B8:08:39:1D:3
8:EB:8D:EA:82:F0:38:9F:E7:1E:21:E7:EA:FD:F6:82:1F:F9:5D:F8:4C:02:0E:D1:A0:A2:09:11:92:D8:F8:93:74:8D:1B:71:77:6E:AD:AB:95:D3:F4:3A:2B:84:62:BF:09:36:34:AC:97:E4:24:B7:
7C:C2:FD:55:76:07:E3:D5:21:A9:10:7E:DF:AB:8F:34:37:49:71:05:24:04:FF:86:FE:DD:17:31:50:CD:23:03:99:1C:68:80:D3:27:D4:4A:88:0F:49:C7:45:C9:66:09:94:2B:79:F0:92:64:25:7A
:76:00:D5:98:99:D6:6F:40:A2:10:F1:A5:1D:79:E1:28:73:AD:06:03:4E:FA:DE:30:FE:AB:88:59:01:5C:30:EC:9E:35:0E:CB:BD:0C:D3:78:CE:23:EE:AF:3D:24:67:1D:DF:F1:F8:CE:D0:8A:3E
B9:83:DC:B7:2F:C1:6C:78:D1:CA:D5:99:D0:3A:08:22:3F:4B:E5:7C:35:82:5A:87:61:91:41:70:81:FD:04:E8:55:19:E6:E6:79:A6:86:67:2F:F1:C1:B4:DF:4D:2A:1A:44:62:07:81:ED:ES:67:0
B:3F:93:2B:34:C8:36:56:E0:44:DD:35:64:78:0E:72:A6:F6:03:4C:D0:F1:A6:E6:FE:A7:52:DA:80:F1:88:29:A3:0C:A8:C3:72:D6:60:86:85:1A:5F:46:4C:7B:4B:BE:3F:EE:B1:97:1B:23:B3:56:
20:63:60:4B:D4:70:F6:D9:83:CA:2F:E0:B5:BC:EE:57:2F:47:B8:D5:ED:54:B9:25:55:F8:58:25:B0:CE:7A:FE:E4:4A:C3:49:27:C1:5C:B7:C0:53:80:DC:73:02:03:01:00:01

Authority Info Access
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <http://www.uanataca.com/public/pki/dpc/>
CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver <http://www.uanataca.com/public/pki/dpc/>]

CRL Distribution Points
http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *35:A9:92:84:A2:20:78:9B:A0:E0:62:EE:FF:1B:5F:2F:74:BE:43:75:44:69:97:7C:B3:18:C7:C8:6A:D4:8F:9F*

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2019-10-28T01:00:00Z

26.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

26.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

26.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.47286.1.1.6*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.47286.1.1.6.2*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.2.6.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.3.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.4.6.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.7.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.8.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.9.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.11.6

Description**26.1.4 - History instance n.1 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] *Qualified Certificates issued by UANATACA CA1 2016*

Name [es] *Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: VATES-A66721499

Subject CN: UANATACA CA1 2016

Subject OU: TSP-UANATACA

Subject O: UANATACA S.A.

Subject L: Barcelona (see current address at www.uanataca.com/address)

Subject C: ES

X509SKI

X509 SK I LXHvsGN/9f3ggyJEf0QQMIFPTeU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-06-24T00:00:00Z

26.1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

26.1.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

26.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAAsURN] urn:oid:1.3.6.1.4.1.47286.1.1.6

Policy Identifier:

Identifier [OIDAAsURN] urn:oid:1.3.6.1.4.1.47286.1.1.6.2

Policy Identifier:

Identifier [OIDAAsURN] urn:oid:1.3.6.1.4.1.47286.1.2.6.2

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.3.6</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.4.6.2</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.7.6</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.8.6</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.9.6</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47286.1.11.6</i>
Description		

26.1.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA1 2016*

Name *[es]* *Certificados Reconocidos emitidos por UANATACA CA1 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SKI *LXHvsGN/9f3ggyJEf0QQMIFPTeU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-02-15T01:00:00Z*

26.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.1.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.47286.1.1.6.2*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.47286.1.2.6.2*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.47286.1.3.6*

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.47286.1.4.6.2*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.7.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.8.6

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47286.1.9.6

Description**26.1.6 - History instance n.3 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by UANATACA CA1 2016

Name [es] Certificados Reconocidos emitidos por UANATACA CA1 2016

Service digital identities**X509SubjectName**

Subject 2.5.4.97: VATES-A66721499

Subject CN: UANATACA CA1 2016

Subject OU: TSP-UANATACA

Subject O: UANATACA S.A.

Subject L: Barcelona (see current address at www.uanataca.com/address)

Subject C: ES

X509SKI

X509 SK I LXHvsGN/9f3ggyJEf0QQMIFPTeU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

26.1.6.7 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.3.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.3.2

26.1.6.8 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

26.1.7 - History instance n.4 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by UANATACA CA1 2016

Name [es] Certificados Reconocidos emitidos por UANATACA CA1 2016

Service digital identities**X509SubjectName**

Subject 2.5.4.97: VATES-A66721499

Subject CN: UANATACA CA1 2016

Subject OU: TSP-UANATACA

Subject O: UANATACA S.A.

Subject L: Barcelona (see current address at www.uanataca.com/address)

Subject C: ES

X509SKI

X509 SK I

LXHvsGN/9f3ggyJEf0QQMIFPTeU=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2016-06-14T22:00:00Z

26.1.7.9 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[OIDsURN]

urn:oid:1.3.6.1.4.1.47286.1.3.1

Policy Identifier:

Identifier

[OIDsURN]

urn:oid:1.3.6.1.4.1.47286.1.3.2

26.2 - Service (granted): Qualified Certificates issued by UANATACA CA2 2016

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en]

Qualified Certificates issued by UANATACA CA2 2016

Name

[es]

Certificados Cualificados emitidos por UANATACA CA2 2016

Service digital identities**Certificate fields details**

Version:

3

Serial Number:

2317042835735686419

Subject Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.uanataca.com/public/pki/dpc/
CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver http://www.uanataca.com/public/pki/dpc/]

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl*
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *00:FF:2F:F2:EF:BA:98:C6:B0:23:AD:10:35:55:9A:60:6D:D9:FC:48:A3:9D:34:07:C
C:07:A6:78:37:9A:79:09*

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA2 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time*2019-12-16T01:00:00Z***26.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.2.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

26.2.3 - History instance n.1 - Status: withdrawn

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by UANATACA CA2 2016

Name	[es]	Certificados Reconocidos emitidos por UANATACA CA2 2016

Service digital identities**X509SubjectName**

Subject 2.5.4.97:	VATES-A66721499

Subject CN:	UANATACA CA2 2016

Subject OU:	TSP-UANATACA

Subject O:	UANATACA S.A.

Subject L:	Barcelona (see current address at www.uanataca.com/address)

Subject C:	ES

X509SKI

X509 SK I	fVfnYHPOB0ap4qNo8OERsnSSc/0=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Status Starting Time	2018-02-15T01:00:00Z

26.2.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

26.2.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA2 2016*

Name *[es]* *Certificados Reconocidos emitidos por UANATACA CA2 2016*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA2 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SK I *fVfnYHPOB0ap4qNo8OERsnSSc/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

26.2.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.2.5 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Qualified Certificates issued by UANATACA CA2 2016*

Name [es] *Certificados Reconocidos emitidos por UANATACA CA2 2016*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA2 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at www.uanataca.com/address)*

Subject C: *ES*

X509SKI

X509 SK I *fVfnYHPOB0ap4qNo8OERSnSSc/0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-14T22:00:00Z*

26.3 - Service (withdrawn): Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA - TSU01

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA - TSU01*

Name [es] *Sellos de tiempo cualificados emitidos por Sello cualificado de tiempo electrónico de UANATACA - TSU01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1067299580870664226*

Authority Info Access	<i>http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt http://ocsp1.uanataca.com/public/pki/ocsp/ http://ocsp2.uanataca.com/public/pki/ocsp/</i>
Subject Key Identifier	<i>ED:FF:D4:0E:4D:9C:97:96:3E:A1:CB:26:51:0F:3F:28:A0:61:DB:59</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.47286.1.5 CPS pointer: https://www.uanataca.com/public/cps/ CPS text: [Certificado de sello cualificado de tiempo electrónico.] Policy OID: 0.4.0.194112.1.3</i>
CRL Distribution Points	<i>http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
Subject Alternative Name	<i>info@uanataca.com</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>F7:E7:B3:C0:34:02:2E:9F:DD:3E:B2:BD:62:6A:B1:9F:E3:BF:56:D8:DB:20:D6:22:B3:13:17:6D:81:D2:9E:B5</i>

X509SubjectName

Subject 2.5.4.97:	<i>VATES-A66721499</i>
Subject CN:	<i>Sello cualificado de tiempo electrónico de UANATACA - TSU01</i>
Subject OU:	<i>TSP-UANATACA</i>
Subject O:	<i>UANATACA S.A.</i>
Subject L:	<i>Barcelona</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>7f/UDk2cl5Y+ocsmUQ8/KKBh21k=</i>

Service Status

Service status description [en]	<i>undefined.</i>
<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>	

[es] undefined.

Status Starting Time 2025-06-10T00:00:00Z

26.3.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [en] Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA - TSU01

Name [es] Sellos de tiempo cualificados emitidos por Sello cualificado de tiempo electrónico de UANATACA - TSU01

Service digital identities

X509SubjectName

Subject 2.5.4.97: VATES-A66721499

Subject CN: Sello cualificado de tiempo electrónico de UANATACA - TSU01

Subject OU: TSP-UANATACA

Subject O: UANATACA S.A.

Subject L: Barcelona

Subject C: ES

X509SKI

X509 SK I 7f/UDk2cl5Y+ocsmUQ8/KKBh21k=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-02-15T01:00:00Z

26.4 - Service (granted): Qualified certificates issued by UANATACA CA1 2021

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified certificates issued by UANATACA CA1 2021

Name [es] *Certificados cualificados emitidos por UANATACA CA1 2021*

Service digital identities

Certificate fields details

```
Version: 3
Serial Number: 8888777927192838790
```

X509 Certificate

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: UANATACA ROOT 2016

Issuer OU: TSP-UANATACA

Issuer 0: UANATACA S.A.

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2021*

Subject OU: *TSP-UANATACA*

Subject 0: *UANATACA S.A.*

Subject L: *Barcelona*

Subject C: ES

Valid from: *Thu Jun 03 12:52:31 CEST 2021*

Valid to: *Sat Jun 03 12:52:31 CEST 2034*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:8D:E7:11:A2:97:D0:BB:6D:88:55:20:E2:17:1E:84:40:BF:26:CF:4D:22:ED:E3:86:54:7E:82:58:E6:09:66:70:C5:4D:A7:FA:3F:B1:7D:12:7A:DD:0F:07:6F:36:62:A3:1C:6E:3C:4F:50:84:77:56:A2:72:1A:94:A2:8A:1A:E5:E8:3C:12:7B:E8:68:69:C3:30:8A:B9:E7:0E:A4:92:EC:18:D9:85:60:1D:CB:13:88:88:1A:B5:7A:78:1A:B4:04:9D:5E:55:54:EC:3D:01:02:64:AA:80:37:AF:AA:27:6E:BE:C0:7F:36:4B:7C:3A:D7:1C:4D:E7:41:10:88:FA:6D:2A:1F:D0:56:A9:37:5F:F4:C5:38:CB:51:8D:9E:73:C4:42:01:7F:F0:C6:80:F5:69:41:78:29:8B:71:70:51:CF:C7:59:F0:DC:5B:C6:D4:A3:52:A2:83:51:9D:85:B6:EE:7B:F5:F6:F1:0F:B7:C2:D5:50:87:27:4C:42:FE:0E:7B:37:17:3E:A7:2D:ED:03:E5:98:2E:02:EF:56:88:86:05:6F:70:FC:3A:DF:99:A2:FE:EF:A7:FD:7F:ED:BF:0E:3F:83:90:25:08:50:6D:BE:74:E1:A7:DE:EA:69:ED:02:CC:6A:A1:48:3A:54:E7:90:F6:84:06:72:53:C1:FA:21:16:81:8C:DE:F8:C1:2A:4B:29:A5:41:35:3F:93:72:CD:C6:AC:CC:54:A6:8D:6C:EF:1E:93:25:80:6E:64:DE:36:4C:80:8B:4C:C0:87:22:79:EA:A1:0F:D6:5B:AA:82:E6:B4:9C:C1:D5:AC:D0:17:3E:BA:4E:B9:01:0B:BE:16:B2:D6:3D:CA:8F:2B:2B:65:55:FC:A4:27:C8:7D:5D:1D:5D:18:32:9A:72:A3:1D:D3:68:0D:F7:DA:45:5E:4E:12:0A:01:7D:E1:16:1E:94:6A:82:10:82:D7:7C:D4:91:25:55:AD:D8:88:89:79:90:24:17:AF:C4:ED:AE:49:30:DC:22:53:8D:22:80:2A:B3:9F:49:73:6E:3A:72:D9:5D:00:8D:BC:91:3F:DF:49:66:68:F0:31:C7:9C:AF:31:0F:A1:04:86:E2:DD:C8:B4:68:33:66:B7:2B:79:9A:65:49:EF:0A:89:D1:A7:83:C7:3A:4A:9B:F8:01:98:7D:28:CA:B1:8A:80:D4:51:76:92:6B:6A:26:23:10:46:3C:50:89:C6:C1:A0:4F:F3:45:81:1A:43:04:E3:0E:0A:1C:EE:32:90:1A:AF:BE:34:DD:8F:D9:5D:46:75:4A:C9:4F:69:BD:88:38:15:8D:F0:1A:E0:AA:9F:9A:5F:AF:43:87:FA:99:77:8F:C5:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Certificado de la Autoridad de Certificación Subordinada de UANATACA. Ver <https://web.uanataca.com/>]*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*

Subject Alternative Name *info@uanataca.com*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9B:08:3D:C4:5B:1B:EC:21:1F:93:09:8F:91:5D:3D:5E:E2:D7:DF:A9:37:20:FE:D4:E2:86:B8:3C:1E:F4:46:9A*

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA1 2021*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona*

Subject C: *ES*

X509SKI

X509 SKI *gc+QWTS7arctGcUo8otbz8r8FWg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-11-16T02:00:00Z*

26.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

26.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

26.5 - Service (granted): Qualified certificates issued by UANATACA CA2 2021

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[en] Qualified certificates issued by UANATACA CA2 2021*

Name *[es] Certificados cualificados emitidos por UANATACA CA2 2021*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2247335441897207227*

Basic Constraints	<i>IsCA: true - Path length: 0</i>
Authority Key Identifier	<i>55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C</i>
Issuer Alternative Name	<i>info@uanataca.com</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://www.uanataca.com/public/cps/</i> <i>CPS text: [Certificado de la Autoridad de Certificación Subordinada de UANATACA. Ver https://web.uanataca.com/]</i>
CRL Distribution Points	<i>http://crl1.uanataca.com/public/pki/crl/arI_uanataca.crl</i> <i>http://crl2.uanataca.com/public/pki/crl/arI_uanataca.crl</i>
Subject Alternative Name	<i>info@uanataca.com</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>15:CE:AB:33:91:44:D4:8D:35:2E:EF:1C:22:7F:4D:2E:F4:FC:17:56:DE:AD:60:2C:22:BE:32:D5:21:00:E6:9A</i>

X509SubjectName

Subject 2.5.4.97:	<i>VATES-A66721499</i>
Subject CN:	<i>UANATACA CA2 2021</i>
Subject OU:	<i>TSP-UANATACA</i>
Subject O:	<i>UANATACA S.A.</i>
Subject L:	<i>Barcelona</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>xecz/djv1I3nU4fKolt1OouW3Uo=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2021-11-16T02:00:00Z</i>

26.5.1 - Extension (critical): additionalServiceInformation

Issuer CN: *UANATACA CA1 2021*
Issuer OU: *TSP-UANATACA*
Issuer O: *UANATACA S.A.*
Issuer L: *Barcelona*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-A66721499*
Subject CN: *Sello de tiempo electrónico de UANATACA – TSU02*
Subject OU: *TSP-UANATACA*
Subject O: *Uanataca S.A.*
Subject L: *Barcelona*
Subject C: *ES*
Valid from: *Tue Sep 21 19:48:02 CEST 2021*
Valid to: *Fri Sep 21 19:48:02 CEST 2029*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E7:E7:F6:D5:D8:63:02:58:36:85:5D:91:5B:4C:60:80:19:75:A2:A7:B4:8F:A8:01:7F:FD:5C:68:52:26:41:ED:2C:AA:6A:AF:B6:22:01:CA:13:E3:43:0B:29:BF:76:D5:C4:12:5B:A7:81:BC:16:6A:D2:91:09:97:9D:6C:62:4B:19:31:18:C9:60:0F:4F:20:5C:3A:09:43:7D:1A:40:BF:55:00:BD:E6:FD:30:8D:B7:9F:90:BB:7C:E4:C2:78:34:A2:4D:B9:18:7D:E3:38:41:BE:80:A7:0D:FA:A6:1A:7F:19:09:24:3E:A8:03:A3:01:EE:74:68:58:34:8E:C3:AD:01:42:AB:33:89:75:37:93:5A:81:DF:E4:4D:A1:9E:BA:99:CD:11:F6:BE:25:62:5A:EA:BC:44:15:74:95:D0:3A:DE:21:26:9D:97:EF:35:48:DB:84:AC:C7:4C:D4:01:23:1E:C8:55:44:D5:49:A7:76:3F:03:A7:6F:72:A7:C7:C4:91:81:52:3B:FA:BA:23:8B:4F:C8:91:4E:34:8F:D8:B3:E5:AD:E4:55:20:20:51:C2:94:6D:A5:06:5F:16:D5:C3:25:23:5A:82:52:60:78:13:88:00:80:66:52:29:1F:A4:AA:CA:72:08:1B:97:44:B2:AB:E4:5E:00:C0:44:DD:4D:02:03:01:00:01*
Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/*
http://ocsp2.uanataca.com/public/pki/ocsp/
Subject Key Identifier *2D:FF:66:C0:73:A2:58:C1:E0:66:7D:B4:2B:F0:79:B5:FD:5D:4B:A3*
Basic Constraints *IsCA: false*
Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*
Issuer Alternative Name *info@uanataca.com*
Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2
CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@uanataca.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AA:59:FB:3B:38:1C:94:7C:BE:22:5B:D8:8A:CE:7E:0C:19:C5:A4:48:E4:3B:BF:7D:30:EA:7D:CD:FB:7E:86:70*

X509SubjectName

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *Sello de tiempo electrónico de UANATACA - TSU02*

Subject OU: *TSP-UANATACA*

Subject O: *Uanataca S.A.*

Subject L: *Barcelona*

Subject C: *ES*

X509SKI

X509 SK I *Lf9mwHOiWMHgZn20K/B5tf1dS6M=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2021-11-16T02:00:00Z

26.7 - Service (granted): Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA - TSU01 2025

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA - TSU01 2025*

Name [es] *Sellos de tiempo cualificados emitidos por Sello cualificado de tiempo electrónico de UANATACA - TSU01 2025*

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B6:87:B9:D9:85:6A:7F:30:43:DB:3C:0F:29:9E:18:55:D2:44:45:17:EA:A9:21:07:F2:3E:77:CF:5C:11:14:9E:DD:82:E3:DF:88:00:00:9B:84:7B:55:50:A6:BF:2E:82:80:50:3B:3F:68:9F:C6:F1:1B:2B:BF:A2:86:E2:6D:96:A0:1A:52:98:68:A6:7F:67:F6:50:49:24:B4:6E:BF:9F:7A:94:39:A7:8A:4F:C4:CF:F8:16:50:16:1D:24:B5:E1:5A:CF:ED:B2:2B:80:C7:18:3D:BA:8B:30:CB:87:E6:4D:2D:BC:2A:48:48:10:D2:63:25:43:09:28:AF:DA:42:E4:C0:49:0C:52:92:31:EC:88:CF:32:34:46:81:9F:E7:B5:84:9D:6F:51:FE:5F:A2:25:1B:1E:98:76:30:89:A0:33:D3:2F:65:91:CD:0B:16:EA:AF:3E:6B:18:6D:A4:4F:A7:FD:02:82:20:95:2C:54:5E:80:E2:06:5A:75:D1:5C:9F:C2:D8:BD:8B:65:D2:5F:92:33:27:0E:D0:63:C4:AE:2E:DA:32:C6:E8:2C:E5:2C:83:6A:74:43:D7:5A:A7:AA:F7:68:E3:CE:FA:B4:51:6B:5F:43:01:B2:6D:B5:35:18:7F:88:93:B3:CA:85:14:2A:25:A7:F8:95:4E:0C:D4:5E:A7:02:03:01:00:01

Authority Info Access

https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer

<http://ocsp1.uanataca.com/public/pki/ocsp/>

<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier

46:C2:44:DD:90:0D:1E:9B:F7:EF:19:08:D3:CD:CC:56:00:64:88:67

Basic Constraints

IsCA: false

Authority Key Identifier

81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

Issuer Alternative Name

info@uanataca.com

Certificate Policies

Policy OID: 1.3.6.1.4.1.47286.2.5

CPS pointer: <https://www.uanataca.com/public/cps/>

CPS text: [Certificado de sello de tiempo electrónico.]

Policy OID: 0.4.0.2042.1.2

CRL Distribution Points

<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>

<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage

id_kp_timeStamping

Subject Alternative Name

info@uanataca.com

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

B4:59:A9:EB:C0:2D:FF:A8:49:14:78:AA:2E:64:AB:CB:9B:A4:F0:F8:12:84:EC:65:23:79:40:4C:F7:B3:9D:87

X509SubjectName**Subject 2.5.4.97:**

VATES-A66721499

Subject CN:

Sello de tiempo electrónico de UANATACA - TSU01

Subject OU:

TSP-UANATACA

Subject O:

Uanataca S.A.

Subject L:

Barcelona

Subject C:

ES

27 - TSP: VINTEGRIS S.L.U.**TSP Name**

Name *[en]* *VINTEGRIS S.L.U.*

Name *[es]* *VINTEGRIS S.L.U.*

TSP Trade Name

Name *[en]* *vinCAsign*

Name *[en]* *VINTEGRIS SLU*

Name *[en]* *VATES-B62913926*

Name *[en]* *VINTEGRIS SL*

Name *[en]* *Víntegris SL*

Name *[en]* *VINTEGRIS*

PostalAddress

Street Address *[en]* *C. Pallars, 99 Planta 3 Oficina 33*

Locality *[en]* *Barcelona*

State Or Province *[en]* *Barcelona*

Postal Code *[en]* *08018*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *C. Pallars, 99 Planta 3 Oficina 33*

Locality *[es]* *Barcelona*

State Or Province *[es]* *Barcelona*

Postal Code *[es]* *08018*

Country Name *[es]* *ES*

ElectronicAddress

URI *[es]* *mailto:info@vintegris.com*

URI	[en]	https://www.vincasign.net/policy/en/
URI	[es]	https://www.vincasign.net/policy/es/

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>	
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificates issued by vinCAsign Global Authority
Name	[es]	Certificados Reconocidos emitidos por vinCAsign Global Authority

Version:	3
Serial Number:	671918045467400215543670222139247462900201383183
X509 Certificate	-----BEGIN CERTIFICATE-----

Page 973

Issuer SERIAL NUMBER: *B62913926*
Issuer OU: *EC-VINTEGRIS*
Issuer L: *Barcelona (see current address at <https://www.vincasign.net/contact>)*
Issuer O: *VINTEGRIS SL*
Issuer C: *ES*
Subject CN: *vinCAsign Global Authority*
Subject SERIAL NUMBER: *B62913926*
Subject OU: *EC-VINTEGRIS*
Subject L: *Barcelona (see current address at <https://www.vincasign.net/contact>)*
Subject O: *VINTEGRIS SL*
Subject C: *ES*
Valid from: *Thu Jan 28 15:02:06 CET 2016*
Valid to: *Fri Jan 28 15:02:06 CET 2022*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:9A:FE:38:9E:C6:0A:93:3F:87:5F:6D:C3:D1:A3:F4:F9:1E:C3:C3:37:52:F6:3E:3C:A1:8B:90:01:9B:D8:CF:5D:1C:7B:A8:DA:00:5F:19:A8:2B:3D:1C:C0:8F:1F:D9:8F:D8:3E:69:C9:A2:48:10:AB:4D:E2:69:D1:21:F8:A1:16:0F:45:00:49:B1:50:F9:8B:8D:0E:20:D0:A2:B6:79:C6:B2:7A:CF:6E:FD:6D:66:67:37:AC:92:68:E5:56:FA:18:7B:42:04:45:47:42:33:9D:8F:97:85:87:9B:C8:79:AF:A2:AE:60:18:8B:E2:54:48:E4:59:C2:3A:0C:82:BA:EB:8C:1A:A3:68:A:E:6A:58:1E:3C:36:4A:54:24:25:A4:75:BA:E3:8B:41:89:C0:34:AE:16:57:EF:FF:34:C9:B2:A0:57:1E:68:D3:90:BB:E7:44:BD:31:8C:C1:2B:67:A8:74:50:5D:AD:21:2E:DF:F1:13:7D:70:67:3C:80:80:86:57:0D:5C:57:1B:33:CB:91:6D:50:9D:FC:64:7A:00:5C:52:3B:ED:71:BC:D8:1A:2C:F6:93:32:AE:71:63:DE:3E:CA:9B:62:C1:68:AE:78:4C:D1:F5:60:9C:E7:B4:70:2E:1F:14:5D:FA:5A:1B:EA:AE:07:1C:C6:2B:BC:95:2F:0C:D4:DA:AC:83:0A:20:96:44:A4:B3:85:10:8B:02:76:59:96:FC:F9:4C:BD:9A:E4:03:0F:31:CD:E1:6D:F5:C2:C6:20:CF:4D:1B:69:74:B8:8D:0E:CF:9D:D9:13:C3:CA:B8:75:22:5B:2C:8D:C6:82:B3:55:6E:B2:70:44:14:E9:6C:79:F2:FE:D9:E6:BE:58:DC:1B:BE:55:E3:EA:D0:62:F4:EF:DF:3E:1F:26:E6:30:BD:90:EA:03:C1:5A:DD:C6:4E:E8:20:3A:FA:86:76:F6:44:9C:EF:31:A7:4C:FC:2B:75:74:D4:20:06:5B:54:EC:0E:2C:BC:BE:EB:12:34:84:65:2E:05:C9:1E:EF:AD:59:F3:89:15:67:27:05:5B:F2:64:17:EC:A0:BF:5B:3C:8E:58:D8:04:8B:D5:2C:F0:53:93:F1:31:E4:F1:81:30:B9:08:1C:3B:C9:9F:2C:B0:E8:49:1B:00:26:09:AE:1A:3A:52:41:36:71:40:7E:85:E5:0A:C4:C1:73:1C:B4:CE:CA:54:16:CD:3C:DB:B1:D2:D0:BC:8F:20:3C:E7:06:5D:C1:E1:50:C2:E6:60:06:58:79:03:87:3E:21:9A:90:BA:22:02:97:D5:C6:E3:B9:42:4F:9B:C6:47:42:D3:8C:56:68:69:41:70:22:C5:85:AA:70:83:02:03:01:00:01*
Authority Key Identifier *A9:8A:AD:59:FD:ED:E8:E1:80:8B:48:B3:0E:D2:63:E6:44:E0:31:03*
Subject Key Identifier *07:46:CB:4B:E5:D4:8E:61:73:44:7A:04:20:B2:E1:BA:8C:34:DE:CB*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://policy.vincasign.net>
CPS text: [Certificado de la vinCAsign Global Authority de la Entidad de certificacion de Vintegris. Ver <https://policy.vincasign.net>]
Subject Alternative Name *info@vincasign.net*
CRL Distribution Points *<http://crl1.vincasign.net/caroot.crl>*
<http://crl2.vincasign.net/caroot.crl>
Authority Info Access *<http://ocsp1.vincasign.net>*
<http://ocsp2.vincasign.net>
Basic Constraints *IsCA: true - Path length: 1*
Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *30:5E:88:A5:EB:B7:DA:E9:E6:6B:F8:A3:D2:1E:64:3C:C2:09:5C:18:FF:7A:F4:7D:FE:1B:AB:2B:88:1D:CB:F8*

X509SubjectName

Subject CN: *vinCAsign Global Authority*

Subject SERIAL NUMBER: *B62913926*

Subject OU: *EC-VINTEGRIS*

Subject L: *Barcelona (see current address at <https://www.vincasign.net/contact>)*

Subject O: *VINTEGRIS SL*

Subject C: *ES*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2017-12-20T01:00:00Z*

Scheme Service Definition URI

URI [en] *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI [es] *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

27.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47155.1.5.2*

27.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.1.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by vinCAsign Global Authority

Name	[es]	Certificados Reconocidos emitidos por vinCAsign Global Authority

Service digital identities**X509SubjectName**

Subject CN:	vinCAsign Global Authority
Subject SERIAL NUMBER:	B62913926
Subject OU:	EC-VINTEGRIS
Subject L:	Barcelona (see current address at https://www.vincasign.net/contact)
Subject O:	VINTEGRIS SL
Subject C:	ES

X509SKI

X509 SK I	B0bLS+XUjmFzRHoEILLhuow03ss=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2016-06-30T22:00:00Z

27.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDAURN]	urn:oid:1.3.6.1.4.1.47155.1.5.1

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.47155.1.5.2*

27.1.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.1.4 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by vinCAsign Global Authority*

Name [es] *Certificados Reconocidos emitidos por vinCAsign Global Authority*

Service digital identities**X509SubjectName**

Subject CN: *vinCAsign Global Authority*

Subject SERIAL NUMBER: *B62913926*

Subject OU: *EC-VINTEGRIS*

Subject L: *Barcelona (see current address at https://www.vincasign.net/contact)*

Subject O: *VINTEGRIS SL*

Subject C: *ES*

X509SKI

X509 SK I *B0bLS+XUjmFzRHoEILLhuow03ss=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2016-06-21T22:00:00Z*

27.1.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.1.5.2

27.2 - Service (withdrawn): Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority

Name [en] Qualified Certificates issued by vinCAsign nebulaSUITE Authority

Service digital identities

Certificate fields details

Version: 3

Serial Number: 580247578624264002174382824980712041798116291597

Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://policy.vincasign.net</i> <i>CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]</i>
Subject Alternative Name	<i>info@vincasign.net</i>
CRL Distribution Points	<i>http://crl3.vincasign.net/casub.crl</i> <i>http://crl4.vincasign.net/casub.crl</i>
Authority Info Access	<i>http://ocsp3.vincasign.net</i> <i>http://ocsp4.vincasign.net</i> <i>https://www.vincasign.net/publickeys/caqualified.cer</i>
Basic Constraints	<i>IsCA: true - Path length: 1</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>D7:CD:55:49:04:DF:D2:2A:22:EB:96:5C:E0:1B:B1:A3:0C:21:51:CA:07:47:3D:4C:B D:45:DF:5D:AF:27:36:A4</i>

X509SubjectName

Subject ST:	<i>Barcelona</i>
Subject CN:	<i>vinCAsign nebulaSUITE Authority</i>
Subject 2.5.4.97:	<i>VATES-B62913926</i>
Subject L:	<i>Hospitalet de Llobregat</i>
Subject O:	<i>Víntegris SL</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>hGvvoiedpgqtH3qv3xdefBjUpKQ=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2018-10-08T01:00:00Z</i>

27.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	<i>[en] undefined.</i>

[es]

undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.6.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.11

Description**27.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.2.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.2.4 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] *Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority*

Name [en] *Qualified Certificates issued by vinCAsign nebulaSUITE Authority*

Service digital identities**X509SubjectName**

Subject ST: *Barcelona*

Subject CN: *vinCAsign nebulaSUITE Authority*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *Hospitalet de Llobregat*

Subject O: *Víntegris SL*

Subject C: *ES*

X509SKI

X509 SK I *hGvvoiedpgqtH3qv3xdefBjUpKQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-12-20T01:00:00Z*

27.2.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsAsURN]	<i>urn:oid:1.3.6.1.4.1.47155.1.1.1</i>

Policy Identifier:

Identifier	[OIDsAsURN]	<i>urn:oid:1.3.6.1.4.1.47155.1.2.1</i>

Policy Identifier:

Identifier	[OIDsAsURN]	<i>urn:oid:1.3.6.1.4.1.47155.1.6.1</i>

Policy Identifier:

Identifier	[OIDsAsURN]	<i>urn:oid:1.3.6.1.4.1.47155.1.2.11</i>

Description

27.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

Issuer 2.5.4.97: *VATES-B62913926*

Issuer L: *Hospitalet de Llobregat*

Issuer O: *Víntegris SL*

Issuer C: *ES*

Subject CN: *vinCASign nebulaSUITE2 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCASign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

Valid from: *Wed Sep 27 16:20:46 CEST 2017*

Valid to: *Fri Sep 27 16:20:46 CEST 2030*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:CE:75:30:A8:77:4F:A3:AF:61:07:19:6B:91:D7:8F:34:57:1D:06:1E:84:74:3D:4A:0E:46:BC:E8:A9:11:E9:E7:5A:F4:D2:8B:52:38:4F:76:E7:0F:29:1E:5C:EE:C9:04:BB:5A:16:67:A5:6C:0B:95:8D:82:70:91:92:3B:AB:4B:67:9E:D9:68:68:87:C8:71:0A:44:F9:D4:55:66:4B:E6:FE:90:36:A1:DF:80:3E:FF:56:5E:CB:76:88:F7:69:8E:4B:83:BD:56:A7:1F:06:F8:D9:81:B1:81:F0:CF:C6:B6:C8:0B:43:D1:10:D5:87:16:6B:99:90:F9:A5:F8:CF:B1:3A:B7:B6:1D:B3:06:AD:54:9D:89:AE:69:8C:8D:93:0F:2B:2E:CD:CD:A7:21:CD:F5:20:57:09:06:13:80:B6:D7:3F:BE:60:68:B0:17:DA:51:ED:8C:B7:9A:16:7C:B4:28:F9:F4:3C:F8:E9:5E:FA:0E:D3:0E:CE:F8:96:31:74:C5:05:9A:ED:37:A8:87:90:87:6D:ED:7F:F7:7F:40:1E:18:4D:96:B6:81:7B:81:19:E5:60:73:BF:11:58:57:63:60:72:58:16:62:EF:AF:0D:C8:4A:38:9C:A9:BA:28:24:33:8F:47:21:68:2D:34:8B:93:B9:AF:EA:D6:62:39:36:19:4F:5E:79:59:8D:D4:57:45:98:24:0A:7E:E4:66:66:3A:CC:CC:A5:9E:6D:5B:99:C4:8B:BF:8E:11:DD:31:4F:58:B4:08:F0:7D:9B:3C:AB:E0:47:EF:A4:F0:53:83:6C:9A:8A:85:06:37:68:90:F9:AC:D2:29:8C:9B:52:3F:C1:FD:2F:AA:00:30:7F:CA:90:E2:E5:B4:FF:34:6D:7A:4B:94:70:B9:67:75:A3:13:6C:9E:89:F6:82:AD:DC:3C:82:03:4C:8D:53:27:18:1B:AD:84:46:27:25:38:72:03:57:51:B5:7F:0D:31:AC:9B:8D:C5:5D:8E:BB:8D:BB:AE:3A:F0:4D:3E:52:A6:C8:67:EC:D5:1A:EA:E3:E2:A6:EB:57:2D:09:C9:A5:54:02:97:B2:BE:B3:A7:D7:DB:34:80:25:8A:95:61:6E:42:15:80:A8:7B:8D:88:68:30:4D:56:98:2B:28:AF:D7:B5:BB:AE:AD:81:E5:8A:79:73:80:D8:5C:E5:E1:3A:AC:12:04:4B:04:77:61:6B:5C:34:6A:01:77:DE:14:C6:CB:EC:3D:16:E6:4B:F9:05:46:4F:99:EC:0E:5B:79:7B:12:6F:CD:AA:51:7C:07:C7:37:E2:EA:BF:9F:5F:5A:3E:27:78:DC:9D:80:07:C0:82:98:0D:F4:D7:C1:02:03:01:00:01

Authority Key Identifier *D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0*

Subject Key Identifier *4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://policy.vincasign.net>
CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

Subject Alternative Name *info@vincasign.net*

CRL Distribution Points
<http://crl3.vincasign.net/casub.crl>
<http://crl4.vincasign.net/casub.crl>

Authority Info Access
<http://ocsp3.vincasign.net>
<http://ocsp4.vincasign.net>
<https://www.vincasign.net/publickeys/caqualified.cer>

Basic Constraints *IsCA: true - Path length: 1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DA:13:26:D2:2E:64:F7:C2:1F:38:81:21:F6:8C:8F:70:0D:30:5C:69:FB:0B:5E:8B:9F:C2:84:6F:7A:E7:CB:70*

X509SubjectName

Subject CN: *vinCAsign nebulaSUITE2 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *TdZ6hiuc9kt699v96VFML3fcFn4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time

2019-11-06T01:00:00Z

27.3.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*

[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.6.1
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.4.1
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.5.1
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.11
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.1.51
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.51
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.151
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.4.11
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.6.51
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.10.1
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.10.51
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47155.1.11.1
Description		

27.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.3.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.3.4 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority

Name	[en]	Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority

Service digital identities**X509SubjectName**

Subject CN:	vinCAsign nebulaSUITE2 Authority

Subject O:	VINTEGRIS SL

Subject OU:	vinCAsign

Subject 2.5.4.97:	VATES-B62913926

Subject L:	HOSPITALET DE LLOBREGAT

Subject ST:	BARCELONA

Subject C:	ES

X509SKI

X509 SK I	TdZ6hiuc9kt699v96VFML3fcFn4=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2019-10-28T01:00:00Z

27.3.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.6.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.4.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.11

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.51

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.51

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.151

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.4.11

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.6.51

Description**27.3.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.3.4.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.3.5 - History instance n.2 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority

Name	[en]	Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority

Service digital identities**X509SubjectName**

Subject CN:	vinCAsign nebulaSUITE2 Authority

Subject O:	VINTEGRIS SL

Subject OU:	vinCAsign

Subject 2.5.4.97:	VATES-B62913926

Subject L:	HOSPITALET DE LLOBREGAT

Subject ST:	BARCELONA

Subject C:	ES

X509SKI

X509 SK I	TdZ6hiuc9kt699v96VFML3fcFn4=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2019-08-02T00:00:00Z

27.3.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.6.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.4.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.11

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.1.51

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.51

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.2.151

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.47155.1.4.11

Policy Identifier:

Identifier [*OIDAsURN*] *urn:oid:1.3.6.1.4.1.47155.1.6.51*

Description

27.3.5.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [*en*] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.3.5.6 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [*en*] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.3.6 - History instance n.3 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [*es*] *Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority*

Name [*en*] *Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority*

Service digital identities**X509SubjectName**

Subject CN: *vinCAsign nebulaSUITE2 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI**X509 SK I***TdZ6hiuc9kt699v96VFML3fcFn4=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2018-04-09T00:00:00Z***27.3.6.7 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.1.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.6.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.4.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.5.1*

Policy Identifier:

Identifier [OIDsURN] *urn:oid:1.3.6.1.4.1.47155.1.2.11*

Description**27.3.6.8 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

Page 993

Issuer OU: *vinCAsign*
Issuer 2.5.4.97: *VATES-B62913926*
Issuer L: *HOSPITALET DE LLOBREGAT*
Issuer ST: *BARCELONA*
Issuer C: *ES*
Subject C: *ES*
Subject ST: *BARCELONA*
Subject L: *HOSPITALET DE LLOBREGAT*
Subject O: *VINTEGRIS SL*
Subject 2.5.4.97: *VATES-B62913926*
Subject OU: *vinCAsign*
Subject CN: *vinTSAsign nebulaSUITE1 Authority*
Valid from: *Thu Jul 11 15:58:42 CEST 2019*
Valid to: *Tue Jul 09 15:58:42 CEST 2024*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:82:3A:E4:0F:4C:2B:91:03:4B:0F:50:80:78:0E:42:18:01:EA:1F:88:66:41:34:25:59:C7:67:2A:D5:7F:9D:1C:6D:49:D6:2C:D3:52:CC:2E:11:5B:8A:51:4B:39:22:3E:D9:16:22:BF:36:0C:30:E4:4B:A4:DD:9D:8C:4E:E2:00:A3:01:32:13:87:29:A6:E0:58:12:03:F6:62:33:FD:64:E0:84:98:3F:FD:12:01:C9:CF:D5:AE:91:4D:C2:19:D7:EA:B7:57:58:D7:9C:DE:18:EA:72:AA:0A:DD:89:80:91:83:89:2B:22:26:39:7D:86:4B:BD:74:EE:47:92:04:DE:CD:F4:07:98:EB:C5:B3:E1:3D:0B:BD:1F:DC:4C:92:C4:2F:28:AB:26:35:FE:DC:C8:43:0F:B0:86:F1:7A:26:A1:D8:ED:CB:E4:D4:0A:C8:EA:56:73:EB:94:24:9C:15:6A:E5:1C:CE:6A:64:C7:27:0D:D7:0D:3D:37:FA:3A:8A:4B:CC:14:2A:E5:CE:8E:F2:0C:D8:66:68:4F:8A:B7:C8:A4:D5:C9:36:D8:AD:CC:EA:39:27:B7:10:8B:C9:30:AB:9A:ED:86:C8:DA:6F:FD:C8:9D:D9:C0:E6:AC:96:56:9B:85:23:16:C5:62:55:8D:28:38:46:EC:5D:96:D0:34:99:1B:F6:57:CD:C1:10:BC:14:56:69:36:DE:34:62:BE:50:5C:5B:B7:B1:87:C6:5F:44:AE:DA:16:07:F6:AD:CE:6E:59:6B:71:D3:59:86:23:1E:A1:C4:79:8E:4C:10:F8:2A:FE:0C:2D:41:0C:6F:91:AF:FA:67:46:43:A0:69:46:70:1B:0B:CF:B5:86:1A:CA:04:4F:5D:E6:E6:6A:7F:29:C1:EC:FA:73:03:CB:8C:F4:DA:0B:7B:FD:8C:8F:76:18:C8:03:C1:98:E8:B5:00:82:1C:62:F1:5F:7F:02:DC:E4:DF:99:19:49:8A:72:67:A4:2D:35:9D:FC:D8:CD:00:E9:0B:A1:10:ES:AF:EB:10:BE:64:88:3B:D6:17:7C:92:1A:0F:87:67:DE:9A:AB:59:A7:45:D5:80:A3:B6:C4:1C:6F:67:5B:67:52:36:71:BE:AD:26:EB:12:1E:D9:C5:30:19:A3:02:24:F6:46:9D:96:66:B3:52:B7:5F:35:C2:39:CA:1B:86:75:4B:63:1A:35:76:37:A4:3D:FF:0F:A7:04:EB:A0:09:A9:0B:D9:2F:84:98:93:79:B9:40:AB:B7:E6:07:00:D5:B3:FC:03:2C:F3:49:E1:01:21:DB:F7:CB:23:05:E1:0F:6A:69:F4:30:24:04:7A:FE:53:34:68:8B:D4:D0:8E:CB:02:03:01:00:01*
Authority Info Access *http://www.vincasign.net/publickeys/canebula2.crt*
http://ocsp.vincasign.net
Subject Key Identifier *93:73:A4:CE:A0:BE:79:96:07:2E:73:1A:40:F9:E2:F6:42:B0:22:EB*
Basic Constraints *IsCA: false*
Authority Key Identifier *4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
Certificate Policies *Policy OID: 1.3.6.1.4.1.47155.1.9.1*
CPS pointer: https://policy.vincasign.net
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points *http://crl1.vincasign.net/canebula2.crl*
http://crl2.vincasign.net/canebula2.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *17:57:14:7A:3A:13:1C:C4:9C:FA:DE:37:4B:00:65:59:FB:A3:F0:EB:2D:9F:6A:4A:FF:41:DE:7B:2F:11:96:9D*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SL*

Subject 2.5.4.97: *VATES-B62913926*

Subject OU: *vinCAsign*

Subject CN: *vinTSAsign nebulaSUITE1 Authority*

X509SKI

X509 SK I *k3OkzqC+eZYHLnMaQPni9kKwlus=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2024-02-08T02:00:00Z*

27.4.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE1 Authority*

Name *[en]* *Qualified time stamps issued by vinTSAsign nebulaSUITE1 Authority*

Service digital identities**X509SubjectName**

Subject C:	ES
Subject ST:	BARCELONA
Subject L:	HOSPITALET DE LLOBREGAT
Subject O:	VINTEGRIS SL
Subject 2.5.4.97:	VATES-B62913926
Subject OU:	vinCAsign
Subject CN:	vinTSAsign nebulaSUITE1 Authority

X509SKI

X509 SK I	k3OkzqC+eZYHLnMaQPni9kKwlus=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2019-08-02T00:00:00Z

27.5 - Service (withdrawn): Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[es]	Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority
Name	[en]	Qualified time stamps issued by vinTSAsign nebulaSUITE2 Authority

Service digital identities**Certificate fields details**

Version:	3
Serial Number:	1601373709008309851

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIISzCCBzOgAwIBAgIFjk452YXDlsWDOYJKozlhvcNAOENBOAwgbMxCzAIBgNVBAYTAkVMTMRIw
EAYDVQQIDAIQVjDRUXPTkEXIDAEAgNBACMF0hPU1BIVEFMRVogREUgTExPOJFR0FUMRgWfGYD
VORhDA9wQVRVUy1CAnJSM5MjE4ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
UKITFNMMSkWjWYDQODDCBzaW5DOXNpZz4qbmVidWw1J1VIVEUEF1dGhvcml0eT8eFw0xOTA3
MTExNDQ0NTFafW0yNDA3MDkxNDQ0NTFafMIGOMsowkAYDVQODDCFzaW5UODFzaWduIG51YnVsYVNV
SVRFMIB8XR0d3p3dHkxQ08gNBASMCZpbkNBczlnbGE1YmYGA1UEYmVkrURVMTQ1YjOTE2
OTI2MRUwEwYDQODDAW5SUURUG5SVMLUwWIDAEAgNBACMF0hPU1BIVEFMRVogREUgTExPOJIF
R0FUMRIwEAYDVQIDAIQVjDRUXPTkEXIDAEAgNBACMF0hPU1BIVEFMRVogREUgTExPOJIF
Ag8AMiCCkAgEAgZys7yzeelJ4WmFtUHEYCDgUjH3BDXYEzYMs32KZlm7mFucmMwbpjnm5pO
skBhL9ZrZizwhWO7Llm7tgevd42xicyGCDTf70e2LbGR0bHfQ0phRAWV6ePfGcnz7YmqZACJ
z4gUliwXClzX+6d65AgY1BnujGgFLyS7HhGNgm60gWVTA3gramUCw1yUZImBCCVdguoDCBz
JB0kM4y8P7xLqPmM3dHm35mQmQJubB3JXmK-c3g1ZodYK30swnvboSK6+Pab5J
+n0+0L7gEg90mE9CJWLDCivKtdfRwVCWfupc74Gec+09aSRR6DzKawB16mL6kOb+ZOUUku0s
+0Gskk5L9H6u+LVwt8OU3tA0I08qhoT3a2xPfI9TwtssTlxupSPpGz+PaxRe6MzFEXnhvfc/
ihhCS56kZEE1j8JLRhveDMbUmwWlePaeMKHfR0VWpXdnvTXWQ0BHUZE6zHGs5K9YjRIPOJS
UeyUknd4J0hagsHf5F6vFVtpZGagayQvIKrH2E3C0IofdcNUHqQ/PKNU/IB5XSuz0XE7EJup
8vdOL8N56QIU0IdpVrOB8COWetfKfAr9mcsixM5TbOyb2N6z9plmYp3fEg8i6PgTL0ro
3yqj0Bt0KxYzCAwEAAs0CA14wggBaMHQCCSQAUIFBwE9BgpwZ498ggrBgEFBQcwAAYkaHR0
CDovL3d3dy5zaW5jYXNpZ24ubmVl3B1YmxpY2hieXMyY2FuzWJ1bGEyLmNydDAIBggrBgEFBQcw
AYZaHR0CDovL29j3AudmluY2FzaWdulm5ldDA6BGNVH04EfgOU8B2IWZcfnuZBIPY9DiMOW+7
qTtW0AYDVOR0TAQIBAlwADA8BGNVH5MEGDAIYgBRInngK5Z53r323pUjWw09wWFCBqYIKWYB
BOUHA0EMegCewqB4wCAYGBACORgEBMAsGBgQAJYBAwIBDzATBgYEA5GAOYwCOYHBA0RGEGA/CB
IwYGBACORgEFMIGEMEAUWomh0dHBzOibvd3d3LnZpbmNhc2lnb5uZQvcG9saWN5L2Vul1BEUy1U
U0EvGReLXRzY1B5ZGYYAmVUeAUMh0dHBzOibvd3d3LnZpbmNhc2lnb5uZQvcG9saWN5
L2Vul1BEUy1U0EvGReLXRzY1cy5wZGYTAmVzMHQBNVH5Aegellwgd8wgdEGCysGAOQ0BvAz
AQBkMIHBMGCGCCSQAUFbWBFhxodHrwczoYL3BvbGlieS52aW5jYXNpZ24ubmVOMIGUBggrBgEF
BQCCAQCBwYB9hNncpZmJYWRWIG1Y1Wap2mJYWRWIGRIHNBGXvG5ZWNNcs0ZbmlyBk
ZSBwZXJzb25hIGp1cs0tZGlySbwYXhGKhIGV4cGVkaWNPw7NuIGRIHNBGXvG5ZWNNcs0ZbmlyBk
Y2Fkb3MgZGldgGlibXBvIGVsZWNNcs0ZbmlybzAIBGCEAlvSQAEBMGCGA1UdhWRgMF4wLaAroCmG
J2h0dHA5bG9icmVwLnZpbmNhc2lnb5uZQvcY2FuzWJ1bGEyLmNydDAIBGCEAlvSQAEBMGCGA1UdhWRgMF4wLaAroCmG
bDUudmluY2FzaWdulm5ldC9jYW51YnVsYTIuY3JsMA4GA1UdWE8wQEAwIGwDAWBgNVH5SUBA8E
DDAKBggrBgEFBQCCDCDFB8gkqhkiG9w0BAQE0Aw2MIA0DC1CaXQgUHVibGJlGtleSBibmNvZGVk
IGluY2F7Z9ZGFUjYUj2d0aCBsR4Mjic5NA0GCSqS4b3QOE6bQJUA4ICAQCWhGf1MgySRFj
DJcoW0o5w76jskqP4hBaTasElF3HnzYK5ec2mweGcHZYhsfgN9pwtMCRZgcKGz061V17bsA
1IcanFULUP5Qil0x5py8/3Lk/sDEokCnKerDX5SymxE36Fd91Vieg9mBHFBBk3Bkcr1jcXUp
1JfRxcC7Yek24u5XikV1kXCVUmjUATT+3c4sdy22nqzEBqBjJcEZVIOOKETi09ESydn
mpmBhU08qtbA71BbRr3dxt56fdtxAVP0dsOXX+Yd5afyxWl460d+hmUAYCgeMQqjY6xw01eYV
ADk5i7KH+jigj/W2gMNZqnAsWEuIF95LgavEFGoguBpHt5hmRLwF59btKXCZ0aIK02QJT71jUj
ZpRgJESNCFB2OpellhriE0cm8xKHPGcsd2540T13QJRYa0IEF8BgMgMvVm0+MG4Mg
oaiAD1Le8hVA1+UgM6ZKxGu5y3ZG2GowixSfaV7zopdt5j1VwSzibTUE5MIU6W5F+isEaw5
lmoM+eQRI0EliQPIttoZy+EqJlUq0vWSGc4A00GHMCndWqVLdYvqJf8ILkwbxFN5I4/kjyqhbYK
fMGg7kmR8WXZ6HilZyQ6BAden8NuFW9gizGcWZApdcjrT3p1cA7fP3TpaIg==

```

-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer CN:

vinCAsign nebulaSUITE2 Authority

Issuer O:

VINTEGRIS SL

Issuer OU:

vinCAsign

Issuer 2.5.4.97:

VATES-B62913926

Issuer L:

HOSPITALET DE LLOBREGAT

Issuer ST:

BARCELONA

Issuer C:

ES

Subject C:

ES

Subject ST:

BARCELONA

Subject L:

HOSPITALET DE LLOBREGAT

Subject O:

VINTEGRIS SL

Subject 2.5.4.97:

VATES-B62913926

Subject OU:

vinCAsign

Subject CN:

vinTSAsign nebulaSUITE2 Authority

Valid from:

Thu Jul 11 16:44:51 CEST 2019

Valid to:

Tue Jul 09 16:44:51 CEST 2024

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CE:AB:05:CB:37:9E:88:92:C0:34:89:85:52:11:18:70:31:A3:74:91:C8:DC:10:F1:60:46:72:32:CD:F6:2A:56:66:FE:59:8F:88:29:8D:C2:93:63:99:2A:0E:82:40:61:04:8F:59:44:8C:F0:85:63:A2:EC:88:C8:9F:BE:A0:7A:F7:78:67:18:9C:CB:A0:98:B4:57:FB:D1:ED:8B:6C:6A:CE:6C:73:EA:D2:98:51:01:65:7A:7B:31:5F:18:39:F3:61:59:A0:64:00:A2:CF:88:14:B4:8C:17:0A:2C:D7:FB:A7:7A:4B:08:18:D4:19:EE:20:91:A0:17:F2:89:2E:E2:1C:63:60:9B:AD:2:0:59:54:C0:DE:0A:DA:99:40:B0:D7:25:19:22:60:42:0A:D5:D8:EA:1F:0C:20:73:FC:10:FC:90:CC:B8:83:FF:0F:EE:F2:EA:D0:F9:A7:DE:C8:AD:17:0E:5B:55:2F:66:45:0D:C9:BA:80:65:C7:72:57:32:17:37:CE:AD:59:E9:D6:0A:DC:04:2C:BE:6B:D8:A1:22:A5:EB:E1:71:6F:99:7F:FB:33:68:FB:E2:FB:80:48:3D:D2:61:3D:08:B2:56:2C:30:A5:BE:44:DD:7D:15:AF:09:69:45:BA:91:BE:ED:61:C:F9:0F:5A:49:14:7A:0F:39:1A:C0:14:E5:EA:62:FA:91:06:FE:65:05:14:92:ED:2C:FB:41:B9:92:44:89:2F:D1:FA:BB:E2:D5:C2:DF:0E:53:7B:40:D2:54:3C:8E:A8:68:4F:76:B6:C4:F1:48:F5:3C:3F:7E:CB:13:53:1B:B4:48:F3:EA:67:E3:DA:5E:B7:BA:33:31:59:13:13:6F:85:F7:3F:8A:11:C2:4B:A1:A4:CC:4D:B5:27:CD:7F:44:7B:C4:DE:60:6E:31:65:BF:7B:F3:C0:78:CA:C:A1:C:F4:4E:8D:6A:57:86:1B:D3:5C:85:8E:80:11:04:D8:4E:B3:1C:60:6C:E4:A8:FD:C9:18:A2:3C:EF:D2:51:E6:14:92:39:DD:E2:33:A1:21:A8:EC:1D:FB:05:EA:F9:45:56:DA:59:A8:68:1A:C:9:0B:E2:2A:B1:F6:13:70:A2:D2:82:5F:75:C3:54:1E:04:F3:E4:34:8B:F0:79:5D:2B:86:41:71:3B:12:3B:8F:F1:57:4E:2F:C3:52:E9:09:54:C3:49:43:A5:5A:CE:07:C7:10:59:EB:5F:4E:41:7:F:69:1F:66:73:98:B1:7C:C4:9F:4D:B3:82:6F:63:7A:CF:D2:69:22:66:29:DD:FB:C4:83:C8:BA:3F:A8:13:2D:0A:E8:DF:2A:BF:94:E0:6E:B4:EC:4A:CB:67:02:03:01:00:01

Authority Info Access

<http://www.vincasign.net/publickeys/canebula2.crt>

<http://ocsp.vincasign.net>

Subject Key Identifier

F0:1D:A5:5B:67:05:9E:EC:C1:20:F6:2E:F4:38:8C:3B:0F:BB:81:32

Basic Constraints

IsCA: false

Authority Key Identifier

4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

Certificate Policies

Policy OID: 1.3.6.1.4.1.47155.1.9.1

CPS pointer: <https://policy.vincasign.net>

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

Policy OID: 0.4.0.194112.1.1

CRL Distribution Points

<http://crl1.vincasign.net/canebula2.crl>

<http://crl2.vincasign.net/canebula2.crl>

Extended Key Usage

id_kp_timeStamping

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

FB:75:52:A8:36:0A:2D:4D:89:4B:F3:8C:4E:B4:A6:A0:9C:8E:CF:1E:25:C5:4F:B1:E2:02:D1:85:76:61:3A:51

X509SubjectName**Subject C:**

ES

Subject ST:

BARCELONA

Subject L:

HOSPITALET DE LLOBREGAT

Subject O:

VINTEGRIS SL

Subject 2.5.4.97:

VATES-B62913926

Subject OU:

vinCAsign

Subject CN:

vinTSAsign nebulaSUITE2 Authority

X509SKI

X509 SK I *8B2IW2cFnuzBIPYu9DiMOw+7gTl=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time

2024-02-08T02:00:00Z

27.5.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority*

Name *[en]* *Qualified time stamps issued by vinTSAsign nebulaSUITE2 Authority*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SL*

Subject 2.5.4.97: *VATES-B62913926*

Subject OU: *vinCAsign*

Subject CN: *vinTSAsign nebulaSUITE2 Authority*

X509SKI

X509 SK I *8B2IW2cFnuzBIPYu9DiMOw+7gTl=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2019-08-02T00:00:00Z

Subject O: VINTEGRIS SL
Subject OU: vinCAsign
Subject 2.5.4.97: VATES-B62913926
Subject L: HOSPITALET DE LLOBREGAT
Subject ST: BARCELONA
Subject C: ES
Valid from: Fri May 08 13:19:48 CEST 2020
Valid to: Sun May 08 13:19:48 CEST 2033
Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C8:BC:81:E5:E6:48:8B:CA:5F:7D:80:A2:24:A9:BC:AB:C2:10:97:10:49:9D:55:44:28:29:49:75:E4:3F:67:46:5F:D4:4E:E9:08:91:64:48:8B:D7:4C:38:2B:99:58:16:9E:11:62:56:83:CE:3C:C8:E6:EE:85:BA:70:2E:C4:64:27:7D:4D:BD:3A:CD:16:C4:76:CC:90:F8:12:1C:83:00:62:90:80:6D:6F:DC:12:6E:E4:E1:68:A7:30:1B:5D:C3:E9:2C:04:E4:C6:1E:30:59:43:53:F2:EF:75:28:37:7D:E6:50:D7:A0:7F:22:3B:94:EB:E5:BE:89:C1:A2:63:0D:16:72:ED:37:94:EF:1E:43:74:80:89:56:AE:B2:80:7D:26:5A:D3:FA:4E:38:85:49:7A:4D:2F:27:2A:64:74:BC:23:AD:52:31:98:88:25:E5:58:99:FA:A6:F1:15:16:F8:1C:17:C1:91:68:EF:33:06:02:E4:EE:AF:EE:8E:27:4E:D4:0F:A9:24:3B:C7:35:83:97:77:70:90:4B:10:91:AA:C9:88:45:8B:DA:9F:11:E5:E3:75:A2:93:9C:84:A0:7E:A0:4C:0F:9F:AF:34:C0:28:78:F7:1D:55:16:5A:9A:68:E7:64:8B:F6:7E:3F:07:20:F6:E5:52:C3:BA:A4:D2:AB:56:F8:3D:B2:F4:18:74:87:8E:A6:56:76:22:80:CE:08:43:48:76:E8:C4:78:EC:E3:61:ED:77:38:CF:AC:14:D0:41:21:C9:83:CE:94:31:FC:70:FF:03:A0:E8:BE:68:49:1E:65:88:08:4C:33:7D:95:75:01:2E:8A:62:B6:EC:17:46:00:07:25:62:E5:B1:E8:95:41:E8:4B:2E:AA:90:A6:3D:1A:FE:57:70:20:EE:6B:00:F8:44:D6:88:28:44:D2:26:64:2A:4C:5C:3F:7B:34:E6:61:20:18:09:02:58:F3:3E:54:94:CF:18:DA:69:92:CC:BD:20:9D:F9:9E:97:2B:44:89:D6:9E:09:86:57:69:90:41:48:5F:3D:91:0E:07:03:05:D5:EF:23:0E:A1:47:42:F8:64:0F:91:10:F8:89:E1:B7:1F:EB:6F:D7:00:FE:B6:BB:3A:E8:4F:A7:EE:F5:95:48:65:59:E0:72:FF:DA:E6:18:83:0A:C6:2E:30:D0:A7:9C:1F:EF:DE:4A:B5:C8:15:19:FE:D3:BD:E2:0E:82:98:AB:8D:3F:D8:1F:B6:E8:22:D9:CF:4D:49:F7:21:A0:D9:0F:E2:2D:76:5B:BA:CC:9E:7D:24:0A:DC:06:58:2E:DE:B3:09:86:46:26:40:95:AE:7C:D4:1D:A5:19:95:02:03:01:00:01
Authority Key Identifier D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0
Subject Key Identifier A3:E7:BE:7D:14:92:B7:75:2B:F0:68:96:CC:78:44:80:97:EE:2E:03
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://policy.vincasign.net>
CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]
Subject Alternative Name info@vincasign.net
CRL Distribution Points
<http://crl3.vincasign.net/casub.crl>
<http://crl4.vincasign.net/casub.crl>
Authority Info Access <http://www.vincasign.net/publickeys/caqualified.cer>
Basic Constraints IsCA: true - Path length: 1
Key Usage: keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 1C:A3:C0:A2:84:F8:94:DB:A0:A9:7C:83:53:1E:8C:06:2D:1D:54:F6:E7:F9:66:FA:32:3E:52:8E:F7:B9:B8:47
X509SubjectName
Subject CN: vinCAsign nebulaSUITE4 Authority
Subject O: VINTEGRIS SL

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *o+e+fRSSt3Ur8GiWzHhEgJfuLgM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2023-09-14T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

27.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

27.6.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority*

Name [es] *Certificados Cualificados emitidos por vinCAsign nebulaSUITE4 Authority*

Service digital identities

X509SubjectName

Subject CN: *vinCAsign nebulaSUITE4 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *o+e+fRSSt3Ur8GiWzHhEgJfuLgM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-11-18T22:00:00Z*

27.6.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

27.7 - Service (withdrawn): Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	<i>Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority</i>

Name	[es]	<i>Certificados cualificados emitidos por vinCAsign nebulaSUITE5 Authority</i>

Service digital identities

Certificate fields details

Version: *3*

Authority Key Identifier	<i>D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0</i>
Subject Key Identifier	<i>29:B0:A3:C6:79:6B:2A:8D:9F:58:35:AC:B1:FC:24:DA:7E:92:7C:11</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://policy.vincasign.net</i> <i>CPS text: [Certificado CA Subordinada. Ver https://policy.vincasign.net]</i>
Subject Alternative Name	<i>info@vincasign.net</i>
CRL Distribution Points	<i>http://crl3.vincasign.net/casub.crl</i> <i>http://crl4.vincasign.net/casub.crl</i>
Authority Info Access	<i>http://www.vincasign.net/publickeys/caqualified.cer</i>
Basic Constraints	<i>IsCA: true - Path length: 1</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>AA:AF:2F:29:EF:52:44:71:CB:4F:15:B7:2D:E6:A5:54:26:29:97:8F:B5:A9:14:A6:11:95:5C:75:AE:5E:F3:C3</i>

X509SubjectName

Subject CN:	<i>vinCAsign nebulaSUITE5 Authority</i>
Subject O:	<i>VINTEGRIS SL</i>
Subject OU:	<i>vinCAsign</i>
Subject 2.5.4.97:	<i>VATES-B62913926</i>
Subject L:	<i>HOSPITALET DE LLOBREGAT</i>
Subject ST:	<i>BARCELONA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>KbCjxnIrKo2fWDWssfwk2n6SfBE=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time 2023-09-14T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

27.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

27.7.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [en] Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority

Name [es] Certificados cualificados emitidos por vinCAsign nebulaSUITE5 Authority

Service digital identities

X509SubjectName

Subject CN: vinCAsign nebulaSUITE5 Authority

Subject O: VINTEGRIS SL

Subject OU: vinCAsign

Subject 2.5.4.97: VATES-B62913926

Subject L: HOSPITALET DE LLOBREGAT

Subject ST: BARCELONA

Subject C: ES

X509SKI

X509 SK I KbCjxnIrKo2fWDWssfwk2n6SfBE=

Issuer ST: BARCELONA
Issuer L: HOSPITALET DE LLOBREGAT
Issuer O: VINTEGRIS SLU
Issuer 2.5.4.97: VATES-B62913926
Issuer CN: CA Vintegris ROOT TrustServices
Subject C: ES
Subject ST: BARCELONA
Subject L: HOSPITALET DE LLOBREGAT
Subject O: VINTEGRIS SLU
Subject 2.5.4.97: VATES-B62913926
Subject CN: CA Vintegris TrustServices
Valid from: Mon Jan 24 14:09:20 CET 2022
Valid to: Thu Jan 22 14:09:19 CET 2032
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DA:A4:A7:31:5A:48:11:09:67:33:83:D5:86:04:71:52:47:39:88:5E:FB:D2:3A:
A9:5A:26:6E:79:9F:CB:1C:AB:2A:EF:82:1F:5E:0D:D0:45:95:99:FC:2F:A1:51:47:32:EC:F8:29:9E:C1:01:70:80:33:ED:68:9A:7D:B7:CD:57:DA:60:7E:13:3E:2D:5A:95:5F:6A:73:D0:10:2F:5
F:28:62:DD:16:64:92:92:20:AB:84:8C:BC:77:F9:4F:62:7E:DE:05:CF:8D:E9:23:08:35:7F:00:D9:F1:78:0F:2A:E7:4E:09:D4:72:63:CD:3B:77:DE:88:DD:2B:10:1F:C3:54:D5:0C:E1:82:69:25:
9C:82:04:71:91:15:B9:5F:9D:E0:5E:44:C6:A8:74:F8:17:BB:6A:47:F4:64:77:BE:46:90:3C:1F:DB:84:5E:6E:05:64:BC:1F:88:74:53:85:44:61:7B:35:99:FF:54:71:28:BF:AC:75:DD:34:06:9B:
7C:88:7D:5F:C1:80:A0:D7:0B:F8:71:84:B3:95:3D:90:DE:11:A3:DF:F7:5C:A2:E0:E7:93:E4:0D:81:F2:4F:8B:63:4F:8C:BD:04:31:93:76:8C:F8:79:A4:F1:F1:20:DC:6F:56:79:35:1C:7E:39:9
7:3F:96:AC:58:70:FF:57:A7:85:80:4B:52:18:2C:DA:F3:6C:A1:02:D2:01:9F:93:80:13:8E:55:4B:1B:75:C1:4A:1A:95:67:F8:7E:08:05:D5:4E:77:DF:59:8A:20:96:17:5D:EE:8F:C5:2A:9D:EF:
80:EB:98:4C:3E:24:C7:6D:5A:3D:50:9C:FE:FD:10:45:C7:7E:F5:E3:6D:8D:C5:D8:46:27:89:3E:26:AA:DE:8A:AE:76:E2:04:44:B9:FB:BB:29:CA:53:25:E5:F8:AD:51:4D:BB:F6:DF:D5:5C:52:
16:83:AD:15:60:EA:A9:31:06:83:96:53:DA:89:6E:B1:C2:3A:91:EE:89:6B:6C:E5:41:30:CE:CC:D1:AE:DD:E9:F2:60:FE:7C:7D:BB:5D:75:AF:0B:71:73:76:CC:8A:40:3E:1D:11:87:7D:16:40:
5D:A2:6A:A8:15:07:78:F8:1D:E8:3F:86:74:C7:C5:79:8B:6E:CB:2D:38:1D:5A:AD:97:40:9F:8E:E9:95:B6:49:7E:45:9E:78:90:45:D9:2F:CA:DC:F6:88:01:B6:03:A7:33:70:7F:5E:9E:B2:9
B:00:34:77:CF:80:A9:15:FC:E7:45:1C:CE:D6:B8:CA:28:86:E5:FE:0F:62:B0:6F:61:34:42:85:D3:0B:76:84:AD:68:AC:53:39:FE:32:BE:C5:6A:84:8B:19:A3:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 1*
Authority Key Identifier *FB:70:16:61:37:9E:DB:E7:32:97:40:3B:44:76:A2:7C:14:E3:B1:24*
Authority Info Access *<http://www.vincasign.net/publickeys/cavintegris.cer>*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://policy.vincasign.net>
CRL Distribution Points *<http://crl1.vincasign.net/cavintegris.crl>*
<http://crl2.vincasign.net/cavintegris.crl>
Subject Key Identifier *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *75:A6:33:0E:D1:67:B2:87:7A:43:87:93:13:03:BA:93:D7:8F:72:F5:5A:13:7A:A5:50:6F:D3:29:30:B7:E2:97*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TrustServices*

X509SKI

X509 SK I *mSDQwgtdwJ0jXtjbTiE29P0sKkl=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2025-06-10T00:00:00Z*

27.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.8.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.8.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.47155.2.1.1*

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.1.51

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.2.1

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.2.51

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.2.11

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.2.151

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.4.1

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.4.11

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.10.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.10.51

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.11.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.5.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.6.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.6.51

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.13.1

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.2.150

Description

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.14.1

Description

Description

27.8.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Cualificados emitidos por «CA Vintegris TrustServices»*

Name *[en]* *Qualified Certificates issued by «CA Vintegris TrustServices»*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TrustServices*

X509SKI

X509 SK I *mSDQwgt dwJ0jXtjbTiE29P0sKkl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2025-02-05T00:00:00Z*

27.8.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.8.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.8.4.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.1.1

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.1.51

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.2.1

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.2.51

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.2.11

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.2.151

Description

Policy Identifier:

Identifier [OIDAURN] urn:oid:1.3.6.1.4.1.47155.2.4.1

Description

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.4.11</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.10.1</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.10.51</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.11.1</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.5.1</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.6.1</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.6.51</i>
Description		
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.47155.2.13.1</i>
Description		
Description		

27.8.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Cualificados emitidos por «CA Vintegris TrustServices»*

Name *[en]* *Qualified Certificates issued by «CA Vintegris TrustServices»*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TrustServices*

X509SKI

X509 SK I *mSDQwgt dwJ0jXtjbTiE29P0sKkl=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-10-10T00:00:00Z*

27.8.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

27.8.5.5 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

27.8.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.1.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.1.51

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.2.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.2.51

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.2.11

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.2.151

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.4.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.4.11

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.10.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.10.51

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.47155.2.11.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.5.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.6.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47155.2.6.51

Description

27.9 - Service (granted): Sellos de tiempo cualificados emitidos por «CA Vintegris TSA1 TrustServices»

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [es] Sellos de tiempo cualificados emitidos por «CA Vintegris TSA1 TrustServices»

Name [en] Qualified time stamps issued by «CA Vintegris TSA1 TrustServices»

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 76172955933336056506690947715413989888149560314

Authority Key Identifier *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*

Authority Info Access *http://www.vincasign.net/publickeys/catrusterservices.crt*
http://ocsp.vincasign.net

Certificate Policies *Policy OID: 1.3.6.1.4.1.47155.2.9.1*
CPS pointer: https://policy.vincasign.net
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl1.vincasign.net/catrusterservices.crl*
http://crl2.vincasign.net/catrusterservices.crl

Subject Key Identifier *9E:14:7B:B5:C9:00:95:3E:F1:0B:A5:4F:D7:9D:4D:AE:C5:F4:50:33*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A5:0B:0A:34:BE:70:FD:13:4F:F2:F4:8E:3D:7F:65:51:7D:46:BE:20:04:CB:7A:F0:17:8E:C2:04:38:3E:B5:24*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TSA1 TrustServices*

X509SKI

X509 SK I *nhR7tckAIT7xC6VP151NrsX0UDM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

27.10 - Service (granted): Sellos de tiempo cualificados emitidos por «CA Vintegris TSA2 TrustServices»

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>	
Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name		
Name	[es]	Sellos de tiempo cualificados emitidos por «CA Vintegris TSA2 TrustServices»
Name	[en]	Qualified time stamps issued by «CA Vintegris TSA2 TrustServices»

Service digital identities

Certificate fields details

```
Version: 3
Serial Number: 177562648785505154439331988964866123659702128382
```

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *BARCELONA*

Issuer L: *HOSPITALET DE LLOBREGAT*

Issuer O: VINTEGRIS SLU

Issuer 2.5.4.97:	VATES-B62913926
Issuer CN:	CA Vintegris TrustServices
Subject C:	ES
Subject ST:	BARCELONA
Subject L:	HOSPITALET DE LLOBREGAT
Subject O:	VINTEGRIS SLU
Subject 2.5.4.97:	VATES-B62913926
Subject CN:	CA Vintegris TSA2 TrustServices
Valid from:	Thu Mar 03 16:12:33 CET 2022
Valid to:	Tue Mar 02 16:12:33 CET 2027
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:85:85:36:94:B9:80:AF:1A:E8:31:0F:46:94:F5:A6:0B:5B:F8:2D:A0:DD:E6:69: 0C:60:C6:5B:FD:BA:C1:A5:90:75:F7:98:95:FA:7B:D4:0B:DA:3C:B1:59:E2:0A:A1:58:80:12:08:61:3C:85:6A:97:00:F5:17:33:B4:ED:71:24:20:BC:BC:16:85:66:09:E9:F5:8A:B0:A6:11:85:3 3:A9:8B:74:FD:E4:40:B6:EA:28:64:EE:8E:5A:CF:B9:71:FF:58:F9:CF:06:F8:AD:AD:9A:AF:2D:2A:6B:AA:80:1C:8C:C6:97:C6:02:0F:66:40:0B:E4:BC:CC:7A:98:C6:25:14:30:07:C4:CD:44:85 1B:14:3A:BB:00:20:8E:76:F8:62:A2:EF:C8:82:BF:DF:19:5C:BF:85:F1:80:FE:5C:88:96:A6:1A:65:D1:4E:4C:22:08:E6:EC:D2:EA:03:7F:06:D6:62:41:0C:10:35:82:E3:F8:A7:9D:26:10:76:1 8:2F:CE:C0:A3:C7:E8:59:C1:C8:03:96:24:CF:58:99:CE:F1:5A:B1:51:94:F7:B1:80:82:9D:EB:84:6C:50:28:EA:E9:06:73:11:AB:8C:AD:C2:34:15:85:82:57:E6:C2:BC:70:74:68:ED:50:BC:55 6F:D1:AA:3D:C9:A6:60:8A:0C:8E:52:06:C8:BD:B9:98:82:EF:45:6E:C4:53:DF:E8:D3:46:4C:58:0C:50:BA:56:23:C9:40:1C:CC:9C:83:EE:AE:39:A7:AC:5B:47:20:1A:B3:7C:40:9F:3F:9A:35 D6:AF:49:C8:B1:31:35:7B:81:E9:62:E4:D0:83:48:28:81:7B:31:FE:5D:94:AF:57:CA:FC:65:62:DF:DA:15:E7:13:73:F9:C4:6C:D4:2A:BC:6C:69:64:31:41:85:6B:51:A6:ED:EE:87:00:00:5D:1 9:8E:04:E3:5C:89:E4:6B:64:AA:22:AC:15:D8:1E:3D:38:65:C4:13:DD:44:9B:13:66:51:B4:0E:92:EC:D2:2E:8A:80:20:84:4A:97:75:F2:C3:9B:95:D8:13:AE:EF:A8:46:D7:89:08:39:72:D1:C E:B2:8C:83:46:E5:BD:54:AC:17:19:E3:1A:A1:92:62:7B:86:5E:0E:94:C4:78:11:E7:F0:CE:6D:71:B1:BE:E5:E9:6C:77:E9:1D:EF:98:C4:1A:4B:41:76:D7:46:75:A1:44:F4:B5:52:3F:FD:4E:40 1A:68:9E:D1:3F:F4:ED:3F:5E:6D:62:5A:D1:C7:5A:C0:FA:4B:C7:3A:7D:52:0A:6D:3E:9A:6C:A7:AD:32:5C:10:BC:58:EB:29:6E:2B:F3:93:FC:B1:DC:1A:31:0D:02:03:01:00:01 </pre>
Basic Constraints	IsCA: false
Authority Key Identifier	99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42
Authority Info Access	http://www.vincasign.net/publickeys/catrustservices.crt http://ocsp.vincasign.net
Certificate Policies	Policy OID: 1.3.6.1.4.1.47155.2.9.1 CPS pointer: https://policy.vincasign.net CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico] Policy OID: 0.4.0.194112.1.1
Extended Key Usage	id_kp_timeStamping
QCStatements - crit. = false	id_etsi_qcs_QcCompliance id_etsi_qcs_RetentionPeriod: 15
CRL Distribution Points	http://crl1.vincasign.net/catrustservices.crl http://crl2.vincasign.net/catrustservices.crl
Subject Key Identifier	EE:FE:81:F8:13:67:83:85:AA:7F:29:F6:4B:49:A0:A5:5A:97:F9:C4
Key Usage:	digitalSignature - nonRepudiation

Thumbprint algorithm: *SHA-256*

Thumbprint: *7F:05:13:8F:19:91:8E:6F:38:D2:86:75:A1:E9:C1:D5:A2:A5:E9:5D:13:1B:47:32:D2:31:21:CA:B6:25:05:5D*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TSA2 TrustServices*

X509SKI

X509 SK I *7v6B+BNng4Wqfyn2S0mgpVqX+cQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2022-10-10T00:00:00Z

27.11 - Service (withdrawn): Certificados Cualificados emitidos por «CA Vintegris SSL TrustServices»

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [es] *Certificados Cualificados emitidos por «CA Vintegris SSL TrustServices»*

Name [en] *Qualified Certificates issued by «CA Vintegris SSL TrustServices»*

Service digital identities

Certificate fields details

Version: *3*

Authority Info Access	<i>http://www.vincasign.net/publickeys/cavintegris.cer</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://policy.vincasign.net</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
CRL Distribution Points	<i>http://crl1.vincasign.net/cavintegris.crl</i> <i>http://crl2.vincasign.net/cavintegris.crl</i>
Subject Key Identifier	<i>11:26:8E:9A:93:EF:0D:83:3A:54:1C:D8:70:17:29:CE:FD:D0:49:1B</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>ED:3F:7F:E9:38:D9:53:AF:0B:E0:99:18:D7:E5:9E:A2:0B:66:2A:FC:46:25:18:7C:A2:44:63:D6:55:20:A2:3F</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject ST:	<i>BARCELONA</i>
Subject L:	<i>HOSPITALET DE LLOBREGAT</i>
Subject O:	<i>VINTEGRIS SLU</i>
Subject 2.5.4.97:	<i>VATES-B62913926</i>
Subject CN:	<i>CA Vintegris SSL TrustServices</i>

X509SKI

X509 SK I	<i>ESaOmpPvDYM6VBzYcBcpzv3QSRs=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2024-02-22T01:00:00Z</i>

27.11.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

27.11.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Certificados Cualificados emitidos por «CA Vintegris SSL TrustServices»*

Name *[en]* *Qualified Certificates issued by «CA Vintegris SSL TrustServices»*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris SSL TrustServices*

X509SKI

X509 SK I *ESaOmpPvDYM6VBzYcBcpzv3QSRs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-10-10T00:00:00Z*

27.11.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

27.12 - Service (granted): Qualified time stamps issued by «CA Vintegris TSA3 TrustServices»

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Name	[en]	Qualified time stamps issued by «CA Vintegris TSA3 TrustServices»

Service digital identities

Version: 3

Serial Number: 385991196561942264113361202170992845073715305999

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *BARCELONA*

Issuer L: *HOSPITALET DE LLOBREGAT*

Issuer 0: VINTEGRIS SLU

Issuer 2.5.4.97: *VATES-B62913926*

Issuer CN: CA Vintegris TrustServices

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject 0: VINTEGRIS SLU

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TSA3 TrustServices*

Valid from: *Thu Nov 07 12:41:11 CET 2024*

Valid to: *Tue Nov 06 12:41:10 CET 2029*

Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:70:72:5E:C5:EB:01:5A:3D:C8:F2:A4:08:FB:42:52:A7:BE:AA:64:A0:AF:65:E7:45:9A:2C:EE:15:ED:A8:38:ED:C3:74:43:DD:16:B8:41:90:7A:17:88:B9:A7:52:AD:F8:A6:DB:27:77:4D:34:AC:98:C6:68:AD:31:40:C0:6C:89*

Basic Constraints *IsCA: false*

Authority Key Identifier *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*

Authority Info Access *http://www.vincasign.net/publickeys/catrusterservices.crt*
http://ocsp.vincasign.net

Certificate Policies *Policy OID: 1.3.6.1.4.1.47155.2.9.1*
CPS pointer: https://policy.vincasign.net
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl1.vincasign.net/catrusterservices.crl*
http://crl2.vincasign.net/catrusterservices.crl

Subject Key Identifier *21:61:6C:A7:C0:5A:08:ED:90:2A:94:14:5F:25:7A:7A:AE:EF:18:FE*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0A:E7:65:97:DF:64:53:93:93:DB:29:7D:2B:A6:FB:B3:C3:C2:1F:39:8F:46:FD:CC:A1:5A:A5:0D:77:AB:8B:A8*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

X509 SK I *IWFsp8BaCO2QKpQUXyV6eq7vGP4=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time	2025-04-08T02:00:00Z

27.13 - Service (granted): Qualified time stamps issued by «CA Vintegris TSA4 TrustServices»

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name	[en]	Qualified time stamps issued by «CA Vintegris TSA4 TrustServices»

Name	[es]	<i>Servicio Sellos de tiempo cualificados emitidos por «CA Vintegris TSA4 TrustServices»</i>

Service digital identities

Certificate fields details

Version: 3

Serial Number: 36891058032294426041987194668158580923901085517

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *BARCELONA*
Issuer L: *HOSPITALET DE LLOBREGAT*
Issuer O: *VINTEGRIS SLU*
Issuer 2.5.4.97: *VATES-B62913926*
Issuer CN: *CA Vintegris TrustServices*
Subject C: *ES*
Subject ST: *BARCELONA*
Subject L: *HOSPITALET DE LLOBREGAT*
Subject O: *VINTEGRIS SLU*
Subject 2.5.4.97: *VATES-B62913926*
Subject CN: *CA Vintegris TSA4 TrustServices*
Valid from: *Thu Nov 07 12:56:16 CET 2024*
Valid to: *Tue Nov 06 12:56:15 CET 2029*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:AC:44:EE:C8:17:5D:5B:CF:2A:C4:8C:57:77:2F:3B:A3:3B:FC:51:A3:51:18:A2:33:EF:B3:5C:A8:11:64:DB:B2:51:FC:C5:77:D7:AA:BB:78:16:24:B1:90:51:A6:FE:5D:00:EA:98:0D:F4:5B:02:E2:8C:8E:9E:E8:96:E2:03:FA*
Basic Constraints *IsCA: false*
Authority Key Identifier *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*
Authority Info Access *http://www.vincasign.net/publickeys/catrustservices.crt*
http://ocsp.vincasign.net
Certificate Policies *Policy OID: 1.3.6.1.4.1.47155.2.9.1*
CPS pointer: https://policy.vincasign.net
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
Policy OID: 0.4.0.194112.1.1
Extended Key Usage *id_kp_timeStamping*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
CRL Distribution Points *http://crl1.vincasign.net/catrustservices.crl*
http://crl2.vincasign.net/catrustservices.crl

Subject Key Identifier *65:DA:05:CE:95:77:51:D7:11:25:53:31:A5:29:00:D5:B9:E6:67:82*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A5:83:76:8E:B3:78:14:1B:52:A7:FF:F6:EC:49:A1:19:87:A3:ED:25:02:61:EE:64:54:5E:54:39:21:03:F6:2E*

X509SubjectName

Subject C: *ES*

Subject ST: *BARCELONA*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject O: *VINTEGRIS SLU*

Subject 2.5.4.97: *VATES-B62913926*

Subject CN: *CA Vintegris TSA4 TrustServices*

X509SKI

X509 SK I *ZdoFzpV3UdcRJVMxpSkA1bnmZ4I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-04-08T02:00:00Z*

28 - TSP: ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.**TSP Name**

Name *[en]* *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

Name *[es]* *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

TSP Trade Name

Name *[en]* *esFIRMA*

Name *[es]* *esFIRMA*

Name *[en]* *VATES-A50878842*

Name *[en]* *AULOCE S.A.U.*

Name *[en]* *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

Name *[en]* *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

PostalAddress

Street Address *[en]* *Calle Bari 39 (Edificio Binary Building)*

Locality *[en]* *Zaragoza*

State Or Province *[en]* *Zaragoza*

Postal Code *[en]* *50197*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Calle Bari 39 (Edificio Binary Building)*

Locality *[es]* *Zaragoza*

State Or Province *[es]* *Zaragoza*

Postal Code *[es]* *50197*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *http://www.esfirma.com*

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificates issued by ESFIRMA AC AAPP
Name	[es]	Certificados Reconocidos emitidos por ESFIRMA AC AAPP

Version:	3
Serial Number:	6494265473925466579
X509 Certificate	-----BEGIN CERTIFICATE-----

Signature algorithm:	SHA512withRSA
Issuer C:	ES

Issuer L: Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

Issuer O: AULOCE S.A.U.

Issuer OU: AUTORIDAD DE CERTIFICACION ESFIRMA

Issuer CN: ESFIRMA AC RAIZ

Issuer 2.5.4.97: VATES-A50878842

Subject C: ES

Subject L: Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

Subject O: AULOCE S.A.U.

Subject OU: AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

Subject CN: ESFIRMA AC AAPP

Subject 2.5.4.97: VATES-A50878842

Valid from: Thu Apr 28 18:05:14 CEST 2016

Valid to: Sat Apr 28 18:05:14 CEST 2029

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:9B:2C:F3:07:C9:9E:9E:ED:20:66:2B:84:BC:B0:21:DE:78:37:76:19:B3:ED:
9C:F1:9D:12:70:94:4A:71:46:18:8C:09:D8:76:0E:F8:F1:E7:F4:2A:E1:A3:9C:76:CD:69:17:F0:B8:CA:C6:DF:08:67:3B:F9:FF:01:97:98:01:A7:0F:61:43:FE:12:5A:B8:AE:23:6C:EF:23:A3:A5:
57:94:F9:08:4C:C1:27:DC:65:5A:BE:C2:42:92:1C:62:33:9F:05:05:8F:DC:64:87:41:D4:07:40:53:BC:9A:58:59:68:B9:40:C7:FA:E8:FC:3B:77:76:72:2B:0D:D9:0A:A0:9C:88:DD:70:23:07:5
4:F6:CB:C8:EB:32:4F:39:0E:57:BA:33:F1:48:E8:E5:DF:D7:55:8F:86:70:4B:26:69:BF:32:15:C3:28:4E:A7:70:4A:05:E5:77:AC:6B:31:6A:AD:E5:02:96:03:89:4B:40:AF:72:4E:55:0E:60:1E:3
9:85:4B:EB:F9:07:47:A6:1E:3C:33:89:4A:8D:EC:6F:40:50:AE:97:7B:EB:93:FC:AB:45:D2:CB:02:79:96:86:D1:01:64:47:30:45:A8:BD:74:CB:A9:85:C7:91:57:76:1A:09:F5:F8:34:22:6F:A3:
CB:FB:EB:85:F9:A7:24:04:0A:B3:D9:0D:47:87:39:A7:00:82:ED:47:8A:7A:93:21:F3:48:DD:5E:9D:A3:37:42:36:25:26:5C:BF:88:3D:60:9D:B3:3B:F7:6A:11:86:07:86:4F:13:88:24:2A:DD:2
1:16:D8:FF:55:D9:47:6D:89:90:CD:62:64:50:7C:3C:DA:1A:0B:20:95:DD:AC:99:BF:03:11:B1:F3:CA:A2:3E:F5:AF:18:40:66:C7:6D:5A:42:C0:CF:D3:98:45:BB:76:59:A8:09:5C:BD:95:5F:2
E:97:75:1C:42:C2:7C:FD:21:58:70:26:37:7E:CD:F0:98:C1:E1:B3:50:1B:5B:A2:F6:DF:AC:27:65:88:0F:61:25:32:04:6E:88:CD:A4:D9:86:42:49:F2:1D:53:9E:0B:58:EA:93:26:80:CE:25:63:
AA:30:CB:4A:E2:F5:2F:39:DC:20:A7:AA:B1:53:BA:C2:78:A6:AE:3B:B9:3F:45:1F:A7:6E:76:C0:93:A3:B7:BA:7B:D3:B9:8B:A3:99:94:C1:FA:E9:74:1F:59:F8:D0:E0:4D:54:51:39:18:03:13:F
8:D6:78:1A:99:0A:30:44:6D:6C:B8:C2:8B:F5:3F:8B:FD:66:6A:C7:5E:F9:1F:F0:5A:8B:04:41:F2:A9:36:F6:24:9D:37:B8:06:20:C7:52:06:D5:47:C6:F3:02:03:01:00:01

```

Authority Info Access <https://www.esfirma.com/doc-pki/esfirma-acraiz.crt>

Subject Key Identifier 61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier FC:EF:B3:1E:C8:78:35:F7:2B:39:3F:16:D4:F5:8C:C1:D1:71:B2:99

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://www.esfirma.com/doc-pki/>
CPS text: [Autoridad de certificación Intermedia de esFirma. Ver <https://www.esfirma.com/doc-pki/>]

CRL Distribution Points <https://crls1.esfirma.com/acraiz/acraiz.crl>
<https://crls2.esfirma.com/acraiz/acraiz.crl>

Subject Alternative Name info@esfirma.com

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A2:8B:23:0D:EF:38:3D:C6:A0:39:5F:37:63:E1:01:CC:8C:3F:F6:4D:96:2C:6A:F3:3A:59:28:41:A9:61:26:82*

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)*

Subject O: *AULOCE S.A.U.*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Subject CN: *ESFIRMA AC AAPP*

Subject 2.5.4.97: *VATES-A50878842*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2018-06-25T00:00:00Z*

Scheme Service Definition URI

URI [en] *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI [es] *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

28.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.47281.1.2.1*

28.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

28.1.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

28.1.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

28.1.5 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by ESFIRMA AC AAPP

Name	[es]	Certificados Reconocidos emitidos por ESFIRMA AC AAPP

Service digital identities**X509SubjectName**

Subject C:	ES
Subject L:	Zaragoza (see current address at https://www.esfirma.com/doc-pki/)
Subject O:	AULOCE S.A.U.
Subject OU:	AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP
Subject CN:	ESFIRMA AC AAPP
Subject 2.5.4.97:	VATES-A50878842

X509SKI

X509 SK I	YYlsuzwevS1E4MvwZ0ApgE21o1A=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2018-05-24T00:00:00Z

28.1.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47281.1.2.1

28.1.5.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

28.1.5.3 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

28.1.5.4 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

28.1.6 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [en] Qualified Certificates issued by ESFIRMA AC AAPP

Name [es] Certificados Reconocidos emitidos por ESFIRMA AC AAPP

Service digital identities

X509SubjectName

Subject C: ES

Subject L: Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

Subject O: AULOCE S.A.U.

Subject OU: AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

Subject CN: ESFIRMA AC AAPP

Subject 2.5.4.97: VATES-A50878842

X509SKI

X509 SK I YYlsuzwevS1E4MvwZ0ApgE21o1A=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

28.1.6.5 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47281.1.2.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47281.1.2.2

28.1.6.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

28.1.7 - History instance n.3 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name	[en]	Qualified Certificates issued by ESFIRMA AC AAPP

Name [es] *Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)*

Subject O: *AULOCE S.A.U.*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Subject CN: *ESFIRMA AC AAPP*

Subject 2.5.4.97: *VATES-A50878842*

X509SKI

X509 SK I *YYIsuzwevS1E4MvwZ0ApgE21o1A=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

Status Starting Time *2016-06-23T22:00:00Z*

28.1.7.7 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.47281.1.2.1*

Policy Identifier:

Identifier [OIDAURN] *urn:oid:1.3.6.1.4.1.47281.1.2.2*

28.2 - Service (withdrawn): Qualified timestamps issued by ESFIRMA TSA

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *AULOCE S.A.U.*

Subject L: *Zaragoza*

Subject C: *ES*

Valid from: *Tue May 23 15:28:05 CEST 2017*

Valid to: *Fri May 23 15:28:05 CEST 2025*

Public Key:
 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:60:A9:3F:AE:03:C8:F9:27:DC:B9:61:DB:18:FA:CD:F5:95:E8:F1:4B:94:47:42:E6:22:C2:EB:10:70:45:87:48:34:7E:D2:72:DC:6A:0A:F4:79:57:1F:5F:A6:52:53:78:96:A0:23:83:02:97:DD:03:0D:A2:88:6D:8B:82:55:F8:83:A1:F9:21:4A:D4:12:3E:77:DF:3B:EC:AD:31:0E:E9:E8:96:80:25:50:A1:E3:F7:88:1C:B9:9C:2E:E9:FA:4B:10:A4:91:D3:68:0A:7E:A5:0B:C1:B8:1B:1B:A7:48:AC:11:6E:18:DB:61:0B:DD:01:08:C4:27:5F:DA:93:E5:88:E3:CF:66:A5:C5:E4:52:42:62:CE:7E:E9:D3:F0:AB:9B:8B:4E:DC:48:5A:6B:83:95:6C:E3:6E:F0:78:9B:AD:6C:96:D1:B4:3D:AA:D3:6F:0B:4C:74:93:F5:1F:24:95:5E:DD:46:AA:07:86:27:3A:C7:FF:B8:F0:32:CF:83:15:1E:1A:50:23:87:E9:62:C6:72:EE:01:49:6C:CE:44:E6:29:0E:60:6B:CC:3C:6D:99:D8:3E:E3:EB:14:0F:E2:F8:C0:F6:4C:50:E2:38:65:57:42:4E:0B:C0:F2:8B:DB:62:31:CC:F0:79:C8:09:0C:27:43:43:46:15:BE:09:36:7E:F8:DF:FE:1B:36:70:8F:BC:82:FF:98:65:03:7D:7B:1E:66:F6:61:39:D1:1C:BE:D1:D7:56:5A:E4:69:F6:F0:76:EF:75:AF:6D:D8:C6:BF:00:F2:E3:D6:E6:91:E3:5E:46:E6:15:00:89:3A:BB:70:97:72:6A:04:61:9A:A3:36:60:51:93:D9:3C:15:C7:0F:0A:7B:14:35:98:D5:C9:89:7A:E4:87:D3:2B:3D:D4:0D:64:AD:65:39:84:61:C0:F2:79:3B:0C:29:55:7E:50:6D:7E:DA:12:3D:83:1C:28:33:84:C5:78:D2:E7:E9:9B:D3:97:02:6D:71:55:AF:CB:64:31:EB:11:90:3E:86:D4:39:04:0B:5B:14:C8:A8:B9:10:AA:C6:FC:BD:C2:9F:D2:38:9F:D0:6D:31:15:BE:FA:37:04:05:EB:7A:DF:71:14:DC:68:94:75:D7:27:44:35:A8:D9:FF:5F:B1:AA:A3:E8:1E:15:84:46:1B:65:A0:72:A9:CB:B1:E4:72:0E:BF:3C:9B:8F:85:67:33:42:2D:CE:9F:CE:3C:B3:7B:E7:AE:93:14:70:22:AD:57:4F:D8:A7:AC:86:F9:53:F9:A0:69:AD:A1:CD:26:8B:15:13:A5:59:50:44:EB:E3:EE:C0:95:6F:72:52:7D:B4:A6:DB:31:B7:02:03:01:00:01

Certificate Policies
Policy OID: 0.4.0.194112.1.1
Policy OID: 1.3.6.1.4.1.47281.1.5.2
CPS pointer: <https://www.esfirma.com/doc-pki/>
CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte <https://www.esfirma.com/doc-pki/>]

Subject Key Identifier *34:6A:D2:15:11:32:DD:1C:DD:A7:59:8F:E9:09:D4:8E:A6:FC:8E:77*

Authority Key Identifier *61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points
<http://crls1.esfirma.com/acaapp/acaapp.crl>
<http://crls2.esfirma.com/acaapp/acaapp.crl>

Authority Info Access
<http://ocsp1.esfirma.com/acaapp/>
<http://ocsp2.esfirma.com/acaapp/>
<http://www.esfirma.com/doc-pki/esfirma-acaapp.crt>

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Issuer Alternative Name *info@esfirma.com*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A7:DC:18:B2:E8:2F:38:19:8E:AC:20:69:90:EE:5C:62:B9:85:92:82:A5:AB:B7:7A:C2:A8:65:A5:85:2C:97:A2*

X509SubjectName

Subject CN: *ESFIRMA TSA*

Subject 2.5.4.97: *VATES-A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *AULOCE S.A.U.*

Subject L: *Zaragoza*

Subject C: *ES*

X509SKI

X509 SK I *NGrSFREy3Rzdp1mP6QnUjqb8jnc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2018-06-25T00:00:00Z

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

28.2.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name [en] *Qualified timestamps issued by ESFIRMA TSA*

Name [es] *Sellos de tiempo cualificados emitidos por ESFIRMA TSA*

Service digital identities**X509SubjectName**

Subject CN: *ESFIRMA TSA*

Subject 2.5.4.97: *VATES-A50878842*

X509 SK I NGrSFREy3Rzdp1mP6QnUjqb8jnc=

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time 2018-05-24T00:00:00Z

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services. [es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.	

Name	[en]	Qualified Certificates issued by ESFIRMA AC AAPP 2

Name [es] *Certificados Cualificados emitidos por ESFIRMA AC AAPP 2*

Version: 3

Serial Number: 4761709294065530426

[illegible]

-----END CERTIFICATE-----

Signature algorithm:	SHA512withRSA
Issuer CN:	ESFIRMA AC RAIZ 2
Issuer SERIAL NUMBER:	A50878842
Issuer OU:	AUTORIDAD DE CERTIFICACION ESFIRMA
Issuer O:	ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA
Issuer L:	ZARAGOZA
Issuer C:	ES
Subject CN:	ESFIRMA AC AAPP 2
Subject SERIAL NUMBER:	A50878842
Subject OU:	AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP
Subject O:	ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA
Subject L:	ZARAGOZA
Subject C:	ES
Valid from:	Thu Nov 02 14:12:47 CET 2017
Valid to:	Sat Nov 02 14:12:47 CET 2030
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:8F:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:88:B0:A4:22:B9:A1:D6:16:21:7B:07:0D:52:3E:8D:18:79:D0:7D:16:C5:4F:A2 EA:2D:F1:D6:18:90:F7:04:70:30:80:4F:95:60:09:C8:22:8E:91:89:E3:72:E7:29:03:96:2A:3E:60:92:F7:C2:58:48:E7:11:33:AC:C3:06:D3:C0:D4:F6:D5:D5:CB:31:5A:16:86:3A:6D:D8:D6: 45:14:3D:2C:55:4D:FC:9C:28:87:CA:B1:6E:D0:0A:53:6D:BE:D5:F1:EA:00:DC:7D:E5:6C:01:82:3A:7E:C9:10:F6:23:FD:2C:23:7C:05:37:F1:0F:02:5A:0D:FB:44:7F:D1:0D:8B:A3:B1:C8:C5: BB:A4:33:E5:A7:4D:BA:6A:1B:7B:2B:BA:3B:B7:5A:6B:0E:2B:2E:63:DA:9E:7E:2B:76:B7:FF:C3:36:7D:37:CF:F6:4E:4E:DA:FF:73:C4:F2:C1:23:EE:69:A9:CB:76:4E:8E:A9:67:C0:F1:03:45:0 6:03:3C:A1:C3:80:AE:59:E6:8F:A7:3C:73:02:78:E9:F0:65:83:82:38:7B:80:8F:66:6A:12:D8:44:3A:DA:7F:07:D2:42:7F:09:51:72:42:1E:B2:74:30:5D:AA:A2:EB:46:8C:E3:0E:35:D8:30:03: 4C:AE:52:CB:23:B9:84:50:23:94:50:76:87:06:35:F1:3C:23:73:0D:32:1C:43:AE:A3:29:5F:31:19:67:72:64:A9:2B:08:21:2E:5F:93:8F:EF:BC:AB:E9:38:1D:12:F4:E1:C7:08:ED:A6:E4:E8:70: 74:80:0B:2F:95:6F:A7:3A:3D:19:9A:03:06:FB:27:9A:8F:AA:AE:05:4A:97:96:09:11:A6:DB:16:CC:42:EC:18:88:41:C1:72:A2:0C:4A:B0:D6:C8:6A:0F:E0:5A:B6:16:5C:CF:41:EC:F7:EE:0A:2 D:BF:CF:A7:1B:93:26:81:F4:7A:BF:AB:D6:5D:58:EF:4B:2F:92:77:39:0A:88:D4:26:82:93:24:D8:81:8D:A2:EC:FA:4B:2F:FB:ED:5D:A0:87:3AE6:58:C7:D6:1F:CE:7F:73:49:AB:9F:1B:05:67: DA:77:94:F0:EB:1A:03:B2:A7:B7:98:5F:B8:C5:CC:65:1B:42:A8:54:AE:9A:30:AD:95:14:AE:D3:64:E1:18:0C:8B:E4:36:DA:4B:4A:95:F4:D8:5C:C2:FD:0B:C0:E5:0D:DE:59:91:A6:99:E3:D1: 55:C0:8C:F3:0C:18:57:FC:2C:E2:86:C4:7B:C3:C6:19:C3:E8:95:95:CA:4A:C8:DB:7E:9D:4C:F2:D4:91:C7:4A:F1:66:94:E6:EE:DD:E6:5E:BD:60:21:2F:23:9D:02:03:01:00:01 </pre>
Authority Info Access	https://www.esfirma.com/doc-pki/esfirma-acraiz2.crt http://ocsp.esfirma.com/acraiz2/
Subject Key Identifier	F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58
Basic Constraints	IsCA: true - Path length: 0
Authority Key Identifier	83:80:E5:D6:27:BD:EF:30:B2:AE:1D:9D:CA:A8:F2:32:14:C7:13:32
Certificate Policies	Policy OID: 2.5.29.32.0 CPS pointer: https://www.esfirma.com/doc-pki/ CPS text: [Autoridad de certificación AAPP 2 de esFirma. Ver https://www.esfirma.com/doc-pki/]
CRL Distribution Points	https://crls1.esfirma.com/acraiz/acraiz2.crl https://crls2.esfirma.com/acraiz/acraiz2.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2C:18:23:61:9D:80:73:11:6C:8F:14:8B:D3:85:79:DE:9C:05:39:16:02:DB:CE:B9:65:73:E4:A1:88:E1:32:6E*

X509SubjectName

Subject CN: *ESFIRMA AC AAPP 2*

Subject SERIAL NUMBER: *A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject L: *ZARAGOZA*

Subject C: *ES*

X509SKI

X509 SK I *9kDvw6crTeW/Men67sN5eR8qA1g=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-10-26T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

28.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

28.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**28.3.3 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified Certificates issued by ESFIRMA AC AAPP 2

Name

[es]

Certificados Cualificados emitidos por ESFIRMA AC AAPP 2

Service digital identities**X509SubjectName****Subject CN:**

ESFIRMA AC AAPP 2

Subject SERIAL NUMBER:

A50878842

Subject OU:

AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

Subject O:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Subject L:

ZARAGOZA

Subject C:

ES

X509SKI**X509 SK I**

9kDvw6crTeW/Men67sN5eR8qA1g=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2018-06-25T00:00:00Z

28.3.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**28.3.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

Issuer O:	<i>ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA</i>
Issuer L:	<i>ZARAGOZA</i>
Issuer C:	<i>ES</i>
Subject CN:	<i>ESFIRMA TSA 2</i>
Subject 2.5.4.97:	<i>VATES-A50878842</i>
Subject SERIAL NUMBER:	<i>A50878842</i>
Subject OU:	<i>AUTORIDAD DE CERTIFICACION ESFIRMA</i>
Subject O:	<i>ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA</i>
Subject L:	<i>ZARAGOZA</i>
Subject C:	<i>ES</i>
Valid from:	<i>Wed Jun 20 11:28:38 CEST 2018</i>
Valid to:	<i>Tue Jun 20 11:28:38 CEST 2023</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:94:C8:59:19:2C:68:1A:A8:0E:47:E7:ED:62:66:82:83:60:D1:70:11:B9:17:76: 8D:91:43:92:4E:A3:C0:2E:01:83:8C:39:DD:34:B5:B3:CE:F9:91:7F:5E:59:78:BE:51:F8:E6:25:72:2A:5D:BE:5E:A9:79:E8:43:C9:AE:7B:E0:76:D5:0C:A8:92:F7:E8:DD:33:05:04:6A:A3:E2:A 9:C1:0E:A7:29:4E:A5:83:3D:97:15:C0:7E:1D:0B:2F:FD:95:08:80:AB:D1:C3:72:CC:18:5A:AD:FD:03:F4:4E:3C:B3:D8:38:DE:4A:92:04:00:DA:69:68:F9:A0:4E:D2:3F:E3:EB:3E:0E:FD:64:AE A3:EC:62:BC:7E:D4:33:2A:91:48:D3:ED:2C:F6:32:86:38:EA:CD:4C:56:5E:9F:FD:57:DD:47:A3:CE:24:BB:D7:E8:80:53:D4:52:DC:44:46:DB:4F:C8:23:B2:AF:90:DD:6C:59:5F:A4:50:E9:54 :54:BC:E9:CA:42:17:41:6C:08:19:C0:74:6B:F0:31:22:D7:EE:64:93:BE:39:4A:28:F0:76:3A:9C:73:5D:89:F3:B4:86:29:1E:C1:F0:CD:E2:84:7A:3D:16:C5:94:C1:3A:70:0B:C4:56:9B:1D:74:B A:47:5E:8C:A1:04:2D:E8:B6:13:6C:74:3B:20:19:D4:D2:02:51:01:93:A9:FF:E6:91:29:AB:97:B3:32:3F:29:F7:3A:7B:C6:AE:4E:29:27:E4:B3:F7:BD:08:EB:5C:BE:8F:64:B1:42:A9:D7:11:B0: 59:FA:E0:FB:49:33:FF:E3:CD:E3:57:FF:BF:76:79:98:9F:20:FF:40:AB:51:60:CE:A4:C8:12:7E:D8:5C:59:88:99:BF:83:DE:3E:90:95:3D:E0:2A:84:2C:E5:C4:2C:6F:6D:26:73:48:1B:09:AF:20: D8:93:D8:1D:4D:A7:80:5A:06:3D:A1:77:3B:9C:94:41:3E:72:AE:41:4A:F5:6B:9B:FC:53:5B:40:81:13:3E:BC:E7:AA:75:FC:E1:9A:1B:22:FC:C7:68:4A:B9:6F:B2:0F:73:32:D2:10:AE:29:D3:8 B:39:BB:E9:D2:8F:BD:CF:D3:69:C5:F1:B3:E4:C1:BB:A5:37:73:93:41:DB:57:27:F5:4F:CA:36:C9:BB:CC:B8:E4:AF:43:F1:BF:54:25:CB:47:FE:B9:F7:B5:93:CC:E6:97:C4:00:A5:06:DD:EE:99 :9E:56:D0:C8:8A:41:08:3E:02:74:DD:D9:77:99:7B:0B:64:87:2B:D5:3F:34:42:57:EE:7E:EE:61:7B:2F:CA:4C:7C:6D:72:9B:64:6D:6B:85:99:D7:5B:A2:81:02:03:01:00:01 </pre>
Certificate Policies	<i>Policy OID: 0.4.0.194112.1.1</i> <i>Policy OID: 1.3.6.1.4.1.47281.1.5.2</i> <i>CPS pointer: https://www.esfirma.com/doc-pki/</i> <i>CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte https://www.esfirma.com/doc-pki/]</i>
Subject Key Identifier	<i>2D:A6:23:DD:87:8F:07:E7:D8:3D:32:1F:EE:69:E4:37:7F:55:F5:5D</i>
Authority Key Identifier	<i>F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58</i>
Basic Constraints	<i>IsCA: false</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	<i>http://crls1.esfirma.com/acaapp/acaapp2.crl</i> <i>http://crls2.esfirma.com/acaapp/acaapp2.crl</i>
Authority Info Access	<i>http://ocsp1.esfirma.com/acaapp2/</i> <i>http://ocsp2.esfirma.com/acaapp2/</i> <i>https://www.esfirma.com/doc-pki/acaapp2.crt</i>

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F7:D4:39:1C:50:C3:42:98:9B:94:63:F8:5F:DB:BB:71:18:AC:03:A5:64:4A:3A:68:A1:83:65:AB:A5:07:9E:52*

X509SubjectName

Subject CN: *ESFIRMA TSA 2*

Subject 2.5.4.97: *VATES-A50878842*

Subject SERIAL NUMBER: *A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject L: *ZARAGOZA*

Subject C: *ES*

X509SKI

X509 SK I *LaYj3YePB+fYPTIf7mnkN39V9V0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

28.4.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by ESFIRMA TSA 2*

Name *[es]* *Sellos de tiempo cualificados emitidos por ESFIRMA TSA 2*

Service digital identities

X509SubjectName

Subject CN: *ESFIRMA TSA 2*

Subject 2.5.4.97: *VATES-A50878842*

Subject SERIAL NUMBER: *A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject L: *ZARAGOZA*

Subject C: *ES*

X509SKI

X509 SK I *LaYj3YePB+fYPTIf7mnkN39V9V0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-06-25T00:00:00Z*

28.5 - Service (granted): Sellos de tiempo cualificados emitidos por ESFIRMA TSA - QTSU 2023

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por ESFIRMA TSA - QTSU 2023*

Name *[en]* *Qualified timestamps issued by ESFIRMA TSA - QTSU 2023*

Service digital identities

Certificate fields details

Version: *3*

Serial Number:

90804929519106285598314512538477159492

X509 Certificate

-----BEGIN CERTIFICATE-----

```
MIATCCBemgAwIBAQRFbkrmlw15DKTqhn4w5KRdANBqkqhkiG9w0BAQOFAADCBvDELMakGA1UE
BhMCRVmkETAPBgNVBACTCFpBUkFHTlBMTYwNAyDVQoKEY1FU18VOKxIO08gUOVSVkIOSU9TIFBB
UKETEEgQUINNSUjU1RSQUJNT040UEMxawBgNVBAsTKUUFVVE99SURBACBESBDRVJUSUZOOFD
SU90IEVTRkISTUEglSBBOvBQMRIwEAYDVQoFEWBNTA4Nzg4NDIxGjAYBgNVBAMTEUVRkISTUEg
QUIMgOUFOUCAyMB4XDTE2MDMxNjEwXjE0NDI4MDMxNDExNTQ0NjowYXc2AABGNvBAYTAkVT
MTYwNAyDVQoKEY1FU18VOKxIO08gUOVSVQ9TIFBBUKETEEgQUINNSUjU1RSQUJNT040UEMx
GDAwBgNVBGETD1ZBVEVTLUE1MDg3ODg0MjEgMB4GA1UEAxMxRVNNGSVJNOSBUU0EUSBRVFNVDIw
MjMwggijMA0GCSCgS1b3DOEBAQUAA4CDAWAggikAoiCAQCI++snpduLarHu/RzVlwyCzQLPoyEA
ZlhpY6F6b8H6sWgPolCVZGesVhCq4Hf0074zwauA8KHsOCBmicZwczqelrYVbVJZVSAME
rwf+hZdKYXe9xkn4nlijwNFiz3Jfqn93tegO290FUL1T1D1N+whKDI5xiq3tmfQYD1Apmgp0/3t
F8/ruxunjyCAxLrwfegUloAGe+LyunYkOWE7CXRA0ikY9hEudeWtDSoS/af3NuavHYa+laVOV3
ZESdKRN19GOS3MqQkVdorca+DnviOnUv158KisYiaELwIaxOmnnRMItdAx8j0YhU0uM215vV
DwV4pZAFH0ccb/LT60SQA8W37JKisWf8m8PF6YKaGyUlv3u7ndfpvN2TtW4mW7CS9Eujt7aNAH
bXp5NEFUSfjwY6zhZEDTjUOVEDM8NnlDyo8OJ1MiHibCVtmBgFAPZBy95pAPNXH1RIRppD
UhgE4Pwihf6ewHwJxS1ZVw8RwmtfjB7WALAPrd0kzO2SfAMbzYUSiku+4yDbea6vX06
u3b5MID8eopFHA0/+JangSvWzDshlidaqbqe4zRhRLA6OmnykOCxQoZeOfK8qeOzR6Kid8n0Lfb
ydeQeHtaRU6gK7vHz+v1bWNjs+aD9vDb8TgThAqb61HwIDAQABo4ICNjCAIwDAYDVROTAAQH/
BAIwADA8BgNVHSMEGDAIWs6T200DpyNs5b86fWw3i5Hy0WD0b08gBgF8CzBAORAMCYNWgYI
KwYBQUHMAKGKmh0dHA6Ly93d3cuZXNmaXJlYS5jb20vZG9jLXBra59hY2FhcHAyLmNydDA8Bggg
BgEFFQcWAYYgaHR0cDovL290c3AuzXNmaXJlYS5jb20vYWNhYXBwMi8wUWYDVROgBEwwSJA9Bgsr
BgEEAYILNQETAJuMwGCCGAQUFBWIBfB8wHicwZS50cmlhLmNv59BkZMcGp
LZAJBgcEAlvsQAE8MBYGA1UdQE8wQMMAGCCSGAQUFBwMIMFEGCCSGAQUFBwEDBEUwQzA8Bggg
BgEFFQcLajAJBgcEAlvsQECMAGBgGQAikYBATALBgYEA15GAOMCAQ8wEwYGBACORgEGMAGKGBwQA
jK1B8gimwYDVR0BGgwZJAoc+gLYYrahR0cDovL2NybmHMLmVzZmlybWUyZ9L2FjYWwFwcC9hY2FhcHAy
LmNydDA8BGNVH04EfgQUB+gUpnZx8Mgnf8OjEYRmyoYDilwKwYDVRO0BCQwloAPMjAyMzAzMTYx
MTU0NDUgOjB5MDI1MDMxNDExNTQ0NjowYXc2AABGNvBAYTAkVTMTYwNAyDVQoKEY1FU18VOKxIO08g
AOCACIEIDLxRBKG+5xLRssZRE5OT05cDbyrti+voouGfXpw6PKUjF+koGmfOIPE47ECX0z6c63C
im67mvrKhyAl66hs3ygPwUg+JcY4Xy1Hx+zhRfYfKbyuFTRMNRkVPmJiVaQORfHxyYWM4g0+
LcSLcdRYMgVcQeK1P25NtUfR6XUJSgOsTqjCPRPEe7KS3ygeHhPRAHwVn630680hW79Uv1
1qjABxxtPxHsAYnxLb66A5wmxojO420YBNTAmj151CKON7bdXoKClcae3QaOHa7115M4gKs9C
/diY1LoV7h5BSZgkApeP1oDyI7PwM52CCMMaI4XCqITt4Gt+uJ0GhVXM34azkEDQCaNo4ZI
Nfgwvd2OWV7WQ9AhYU2XtGRDD8G+Oj0JpveGf23gd+ZITL5BGSdXswfO7n0eaG8lbtbc
bPM113LOAHHD++Hj0B8eB0kij51wW++9pZ+CW87aocDMHHzVZGEBB4A/kz4nWFLAvj90IVQy7
Wnuro8tw06mubZtAC23kNIA8HemGuW09bXmgP+7dzox78TNuonba101PAOTVa8aqO465yXdtuCj
AGj9ukDnuq6afCfYj0uzif260czMb0EVBRYA+y5z3W2H6Gsr1TBTvhaLQTUuWrxaujAKXB1Jed
KQ==
```

-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer CN:

ESFIRMA AC AAPP 2

Issuer SERIAL NUMBER:

A50878842

Issuer OU:

AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

Issuer O:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Issuer L:

ZARAGOZA

Issuer C:

ES

Subject CN:

ESFIRMA TSA - QTSU 2023

Subject 2.5.4.97:

VATES-A50878842

Subject O:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Subject C:

ES

Valid from:

Thu Mar 16 12:54:47 CET 2023

Valid to:

Tue Mar 14 12:54:47 CET 2028

Public Key:

```
30:82:02:22:30:00:06:09:2A:86:48:86:F7:00:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:88:FB:EB:27:A5:D8:8B:6A:81:EE:FD:16:6F:97:0C:82:CD:02:CF:3B:21:00:D8
:B8:60:FB:7A:15:BF:07:EA:CS:A0:3E:8D:42:59:91:9E:B1:51:C2:72:0E:07:7D:DD:3B:03:3C:1A:BA:D0:3C:28:78:AC:38:26:CC:AD:C6:70:CD:CA:A4:7A:5A:F2:FD:56:D5:25:95:52:8C:03
:04:AF:01:7E:B5:97:4A:61:77:BD:C6:49:BB:9C:88:FF:C0:D1:4B:CF:72:5F:AA:7F:77:B6:C8:3F:3B:6F:68:15:4D:45:D5:37:75:37:EC:07:90:38:92:C6:2A:B7:B6:61:5D:60:3D:40:A6:68:29:0
F:FD:ED:17:CF:EB:8B:1B:4F:07:00:C4:82:EB:CF:77:86:52:5A:00:19:EF:8B:CA:E9:D8:9D:E5:84:EC:2C:51:03:49:71:63:D8:44:51:D7:96:B4:34:A8:4B:F8:94:17:73:6E:69:51:72:68:E2
:1A:54:E5:77:65:98:03:91:19:E5:F7:A3:89:DC:C4:2A:93:8B:DD:6E:B7:1A:FA:20:E1:BE:23:47:52:FD:52:F0:D2:89:B3:22:7F:68:42:F0:61:AC:6D:3A:69:D1:33:58:5F:03:10:63:D1:88:54:3
A:E3:19:D5:2B:D5:0F:05:78:E2:9C:0C:16:1D:1C:71:BF:C8:4F:AD:12:41:A1:FC:5B:7E:E3:28:8B:16:7F:C9:BC:3C:5E:98:2A:A1:B2:51:8B:F7:BB:89:D0:7E:98:CD:DA:04:F0:E2:65:BB:09:2
F:44:88:9B:7B:6B:DE:07:6D:73:F9:34:41:54:49:FE:E3:0C:9C:BA:CC:7C:C4:0C:94:E9:25:43:95:10:33:3C:36:72:DD:CA:8F:0E:27:53:22:FC:78:5B:09:5B:66:6E:01:7C:00:F6:41:CB:0E:4F
:6B:CF:57:1F:54:65:46:0A:43:52:11:84:BF:83:EF:C0:89:47:AF:A7:80:37:05:2C:5F:96:19:5B:C4:6F:C1:87:FF:27:CE:D6:00:80:0F:AD:DD:0E:8E:4C:EF:39:94:87:00:C6:F6:C9:44:88:91:4F
:8B:C8:30:5E:68:AF:D8:BD:79:7A:BB:76:F9:32:50:FC:7A:8A:45:1C:0D:3F:F8:9E:A7:82:C1:16:CC:3B:21:94:87:5A:A9:BA:9E:E3:34:61:AC:BD:3A:3A:69:89:90:E7:17:80:E6:5E:41:F9:3C:A
9:E3:83:47:A2:88:77:C9:F4:2D:F8:5B:C9:D6:D0:78:7B:5A:45:4E:AD:2B:8B:C8:87:3F:AF:D5:B5:8D:8D:2F:9A:0F:D8:C3:6C:1B:38:A9:38:40:41:BE:85:1F:02:03:01:00:01
```

Basic Constraints

IsCA: false

Authority Key Identifier

F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58

Authority Info Access

<http://www.esfirma.com/doc-pki/acaapp2.crt><http://ocsp.esfirma.com/acaapp2/>

Certificate Policies*Policy OID: 1.3.6.1.4.1.47281.1.5.2**CPS pointer: <https://www.esfirma.com/doc-pki/>**Policy OID: 0.4.0.194112.1.1***Extended Key Usage***id_kp_timeStamping***QCStatements - crit. = false***id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15***CRL Distribution Points***<http://crls1.esfirma.com/acaapp/acaapp2.crl>**<http://crls2.esfirma.com/acaapp/acaapp2.crl>***Subject Key Identifier***07:E7:54:A6:76:71:04:C8:27:7F:C3:BF:11:84:66:CA:88:F2:0C:82***Key Usage:***nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***A3:F6:62:B0:19:C7:5D:A7:82:3B:A5:BF:5F:EE:B2:AC:77:A9:C2:04:FD:7E:C6:4B:2B:F0:15:9C:57:89:36:A0***X509SubjectName****Subject CN:***ESFIRMA TSA - QTSU 2023***Subject 2.5.4.97:***VATES-A50878842***Subject O:***ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA***Subject C:***ES***X509SKI****X509 SK I***B+dUpnZxBMgnf8O/EYRmyojyDII=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2023-04-20T00:00:00Z***28.6 - Service (granted): Qualified timestamps issued by ESFIRMA TSA QTSU 2024****Service Type Identifier***<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>***Service type description** [en]*A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by ESFIRMA TSA QTSU 2024

Name [es] Sellos de tiempo cualificados emitidos por ESFIRMA TSA QTSU 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 68077614054255853789592111418370833794

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *ESFIRMA AC AAPP 2*

Issuer SERIAL NUMBER: *A50878842*

Issuer OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Issuer O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Issuer L: *ZARAGOZA*

Issuer C: *ES*

Subject CN: *ESFIRMA TSA - QTSU 2024*

Subject 2.5.4.97: *VATES-A50878842*

Subject 0: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject C: ES

Valid from: Thu Aug 29 11:07:09 CEST 2024

Valid to: Tue Aug 28 11:07:09 CEST 2029

Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:97:1A:A9:30:3D:01:1E:A7:40:9A:05:CB:30:29:1D:9A:6C:87:6C:23:65:5F:2A:7F:6E:5F:21:80:1F:1C:F5:8B:24:88:39:D1:8F:F5:80:8A:75:24:C0:8B:9A:AE:22:08:46:DE:EF:9C:5C:5A:4A:00:6F:A2:9B:7D:DC:BC:70:51:06:52:88:9F:15:59:40:8A:1E:3E:F9:93:E3:DF:26:F7:2C:16:0A:4E:98:3E:85:DE:9E:51:CD:DD:BD:FC:83:CF:97:61:59:0D:63:68:7E:39:07:43:58:EB:D0:13:19:FA:DD:23:4F:CA:F8:B1:C2:A2:FD:E0:8F:B7:DE:66:1A:50:9E:8E:3E:FC:AD:1C:91:50:9D:C8:59:9E:2F:4D:16:A6:22:4B:7D:22:AC:D8:8B:D8:41:23:DE:FD:24:EB:8A:86:7A:80:A3:5A:E0:EB:61:2C:87:99:BB:66:D5:C1:C1:C0:49:A6:03:59:B2:37:46:80:35:23:F3:8F:71:1D:DD:54:E7:AB:06:5B:01:26:A8:83:50:93:18:C8:41:01:AD:4C:AB:31:C9:DE:C2:FE:60:4B:87:47:4B:FD:46:65:C6:33:9A:AA:83:11:21:DE:53:C4:48:DC:58:1F:79:F8:5E:05:D8:A3:F5:A8:8B:96:08:6A:71:C4:38:C1:D1:B3:F2:91:F8:98:04:0B:A4:63:88:85:01:A7:9A:71:5A:75:70:AD:38:89:E3:CC:1D:90:A7:0E:4D:92:89:30:8B:FD:19:CB:25:53:12:D2:AA:79:0E:02:F1:CB:E7:00:70:5D:9E:2F:37:85:2D:3B:67:D0:A9:46:26:D8:85:B1:14:C3:27:4F:9C:9A:B9:76:83:EC:EB:71:AE:86:8F:DD:7F:F7:1E:4F:A3:15:56:65:D6:0E:52:DC:8B:3F:26:1E:DB:44:49:0B:78:E7:89:16:99:80:6C:88:D5:32:12:6E:9B:6F:DC:36:84:8E:17:A5:1F:DE:1A:D3:14:6E:91:6D:DD:FD:67:C7:50:88:16:4B:56:A5:28:7F:6E:28:F1:85:DA:FB:42:8B:9E:B1:68:61:17:98:28:A7:AB:19:DF:4A:57:13:A9:62:D8:C4:5B:B2:A3:55:40:FE:9A:CF:84:9C:CD:E2:C7:55:31:2F:1D:28:63:B5:5A:49:5A:89:AE:13:02:66:C1:F5:AB:1B:1C:D4:9D:8A:73:E8:A5:EA:0B:C6:1F:60:A3:49:0E:9:79:94:40:40:35:79:C3:0A:27:25:6D:3B:E7:36:8E:88:E2:2D:EC:99:2D:84:83:1A:53:20:5D:5C:CE:E7:58:BB:37:3C:C6:61:65:AE:DB:A5:85:F8:8D:7A:57:02:03:01:00:01

Basic Constraints IsCA: false

Authority Key Identifier F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58

Authority Info Access
http://www.esfirma.com/doc-pki/acaapp2.crt
http://ocsp.esfirma.com/acaapp2/

Certificate Policies
Policy OID: 1.3.6.1.4.1.47281.1.5.2
CPS pointer: https://www.esfirma.com/doc-pki/
Policy OID: 0.4.0.194112.1.1

Extended Key Usage id_kp_timeStamping

QCStatements - crit. = false id_etsi_qcs_QcCompliance
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points
http://crls1.esfirma.com/acaapp/acaapp2.crl
http://crls2.esfirma.com/acaapp/acaapp2.crl

Subject Key Identifier F7:30:96:F4:40:7A:9A:B3:77:A8:E8:7E:6B:61:A5:C3:00:DA:C3:08

Key Usage: nonRepudiation

Thumbprint algorithm: SHA-256

Thumbprint: 01:D4:9B:10:16:12:25:B4:F6:70:2C:FD:44:EA:01:B0:B2:87:37:1C:84:77:C1:FF:C
D:FD:7E:71:91:80:7A:8A

X509SubjectName

Subject CN: ESFIRMA TSA - QTSU 2024

Subject 2.5.4.97: VATES-A50878842

Subject O: ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Subject C: ES

X509SKI

X509 SK I 9zCW9EB6mrN3qOh+a2GllwwDawwg=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.

28.7 - Service (granted): Qualified electronic time stamp issued by ESFIRMA TSA - QTSU
2025

Service type description	<i>[en] A time-stamping generation service creating and signing qualified time-stamps tokens.</i> <i>[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name [es] *Sellos cualificados de tiempo electrónico emitidos por ESFIRMA TSA - QTSU 2025*

Issuer C: *ES*

Subject CN: *ESFIRMA TSA - QTSU 2025*

Subject 2.5.4.97: *VATES-A50878842*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject C: *ES*

Valid from: *Wed Dec 17 11:59:44 CET 2025*

Valid to: *Sat Nov 02 14:12:47 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AA:28:80:C1:F9:26:ED:28:10:87:CE:81:FB:70:B2:5A:BD:A4:C2:F7:6F:D1:0A:
D8:8D:F1:4A:3F:D5:12:CE:06:57:20:40:96:FD:33:11:D3:03:F8:EF:F2:46:63:85:85:E1:36:1A:A6:61:89:78:BE:C8:C2:C8:BD:19:3E:98:0E:12:4E:8A:FD:B8:EB:82:D8:77:E2:18:A8:86:6A:B
D:78:C6:DA:18:F5:74:6D:7D:E3:38:39:59:1C:8F:F5:E0:1A:52:13:97:62:69:33:19:74:F5:D2:F1:88:BF:A1:CA:93:1C:55:81:E3:CE:3E:5C:9D:24:8A:D9:04:69:8A:25:32:DD:AC:89:4A:EF:16:
12:1B:44:73:80:25:ED:11:2C:68:90:9F:36:C7:0F:46:FF:7C:DE:17:91:76:F3:45:83:D7:5B:61:45:90:46:B6:50:77:DE:8C:EB:DA:B8:BB:EA:0D:2B:A3:47:E9:43:5E:D0:36:F6:8A:49:A4:7B:1
0:9E:95:51:81:1C:13:A5:73:82:C1:01:19:82:5B:6F:92:27:01:42:DD:5E:22:81:F7:5A:08:57:E2:35:88:D7:46:25:D4:A0:AE:7D:B9:FC:E8:14:78:3E:10:0A:1A:AA:27:DD:B7:80:EB:C9:B3:B5
:06:5A:BE:B4:AC:B8:CF:7A:81:28:12:A2:69:1D:48:F8:35:7A:72:2E:80:A3:7F:4D:8F:BF:18:BF:08:66:09:5C:78:02:8C:AE:D3:3A:FB:CD:D9:CD:47:11:8F:9D:B7:3A:A2:F0:1F:E5:CE:1D:F9:7
2:32:C2:DE:AE:D1:83:2A:9A:92:A6:E3:C5:1F:F7:EE:82:2E:80:74:80:51:90:D6:DE:63:9C:E5:49:7B:11:58:CA:E8:D6:18:4F:6E:9C:38:A6:20:60:FA:4F:27:6E:EF:31:CD:99:C6:00:8E:EF:5C:
FA:AB:D2:84:A1:1E:E1:2A:02:16:97:C7:F0:D3:C1:08:03:79:01:AA:C8:E6:CA:0D:C9:D7:60:7A:17:CD:EB:69:C8:9C:3E:89:A5:FC:E9:AA:3E:0E:80:05:61:CB:C1:2B:01:51:96:C3:23:31:A8:5
E:95:4C:7A:FC:C4:B0:6B:09:1A:49:84:F5:6E:8A:75:6B:12:E9:94:E0:26:03:9C:E3:E0:8D:42:60:69:09:41:C1:71:FD:4A:35:D7:F0:ED:73:59:24:D9:25:D8:D6:2F:C8:44:13:E7:17:A1:FE:80:
9B:86:25:D8:3E:5D:89:A8:6A:24:63:3C:B9:C4:7E:8C:D8:6D:1B:14:B0:08:14:70:E2:78:22:1B:3B:A1:BF:A7:5A:D5:B2:73:D7:5C:BD:3B:6A:51:6C:A5:AB:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58*

Authority Info Access

http://www.esfirma.com/doc-pki/acaapp2.crt

http://ocsp.esfirma.com/acaapp2/

Certificate Policies

Policy OID: 1.3.6.1.4.1.47281.1.5.2

CPS pointer: https://www.esfirma.com/doc-pki/

Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

http://crls1.esfirma.com/acaapp/acaapp2.crl

http://crls2.esfirma.com/acaapp/acaapp2.crl

Subject Key Identifier *F5:44:9B:F6:1E:7F:D2:13:0D:2B:22:94:E8:B4:9C:95:D8:02:4A:04*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint:

6F:16:19:3F:7B:33:25:EC:42:9C:2F:60:A9:73:17:10:7E:2D:0C:86:5D:EB:FC:05:DC
:85:F3:96:C2:E7:86:C5

X509SubjectName

Subject CN: *ESFIRMA TSA - QTSU 2025*

Subject 2.5.4.97: *VATES-A50878842*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject C: *ES*

X509SKI

X509 SK I *9USb9h5/0hMNKyKU6LSclDgCSgQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

Status Starting Time *2026-02-26T03:00:00Z*

29 - TSP: SIGNATURIT SOLUTIONS, S.L.U.

TSP Name

Name [en] *SIGNATURIT SOLUTIONS, S.L.U.*

Name [es] *SIGNATURIT SOLUTIONS, S.L.U.*

TSP Trade Name

Name [en] *Signaturit Solutions S.L.*

Name [en] *VATES-B66024167*

Name [en] *SIGNATURIT SOLUTIONS, SL*

Name [en] *SIGNATURIT SOLUTIONS, S.L.U.*

PostalAddress

Street Address [en] *Avila Street 29*

Locality [en] *Barcelona*

State Or Province [en] *Barcelona*

Postal Code [en] *08005*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Calle Ávila 29*

Locality [es] *Barcelona*

State Or Province [es] *Barcelona*

Postal Code [es] *08005*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:legal@signaturit.com*

URI [es] *mailto:legal@signaturit.com*

URI [en] *https://www.signaturit.com/en*

URI	[en]	https://www.signaturit.com/en/pki

URI	[es]	https://www.signaturit.com/es/pki

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name [es] *Sellos de tiempo cualificados emitidos por Signaturit TSA*

Name	[en]	Qualified timestamps issued by Signaturit TSA

Version: 3

Serial Number: 2519984208954736786909103762859173925957402916

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Signaturit Issuing CA*

Issuer DC: *signaturit*

Issuer DC: *com*

Issuer C: *ES*

Issuer O: *Signaturit Solutions S.L.*
Issuer 2.5.4.97: *VATES-B66024167*
Subject CN: *Signaturit TSA*
Subject C: *ES*
Subject L: *Barcelona*
Subject O: *Signaturit Solutions S.L.*
Subject 2.5.4.97: *VATES-B66024167*
Valid from: *Tue Jul 03 11:21:11 CEST 2018*
Valid to: *Sun Jul 02 11:21:11 CEST 2023*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F0:77:8D:50:CF:9A:2F:F4:AD:7F:11:85:12:13:85:4E:4A:62:65:E0:5C:C0:7C:8F:E6:80:C8:3C:79:5A:6B:06:15:06:F8:3F:AB:64:E8:58:10:8C:ED:F7:6A:61:FF:FA:ED:F7:BA:DA:36:07:35:4B:98:59:AF:7C:52:16:C7:52:8B:C0:1F:F7:52:07:38:3C:85:9C:AA:83:0D:D6:E4:58:2D:2D:D3:2D:5C:12:A9:8C:25:02:1B:58:AF:36:C3:8B:13:72:0C:5C:89:64:B1:A5:DF:95:89:4B:42:42:12:02:11:E0:AB:75:21:ED:3D:48:93:13:85:A4:D2:D3:02:C5:D9:76:9E:B4:4C:35:64:DB:F5:9F:6D:3B:F3:4F:A9:BD:91:9A:3C:74:6B:89:DC:93:D9:06:86:DF:E6:E2:D6:3C:32:2F:7D:AD:F5:AF:72:F2:D3:0F:55:53:91:46:D6:7A:70:FD:A6:D4:5B:1A:01:27:D0:8C:FD:B7:E2:55:73:95:E9:DA:60:E6:34:A5:11:02:73:5F:A1:11:70:0D:9F:14:50:AF:9D:A7:23:2A:3C:39:95:46:DF:74:E1:9D:71:74:24:4A:6F:5E:D3:55:B0:8C:78:F9:1E:ED:A1:D8:10:FF:74:BD:12:6A:08:17:DA:1A:F8:02:F0:12:5D:06:31:C3:02:03:01:00:01*
Subject Key Identifier *48:A3:10:E6:69:DA:C3:EC:47:A1:BB:6C:34:F5:15:24:48:20:4E:DF*
Authority Key Identifier *8A:AD:21:CB:B2:26:6C:30:CC:D2:D3:24:78:87:21:2E:5E:BA:01:29*
CRL Distribution Points *http://pki.signaturit.com/crl/Signaturit%20Issuing%20CA.crl*
Authority Info Access *http://pki.signaturit.com/cert/CA02.signaturit.com_Signaturit%20Issuing%20CA.crt*
http://pki.signaturit.com/ocsp
Extended Key Usage *id_kp_timeStamping*
Certificate Policies *Policy OID: 1.3.6.1.4.1.50646.3.1*
CPS pointer: http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf
Key Usage: *digitalSignature - nonRepudiation*
Thumbprint algorithm: *SHA-256*
Thumbprint: *49:77:F6:AA:EA:C4:E2:A0:45:E8:37:10:1D:CE:BA:10:A3:FE:5E:57:F7:41:55:87:FD:04:30:0F:B2:19:87:86*

X509SubjectName

Subject CN: *Signaturit TSA*
Subject C: *ES*
Subject L: *Barcelona*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *SKMQ5mnaw+xHobtsNPUVJEggTt8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2024-01-24T02:00:00Z*

29.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[es] Sellos de tiempo cualificados emitidos por Signaturit TSA*

Name *[en] Qualified timestamps issued by Signaturit TSA*

Service digital identities

X509SubjectName

Subject CN: *Signaturit TSA*

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *SKMQ5mnaw+xHobtsNPUVJEggTt8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-11-22T01:00:00Z*

29.2 - Service (withdrawn): Qualified certificates issued by Signaturit Qualified Issuing CA

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en]

Qualified certificates issued by Signaturit Qualified Issuing CA

Name [es]

Certificados cualificados emitidos por Signaturit Qualified Issuing CA

Service digital identities

Certificate fields details

Version:

3

Serial Number:

2631487933452175089094375804079080061651648516

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDCCBgigAwIQAgtDgAAATsDm5dwZmVAAAAAABDANBqkqhkig9w0BAQwFADBoMRgwfGyD
VORHew9WVRfUy1CNjYwMjQxNjcxJAgBgNVBAoTGVNpZ25hdHVaXG9U29sdXRpb25zIFMuTC4x
CzAjBgNVBAYTAKVTRswGQYDQ0ODETaWduYXR1cm0lTjVh3QgO0EwhhcAMTkwMjA4MTQyOTAz
WhcNMjkwMjA4MTQyOTAzWjCBdIEYMBYGA1UEYRMPVkfURVMTQyZMDIOMTY3MSIwIAYDVQKExIT
aWduYXR1cm0lTjVh3QgO0EwhhcAMTkwMjA4MTQyOTAzWjCBdIEYMBYGA1UEYRMPVkfURVMTQyZMDIOMTY3MSIwIA
bTBAEAgGCGnSjcm0lTjVh3QgO0EwhhcAMTkwMjA4MTQyOTAzWjCBdIEYMBYGA1UEYRMPVkfURVMTQyZMDIOMTY3MSIwIA
aWVKElE3V3p0bmcqQ0EwagIiMA0GCsGqSib3DDEBAQUAA4ICDwAwgglKAQCAQDMfyH0YbUEDzbZ
LOO0to5XimNbdK6w3rYx8Mso3T7iwp8+178RkK/GUpPC6cviVilvY46b1mT+29HvH2fjdt7TLb
c3VeXoaUkxjelepbu3BKLJLLPv6IS4WexXv44Wp4WtmRhaenn7i/n+eQMfHm4wObM7LqTnm
TZrTHiBxowWX3QwFuiMn1L4qWO7roW4wpanKGr7ny0Rx9e8adWwKR3D4IzpldCJW4UA1wOgXm
35qWRK6wPhdrpeHobz5HudVWixmRN1gyVg8LEBT0QKjCvWoaZebmWLGadPhDgh/zx6uh4Sprl
mgd5yZmP0prchdIQ3itL1D9yZuhtuerCS9+1yIzgrT13ntrhwKpPMpsGir3is09W7JUSHR
5YkvaGGURG5y1Kkrh5jvkvcl+JGntWP7TC3ciW4JedDmZGIZoiS2w3pODNORPZCHxAg6Tyv/n4
tdsdl3a3fM0VtO4xx3327loy83oaYNuVerDyqhtuif+E0zouMaggm0p0+pMlpfZRI4T52w5i
JyIE1LouTLuncyWALBwyQYX85bU990jBzU9gIReNpvrUwAp0D0GpXp4OoyKa0+pph6gbX9
wcGhpV3g8Y2aACyBqVvktZheOsko7HBS469RDNxhLyuy5pMZhs535WHGexSd9wiDAQAB64CgICC
An4wdgYDVR0PAQH/BAQDAgGMBAGCsGAQOBgicVAQDDAgEBMCMGCSGSAQOBgicVAgQWBBRebN/
MlWptdm354q4Wz7L4no2MDAdbgNVHQEFgQUCBUXKMyakIDN596sBtkCKSCW99ggg9bVHSAE
ggEXMIBEzB0BgorBgEEAYOLVgIBEIwQAYIKwYBBQUHAgEWWGh0dHA6Ly9wa2ku2Inbmf0dXlp
dC5jb2VvcGtpL0NQL5hdHvYVWwUGVyc29ucy5w2GyWv9YkKwYBBAGDI1YDATBIMEYGCsGAQUP
BwIBtpidRwOibvGpLnPZ25hdHVaXG9U29L3Bras9DUC5Z4WdhbCS5X2ByZXNlbnRhdG92
ZXMuGCRmMFEgcSgAQOBg4tWBAEwQzBBggrBgEFBQcCARY1aHR0cDovL3Bra55zaWduYXR1cm0
LmNvb59wa2kvQ1AurWxly3Ryb25pYy5tZWZscysw2GyWv9YkKwYBBACL7EABAJAIBgcEAlvsQAEEDMBK
CSGSAQOBgicUAgQMhgoUw81AGIAQwBBMA8G1UdeWE8wQFMA8BAfBwIwYDVR0JB8BwFoAU33xS
40bKTDCKGeNBdjd08LH0wsQYDVR0RBEIwQDA+oDygoY4aHR0cDovL3Bra55zaWduYXR1cm0
LmNvb59cmwvU2Inbmf0dXlpdC5jb2VvcGtpL0NQL5hdHvYVWwUGVyc29ucy5w2GyWv9YkKwYBBQUHAgEETBMMEOGCCSG
AQUPBzACn5odRwOibvGpLnPZ25hdHVaXG9U29L2WicnQvO0EwMw9TAWduYXR1cm0lTjVh
Um9vduClyMENBMLNydDANBqkqhkig9w0BAQwFAAOACAgEAHv6q2K9i9094vxa5S2Pv67pA5GpgKXHR
BLm25gU1kwtqfP9ZgjxTcG+r9oGajak2+eDR5wak1GF7B4ERxGFxPe9k68UODgOZe0nfq8yY01
zC7KdFTox2qLMS5B1CzYQWz5W4aZKBA5VadaNocVY04eTgYimS8Nw9wibC24Vg9urhc08/H
Jaj6MUEKT4S0mjFLNclci62j5m3etupt1ZXcsp4r9y945ivar29Iv8rcxD0UKVrYKJEW3WT
Uib33cipQULHY3QCD42xyQ+hW8L3CmId3pXsHgXWcYm5PGHnleBt19k4W3W09japUKYvNVFq
KB9mrk2uoIUwbsnID7Y9dgMVAZser24ZtLyIjeH1CG9lvW8691ZvkiYKvIBSElnqOK3
dB2gXezWF5MSDg5RYGolt0Db+idmOYG4GxOfn+IsLG6Ph928Q2ra7VY5JfRDKiOGPSFdmf
uhn6rhyrvx+/V+sa4m4GUaebh0eU08mkhLbQgzyYwelrokUwwB8j@wio85N5Xfz8Veg5jToB
vnt0G5v0R9W2xTmMwBfSPJjeQvIwRinRWDSW83u8t0Qhjbz73opy53mZnDzWpExhkJ
zyceQ0YGPW7d4B+QPe7pHGDSYk4REkYD3nMo2xsd8Y=

```

-----END CERTIFICATE-----

Signature algorithm:

SHA384withRSA

Issuer CN:

Signaturit Root CA

Issuer C:

ES

Issuer O:

Signaturit Solutions S.L.

Issuer 2.5.4.97:

VATES-B66024167

Subject CN:

Signaturit Qualified Issuing CA

Subject DC:

signaturit

Subject DC:

com

Subject C: *ES*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

Valid from: *Fri Feb 08 15:29:03 CET 2019*

Valid to: *Thu Feb 08 15:39:03 CET 2029*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E6:7F:21:F4:61:B5:04:0F:36:D9:2C:E3:8E:B6:8E:57:8A:63:5B:74:AE:80:DE:2B:5B:C7:C3:2C:A3:74:F8:88:0A:7C:FA:2E:FC:85:12:BF:19:48:0F:0B:A7:2F:89:58:88:8D:8E:1C:6F:59:93:F8:3F:68:1E:F1:F3:17:F7:53:ED:32:DB:73:75:5E:5C:E6:94:93:18:E5:7A:59:E9:6E:ED:C1:94:A2:E3:94:B2:CF:BF:A9:52:E1:67:B1:5E:F5:F8:5A:9E:22:5A:D9:91:1D:A7:A7:98:BF:EB:37:E9:1E:40:C1:DF:31:DC:0E:6C:CE:CB:A9:39:E6:4D:9A:D3:1E:20:6D:C6:85:96:5F:74:30:16:E8:8C:9F:52:F8:96:05:8E:EE:BA:16:E3:0A:5A:9E:41:AB:EE:7C:B4:47:1F:5E:F1:A7:56:C0:A4:77:0F:88:A2:66:99:5D:0A:55:8B:50:0D:70:3A:A5:E6:DF:9A:96:46:4E:B0:3E:17:68:A5:E1:E8:6F:34:87:89:D5:56:23:19:91:37:52:20:C9:51:BC:20:B1:01:4F:44:2D:2A:37:15:5A:86:99:11:89:96:2C:66:9D:3E:70:E0:87:FC:F1:EA:E8:78:4A:9A:E5:9A:08:10:E7:26:66:3C:EA:6B:72:18:49:25:0D:C8:AE:DD:43:C5:3F:71:66:F8:53:89:EA:C2:F4:9F:85:C8:86:60:3D:3D:77:9E:B6:E1:C0:F9:0F:34:F9:AC:1A:3A:C1:DE:2E:4E:F5:6E:E3:51:21:D1:E5:59:2F:68:61:94:AC:6E:72:D4:A9:2B:87:92:6A:8E:47:08:FA:31:A7:86:D5:8F:FE:5E:C2:8F:77:22:5B:88:C4:74:39:99:1A:56:68:89:26:70:DE:93:83:34:E3:D9:08:7C:40:E9:36:2F:A7:F9:F8:B5:DB:1D:D6:CD:DA:DC:53:0E:58:D3:9F:E3:1C:77:0D:9E:E5:A3:29:BC:DE:86:98:36:E5:5E:AC:3C:AA:1E:D8:EE:21:FF:84:3B:3A:2E:31:A8:26:D2:93:BE:A4:C9:65:A4:56:51:23:84:F9:0B:0E:62:27:29:6D:13:5A:2E:17:F2:EF:9C:2C:96:00:BF:16:C9:02:18:5F:CE:5B:51:8F:4E:27:F6:F6:53:D8:25:21:17:8D:A6:F4:6E:C0:0A:50:8B:41:A0:89:7A:B8:42:8C:8A:69:0F:A9:A6:1B:FA:81:B5:FD:C1:C1:A1:A5:5D:E0:F1:8D:80:68:26:01:81:5B:E4:7D:98:5E:3A:C9:28:EC:70:79:E3:AF:62:44:39:D7:84:BC:AE:CB:9A:4C:66:14:87:E5:68:46:7B:14:9D:F7:02:03:01:00:01

Subject Key Identifier *73:C5:0A:5C:CC:9A:93:F0:CD:C5:2F:7A:B0:16:CA:40:AB:02:5B:D8*

Certificate Policies
Policy OID: 1.3.6.1.4.1.50646.2.1
CPS pointer: <http://pki.signaturit.com/pki/CP.Natural.Persons.pdf>
Policy OID: 1.3.6.1.4.1.50646.3.1
CPS pointer: <http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf>
Policy OID: 1.3.6.1.4.1.50646.4.1
CPS pointer: <http://pki.signaturit.com/pki/CP.Electronic.Seals.pdf>
Policy OID: 0.4.0.194112.1.2
Policy OID: 0.4.0.194112.1.3

Basic Constraints *IsCA: true*

Authority Key Identifier *DF:7C:52:E1:06:CA:6D:30:C2:7C:67:8D:0C:18:9D:0C:EF:0B:7C:7D*

CRL Distribution Points *<http://pki.signaturit.com/crl/Signaturit%20Root%20CA.crl>*

Authority Info Access *http://pki.signaturit.com/cert/CA01_Signaturit%20Root%20CA.crt*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C9:DD:26:58:A3:05:CA:25:75:1E:35:90:D5:5D:61:9A:22:AE:67:D9:98:F1:E7:E9:8A:BE:91:F6:3A:9B:2A:90*

X509SubjectName

Subject CN: *Signaturit Qualified Issuing CA*

Subject DC: *signaturit*

Subject DC: *com*

Subject C: *ES*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *c8UKXMyak/DNxS96sBbKQKsCW9g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2024-01-24T02:00:00Z*

29.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

29.2.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.50646.2.1*

Description

29.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by Signaturit Qualified Issuing CA*

Name [es] *Certificados cualificados emitidos por Signaturit Qualified Issuing CA*

Service digital identities

X509SubjectName

Subject CN: *Signaturit Qualified Issuing CA*

Subject DC: *signaturit*

Subject DC: *com*

Subject C: *ES*

Subject O: *Signaturit Solutions S.L.*

Subject 2.5.4.97: *VATES-B66024167*

X509SKI

X509 SK I *c8UKXMyak/DNxS96sBbKQKsCW9g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-10-01T01:00:00Z*

29.2.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

29.2.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	<i>undefined.</i>
	[es]	<i>undefined.</i>

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier	[OIDA sURN]	<i>urn:oid:1.3.6.1.4.1.50646.2.1</i>

Description

29.3 - Service (withdrawn): Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description	[en]	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	[es]	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>

Subject C: *ES*

Subject O: *SIGNATURIT SOLUTIONS, SL*

Subject OU: *LEGAL*

Subject 2.5.4.97: *VATES-B66024167*

Subject CN: *SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

Valid from: *Fri Jan 24 09:18:42 CET 2020*

Valid to: *Mon Jan 23 09:18:42 CET 2023*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E2:6D:10:D2:9F:6E:BD:38:FB:95:DD:F8:C8:0E:01:E5:0B:C2:40:FF:A2:9C:D2:FB:33:DC:8E:1E:1B:FE:90:28:9E:EA:39:0A:46:0B:DA:E0:03:E7:33:36:9E:2A:B2:B7:DA:43:B7:A2:AA:26:00:1D:57:56:EB:09:85:88:79:F6:19:D9:8E:6C:23:E2:EE:88:12:29:89:AE:AA:3E:BE:8A:EC:7A:62:6B:35:7D:2B:14:0D:EB:7C:7E:CE:75:14:37:E9:3D:E6:35:C8:BC:3D:D6:80:27:09:4D:7B:45:2B:8C:09:DE:E7:53:EB:8E:49:9D:49:E3:E1:5F:DD:4B:51:15:A1:31:C5:03:6C:99:4A:64:97:D8:5E:1C:EF:9E:04:44:8B:5E:A0:B3:2E:42:6B:33:FE:18:86:39:87:9C:09:88:4A:80:1D:BB:B7:D2:5A:37:FE:06:AA:8A:13:63:41:67:56:AC:79:24:7A:F4:75:EB:DA:AB:3C:68:0B:8B:4C:A3:AB:6D:E0:11:A1:F8:EC:7A:B4:F6:1A:09:42:7A:A2:EF:D7:44:77:B8:6F:DE:0D:93:6C:BD:A9:98:18:D3:FD:11:CA:76:10:A2:08:B8:97:A8:43:56:88:CB:A6:CC:07:4E:6A:12:A0:1D:25:03:0E:E4:E2:1E:14:2D:EC:F4:DC:8F:02:03:01:00:01*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_clientAuth*

Subject Key Identifier *B1:0E:7D:B4:B9:8E:7B:DF:00:7E:1F:D7:7C:B4:C9:12:87:A6:27:0D*

Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt*
http://ocsp.camerfirma.com

Authority Key Identifier *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl*
http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl

Subject Alternative Name *legal@signaturit.com*
OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO

Issuer Alternative Name *ca@camerfirma.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2*
CPS pointer: https://policy.camerfirma.com
CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E1:89:8C:7B:47:8C:21:F3:CB:45:48:D7:A6:CA:F5:AC:F2:C9:DE:B5:6D:9D:70:65:BA:B2:E1:4D:1E:3D:BD:14*

X509SubjectName

Subject C: *ES*

Subject O: *SIGNATURIT SOLUTIONS, SL*

Subject OU: *LEGAL*

Subject 2.5.4.97: *VATES-B66024167*

Subject CN: *SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

X509SKI

X509 SK I *sQ59tLmOe98AfH/XfLTJEoemJw0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-07-01T01:00:00Z*

29.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[en]* *Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*

Name *[es]* *Servicio cualificado de entrega electrónica certificada "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *SIGNATURIT SOLUTIONS, SL*

Subject OU: *LEGAL*

Subject 2.5.4.97: *VATES-B66024167*

Subject CN: *SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

Page 1068

Issuer OU: *TRUST SERVICES*
Issuer ST: *VALENCIA*
Issuer C: *ES*
Subject CN: *Signaturit Global CA*
Subject O: *Signaturit Solutions S.L.U.*
Subject 2.5.4.97: *VATES-B66024167*
Subject ST: *BARCELONA*
Subject C: *ES*
Valid from: *Thu Mar 02 10:51:30 CET 2023*
Valid to: *Fri Mar 02 10:51:30 CET 2035*
Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CC:97:29:EA:0F:D8:A9:6B:10:27:30:32:C4:14:B8:A1:AB:33:92:D7:E2:2A:76:
20:C3:53:B2:87:62:8B:5F:4D:EF:D0:DC:1A:5E:59:62:38:B1:EA:F3:95:E1:E4:44:9A:2A:A7:E4:F9:D7:53:89:96:28:D8:56:88:11:CC:7D:2E:50:54:50:ED:EB:65:A7:49:BC:75:93:75:0C:6F:D
E:4D:C9:D9:1E:25:87:D5:BE:07:23:49:0B:E8:80:B4:6B:E3:C3:05:CC:6E:7E:CD:6E:48:EF:AD:BB:1B:47:F0:59:1D:E6:1A:A1:49:AA:34:2D:03:9B:33:42:54:72:A4:6F:C2:08:27:1C:01:04:59
:0A:90:4F:42:C9:33:0F:2B:EB:20:03:79:0E:33:63:62:4C:58:2F:FC:59:16:33:21:25:67:4B:6D:38:80:39:99:25:83:E7:AA:25:3E:D5:7B:E4:53:FB:41:AC:5B:D9:97:95:2F:CC:84:29:1B:04:6F
:9E:D8:93:43:06:79:A2:EF:5C:67:EC:1B:C0:E2:4E:21:D8:17:9D:CE:C5:1A:25:98:63:99:39:EE:DE:5E:40:D3:DF:02:74:F8:45:21:EE:83:FA:07:8A:F5:D6:8F:31:70:87:F3:C1:A3:9A:7D:69:B
A:86:E5:C6:D1:97:14:7F:C5:33:9E:61:9B:FF:6E:F5:C8:C0:31:43:46:13:97:E4:28:8C:F7:03:A5:BB:0D:B6:38:24:C5:6A:34:9E:32:2F:09:8A:A5:AC:F5:CB:D0:CB:2C:1E:A3:F7:49:8F:80:91:
3B:BA:51:02:80:DC:00:98:44:80:54:7D:5E:B4:16:75:2B:A5:90:20:19:1A:8A:6E:68:A1:D0:BF:94:DC:00:9F:23:14:C5:6F:4F:07:76:F9:D5:80:E9:80:61:63:94:ED:DE:65:96:08:EB:23:5D:2
3:97:33:9E:1A:87:CF:BD:41:3A:BE:82:97:9C:40:D1:39:7B:6E:76:49:35:81:7A:55:24:01:62:68:6F:DA:64:74:0B:25:D4:BF:92:75:BF:3C:59:54:8D:FC:AB:22:F5:39:21:36:49:10:F7:49:74:
AC:A4:B3:F1:16:E8:5F:EF:87:7C:9D:22:5F:AA:AA:B2:2A:5C:CE:B0:6F:34:C4:EC:97:1B:D4:E9:B0:A2:02:3A:53:94:3C:D1:2B:8A:37:C7:44:38:97:37:CF:52:18:8A:9A:9B:2F:1E:1C:48:36:8
6:11:E1:E3:A5:AB:65:48:CE:EC:62:6A:14:59:21:DE:BA:04:42:F4:1A:20:6E:CB:0E:06:78:43:C7:03:3D:42:50:8B:C1:BB:F4:DC:67:1A:B2:A2:2A:78:77:02:03:01:00:01
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *12:30:E9:1B:12:E6:3F:40:D3:E3:EE:9C:E1:EF:FF:64:EC:AF:25:97*
Authority Key Identifier *38:D0:55:F8:59:2B:12:53:08:44:48:8A:2F:70:03:49:71:80:13:1E*
Authority Info Access
http://ca.ivsign.com/certs/ivsignrootca.crt
http://ocsp.ivsign.com
http://ocsp2.ivsign.com
Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: https://policy.signaturit.com
CPS text: [Signaturit Global CA. Certification Practice Statements and Certificate Policies: https://policy.signaturit.com]
CRL Distribution Points
http://crl1.ivsign.com/ivsignroot.crl
http://crl2.ivsign.com/ivsignroot.crl
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *3B:E0:56:DA:32:62:3D:5E:00:6C:90:00:6A:84:66:15:EF:C4:A7:57:3F:F3:39:60:7F
:A0:14:4B:F9:20:FA:F4*

X509SubjectName

Subject CN: *Signaturit Global CA*

Subject O: *Signaturit Solutions S.L.U.*

Subject 2.5.4.97: *VATES-B66024167*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *EjDpGxLmP0DT4+6c4e//ZOyvJZc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2025-08-06T00:00:00Z*

29.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

29.4.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified certificates issued by Signaturit Global CA*

Name [es] *Certificados cualificados de firma expedidos por Signaturit Global CA*

Service digital identities

X509SubjectName

Subject CN: *Signaturit Global CA*

Subject O: *Signaturit Solutions S.L.U.*

Subject 2.5.4.97: *VATES-B66024167*

Subject ST: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *EjDpGxLmP0DT4+6c4e//ZOyvJZc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-10-24T00:00:00Z*

29.4.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30 - TSP: IVNOSYS SOLUCIONES S.L.U.**TSP Name**

Name *[es]* *IVNOSYS SOLUCIONES S.L.U.*

Name *[en]* *IVNOSYS SOLUCIONES S.L.U.*

TSP Trade Name

Name *[en]* *IVNOSYS*

Name *[en]* *IVNOSYS SOLUCIONES S.L.*

Name *[en]* *VATES-B98333362*

Name *[es]* *VATES-B98333362*

Name *[en]* *SIGNATURIT-IVNOSYS*

PostalAddress

Street Address *[en]* *C/Acceso Ademuz 12-1º-Oficina 1*

Locality *[en]* *Paterna*

State Or Province *[en]* *Valencia*

Postal Code *[en]* *46980*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *C/Acceso Ademuz 12-1º-Oficina 1*

Locality *[es]* *Paterna*

State Or Province *[es]* *Valencia*

Postal Code *[es]* *46980*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:administracion@ivnosys.com*

URI *[es]* *https://ivnosys.com*

Issuer O: AC CAMERFIRMA S.A.
Issuer 2.5.4.97: VATES-A82743287
Issuer SERIAL NUMBER: A82743287
Issuer OU: CHAMBERS OF COMMERCE ROOT - 2016
Issuer OU: see current address at www.camerfirma.com/address
Issuer L: MADRID
Issuer ST: MADRID
Issuer C: ES
Subject CN: IVSIGN CA
Subject O: IVNOSYS SOLUCIONES S.L.
Subject 2.5.4.97: VATES-B98333362
Subject OU: see current address at <https://psec.ivnosys.com/address>
Subject L: PATERNA
Subject C: ES
Valid from: Thu Oct 05 12:09:20 CEST 2017
Valid to: Fri Mar 16 11:09:20 CET 2040
Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D6:CB:04:57:B9:20:19:CE:3F:A4:D9:6B:7A:15:EF:05:BB:F7:4C:FE:EA:35:98:
BC:85:F1:82:79:78:C9:CE:F8:0C:87:41:53:87:79:CA:71:42:1E:54:26:09:12:9B:68:3A:06:6F:6A:DF:C4:F9:15:E4:25:38:D9:59:9F:C0:81:C6:98:4F:85:8A:96:50:BA:0E:FF:4D:FC:1D:0F:51:
9B:D6:C6:59:4D:AD:65:A0:0F:00:54:F2:A2:91:38:EE:84:DB:07:42:BF:55:BF:01:AB:25:76:E3:85:A2:D7:61:13:C0:58:C6:26:4C:C8:35:9F:06:58:AA:AA:36:AF:4B:0E:59:52:4E:D9:89:CD:F
E:6C:56:2A:10:EE:27:74:A1:FE:D5:DB:EB:EC:9C:4C:94:FA:01:4D:BA:5B:06:01:87:D1:00:BD:3D:DB:3A:89:17:FF:25:BB:8D:A7:AF:64:03:6D:E8:C8:E4:66:7F:FF:9B:34:64:91:A9:5C:64:78
5E:75:2A:8A:04:DB:87:1D:CF:AC:67:CD:23:E0:02:3A:34:1D:F6:F7:75:3E:2C:4A:D7:15:7B:E2:3A:3E:FA:D4:87:50:5C:D6:8E:73:6A:B9:86:55:83:89:66:AD:70:C3:81:63:AB:68:5C:1C:09:
28:59:94:78:EA:A1:AF:57:20:4E:AC:93:0E:87:E8:CD:56:6F:74:17:F2:37:D2:0F:DD:73:5C:DF:DE:96:9C:88:BA:6D:D3:67:50:97:42:C3:E9:BD:16:FD:88:70:34:C1:88:9F:C8:F7:E6:0D:54:1
C:63:C6:E3:37:CF:BC:16:E2:7C:5C:B5:A4:9B:D7:35:A7:87:C8:00:F8:7C:AB:61:83:5E:D2:24:B2:B5:20:F0:95:B9:86:7F:09:6C:44:78:1D:CD:39:35:59:7A:37:46:D3:61:BA:22:C4:EE:42:B0
39:43:38:48:4C:8C:13:AC:DD:70:0A:D1:2F:8B:9C:8F:C8:6F:57:45:78:3F:D1:53:28:FD:CA:34:74:8F:93:AC:5D:06:57:6C:FC:16:21:ED:FD:1F:1E:B2:91:D8:AD:2A:8F:22:8E:22:15:98:F6
89:1B:4D:AD:F5:2F:41:CC:A1:5A:14:A5:46:8A:8E:A8:50:84:AC:AB:99:85:7B:85:95:61:AE:9D:95:03:9E:10:4B:9C:B9:A2:69:69:06:45:63:65:46:44:D0:81:F3:AC:4F:7B:F2:61:5F:26:B5:85
:BB:F2:C7:7F:4D:91:33:C9:AB:8E:70:96:8F:0D:48:BC:C3:1A:D9:F9:6D:66:8B:43:6B:63:A2:6F:0F:2F:97:B4:E1:00:D2:0B:10:08:6B:18:28:BF:3A:75:2D:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier 05:2D:62:F4:9B:C8:FD:62:24:F9:26:8C:21:35:1F:3D:2E:7C:12:0A
Authority Key Identifier 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B
Authority Info Access <http://www.camerfirma.com/certs/chambersofcommerceroor-2016.crt>
<http://ocsp.camerfirma.com>
Extended Key Usage *id_kp_clientAuth*
Certificate Policies *Policy OID: 2.23.140.1.2.2*
CPS pointer: <https://policy.camerfirma.com>

CRL Distribution Points

http://crl.camerfirma.com/chambersofcommercerooot-2016.crl
http://crl1.camerfirma.com/chambersofcommercerooot-2016.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

92:19:3F:42:7D:FD:45:D1:F7:EE:0C:0A:3B:1A:97:4E:A7:AF:76:79:18:39:90:E2:87:62:C1:3A:26:3D:B9:78

X509SubjectName**Subject CN:**

IVSIGN CA

Subject O:

IVNOSYS SOLUCIONES S.L.

Subject 2.5.4.97:

VATES-B98333362

Subject OU:

see current address at https://psec.ivnosys.com/address

Subject L:

PATERNA

Subject C:

ES

X509SKI**X509 SK I**

BS1i9JvI/Wik+SaMITUfPS58Ego=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2023-05-22T00:00:00Z

30.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

30.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en]

undefined.

[es]

undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3
Description		

30.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by IVSIGN CA*

Name [es] *Certificados cualificados emitidos por IVSIGN CA*

Service digital identities

X509SubjectName

Subject CN: *IVSIGN CA*

Subject O: *IVNOSYS SOLUCIONES S.L.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *see current address at https://psec.ivnosys.com/address*

Subject L: *PATERNA*

Subject C: *ES*

X509SKI

X509 SK I *BS1i9JvI/Wik+SaMITUfPS58Ego=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-10-28T01:00:00Z*

30.1.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

30.1.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3

Description**30.1.4 - History instance n.2 - Status: granted**

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by IVSIGN CA

Name	[es]	Certificados cualificados emitidos por IVSIGN CA

Service digital identities**X509SubjectName**

Subject CN:	IVSIGN CA

Subject O: *IVNOSYS SOLUCIONES S.L.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *see current address at <https://psec.ivnosys.com/address>*

Subject L: *PATERNA*

Subject C: *ES*

X509SKI

X509 SK I *BS1i9jvI/Wik+SaMITUfPS58Ego=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2018-11-22T01:00:00Z*

30.1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

30.1.4.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	<i>undefined.</i>
	[es]	<i>undefined.</i>

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3</i>

Policy Identifier:

Identifier	[OIDsURN]	<i>urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3</i>

Description

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[es]	Certificados Cualificados emitidos por IvSign Global CA
Name	[en]	Qualified Certificates issued by IvSign Global CA

Certificate fields details

```

Version: 3
Serial Number: 3791543443661982744169

```

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN:	IvSign Root CA
Issuer O:	IVNOSYS SOLUCIONES S.L.U.
Issuer 2.5.4.97:	VATES-B98333362
Issuer OU:	TRUST SERVICES
Issuer ST:	VALENCIA
Issuer C:	ES
Subject CN:	IvSign Global CA

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

Valid from: *Fri Sep 11 11:59:33 CEST 2020*

Valid to: *Sat Sep 11 11:59:33 CEST 2032*

Public Key:

```

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B5:D9:11:D2:CC:61:0A:97:75:0D:25:3D:B5:2D:70:47:04:03:59:70:0D:40:56
1E:6F:60:77:0E:D1:A2:CF:37:6F:F8:21:FC:57:61:47:78:84:51:2F:DC:D8:C3:85:A9:D2:88:78:12:09:E1:1B:52:A6:78:F3:82:62:08:85:53:91:63:BD:C9:14:99:9C:69:7C:09:DF:15:31:D8:1
8:21:1C:3:56:83:0E:6A:2D:6A:AD:02:CC:3C:74:48:CB:7A:15:21:5E:B2:09:ED:BA:14:1B:27:DE:29:75:BD:BD:95:A5:E9:C8:20:0B:62:47:78:FD:57:45:58:89:09:CE:E5:F2:8C:A0:9C:1F:3
B:65:1D:6E:C3:FF:67:A3:53:F8:EB:2E:1E:D1:7B:90:2F:97:E4:D3:EE:4A:33:95:C5:87:AB:2E:B8:32:91:41:48:BD:15:F7:B7:F9:BB:E5:D0:C2:BD:21:BE:26:86:68:B6:4A:B6:F8:7C:31:51:44:
C4:5E:51:44:79:F7:88:37:85:06:E2:36:3D:2A:18:5E:50:54:3C:29:5B:3C:8A:2C:4A:8F:09:67:80:E8:14:95:1E:7B:37:A9:DF:9C:F7:79:59:22:24:87:9A:9C:6E:45:EE:0A:18:03:09:63:6B:40:
27:0C:7E:75:FE:7E:64:F9:65:77:D1:31:DA:2E:D9:0B:F2:87:9E:F6:F6:0A:F5:A7:DC:FF:32:27:4D:7C:1D:48:67:86:B2:7D:A0:69:F6:46:A3:DD:38:02:90:EB:F8:16:19:2B:11:55:CF:98:80:57
41:44:2E:BC:59:48:57:67:28:7B:FD:F2:F0:E8:8C:D7:9D:5B:6D:0F:71:CF:AC:C5:1C:A2:80:18:52:52:A1:0F:D3:E3:FD:4F:F9:0F:4C:71:52:88:D2:58:EE:CA:0D:FE:C6:1D:C7:18:EA:4D:3D:
5B:1E:FL:CA:68:92:42:07:D3:72:98:2B:0F:0F:88:62:BA:88:2E:42:12:F2:FD:BD:22:C8:FF:A5:AF:27:32:09:90:09:75:30:53:1D:0F:E0:E2:58:DE:45:62:AE:E7:18:06:58:9D:03:CC:0E:71:30:
EB:F8:16:04:0C:B6:0A:1A:7E:13:75:17:76:88:8E:E1:16:66:6A:15:DB:C3:91:8A:A8:5C:54:10:9F:5A:50:81:AF:3D:FF:A9:0A:D6:C2:6C:53:EE:88:5D:F1:91:7F:9A:DD:34:A5:21:C8:2C:E0:6
E:A7:56:5F:66:0B:CA:03:5F:EF:5E:13:21:F2:C4:79:DA:5D:6F:72:26:9E:2C:85:D0:00:64:20:68:1C:73:A3:DD:37:26:85:C1:FE:78:66:D1:15:65:1E:87:02:03:01:00:01

```

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

Authority Key Identifier *38:D0:55:F8:59:2B:12:53:08:44:48:8A:2F:70:03:49:71:80:13:1E*

Authority Info Access

<http://ca.ivsign.com/certs/ivsignrootca.crt>

<http://ocsp.ivsign.com>

<http://ocsp2.ivsign.com>

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: <https://policy.ivsign.com>

CPS text: [IvSign Global CA. Certification Practice Statements and Certificate Policies: <https://policy.ivnosys.com>]

CRL Distribution Points

<http://crl1.ivsign.com/ivsignroot.crl>

<http://crl2.ivsign.com/ivsignroot.crl>

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D6:EA:13:D3:B7:70:57:17:E3:AD:56:07:3B:1A:9D:DE:00:57:97:60:3B:9A:A7:3A:71:04:48:E9:62:F5:41:C5*

X509SubjectName

Subject CN: *IvSign Global CA*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-07-04T00:00:00Z*

30.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

30.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.2.3.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.12.3.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.1.3

Description**30.2.4 - History instance n.1 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] *Certificados Cualificados emitidos por IvSign Global CA*

Name [en] *Qualified Certificates issued by IvSign Global CA*

Service digital identities**X509SubjectName**

Subject CN: *IvSign Global CA*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-11-17T00:00:00Z*

30.2.4.1 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30.2.4.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

30.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier *[OIDASURN]* *urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3.1

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.2.3.1

Description**30.2.5 - History instance n.2 - Status: granted**

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] Certificados Cualificados emitidos por IvSign Global CA

Name [en] Qualified Certificates issued by IvSign Global CA

Service digital identities**X509SubjectName**

Subject CN: IvSign Global CA

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-03-17T01:00:00Z*

30.2.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

30.2.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *undefined.*
[es] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3*

Policy Identifier:

Identifier *[OIDA sURN]* *urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3*

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3
Description		

30.3 - Service (withdrawn): Qualified electronic registered delivery service "SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS"

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/EDS/Q	
Service type description	[en]	An electronic delivery service providing qualified electronic deliveries.
	[es]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.
Service Name		
Name	[en]	Qualified electronic registered delivery service "SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS"
Name	[es]	Servicio cualificado de entrega electrónica certificada "SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS"

Service digital identities

Certificate fields details

Version:	3
Serial Number:	1201545153274936677250

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:82:97:98:40:EB:AA:62:7B:0C:8B:AF:77:FD:5D:18:A7:4C:4C:8E:DF:75:B9:F6:00:86:76:AA:01:2E:CE:6C:99:80:2E:F4:14:80:B6:F8:A9:1C:F6:3F:22:22:3F:3A:87:5F:F8:29:31:86:6F:32:AC:06:4A:39:51:0A:1B:4D:85:0C:5F:DC:09:5A:FE:90:66:56:4A:02:61:7F:C2:DA:2C:B5:C3:78:45:AF:19:8C:BC:24:CF:39:ED:30:A9:3D:AD:BD:1C:9F:17:D5:6C:A8:02:DC:FB:2C:DD:15:8B:06:80:32:C8:08:BA:6F:5A:2E:D6:61:91:E5:91:27:C6:69:F1:BE:C8:43:0A:A7:A8:6A:11:6C:4B:87:83:34:DB:92:E3:8E:DD:6E:88:A5:09:2D:BF:EC:A9:08:B1:69:48:8F:4E:D4:4C:69:8E:50:22:07:BC:0F:C7:AA:84:70:68:73:DF:DA:8B:10:D3:6B:A7:09:7A:AA:0B:C1:1B:09:BD:2C:9E:D2:66:F2:81:5F:92:C6:EB:18:08:18:08:B1:89:3D:AD:A2:FF:3E:16:F6:54:12:65:1A:5A:E4:20:64:02:8B:07:65:6A:6B:4E:26:86:C5:1F:A9:29:FC:F4:15:C4:65:6A:79:C2:E4:2F:78:4E:5E:E7:4C:97:AE:10:95:CA:67:C9:02:03:01:00:01

Basic Constraints*IsCA: false***Extended Key Usage***id_kp_clientAuth***Subject Key Identifier***AD:A9:06:A9:AA:80:F5:47:5B:2B:95:6D:4B:71:07:4F:6D:63:1F:91***Authority Info Access**

http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt
http://ocsp.camerfirma.com

Authority Key Identifier*C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42***CRL Distribution Points**

http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl
http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl

Subject Alternative Name

administracion@ivnosys.com
OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO

Issuer Alternative Name*ca@camerfirma.com***Certificate Policies**

Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2
CPS pointer: https://policy.camerfirma.com
CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false

id_etsi_qcs_QcCompliance
id_etsi_qcs_RetentionPeriod: 15

Key Usage:*digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***DB:9B:AF:22:84:63:BA:F4:AD:C8:3D:6A:AA:2E:88:69:2A:AD:0C:D3:A4:B6:C3:CD:27:00:1B:5A:86:AE:DD:AA***X509SubjectName****Subject C:***ES***Subject O:***IVNOSYS SOLUCIONES S.L.U.***Subject OU:***GERENCIA***Subject OU:***DIRECCION IT*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS SOLUCIONES*

X509SKI

X509 SK I *rakGqaqA9UdbK5VtS3EHT21jH5E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2024-03-13T02:00:00Z*

30.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[en] Qualified electronic registered delivery service "SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS"*

Name *[es] Servicio cualificado de entrega electrónica certificada "SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS"*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject OU: *GERENCIA*

Subject OU: *DIRECCION IT*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *SERVICIOS ELECTRONICOS DE CONFIANZA - IVNOSYS SOLUCIONES*

X509SKI

X509 SK I *rakGqaqA9UdbK5VtS3EHT21jH5E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-10-26T01:00:00Z*

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified electronic time stamps issued by "IvSign Qualified TSA 2021"
Name	[es]	Sellos electrónicos cualificados de tiempo emitidos por "IvSign Qualified TSA 2021"

Certificate fields details

Version: 3

Serial Number: 404100734891941768288075753007301544443672661421

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *IvSign Global CA*

Issuer O: *IVNOSYS SOLUCIONES S.L.U.*

Issuer 2.5.4.97: *VATES-B98333362*

Issuer OU: TRUST SERVICES

Issuer ST: VALENCIA

Issuer C: *ES*

Subject C: *ES*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *IvSign Qualified TSA 2021*

Valid from: *Wed Mar 10 11:06:18 CET 2021*

Valid to: *Sun Mar 09 11:06:17 CET 2025*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:82:E9:85:72:93:87:80:0D:1F:AB:DB:11:88:A8:19:8E:4D:6D:C6:87:9A:6D:C8:D3:7E:89:DE:F0:51:04:09:0A:DD:25:C9:BA:2E:3E:21:9B:67:4B:B8:D8:7B:1C:62:3C:47:FB:77:22:D1:80:8B:A1:EAE6:BC:81:C8:79:92:D5:52:8C:50:39:AA:86:AA:BB:54:2C:DD:11:45:43:CC:18:7E:E8:BC:16:48:3D:F8:57:87:2D:E8:66:2D:AE:FB:01:75:33:1F:FA:5F:AB:6B:33:23:2B:3C:D6:85:A5:D2:75:E6:9F:FA:EA:1E:DD:AA:40:84:D0:BB:DF:30:B9:AC:3B:42:A6:55:85:5B:F1:91:0F:F8:D5:F4:26:AE:D1:E3:38:85:5E:6C:70:D3:F1:7E:70:C4:2D:41:CC:EA:C4:E9:25:F3:07:52:B0:41:4B:C5:41:1D:0C:2C:0F:25:AD:F1:EC:B6:1B:B6:87:A6:72:5F:9E:C0:8F:36:AD:6:9:90:AA:95:0C:6C:3C:B5:0F:4D:AB:60:04:99:AE:CC:EF:86:5B:03:64:66:97:F1:0C:FB:D2:F2:D5:B5:21:F2:3D:01:93:5B:F5:CF:8A:05:7B:60:92:84:0E:F8:95:C2:66:74:39:01:AD:3F:CF:33:26:C1:30:34:F6:15:A3:E1:EA:A0:9C:C7:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

Authority Info Access *http://ca.ivsign.com/certs/ivsignglobalca.crt*
http://ocsp.ivsign.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.47304.3.16.6.8.4*
CP5 pointer: https://policy.ivnosys.com
CP5 text: [Certificado cualificado de sello electrónico de TSA. Consulte las condiciones de uso en https://policy.ivnosys.com]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl1.ivsign.com/ivsignglobal.crl*
http://crl2.ivsign.com/ivsignglobal.crl

Subject Key Identifier *FF:DA:12:CA:D5:64:1C:9C:3C:50:76:99:EC:3E:6E:E8:5A:4A:FC:18*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A5:C2:AA:07:A1:59:F4:ED:C9:F5:67:EC:5D:01:BC:D1:46:91:52:30:58:9E:4B:B7:E4:41:08:DA:93:B3:2E:AF*

X509SubjectName

Subject C: *ES*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *IvSign Qualified TSA 2021*

X509SKI

X509 SK I */9oSytVkHJw8UHaZ7D5u6FpK/Bg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-05-27T00:00:00Z*

30.4.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified electronic time stamps issued by "IvSign Qualified TSA 2021"*

Name *[es] Sellos electrónicos cualificados de tiempo emitidos por "IvSign Qualified TSA 2021"*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject CN: *IvSign Qualified TSA 2021*

X509SKI

X509 SK I */9oSytVkHJw8UHaZ7D5u6FpK/Bg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-10-26T01:00:00Z*

30.5 - Service (granted): Servicio cualificado de entrega electrónica certificada "Ivnosys Qualified ERDS 2024"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Subject C: *ES*

Valid from: *Tue Jan 23 16:04:42 CET 2024*

Valid to: *Sun Jan 21 16:04:41 CET 2029*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:CD:07:7C:16:89:68:3D:CD:69:43:D7:6A:06:96:AE:E2:D6:74:A4:F3:0A:F7:7C:C4:E9:08:9A:E3:57:82:04:F4:23:58:E4:A2:84:DF:39:F6:D8:D6:0A:F7:BA:D6:DC:0C:C3:8C:16:39:E6:82:E6:9E:B5:02:52:AB:6C:A2:8E:3F:32:E2:D0:12:76:55:8E:EE:D3:A6:E7:D9:5C:56:EE:BC:55:47:58:02:5B:26:91:78:3B:49:06:16:8B:92:6C:E6:58:99:65:C7:76:71:C4:86:85:7D:F9:F8:79:5C:AC:79:1B:05:8A:F5:D7:8B:40:57:7A:F7:BC:79:03:5D:47:DD:54:F9:C2:2F:36:C7:7F:AA:69:72:F1:56:9D:CD:7C:F8:79:84:41:00:06:56:22:BF:72:1C:31:62:4F:B0:66:5F:15:73:F8:82:4E:40:0E:0C:4A:CC:43:0B:99:80:9B:EE:51:96:3F:D8:5D:26:26:C9:33:8E:AC:04:24:95:02:D1:DF:4D:03:91:0F:9B:C8:C4:D8:B5:C5:78:F7:B4:F2:BC:80:F4:8E:30:35:22:FF:D8:4E:8C:69:0F:9E:FD:56:CE:92:41:25:CD:71:5B:DC:8A:EA:86:08:A8:00:DD:D5:C0:A2:94:15:D8:2C:AB:23:08:8E:F8:DF:10:F3:51:B9:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

Authority Info Access *http://ca.ivsign.com/certs/ivsignglobalca.crt*
http://ocsp.ivsign.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.47304.3.16.6.2.1*
CPS pointer: https://policy.ivnosys.com
CPS text: [Certificado cualificado de sello electrónico empresarial centralizado. Consulte las condiciones de uso en https://policy.ivnosys.com]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl1.ivsign.com/ivsignglobal.crl*
http://crl2.ivsign.com/ivsignglobal.crl

Subject Key Identifier *84:D6:AE:B3:CC:BB:63:44:66:9C:1C:15:1E:44:4E:A1:38:EE:83:E2*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D3:11:64:DE:C1:29:9A:C2:E3:C6:AC:DB:3E:2E:2D:BA:75:28:A6:49:D1:D3:4A:E0:73:21:AA:AA:A3:67:AC:21*

X509SubjectName

Subject SERIAL NUMBER: *B98333362*

Subject CN: *Ivnosys Qualified ERDS 2024*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>
Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>
Service Name		
Name	<i>[en]</i>	<i>Qualified electronic time stamps issued by IvSign Qualified TSU 2023</i>
	<i>[es]</i>	<i>Sellos electrónicos cualificados de tiempo emitidos por IvSign Qualified TSU 2023</i>

Certificate fields details

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *IvSign Global CA*

Issuer O: *IVNOSYS SOLUCIONES S.L.U.*

Issuer 2.5.4.97: *VATES-B98333362*

Issuer OU: *TRUST SERVICES*

Issuer ST: *VALENCIA*

Issuer C: *ES*

Subject CN: *IvSign Qualified TSU 2023*

Subject 2.5.4.97: *VATES-B98333362*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject C: *ES*

Valid from: *Thu Dec 21 10:17:41 CET 2023*

Valid to: *Thu Dec 21 10:17:41 CET 2028*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9B:3F:96:38:81:37:6D:1B:3C:11:92:7E:71:5E:95:D5:AF:F9:F1:49:ED:08:7E:61:17:6F:59:6E:55:22:8A:24:06:68:33:0A:0D:9D:B1:A3:3E:94:97:69:DC:74:EA:DE:CD:92:20:C7:5D:AF:3A:F1:F8:22:86:C6:45:AE:8B:53:59:7D:93:04:B5:A6:62:2F:66:82:7B:2D:A2:18:51:2B:5B:41:F1:F4:3F:A8:2A:89:6C:8E:56:36:0F:FB:FA:20:42:06:69:58:93:53:F6:9C:48:5C:94:B8:20:63:8F:C2:E6:DE:9E:AD:7B:FA:34:EF:6F:CD:98:15:15:88:03:1B:AC:C9:61:F8:DB:A0:8B:9E:A5:2D:3C:CC:0B:61:68:F1:DB:F4:60:97:8D:2B:C2:58:4A:10:A6:34:C6:28:77:4C:DE:36:D1:1F:30:19:71:F1:A0:E4:7A:7A:B0:20:25:8B:C5:E9:0E:33:DC:54:C1:A4:12:DB:5F:2D:8C:73:AA:C3:B4:05:27:01:F8:B4:2F:61:80:38:98:23:0D:1C:BF:52:BB:BE:5B:74:32:87:42:8E:95:71:3A:77:DC:76:75:B4:45:C1:63:67:9D:B4:4E:35:EA:7C:56:36:AE:CA:70:06:E0:85:BC:87:0F:3E:C0:81:AC:C2:C2:DE:BA:3A:EB:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

Authority Info Access *http://ca.ivsign.com/certs/ivsignglobalca.crt*
http://ocsp.ivsign.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.47304.3.16.6.8.4*
CPS pointer: https://policy.ivnosys.com
CPS text: [Certificado cualificado de sello electrónico de TSA. Consulte las condiciones de uso en https://policy.ivnosys.com]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl1.ivsign.com/ivsignglobal.crl*
http://crl2.ivsign.com/ivsignglobal.crl

Subject Key Identifier *76:9F:39:1C:BA:E0:D8:94:B4:F3:07:47:4B:E3:A0:25:9C:73:DC:C1*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm:	SHA-256
Thumbprint:	27:0A:27:29:B5:23:9B:4E:A6:BB:20:65:2B:E7:63:29:0F:76:25:93:58:D4:DB:4F:46:D8:02:AE:2E:E3:17:4B
X509SubjectName	
Subject CN:	IvSign Qualified TSU 2023
Subject 2.5.4.97:	VATES-B98333362
Subject O:	IVNOSYS SOLUCIONES S.L.U.
Subject C:	ES
X509SKI	
X509 SK I	dp85HLrg2JS08wdHS+OgjZxz3ME=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2024-03-13T02:00:00Z

31 - TSP: Logalty Prueba por Interposición, S.L.

TSP Name

Name	[en]	Logalty Prueba por Interposición, S.L.
Name	[es]	LOGALTY SERVICIOS DE TERCERO DE CONFIANZA, S.L

TSP Trade Name

Name	[en]	Logalty Servicios de Tercero de Confianza SL
Name	[es]	Logalty Servicios de Tercero de Confianza SL
Name	[en]	VATES-B84492891
Name	[es]	VATES-B84492891
Name	[en]	Logalty Prueba por Interposicion SL
Name	[es]	Logalty Prueba por Interposicion SL
Name	[en]	LOGALTY PRUEBA POR INTERPOSICION SL
Name	[en]	LOGALTY PRUEBA POR INTERPOSICIÓN SL
Name	[es]	LOGALTY PRUEBA POR INTERPOSICIÓN SL

PostalAddress

Street Address	[en]	Calle Valportillo Primera, 22, 1ª planta modulo 7 y 8
Locality	[en]	Alcobendas
State Or Province	[en]	Madrid
Postal Code	[en]	28108
Country Name	[en]	ES

ElectronicAddress

URI	[en]	mailto:info.ca@logalty.com
URI	[en]	https://www.logalty.com/en/
URI	[es]	https://www.logalty.com

TSP Information URI

URI [en] <https://www.logalty.com/en/>

URI [es] <https://www.logalty.com/>

31.1 - Service (withdrawn): Certificados cualificados emitidos por Logalty Qualified CA G2

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados cualificados emitidos por Logalty Qualified CA G2

Name [en] Qualified Certificates issued by Logalty Qualified CA G2

Service digital identities

Certificate fields details

Version: 3

Serial Number: 6317076465733621721

X509 Certificate

Signature algorithm: SHA512withRSA

Issuer C: ES

Issuer ST: Madrid

Issuer L: Alcobendas

Issuer O: Logalty Servicios de Tercero de Confianza SL

Issuer OU: *Logalty Trust Services*
Issuer CN: *Logalty CA ROOT 03*
Issuer 2.5.4.97: *VATES-B84492891*
Subject C: *ES*
Subject ST: *Madrid*
Subject L: *Alcobendas*
Subject O: *Logalty Servicios de Tercero de Confianza SL*
Subject 2.5.4.97: *VATES-B84492891*
Subject OU: *Logalty Trust Services*
Subject CN: *Logalty Qualified CA G2*
Valid from: *Wed Jun 06 13:08:49 CEST 2018*
Valid to: *Fri Jun 06 13:08:49 CEST 2031*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:02:02:01:00:D1:51:75:BF:DB:1F:FC:53:26:34:7D:BB:C9:72:8B:8F:BC:B4:28:D8:C3:9C:8C:06:0E:0C:5E:77:8B:4E:FA:5D:9E:18:29:6A:D2:1E:5D:05:E7:E4:E1:33:C6:A9:BA:CB:35:82:29:6C:B4:45:20:A8:2F:CA:53:84:1F:8C:81:95:96:89:9A:4F:27:5B:AD:72:E9:C7:7B:96:30:C0:20:58:33:AE:7E:49:06:DD:D9:8B:92:CE:C7:CB:8F:26:2E:BA:37:ES:8A:26:17:5F:A7:80:7B:1B:87:6E:67:86:98:DE:76:C5:11:84:92:E6:47:F2:05:19:A1:EC:FC:2A:C1:FA:5C:D9:35:E8:AB:2E:4E:61:F9:5D:77:6F:77:CD:DF:9B:87:6C:56:F0:A3:27:A2:F0:D8:15:DA:B8:D1:36:60:10:D9:53:50:4B:45:9E:5F:0F:D3:73:D0:AC:D8:EA:D8:0A:4D:C5:EB:7C:B5:F1:10:34:69:08:85:5C:87:C0:FD:21:07:AC:55:28:50:79:3F:89:23:47:47:A6:9D:66:9E:FC:C5:F4:1A:88:F2:F2:F1:E1:9B:09:BD:EA:B9:27:F1:C6:60:EE:4A:1B:CD:0D:76:CA:02:81:2D:69:66:26:E5:03:AB:EB:AD:9E:92:29:F9:92:94:44:48:85:4F:A2:23:2D:78:13:74:0E:F9:F7:3F:D9:22:7B:77:40:84:28:4D:F5:E6:E0:00:AB:59:72:67:99:13:30:25:46:7E:FE:AD:D7:64:91:17:58:18:01:7E:3F:3E:F5:32:18:7B:86:0D:CD:51:75:EA:DC:3E:0C:B9:19:B3:2B:D7:84:AB:F2:89:C8:E1:A9:D6:17:04:4C:E3:86:95:51:62:5D:67:26:FD:2C:88:FF:37:E4:C9:FC:15:4B:00:AB:87:D8:AC:26:18:50:3D:CF:79:E1:95:22:C0:A5:64:F1:82:78:9C:FE:37:DA:0D:41:3D:E2:C8:5F:64:30:73:5F:59:26:50:2D:52:A7:FE:F6:23:3A:58:B1:5C:32:01:53:07:AE:A4:A8:5D:0F:18:98:CF:26:C4:39:AD:17:AB:3C:BC:FD:4C:FE:72:CC:49:FD:31:67:35:88:54:51:38:F7:75:E9:2F:E9:C6:EA:09:33:18:77:E1:BC:87:7E:F3:3D:54:BC:9A:F4:53:1A:06:34:5B:EA:81:A3:3E:4D:AF:10:B4:21:1D:B1:62:F0:02:23:24:3B:DE:18:32:80:8D:EE:A3:40:2A:C4:17:2E:AE:8C:3C:D0:66:C3:24:8A:6F:97:33:D6:D2:F7:88:93:9A:45:72:F5:E7:B1:84:98:1F:B4:1E:C9:76:EB:B1:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Authority Key Identifier *7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82*
Authority Info Access *https://www.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt
http://ocsp1.logalty.es; http://ocsp2.logalty.es*
Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://www.logalty.es/PKI/documentacion/*
CRL Distribution Points *http://crl1.logalty.es/logaltyCARoot03.crl
http://crl2.logalty.es/logaltyCARoot03.crl*
Subject Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
Key Usage: *keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *05:95:C5:69:7A:6A:90:AE:41:15:6F:BF:8A:79:52:40:F9:54:B6:4D:77:61:8A:AC:81:2A:55:62:3E:9A:13:6F*

Valid to: *Sun Sep 04 14:07:18 CEST 2033*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:51:75:BF:DB:1F:FC:53:26:34:7D:BB:C9:72:88:8F:BC:84:28:D8:C3:9C:8C:06:0E:0C:5E:77:88:4E:FA:5D:9E:18:29:6A:D2:1E:5D:D5:E7:F4:E1:33:C6:AB:8A:CB:35:82:29:6C:84:45:20:A8:2F:CA:53:84:1F:8C:81:95:96:89:9A:4F:27:5B:AD:72:E9:C7:7B:96:30:C0:20:58:33:AE:7E:49:06:DD:D9:8B:92:CE:C7:CB:BF:26:2E:BA:37:ES:8A:26:17:5F:A7:80:7B:1B:87:6E:67:86:98:DE:76:C5:11:84:92:E6:47:F2:05:19:A1:EC:FC:2A:C1:FA:5C:D9:35:E8:AB:2E:4E:61:F9:5D:77:6F:77:CD:DF:9B:87:6C:56:F0:A3:27:A2:F0:D8:15:DA:88:D1:36:60:10:D9:53:50:4B:45:9E:5F:0F:D3:73:D0:AC:D8:EA:D8:0A:4D:C5:EB:7C:85:F1:10:34:69:08:85:5C:87:C0:FD:21:07:AC:55:28:50:79:3F:89:23:47:47:A6:9D:06:9E:FC:C5:F4:1A:88:F2:F2:F1:E1:9B:09:BD:EA:B9:27:F1:C6:60:EE:4A:18:C0:0D:76:CA:02:81:2D:69:66:26:E5:03:AB:EB:AD:9E:92:29:F9:92:94:44:48:85:4F:A2:23:2D:78:13:74:0E:F9:F7:3F:D9:22:7B:77:40:84:28:4D:F5:E6:E0:00:AB:59:72:67:99:13:30:25:46:7E:FE:AD:D7:64:91:17:58:18:01:7E:3F:3E:F5:32:18:7B:86:0D:CD:51:75:EA:DC:3E:0C:B9:19:B3:2B:D7:84:AB:F2:89:C8:E1:A9:D6:17:04:4C:E3:86:95:51:62:5D:67:26:FD:2C:88:FF:37:F4:C9:FC:15:4B:00:A8:87:D8:AC:26:18:50:3D:CF:78:E1:95:22:C0:A5:64:F1:82:78:9C:FE:37:0A:0D:41:3D:E2:C8:5F:64:30:73:5F:59:26:50:2D:52:A7:FE:F6:23:3A:58:B1:5C:32:01:53:07:AE:A4:A8:5D:0F:18:98:CF:22:6C:44:39:AD:17:AB:3C:BC:F0:4C:FE:72:CC:49:FD:31:67:35:88:54:51:38:F7:75:E9:2F:E9:C6:EA:09:33:18:77:E1:BC:87:7E:F3:3D:54:BC:9A:F4:53:1A:06:34:5B:EA:81:A3:3E:4D:AF:10:64:21:1D:B1:62:F0:02:23:24:3B:DE:18:32:80:8D:EE:A3:40:2A:C4:17:2E:AE:8C:3C:D0:66:C3:24:8A:6F:97:33:D6:D2:F7:88:93:9A:45:72:F5:E7:B1:84:98:1F:84:1E:C9:76:EB:B1:02:03:01:00:01*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82*

Authority Info Access *http://crt.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt
http://ocsp1.logalty.es*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://www.logalty.es/PKI/documentacion/*

CRL Distribution Points *http://crl1.logalty.es/logaltyCARoot03.crl
http://crl2.logalty.es/logaltyCARoot03.crl*

Subject Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C0:70:69:EB:4A:AE:CF:16:0B:7D:EC:65:52:69:5F:28:8F:8D:75:2B:DA:C9:2B:E2:0B:C6:C1:C3:F6:C5:7A:C8*

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified CA G2*

X509SKI

X509 SK I *Jkk+pa/3Zuk6lChXW+EbOKNS4mw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] undefined.

Status Starting Time 2026-05-20T03:00:00Z

Scheme Service Definition URI

URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

31.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

31.1.2 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.30210.1.3.1
Description		
Description		

31.1.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[es]	Certificados cualificados emitidos por Logalty Qualified CA G2
Name	[en]	Qualified Certificates issued by Logalty Qualified CA G2

Service digital identities

X509SubjectName

Subject C: ES

Subject ST: Madrid

Subject L: Alcobendas

Subject O: Logalty Servicios de Tercero de Confianza SL

Subject 2.5.4.97: VATES-B84492891

Subject OU: Logalty Trust Services

Subject CN: Logalty Qualified CA G2

X509SKI

X509 SK I Jkk+pa/3ZUk6lChXW+EbOKNS4mw=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2024-10-16T00:00:00Z

31.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

31.1.3.2 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.30210.1.3.1

Description

Description

31.1.4 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name [es] *Certificados cualificados emitidos por Logalty Qualified CA G2*

Name [en] *Qualified Certificates issued by Logalty Qualified CA G2*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified CA G2*

X509SKI

X509 SK I *Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2024-01-24T02:00:00Z*

31.1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

31.1.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

31.1.4.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

31.1.4.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.30210.1.1.1

Policy Identifier:

Identifier [OIDsAsURN] urn:oid:1.3.6.1.4.1.30210.1.3.1

Description

31.1.5 - History instance n.3 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [es] Certificados cualificados emitidos por Logalty Qualified CA G2

Name [en] Qualified Certificates issued by Logalty Qualified CA G2

Service digital identities

X509SubjectName

Subject C: ES

Subject ST: Madrid

Subject L: Alcobendas

Subject O: Logalty Servicios de Tercero de Confianza SL

Subject 2.5.4.97: VATES-B84492891

Subject OU: Logalty Trust Services

Subject CN: Logalty Qualified CA G2

X509SKI

X509 SK I*Jkk+pa/3ZUk6lChXW+EbOKNS4mw=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2019-10-28T01:00:00Z***31.1.5.7 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***31.1.5.8 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals***31.1.5.9 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[en]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication***31.1.5.10 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]****Qualifier type description** *[en]**undefined.**[es]**undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier***[OIDsURN]**urn:oid:1.3.6.1.4.1.30210.1.1.1***Policy Identifier:****Identifier***[OIDsURN]**urn:oid:1.3.6.1.4.1.30210.1.2.1***Policy Identifier:****Identifier***[OIDsURN]**urn:oid:1.3.6.1.4.1.30210.1.6.1***Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.30210.1.7.1
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.30210.1.3.1
Description		

31.1.6 - History instance n.4 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[es]	Certificados cualificados emitidos por Logalty Qualified CA G2
Name	[en]	Qualified Certificates issued by Logalty Qualified CA G2

Service digital identities**X509SubjectName**

Subject C:	ES
Subject ST:	Madrid
Subject L:	Alcobendas
Subject O:	Logalty Servicios de Tercero de Confianza SL
Subject 2.5.4.97:	VATES-B84492891
Subject OU:	Logalty Trust Services
Subject CN:	Logalty Qualified CA G2

X509SKI

X509 SK I	Jkk+pa/3ZUk6lChXW+EbOKNS4mw=

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2018-11-28T01:00:00Z*

31.1.6.11 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

31.1.6.12 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

31.1.6.13 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

31.1.6.14 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.30210.1.1.1>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.30210.1.2.1>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.30210.1.6.1>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.30210.1.7.1>

Policy Identifier:

Identifier [OIDsURN] <urn:oid:1.3.6.1.4.1.30210.1.3.1>

Description

31.2 - Service (withdrawn): Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU005*

Valid from: *Tue Oct 23 18:32:20 CEST 2018*

Valid to: *Sun Oct 22 18:32:20 CEST 2023*

Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:94:EB:91:CF:4E:E8:AC:75:30:2C:42:85:55:CF:42:2A:E7:56:8C:D6:56:D6:1A:83:07:5D:A7:D6:6C:6E:E2:07:05:C8:DF:8E:7C:28:36:F8:C9:99:40:38:C1:97:A8:67:63:6A:58:53:81:CF:4E:C5:57:E8:2D:54:77:DC:ED:68:FC:97:12:DF:63:EB:C2:74:FA:AE:2C:7E:67:4C:E3:7E:A4:46:0C:FE:52:30:69:39:CF:30:18:F6:B7:7F:A3:E0:E1:46:D0:42:1D:C6:DE:15:1F:BC:25:64:0A:5F:39:0C:F5:70:A7:6E:A1:79:AA:03:02:98:6C:07:5B:20:8D:F5:86:80:E3:C5:88:20:1E:8D:AA:F0:13:D2:61:88:69:79:1F:15:4F:A8:00:74:AB:52:FA:7C:BF:27:99:F8:9F:84:43:A2:F0:4F:37:C9:8C:8A:6A:1E:6D:B2:8E:37:9A:5B:5A:17:02:7F:E4:EF:74:87:58:6E:32:88:32:EE:0F:04:6D:63:94:3E:35:E9:1F:23:55:09:56:A4:72:3A:54:AA:A7:2E:B1:86:43:E7:CD:6D:1E:18:CC:D1:D6:3E:9C:7B:BA:61:3F:96:85:DC:32:08:4B:62:F1:71:6E:68:7A:24:53:FA:05:6D:12:35:C0:3D:DE:3B:90:1D:90:1B:39:69:DE:59:DF:CB:84:CC:DB:1C:98:06:CB:C1:C6:47:81:08:AE:AF:95:84:A1:FA:8E:6C:88:86:1A:47:11:D2:6E:68:34:D6:95:23:68:53:67:E2:13:B3:C5:B3:D3:7D:A6:6C:FA:FC:2D:00:6F:69:13:12:07:DF:D2:0E:B7:F4:2D:61:D9:37:01:77:26:87:E0:35:5D:37:3E:99:F4:BD:C4:00:39:92:39:3A:4A:3F:FF:5F:48:85:CF:52:85:11:67:A2:A6:AE:0F:4D:78:33:40:02:E3:70:E4:13:F2:08:52:9D:A3:71:67:88:EA:8E:27:81:87:24:C1:1E:8D:74:28:02:3F:07:FD:50:16:50:D2:64:99:27:25:87:EB:93:AD:44:EB:4C:FC:89:8B:86:9E:14:DC:79:67:A1:0D:BC:DE:14:F3:88:3E:B0:D7:F2:85:44:55:DD:71:4F:05:C5:E8:0E:E7:23:63:BC:23:AE:7D:74:A3:38:F2:31:53:EF:49:00:8D:88:19:0C:73:CB:3F:E5:ED:21:31:83:67:60:37:39:1F:30:F9:CA:69:20:68:E8:7E:70:F8:24:EB:EC:29:85:98:79:34:DD:72:73:65:3D:B6:63:F4:DC:2C:B3:C6:10:DA:57:12:0C:7C:14:91:23:DA:E3:C7:09:76:93:CD:73:02:03:01:00:01*

Authority Info Access *https://www.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt*
http://ocsp1.logalty.es

Subject Key Identifier *E2:43:C3:51:53:46:A0:32:47:35:3C:30:9C:3D:2B:3F:69:D5:A7:9E*

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Certificate Policies *Policy OID: 0.4.0.194112.1.1*
Policy OID: 1.3.6.1.4.1.30210.1.5.1
CPS pointer: https://www.logalty.es/certificateauthority/CPS
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CRL Distribution Points *http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*
http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8D:6F:1A:8B:DC:60:5B:88:10:DC:3F:F5:C0:A3:7C:A8:4A:ED:E7:13:DF:9D:87:82:E0:F7:3F:80:8D:82:F0:BA*

X509SubjectName

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU005*

X509SKI

X509 SK I *4kPDUVNGoDJHNTwwnD0rP2nVp54=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-12-21T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[es] Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005*

Name *[en] Qualified timestamps issued by Logalty Qualified TSA TSU005*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU005*

X509SKI

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty Qualified CA G2*

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject SERIAL NUMBER: *B84492891*

Subject CN: *Sello de entrega electrónica certificada cualificada de Logalty*

Valid from: *Wed Sep 12 11:08:48 CEST 2018*

Valid to: *Sat Sep 11 11:08:48 CEST 2021*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:95:FF:37:7B:7E:2C:D9:70:D9:10:EA:BD:AA:D1:B2:E0:6F:0E:7F:D7:87:47:E0:F0:CC:35:D9:60:9FA4:E4:05:9E:85:AD:45:AD:61:84:F1:83:1E:06:B6:A9:ES:E6:36:AD:8F:9A:87:2E:05:8A:56:0D:09:FA:12:65:76:39:40:89:6D:93:1F:84:76:2A:0B:C1:5F:4A:47:C2:BC:08:F9:87:33:AC:37:1A:3F:1C:41:EF:8A:87:EE:EC:64:71:80:32:40:C8:C2:34:22:D0:22:35:F6:BF:CD:BD:9E:07:EB:5D:8C:C4:32:75:AD:FB:5F:5C:3A:CD:08:F1:A6:A3:53:CF:E5:D1:75:26:DA:98:01:D9:6F:A3:DA:A9:C5:50:08:95:8F:0C:27:80:1E:D1:AE:EB:99:8A:CD:08:0E:7E:33:F3:37:72:9E:91:6A:85:97:33:98:75:D2:0D:C4:F7:D8:25:58:41:36:AE:DA:6D:19:B9:95:76:CB:70:D3:E6:C8:0C:9E:B6:CA:11:E3:6D:B6:BD:AD:F2:25:04:CE:A2:1F:BC:FE:B6:4E:ES:77:9D:22:C1:99:B2:2D:A9:E8:02:7F:C9:3F:2A:A4:C4:32:56:9D:A8:72:7D:72:A1:57:B7:08:46:82:D2:47:AA:AA:57:06:91:A2:57:77:E0:78:2F:8F:02:03:01:00:01

Authority Info Access *https://www.logalty.es/certificateauthority/LogaltyQualifiedCAG1.cacert.crt*
http://ocsp1.logalty.es

Subject Key Identifier *86:D4:F8:CF:75:9C:01:89:F8:FA:58:DE:8B:38:3C:05:D0:C1:EC:8B*

Basic Constraints *IsCA: false*

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Certificate Policies *Policy OID: 1.3.6.1.4.1.30210.1.3.3*
CPS pointer: https://www.logalty.es/PKI/documentacion/
CPS text: [Certificado cualificado de sello electrónico avanzado de persona jurídica]
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points *http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*
http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *info.ca@logalty.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *92:B6:E3:71:3C:78:86:89:D6:52:E7:59:83:6C:D9:6E:75:85:BF:B5:A1:CC:DE:22:D7:F2:1E:80:A3:4E:88:01*

X509SubjectName

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject SERIAL NUMBER: *B84492891*

Subject CN: *Sello de entrega electrónica certificada cualificada de Logalty*

X509SKI

X509 SK I *htT4z3WcAYn4+ljeizg8BdDB7ls=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2022-04-22T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.3.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[es] Servicio cualificado de entrega electrónica certificada*

Name [en] *Qualified electronic registered delivery service*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject L: *Alcobendas*

Subject O: *Logalty Servicios de Tercero de Confianza SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject SERIAL NUMBER: *B84492891*

Subject CN: *Sello de entrega electrónica certificada cualificada de Logalty*

X509SKI

X509 SK I *htT4z3WcAYn4+ljeizg8BdDB7Is=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-04-05T00:00:00Z*

31.4 - Service (withdrawn): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU006

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU006*

Name [en] *Qualified timestamps issued by Logalty Qualified TSA TSU006*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5762382065790029706*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:93:82:10:40:3C:D6:89:D1:85:0C:23:4C:B1:78:64:52:BC:2C:99:28:F1:CE:0E:C6:EA:E4:CA:46:22:C8:8A:9B:94:A7:F8:C3:15:35:1B:78:0E:45:88:E9:7D:9A:8F:A3:28:3E:60:90:C4:E2:28:FE:30:1C:66:D4:24:E2:68:A3:2C:E8:FC:74:E1:AC:AA:8E:59:83:DA:33:75:20:66:B3:83:76:F8:49:0B:D4:52:4C:8E:03:85:3C:7B:7C:3C:FE:E2:67:2D:6C:9C:63:0F:A1:84:67:E0:94:E6:5E:06:74:62:22:A4:B7:1B:DA:E3:E0:EB:D2:6F:FA:84:24:76:08:01:68:73:0E:60:FF:7F:9B:DB:94:4A:F2:43:38:13:09:1D:E8:44:20:BE:90:40:5A:BD:AD:1B:53:06:71:A1:85:F8:12:24:8D:74:54:36:84:00:DC:34:A7:05:C1:35:86:F8:29:6E:D1:BF:3D:AD:96:4E:96:6E:85:DF:65:07:E1:37:92:88:CB:0B:7F:F5:92:69:7B:48:90:5E:0F:40:34:5A:14:51:8D:3A:86:A0:10:32:87:D6:E5:82:CB:8A:F9:BC:BA:0F:BB:95:62:5F:EB:A0:24:D5:BF:AA:87:45:C1:70:71:60:DC:A9:A0:01:0F:85:4F:8A:3B:3F:9A:81:27:47:F4:62:CB:D8:64:FC:98:E4:CD:F8:8D:D1:76:DE:87:26:81:16:9C:0D:4E:74:C9:1A:6C:08:85:D9:75:98:9D:03:C5:F4:D4:FD:92:D5:EA:40:28:83:68:DF:F3:52:8A:7B:06:8B:13:68:C3:04:D1:15:34:DE:9E:BD:1C:4A:0D:BE:0C:D8:4F:3C:03:95:24:4C:63:AA:03:3F:A0:25:2F:41:68:FC:E1:83:F0:BF:A9:10:42:8D:BE:79:74:42:A3:01:29:7B:7E:D8:3F:E0:07:E6:09:9F:66:0A:6A:C9:DA:CA:3E:44:86:73:EC:8D:35:B5:85:E5:48:A5:6C:D5:3E:02:38:FD:25:52:FC:E8:9B:3A:88:9D:00:27:89:87:09:86:28:3E:8F:87:7A:5D:5F:13:98:C5:63:3B:73:A7:D3:DC:4F:AA:BD:BD:A5:FA:77:6C:F9:10:A5:3E:3B:AA:C6:F5:64:16:09:FC:EA:17:2B:4B:A6:98:82:45:7C:F5:B3:64:FC:5F:CE:E5:53:98:56:ED:CC:D2:48:3D:44:E1:80:27:01:4A:8E:8A:44:76:7F:CF:F8:0F:AE:9A:4F:EA:5E:D6:FC:95:34:DC:38:42:FD:EE:E4:4E:85:70:56:E8:84:D7:09:DF:9D:FB:A3:A7:7D:70:68:FB:AE:E5:37:FA:15:02:03:01:00:01

Authority Key Identifier

26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

Authority Info Access

<http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>
<http://ocsp1.logalty.es>

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.30210.1.5.1

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CPS pointer: <https://www.logalty.com/certificateauthority/>

Extended Key Usage

id_kp_timeStamping

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

<http://crl1.logalty.es/qualifiedLogaltySubCA02.crl>

<http://crl2.logalty.es/qualifiedLogaltySubCA02.crl>

Subject Key Identifier

86:38:96:DC:F8:77:04:90:71:1F:15:2D:81:0F:FD:B3:2D:47:A6:7E

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

D0:0B:B9:7B:7A:BA:BF:95:F5:78:A8:63:95:BA:8B:01:6B:C1:79:8C:57:40:08:12:D7:31:17:97:A0:A2:C1:C2

X509SubjectName**Subject C:**

ES

Subject ST:

Madrid

Subject L:

Alcobendas

Subject O:

Logalty Prueba por Interposicion SL

Subject 2.5.4.97:

VATES-B84492891

Subject OU:

Logalty Trust Services

Subject CN:

Logalty Qualified TSA TSU006

X509SKI

X509 SK I*hjiW3Ph3BjBxHxUtgQ/9sy1Hpn4=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time*2026-05-20T03:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.4.1 - History instance n.1 - Status: granted**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST***Service Name**

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU006*

Name [en] *Qualified timestamps issued by Logalty Qualified TSA TSU006*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU006*

X509SKI

X509 SK I *hjiW3Ph3BjBxHxUtgQ/9sy1Hpn4=*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

31.5 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty
Qualified TSA TSU007

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>	
Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name		
Name	[es]	Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU007
Name	[en]	Qualified timestamps issued by Logalty Qualified TSA TSU007

Service digital identities

Certificate fields details

```
Version: 3
Serial Number: 8216736880441155060
X509 Certificate -----BEGIN CERTIFICATE-----
```

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer ST: *Madrid*

Issuer L: *Alcobendas*

Issuer 0: *Logalty Servicios de Tercero de Confianza SL*

Issuer 2.5.4.97: *VATES-B84492891*

Issuer OU: *Logalty Trust Services*

Issuer CN: *Logalty Qualified CA G2*

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU007*

Valid from: *Wed Apr 07 15:22:02 CEST 2021*

Valid to: *Mon Apr 06 15:22:02 CEST 2026*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C6:C7:6F:6A:D8:6F:0C:0D:BB:DF:C8:3C:45:8B:7E:96:00:E4:66:0A:C7:B7:EA:38:FF:0C:DE:09:09:87:85:9B:9B:1B:30:6F:9F:90:1B:83:66:21:02:01:D4:9E:6B:B1:32:22:3A:80:95:50:52:F8:E3:19:22:93:45:CE:01:E9:3F:E5:6A:D2:16:C4:86:02:D8:0E:FC:3B:3A:33:B4:48:8A:3D:2C:DC:9F:2D:2B:32:69:8A:E1:8F:66:18:A9:4F:87:46:34:7A:0D:B3:1F:F3:3B:AC:45:20:A9:65:64:4B:7B:E1:A7:93:7A:F1:A6:30:C4:A1:94:87:2D:B6:8B:7D:0F:0F:00:25:1A:70:B8:80:66:E1:40:2B:0C:95:FC:50:0D:DE:4D:9B:E9:A8:45:0A:43:0B:18:B6:83:4F:7E:3C:5E:D7:DD:61:B0:9B:89:4F:1B:04:57:5D:D0:D6:81:6E:6E:21:98:57:61:85:5E:1D:7F:D6:94:0B:EB:DE:F5:00:F1:60:A7:6C:A9:22:78:05:72:55:D8:3D:83:44:A3:11:03:02:A9:B2:62:3B:A9:26:03:0E:AF:30:31:32:8A:CE:AA:46:91:0F:64:84:AA:8A:DE:44:F9:49:30:B1:EB:14:63:46:31:12:C2:F8:9A:C8:C1:42:AF:5E:AD:4E:11:89:25:6E:86:25:E1:FC:79:F9:CF:2F:A3:42:86:A9:63:C1:61:F4:90:30:F8:CD:EA:3D:47:35:A3:CD:8E:83:8B:8B:1B:70:6E:F8:C6:41:98:6F:63:50:4A:64:71:22:53:F8:C7:6E:17:67:67:55:1F:48:F4:FF:FF:3E:7E:D4:8B:7A:41:EF:2A:56:CD:43:40:8A:FC:8D:EB:6C:65:EC:55:D5:11:C4:A6:AA:92:03:46:0B:33:52:81:F5:F4:6A:70:55:6C:83:84:CE:22:AC:2F:1F:30:89:09:22:0A:B1:3A:C2:6F:1A:5C:8B:85:DE:A2:6A:97:FF:5C:F8:EA:6C:88:C3:92:CC:9F:56:84:9C:6F:E9:0B:20:42:A1:15:5A:73:C2:83:9D:C2:3D:AD:9E:9A:BF:0A:11:3E:55:BE:78:ED:97:6C:68:F4:44:61:29:16:69:30:F0:00:31:94:39:59:2B:0E:F1:68:9F:9A:C9:5D:F4:C9:33:C2:37:22:37:2F:78:69:A3:D8:F3:7A:88:36:1F:70:50:1E:71:ED:48:E8:EF:24:5A:CE:A4:D8:2C:FE:58:9D:55:3B:E8:11:33:A8:9F:1A:27:54:BE:E2:5F:A8:2A:FD:7A:C7:08:4D:17:1A:E5:EE:F4:A6:DC:EF:EE:10:79:13:1E:86:50:15:13:DA:F7:02:03:01:00:01

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

Authority Info Access
http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt
http://ocsp1.logalty.es

Certificate Policies
Policy OID: 0.4.0.194112.1.1
Policy OID: 1.3.6.1.4.1.30210.1.5.1
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
CPS pointer: https://www.logalty.com/certificateauthority/

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points
http://crl1.logalty.es/qualifiedLogaltySubCA02.crl
http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Subject Key Identifier *85:4E:F9:3D:FA:10:11:A0:B9:02:96:B5:90:B4:24:BA:B1:37:E2:92*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:06:46:45:E1:06:1E:A5:87:8B:12:43:EA:82:B2:C1:1C:11:71:B7:F4:CC:F3:01:E3:6C:88:B5:8D:DF:A8:A6*

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU007*

X509SKI

X509 SK I *hU75PfoQEaC5Apa1kLQkurE34pl=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2021-07-01T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.6 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU008

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU008*

Valid from: *Wed Apr 07 15:28:37 CEST 2021*

Valid to: *Mon Apr 06 15:28:37 CEST 2026*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EA:5D:1A:63:67:89:B2:0C:55:C9:02:B1:AB:73:5D:52:89:09:44:6E:7F:51:B1:6C:4C:67:FF:5E:90:F4:84:57:76:22:42:4C:8F:9F:04:56:28:19:07:4B:15:79:44:ED:81:37:31:5A:7C:EE:1D:52:96:62:9E:08:55:E2:55:F2:70:1E:58:2E:6C:F1:C0:F2:08:F1:3A:9E:A1:F1:E4:C6:02:78:67:FA:77:80:33:41:0A:FE:5A:BC:FC:99:84:05:00:49:10:39:44:00:1C:F8:68:BA:46:BC:A0:70:EB:7A:0F:E8:AD:B5:89:05:12:6A:9C:4A:68:B3:7E:E4:8B:31:C2:75:76:D0:BA:AB:C6:2F:25:41:F7:A6:A2:DF:4C:35:68:BB:82:34:36:BB:F1:27:83:F1:EA:79:5C:22:04:7D:0D:31:96:5D:23:F8:5E:AE:6D:DD:DA:36:6C:B7:0D:8F:FE:C1:45:A8:D7:A3:06:97:0D:D2:18:84:D2:8D:C4:4B:4E:0C:61:6E:61:F5:CF:35:3D:26:AE:90:4B:91:83:2F:2D:35:5A:02:15:07:A5:64:99:FE:DF:C8:1A:E1:3E:2E:A0:A0:F3:D5:1F:43:81:84:59:30:F3:10:6E:D7:EF:2D:24:B7:03:58:8D:CC:DB:D1:E3:5A:63:7F:8B:8B:AA:6F:25:1D:A7:97:74:30:E5:E7:A8:09:FC:07:6D:B3:01:F0:D7:79:4D:93:5E:4B:69:E9:6B:AF:B1:7F:5D:FC:57:D3:CB:24:3A:8D:CF:5C:30:4B:6F:2E:3F:15:32:85:D7:B1:2D:44:D0:3D:0F:43:BF:95:69:55:4A:FD:ED:78:9A:AD:85:2E:82:6D:E4:09:A7:50:21:D6:1A:E2:2F:3A:CC:B1:85:8A:D2:C9:1B:73:88:9A:E7:4F:E1:7C:F5:11:ED:63:DB:7F:F0:5C:1D:E5:3D:82:70:8C:5C:E0:FF:E9:C2:1D:33:C4:16:FE:8E:62:08:F2:22:3C:72:C7:8F:9F:39:AD:AC:7C:8E:94:3D:51:99:E3:8F:8A:6B:46:8A:BB:0B:77:7A:7C:4C:20:2E:82:07:EC:E7:05:E6:1A:54:51:1B:89:C1:6A:47:C8:7D:CB:79:C7:73:44:53:4A:49:5F:75:AD:BF:EF:CE:2A:FB:A7:73:54:5F:CE:9A:A3:F4:5D:DE:E3:82:14:DF:31:68:9D:03:E2:C0:9C:ED:9E:77:A9:A9:B3:2E:E3:C2:3C:15:77:5B:09:80:67:38:55:D0:11:AA:BE:DB:79:59:BB:D7:75:66:78:99:1B:48:BA:BC:13:C6:A5:9A:82:22:B5:01:5F:52:F6:8B:75:68:00:25:BF:45:02:03:01:00:01

Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

Authority Info Access
http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt
http://ocsp1.logalty.es

Certificate Policies
Policy OID: 0.4.0.194112.1.1
Policy OID: 1.3.6.1.4.1.30210.1.5.1
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
CPS pointer: https://www.logalty.com/certificateauthority/

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points
http://crl1.logalty.es/qualifiedLogaltySubCA02.crl
http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

Subject Key Identifier *E1:CD:3E:71:4A:33:7C:38:40:14:3A:C3:B4:0D:D6:B6:D4:D3:97:20*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *89:DD:A8:76:2B:40:6C:5F:63:97:26:B8:43:7B:23:5B:1F:B9:67:2E:DC:70:C6:EA:65:90:8D:83:12:B8:15:34*

X509SubjectName

Subject C: *ES*

Subject ST: *Madrid*

Subject L: *Alcobendas*

Subject O: *Logalty Prueba por Interposicion SL*

Subject 2.5.4.97: *VATES-B84492891*

Subject OU: *Logalty Trust Services*

Subject CN: *Logalty Qualified TSA TSU008*

X509SKI

X509 SK I *4c0+cUozfDhAFDrDtA3WttTTlyA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-07-01T01:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.7 - Service (withdrawn): Qualified electronic registered delivery service issued for “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en] An electronic delivery service providing qualified electronic deliveries.*
[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name *[en] Qualified electronic registered delivery service issued for “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”*

Name *[es] Servicio Cualificado de entrega electrónica certificada emitido para “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3338844724482481780*

Authority Key Identifier	<i>26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C</i>
Authority Info Access	<i>http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt http://ocsp1.logalty.es</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.30210.1.3.1</i> <i>CPS text: [Certificado cualificado de sello electrónico cualificado de persona jurídica con gestión de datos de creación de sello electrónico en nombre del creador de sellos]</i> <i>CPS pointer: https://www.logalty.com/certificateauthority/</i> <i>Policy OID: 0.4.0.194112.1.3</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_RetentionPeriod: 15</i> <i>id_etsi_qcs_QcSSCD</i>
CRL Distribution Points	<i>http://crl1.logalty.es/qualifiedLogaltySubCA02.crl http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</i>
Subject Key Identifier	<i>85:98:6D:93:D1:AF:61:4E:D0:A2:F3:1A:E8:6A:F9:EE:E2:4F:59:92</i>
Key Usage:	<i>digitalSignature - nonRepudiation - keyEncipherment</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>D9:8A:8D:C3:43:F2:C5:3B:2D:D2:26:9A:25:22:41:4C:E1:42:93:C7:2B:EF:35:B5:F D:6D:5F:0A:7F:FA:23:A2</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Alcobendas</i>
Subject O:	<i>Logalty Prueba por Interposicion SL</i>
Subject 2.5.4.97:	<i>VATES-B84492891</i>
Subject SERIAL NUMBER:	<i>B84492891</i>
Subject CN:	<i>Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada</i>

X509SKI

X509 SK I	<i>hZhtk9GvYU7QovMa6Gr57uJPWZI=</i>

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2024-12-03T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>
URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

31.7.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [en] Qualified electronic registered delivery service issued for "Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada"
Name [es] Servicio Cualificado de entrega electrónica certificada emitido para "Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada"

Service digital identities

X509SubjectName

Subject C: ES
Subject L: Alcobendas
Subject O: Logalty Prueba por Interposicion SL
Subject 2.5.4.97: VATES-B84492891
Subject SERIAL NUMBER: B84492891
Subject CN: Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada

X509SKI

X509 SK I hZhtk9GvYU7QovMa6Gr57uJPWZI=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2022-04-22T00:00:00Z

Subject C: *ES*
Subject ST: *Madrid*
Subject L: *Alcobendas*
Subject O: *Logalty Prueba por Interposicion SL*
Subject 2.5.4.97: *VATES-B84492891*
Subject OU: *Logalty Trust Services*
Subject CN: *Logalty Qualified TSA TSU009*
Valid from: *Thu Nov 25 13:01:06 CET 2021*
Valid to: *Tue Nov 24 13:01:06 CET 2026*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:5D:74:83:95:CB:FF:92:AB:62:01:01:45:D1:39:06:35:32:59:CF:8B:BD:6B:16:B1:5A:87:78:9B:E1:03:9E:10:E3:40:A2:05:30:C0:10:02:DD:74:C7:8E:F4:4C:55:C6:F1:68:3C:DC:2C:70:E6:0D:06:D3:1A:43:F1:0B:22:01*
Authority Key Identifier *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*
Authority Info Access *http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt*
http://ocsp1.logalty.es
Certificate Policies *Policy OID: 0.4.0.194112.1.1*
Policy OID: 1.3.6.1.4.1.30210.1.5.1
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]
CPS pointer: https://www.logalty.com/certificateauthority/
Extended Key Usage *id_kp_timeStamping*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
CRL Distribution Points *http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*
http://crl2.logalty.es/qualifiedLogaltySubCA02.crl
Subject Key Identifier *C4:D2:E7:3B:AC:D0:86:E5:6C:B9:9B:BE:A2:5A:B0:15:05:21:74:F5*
Key Usage: *digitalSignature*
Thumbprint algorithm: *SHA-256*
Thumbprint: *0D:AE:9C:B8:7F:52:B6:CD:A7:A7:84:73:03:97:46:6A:E5:54:72:79:BB:9D:B9:BE:70:97:C2:90:9D:B6:99:8A*
X509SubjectName

Subject C: ES

Subject ST: Madrid

Subject L: Alcobendas

Subject O: Logalty Prueba por Interposicion SL

Subject 2.5.4.97: VATES-B84492891

Subject OU: Logalty Trust Services

Subject CN: Logalty Qualified TSA TSU009

X509SKI

X509 SK I xNLnO6zQhuVsuZu+olqwFQUhdPU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2022-04-22T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

31.9 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU010

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.

[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [es] Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU010

Name [en] Qualified timestamps issued by Logalty Qualified TSA TSU010

Service digital identities

Certificate fields details

Page 1132

Public Key:

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:09:DE:3A:45:14:EF:B2:81:A0:47:83:A4:DE:5B:73:A4:0B:25:BA:86:88:7B:CF:61:DA:D8:C6:A8:E3:F5:F0:89:78:57:60:8C:C8:4D:92:7F:61:50:38:EA:10:0C:25:DF:7E:19:D6:DE:7F:3E:DD:53:68:95:27:00:D0:E9:F1:14

Authority Key Identifier

26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

Authority Info Access

<http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>
<http://ocsp1.logalty.es>

Certificate Policies

Policy OID: 0.4.0.194112.1.1

Policy OID: 1.3.6.1.4.1.30210.1.5.1

CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]

CPS pointer: <https://www.logalty.com/certificateauthority/>

Extended Key Usage

id_kp_timeStamping

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points

<http://crl1.logalty.es/qualifiedLogaltySubCA02.crl>

<http://crl2.logalty.es/qualifiedLogaltySubCA02.crl>

Subject Key Identifier

0F:5F:E7:84:74:08:2C:AD:F4:CC:9E:D2:33:79:8F:E4:57:A1:D3:39

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

F0:30:DA:FC:7B:51:C4:BF:49:2B:C5:B0:FC:67:6B:93:72:48:0E:47:7F:12:6D:34:B2:91:9F:84:09:CD:44:90

X509SubjectName**Subject C:**

ES

Subject ST:

Madrid

Subject L:

Alcobendas

Subject O:

Logalty Prueba por Interposicion SL

Subject 2.5.4.97:

VATES-B84492891

Subject OU:

Logalty Trust Services

Subject CN:

Logalty Qualified TSA TSU010

X509SKI**X509 SK I**

D1/nhHQILK30zJ7SM3mP5Feh0zk=

Page 1134

Issuer CN: *AC Firmaprofesional - CUALIFICADOS*
Issuer SERIAL NUMBER: *A62634068*
Issuer OU: *Certificados Cualificados*
Issuer O: *Firmaprofesional S.A.*
Issuer C: *ES*
Subject CN: *Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada*
Subject SERIAL NUMBER: *B84492891*
Subject 2.5.4.97: *VATES-B84492891*
Subject O: *LOGALTY PRUEBA POR INTERPOSICION SL*
Subject ST: *MADRID*
Subject C: *ES*
Valid from: *Tue May 28 12:19:53 CEST 2024*
Valid to: *Sun May 27 12:19:52 CEST 2029*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A3:FF:A7:5A:35:69:17:A8:C4:80:9A:CD:B4:4A:D9:EE:3D:3D:E7:6D:77:80:80:F3:84:3D:88:DC:17:2C:80:41:87:81:50:00:90:AD:AD:73:4E:88:AA:AA:46:43:E4:EA:46:06:C4:74:49:9C:13:A1:98:21:4B:4D:C1:97:9A:53:02:EF:DB:A4:C7:90:D9:A6:2C:6D:47:65:4F:6D:16:DA:80:A3:4E:9E:10:5C:89:F1:43:77:3B:14:84:C5:63:33:9A:55:66:A8:9F:04:0A:92:8C:0E:D0:1D:C3:22:B1:68:52:F9:2D:D3:A8:0E:D2:A4:DB:88:8E:FA:5C:30:A2:61:6B:04:DE:CC:4A:55:72:80:25:A3:25:FF:86:03:9A:95:60:F9:97:8C:80:FF:D1:67:F2:97:14:2C:75:13:96:94:DC:3C:9B:44:F9:B4:A3:E7:47:48:21:BB:03:BB:10:38:40:2E:03:4D:89:B1:57:7D:BB:06:19:BA:49:84:D2:54:87:10:55:0F:8E:74:A9:AE:4B:BC:FA:44:A7:EF:A4:76:12:8B:1D:88:95:B1:A6:33:0F:8E:6E:E4:13:2A:C0:78:79:E8:EF:B0:2F:13:A0:76:44:6E:95:F1:B2:8B:35:7C:8D:54:67:AA:A7:B2:A7:DC:E9:F4:0D:F5:23:80:EC:D7:02:03:01:00:01*
Basic Constraints *IsCA: false*
Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*
Authority Info Access *http://crl.firmaprofesional.com/cualificados.crt*
http://ocsp.firmaprofesional.com
Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.1.10.3*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.3
Extended Key Usage *id_kp_clientAuth*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*

Subject Key Identifier *76:79:4C:F1:FE:D4:4B:88:F2:BD:3B:FF:89:74:0A:D6:79:27:0B:7E*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2B:8E:BF:3D:E7:F5:96:33:C8:0E:A9:89:A0:14:75:D0:3A:61:05:8D:81:01:69:45:7A:DF:19:75:DC:88:4A:44*

X509SubjectName

Subject CN: *Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada*

Subject SERIAL NUMBER: *B84492891*

Subject 2.5.4.97: *VATES-B84492891*

Subject O: *LOGALTY PRUEBA POR INTERPOSICION SL*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *dnIM8f7US4jyvTv/iXQK1nknC34=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2024-12-03T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

31.11 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals LOGALTY QUALIFIED PRESERVATION SERVICE 2025

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service type description *[en] A preservation service for qualified electronic signatures.*

Name	[en]	Qualified preservation service for qualified electronic signatures and qualified electronic seals LOGALTY QUALIFIED PRESERVATION SERVICE 2025

Name	[es]	Servicio cualificado de conservación de firmas electrónicas cualificadas y sellos electrónicos cualificados LOGALTY QUALIFIED PRESERVATION SERVICE 2025

Certificate fields details

Certificate fields details

Version: 3

Serial Number: 92831083268599016740157410834268696514

X509 Certificate

[illegible]

Signature algorithm: *SHA384withECDSA*

Issuer CN: *FIRMAPROFESIONAL ICA B02 QUALIFIED OTSA 2022*

Issuer 2.5.4.97: *VATES-A62634068*

Issuer O: *Firmaprofesional SA*

Issuer C: *ES*

Subject CN: *LOGALTY QUALIFIED PRESERVATION SERVICE 2025*

Subject 2.5.4.97: *VATES-B84492891*

Subject O: *LOGALTY PRUEBA POR INTERPOSICIÓN SL*

Subject C: FS

Valid from: *Wed Oct 15 11:40:44 CEST 2025*

Valid to: Tue Oct 14 11:40:43 CEST 2031

Public Key:

Basic Constraints *IsCA: false*

Authority Key Identifier *62:86:15:B9:E8:FD:95:F4:49:13:F6:7F:0F:AD:06:B3:55:A1:1F:BB*

Authority Info Access *http://crl.firmaprofesional.com/ica-b02-qtsa.crt*
http://ocsp.firmaprofesional.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.1.4.1*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Certificado de Servicio Seguro de TSA cualificada]

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl.firmaprofesional.com/ica-b02-qtsa.crl*

Subject Key Identifier *16:34:D4:6F:47:EF:58:03:E9:39:B6:99:F7:F2:1C:00:FB:6C:39:06*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AE:2A:83:2F:E8:C2:FD:2B:3C:88:80:BD:BD:FC:13:EB:DC:DC:A4:B0:61:A2:00:9B:C2:7B:40:0C:8C:08:3D:50*

X509SubjectName

Subject CN: *LOGALTY QUALIFIED PRESERVATION SERVICE 2025*

Subject 2.5.4.97: *VATES-B84492891*

Subject O: *LOGALTY PRUEBA POR INTERPOSICIÓN SL*

Subject C: *ES*

X509SKI

X509 SK I *FjTUb0fvWAPpObaZ9/lcAPtsOQY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2026-05-20T03:00:00Z

31.11.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

Subject CN: *LOGALTY QUALIFIED VALIDATION SERVICE 2025*

Subject SERIAL NUMBER: *B84492891*

Subject 2.5.4.97: *VATES-B84492891*

Subject O: *LOGALTY PRUEBA POR INTERPOSICION SL*

Subject ST: *MADRID*

Subject C: *ES*

Valid from: *Mon Nov 03 15:28:44 CET 2025*

Valid to: *Sat Nov 02 15:28:43 CET 2030*

Public Key:

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A9:A4:3F:F5:85:D3:25:CA:74:39:41:6C:3E:2C:B2:2F:95:AA:90:FC:6B:BE:C9:
82:35:8C:A2:99:BE:8B:4A:5B:7E:9F:19:C3:91:F2:EB:66:7A:4C:7E:BF:8C:B2:78:28:6C:18:1D:5C:F0:33:D9:8A:DC:77:9D:46:8F:17:30:5B:AC:1F:56:A7:1C:26:35:37:09:D6:80:58:CF:98:6
D:86:C8:04:CB:1A:DE:F2:46:D1:15:18:95:65:96:36:8E:82:AC:57:8C:DF:57:95:54:03:BA:2F:41:07:7B:78:6D:0B:D5:97:88:C2:77:92:F2:0B:A9:D6:F7:67:45:EF:9F:F0:C5:88:9B:60:07:C6:
5D:D4:53:90:BE:95:8A:0B:25:65:48:92:1B:DE:89:4F:6E:74:E9:26:60:61:53:DE:E9:7B:25:E0:1E:CD:82:26:60:DC:69:91:80:C9:3F:2E:5E:DE:83:16:20:FC:55:E7:4F:5A:35:EB:9D:B
4:1A:86:5E:5F:E4:F2:88:42:79:F2:68:03:50:D7:AC:DD:F2:44:02:65:3C:1F:F5:69:AC:C2:45:BA:C7:93:48:0A:31:85:01:48:86:53:AD:A3:17:73:DD:64:EC:39:E3:66:2A:D1:C2:A5:1E:72:45:
C5:4A:68:80:56:1A:7B:9D:D7:21:5C:C5:40:28:0F:6E:9E:B5:45:C3:CD:A0:3A:DF:F6:91:24:EF:12:2D:B8:68:92:D1:68:23:52:88:4A:58:47:8E:CD:39:2C:17:C7:BF:F6:CE:B4:FF:21:D4:0E:7
7:73:E0:75:6E:73:6E:20:E7:BD:BD:61:AE:03:7D:DA:AC:80:EE:CD:4D:EC:80:8E:5D:C3:74:83:AD:D3:CF:0F:74:CA:C0:6E:96:08:F7:66:80:F4:97:37:DF:9F:60:36:BF:C1:03:23:17:87:D5:A3
91:14:2E:10:84:04:80:66:FB:42:E5:1C:66:92:A9:80:A4:56:6D:60:15:C4:D1:C9:85:EF:C2:95:EA:C6:11:A6:38:84:2B:FE:44:C9:E0:87:4A:89:6A:17:D2:89:AE:D9:2F:35:86:0C:9A:02:98:1
5:86:04:CD:3C:D4:49:D2:E7:76:FD:D3:26:59:01:70:24:08:DC:4F:57:23:97:D1:D7:0F:0E:2F:25:84:1A:6C:80:89:74:5E:4A:E0:84:61:1A:91:64:5C:66:41:3F:DE:6E:99:68:55:D4:68:2D:BB
4C:94:16:C0:67:24:5C:8B:84:21:DB:90:15:C4:08:64:54:85:4B:E1:94:72:BC:EE:CA:2B:00:C1:B5:A7:DB:48:EB:7F:72:8F:A8:75:0F:E0:FB:1C:67:FA:13:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *4B:CD:B9:DA:13:26:56:AA:8C:7E:88:78:80:84:7E:CE:89:92:93:80*

Authority Info Access *http://crl.firmaprofesional.com/ica-b01-q.crt*
http://ocsp.firmaprofesional.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.1.10.3*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.3

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.firmaprofesional.com/ica-b01-q.crl*

Subject Key Identifier *78:66:2F:4A:06:1A:95:0A:86:19:3D:2B:E7:82:E3:88:77:DB:6A:55*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F9:06:60:AD:14:99:66:2B:1F:4E:DB:66:41:88:0E:1F:26:79:A1:C2:9B:D1:D9:4A:A7:39:AC:5D:BF:F4:2D:4C*

X509SubjectName

Subject CN: *LOGALTY QUALIFIED VALIDATION SERVICE 2025*

Subject SERIAL NUMBER: *B84492891*

Subject 2.5.4.97: *VATES-B84492891*

Subject O: *LOGALTY PRUEBA POR INTERPOSICION SL*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *eGYvSgYalQqGGT0r54LjiHfbalU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-05-20T03:00:00Z*

31.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

31.12.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

32 - TSP: LLEIDANETWORKS SERVEIS TELEMATICS, S.A.**TSP Name**

Name *[en]* *LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*

Name *[es]* *LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*

TSP Trade Name

Name *[en]* *LLEIDA.NET*

Name *[es]* *LLEIDA.NET*

Name *[en]* *VATES-A25345331*

Name *[es]* *VATES-A25345331*

Name *[en]* *Lleidanetworks Serveis Telemàtics, S.A*

Name *[es]* *Lleidanetworks Serveis Telemàtics, S.A*

PostalAddress

Street Address *[en]* *C/ Téllez, 56 Oficina C*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28007*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *C/ Téllez, 56 Oficina C*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28007*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:info@lleida.net*

URI	[en]	http://www.lleida.net/en
URI	[es]	http://www.lleida.net/es

Page 1143

Issuer OU: *Certificados Cualificados*
Issuer O: *Firmaprofesional S.A.*
Issuer C: *ES*
Subject CN: *Lleidanetworks Serveis Telemàtics, S.A.*
Subject SERIAL NUMBER: *A25345331*
Subject OU: *TECHNICAL DEPARTMENT*
Subject 2.5.4.97: *VATES-A25345331*
Subject O: *Lleidanetworks Serveis Telemàtics, S.A.*
Subject ST: *LLEIDA*
Subject C: *ES*
Valid from: *Mon Feb 19 13:37:00 CET 2018*
Valid to: *Sat Feb 18 13:37:00 CET 2023*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D9:1C:22:66:AB:75:50:8B:2A:67:70:43:2A:F4:02:5F:BC:69:61:63:6F:FB:B2:22:AB:DA:46:13:A2:AA:01:30:15:AC:CD:0F:0A:9C:58:0B:F0:D4:72:15:D4:B5:C5:C8:E7:63:E7:61:E7:99:78:61:CC:84:AA:F8:19:CB:67:E9:76:28:0D:F9:B6:C6:81:82:0E:3F:47:4F:4F:DD:AB:95:38:72:7E:21:82:12:46:32:59:02:F0:C9:AE:C8:AA:66:A0:A1:9D:2A:18:76:12:85:20:19:AF:6B:2C:36:ED:98:0E:CC:47:2A:9E:1D:A5:E7:63:31:31:5B:A7:87:AA:40:3F:3D:9D:29:3B:31:C7:79:58:AD:02:98:46:6D:EC:34:D1:DC:FF:D3:B9:74:BE:6C:8A:3C:14:09:4E:AD:45:B7:B4:22:29:2D:16:20:8F:DE:D8:75:C9:43:59:DB:89:68:FB:F9:5D:AD:3F:FC:24:5A:60:C9:9D:D5:26:4C:8B:DB:2A:4B:0E:DE:46:60:00:42:C4:9C:FD:10:ED:9E:99:1B:88:17:03:71:4A:71:8A:1A:E0:FD:0E:84:B9:A2:32:B8:24:12:93:69:1C:FF:88:78:F8:37:8C:5B:76:D6:6F:50:33:D7:F2:AF:CE:9A:07:9F:63:48:C4:70:11:AF:FB:3D:02:03:01:00:01*
Authority Info Access *http://crl.firmaprofesional.com/cualificados.crt*
http://ocsp.firmaprofesional.com
Subject Key Identifier *83:73:0A:37:EB:18:17:66:AA:E7:07:A7:7C:DC:9A:41:C4:B2:AD:46*
Basic Constraints *isCA: false*
Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.1.10.2*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.1
CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*
Extended Key Usage *id_kp_clientAuth*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CF:14:2F:21:78:F3:FC:04:77:E7:0A:B8:24:38:8D:8D:CB:D9:4E:1C:9D:89:20:DC:E
E:BA:57:0B:7E:24:4F:7B*

X509SubjectName

Subject CN: *Lleidanetworks Serveis Telemàtics, S.A.*

Subject SERIAL NUMBER: *A25345331*

Subject OU: *TECHNICAL DEPARTMENT*

Subject 2.5.4.97: *VATES-A25345331*

Subject O: *Lleidanetworks Serveis Telemàtics, S.A.*

Subject ST: *LLEIDA*

Subject C: *ES*

X509SKI

X509 SK I *g3MKN+sYF2aq5wenfNyaQcSyrUY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2022-11-17T00:00:00Z*

32.1.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada "Openum eIDAS"*

Name *[en]* *Qualified electronic registered delivery service "Openum eIDAS"*

Service digital identities**X509SubjectName**

Subject CN: *Lleidanetworks Serveis Telemàtics, S.A.*

Subject SERIAL NUMBER: A25345331

Subject OU: TECHNICAL DEPARTMENT

Subject 2.5.4.97: VATES-A25345331

Subject O: Lleidanetworks Serveis Telemàtics, S.A.

Subject ST: LLEIDA

Subject C: ES

X509SKI

X509 SK I g3MKN+sYF2aq5wenfNyaQcSyrUY=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-10-26T01:00:00Z

32.1.2 - History instance n.2 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [es] Servicio cualificado de entrega electrónica certificada "Connectaclick"

Name [en] Qualified electronic registered delivery service "Connectaclick"

Service digital identities

X509SubjectName

Subject CN: Lleidanetworks Serveis Telemàtics, S.A.

Subject SERIAL NUMBER: A25345331

Subject OU: TECHNICAL DEPARTMENT

Subject 2.5.4.97: VATES-A25345331

Subject O: Lleidanetworks Serveis Telemàtics, S.A.

Subject ST: LLEIDA

Subject C: ES

X509SKI

Issuer O: *inDenova SL*
Issuer 2.5.4.97: *VATES-B97458996*
Issuer SERIAL NUMBER: *B97458996*
Issuer OU: *Certification Authority inDenova SL*
Issuer T: *Subordinate Certificate Authority inDenova SL*
Issuer L: *VALENCIA*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-A25345331*
Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*
Subject T: *Gerente*
Subject CN: *(A25345331) Lleidanetworks Serveis Telemàtics, S.A. - FRANCISCO*
Subject OU: *Gerencia*
Subject O: *Lleidanetworks Serveis Telemàtics, S.A.*
Subject GIVEN NAME: *FRANCISCO*
Subject SERIAL NUMBER: *IDCES-40897755Y*
Subject ST: *LLEIDA*
Subject L: *ALPICAT*
Subject SURNAME: *SAPENA SOLER*
Subject E: *claves@lleida.net*
Subject C: *ES*
Valid from: *Mon Oct 17 13:41:00 CEST 2022*
Valid to: *Tue Oct 17 13:51:00 CEST 2023*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:06:79:53:87:74:8D:11:6E:77:A5:0B:F5:B8:81:21:AD:D1:1E:75:37:3A:EA:D1:C1:2D:B9:ED:96:A4:50:B6:79:7E:83:4D:31:4D:34:F9:0E:72:EB:58:60:4C:F7:73:79:89:92:84:86:95:DE:E8:90:16:45:D8:2F:73:2D:54:65:58:E7:1C:F2:02:92:CD:3F:3E:ES:DE:B7:90:8A:36:39:42:05:29:91:67:31:81:1E:D1:D9:BA:A3:95:32:32:DC:66:FB:1C:20:8C:E4:72:50:9C:F4:41:94:22:6F:75:15:7A:DB:45:D5:72:C9:2E:77:CD:A8:17:A7:90:EA:79:43:5A:D7:25:A1:70:08:41:85:F8:BA:19:2F:D9:26:37:00:31:62:54:8A:83:DD:C3:86:69:F9:94:71:2B:07:93:5A:A7:3B:AC:F0:71:4A:14:98:BE:2D:13:3E:68:12:98:20:58:93:93:4A:5C:DC:1F:4D:04:DD:69:63:C:C:16:A8:51:52:04:02:03:4A:C9:7C:31:31:97:DF:73:44:03:77:85:29:C4:03:F2:61:8D:09:96:58:FB:C0:8E:3E:F3:14:8D:64:7F:68:D0:C6:0F:B4:D1:B8:56:4B:D0:F6:CD:B0:6D:4C:AD:55:92:28:4A:68:17:98:69:27:72:60:CA:1E:BB:78:83:07:ED:DA:80:11:F5:29:41:76:1C:92:00:BB:51:42:77:5D:A2:60:0F:4A:28:39:9F:62:14:82:05:44:FA:76:34:54:43:BE:32:02:43:0D:AE:71:9F:38:93:3C:5D:75:28:E1:8F:BE:BB:23:F2:9C:DD:66:1B:DA:68:C6:25:3E:C8:08:16:2C:17:79:A7:6E:DF:CF:F0:6B:81:9A:DA:37:2B:5A:93:3C:A0:36:79:A0:64:34:43:CF:BC:68:60:4C:E5:C7:D1:BA:38:A7:EA:2F:6F:60:FB:09:D0:1C:B2:78:90:C0:AF:C1:F9:BE:23:40:89:70:EA:F8:76:7D:78:D3:76:18:FA:35:F0:1D:B8:38:3B:7D:12:55:7F:46:6D:A4:B2:D7:90:DB:63:79:13:1E:BB:6D:F2:BE:4D:8F:6F:34:5D:E7:35:1F:B7:C3:16:97:9F:3A:95:9A:57:53:B1:AD:4A:24:A2:9B:47:0C:F7:C4:1C:7A:21:59:D7:4D:B1:59:77:AD:13:EC:EA:07:C3:D8:70:33:9B:21:A4:94:FA:AF:3D:A2:2E:93:14:2E:97:76:5A:03:48:1F:5F:61:C3:A2:29:3E:83:1D:CC:43:1C:DA:44:AF:11:EC:FF:37:01:FC:31:A7:34:37:3A:DD:E4:FE:74:EE:AF:57:3F:49:02:03:01:00:01*
Basic Constraints *IsCA: false*

Extended Key Usage	<i>Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id_kp_clientAuth - id_kp_smartcardlogon</i>
Subject Key Identifier	<i>32:D2:C8:42:B1:B4:F9:82:2E:5A:FA:B4:BA:74:17:5A:A7:E8:E0:5E</i>
Authority Info Access	<i>http://ocsp2.esigna.es http://certs.esigna.es/ca/indenova_pki_003.crt</i>
Authority Key Identifier	<i>C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46</i>
CRL Distribution Points	<i>http://crl1.esigna.es/sub/indenova_pki_003.crl http://crl.esigna.es/sub/indenova_pki_003.crl</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.1 CPS pointer: http://cps.esigna.es/sub/cps_sub003_ca.pdf CPS text: [Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio. Consulte las condiciones de uso en http://cps.esigna.es/sub/cps_sub003_ca.pdf] Policy OID: 0.4.0.194112.1.1 Policy OID: 2.16.724.1.3.5.6.2</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance id_etsi_qcs_RetentionPeriod: 15</i>
Key Usage:	<i>digitalSignature - nonRepudiation - keyEncipherment</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>07:2A:C4:A8:1C:43:E3:E5:9D:FB:7B:5B:BA:08:D2:C3:0A:67:E5:09:F6:10:2A:F5:E6:73:C3:E1:63:7B:64:E9</i>
X509SubjectName	
Subject 2.5.4.97:	<i>VATES-A25345331</i>
Subject 2.5.4.13:	<i>Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003</i>
Subject T:	<i>Gerente</i>
Subject CN:	<i>(A25345331) Lleidanetworks Serveis Telemàtics, S.A. - FRANCISCO</i>
Subject OU:	<i>Gerencia</i>
Subject O:	<i>Lleidanetworks Serveis Telemàtics, S.A.</i>
Subject GIVEN NAME:	<i>FRANCISCO</i>
Subject SERIAL NUMBER:	<i>IDCES-40897755Y</i>

Subject ST: *LLEIDA*

Subject L: *ALPICAT*

Subject SURNAME: *SAPENA SOLER*

Subject E: *claves@lleida.net*

Subject C: *ES*

X509SKI

X509 SK I *MtLIQrG0+YluWvq0unQXWqfo4F4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2024-02-08T02:00:00Z*

32.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada "Openum eIDAS" (2022)*

Name [en] *Qualified electronic registered delivery service "Openum eIDAS" (2022)*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A25345331*

Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

Subject T: *Gerente*

Subject CN: *(A25345331) Lleidanetworks Serveis Telemàtics, S.A. - FRANCISCO*

Subject OU: *Gerencia*

Subject O: *Lleidanetworks Serveis Telemàtics, S.A.*

Subject GIVEN NAME: *FRANCISCO*

Subject SERIAL NUMBER: *IDCES-40897755Y*

Subject ST: *LLEIDA*

Subject L: *ALPICAT*

Subject SURNAME: *SAPENA SOLER*

Subject E: *claves@lleida.net*

Subject C: *ES*

X509SKI

X509 SK I *MtLIQrG0+YluWvq0unQXWqfo4F4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-11-17T00:00:00Z*

32.3 - Service (granted): Servicio cualificado de entrega electrónica certificada "Openum eIDAS" (2023)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en]* *An electronic delivery service providing qualified electronic deliveries.*
[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada "Openum eIDAS" (2023)*

Name *[en]* *Qualified electronic registered delivery service "Openum eIDAS" (2023).*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1212304926833285336*

Subject GIVEN NAME: FRANCISCO
Subject SERIAL NUMBER: IDCES-40897755Y
Subject ST: LLEIDA
Subject L: ALPICAT
Subject SURNAME: SAPENA SOLER
Subject E: claves@lleida.net
Subject C: ES
Valid from: Wed Oct 11 11:14:43 CEST 2023
Valid to: Sun Oct 10 11:24:43 CEST 2027
Public Key: 30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:CA:0C:19:E0:C2:F5:74:46:98:0A:84:BF:5A:72:ED:B9:B7:E5:F4:C8:1F:2D:F3:09:5E:82:6C:A5:A8:84:51:92:4E:68:0E:37:CA:2A:06:F8:CE:E2:56:39:8B:5C:AC:51:26:85:4E:C2:40:0F:67:5B:2C:35:B8:BF:F5:B4:B6:58:CE:BE:10:44:FF:FC:DD:0F:10:D8:1E:14:C1:EC:10:80:6B:05:CF:EF:D0:88:CC:82:B4:C8:D3:09:2B:F4:F3:D6:C0:43:A5:2E:8B:17:28:56:4F:EA:40:32:8D:AF:54:1F:4E:A2:A3:21:30:4B:43:98:22:6D:63:C4:5C:51:B9:D5:7E:5A:10:76:69:12:31:AF:AE:7E:60:D2:A0:C7:EA:C8:C2:B1:9C:E3:49:F5:C6:8B:20:03:E7:3A:06:CE:56:11:FA:67:21:55:04:95:C8:F0:33:5D:7D:25:28:FF:D0:61:59:B8:AC:BC:9D:5B:15:92:31:59:EF:9C:EF:50:8B:39:C9:05:2F:D4:46:A5:70:EF:6A:65:02:16:2A:6C:86:EC:C6:3C:C1:97:0F:53:00:4C:52:42:B2:96:34:04:CF:9D:03:D6:EF:CD:46:43:D6:CE:4E:29:A3:FE:A8:7F:5E:69:DC:D2:4D:35:21:5F:12:B9:A0:6D:EA:38:2E:CD:0B:02:03:01:00:01
Basic Constraints IsCA: false
Extended Key Usage Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id_kp_clientAuth - id_kp_smartcardlogon
Subject Key Identifier EE:44:BB:94:EE:FC:4E:43:5F:9C:1A:89:2C:7B:69:CD:CE:80:AA:B3
Authority Info Access http://ocsp2.esigna.es
http://certs.esigna.es/ca/indenova_pki_003.crt
Authority Key Identifier C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46
CRL Distribution Points http://crl1.esigna.es/sub/indenova_pki_003.crl
http://crl.esigna.es/sub/indenova_pki_003.crl
Subject Alternative Name claves@lleida.net
OID.2.16.724.1.3.5.6.1.2="Lleidanetworks Serveis Telemàtics, S.A."
OID.2.16.724.1.3.5.6.1.9=claves@lleida.net
OID.2.16.724.1.3.5.6.1.8=SOLER
OID.2.16.724.1.3.5.6.1.6=FRANCISCO
OID.2.16.724.1.3.5.6.1.1=SELLO ELECTRONICO DE NIVEL ALTO
OID.2.16.724.1.3.5.6.1.7=SAPENA
OID.2.16.724.1.3.5.6.1.3=A25345331
OID.2.16.724.1.3.5.6.1.4=40897755Y

Certificate Policies*Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.4**CPS pointer: http://cps.esigna.es/sub/cps_sub003_ca.pdf**CPS text: [Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en http://cps.esigna.es/sub/cps_sub003_ca.pdf]**Policy OID: 0.4.0.194112.1.3**Policy OID: 2.16.724.1.3.5.6.1***QCStatements - crit. = false** *id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15**id_etsi_qcs_QcSSCD***Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:** *SHA-256***Thumbprint:** *9F:93:A3:7E:7D:10:32:F1:F3:7C:F4:92:79:CE:61:0F:20:62:B8:2F:CC:E4:2F:CF:F8:3A:70:5E:63:BF:30:8D***X509SubjectName****Subject 2.5.4.97:** *VATES-A25345331***Subject 2.5.4.13:** *Certificado de Sello Electrónico Centralizado UP (QSCD) - Emitido por inDenova SUB CA 003***Subject T:** *Gerente***Subject CN:** *(A25345331) Lleidanetworks Serveis Telemàtics, S.A.***Subject OU:** *SELLO ELECTRÓNICO***Subject OU:** *Gerencia***Subject O:** *Lleidanetworks Serveis Telemàtics, S.A.***Subject GIVEN NAME:** *FRANCISCO***Subject SERIAL NUMBER:** *IDCES-40897755Y***Subject ST:** *LLEIDA***Subject L:** *ALPICAT***Subject SURNAME:** *SAPENA SOLER***Subject E:** *claves@lleida.net***Subject C:** *ES*

X509SKI

X509 SK I

7kS7lO78TkNfnBqJLHtpzc6AqrM=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en]

undefined.

[es]

undefined.

Status Starting Time

2024-02-08T02:00:00Z

33 - TSP: TrustCloud Solutions, S.L.

TSP Name

Name *[en]* *TrustCloud Solutions, S.L.*

Name *[es]* *TrustCloud Solutions, S.L.*

TSP Trade Name

Name *[en]* *Branddocs SL*

Name *[es]* *Branddocs SL*

Name *[en]* *BRANDDOCS SL*

Name *[en]* *VATES-B87142618*

Name *[es]* *VATES-B87142618*

Name *[en]* *TRUSTCLOUD*

PostalAddress

Street Address *[en]* *PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*

Locality *[en]* *POZUELO DE ALARCON*

State Or Province *[en]* *MADRID*

Postal Code *[en]* *28223*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*

Locality *[es]* *POZUELO DE ALARCON*

State Or Province *[es]* *MADRID*

Postal Code *[es]* *28223*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:contact@trustcloud.tech*

Issuer CN: *UANATACA CA1 2016*
Issuer OU: *TSP-UANATACA*
Issuer O: *UANATACA S.A.*
Issuer L: *Barcelona (see current address at www.uanataca.com/address)*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-B87142618*
Subject CN: *Servicio preservación de firmas y sellos cualificados*
Subject SERIAL NUMBER: *B87142618*
Subject O: *Branddocs SL*
Subject C: *ES*
Valid from: *Thu Mar 14 20:24:00 CET 2019*
Valid to: *Sun Mar 13 20:24:00 CET 2022*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DD:FF:CB:97:76:5B:4E:3C:77:D3:E0:80:55:40:75:9B:A3:CF:35:40:9A:73:B1:30:FC:1C:C9:66:B8:22:17:CB:1C:86:E4:BA:D4:D7:A4:94:EF:BA:98:55:97:73:B8:57:C0:F0:60:94:34:14:1C:C4:B8:E1:94:10:91:1D:7E:20:5B:3C:03:58:06:05:C6:60:F4:B9:0C:08:E6:E0:8B:02:31:4F:1F:E7:D8:1C:52:FE:B0:22:0E:AE:26:FD:D6:02:EF:B3:AC:2E:8C:41:51:44:33:9F:9A:65:E0:B1:E6:88:ED:69:41:34:7F:4A:B7:89:38:E7:94:FC:24:CB:A0:F7:E3:6C:E4:70:7A:9C:17:40:85:20:D9:3F:22:EE:95:60:68:60:85:88:C7:05:A6:4B:CB:5E:38:15:E5:0E:FD:A7:80:A0:58:F2:4F:F0:B1:37:FA:97:90:40:76:07:67:B7:1F:CF:30:71:9F:A3:0B:13:97:BA:1C:18:56:F2:40:4E:F3:7A:CB:D8:58:18:4A:16:A6:96:E4:50:DD:89:B7:CB:EC:40:3C:68:44:33:1C:6F:4A:E5:64:F3:95:2E:63:73:76:38:B6:CB:58:82:0C:07:A5:51:AE:10:7D:E9:C5:74:E5:0C:A6:F6:DA:22:E1:18:D4:74:23:E5:25:0D:75:02:03:01:00:01*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD
Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt*
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>
Subject Key Identifier *CA:49:7B:9E:71:FF:22:2A:73:BF:E0:D0:41:D0:36:C9:32:C9:2F:A4*
Basic Constraints *IsCA: false*
Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*
Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Qualified certificate for e-seal in Remote QSCD]
CRL Distribution Points *<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>*
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *certificates@brand-docs.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *65:04:C5:1D:4F:9F:6B:E4:C2:6F:AD:85:03:B5:CC:6E:3D:39:E9:40:C7:0B:1F:5E:75:4D:2A:DA:BE:17:66:AC*

X509SubjectName

Subject 2.5.4.97: *VATES-B87142618*

Subject CN: *Servicio preservación de firmas y sellos cualificados*

Subject SERIAL NUMBER: *B87142618*

Subject O: *Branddocs SL*

Subject C: *ES*

X509SKI

X509 SK I *ykl7nnH/lipzv+DQQdA2yTLJL6Q=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2022-10-10T00:00:00Z*

33.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

33.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

33.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service Name

Name *[en]* *Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L.*

Name *[es]* *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor BRANDDOCS, S.L.*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B87142618*

Subject CN: *Servicio preservación de firmas y sellos cualificados*

Subject SERIAL NUMBER: *B87142618*

Subject O: *Branddocs SL*

Subject C: *ES*

X509SKI

X509 SK I *ykl7nnH/lipzv+DQQdA2yTLJL6Q=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-06-24T00:00:00Z*

33.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

33.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

33.2 - Service (withdrawn): Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L. (2022)

Subject O: *BRANDDOCS SL*

Subject C: *ES*

Valid from: *Tue Mar 15 10:35:00 CET 2022*

Valid to: *Fri Mar 14 10:35:00 CET 2025*

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D4:C8:A0:3F:90:BE:69:76:FA:C4:1C:04:95:30:91:02:28:94:FB:33:56:30:65:13:21:85:A6:78:71:13:FD:E1:BE:90:D6:50:5C:0A:A2:C3:38:60:05:84:3D:D0:1D:61:1E:C4:54:92:25:7C:D7:4F:3B:75:C6:68:86:BC:ED:57:BF:CC:CB:96:AE:A7:CE:1F:0F:6D:BE:9C:F6:E5:AC:F2:D2:E3:9E:E3:FE:2A:FE:5A:52:35:20:10:13:D1:11:D3:61:74:2B:68:95:C4:40:87:C8:72:B9:53:53:DB:8D:F3:19:81:CF:99:5C:2B:9C:62:54:5A:8E:F3:1C:C8:21:65:CB:FF:EB:C5:2A:A2:93:98:11:9F:1E:D3:6D:D4:A1:7E:59:EE:FC:7D:E7:E9:6C:C0:E5:FB:2D:04:35:43:C2:B9:32:AF:C5:27:83:3F:24:AD:86:69:D9:A6:8F:87:F7:20:1A:3C:02:7A:05:82:1B:D0:A6:CD:53:17:AE:AE:41:22:40:1F:62:FE:E0:A0:3D:A9:A2:33:D1:24:56:9C:0E:3D:B6:A1:10:E1:31:13:17:AD:E5:52:15:83:E2:39:12:9F:15:DF:D4:AA:65:F6:04:1D:A8:2E:AE:F1:61:B2:A5:5B:DC:19:32:A5:22:BB:2F:B9:DC:EF:37:B7:C9:49:CD:37:02:03:01:00:01

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_RetentionPeriod: 15

id_etsi_qcs_QcSSCD

Authority Info Access

http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier

D6:83:3D:D6:08:D6:88:D9:20:B0:7D:FD:95:93:C3:79:85:8D:D8:4B

Basic Constraints

IsCA: false

Authority Key Identifier

2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5

Certificate Policies

Policy OID: 0.4.0.194112.1.3

Policy OID: 1.3.6.1.4.1.47286.1.9.6

CPS pointer: https://www.uanataca.com/public/cps/

CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points

http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl

http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

Extended Key Usage

id_kp_clientAuth

Subject Alternative Name

certificates@branddocs.com

Key Usage:

digitalSignature - nonRepudiation - keyEncipherment

Thumbprint algorithm:

SHA-256

Thumbprint:

09:CC:A5:F5:EC:32:42:FE:FA:C0:38:5E:27:CF:CD:75:28:B7:84:DB:9B:1D:AB:63:D8:C8:40:F5:C4:B4:4A:00

X509SubjectName**Subject 2.5.4.97:**

VATES-B87142618

Subject CN:

Servicio preservación de firmas y sellos cualificados

Subject SERIAL NUMBER: *B87142618*

Subject O: *BRANDDOCS SL*

Subject C: *ES*

X509SKI

X509 SK I *1oM91gjWiNkgsH39lZPDeYWN2Es=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2025-04-16T02:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

33.2.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

33.2.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

33.2.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service Name

Name [en] *Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L. (2022)*

Name [es] *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor BRANDDOCS, S.L. (2022)*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B87142618*

Subject CN: *Servicio preservación de firmas y sellos cualificados*

Subject SERIAL NUMBER: *B87142618*

Subject O: *BRANDDOCS SL*

Subject C: *ES*

X509SKI

X509 SK I *1oM91gjWiNkgsH39lZPDeYWN2Es=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-10-10T00:00:00Z*

33.2.3.1 - Extension (not critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

33.2.3.2 - Extension (not critical): additionalServiceInformationAdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

34 - TSP: Ecertic Digital Solutions, S.L.

TSP Name

Name [en] *Ecertic Digital Solutions, S.L.*

Name [es] *Ecertic Digital Solutions, S.L.*

TSP Trade Name

Name [en] *ECERTIC*

Name [es] *ECERTIC*

Name [en] *VATES-B87428728*

Name [es] *VATES-B87428728*

PostalAddress

Street Address [en] *Avda. Europa, 24, Edificio B, Planta 1, Parque Empresarial de La Moraleja*

Locality [en] *Alcobendas*

State Or Province [en] *Madrid*

Postal Code [en] *28108*

Country Name [en] *ES*

ElectronicAddress

URI [en] *mailto:info@ecertic.com*

URI [en] *http://www.ecertic.com*

TSP Information URI

URI [en] *http://www.ecertic.com*

34.1 - Service (withdrawn): Qualified timestamps issued by ECERTIC

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Certificate fields details

Version: 3

Serial Number: 8085602031753677786

[illegible]

Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-A66721499
Issuer CN:	UANATACA CA2 2016
Issuer OU:	TSP-UANATACA
Issuer O:	UANATACA S.A.
Issuer L:	Barcelona (see current address at www.uanataca.com/address)
Issuer C:	ES
Subject 2.5.4.97:	VATES-B87428728
Subject CN:	ECERTIC QUALIFIED TSU01
Subject OU:	ECERTIC TSP
Subject O:	ECERTIC DIGITAL SOLUTIONS SL
Subject L:	MADRID
Subject C:	ES
Valid from:	Thu Oct 17 13:31:47 CEST 2019

Valid to: *Sun Oct 17 13:31:47 CEST 2027*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:77:C2:DF:B1:2C:1F:71:EB:A5:CE:AD:E3:76:8A:A1:F2:3D:1A:94:4D:49:3D:DF:1F:79:D6:82:B3:87:42:D2:68:74:41:5E:AF:88:CE:91:87:0E:4D:8C:C1:4E:17:83:CD:86:6A:70:20:0E:90:BF:1F:13:80:EC:6A:9A:F8:70:66:ED:0E:5A:6C:0A:63:AD:81:3B:83:1F:CB:8A:44:AE:E0:17:AA:6E:2D:A3:2A:95:CF:64:B0:A0:03:2C:DF:D6:05:9B:1B:B7:E2:35:D8:5E:D3:6F:B1:0C:7C:AE:27:D1:7B:68:FD:CC:35:7D:E6:5A:56:D3:74:F9:A2:24:05:18:D4:2B:78:9D:72:C2:AB:A6:A8:8D:C0:F0:38:4D:BA:B4:D3:4C:9F:D9:0A:13:AC:25:E8:6C:37:EC:4D:2C:19:BD:3A:7E:D0:8E:2C:46:8F:FE:91:30:78:6C:B3:87:F0:CD:AF:0C:55:EA:90:76:67:A9:2E:33:65:88:2D:9B:84:14:8F:44:41:95:80:F9:90:31:44:9C:7A:BE:CA:1A:1B:C3:8E:D5:A5:FC:79:E4:3E:1F:64:96:D3:7D:2D:DA:61:01:13:84:4A:7D:57:2E:13:A4:65:54:A8:E7:CF:95:02:65:E8:70:C1:F3:F9:BD:97:A1:2E:55:5C:92:E6:19:49:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *C1:1A:67:92:D4:E3:D8:30:84:24:3D:D5:1A:4C:35:27:97:18:5D:99*

Basic Constraints *IsCA: false*

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@ecertic.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0C:74:B1:2B:AE:CE:B8:32:22:44:C2:03:69:CA:00:2F:AE:74:CA:F3:61:5D:C0:FC:9D:C2:4B:39:5E:DC:EC:78*

X509SubjectName

Subject 2.5.4.97: *VATES-B87428728*

Subject CN: *ECERTIC QUALIFIED TSU01*

Subject OU: *ECERTIC TSP*

Subject O: *ECERTIC DIGITAL SOLUTIONS SL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I*wRpnktTj2DCEJD3VGkw1J5cYXZk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2021-10-26T01:00:00Z***34.1.1 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST***Service Name****Name** [en]*Qualified timestamps issued by ECERTIC***Name** [es]*Sellos de tiempo cualificados emitidos por ECERTIC***Service digital identities****X509SubjectName****Subject 2.5.4.97:***VATES-B87428728***Subject CN:***ECERTIC QUALIFIED TSU01***Subject OU:***ECERTIC TSP***Subject O:***ECERTIC DIGITAL SOLUTIONS SL***Subject L:***MADRID***Subject C:***ES***X509SKI****X509 SK I***wRpnktTj2DCEJD3VGkw1J5cYXZk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2019-11-06T01:00:00Z*

35 - TSP: DIGITEL ON TRUSTED SERVICES S.L.U.**TSP Name**

Name *[es]* *DIGITEL ON TRUSTED SERVICES S.L.U.*

Name *[en]* *DIGITEL ON TRUSTED SERVICES S.L.U.*

TSP Trade Name

Name *[es]* *DIGITEL ON TRUSTED SERVICES*

Name *[en]* *DIGITEL ON TRUSTED SERVICES*

Name *[en]* *VATES-B47447560*

Name *[en]* *DIGITEL ON TRUSTED SERVICES SLU*

PostalAddress

Street Address *[es]* *C/ ENRIQUE CUBERO, 9*

Locality *[es]* *VALLADOLID*

State Or Province *[es]* *VALLADOLID*

Postal Code *[es]* *47014*

Country Name *[es]* *ES*

PostalAddress

Street Address *[en]* *C/ ENRIQUE CUBERO 9*

Locality *[en]* *VALLADOLID*

State Or Province *[en]* *VALLADOLID*

Postal Code *[en]* *47014*

Country Name *[en]* *ES*

ElectronicAddress

URI *[es]* *mailto:contratacion@madisonmk.com*

URI *[es]* *https://www.digitelts.es*

URI *[en]* *https://www.digitelts.es*

URI [es] <https://www.digitelts.es>

URI	[en]	https://www.digitelts.es

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en] A time-stamping generation service creating and signing qualified time-stamps tokens.</i> <i>[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name [es] Sellos de tiempo cualificados emitidos por DIGTEL ON TRUSTED SERVICES

Name	[en]	Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES

Version: 3

Serial Number: 1128729369994969674913

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: AC CAMERFIRMA TSA - 2016

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA TSA - 2016*

Issuer OU: *see current address at <https://www.camerfirma.com/address>*

Issuer L: *MADRID*

Issuer ST: *MADRID*

Issuer C: *ES*

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject CN: *DIGITEL ON TRUSTED SERVICES*

Valid from: *Fri Aug 23 13:13:17 CEST 2019*

Valid to: *Wed Aug 21 13:13:17 CEST 2024*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:EA:AF:CF:0A:08:67:D4:56:24:A6:E7:83:F5:CD:F8:B3:64:3B:A0:8A:2B:83:A0:ED:00:91:3C:7F:56:52:7C:A1:22:C9:0D:1A:90:B7:05:82:8B:35:57:C8:F1:4E:9F:64:C5:47:56:00:83:7C:8B:C9:EB:53:C7:43:11:05:AF:C5:AE:B3:21:F3:34:D6:21:2E:65:2F:50:8D:49:2D:9B:9F:75:8A:07:87:F9:11:E6:E1:B4:73:1E:81:08:EF:A3:7A:0B:2E:86:60:EB:BE:A7:40:B5:92:E3:4E:1B:B5:70:54:5E:DF:83:17:72:23:F9:99:86:A8:36:51:D6:B4:E0:1F:CA:57:5B:D1:18:32:24:58:C6:99:09:F8:54:9D:E1:39:DE:92:09:38:C3:DF:EB:0D:A7:66:F1:75:13:09:A6:B2:D2:71:F6:D9:80:FA:66:99:A8:EB:06:03:A7:44:CB:03:E5:FE:0D:B2:84:60:02:68:66:FF:B5:13:E9:4C:97:E8:18:11:3E:A9:28:8B:53:36:69:60:C5:75:51:BF:55:AA:DE:43:42:53:8B:BB:EE:54:13:DC:D1:3D:3E:63:B1:5A:C3:21:57:DC:C8:FC:E3:E9:D0:7E:31:35:04:E8:AA:6D:79:35:4B:2B:00:62:65:0C:E3:22:9D:AB:F1:C5:02:03:01:00:01*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *F5:80:B3:6F:A3:FA:39:44:54:4F:13:C7:61:EF:06:F0:88:CC:D6:E1*

Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt
<http://ocsp.camerfirma.com>*

Authority Key Identifier *1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*

CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl
http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl*

Issuer Alternative Name *ca@camerfirma.com*

Certificate Policies*Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1**CPS pointer: <https://policy.camerfirma.com>**CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en <https://policy.camerfirma.com>]**Policy OID: 0.4.0.194112.1.3***QCStatements - crit. = false***id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15**id_etsi_qcs_QcSSCD***Key Usage:***nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***B9:90:57:F8:85:AD:50:70:55:A0:34:D0:29:5C:12:CD:E9:10:EA:47:51:61:51:18:D
C:E2:9A:81:4F:AB:B0:FA***X509SubjectName****Subject C:***ES***Subject O:***DIGITEL ON TRUSTED SERVICES SLU***Subject 2.5.4.97:***VATES-B47447560***Subject CN:***DIGITEL ON TRUSTED SERVICES***X509SKI****X509 SK I***9YCzb6P6OURUTxPHYe8G8ljM1uE=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2022-02-08T00:00:00Z***35.1.1 - History instance n.1 - Status: granted****Service Type Identifier***<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>***Service Name****Name***[es]**Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES***Name***[en]**Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES***Service digital identities**

X509SubjectName

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject CN: *DIGITEL ON TRUSTED SERVICES*

X509SKI

X509 SK I *9YCzb6P6OURUTxPHYe8G8ljM1uE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2019-12-16T01:00:00Z

35.2 - Service (withdrawn): Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020*

Name *[es]* *Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES 2020*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *870476239836202459339*

Subject Key Identifier	<i>D1:4E:10:0A:D0:4F:FC:71:B6:91:1D:1B:83:C7:A1:3B:D4:81:8C:9E</i>
Authority Info Access	<i>http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt</i> <i>http://ocsp.camerfirma.com</i>
Authority Key Identifier	<i>1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C</i>
CRL Distribution Points	<i>http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl</i> <i>http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl</i>
Issuer Alternative Name	<i>ca@camerfirma.com</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1</i> <i>CPS pointer: https://policy.camerfirma.com</i> <i>CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en https://policy.camerfirma.com]</i> <i>Policy OID: 0.4.0.194112.1.3</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_RetentionPeriod: 15</i> <i>id_etsi_qcs_QcSSCD</i>
Key Usage:	<i>nonRepudiation</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>D1:A9:E8:21:8D:8D:4C:33:3F:41:F3:0F:7F:03:0B:39:5F:F8:C6:5C:8E:88:07:1F:DE:09:0B:CF:63:40:21:BF</i>
X509SubjectName	
Subject C:	<i>ES</i>
Subject O:	<i>DIGITEL ON TRUSTED SERVICES SLU</i>
Subject 2.5.4.97:	<i>VATES-B47447560</i>
Subject CN:	<i>DIGITEL ON TRUSTED SERVICES</i>
X509SKI	
X509 SK I	<i>0U4QCtBP/HG2kR0bg8ehO9SBjj4=</i>
Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>
Status Starting Time	<i>2023-05-22T00:00:00Z</i>

35.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020*

Name *[es]* *Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES 2020*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject CN: *DIGITEL ON TRUSTED SERVICES*

X509SKI

X509 SK I *0U4QCtBP/HG2kR0bg8ehO9SBjj4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-02-25T01:00:00Z*

35.3 - Service (granted): Qualified timestamps issued by "DIGITEL TS QUALIFIED TSU 01 G1"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by "DIGITEL TS QUALIFIED TSU 01 G1"*

Name *[es]* *Sellos de tiempo cualificados emitidos por "DIGITEL TS QUALIFIED TSU 01 G1"*

Service digital identities**Certificate fields details**

Public Key:

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:88:CD:54:66:DF:EF:11:5E:4C:74:FF:AC:17:22:C3:80:BC:5B:49:16:48:47:7A:1A:DC:F0:5F:8D:15:85:74:F5:53:8D:84:7E:D3:80:5B:E9:93:4A:20:45:E3:33:05:BF:01:A6:3A:4D:F4:8F:0C:EA:F7:E2:36:42:A5:F4:4A:AC:4B:B6:14:56:BF:D4:CC:CC:2C:83:0A:D5:6D:21:A7:5A:93:D8:BD:9B:86:FF:23:B2:A0:DA:7E:27:9B:2D:95:F5:41:57:A2:4B:75:81:80:E5:AC:4F:61:13:B7:D9:1D:44:5E:08:5F:40:98:F2:69:3C:F6:8E:39:25:F5:F0:82:CE:F8:07:71:3D:E2:4F:AA:28:92:D9:86:93:C5:00:5B:DF:67:C7:EB:F7:94:B8:11:28:19:A0:99:1B:07:67:03:76:7D:30:A2:79:25:A3:DC:72:CE:2B:AB:F7:61:C4:71:1E:8D:7B:77:F9:BE:D5:47:17:1F:44:F2:73:A8:9C:C8:6D:19:A0:8B:60:B5:FC:CF:E7:45:CD:C0:1F:53:8F:C8:F0:9F:A9:E6:A2:F0:2E:7B:C8:67:06:09:98:52:6A:BF:9B:95:4D:2D:10:E7:51:78:71:BA:D4:4C:5D:50:A5:6C:5B:4F:89:7C:C6:61:BE:3C:CF:D6:0A:9F:59:04:5F:FA:5C:4F:BB:1B:DB:E6:85:8E:B3:C2:70:14:E3:2D:6E:34:97:B4:49:11:61:0F:7F:DD:F6:1D:84:A8:44:0B:E6:92:A4:B8:01:D8:53:64:0C:EC:FF:63:8B:C5:E8:82:E9:87:0C:63:33:BF:30:77:0E:FD:83:D4:AF:83:25:03:98:26:A1:90:8C:35:6A:E3:6C:ED:B7:92:80:CD:66:A8:F3:40:62:E8:93:8A:B9:95:C1:71:52:A5:8A:4E:3A:EC:3E:88:92:98:23:E5:0F:97:84:64:F0:5E:2E:72:30:CA:2D:E4:DE:E7:A5:54:8E:C0:2B:24:EF:2B:83:2D:65:2F:AA:40:47:81:88:C7:7E:4E:1E:A0:94:D1:42:A2:CB:BF:A6:DC:F9:E0:DE:F4:85:75:62:6D:2D:05:42:A3:EF:7D:71:DD:2D:D1:09:4A:91:4E:92:50:11:5B:3B:29:43:03:50:B5:72:C7:E8:3A:8D:1A:0F:E3:86:4B:2A:3B:25:91:C1:F1:84:6C:27:E0:29:C8:E8:12:ED:29:BF:FB:17:0A:B7:03:55:D1:1A:73:68:23:78:9B:2F:2F:67:A4:E3:FB:9F:24:4D:57:FF:18:B7:8D:5F:34:CD:F7:68:F5:72:E4:0F:2A:29:19:FB:A4:D4:4D:D7:5F:FC:D8:E7:24:4B:47:45:02:03:01:00:01

Basic Constraints

IsCA: false

Authority Key Identifier

90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

Authority Info Access

http://pki.digitalts.es/DIGITELTSQUALIFIEDCATSAG1.crt

http://ocsp.digitalts.es

Certificate Policies

Policy OID: 1.3.6.1.4.1.54225.10.1.1

CPS pointer: https://pki.digitalts.es/dpc/

Policy OID: 0.4.0.2042.1.2

Extended Key Usage

id_kp_timeStamping

CRL Distribution Points

http://crl1.pki.digitalts.es/DTSQualifiedCATSAG1.crl

http://crl2.pki.digitalts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier

C6:00:6E:47:EF:24:09:E7:E0:AB:E1:04:72:B2:4D:10:E4:2B:D6:56

Key Usage:

digitalSignature

Thumbprint algorithm:

SHA-256

Thumbprint:

*BA:7F:C0:35:E5:D2:E5:87:4C:6A:65:ED:FA:AD:C6:CC:39:31:AE:02:14:F6:0F:CC:D
A:33:08:AB:14:33:74:1C*

X509SubjectName**Subject C:**

ES

Subject L:

Valladolid

Subject O:

DIGITEL ON TRUSTED SERVICES SLU

Subject 2.5.4.97:

VATES-B47447560

Subject OU:

Digital Qualified Time Stamp Services

Subject SERIAL NUMBER:

B47447560

Subject CN:

DIGITEL TS QUALIFIED TSU 01 G1

X509SKI**X509 SK I**

xgBuR+8kCefgq+EEcrJNEOQr1IY=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

35.4 - Service (granted): Qualified timestamps issued by "DIGITEL TS QUALIFIED TSU 01 G2"

Service type description	<i>[en]</i> <i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i> <i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[es]	Sellos de tiempo cualificados emitidos por “DIGITEL TS QUALIFIED TSU 01 G2”

Issuer SERIAL NUMBER: *B47447560*

Issuer CN: *DIGITEL TS QUALIFIED CA TSA G1*

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G2*

Valid from: *Thu Jun 30 13:30:58 CEST 2022*

Valid to: *Wed Jun 28 13:30:57 CEST 2028*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:C8:2E:25:5C:F8:90:A4:9E:4A:C8:65:5F:3B:CD:4C:C8:10:07:25:3F:3C:0E:
7D:8E:6E:1B:60:AF:A7:EF:05:65:DD:45:49:98:29:75:E4:7E:68:DD:0F:38:95:CD:31:44:CB:6B:57:AB:C6:76:FC:02:C8:9D:1B:26:D0:7B:2A:FF:AE:82:ED:73:2F:21:33:85:1D:88:E9:CF:5
2:26:AE:90:10:96:E6:22:92:03:68:D6:6A:F1:1C:4F:58:98:B9:9C:12:17:89:15:1E:12:E2:CD:ED:96:29:B6:57:C0:C5:F7:E3:89:60:85:EC:D8:65:AC:C8:98:6C:94:FC:2A:82:93:A0:84:E4:E8:
D9:CC:21:CC:2E:F3:DB:D6:71:67:C1:3E:CB:98:4C:C5:6A:AF:D3:A8:8E:58:3A:36:46:40:7B:DA:A6:EB:13:1E:12:AB:79:1E:85:34:9A:BD:03:52:54:8A:01:11:5F:C4:AF:63:A5:3E:16:99:1C:
3D:BD:9A:40:D2:E3:98:CB:94:6D:9A:1D:10:8C:B6:F4:9E:1A:72:98:BE:50:FC:8A:6A:D5:43:CE:96:A3:96:04:0E:B0:A7:59:99:63:65:15:1F:33:82:FA:B3:95:40:C2:06:7D:05:FD:AB:17:E8:5
4:AE:32:FD:FE:0C:28:BE:BC:F0:E0:CC:86:F4:BE:15:2D:1D:EC:26:A8:B7:2D:26:83:66:1B:7C:A7:BF:6D:3E:13:03:71:B9:B4:48:29:A7:1F:D9:4C:09:0F:72:06:00:EC:96:01:D6:A2:BA:FF:E7:
69:81:97:FA:1A:F5:11:03:EA:F4:5A:8F:9B:E0:4D:E7:F9:7B:F8:BE:0E:32:01:5B:17:8B:78:77:90:6D:FE:2C:7D:2A:CC:35:7A:F3:F6:21:D1:68:07:F9:D1:1D:B5:29:98:71:EF:0A:A9:E3:E3:B4
34:BE:68:87:DD:36:94:A6:76:0A:9B:B6:E9:40:1F:3F:26:AA:12:FE:EF:0A:5E:D8:F4:0A:93:A2:77:21:A6:48:15:B6:3F:BD:53:7A:6E:8E:2E:07:27:25:D7:D8:72:62:0B:FA:9C:AD:18:10:2E:8
1:45:12:1F:BA:34:EB:7C:36:A1:68:2B:B5:CF:40:B4:E8:B9:2D:D1:61:54:4F:21:58:CD:BA:45:36:AE:9A:B0:D0:88:FD:77:A3:CF:F6:3E:8F:A6:EC:EC:C2:01:73:68:20:9C:D0:4C:9D:4D:8A:91
:CD:9B:F5:99:91:6B:BD:A3:5F:45:9E:F2:95:3E:72:92:4F:E7:20:CE:BD:83:F1:C4:15:C1:0F:2D:D6:69:2B:F7:E0:C3:1A:2B:25:2F:F8:63:75:E3:35:66:BD:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

Authority Info Access

http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt

http://ocsp.digitelts.es

Certificate Policies

Policy OID: 1.3.6.1.4.1.54225.10.1.1

CPS pointer: https://pki.digitelts.es/dpc/

Policy OID: 0.4.0.2042.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points

http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl

http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier *33:13:4D:09:C7:27:E0:3B:BA:B3:5E:E5:8D:89:52:80:1A:80:70:5C*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *42:20:4F:FC:35:09:CF:25:00:F2:03:07:F5:68:6F:10:0A:FD:84:FA:CC:9C:ED:B1:91:1E:15:4E:B5:6B:F7:AC*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G2*

X509SKI

X509 SK I *MxNNCccn4Du6s17ljYISgBqAcFw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time

2022-11-17T00:00:00Z

35.5 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G3 EDCSA

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G3 EDCSA*

Name [en] *Qualified timestamps issued by DIGITEL TS QUALIFIED TSU 01 G3 EDCSA*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *480465820508810237697165621069661986486501866851*

Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.54225.10.1.1</i> <i>CPS pointer: https://pki.digitel.es/dpc/</i> <i>Policy OID: 0.4.0.2042.1.2</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	<i>http://crl1.pki.digitel.es/DTSQualifiedCATSAG1.crl</i> <i>http://crl2.pki.digitel.es/DTSQualifiedCATSAG1.crl</i>
Subject Key Identifier	<i>F0:A2:B9:62:9F:51:E5:78:F2:A1:95:3E:68:06:74:61:C2:D4:09:6E</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>46:08:11:36:5D:55:B6:60:BB:73:D1:50:56:2D:06:59:68:8E:A0:9A:B5:9E:45:0F:56:18:9E:D6:EE:71:5F:C4</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Valladolid</i>
Subject O:	<i>DIGITEL ON TRUSTED SERVICES SLU</i>
Subject 2.5.4.97:	<i>VATES-B47447560</i>
Subject OU:	<i>Digitel Qualified Time Stamp Services</i>
Subject SERIAL NUMBER:	<i>B47447560</i>
Subject CN:	<i>DIGITEL TS QUALIFIED TSU 01 G3 EDCSA</i>

X509SKI

X509 SK I	<i>8KK5Yp9R5XjyoZU+aAZ0YcLUCW4=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description <i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2023-05-22T00:00:00Z</i>

35.6 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

A time-stamping generation service creating and signing qualified time-stamps tokens.

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Name

Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

Name

Qualified timestamps issued by DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

Version:

3

Serial Number:

607932644424710360540674319403629739410233125839

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer C:

ES

Issuer L:

Valladolid

Issuer 0:

DIGITEL ON TRUSTED SERVICES SLU

Issuer OU:

DIGITEL TS CERTIFICATION AUTHORITY

Issuer SERIAL NUMBER:

B47447560

Issuer CN:

DIGITEL TS QUALIFIED CA TSA G1

Subject C:

ES

Subject L:

Valladolid

Subject O:

DIGITEL ON TRUSTED SERVICES SLU

Subject 2.5.4.97:

VATES-B47447560

Subject OU:

Digital Qualified Time Stamp Services

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G4 EDCSA*

Valid from: *Thu Mar 16 13:21:58 CET 2023*

Valid to: *Wed Mar 14 13:21:57 CET 2029*

Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:7F:15:4C:55:91:45:8D:95:F0:4F:80:C9:0A:A6:41:D4:ED:D0:1A:12:25:16:86:00:51:B7:3A:A8:9A:28:B9:D9:1D:6D:A7:06:8C:47:66:79:E5:23:B9:51:0A:C3:10:32:1D:59:3A:33:74:A2:AA:48:AB:F0:CB:4B:25:E5:DB:BB*

Basic Constraints *IsCA: false*

Authority Key Identifier *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

Authority Info Access *http://pki.digitalts.es/DIGITELTSQUALIFIEDCATSAG1.crt*
http://ocsp.digitalts.es

Certificate Policies *Policy OID: 1.3.6.1.4.1.54225.10.1.1*
CPS pointer: https://pki.digitalts.es/dpc/
Policy OID: 0.4.0.2042.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl1.pki.digitalts.es/DTSQualifiedCATSAG1.crl*
http://crl2.pki.digitalts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier *72:8B:D8:EC:D8:DC:B3:FD:B7:44:B6:F0:78:0E:FC:04:48:EC:1D:6D*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E6:7A:2E:75:8C:88:73:5D:5A:76:F0:BA:53:3B:36:33:8F:5A:9D:B9:05:4C:E5:83:1C:30:A1:04:9F:12:5C:1B*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digital Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G4 EDCSA*

Issuer OU: *DIGITEL TS CERTIFICATION AUTHORITY*

Issuer SERIAL NUMBER: *B47447560*

Issuer CN: *DIGITEL TS QUALIFIED CA TSA G1*

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G5 EDCSA*

Valid from: *Thu Mar 16 13:18:36 CET 2023*

Valid to: *Wed Mar 14 13:18:35 CET 2029*

Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:3A:B9:F9:26:FB:F0:32:9A:FF:1D:4E:81:93:E8:2D:1B:9B:BF:2C:4A:3E:F1:78:D7:80:07:6E:BB:49:63:28:30:5A:D9:14:F3:F9:70:B2:69:62:65:B1:B8:3B:48:41:DA:7A:13:05:7A:F7:AE:9F:00:A2:C6:37:E1:FC:7B:30:E8*

Basic Constraints *IsCA: false*

Authority Key Identifier *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

Authority Info Access *http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt*
http://ocsp.digitelts.es

Certificate Policies *Policy OID: 1.3.6.1.4.1.54225.10.1.1*
CPS pointer: https://pki.digitelts.es/dpc/
Policy OID: 0.4.0.2042.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl*
http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier *B7:72:0D:47:7C:A1:82:24:D9:AA:94:6E:BF:65:AE:A8:1A:DB:7B:C7*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *18:33:FE:5F:4E:B1:0F:4E:98:00:6F:29:28:1A:49:B8:57:85:73:52:59:97:0D:DF:69:FA:E3:DA:A1:0B:67:5A*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU 01 G5 EDCSA*

X509SKI

X509 SK I *t3INR3yhgiTZqpRuv2WuqBrbe8c=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2023-05-22T00:00:00Z

35.8 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU EDCSA 01 G6

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU EDCSA 01 G6*

Name [en] *Qualified timestamps issued by DIGITEL TS QUALIFIED TSU EDCSA 01 G6*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *185422771044559183809484007942066712831832645039*

Certificate Policies*Policy OID: 1.3.6.1.4.1.54225.10.1.1**CPS pointer: https://pki.digitel.es/dpc/**Policy OID: 0.4.0.2042.1.2***Extended Key Usage***id_kp_timeStamping***CRL Distribution Points***http://crl1.pki.digitel.es/DTSQualifiedCATSAG1.crl**http://crl2.pki.digitel.es/DTSQualifiedCATSAG1.crl***Subject Key Identifier***21:02:63:16:C1:F8:84:80:77:D6:EC:8B:DE:59:AF:A2:5B:4C:2F:54***Key Usage:***digitalSignature***Thumbprint algorithm:***SHA-256***Thumbprint:***4E:5A:0E:99:9E:1C:D9:12:75:C5:7D:F2:94:C4:8A:23:00:D0:4E:A7:06:5D:58:31:25:63:C2:59:42:86:E8:D7***X509SubjectName****Subject C:***ES***Subject L:***Valladolid***Subject O:***DIGITEL ON TRUSTED SERVICES SLU***Subject 2.5.4.97:***VATES-B47447560***Subject OU:***Digitel Qualified Time Stamp Services***Subject SERIAL NUMBER:***B47447560***Subject CN:***DIGITEL TS QUALIFIED TSU EDCSA 01 G6***X509SKI****X509 SK I***IQJfSh4hIB31uyL3ImvoltML1Q=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2023-05-22T00:00:00Z***35.9 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU RSA2048 01 G7****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Name	[es]	Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU RSA2048 01 G7
Name	[en]	Qualified timestamps issued by DIGITEL TS QUALIFIED TSU RSA2048 01 G7

Version: 3

Serial Number: 371184069619154176167623148387204370136767472539

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer C: *ES*

Issuer L: *Valladolid*

Issuer 0: DIGITEL ON TRUSTED SERVICES SLU

Issuer OU: DIGITEL TS CERTIFICATION AUTHORITY

Issuer SERIAL NUMBER: *B47447560*

Issuer CN: DIGITEL TS QUALIFIED CA TSA G1

Subject C: ES

Subject L: *Valladolid*

Subject 0: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU RSA2048 01 G7*

Valid from: *Fri Mar 10 10:40:17 CET 2023*

Valid to: *Thu Mar 08 10:40:16 CET 2029*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:F6:E2:BC:E7:7D:CE:32:3C:73:55:67:33:90:F7:49:A5:21:ED:24:61:05:ED:00:67:5E:A7:E1:93:DD:A1:CD:64:3A:E2:90:4A:97:60:C3:34:AC:73:72:79:1B:70:C1:87:3B:F5:F4:F0:A0:5C:6E:47:AA:E7:5F:84:23:DA:0F:6F:50:5A:F9:A9:0D:22:0E:19:22:03:73:27:4D:B D:4B:C1:F9:24:88:55:AA:15:46:9D:4B:18:C4:A9:38:F8:07:40:38:06:F3:DA:33:32:98:A3:17:7B:44:49:4C:0D:F6:E3:88:17:81:6D:E4:CD:57:C1:99:4C:8A:8B:1F:14:63:A8:E3:34:95:04:64: 7E:75:C5:83:7F:C4:85:7E:41:19:AD:9F:CD:10:E9:96:2F:78:AD:22:CC:51:23:2F:80:B2:A1:82:E6:AD:E9:E0:F9:BC:54:E5:96:01:68:4A:63:61:DD:75:43:A3:B5:F8:C3:1B:24:80:90:52:60:2 A:78:3F:A3:EA:06:50:4D:80:30:44:48:1E:88:77:CD:5A:44:D9:17:A9:C3:FA:13:95:7B:BF:6F:12:6D:81:55:21:5C:2C:AF:79:94:F8:E3:B2:7D:DF:67:98:E5:ED:F1:3F:AB:E2:76:C8:5C:C7:85: BC:54:13:9E:92:34:03:31:80:EF:B7:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

Authority Info Access *http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt*
http://ocsp.digitelts.es

Certificate Policies *Policy OID: 1.3.6.1.4.1.54225.10.1.1*
CPS pointer: https://pki.digitelts.es/dpc/
Policy OID: 0.4.0.2042.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl*
http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier *16:79:94:50:42:F3:1E:08:4B:C2:DD:9E:D7:32:A4:64:04:11:85:00*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F6:D3:2D:AB:31:27:F5:0B:88:A1:A5:36:AA:83:22:A1:73:A3:4B:82:C6:BE:CF:4B:D D:9A:5D:36:FB:49:08:04*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Issuer C: *ES*
Issuer L: *Valladolid*
Issuer O: *DIGITEL ON TRUSTED SERVICES SLU*
Issuer OU: *DIGITEL TS CERTIFICATION AUTHORITY*
Issuer SERIAL NUMBER: *B47447560*
Issuer CN: *DIGITEL TS QUALIFIED CA TSA G1*
Subject C: *ES*
Subject L: *Valladolid*
Subject O: *DIGITEL ON TRUSTED SERVICES SLU*
Subject 2.5.4.97: *VATES-B47447560*
Subject OU: *Digital Qualified Time Stamp Services*
Subject SERIAL NUMBER: *B47447560*
Subject CN: *DIGITEL TS QUALIFIED TSU RSA2048 01 G8*
Valid from: *Fri Mar 10 10:47:43 CET 2023*
Valid to: *Thu Mar 08 10:47:42 CET 2029*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AD:CD:38:C4:BE:E2:C2:D6:16:BA:24:A5:0A:A4:63:BA:73:4C:D1:32:33:7F:AF:2D:0A:6E:86:14:33:4D:5F:0A:75:B1:7E:C7:1E:D7:5D:DF:75:0F:D5:8A:BB:F3:84:F7:F8:F1:AE:97:52:6E:66:C0:E4:D5:E6:17:6F:F0:6C:F1:A1:F0:89:95:FE:98:8B:E3:44:A3:D1:DA:A1:1E:6B:2D:D7:AB:66:A9:58:9E:D8:13:8E:0E:40:53:79:31:AE:17:35:87:48:7C:66:69:8A:0C:8D:AD:3E:77:4B:50:96:38:0E:42:DB:E4:48:26:03:74:4C:D2:B3:9F:EE:3B:6F:18:E6:D0:D2:86:6E:A2:61:29:63:17:80:D7:E5:34:AD:D9:D0:68:89:19:E6:0A:E3:E2:24:4D:DA:03:1A:3A:4D:9B:8C:84:16:99:0D:7D:46:07:0E:6B:75:0D:E1:1E:BD:CC:A3:DA:35:DE:70:28:78:D1:94:27:EE:CD:28:0E:E7:CA:19:91:9B:C3:A9:FD:F1:DA:82:55:0C:91:81:26:F8:ED:E0:81:5D:46:2D:25:8F:D9:08:C3:33:26:A8:0F:FD:EA:3A:72:D2:C1:0C:51:DF:D3:37:14:4F:03:7F:90:C2:BC:C6:EF:D1:C7:6B:C8:8E:1E:6D:68:06:A3:9A:9F:3E:C1:02:03:01:00:01*
Basic Constraints *IsCA: false*
Authority Key Identifier *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*
Authority Info Access *http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt*
http://ocsp.digitelts.es
Certificate Policies *Policy OID: 1.3.6.1.4.1.54225.10.1.1*
CPS pointer: https://pki.digitelts.es/dpc/
Policy OID: 0.4.0.2042.1.2
Extended Key Usage *id_kp_timeStamping*
CRL Distribution Points *http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl*
http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl

Subject Key Identifier *67:25:CC:83:09:F4:50:6C:7A:11:6A:C6:19:9D:5F:D1:5B:A3:6F:AA*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *35:AD:EC:97:9B:5A:AE:56:1E:D4:04:4F:4D:CA:B7:86:BF:B6:51:28:35:96:96:02:55:E1:B0:80:69:39:AF:73*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel Qualified Time Stamp Services*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED TSU RSA2048 01 G8*

X509SKI

X509 SK I *ZyXMgwn0UGx6EWrGGZ1f0Vujb6o=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2023-05-22T00:00:00Z*

35.11 - Service (granted): Qualified Certificates issued by «DIGITEL TS QUALIFIED CA G1»

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by «DIGITEL TS QUALIFIED CA G1»*

Name *[es]* *Certificados Cualificados emitidos por «DIGITEL TS QUALIFIED CA G1»*

Authority Key Identifier *39:95:88:B5:46:90:7A:C4:6D:C0:24:23:27:87:5C:7E:0D:7E:43:8B*

Authority Info Access *http://pki.digitalts.es/DTSROOTCA01.crt*
http://ocsp.pki.digitalts.es

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://pki.digitalts.es/dpc/

CRL Distribution Points *http://crl1.pki.digitalts.es/DTSROOTCA01.crl*
http://crl2.pki.digitalts.es/DTSROOTCA01.crl

Subject Key Identifier *45:7C:7F:95:2C:02:9E:BC:22:16:49:90:5A:B5:0C:3D:D6:73:C9:62*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *86:A6:2F:63:DC:AB:EC:9F:3D:50:BE:B1:85:F4:3B:A0:F4:42:53:D6:7C:D2:3B:6C:79:59:11:7A:C5:50:BA:61*

X509SubjectName

Subject C: *ES*

Subject L: *Valladolid*

Subject O: *DIGITEL ON TRUSTED SERVICES SLU*

Subject OU: *DIGITEL TS CERTIFICATION AUTHORITY*

Subject SERIAL NUMBER: *B47447560*

Subject CN: *DIGITEL TS QUALIFIED CA G1*

X509SKI

X509 SK I *RXx/ISwCnrwiFkmQWrUMPdZzyWI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-03-27T00:00:00Z*

35.11.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

35.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

35.11.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.54225.10.3.15>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.54225.10.3.25>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.54225.10.3.35>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.54225.10.3.5>

Description

Policy Identifier:

Identifier [OIDASURN] <urn:oid:1.3.6.1.4.1.54225.10.2.5>

Description

Description

Service type description	[en]	An electronic delivery service providing qualified electronic deliveries.
	[es]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Name	[en]	Qualified electronic registered delivery service by "DIGITELTS eDelivery Services"
Name	[es]	Servicio cualificado de entrega electrónica certificada "DIGITELTS eDelivery Services"

Certificate fields details

Version: 3

Serial Number: 83608658038724291022118255919206620959392352873

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer ST: *BARCELONA*

Issuer L: *HOSPITALET DE LLOBREGAT*

Issuer O: VINTEGRIS SLU

Issuer 2.5.4.97: *VATES-B62913926*

Issuer CN: CA Vintegris TrustServices

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SL*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel QTSP Signature Services*

Subject CN: *DIGITELTS eDelivery Services*

Valid from: *Wed May 29 18:55:08 CEST 2024*

Valid to: *Fri May 29 18:55:07 CEST 2026*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:5B:00:EE:11:7A:04:80:40:E6:83:37:83:56:ED:42:89:2E:91:2B:EA:F0:40:06:C6:08:FE:E6:8F:15:C8:C6:02:47:85:70:1A:1E:EC:6F:B4:FA:E9:0C:DA:20:F1:15:01:F8:32:2A:BC:A1:EF:2A:FD:A8:B1:C0:29:FA:D3:E5:68:F3:44:B9:2A:12:3C:D8:90:78:0E:92:C5:80:B D:01:C5:6C:34:3D:31:80:F2:86:36:7F:44:51:58:B7:52:D5:77:67:85:2F:D2:EE:AB:AF:88:0E:6C:3A:B6:5B:18:0D:9C:E2:AB:37:28:8B:A6:E6:C4:F9:AD:15:1F:CE:FE:29:91:84:36:09:36:DF: AB:E4:DA:A4:35:28:CB:7C:47:AC:26:C0:42:04:6C:36:3E:F2:95:4D:D6:B1:C2:EF:08:C0:93:DA:72:45:F2:D7:FC:20:2F:8D:66:96:F9:68:30:55:A5:A0:2D:55:0F:69:95:8B:2F:0D:5A:2A:2A:7 0:FF:CF:69:0C:10:8A:8F:53:CD:2F:39:A8:E2:82:F8:29:A9:8F:06:5E:D2:C0:3C:45:D5:53:C3:B7:F3:7C:4A:DA:2C:CD:7F:77:7F:09:F2:4D:1F:A8:E8:33:01:FA:46:10:99:E5:6D:37:73:5F:67: A7:21:80:FC:E7:A4:F8:FE:F1:C8:C3:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*

Authority Info Access *http://www.vincasign.net/publickeys/catrustservices.crt*
http://ocsp.vincasign.net

Subject Alternative Name *pkc@digitelts.com*
OID.1.3.6.1.4.1.47155.1.6=DIGITEL ON TRUSTED SERVICES SL,
OID.1.3.6.1.4.1.47155.1.7=VATES-B47447560

Certificate Policies *Policy OID: 1.3.6.1.4.1.47155.2.6.2*
CPS pointer: https://policy.vincasign.net
CPS text: [Certificado cualificado de sello electrónico de persona jurídica emitido en software. Ver https://policy.vincasign.net]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl1.vincasign.net/catrustservices.crl*
http://crl2.vincasign.net/catrustservices.crl

Subject Key Identifier *60:91:86:2B:65:5A:53:E8:71:20:6C:10:B0:EE:6D:BD:CB:6C:75:17*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C4:9C:A5:89:9C:4D:7B:62:E6:D3:DC:03:47:5F:CD:DB:C9:0F:BF:19:5B:51:66:BE:07:6A:79:CB:B0:FB:C3:FD*

X509SubjectName

Subject C: *ES*

Subject O: *DIGITEL ON TRUSTED SERVICES SL*

Subject 2.5.4.97: *VATES-B47447560*

Subject OU: *Digitel QTSP Signature Services*

Subject CN: *DIGITELTS eDelivery Services*

X509SKI

X509 SK I *YJGGK2VaU+hxIGwQsO5tvctsdRc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-03-27T00:00:00Z*

36 - TSP: VIAFIRMA, S.L.

TSP Name

Name [es] VIAFIRMA, S.L.

Name [en] VIAFIRMA, S.L.

TSP Trade Name

Name [en] VIAFIRMA

Name [en] VATES-B91052142

Name [en] VIAFIRMA SOCIEDAD LIMITADA

PostalAddress

Street Address [en] Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.

Locality [en] Tomares

State Or Province [en] Sevilla

Postal Code [en] 41940

Country Name [en] ES

PostalAddress

Street Address [es] Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.

Locality [es] Tomares

State Or Province [es] Sevilla

Postal Code [es] 41940

Country Name [es] ES

ElectronicAddress

URI [en] mailto:psc@viafirma.com

URI [en] https://qtsp.viafirma.com

TSP Information URI

URI [en] https://qtsp.viafirma.com

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name [es] Sellos de tiempo cualificados emitidos por VIAFIRMATSA

Name	[en]	Qualified timestamps issued by VIAFIRMATSA

Service digital identities

Certificate fields details

Version: 3

Serial Number: 327191426851532438764718424645512795330867118978

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: VIAFIRMA TSA SUB CA

Issuer SERIAL NUMBER: *VATES-B91052142*

Issuer OU: VIAFIRMA QTSP

Issuer O: *VIAFIRMA SOCIEDAD LIMITADA*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B91052142*

Subject CN: VIAFIRMA TSA

Subject OU: *VIAFIRMA QTSP*

Subject O: *VIAFIRMA SOCIEDAD LIMITADA*
Subject C: *ES*
Valid from: *Thu Oct 17 14:35:39 CEST 2019*
Valid to: *Thu Oct 17 14:35:39 CEST 2024*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:61:7F:AD:75:24:34:55:0F:BB:40:E4:67:CF:33:3A:8E:C1:F6:33:F6:E3:5A:88:45:D3:25:E8:03:34:14:91:DC:52:5D:09:86:3E:40:AC:13:3A:AC:EB:F4:93:A5:04:0E:1E:29:A4:15:C3:70:BF:E4:8A:37:1A:04:BF:8A:48:0E:5E:02:23:94:D3:DA:81:E2:57:7C:B1:03:05:03:02:0A:AE:BD:F0:10:ED:41:24:E6:3D:2E:AC:C2:E8:DF:64:39:76:B5:0E:D4:5A:96:74:88:D3:4D:FE:C3:AD:1F:42:2B:AA:BF:A0:83:63:B1:37:00:33:19:86:F3:F5:CF:03:99:53:8D:76:3F:64:E9:51:FS:EE:7E:5E:12:03:47:F9:6A:25:26:EC:43:7D:5F:BB:DC:3C:3A:80:B4:09:01:EF:39:5B:0A:FC:49:E5:7B:89:5A:D4:93:D3:03:BC:2E:6E:CF:09:98:83:4F:21:91:2F:CE:4F:F3:41:95:AD:77:8E:B3:E6:D9:01:80:2D:8B:8B:80:EB:9E:C6:64:1D:77:8F:16:68:06:CF:D5:EF:EB:24:6A:E2:21:E7:D1:75:B6:FF:92:9E:3F:BA:99:A9:54:D4:BF:70:1D:6A:DE:CE:A6:96:61:2C:CD:ED:62:5F:75:89:E5:FE:B5:32:BA:0D:EA:23:02:03:01:00:01*
Authority Info Access *http://qtsp.viafirma.com/tsp/subca.crt*
http://qtsp.viafirma.com/ocsp
Subject Key Identifier *4A:55:48:CA:14:B0:D4:A4:39:84:6F:D3:AA:6B:C6:45:B1:ED:1F:C0*
Basic Constraints *IsCA: false*
Authority Key Identifier *4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26*
Certificate Policies *Policy OID: 1.3.6.1.4.1.34253.7.3*
CPS pointer: http://qtsp.viafirma.com/cps
CRL Distribution Points *http://qtsp.viafirma.com/tsp/tsa_subca.crl*
http://qtsp1.viafirma.com/tsp/tsa_subca.crl
Extended Key Usage *id_kp_timeStamping*
Key Usage: *digitalSignature - nonRepudiation*
Thumbprint algorithm: *SHA-256*
Thumbprint: *84:7E:85:86:E8:42:BD:34:C7:F5:30:8B:9C:28:73:E5:45:BE:79:CA:80:53:7F:E7:BC:6A:2C:A5:C8:26:B0:26*

X509SubjectName

Subject 2.5.4.97: *VATES-B91052142*
Subject CN: *VIAFIRMA TSA*
Subject OU: *VIAFIRMA QTSP*
Subject O: *VIAFIRMA SOCIEDAD LIMITADA*
Subject C: *ES*

X509SKI

X509 SK I *SIVlyhSw1KQ5hG/TqmvGRbHtH8A=*

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>	
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time	<i>2025-03-13T00:00:00Z</i>	

36.1.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name	<i>[es]</i>	<i>Sellos de tiempo cualificados emitidos por VIAFIRMATSA</i>
Name	<i>[en]</i>	<i>Qualified timestamps issued by VIAFIRMATSA</i>

Service digital identities

X509SubjectName

Subject 2.5.4.97:	<i>VATES-B91052142</i>
Subject CN:	<i>VIAFIRMA TSA</i>
Subject OU:	<i>VIAFIRMA QTSP</i>
Subject O:	<i>VIAFIRMA SOCIEDAD LIMITADA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>SIVlyhSw1KQ5hG/TqmvGRbHtH8A=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time	<i>2020-04-28T00:00:00Z</i>

36.2 - Service (granted): Qualified timestamps issued by VIAFIRMA TSA 2022

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name	<i>[en]</i>	<i>Qualified timestamps issued by VIAFIRMA TSA 2022</i>

Authority Info Access	<i>http://qtsp.viafirma.com/tsp/subca.crt</i> <i>http://qtsp.viafirma.com/ocsp</i>
Subject Key Identifier	<i>F8:1E:F7:90:D9:C2:FE:2C:A7:3E:DC:82:55:0F:49:D4:E2:CD:D1:CD</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.34253.7.3</i> <i>CPS pointer: http://qtsp.viafirma.com/cps</i>
CRL Distribution Points	<i>http://qtsp.viafirma.com/tsp/tsa_subca.crl</i> <i>http://qtsp1.viafirma.com/tsp/tsa_subca.crl</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
Key Usage:	<i>digitalSignature - nonRepudiation</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>24:9D:7B:F9:C1:6E:BC:DA:81:45:FC:88:5A:15:04:D1:56:F0:A1:88:A2:78:F8:F6:D5:73:D2:CD:71:6D:AF:07</i>

X509SubjectName

Subject 2.5.4.97:	<i>VATES-B91052142</i>
Subject CN:	<i>VIAFIRMA TSA</i>
Subject OU:	<i>VIAFIRMA QTSP</i>
Subject O:	<i>VIAFIRMA SOCIEDAD LIMITADA</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>+B73kNnC/iynPtyCVQ9J1OLN0c0=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2022-12-15T00:00:00Z</i>

36.3 - Service (granted): Sellos de tiempo cualificados emitidos por VIAFIRMA TSA 003

Service Type Identifier

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[es]	Sellos de tiempo cualificados emitidos por VIAFIRMA TSA 003
Name	[en]	Qualified timestamps issued by VIAFIRMA TSA 003

Service digital identities

Certificate fields details

Version:	3
Serial Number:	502935155163419937520047732467136041576549946305

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHXTCBjWqAwIBAgIUWbhkcE+zHpdG4CEZ0qOKZNDdk8EwDOYIKoZihvcNAOELBOAwYIxGzAJBgNVBAYTAkVTMSMwIQYDVQOQDBpWSUFGSVjNQSBTTONIRURBRCBMSUJVEFEQTEWMBQGA1UECwwN
VklBRkISTUEgUVRtUjUeYmYGA1UEBRMPVtFURVMTQjxMDUyMTQyMRwwGgYDVQODDBNWSUFGSVjN
OSBUUeGU1VCIENBMB4ODTzMDIwNDASNDcwNfowFEELNAKGA1UEBhMC
RVXmZaZnBzNVBAoMGIZjOUZjUk1BIFNPOQFREFEExJTUIUOURBMRYwFAYDVOQLDA1WSUFGSVjN
OSBRVFNQMRkwFwYDVQDDDBBWSUFGSVjNQSBUUEGMDA2MRgwFgYDVQRhDA9WQVRFluY1COTewNTX
NDIwregIMAOCSqSb3DQEBAQUAA4ICDWAwagKaoCAQICPhwwLTybiLCDOly4Se700briD
vhuoRW6ad/swH1lgX4kn6IT5B6W/E3hgHujWT774IWigYXagV+5XXRnxflkWCdj6fEDTxoIxA
d/hN5TeyTvpDWWbsfj9luOK+opAxtT/HRIwaaOueq6N25COqf1u1Q7L6h019eD+xp/YmFhxH7v
dscKigvovBns2B03L1LXF69225WwKcTlmpP5Hj0ba8mLy0ip8RAOJA1BDeZ8g5uMTwZPzrC
nQNKmIK8rgD8TzV3icm85Q9hh95KhscvUkoXvjOC2qvbftpio4GmDINlrz8DisZpuWjZ4B2
sIzXDD3cp8GduA0OpwsmfRMRvtj583LBP7LrgpVb5oNVNlU9v902cw7IDu64dEnseqVqr0BZ
OVRkuGa6j9x36ioXlWwKAdnFEU05a37YMasYRvHFZ3+YoaKl7j1+n102o6NB0ul6cp2SYwt
CqKHhHAM6dQdbOIBWFnMkM7wruTATxVbILuK8xBeUYVpkxY5DM5q2x3Q1NWKzTDVWw/INF
0r5FakXOMUWDPm1Ma/mrN6uwgTLZojw90jybOcxWKO6UvtpLleAhwdug8frNBW753hgLdsL/aU
86dUe+dysE4Ytr3XCaA8nv6TrecGLPSTaesj0055i8kuACODIAQABo4IBzCCAccw0YKwYBBQUH
AOEETBMDIGCCSGAOUFBZACHizodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwHwYDVROB8wFwALU5qCB8hDnwL1ASC4
j/CtYMy+viYkwYDVR0QBQCBwloAPMjAyMzYzMDUwOTQ3MDRagQ8yMDI2MDIwMzA5NDcwNfowQwYD
VR0gBdwwOJA4BgorBgEAYKLTQCDMcowKAYIKwYBBQUHAgEWHGhodHhA6Ly9kdHnwLnZpYWZpcmlh
LnwvBz9icHwbgYDVROBgcwZTAwCgglYgAHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3RzcC90
C2Ffc3VY2Euy3jsMDGgl6AthitodHRwOi8vcXRzcC52aWFnmaxJTY55jb20vdHnwL3N1YmNhLmNy
dDAPBgggBgEFBQcwAYYdaHR0cDovL3R0c3AudmlhZmlybWUy29tL29jc3AwHQYDVROOB8YEFD3p
RjlpudGQY1YU9BdUgtrPCMAAGAU1UEuE8wQCMAAwH

Valid from: *Fri Feb 03 10:47:04 CET 2023*

Valid to: *Fri Feb 04 10:47:04 CET 2028*

Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A5:70:F1:EF:C2:D8:8B:4F:28:FA:20:B7:03:D2:5C:B8:E5:EE:F4:0D:B9:C3:BE:1B:8E:7D:6E:9A:77:F8:30:1F:59:60:5F:89:27:E8:84:F9:07:A5:8F:13:78:6A:1E:E8:D6:4F:BE:F8:21:68:86:C9:85:DA:81:5F:B9:5D:74:67:C4:59:64:58:27:62:8F:A7:C4:75:3C:68:FE:5C:40:77:F8:4D:E5:37:B2:4D:5A:43:59:56:EC:16:58:FD:22:ED:0A:FA:8A:40:CS:34:FF:1D:19:70:69:A3:AE:12:AE:8D:DB:90:8E:A8:5D:6E:D5:0E:CB:EA:1D:35:F5:E0:FE:C4:8A:7F:62:61:61:C4:7E:FF:76:C7:0A:22:0B:E8:57:C9:EC:67:C0:F7:33:5A:57:17:AF:67:D9:9E:56:C2:40:BB:96:79:8F:E4:78:D0:6F:10:66:2E:DC:B4:8A:9F:11:01:08:C0:96:D0:43:B0:4C:FC:83:9B:CC:EF:06:4F:87:37:C2:9D:03:4A:98:82:8C:AE:00:FC:4D:98:95:DE:27:3F:9B:C4:90:88:D8:61:F5:22:A1:B1:CB:D4:92:85:EF:8C:E0:B6:AA:F6:DF:22:D8:E9:8A:BE:06:98:32:0D:96:BC:FC:0C:8B:19:A6:E5:A3:67:80:76:80:86:57:0C:3D:DC:A7:C1:83:88:0D:10:A7:0B:26:16:D4:4C:46:D5:6D:8F:9F:37:2D:FF:0F:EC:BA:E0:A5:56:F9:A0:D5:4D:89:4F:6F:F7:4D:9C:C3:B9:43:BB:AE:1D:12:74:9E:A9:F5:6A:AF:40:59:41:54:64:88:66:BA:27:DC:77:EA:2A:57:37:0C:24:01:D9:DF:11:55:34:E5:AD:FF:4F:23:00:B1:84:71:1C:5D:B7:F9:8B:68:69:19:78:8E:AD:7E:9C:8D:36:A3:A3:41:0E:E2:3A:72:A3:09:49:8C:2D:0A:A2:87:1E:11:C0:33:A7:50:19:06:D0:94:1C:05:9C:C9:0C:EF:0A:EE:7C:04:F1:55:89:4B:68:AF:31:05:E5:18:95:5A:64:C5:8E:68:0C:C4:AA:FF:9C:77:8D:0D:4D:5A:4C:D3:0D:57:F0:FE:23:45:D2:B4:85:6A:48:D7:D0:C5:16:0C:F9:B5:88:C6:BF:9E:B3:7A:BB:0B:13:2D:9A:09:C3:0D:09:C9:B3:8E:C5:62:8E:E9:45:6D:A4:88:9E:02:1C:34:BA:0F:1F:AC:D6:D6:EE:CD:E1:A8:B7:6C:2F:F6:94:F1:D7:54:68:E7:72:80:4E:18:AE:BD:D7:39:A0:01:9F:1E:93:AD:E1:88:3D:2E:DA:7A:C2:74:D3:94:A2:F2:4B:80:09:02:03:01:00:01*

Authority Info Access *http://qtsp.viafirma.com/tsp/subca.crt*

http://qtsp.viafirma.com/ocsp

Subject Key Identifier *3D:E9:46:3F:C9:A6:E6:C6:5D:0A:F5:95:85:3D:11:D5:2A:7F:13:C2*

Basic Constraints *IsCA: false*

Authority Key Identifier *4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26*

Certificate Policies *Policy OID: 1.3.6.1.4.1.34253.7.3*
CPS pointer: http://qtsp.viafirma.com/cps

CRL Distribution Points *http://qtsp.viafirma.com/tsp/tsa_subca.crl*
http://qtsp1.viafirma.com/tsp/tsa_subca.crl

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1A:2B:FC:30:34:EE:CF:4C:E1:71:DF:3A:D6:A1:5C:D4:49:2D:51:EB:31:40:DF:51:9E:38:5C:18:DB:D0:7F:55*

X509SubjectName

Subject 2.5.4.97: *VATES-B91052142*

Subject CN: *VIAFIRMA TSA 003*

Subject OU: *VIAFIRMA QTSP*

Subject O: *VIAFIRMA SOCIEDAD LIMITADA*

Subject C: *ES*

X509SKI

X509 SK I *PeIGP8mm5sZdCvWVhT0R1Sp/E8I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

Status Starting Time *2023-03-28T00:00:00Z*

36.4 - Service (granted): Sellos de tiempo cualificados emitidos por VIAFIRMA TSA 006

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por VIAFIRMA TSA 006*

Name	[en]	Qualified timestamps issued by VIAFIRMA TSA 006

Service digital identities

Certificate fields details

Version: 3

Serial Number: 282842426295646064374375014546969808197038752310

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer CN: VIAFIRMA TSA SUB CA

Issuer SERIAL NUMBER: *VATES-B91052142*

Issuer OU: VIAFIRMA QTSP

Issuer O: *VIAFIRMA SOCIEDAD LIMITADA*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B91052142*

Subject CN: *VIAFIRMA TSA 006*
Subject OU: *VIAFIRMA QTSP*
Subject O: *VIAFIRMA SOCIEDAD LIMITADA*
Subject C: *ES*
Valid from: *Wed Oct 15 12:49:17 CEST 2025*
Valid to: *Wed Oct 16 12:49:17 CEST 2030*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:81:B1:EC:F9:29:A3:6E:18:DF:BD:C2:59:49:9D:28:0C:47:07:15:8E:BD:EC:13:68:23:4B:77:E7:23:E7:AF:46:25:67:E4:9C:DE:FC:C9:F0:68:F1:E7:7F:FF:44:00:69:4C:94:58:14:13:8A:62:69:9C:FA:E5:21:6F:08:7D:05:18:71:55:D0:78:8D:B3:C0:CE:85:43:F2:96:EE:59:97:AB:84:0E:50:59:28:29:71:41:49:04:5B:AD:87:08:93:76:15:79:D6:2E:F3:06:87:EB:57:18:F6:06:D9:41:5A:87:5B:68:73:38:BD:F9:08:BB:AE:CC:E8:28:0A:87:1D:30:29:50:96:E1:AE:D0:83:0E:48:99:ED:0E:FB:AC:25:86:02:63:0E:80:AE:28:6A:0E:EC:D3:78:01:1C:E9:3D:3D:4F:99:DE:92:BB:A1:3E:B2:E7:8A:8C:78:74:08:5F:4D:E0:65:F5:8D:BB:EF:6C:AE:E9:7A:91:5B:8A:55:C5:98:46:B6:83:60:1A:84:1E:9A:74:24:B3:05:B6:91:D6:D9:A6:B8:E9:19:FE:37:84:0A:75:D8:16:BE:F2:01:67:1E:F4:88:C0:61:EB:2E:AD:62:0A:C5:EC:8E:7A:49:FA:D0:CA:90:B2:C9:D5:2F:CL:6D:34:76:7C:BF:12:8D:5E:56:8F:DA:B5:DF:38:66:D8:6E:D0:B3:FC:85:2D:13:25:22:E4:7C:E1:15:4C:62:4B:70:AD:0B:54:53:66:8C:74:7A:00:84:74:F2:B6:34:BD:2C:FB:AB:20:2C:1F:10:6D:98:67:24:72:D0:11:AE:31:8C:D1:36:6E:F2:47:34:34:73:F1:28:6A:2F:4A:D6:B6:EF:73:64:2E:78:14:79:34:E5:AF:34:AB:54:70:FB:8F:95:BA:2A:32:4E:4D:F8:0E:39:1F:3E:8F:73:19:87:EE:70:18:04:68:AD:51:D0:87:48:97:D3:F5:EF:93:FC:99:01:E0:6B:1E:25:F8:21:74:2E:94:E6:6D:0F:42:56:ED:A5:B2:98:D6:AB:17:82:5C:4B:28:67:8C:84:3D:20:B9:82:13:08:06:53:AI:20:5B:2B:AD:65:39:08:84:AF:1A:F8:05:62:8E:F8:68:CF:5A:EA:8F:83:2A:18:75:BB:74:76:58:93:E9:CF:96:E0:92:43:F5:C7:F5:C5:F9:76:11:2A:4F:1C:80:23:6C:07:4B:0A:6D:0D:AF:06:C1:92:E1:42:C0:AE:E2:0E:1F:F3:71:BB:F0:A8:43:11:68:77:78:E9:02:83:F8:F0:D7:A8:9F:D1:A7:C6:B0:DC:F2:27:05:19:BB:0F:C2:5E:B5:1D:E3:02:03:01:00:01*
Authority Info Access *http://qtsp.viafirma.com/tsp/subca.crt*
http://qtsp.viafirma.com/ocsp
Subject Key Identifier *57:87:1C:6F:17:CA:F2:A9:2A:14:A6:58:CE:C9:F8:07:AC:7E:FA:26*
Basic Constraints *IsCA: false*
Authority Key Identifier *4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26*
Certificate Policies *Policy OID: 1.3.6.1.4.1.34253.7.3*
CPS pointer: http://qtsp.viafirma.com/cps
CRL Distribution Points *http://qtsp.viafirma.com/tsp/tsa_subca.crl*
http://qtsp1.viafirma.com/tsp/tsa_subca.crl
Extended Key Usage *id_kp_timeStamping*
Key Usage: *digitalSignature - nonRepudiation*
Thumbprint algorithm: *SHA-256*
Thumbprint: *72:1E:1F:16:05:54:18:74:2A:19:34:13:02:57:CF:DE:86:BA:AB:0D:56:46:59:CC:19:B6:AB:B6:69:EE:12:93*

X509SubjectName

Subject 2.5.4.97: *VATES-B91052142*
Subject CN: *VIAFIRMA TSA 006*
Subject OU: *VIAFIRMA QTSP*
Subject O: *VIAFIRMA SOCIEDAD LIMITADA*

Subject C:		<i>ES</i>
X509SKI		
X509 SK I		<i>V4ccbxfK8qkqFKZYzsn4B6x++iY=</i>
Service Status		<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time		<i>2026-01-29T01:00:00Z</i>

37 - TSP: VALIDATED ID, S.L

TSP Name

Name *[es]* *VALIDATED ID, S.L*

Name *[en]* *VALIDATED ID, S.L*

TSP Trade Name

Name *[en]* *VALIDATED ID SL*

Name *[en]* *VATES-B65750721*

Name *[en]* *Validated ID SL*

PostalAddress

Street Address *[en]* *C/ Ávila, 29*

Locality *[en]* *BARCELONA*

State Or Province *[en]* *BARCELONA*

Postal Code *[en]* *08005*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *C/ Ávila, 29*

Locality *[es]* *BARCELONA*

State Or Province *[es]* *BARCELONA*

Postal Code *[es]* *08005*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:tsp@validatedid.com*

URI *[en]* *https://validatedid.com*

TSP Information URI

URI *[en]* *validatedid.com*

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name [es] Sellos de tiempo cualificados emitidos por VALIDATED ID

Name	[en]	Qualified timestamps issued by VALIDATED ID

Service digital identities

Certificate fields details

Version: 3

Serial Number: 7427016217577742020

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA2 2016

Issuer OU: TSP-UANATACA

Issuer O: UANATACA S.A.

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B65750721*

Subject CN: *VALIDATED ID QUALIFIED TSU01*

Subject OU: *VALIDATED ID TSP*

Subject O: *VALIDATED ID SL*

Subject L: *BARCELONA*

Subject C: *ES*

Valid from: *Tue Nov 26 18:45:11 CET 2019*

Valid to: *Fri Nov 26 18:45:11 CET 2027*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CA:F1:D8:EA:3C:95:70:23:8D:8D:19:AE:2F:1D:2A:E9:35:E4:46:AD:AD:A4:62:5E:38:2E:D6:F4:05:68:74:23:06:87:D1:13:0A:B3:D4:C9:05:30:96:27:D5:B1:75:9E:04:E7:60:D2:F9:22:DA:BF:B1:D3:5D:84:32:6D:6D:1E:2B:84:AE:6B:49:6D:CD:29:43:2A:D6:B7:BA:B6:AC:46:FF:91:6D:03:AB:14:EF:FC:C1:E0:99:3D:1A:26:27:B9:A0:2F:7D:5E:2B:15:5B:19:03:F1:D5:B3:9C:42:26:64:27:71:25:12:02:ED:DF:B5:34:7A:CF:00:45:5E:95:2B:AD:E3:15:68:A3:85:F5:C4:48:EF:99:A0:78:2B:26:B4:E8:9F:AF:A7:BC:89:47:58:38:5F:E3:55:C4:00:9E:23:C2:DC:89:1C:69:A3:D4:C0:16:2A:82:EF:A5:E7:BE:AF:94:46:95:34:76:5E:7A:8E:D3:29:BD:43:6C:34:CC:36:F3:A8:AB:F9:ED:95:C0:02:54:68:FA:A4:C3:56:A3:21:CF:F0:A7:DF:F8:BD:FC:7A:A7:77:CD:05:31:70:C1:5D:CF:5F:7D:EB:DC:52:53:15:84:B2:AB:8B:17:E4:2C:FD:99:01:49:CD:9D:30:DE:85:F6:F9:12:1D:72:D9:4B:18:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *E8:51:4E:DD:BC:CC:78:9C:11:37:26:F3:CA:D8:98:E1:B8:58:9E:97*

Basic Constraints *isCA: false*

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *tsp@validatedid.net*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E3:00:17:A1:84:38:64:F7:C5:AE:60:4C:E2:12:61:39:C2:11:B4:D2:FE:F8:3E:F1:3E:DE:8F:72:57:B6:57:B3*

X509SubjectName

Subject 2.5.4.97: *VATES-B65750721*

Subject CN: *VALIDATED ID QUALIFIED TSU01*

Subject OU: *VALIDATED ID TSP*

Subject O: *VALIDATED ID SL*

Subject L: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *6FFO3bzMeJwRNybytiY4bhYnpc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2026-02-19T03:00:00Z*

37.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por VALIDATED ID*

Name [en] *Qualified timestamps issued by VALIDATED ID*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B65750721*

Subject CN: *VALIDATED ID QUALIFIED TSU01*

Subject OU: *VALIDATED ID TSP*

Subject O: *VALIDATED ID SL*

Subject L: *BARCELONA*

Subject C: *ES*

X509SKI

X509 SK I *6FFO3bzMeJwRNybytiY4bhYnpc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

37.2 - Service (granted): Qualified Certificates issued by Validated ID Subordinate CA 01

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by Validated ID Subordinate CA 01

Name	[es]	Certificados Cualificados emitidos por Validated ID Subordinate CA 01

Service digital identities

Certificate fields details

Version: 3

Serial Number: 2673564476656545333

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Barcelona*

Issuer O: *Validated ID SL*

Issuer 2.5.4.97: *VATES-B65750721*

Issuer OU: *TSP - Validated ID*

Issuer CN: *Validated ID Root CA*

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *Validated ID SL*

Subject OU: *TSP - Validated ID*

Subject CN: *Validated ID Subordinate CA 01*

Subject 2.5.4.97: *VATES-B65750721*

Valid from: *Thu Oct 21 14:10:03 CEST 2021*

Valid to: *Sat Oct 21 14:10:03 CEST 2034*

Public Key:

30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:A4:33:94:38:57:A4:19:92:73:B1:CB:DC:72:80:99:CE:A1:8E:45:7D:F2:04:
28:53:88:3A:0F:F1:9E:D1:DA:82:35:AE:64:7B:10:8B:A7:4B:06:AC:62:AD:70:F0:98:01:D1:1B:08:81:C0:3E:6E:D9:A8:8A:F2:99:15:7C:79:D8:B3:7A:D4:AC:DA:18:CD:95:9C:74:64:B1:92:
A2:89:8D:22:3F:F1:09:8A:15:FC:B9:C5:DE:17:71:52:79:34:67:61:DB:D9:98:CB:93:08:C8:52:F3:DD:28:97:DA:A3:2D:3E:E9:67:C0:C9:93:ED:40:7F:EC:84:5A:55:06:31:88:4F:22:C9:D0:7
0:40:FD:6D:45:E5:4A:F9:95:F9:45:A1:59:7A:7F:CC:7D:50:CA:5C:4F:79:89:9B:7F:91:4D:35:8D:09:2E:56:18:75:24:50:7E:E7:E6:D0:9E:4D:F2:82:15:C1:50:67:74:16:67:2C:B0:91:47:53:
9D:D1:89:2D:AB:15:0F:0F:00:51:85:78:87:CB:1E:CF:3F:8F:34:F3:6E:43:45:7A:CE:14:39:5D:00:00:3C:DF:A3:AF:51:F4:7A:8B:69:8D:56:F1:CB:99:49:85:F6:DA:07:7E:DA:CF:88:F1:31:3
1:42:47:1E:DF:AE:9C:43:D9:A9:67:2D:50:3D:54:7C:70:07:9E:32:89:64:E3:CF:29:00:24:50:F2:92:96:8A:C6:F2:58:C7:58:1B:41:39:C6:CF:47:37:16:A7:0C:B6:84:60:0F:7B:0C:71:6A:96:
89:2E:CF:8E:08:E8:13:93:E9:0B:07:80:AB:48:8A:BD:9A:DF:62:72:4D:A2:DB:FD:3B:B4:44:C8:0D:CB:46:F7:66:7B:C1:E7:F2:8D:DE:42:75:9E:0E:8C:1F:6E:7A:A3:47:EF:44:8E:58:16:46:F
EA2:16:8C:89:CD:12:65:23:52:DF:97:95:4A:1C:20:41:4A:F5:6C:2D:0B:35:23:3A:52:99:9D:7A:F8:41:FC:A2:AD:D5:42:EE:3F:AC:D1:32:96:8D:BF:FF:75:F8:AE:01:08:DD:C3:4F:2B:87:12
:A3:DD:5B:64:38:F9:0D:9C:F4:6E:62:68:68:53:05:22:BE:FF:94:E7:F5:0D:98:83:CF:D9:EA:96:9F:8E:82:8B:26:EE:69:8E:5B:60:47:D5:58:46:55:94:C9:01:E3:85:D8:29:71:F7:11:96:F0:C1
:5D:9A:08:C9:97:8B:26:2F:8E:C5:6D:8B:88:93:93:C8:61:A7:69:07:8D:37:76:C2:22:CE:A0:17:E1:51:4C:65:A0:8D:8B:29:2E:25:7D:7F:CA:E4:FE:2E:43:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *20:F9:B2:8C:7F:C7:4C:BF:01:26:DA:09:D3:77:54:B8:CC:7D:60:FA*

Issuer Alternative Name *tsp@validatedid.com*

Subject Alternative Name *tsp@validatedid.com*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <https://www.validatedid.com/tsp>
CPS text: [Validated ID Subordinate CA Certificate - <https://www.validatedid.com/>]

CRL Distribution Points *http://crl1.validatedid.com/tsp/crl/arl_validatedid.crl*
http://crl2.validatedid.com/tsp/crl/arl_validatedid.crl

Subject Key Identifier *26:4E:8E:6F:4A:52:54:00:83:28:70:CF:F1:88:B0:51:25:39:55:57*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A8:3D:44:88:25:5C:46:9F:66:26:E3:71:1C:69:22:9B:DC:8A:DA:56:7C:F2:9B:2E:A6:5F:AD:19:29:28:31:C2*

X509SubjectName

Subject C: *ES*

Subject L: *Barcelona*

Subject O: Validated ID SL

Subject OU: TSP - Validated ID

Subject CN: Validated ID Subordinate CA 01

Subject 2.5.4.97: VATES-B65750721

X509SKI

X509 SKI Jk6Ob0pSVACDKHDP8YiwUSU5VVc=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2022-05-31T00:00:00Z

37.2.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

37.2.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

37.2.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.54932.2.1.3

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.54932.2.2.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.54932.2.3.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.54932.2.4.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.54932.2.5.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.54932.2.6.3
Policy Identifier:		
Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.54932.2.8.3

37.3 - Service (withdrawn): Qualified timestamps issued by Validated ID Qualified TSU02

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST	
Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.
Service Name		
Name	[en]	Qualified timestamps issued by Validated ID Qualified TSU02
Name	[es]	Sellos de tiempo cualificados emitidos por Validated ID Qualified TSU02

Service digital identities

Certificate fields details

Version:	3
Serial Number:	5083852779122873729

Authority Info Access	<i>https://www.validatedid.com/tsp/tsp_certificates/validatedid_ca.crt</i> <i>http://ocsp1.validatedid.com/tsp/ocsp/</i> <i>http://ocsp2.validatedid.com/tsp/ocsp/</i>
Subject Key Identifier	<i>59:D3:96:B6:97:10:95:1C:40:4A:F3:26:F1:C1:11:C8:F2:CA:1F:C6</i>
Basic Constraints	<i>IsCA: false</i>
Authority Key Identifier	<i>26:4E:8E:6F:4A:52:54:00:83:28:70:CF:F1:88:B0:51:25:39:55:57</i>
Issuer Alternative Name	<i>tsp@validatedid.com</i>
Certificate Policies	<i>Policy OID: 0.4.0.194112.1.3</i> <i>Policy OID: 1.3.6.1.4.1.54932.3.10</i> <i>CPS pointer: https://www.validatedid.com/tsp</i> <i>CPS text: [Qualified time stamp certificate]</i>
CRL Distribution Points	<i>http://crl1.validatedid.com/tsp/crl/validatedid.crl</i> <i>http://crl2.validatedid.com/tsp/crl/validatedid.crl</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
Subject Alternative Name	<i>tsp@validatedid.com</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>E8:68:AE:7E:58:0C:5F:6A:C7:78:D9:FE:50:AC:5E:A7:AA:A1:93:B4:29:BC:46:67:44:73:2D:F7:6D:0D:00:B6</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Barcelona</i>
Subject O:	<i>Validated ID SL</i>
Subject OU:	<i>TSP - Validated ID</i>
Subject CN:	<i>Validated ID Qualified TSU02</i>
Subject 2.5.4.97:	<i>VATES-B65750721</i>

X509SKI

X509 SK I	<i>WdOWtpcQIRxASvMm8cERyPLKH8Y=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>	
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time	<i>2026-02-19T03:00:00Z</i>	

37.3.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name	<i>[en]</i>	<i>Qualified timestamps issued by Validated ID Qualified TSU02</i>
Name	<i>[es]</i>	<i>Sellos de tiempo cualificados emitidos por Validated ID Qualified TSU02</i>

Service digital identities

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>Barcelona</i>
Subject O:	<i>Validated ID SL</i>
Subject OU:	<i>TSP - Validated ID</i>
Subject CN:	<i>Validated ID Qualified TSU02</i>
Subject 2.5.4.97:	<i>VATES-B65750721</i>

X509SKI

X509 SK I	<i>WdOWtpcQIRxASvMm8cERyPLKH8Y=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>	
Status Starting Time	<i>2022-05-31T00:00:00Z</i>	

37.4 - Service (granted): Qualified electronic timestamps issued by Validated ID Qualified TSU 03

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Subject CN: *Validated ID Qualified TSU 03*

Valid from: *Wed Dec 10 11:45:19 CET 2025*

Valid to: *Tue Dec 10 11:45:19 CET 2030*

Public Key: *30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:C1:7F:96:58:E7:0E:A9:0A:9C:12:5A:FC:7C:3F:14:CF:0F:BA:AD:0B:70:A8:7F:82:90:50:A5:15:FC:1B:1D:1B:A9:C1:12:75:D9:A1:CE:A0:90:3B:C3:81:83:55:B9:FE:4B:57:41:C6:AA:F1:10:E5:14:67:72:38:9F:F9:FD:11:04:11:86:8A:AB:F3:13:DE:AD:90:38:45:50:B3:74:57:DE:66:01:38:1D:47:8A:BE:11:09:61:6A:C7:7E:6E:EB:7B:6A:FE:E1:42:FE:E7:FE:EE:56:8C:B3:2D:2A:EE:39:FA:F2:C7:7A:A1:DF:74:DF:87:67:43:81:CF:7B:76:19:30:E0:00:A5:BA:06:8B:59:F6:16:3A:0D:88:26:F8:FE:0D:2D:6B:68:64:93:36:96:E8:4C:0E:D9:BC:78:C7:DC:C3:87:0F:CA:6B:18:25:21:A4:64:F8:C4:6C:56:C7:51:89:54:61:0E:6E:9F:70:32:88:FC:1B:8B:13:AE:66:A7:BB:9B:80:14:C0:FD:4C:5A:7F:68:42:93:7A:F8:3E:15:00:9D:F7:FD:78:F7:CD:8E:08:4B:2A:4D:08:E9:97:EC:48:76:CB:93:AF:13:1A:6A:D5:18:C3:E8:87:1F:50:B5:AA:C0:80:C4:80:D3:CA:5A:94:F7:21:5B:24:1D:86:6B:CF:B3:8A:F2:5E:9A:E4:12:77:ED:84:5D:70:B2:02:52:49:36:71:D2:C5:A5:6A:4F:03:EF:5A:BE:70:D9:DF:DA:04:45:4A:1D:4F:98:47:90:BB:92:C4:81:38:B2:79:D1:E0:89:3E:35:5D:A3:8B:5E:8A:36:40:52:AF:90:D6:03:02:C3:AB:57:05:C0:AB:FB:C8:4D:88:CE:F6:55:1E:24:35:36:AC:44:00:22:00:75:22:2C:77:CD:F6:F2:EF:D7:18:24:EA:2F:28:12:3C:C1:0F:1E:77:20:AC:86:35:3B:F8:37:C4:62:D3:2B:03:9F:F9:27:6A:DD:47:FF:8D:02:03:01:00:01*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Basic Constraints *IsCA: false*

Authority Key Identifier *26:4E:8E:6F:4A:52:54:00:83:28:70:CF:F1:88:B0:51:25:39:55:57*

Authority Info Access *https://www.validatedid.com/tsp/tsp_certificates/validatedid_ca.crt*
http://ocsp1.validatedid.com/tsp/ocsp/
http://ocsp2.validatedid.com/tsp/ocsp/

Issuer Alternative Name *tsp@validatedid.com*

Subject Alternative Name *tsp@validatedid.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.54932.3.10*
CPS pointer: https://www.validatedid.com/tsp
CPS text: [Qualified time stamp certificate]

Policy OID: 0.4.0.194112.1.3

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl1.validatedid.com/tsp/crl/validatedid.crl*
http://crl2.validatedid.com/tsp/crl/validatedid.crl

Subject Key Identifier *A0:C7:48:25:A4:BD:E0:23:90:AD:26:99:77:9F:BF:1C:B5:B1:92:38*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EB:B9:CE:56:1D:0B:EE:9E:D9:5C:36:FF:1C:75:41:41:74:9B:C5:FE:5B:50:65:AD:84:F1:1F:75:AD:15:DF:8D*

X509SubjectName

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *Validated ID SL*

Subject 2.5.4.97: *VATES-B65750721*

Subject OU: *TSP - Validated ID*

Subject CN: *Validated ID Qualified TSU 03*

X509SKI

X509 SK I *oMdIJaS94COQrSaZd5+/HLWxkjg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2026-02-19T03:00:00Z*

38 - TSP: ENTRUST EU SL

TSP Name

Name	[en]	ENTRUST EU SL
Name	[es]	Entrust Datacard Europe S.L.U.

TSP Trade Name

Name	[en]	VATES-B81188047
Name	[en]	Entrust Datacard Europe S.L.
Name	[es]	Entrust Datacard Europe S.L.
Name	[en]	Entrust Datacard Europe, S.L.
Name	[es]	Entrust Datacard Europe S.L.U.
Name	[en]	Entrust Datacard Europe S.L.U.
Name	[en]	Entrust EU, S.L.
Name	[en]	Entrust EU

PostalAddress

Street Address	[en]	P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ
Locality	[en]	Pozuelo de Alarcón
State Or Province	[en]	Madrid
Postal Code	[en]	28233
Country Name	[en]	ES

PostalAddress

Street Address	[es]	P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ
Locality	[es]	Pozuelo de Alarcón
State Or Province	[es]	Madrid
Postal Code	[es]	28233
Country Name	[es]	ES

Issuer CN: *Entrust Root Certification Authority - G2*
Issuer OU: *(c) 2009 Entrust, Inc. - for authorized use only*
Issuer OU: *See www.entrust.net/legal-terms*
Issuer O: *Entrust, Inc.*
Issuer C: *US*
Subject C: *ES*
Subject O: *Entrust Datacard Europe S.L.*
Subject 2.5.4.97: *VATES-B81188047*
Subject CN: *Entrust Certification Authority - QTSP1*
Valid from: *Fri Jul 26 20:31:45 CEST 2019*
Valid to: *Tue Nov 26 20:01:45 CET 2030*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DC:EE:40:BE:EE:37:42:94:5E:37:1F:20:E0:21:5F:E9:26:80:55:5C:3E:00:52:8
EAC:E6:AC:4A:79:D8:72:DC:D4:A2:02:81:54:D0:80:94:32:0E:F7:4C:B7:4A:80:80:0A:AF:52:1C:8A:43:8E:49:85:12:12:16:EF:18:53:2B:9E:5D:F3:17:A1:A6:DF:F7:62:CA:1C:B7:C2:85:81:
32:E0:8C:60:7A:2D:48:E9:50:A9:32:FD:76:B9:D8:E9:10:33:ED:C7:77:8B:40:9A:D6:AE:75:95:2E:D9:78:D2:C1:9C:05:39:88:DF:80:26:4F:0F:B3:DE:88:AE:74:45:08:00:B2:34:49:B4:CB:2
1:C4:2F:DD:83:E9:A5:BE:F8:9A:8C:76:AC:57:F3:1A:1C:FE:9B:30:0A:C4:4F:5D:5B:39:E9:FC:BF:10:79:7D:58:42:D6:E2:77:9A:08:98:3C:21:16:59:EF:4B:92:80:BE:BC:72:11:7E:65:5A:5F:
31:F7:8D:53:E1:F4:98:85:5E:62:3F:5F:C5:63:DC:8B:63:40:5E:99:4F:F1:67:99:E2:4C:9B:62:6D:0B:DE:27:1F:6E:34:19:DE:6B:B8:F8:59:0B:00:99:A5:41:0C:ED:61:15:EE:E0:F4:A2:56:67:
DE:29:E5:DB:D6:FA:23:B2:B4:A5:02:03:01:00:01*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: <http://www.entrust.net/rpa>
Authority Info Access *<http://ocsp.entrust.net>*
CRL Distribution Points *<http://crl.entrust.net/g2ca.crl>*
Subject Key Identifier *1C:AD:3F:9C:D7:2D:22:19:A1:9C:4B:E9:DA:F1:2A:33:F7:FB:BA:0D*
Authority Key Identifier *6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *68:1E:BC:18:22:B0:79:B9:7E:04:04:E4:68:7D:9B:6C:0C:08:92:C8:20:F5:57:38:A2
:82:AA:E6:25:29:BD:D8*
X509SubjectName
Subject C: *ES*

Subject O: *Entrust Datacard Europe S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - QTSP1*

X509SKI

X509 SK I *HK0/nNctIhmhnEvp2vEqM/f7ug0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-10-30T02:00:00Z*

38.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

38.1.2 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://avance.digital.gob.es/en-us/Servicios/FirmaElectronica/Paginas/Informacion-cese-actividad-ENTRUST.aspx*

TSP Name

Name *[en]* *Sectigo (Europe) SL*

Name *[es]* *Sectigo (Europe) SL*

Scheme Operator Name

Name *[en]* *MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION*

Name *[es]* *MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION DIGITAL*

Scheme Territory *ES*

38.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Service Website authentication certificate issued by "Entrust Certification Authority - QTSP1"*

Name *[es]* *Servicio de emisión de certificados autenticación de sitios web por "Entrust Certification Authority - QTSP1"*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *Entrust Datacard Europe S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - QTSP1*

X509SKI

X509 SK I *HK0/nNctIhmhnEvp2vEqM/f7ug0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-07-28T00:00:00Z*

38.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

38.2 - Service (withdrawn): Qualified Certificates issued by "Entrust Certification Authority - ES QSig1"

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name *[en]* *Qualified Certificates issued by "Entrust Certification Authority - ES QSig1"*

Authority Key Identifier *63:F1:84:DD:03:BE:A3:9F:64:FA:76:7A:47:C4:56:7E:C0:6D:A0:20*

Authority Info Access *http://ocsp.entrust.net*

CRL Distribution Points *http://crl.entrust.net/aatl1ca.crl*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: http://www.entrust.net/rpa

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B2:87:4B:58:8A:94:03:47:98:31:9D:5D:32:9D:B2:65:F8:3A:47:F3:15:BA:58:31:A4:97:0C:B5:71:66:D5:94*

X509SubjectName

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSig1*

X509SKI

X509 SK I *WIMlimEwqQ3q1UOX05g7IR4ubQI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-10-30T02:00:00Z*

38.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

38.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *Qualified Certificates issued by “Entrust Certification Authority - ES QSig1”*

Name [es] *Certificados cualificados emitidos por “Entrust Certification Authority - ES QSig1”*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSig1*

X509SKI

X509 SK I *WIMlimEwqQ3q1UOX05g7IR4ubQI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-07-01T01:00:00Z*

38.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

38.3 - Service (withdrawn): Qualified Certificates issued by “Entrust Certification Authority - ES QSeal1”

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by “Entrust Certification Authority - ES QSeal1”*

Name [es] *Certificados cualificados emitidos por “Entrust Certification Authority - ES QSeal1”*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 26492164530593052518015735966780036267

X509 Certificate

[illegible]

Signature algorithm: *SHA512withRSA*

Issuer C: *US*

Issuer O: *Entrust, Inc.*

Issuer CN: *Entrust Certification Authority - AATL1*

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSeal1*

Valid from: Mon Jul 27 16:39:07 CEST 2020

Valid to: *Sun Dec 20 00:59:00 CET 2037*

[illegible]

Extended Key Usage *id_kp_emailProtection - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier 56:80:15:23:95:71:7F:E7:2D:90:D0:CD:06:3A:4F:67:63:7D:3D:75

Authority Key Identifier *63:F1:84:DD:03:BE:A3:9F:64:FA:76:7A:47:C4:56:7E:C0:6D:A0:20*

Authority Info Access <http://ocsp.entrust.net>

CRL Distribution Points *http://crl.entrust.net/aatl1ca.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: http://www.entrust.net/rpa

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *17:01:DE:38:12:4C:44:58:F3:2B:88:AE:7E:62:AC:15:87:6C:42:7A:3A:D3:BB:AE:8F:D1:47:9F:F0:00:30:F3*

X509SubjectName

Subject C: *ES*

Subject O: *Entrust Datacard Europe, S.L.*

Subject 2.5.4.97: *VATES-B81188047*

Subject CN: *Entrust Certification Authority - ES QSeal1*

X509SKI

X509 SK I *VoAVI5Vxf+ctkNDNBjpPZ2N9PXU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-10-30T02:00:00Z*

38.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

38.3.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en] Qualified Certificates issued by "Entrust Certification Authority - ES QSeal1"*

Name *[es] Certificados cualificados emitidos por "Entrust Certification Authority - ES QSeal1"*

Service digital identities**X509SubjectName**

Subject C: ES

Subject O: Entrust Datacard Europe, S.L.

Subject 2.5.4.97: VATES-B81188047

Subject CN: Entrust Certification Authority - ES QSeal1

X509SKI

X509 SK I VoAVI5Vxf+ctkNDNBjpPZ2N9PXU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-07-01T01:00:00Z

38.3.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

38.4 - Service (withdrawn): Qualified Certificates issued by "Entrust Certification Authority - ES QSig2"

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by "Entrust Certification Authority - ES QSig2"

Name [es] Certificados cualificados emitidos por "Entrust Certification Authority - ES QSig2"

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 84522751415613648666417138303639460125

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *46:71:FD:EA:D3:C5:B3:2D:83:4B:36:59:1D:41:49:6F:CB:8A:0D:B7:D4:F9:F4:CB:9D:34:EA:BE:09:47:EE:87*

X509SubjectName

Subject CN: *Entrust Certification Authority - ES QSig2*

Subject 2.5.4.97: *VATES-B81188047*

Subject O: *Entrust EU, S.L.*

Subject C: *ES*

X509SKI

X509 SK I *9VYNadfaasnYyalJbnS+24DGFwA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-10-30T02:00:00Z*

38.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

38.4.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description *[en] undefined.*

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDA sURN] urn:oid:2.16.840.1.114028.10.1.12.2*

38.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	[en]	Qualified Certificates issued by "Entrust Certification Authority - ES QSig2"
Name	[es]	Certificados cualificados emitidos por "Entrust Certification Authority - ES QSig2"

Service digital identities**X509SubjectName**

Subject CN:	Entrust Certification Authority - ES QSig2
Subject 2.5.4.97:	VATES-B81188047
Subject O:	Entrust EU, S.L.
Subject C:	ES

X509SKI

X509 SK I	9VYNadfaasnYyalJbnS+24DGFwA=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2022-07-21T00:00:00Z

38.4.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

38.4.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:2.16.840.1.114028.10.1.12.2

38.5 - Service (withdrawn): Qualified Certificates issued by "Entrust Certification Authority - ES QSeal2"

Public Key:	30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C3:FB:D5:89:DA:7E:6A:FC:56:E9:32:55:46:FA:AA:A7:F6:C2:F0:8D:B9:FE:38:53:F5:F6:4B:65:5F:7E:C2:36:8B:08:A6:AF:82:77:CF:04:6A:FF:8E:05:86:5A:AD:14:14:68:5F:8F:D8:C4:00:F4:A3:1A:90:BD:23:43:7A:DE:E8:EF:38:EB:E1:2D:28:48:99:7B:2C:07:8D:CCA7:B0:3D:0D:5E:76:F6:31:23:44:AA:7E:D8:54:3E:E1:40:DD:F9:1E:EF:E7:FA:88:12:EB:71:73:3E:F0:4A:7C:45:A2:D2:B7:33:BA:6F:AB:59:EF:57:DF:7F:35:F3:7E:15:9C:19:2F:C2:26:0A:C8:51:82:EB:F2:CB:89:C6:EF:A1:5C:80:A9:E7:87:98:AE:A9:C1:01:7E:E7:D8:FA:4C:B1:9F:D8:69:39:D9:C0:C2:F8:82:A3:63:C0:27:DD:11:67:37:E6:DE:E1:44:75:1D:C5:AA:9A:89:2E:68:88:8D:AF:FC:BE:6F:16:DE:40:80:54:10:95:7C:31:9C:3C:99:A5:8C:A1:03:1B:56:70:0B:7C:C6:74:82:CD:A8:F2:1C:1F:E6:CB:8D:A9:05:36:08:83:30:27:30:12:BD:91:32:74:74:5E:CE:94:75:CF:DE:C5:99:8F:02:30:1C:96:DF:1C:DA:DC:1D:5A:AC:C0:BB:7F:28:07:AE:EA:8D:39:D5:4E:E9:54:F5:C9:4B:70:37:AD:E8:03:5C:19:AF:49:77:F9:6A:45:25:58:F1:9A:89:79:89:E9:94:3A:B9:7E:11:04:C7:02:91:0E:B1:60:F1:FF:2D:88:CD:FD:06:DA:81:4B:D2:3F:72:4F:60:A8:44:23:46:4D:F0:71:B9:0D:52:54:B2:31:19:E7:78:1E:EA:68:D9:2B:2E:46:87:B6:DE:DC:3A:83:55:63:34:83:69:60:1C:14:D0:88:37:AE:F3:F3:04:3C:6C:E2:09:98:2A:1E:01:08:4C:39:F8:16:88:45:99:D4:B7:F5:7E:F2:16:C1:19:86:0E:6C:A7:EC:4D:04:58:3E:09:2A:02:16:BF:49:A0:14:48:D9:4A:51:2E:2C:6F:15:BE:02:FE:02:F4:8A:14:C7:82:82:3B:95:75:4B:B7:22:57:0F:06:2F:84:9D:DF:FB:EF:7A:A6:69:29:92:F5:98:1E:2F:95:27:E9:5C:2F:1D:C7:EA:12:27:63:EB:EC:F9:F1:2B:31:AD:F5:7F:18:61:AF:0D:34:70:80:92:F1:93:4A:E4:0C:1E:55:A0:1E:CE:D1:19:2F:63:08:0A:A9:69:0E:C1:85:52:AA:75:3E:F2:AC:AA:F1:C9:88:F5:DD:02:03:01:00:01	
Basic Constraints	IsCA: true - Path length: 0	
Subject Key Identifier	36:18:25:6E:D9:5D:F7:10:05:7C:27:2E:B8:EC:FA:41:4A:60:ED:1F	
Authority Key Identifier	A6:65:41:81:F2:5B:87:05:6A:DD:FD:8A:54:4E:8F:98:7B:DC:23:B8	
Authority Info Access	http://ocsp.entrust.net	
CRL Distribution Points	http://crl.entrust.net/dsr1.crl	
Extended Key Usage	Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12	
Certificate Policies	Policy OID: 2.5.29.32.0	CPS pointer: https://www.entrust.net/rpa
Key Usage:	digitalSignature - keyCertSign - cRLSign	
Thumbprint algorithm:	SHA-256	
Thumbprint:	8C:31:D9:37:51:28:D4:B1:07:F0:76:78:EE:BF:FF:2C:CA:26:A4:CA:BB:46:2F:25:7F:31:A3:6F:E7:BC:E1:04	
X509SubjectName		
Subject CN:	Entrust Certification Authority - ES QSeal2	
Subject 2.5.4.97:	VATES-B81188047	
Subject O:	Entrust EU, S.L.	
Subject C:	ES	
X509SKI		
X509 SK I	Nhglbtld9xAFFCcuuOz6QUpg7R8=	
Service Status		
Service status description	[en]	undefined.
	[es]	undefined.
Status Starting Time	2025-10-30T02:00:00Z	

38.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**38.5.2 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified Certificates issued by "Entrust Certification Authority - ES QSeal2"

Name

[es]

Certificados cualificados emitidos por "Entrust Certification Authority - ES QSeal2"

Service digital identities**X509SubjectName****Subject CN:**

Entrust Certification Authority - ES QSeal2

Subject 2.5.4.97:

VATES-B81188047

Subject O:

Entrust EU, S.L.

Subject C:

ES

X509SKI**X509 SK I**

Nhglbtld9xAffCcuuOz6QUpg7R8=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2022-07-21T00:00:00Z

38.5.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**38.6 - Service (granted): Qualified Certificates issued by "Entrust Certification Authority - ES QWAC2"****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[en]	Qualified Certificates issued by "Entrust Certification Authority - ES QWAC2"

Name	[es]	Certificados cualificados emitidos por “Entrust Certification Authority - ES QWAC2”

Service digital identities

Certificate fields details

Version: 3

Serial Number: 162874294663581112221639096432216076685

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Entrust Root Certification Authority - G2*

Issuer OU: (c) 2009 Entrust, Inc. - for authorized use only

Issuer OU: *See www.entrust.net/legal-terms*

Issuer O: *Entrust, Inc.*

Issuer C: *US*

Subject CN: *Entrust Certification Authority - ES OWAC2*

Subject 2.5.4.97: *VATES-B81188047*

Subject 0: *Entrust EU. S.L.*

Subject C: ES

Valid from: Tue Nov 16 01:00:00 CET 2021

Valid to: *Sun Dec 01 01:00:00 CET 2030*

Public Key:

Basic Constraints	<i>IsCA: true - Path length: 0</i>
Subject Key Identifier	<i>41:CF:AE:2B:1D:63:3B:CB:4C:F5:90:44:79:B6:5A:24:89:DF:92:9C</i>
Authority Key Identifier	<i>6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB</i>
Authority Info Access	<i>http://ocsp.entrust.net</i>
CRL Distribution Points	<i>http://crl.entrust.net/g2ca.crl</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://www.entrust.net/rpa</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>C9:7F:2F:6E:6A:8A:DB:6E:CF:E4:97:8F:08:CA:8F:6F:01:23:A9:47:84:52:2B:61:0A:DF:6A:B5:14:39:FC:62</i>

X509SubjectName

Subject CN:	<i>Entrust Certification Authority - ES QWAC2</i>
Subject 2.5.4.97:	<i>VATES-B81188047</i>
Subject O:	<i>Entrust EU, S.L.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>Qc+uKx1jO8tM9ZBEebZaJlnfkpw=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time*2025-10-30T02:00:00Z***38.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

38.6.2 - Extension (not critical): TakenOverBy**TakenOverBy**

URI	[en]	https://avance.digital.gob.es/en-us/Servicios/FirmaElectronica/Paginas/Informacion-cese-actividad-ENTRUST.aspx

TSP Name

Name	[en]	Sectigo (Europe) SL

Name	[es]	Sectigo (Europe) SL

Scheme Operator Name

Name	[en]	MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION

Name	[es]	MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION DIGITAL

Scheme Territory	ES

38.6.3 - History instance n.1 - Status: granted

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	[en]	Qualified Certificates issued by "Entrust Certification Authority - ES QWAC2"

Name	[es]	Certificados cualificados emitidos por "Entrust Certification Authority - ES QWAC2"

Service digital identities**X509SubjectName**

Subject CN:	Entrust Certification Authority - ES QWAC2

Subject 2.5.4.97:	VATES-B81188047

Subject O:	Entrust EU, S.L.

Subject C:	ES

X509SKI

X509 SK I	Qc+uKx1jO8tM9ZBEebZaJlnfkpw=

Issuer O: *Entrust, Inc.*

Issuer C: *US*

Subject CN: *Entrust Certification Authority - ES QTS1*

Subject 2.5.4.97: *VATES-B81188047*

Subject O: *Entrust EU, S.L.*

Subject C: *ES*

Valid from: *Mon Oct 03 17:12:28 CEST 2022*

Valid to: *Sat Dec 29 01:00:00 CET 2040*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:07:DF:10:A1:83:32:E9:4B:62:12:10:52:35:59:05:C1:3E:EB:4F:AE:77:70:CD:A2:80:03:C0:DF:CF:0A:66:2F:69:32:95:51:F0:D3:C1:1B:3E:5B:12:E5:34:B9:3D:AF:4F:F0:10:E0:81:DC:D2:87:03:83:08:1C:8D:66:85:C7:0B:C4:9B:14:57:EB:61:83:C8:A2:A1:5A:14:6F:EE:C6:D8:D4:A5:98:73:05:45:80:6E:12:18:4C:9F:74:88:81:5E:3B:54:0B:97:93:67:C5:81:4B:02:29:9D:DC:D2:20:82:C0:BF:A0:7F:C1:8D:87:91:10:C3:E9:EF:13:0E:0D:D0:2B:84:4D:C6:68:49:A0:AE:E9:32:3E:6E:D3:58:5E:8B:C6:80:80:9C:3D:68:89:89:60:95:BE:22:D4:5C:6F:96:64:F4:4B:F1:DE:6B:5B:D2:27:DC:FA:2F:8D:A0:C1:18:94:13:4A:1F:4C:E2:81:15:17:A0:71:13:4E:5B:97:17:6E:C6:26:0B:F3:15:C2:0A:5F:A2:C8:94:76:0B:CA:4C:DE:09:6D:02:81:54:81:EC:85:C7:AA:75:1E:C9:8F:7F:AD:FF:96:8B:D6:59:4E:AE:46:DE:0F:71:7B:39:0B:DA:95:E2:6B:DD:C2:0E:C1:4B:87:F8:E0:2C:CE:89:68:B5:B9:BC:D6:74:22:87:C9:3E:55:89:6F:31:73:C6:C9:E3:1A:EC:23:7D:03:97:9F:8B:03:F1:E0:34:F7:A0:63:41:8F:81:24:F6:20:3C:6F:A3:FC:83:45:5A:EB:49:38:FD:6A:1D:82:AE:28:DD:5C:A5:3F:24:AC:8A:EB:11:E7:89:CD:3B:54:21:A2:FD:BD:B1:CD:08:6F:75:AD:F4:F4:E4:32:F1:A6:B3:7C:61:8C:9B:E1:8B:23:7D:CD:6D:8A:22:1D:EE:F4:71:49:00:5D:17:82:BA:8B:F3:CA:E0:A4:B8:BE:0D:FC:C7:47:F6:58:F1:61:9B:76:F2:0D:D8:97:C3:5E:FB:EB:54:82:37:59:3C:57:68:9F:A7:60:1B:F0:34:49:DF:6B:8B:84:A3:E0:CF:62:6C:8F:FA:7B:33:63:4B:4A:38:E3:1E:6B:E9:F8:30:2F:2D:25:29:13:80:C0:34:F6:69:ED:77:E8:8C:36:3A:2A:AA:07:3F:D2:46:F1:F0:F3:F5:F0:A8:7C:33:75:12:5F:32:4A:C4:AF:B2:C4:D7:5C:EB:76:AF:AD:98:94:55:89:D4:A6:66:3A:EB:D8:8B:A7:1C:50:F3:82:D5:E3:AD:6E:C3:6D:56:0A:3D:F9:12:9E:5A:9D:28:49:EC:46:5F:EC:61:55:C0:F9:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *69:63:82:CA:C2:F1:11:9A:71:43:32:85:8B:AE:37:CA:96:76:BE:80*

Authority Key Identifier *A6:65:41:81:F2:5B:87:05:6A:DD:FD:8A:54:4E:8F:98:7B:DC:23:B8*

Authority Info Access *http://ocsp.entrust.net*

CRL Distribution Points *http://crl.entrust.net/dsr1.crl*

Extended Key Usage *id_kp_timeStamping*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://www.entrust.net/rpa

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *25:3F:46:3F:B1:9E:06:D1:88:A1:F8:1A:B6:A3:CA:78:C9:35:2B:08:DC:94:DD:74:C
F:05:33:68:09:36:38:12*

X509SubjectName

Subject CN: *Entrust Certification Authority - ES QTS1*

Subject 2.5.4.97: *VATES-B81188047*

Subject O: *Entrust EU, S.L.*

Subject C: ES

X509SKI

X509 SK I aWOCysLxEZpxQzKFi643ypZ2voA=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-10-30T02:00:00Z

Scheme Service Definition URI

URI [en] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Entrust.aspx

URI [es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Entrust.aspx

38.7.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [en] Qualified timestamps issued by Entrust Certification Authority - ES QTS1

Name [es] Sellos cualificados de tiempo emitidos por Entrust Certification Authority - ES QTS1

Service digital identities

X509SubjectName

Subject CN: Entrust Certification Authority - ES QTS1

Subject 2.5.4.97: VATES-B81188047

Subject O: Entrust EU, S.L.

Subject C: ES

X509SKI

X509 SK I aWOCysLxEZpxQzKFi643ypZ2voA=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2023-07-04T00:00:00Z

39 - TSP: EVICERTIA S.L.U.**TSP Name**

Name *[en]* *EVICERTIA S.L.U.*

Name *[es]* *EVICERTIA S.L.U.*

TSP Trade Name

Name *[en]* *Evicertia*

Name *[es]* *Evicertia*

Name *[en]* *VATES-B86021839*

Name *[es]* *VATES-B86021839*

Name *[en]* *EVIDENCIAS CERTIFICADAS S.L.*

Name *[en]* *EVICERTIA, SL*

PostalAddress

Street Address *[es]* *C/Lagasca, 95*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28006*

Country Name *[es]* *ES*

PostalAddress

Street Address *[en]* *C/Lagasca, 95*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28006*

Country Name *[en]* *ES*

ElectronicAddress

URI *[en]* *mailto:info@evicertia.com*

URI	[en]	http://www.evicertia.com
URI	[es]	http://www.evicertia.com

Page 1251

Issuer OU: *TSP-UANATACA*
Issuer O: *UANATACA S.A.*
Issuer L: *Barcelona (see current address at www.uanataca.com/address)*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-B86021839*
Subject CN: *EVITSU-QE1A*
Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*
Subject O: *EVIDENCIAS CERTIFICADAS S.L.*
Subject L: *MADRID*
Subject C: *ES*
Valid from: *Wed Nov 20 11:28:35 CET 2019*
Valid to: *Sat Nov 20 11:28:35 CET 2027*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:ED:46:D5:53:E8:98:51:4D:21:2F:86:10:66:F3:31:74:83:7D:1F:A7:D4:87:E2:A1:77:FE:19:BC:F8:AD:49:38:7F:C4:8D:AC:C3:55:B7:7F:8E:CE:71:AC:30:18:A8:97:08:86:1A:94:F0:7C:E6:C8:F6:64:45:E2:F0:A0:25:75:93:DC:78:1F:38:5F:BD:42:38:F8:7E:69:D8:8A:84:E4:89:0A:A2:8A:71:87:51:09:5E:0E:07:CE:5C:26:AB:05:93:14:A7:15:C1:78:FA:4F:73:82:8A:ED:86:AA:C1:99:09:82:71:30:F1:18:44:5E:73:C8:AE:D3:EA:AB:AE:4C:28:80:64:1A:C6:31:82:6D:18:8B:BD:CD:2B:5D:DB:25:80:7A:71:15:9C:CD:23:75:C8:CE:CC:A9:0F:C1:41:C0:7D:F2:C0:42:6B:25:0B:E8:C8:DC:87:80:EC:75:09:11:89:4A:8C:EE:30:A0:C0:55:9D:FF:2B:D9:B0:DE:4B:1A:9C:16:59:95:34:14:26:65:07:66:EF:A3:76:5D:76:9F:91:91:D3:10:D2:DB:98:57:A8:85:07:B2:F4:F9:3B:C5:74:B4:FD:8C:4A:9B:BD:F5:05:33:7F:8C:3C:87:D3:A9:06:8E:9D:F1:C1:ED:7E:99:B4:DA:21:E7:BE:29:7E:B9:02:03:01:00:01*
Authority Info Access *<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>*
Subject Key Identifier *44:2C:E2:48:B9:CB:2E:62:B2:B5:92:28:47:9F:34:CA:A6:29:D3:47*
Basic Constraints *isCA: false*
Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*
Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: <https://www.uanataca.com/public/cps/>
Policy OID: 0.4.0.2042.1.2*
CRL Distribution Points *<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>
<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>*
Extended Key Usage *id_kp_timeStamping*
Subject Alternative Name *info@evicertia.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *35:2C:E0:7F:3D:6F:31:AC:2E:48:4F:82:66:BD:4A:6A:1E:ED:1F:B8:AC:E9:7D:39:19:DD:8C:D4:47:D6:D5:DF*

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1A*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *RCziSLnLLmKytZloR580yqYp00c=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2025-02-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

39.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Qualified timestamps issued by EVITSU-QE1A*

Name *[es]* *Sellos de tiempo cualificados emitidos por EVITSU-QE1A*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1A*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *RCziSLnLLmKytZloR580yqYp00c=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-07-28T00:00:00Z*

39.2 - Service (withdrawn): Qualified timestamps issued by EVITSU-QE1B

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by EVITSU-QE1B*

Name *[es]* *Sellos de tiempo cualificados emitidos por EVITSU-QE1B*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *7645472127858035635*

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIHHTCCBQWGAwIBAgIlahosZIEgy7MwDOYJKoZihvcNAQELBQAwgboxCzAIBgNVBAYTAkVTMUOW
OgYDQOHDDECCYXJzWxvbmEgKHNlZSbidXlyZW50IGFkZHIic3MgYXQgd3d3LnVhbmF0YWNhLnNv
b3R5ZGRvZ2NkZXIwBQGA1UECgwwVGVVQVRBQ0EgYy5BLUEVMBEGA1UECgwwVFNQOLVVB7F4UQUOMB
MR0wGAYDQOQDBFVQU5BVEFDOSBDOTIqMjAxNjEYMBYGA1UEYQwPVkFURVVMQTY2ZmNkXDMBA4X
DTESMTEyMDEwMkYnF0xDTI3MTEyMDEwMkYnF0wgaExCzAIBgNVBAYTAkVTMUOWDQOYDQOHDDECC
OURLSUOVTAIBgNVBAAwMEVWVSUAFThKQVYMOOVSVEGSSU8REFTFMuTCAKJABgNVBAAwMUVW
SUNFURJQOSBDE9VRCBRVUFMSUZIRUOgVFNBIFFMTEUMBIGA1UEAwwLRVZlFVNLVFFMuxGDAW
BgNVBGEtMDI2BVEVTLU4NjAyMTQzOTCCASiWDOYJKoZihvcNAQELBQADggEPADCCAOoCggEBAKPx
GhUdbAwc3njtvoPYpFtg7MLxRn67MzFL3IKtWeTnpVMS9bdrCmY2X3BpJA9js9pooDU
AB++xBtb++xqBC+K4DQC8K4B20ts2NwALAIWazemfule30XcctFOjv6lANz1DV++EmLx7Iyz2e++P
Art8anqNCIDESBPApMLDf6VvYTMMPBpwwIMtBLmngLxkaV59wp/5kq2nfcWcuR++YRETuqz7Eo40
V2xHKAjMfHy6mXg55OAu0U5dKMePeBzjvdRPHKee3z20q5in++xY0vRivOCt75KssGfmm
L2aHKAjWvp46GEHLEl5oBv7d353X8barfCzAwEAAbOCA4hwgqI6MH4GCCsGAOUFBwEBBHHwDA2
BggrBgEFBQcwwAYIqaHR0cDovL29ic3AxLnVhbmF0YWNhLnNvbs9wdWJsaWVmcGpL29ic3AvMDYyG
CLCSGAOUFBwEABHn6dHw0b2NccDduWuYXRhY2EuY29l3B1YmXpYy9wa2kvb2NccDduWuYD
YUOCBBYEFCAVISQvDpDiHOP3a++dDooC90CTaMAKGA1UdEwOCMAAwHwIDVR0jBBgwFoAUFvHrYHPO
B0ap4qNo8OERsnSScDwpmZGA1UjQlASBic3BjDBBBgorBgEEAYLXNngIFMG4wOgYIKwYBBQUHAgIw
Lg9w22YyGimaWNhZ3BzZG9pZ2VsoGBzZG9pZG9pZG9pZG9pZG9pZG9pZG9pZG9pZG9pZG9pZG9p
AgEwJGh0dH8Zoi8vd3d3LnVhbmF0YWNhLnNvbs9wdWJsaWVmcGpL29ic3AvMDYyGCLCSGAOUFBw
EABHn6dHw0b2NccDduWuYXRhY2EuY29l3B1YmXpYy9wa2kvb2NccDduWuYD
HwSBhzcBhDBApD6gPIY6aHR0cDovL2NybDEudWVufYXRhY2EuY29l3B1YmXpYy9wa2kvb2NccDdu
MmN1Ym9yZGluYWRhLnNybDA0BgNVHQ8BAf8EBAMCB4AwFgYDVROIAQHBAWwCgYI
a2kvY3lsL0NBMMn1Ym9yZGluYWRhLnNybDA0BgNVHQ8BAf8EBAMCB4AwFgYDVROIAQHBAWwCgYI
KwYBBQUHAgwwHQYDVORBBYwFIEsaW5mb0BldmJzXjQ0aWEuY29tMA0GC5qCSib3DQEBcwUAA4IC
A0DLXmTjUAFmITAGzVEM++czZAgZnEAQ3UQ4b1QZL5egmP40tvmXRGVgGxlvwK79IMXmyk
+Yv4iXPNYAYIG4Dv8dwKCYU0U0tXmGmXwCTFtz+7eh6sner6F7to9s1QO2nFW1QKZ2s66CV2j
v0jczbPdjrgCXQK3knl7bovBoPh7ajneCtBRDmXQrvUf8/q6v4Fz/rwHlvE9qgEk6GNPWk8
E2eNteLZHLV5OXA2BiaMmMjMwZclmXwBsdTHITFOjpaVdeWzEjueB2JA19dr++vH5SnXt
8g3Y/rI4IpcjAzDweuRH15wvDnIFwLS0OmdgKNEFE00ae20vGDDDBcUa6YPbD3ztBl++bEK
YAg95Bk8Nijlswgs3llwcQrpikdptRi3ePiOZWYS9AiAcIdusgIy6HqX3WlZe++rEjMeND
ACMhuBgcGfACc9AKNfbXmfmM0ZLHmD4wWEIYxInKegOPfK9kXkicpES9TsXZNYfluvSL
r7vO3fFNj5kc7vkMuig7jAAZlryFPB9n3MHk83q0Gpz/duISFGUuOxehgNTPYOBMRq++0iB88Veb
CgWj4sO3jw8BzNWskPjFvZwSlovNdtXQMrguXcpjWX6RHBx1dUilq7Aq3Q0C0cXek5Qol
hg==

```

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer 2.5.4.97:

VATES-A66721499

Issuer CN:

UANATACA CA2 2016

Issuer OU:

TSP-UANATACA

Issuer O:

UANATACA S.A.

Issuer L:Barcelona (see current address at www.uanataca.com/address)**Issuer C:**

ES

Subject 2.5.4.97:

VATES-B86021839

Subject CN:

EVITSU-QE1B

Subject OU:

EVICERTIA CLOUD QUALIFIED TSA QE1

Subject O:

EVIDENCIAS CERTIFICADAS S.L.

Subject L:

MADRID

Subject C:

ES

Valid from:

Wed Nov 20 11:29:24 CET 2019

Valid to:

Sat Nov 20 11:29:24 CET 2027

Public Key:

```

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A3:F1:18:95:18:02:FC:1C:DE:72:6D:BE:83:D8:3D:81:58:AB:83:08:8F:14:6D
:34:84:7B:88:CC:C5:3F:79:4A:4D:67:93:4E:7A:55:31:3F:6D:6E:8D:91:99:8D:97:0C:13:E0:8C:0D:20:48:13:E9:A2:4D:04:00:1F:81:0C:06:FE:C6:A6:C2:A6:41:38:0D:00:BC:28:8F:08:0B:
:4B:6C:D8:D5:80:2C:02:16:6A:A7:A6:7E:E2:5E:DC:E5:DC:72:D1:5F:3A:5C:BA:20:03:73:D4:35:7E:12:62:F1:EE:5C:B3:D9:EF:8F:02:BB:7C:02:7A:8D:0A:D0:ED:4B:C3:C8:02:93:0B:0D:FF:
:FA:57:24:CC:30:13:F0:C2:53:2D:8C:12:E6:9E:05:31:29:A5:79:F7:0A:7F:E6:4A:B6:9D:F7:16:72:E4:7E:61:11:13:BA:A6:78:12:BE:34:8D:9C:61:7E:46:89:30:58:63:EA:65:E0:E7:94:00:C6:
:5D:14:E5:00:8C:93:F3:0E:07:32:6F:75:13:C1:29:EB:22:DF:3D:B4:AB:98:BF:EB:F1:63:4B:D1:AD:18:CE:71:3E:02:2A:CB:06:7E:29:C8:2F:66:87:28:05:AF:83:8E:86:12:11:C4:2E:3E:6
:8:06:FE:EC:97:74:B7:5F:C6:DA:AF:47:02:03:01:00:01

```

Authority Info Access<http://ocsp1.uanataca.com/public/pki/ocsp/><http://ocsp2.uanataca.com/public/pki/ocsp/>**Subject Key Identifier**

26:95:95:24:2F:8A:90:E2:84:E3:F7:6B:E7:43:A3:47:3D:D0:24:DA

Basic Constraints

IsCA: false

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl*
http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@evicertia.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *63:F3:67:59:42:A9:AB:49:5A:AA:5F:46:36:BD:FE:60:EA:7A:98:68:A9:6C:4A:5B:A5:34:2E:D8:F7:26:3B:5E*

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1B*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *JpWVJC+KkOKE4/dr500jRz3QJNo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2025-02-05T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

39.2.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [en] *Qualified timestamps issued by EVITSU-QE1B*

Name [es] *Sellos de tiempo cualificados emitidos por EVITSU-QE1B*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVITSU-QE1B*

Subject OU: *EVICERTIA CLOUD QUALIFIED TSA QE1*

Subject O: *EVIDENCIAS CERTIFICADAS S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *JpWVJC+KkOKE4/dr500jRz3QJNo=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2020-07-28T00:00:00Z*

39.3 - Service (granted): Qualified electronic registered delivery service Evicertia QERDS QE1B

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description [en] *An electronic delivery service providing qualified electronic deliveries.*
[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name [en] *Qualified electronic registered delivery service Evicertia QERDS QE1B*

Service digital identities

Version: 3

Serial Number: 71166263957444923512048386468114844203

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: AC Firmaprofesional - CUALIFICADOS

Issuer SERIAL NUMBER: *A62634068*

Issuer OU: *Certificados Cualificados*

Issuer O: *Firmaprofesional S.A.*

Issuer C: *ES*

Subject CN: *EVICERTIA, SL*

Subject SERIAL NUMBER: *B86021839*

Subject 2.5.4.97: *VATES-B86021839*

Subject 0: *EVICERTIA, SL*

Subject ST: MADRID

Subject C: *ES*

Valid from: *Thu Apr 29 17:53:37 CEST 2021*

Valid to: Tue Apr 28 17:53:36 CEST 2026

Public Key:[illegible]

Basic Constraints *IsCA: false*

Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Authority Info Access *http://crl.firmaprofesional.com/cualificados.crt*
http://ocsp.firmaprofesional.com

Certificate Policies *Policy OID: 1.3.6.1.4.1.13177.10.1.10.2*
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.1

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*

Subject Key Identifier *7E:2B:34:4C:EE:A3:59:9D:A5:4D:75:C4:0C:4B:48:9A:CB:0B:D4:67*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:AE:3B:30:3D:B1:91:7D:16:FE:1D:FF:54:06:C8:E0:E8:3A:7D:D3:CC:9F:A0:39:00:FE:4E:9C:08:D6:28:F4*

X509SubjectName

Subject CN: *EVICERTIA, SL*

Subject SERIAL NUMBER: *B86021839*

Subject 2.5.4.97: *VATES-B86021839*

Subject O: *EVICERTIA, SL*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *fis0TO6jWZ2ITXXEdeImssL1Gc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description *[en] undefined.*

[es] undefined.

Status Starting Time 2025-02-05T00:00:00Z

Scheme Service Definition URI

URI	[en]	https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx
URI	[es]	https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

39.3.1 - Extension (not critical): TakenOverBy

TakenOverBy

URI	[en]	https://avance.digital.gob.es/en-us/servicios/firmaelectronica/paginas/informacion-cese-actividad- evicertia.aspx

TSP Name

Name	[en]	UANATACA, S.A
Name	[es]	UANATACA, S.A

Scheme Operator Name

Name	[en]	MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION
Name	[es]	MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION DIGITAL
Scheme Territory	ES	

39.3.2 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name	[en]	Qualified electronic registered delivery service Evicertia QERDS QE1B
Name	[es]	Servicio cualificado de entrega electrónica certificada Evicertia QERDS QE1B

Service digital identities

X509SubjectName

Subject CN: EVICERTIA, SL

Subject SERIAL NUMBER: *B86021839*

Subject 2.5.4.97: *VATES-B86021839*

Subject O: *EVICERTIA, SL*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *fis0TO6jWZ2ITXXEDEtImssL1Gc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-12-15T00:00:00Z*

39.3.3 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[en]* *Qualified electronic registered delivery service Evicertia QERDS*

Name *[es]* *Servicio cualificado de entrega electrónica certificada Evicertia QERDS*

Service digital identities

X509SubjectName

Subject CN: *EVICERTIA, SL*

Subject SERIAL NUMBER: *B86021839*

Subject 2.5.4.97: *VATES-B86021839*

Subject O: *EVICERTIA, SL*

Subject ST: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *fis0TO6jWZ2ITXXEDEtImssL1Gc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</i>	
Service type description	[en]	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	[es]	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>

Name	[en]	Qualified electronic registered delivery service Evicertia QERDS QE1A

Service digital identities

Version: 3

Serial Number: 7685577479348319478

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: UANATACA CA1 2016

Issuer OU: *TSP-UANATACA*

Issuer 0: UANATACA S.A.

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVISEAL-QE1A*

Subject SERIAL NUMBER: *B86021839*

Subject O: *Evicertia S.L.*

Subject C: *ES*

Valid from: *Thu Feb 10 12:47:00 CET 2022*

Valid to: *Tue Feb 09 12:47:00 CET 2027*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D3:F8:11:0F:55:20:B9:20:9E:D6:0D:A7:5C:51:E3:E3:8C:93:3C:F7:D9:26:72:F4:78:DC:3E:EF:82:C1:57:E6:95:AB:37:65:78:4E:62:19:54:CC:E4:D0:41:3E:76:63:26:71:0E:81:25:07:E6:22:0E:0D:7C:BB:DA:61:85:1F:07:5D:3C:ED:57:92:F7:9A:E5:57:FD:BD:98:E2:7E:46:29:9F:DC:28:76:12:A6:51:EA:B5:29:C2:09:0E:02:89:4F:0F:48:A8:87:D6:27:8D:4F:43:BF:C2:5A:24:78:E2:B0:E1:7A:8B:AE:DD:7F:B7:E4:38:32:57:78:75:10:53:C3:D4:54:4A:82:A1:0E:08:B7:AC:2E:FF:73:10:DB:12:3C:C5:E8:A0:0C:C6:2E:D0:E1:0B:94:67:E0:11:F5:2E:5E:22:13:73:92:21:C7:47:5C:08:1C:96:91:EF:35:58:0F:38:D0:E5:0E:EB:F4:F2:D1:3B:49:16:E6:C9:E6:01:5B:0C:D6:D2:A8:40:18:6C:06:68:67:ED:00:A7:A9:59:0E:B5:98:ED:4D:2E:06:3A:3A:13:AF:C8:7F:48:F3:BC:BE:5D:C9:25:7D:69:A7:B2:42:4D:91:81:EF:A5:5B:62:7E:9E:D2:BE:E3:33:38:AB:67:BC:EF:92:B2:6C:F4:F5:02:03:01:00:01

Authority Info Access
http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *29:EA:16:7A:9C:85:34:6B:27:75:C8:B6:7D:73:B0:80:55:1F:A4:14*

Basic Constraints *IsCA: false*

Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.1.9.1
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado cualificado de Sello Electrónico en software.]
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points
http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *info@evicertia.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *94:56:67:7A:2B:05:D8:19:18:D9:CB:BA:C5:50:1B:29:6E:32:03:67:E5:F4:64:6E:1D:4D:02:39:38:E6:07:66*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *29:EA:16:7A:9C:85:34:6B:27:75:C8:B6:7D:73:B0:80:55:1F:A4:14*

Basic Constraints *IsCA: false*

Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.1.9.1*
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado cualificado de Sello Electrónico en software.]
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl*
http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *info@evicertia.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *10:F9:DF:B5:26:1C:36:CA:10:CF:F6:C5:E0:D8:D9:C5:8C:D1:5E:03:18:2B:E3:66:E5:F8:E2:56:01:D4:B2:C0*

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVISEAL-QE1A*

Subject SERIAL NUMBER: *B86021839*

Subject O: *Evicertia S.L.*

Subject C: *ES*

X509SKI

X509 SK I *KeoWepyFNGsndci2fXOwgFUfpBQ=*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time*2025-02-05T00:00:00Z***Scheme Service Definition URI**

URI *[en]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

39.4.1 - Extension (not critical): TakenOverBy**TakenOverBy**

URI *[en]* *https://avance.digital.gob.es/en-us/servicios/firmaelectronica/paginas/informacion-cese-actividad-
evicertia.aspx*

TSP Name

Name *[en]* *UANATACA, S.A*

Name *[es]* *UANATACA, S.A*

Scheme Operator Name

Name *[en]* *MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL
TRANSFORMATION*

Name *[es]* *MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION
DIGITAL*

Scheme Territory *ES*

39.4.2 - History instance n.1 - Status: granted**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/EDS/Q***Service Name**

Name *[en]* *Qualified electronic registered delivery service Evicertia QERDS QE1A*

Name *[es]* *Servicio cualificado de entrega electrónica certificada Evicertia QERDS
QE1A*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVISEAL-QE1A*

Subject SERIAL NUMBER: *B86021839*

Subject O: *Evicertia S.L.*

Subject C: *ES*

X509SKI

X509 SK I *KeoWepyFNGsndci2fXOwgFUfpBQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-10-24T00:00:00Z*

39.4.3 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[en]* *Qualified electronic registered delivery service Evicertia QERDS QE1A*

Name *[es]* *Servicio cualificado de entrega electrónica certificada Evicertia QERDS QE1A*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B86021839*

Subject CN: *EVISEAL-QE1A*

Subject SERIAL NUMBER: *B86021839*

Subject O: *Evicertia S.L.*

Subject C: *ES*

X509SKI

X509 SK I *KeoWepyFNGsndci2fXOwgFUfpBQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time

2022-12-15T00:00:00Z

40 - TSP: EAD TRUST European Agency of Digital Trust, S.L.

TSP Name

Name *[en]* *EAD TRUST European Agency of Digital Trust, S.L.*

Name *[es]* *EAD TRUST European Agency of Digital Trust, S.L.*

TSP Trade Name

Name *[en]* *EADTrust*

Name *[es]* *EADTrust*

Name *[en]* *VATES-B85626240*

Name *[es]* *VATES-B85626240*

Name *[en]* *European Agency of Digital Trust, S.L.*

Name *[es]* *European Agency of Digital Trust, S.L.</i>*

Name *[en]* *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Name *[es]* *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Name *[en]* *EAD Trust*

Name *[es]* *EAD Trust*

PostalAddress

Street Address *[en]* *Mentrida, 6 - local*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28043*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Mentrida, 6 - local*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code [es] 28043

Country Name [es] ES

ElectronicAddress

URI [en] mailto:info@eadtrust.eu

URI [es] mailto:info@eadtrust.eu

URI [en] https://www.eadtrust.eu/en/

URI [es] https://www.eadtrust.eu

TSP Information URI

URI [en] https://eadtrust.eu/en/

URI [es] https://eadtrust.eu

40.1 - Service (granted): Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP

Name [es] Certificados cualificados emitidos por EADTrust RSA 2048 SubCA For Qualified Certificates 2019-NP

Service digital identities

Certificate fields details

Version: 3

Serial Number: 10810916776045676818

Subject Alternative Name

ca@eadtrust.eu
http://www.eadtrust.eu
http://ca.eadtrust.eu
http://policy.eadtrust.eu

Authority Key Identifier *1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *82:34:0E:A4:D7:AC:D8:0D:F9:7D:C7:59:8C:94:95:58:8C:C8:87:3E:C9:50:6D:AD:0C:11:EA:11:94:33:39:9D*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 2048 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *a96Tsqr7utr+70ZOyWfcPf57p3U=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust RSA 4096 Root CA For Qualified Certificates 2019*

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 12:56:35 CEST 2019*

Valid to: *Sat Jun 02 12:56:35 CEST 2035*

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BF:82:E1:DE:E6:56:0F:54:32:10:4A:63:4A:B3:DD:62:26:79:75:56:3C:06:A1:63:C7:68:6F:36:5A:1D:93:CA:84:47:DF:C8:F0:05:F1:B5:34:76:02:6A:A0:B0:37:55:5C:E3:C2:83:78:51:AF:E9:71:69:8F:9F:B2:55:A4:C9:F9:27:4D:94:E3:5C:4C:BD:77:15:0D:F5:9D:0C:3E:54:4B:23:70:3D:A1:93:64:14:BB:90:72:EF:EA:AB:5F:5B:2D:5D:62:81:15:86:C2:04:49:5C:FC:98:F5:3D:2B:01:D4:A1:7C:EF:B5:A6:E9:F9:51:74:65:64:0B:23:B4:50:4C:F0:50:90:52:EF:BC:83:4C:84:85:17:FC:C8:97:E3:86:56:90:BD:34:42:86:DE:B7:D3:96:81:B1:4C:32:8E:44:92:66:5D:74:2F:72:31:81:40:AC:F4:AC:EF:DA:24:17:9F:CB:5E:07:A1:AC:73:7F:0E:06:98:03:4F:79:69:AS:2D:60:AD:15:30:CD:CE:E7:95:8C:3B:F8:DB:AC:47:13:2F:BD:9D:31:09:DC:8C:97:6E:3E:3E:06:7D:F5:F2:86:CC:32:24:3A:82:B0:20:92:CB:51:AD:DE:73:18:00:E3:18:25:91:CA:BF:17:97:38:3D:F6:C9:9D:4B:BC:A1:6B:29:E8:C3:BB:67:D5:34:F4:C1:CD:97:C2:05:52:BC:3A:CB:9A:B4:E5:A4:0E:46:6D:EA:2E:A3:97:09:43:BE:03:A0:7B:11:57:49:E5:5B:50:65:E6:6C:4B:BD:77:1B:DB:B9:42:50:39:C4:0D:BC:28:0B:AA:C6:92:2A:48:40:17:5A:C0:EE:9F:1D:E3:E4:A2:AF:39:B2:19:8D:50:F5:D6:23:DC:5E:EA:6A:9F:65:68:00:DA:61:4B:63:C7:47:5A:64:24:89:13:6D:01:68:02:61:33:EE:9C:3A:55:2C:F8:AC:23:29:D6:D1:3A:BB:01:CA:3F:27:A1:5C:15:1E:9C:B1:18:1C:BC:8E:5A:55:D4:11:DE:2D:78:D5:01:F9:66:69:10:50:BB:47:22:D8:74:94:4A:8D:FA:4D:5C:2F:BE:B2:17:38:85:2B:26:07:31:FA:09:15:9C:77:2C:44:6E:03:5F:68:B5:7C:DB:30:86:93:4C:18:F4:E5:EC:41:F4:19:32:A0:00:13:F9:18:0C:26:5E:94:AA:F9:1A:52:61:FC:34:7C:49:D1:DE:B7:D1:2E:05:3F:76:02:CA:45:90:1B:C1:1E:87:84:DA:A5:35:C8:C1:BF:D5:7F:5A:A4:DA:B8:E0:FF:B3:DE:DD:5A:43:CC:F4:9B:B1:8E:27:B5:02:03:01:00:01

Certificate Policies
Policy OID: 2.5.29.32.0
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: <http://policy.eadtrust.eu>
CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

Basic Constraints
IsCA: true - Path length: 0

Subject Key Identifier
06:33:DA:2B:CE:E9:81:51:4F:69:DD:CD:C8:AF:DF:2C:2F:3D:BE:5E

Issuer Alternative Name
ca@eadtrust.eu

Subject Alternative Name
ca@eadtrust.eu
<http://www.eadtrust.eu>
<http://ca.eadtrust.eu>
<http://policy.eadtrust.eu>

Authority Key Identifier
E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4

CRL Distribution Points
<http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl>

Authority Info Access
<http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt>
<http://ocsp.eadtrust.eu>

Key Usage:
digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:
SHA-256

Thumbprint: 04:BF:1D:A6:D0:16:8B:DD:3F:2D:EC:2E:22:C5:0D:55:8B:DE:5C:7C:C9:51:6C:83:CB:63:93:35:2A:9F:0F:9C

X509SubjectName

Subject OU: Natural Person

Subject 2.5.4.97: VATES-B85626240

Subject C: ES

Subject O: European Agency of Digital Trust, S.L.

Subject CN: EADTrust RSA 4096 SubCA For Qualified Certificates 2019

X509SKI

X509 SK I BjPaK87pgVFPad3NyK/fLC89vI4=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2020-10-05T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

40.3 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP

Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For
Qualified Certificates 2019- NP

Service digital identities

Certificate fields details

Version: 3

Serial Number: 5842919634329022553

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer 0: *European Agency of Digital Trust. S.L.*

Issuer CN: *EADTrust RSA 8192 Root CA For Qualified Certificates 2019*

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust. S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

Valid from: *Thu Jun 06 13:20:51 CEST 2019*

Valid to: *Sat Jun 02 13:20:51 CEST 2035*

Public Key:

```

30:82:04:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:8D:D6:DC:08:00:8E:54:D3:A6:35:2C:EE:2C:26:C8:F1:46:25:13:FA:38:25
:B6:63:7F:FE:C4:F5:F8:84:04:55:6C:82:20:52:A8:33:85:D7:D4:8C:2D:D9:82:64:38:9D:EB:D6:F0:8C:A0:27:A4:8C:8F:71:19:3D:C8:1C:57:D6:02:51:C9:C7:A2:05:CD:CD:25:C0:B7:D
D:78:7F:DF:6E:DD:D3:D1:73:E0:FA:CB:59:11:AE:1C:5A:D8:ED:9B:CS:34:02:28:62:F5:71:D1:0F:97:7E:D0:F9:D3:18:63:F2:8D:8A:D6:13:6C:12:52:AA:8E:9D:85:12:1C:F9:7B:58:95:7B:0
C:3D:F8:65:01:42:16:50:4E:C9:59:3C:5C:22:58:42:8C:45:A0:14:A7:0B:E4:92:38:3C:EF:90:AC:D1:D5:AD:8B:E1:8C:83:CC:BF:F2:B4:F2:03:7E:98:0F:D2:A5:88:99:4C:8D:19:AC:AF:54:09
:12:43:C8:F1:3A:7D:C2:ED:78:2D:C2:F4:E6:00:54:BE:4C:9B:0E:E2:69:26:2D:2D:37:13:06:AE:80:81:D9:54:45:68:82:44:1D:86:02:F5:74:57:BE:24:52:94:38:D4:A5:70:38:FD:53:CD:09
:E7:F0:F8:0E:88:30:07:35:18:CF:85:F1:FE:52:D5:C6:64:E4:EC:0F:FB:6E:EF:AA:9A:72:A2:FB:2D:4D:96:D2:0A:08:CS:8C:49:09:19:64:C7:8F:CL:81:86:FD:3F:36:9F:14:78:96:7F:80:C9:66
:09:5A:93:0F:F7:73:B4:5C:FF:3F:48:C0:64:E5:DD:F1:97:E6:8D:97:9A:5D:CD:35:0F:10:A1:90:F0:91:80:17:E1:CD:7F:26:69:A4:53:69:04:4A:57:CF:D2:D1:89:37:50:75:C2:47:56:92:7B:13
:B7:70:74:47:DB:53:8E:18:04:2C:FC:15:93:08:1F:14:40:81:FB:F0:44:A1:14:99:65:91:DB:A1:C1:F8:28:1D:AA:30:BA:94:1C:59:44:7F:9E:DA:7E:90:CD:09:7B:53:6E:44:8F:77:58:F3:80:8
3:B5:6B:38:AA:EF:01:16:33:67:80:41:30:43:C1:BF:CC:E8:65:A7:9D:3C:F3:C4:CA:9F:36:70:64:46:15:EB:36:AC:CF:FD:C8:DF:88:40:1C:A8:5F:88:49:1E:E8:A7:61:4F:47:C4:44:6B:EB:D5
:40:60:EE:3A:66:40:D6:33:2C:74:A1:38:2B:3E:4E:AD:AA:07:06:25:38:43:88:18:52:02:69:40:8B:82:F5:CA:B7:38:72:AE:8A:8B:F0:66:F3:E0:8D:D5:C6:CA:A5:81:59:AB:7B:92:8E:CD:5E:5
E:10:78:41:2A:31:05:F4:46:45:C8:1C:43:03:06:BA:E5:33:59:71:B4:86:1A:AD:E4:73:83:40:45:45:9D:9A:41:4C:85:01:C5:E8:61:D4:23:12:9E:C5:F4:18:3E:EF:D4:0E:91:6A:C0:51:88:48
:6C:72:C2:70:50:08:66:84:B6:A2:23:0A:E2:08:05:0A:5C:39:12:93:BD:1F:83:84:10:12:FE:5F:28:FB:93:78:AC:4F:20:A9:8D:61:9F:4F:FF:BF:1C:D0:67:9F:03:42:D7:F4:42:87:44:41:85:23
:00:FF:D5:66:82:6A:D9:89:A3:55:67:5F:7B:5D:D4:25:0E:8F:5D:82:A4:32:69:49:AD:A6:EA:2A:FE:69:04:73:C0:15:56:D4:A6:2B:4E:53:40:8A:FB:5A:D8:D1:42:96:2D:65:09:95:08:31:FB:F
4:DC:9C:82:8F:BC:09:DE:BC:07:13:74:AC:95:A9:0C:CA:09:82:AC:BF:86:70:53:1A:59:35:AC:00:78:91:CC:4E:96:34:12:78:56:57:3C:FF:E4:99:C7:1C:DA:B2:53:DD:FB:73:24:5F:C8:E3:06
:A2:F4:1F:86:83:5C:FD:16:E4:6D:6C:02:D1:66:3C:F8:80:02:E3:59:01:3D:2A:BA:E2:80:3A:63:9C:8A:42:2C:F3:A2:0C:A9:EB:EE:16:18:7A:B2:86:18:91:EC:E1:E2:E3:58:17:81:23:CE:82:0
2:37:A0:47:D3:83:72:3F:37:38:17:C8:A8:85:6C:24:2C:C9:EE:32:D2:81:CF:77:80:51:BB:36:9F:44:83:FA:DC:50:21:8B:22:7B:02:54:87:F8:11:88:80:30:F3:AA:AA:64:9D:86:DD:6B:2B:00
:C9:07:70:8C:FA:9F:87:A3:CE:E8:3F:34:14:F7:FE:59:FD:6B:85:3B:7F:99:43:0B:20:88:13:4C:91:D6:44:5D:5C:A4:2E:38:05:CF:93:C7:76:FF:8F:9A:E1:FD:7E:1D:F2:31:C8:50:37:F8:BF:37
:68:C2:3D:46:83:6A:9D:C0:9B:86:A3:48:A4:6D:46:B6:3D:A7:D8:99:A0:E4:7D:BE:F4:5A:09:C7:03:F8:D5:F3:E8:CF:4F:3F:40:46:01:1C:3D:8F:C8:19:2E:76:D8:A7:55:42:2B:C4:E3:8F:44:3
F:7D:D2:31:8F:CC:7D:BE:90:DA:1E:A7:F9:35:29:23:9B:BC:48:BB:2F:0C:F4:EE:82:FC:15:53:45:A2:52:9A:76:B5:ED:F0:71:8D:B1:8F:B7:62:57:48:0A:C2:CC:53:EA:C4:8B:02:F7:B3:74:BB
AC:29:02:03:01:00:01

```

Certificate Policies *Policy OID: 2.5.29.32.0*

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: <http://policy.eadtrust.eu>

CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *EA:99:CF:6B:01:18:F9:81:44:69:FD:C8:9A:68:AD:D5:37:D3:73:98*

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
<http://www.eadtrust.eu>
<http://ca.eadtrust.eu>
<http://policy.eadtrust.eu>

Authority Key Identifier *06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB*

CRL Distribution Points *<http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl>*

Authority Info Access *<http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt>*
<http://ocsp.eadtrust.eu>

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *20:02:B8:D5:AF:02:C5:A9:61:E1:0A:4D:A3:C2:7F:63:F3:5D:7F:7A:AD:94:15:99:D
A:36:D5:2E:03:B7:A8:9D*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *6pnPawEY+YFEaf3Immit1TfTc5g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.4 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name *[en] Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP*

Name *[es] Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Certificates 2019- NP*

Service digital identities

Certificate fields details

Version: *3*

Subject Alternative Name *ca@eadtrust.eu*
http://www.eadtrust.eu
http://ca.eadtrust.eu
http://policy.eadtrust.eu

Authority Key Identifier *01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E5:F7:80:53:30:0C:16:9D:79:A7:FB:38:73:61:AD:2A:8D:1A:9B:B7:50:B9:18:3C:7B:B1:97:34:D5:42:F0:7C*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *w+LbEe82PGqASYsjRo07pzNrmQw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

Subject OU: *Natural Person*
Subject 2.5.4.97: *VATES-B85626240*
Subject C: *ES*
Subject O: *European Agency of Digital Trust, S.L.*
Subject CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*
Valid from: *Thu Jun 06 13:23:16 CEST 2019*
Valid to: *Sat Jun 02 13:23:16 CEST 2035*
Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:D9:CE:B1:A4:B4:20:04:89:46:55:D9:9A:87:0D:F6:FB:BA:26:90:47:04:E9:CC:02:EB:75:01:D3:E0:31:C2:02:E4:C6:20:D7:C8:20:E7:68:74:F9:24:B5:57:4C:69:53:1B:66:60:F3:38:11:DF:0F:6B:89:B3:5C:44:23:AB:F8:CE:D9:D2:5E:1D:C8:6F:49:CA:EF:FD:03:36:3B:4A:D6:07:C5:F0:1A:51:81:0B:1B:C0:83:F5:56:6E:36:98:3E*
Certificate Policies *Policy OID: 2.5.29.32.0*
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: <http://policy.eadtrust.eu>
CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *8F:BA:E8:66:72:74:22:4C:CC:27:89:48:08:31:73:0B:1E:9B:4B:82*
Issuer Alternative Name *ca@eadtrust.eu*
Subject Alternative Name *ca@eadtrust.eu*
<http://www.eadtrust.eu>
<http://ca.eadtrust.eu>
<http://policy.eadtrust.eu>
Authority Key Identifier *78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01*
CRL Distribution Points *<http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl>*
Authority Info Access *<http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt>*
<http://ocsp.eadtrust.eu>
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *F8:EA:34:65:13:55:C4:07:C9:03:87:56:08:B0:FF:A1:88:80:5E:93:08:1A:D0:3A:39:B8:22:6D:C3:5E:AD:B4*

X509SubjectName

Subject OU: *Natural Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *j7roZnJ0lkzMJ4IICDFzCx6bS4I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

40.6 - Service (granted): Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP*

Certificate Policies*Policy OID: 2.5.29.32.0**Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401**CPS pointer: <http://policy.eadtrust.eu>**CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]***Basic Constraints***IsCA: true - Path length: 0***Subject Key Identifier***FA:D9:0A:A2:69:CB:FF:68:AF:F2:9A:89:FF:56:94:54:1B:B3:99:8F***Issuer Alternative Name***ca@eadtrust.eu***Subject Alternative Name***ca@eadtrust.eu**<http://www.eadtrust.eu>**<http://ca.eadtrust.eu>**<http://policy.eadtrust.eu>***Authority Key Identifier***1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99***CRL Distribution Points***<http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl>***Authority Info Access***<http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt>**<http://ocsp.eadtrust.eu>***Key Usage:***digitalSignature - keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***29:40:0D:5D:52:0D:A0:85:2E:4D:D5:3A:5B:85:D3:26:8F:9A:3D:CC:60:61:C2:85:47:44:40:CB:85:9E:09:A8***X509SubjectName****Subject OU:***Legal Person***Subject 2.5.4.97:***VATES-B85626240***Subject C:***ES***Subject O:***European Agency of Digital Trust, S.L.***Subject CN:***EADTrust RSA 2048 SubCA For Qualified Certificates 2019***X509SKI****X509 SK I***+tkKomnL/2iv8pqj/1aUVBuzmY8=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description** [en]*undefined.*

[es] undefined.

Status Starting Time 2020-10-05T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

40.7 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP

Name [es] Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Certificates 2019-LP

Service digital identities

Certificate fields details

Version: 3

Serial Number: 7219277311459685234

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
http://www.eadtrust.eu
http://ca.eadtrust.eu
http://policy.eadtrust.eu

Authority Key Identifier *E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7F:D0:FF:DF:3A:A0:C9:69:93:DC:6D:1A:DA:D7:79:22:63:81:AC:7B:5C:48:A0:1D:1A:2E:4A:FC:6C:2F:77:7A*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *MS5X72kv2esv2yA4CeOEpyxJ/0U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

Issuer 2.5.4.97:	<i>VATES-B85626240</i>
Issuer C:	<i>ES</i>
Issuer O:	<i>European Agency of Digital Trust, S.L.</i>
Issuer CN:	<i>EADTrust RSA 8192 Root CA For Qualified Certificates 2019</i>
Subject OU:	<i>Legal Person</i>
Subject 2.5.4.97:	<i>VATES-B85626240</i>
Subject C:	<i>ES</i>
Subject O:	<i>European Agency of Digital Trust, S.L.</i>
Subject CN:	<i>EADTrust RSA 8192 SubCA For Qualified Certificates 2019</i>
Valid from:	<i>Thu Jun 06 13:23:01 CEST 2019</i>
Valid to:	<i>Sat Jun 02 13:23:01 CEST 2035</i>
Public Key:	<pre> 30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:BD:C1:7A:9A:EA:B2:22:39:30:B9:D4:26:56:67:BA:3A:0A:DF:43:AA:C3:27:5B 2C:50:CF:29:AD:74:8D:92:E3:74:88:09:F7:5D:12:DA:54:1B:BF:C2:9D:08:CF:D7:68:19:8C:72:88:25:B1:03:F9:BC:9F:11:60:A5:A9:14:00:73:EB:60:22:9B:63:10:1C:BE:C0:7C:24:68:72 83:EE:AB:9C:68:08:C9:A9:2D:1F:89:ED:9F:3E:18:89:C2:91:7F:D5:F8:19:E1:79:92:7A:46:80:DD:1D:07:97:52:B4:CD:C3:2B:81:D8:D7:78:1F:41:59:ED:07:34:52:9A:A5:C3:01:C5:7A:EF:5 1:DE:61:D2:EE:B5:D2:C6:92:91:60:B9:D5:52:B1:46:B7:CC:B9:1E:C5:59:80:3B:A5:C1:C5:8C:3C:59:9E:C6:61:68:14:35:27:6E:D0:1A:F4:5D:AE:FA:D2:E7:62:FC:F2:BA:9D:05:32:C2:48:A 9:5E:36:39:E4:39:1E:9D:D0:64:2D:46:A5:E1:C6:7B:20:14:78:88:06:54:0D:86:E6:7C:F0:4B:E1:9B:89:D9:DC:9B:E3:18:F1:8F:3D:1C:E1:C0:78:94:D3:CB:13:87:89:C3:D0:DA:1B:CA:63:B 2:9F:D8:83:90:5E:E6:AD:78:D3:D6:C2:5A:34:73:C8:77:D8:A7:F5:1D:0A:56:2B:AB:6E:35:21:23:52:4D:06:E2:2E:E3:38:36:A4:D4:56:33:A1:80:83:1E:CF:75:CB:FC:E5:D3:E9:58:5D:23:19 94:C5:AB:1F:29:28:9B:24:76:B9:F2:FC:29:E0:28:C1:CC:0C:2B:2C:ED:83:A3:32:8A:B1:E4:FC:24:DA:71:4F:C4:2E:8F:CA:71:66:4C:60:21:63:4F:70:EB:C4:90:A1:15:58:D8:48:7D:30:13:3 5:0A:80:E7:BC:CB:FE:7F:5E:D3:A3:F4:4B:82:E9:15:F6:E0:91:C7:05:F5:35:FC:CF:C5:34:6A:4B:C5:C8:76:8F:0C:65:C8:EB:0A:CD:97:2D:7B:90:49:43:F8:23:9C:F2:5A:55:4A:A4:80:8C:CC 21:95:E0:4E:93:DC:E6:ED:DA:60:02:C7:EB:4E:C7:D9:83:68:2A:2B:D0:39:96:C1:F1:36:6D:80:80:36:83:AD:2B:C4:BF:66:F3:95:75:33:CF:2C:5F:F9:87:59:CD:9F:08:4A:C5:EF:BA:D9:4C:1 8:05:69:D8:A8:03:76:6D:D6:D4:26:E1:63:8E:69:36:B8:EB:98:5F:40:32:40:00:A6:C4:9C:CA:3D:2F:82:86:DC:E9:78:8F:BE:76:5C:39:FE:01:F6:B1:29:B8:C7:6F:13:D9:94:0A:97:5D:E4:A8 44:C2:D2:01:07:20:3A:3D:FD:BF:99:46:BE:FF:1F:AF:66:CB:72:61:07:85:4A:48:78:1C:04:1C:A3:03:66:A7:1D:B9:D8:8D:25:0D:0A:0B:DC:A8:44:82:AD:0F:CA:C7:11:E9:91:03:F6:45:C6 D1:B8:C6:91:2C:DC:63:5B:08:1E:C9:CF:4E:86:FD:7E:4D:DA:3B:9A:5A:2B:35:88:F9:D6:15:BA:37:42:D2:8C:46:4E:89:92:68:6D:38:45:9C:FD:7D:4A:F0:46:0A:E6:85:E6:74:F4:2E:E2:AD DA:07:A4:D0:13:A4:7A:A7:10:3E:10:5C:3C:46:3D:BB:97:14:4C:C2:4E:D0:FE:F0:7C:0A:F3:67:AD:09:B5:FF:E1:06:32:EB:2C:A4:68:0A:F0:24:C6:EA:DE:08:F0:9B:DC:41:7B:BF:4C:63:AD:7 1:18:4A:05:E4:86:AE:2E:5D:1B:56:D0:77:94:80:1A:E0:63:FA:FC:9A:52:88:07:D8:F3:97:12:D3:EC:D7:70:3E:C3:F2:A0:8B:10:1D:79:98:38:EB:86:7B:C9:90:1E:CF:EE:D4:49:68:A3:7D:9B 1C:46:AE:C6:A9:A7:9A:43:8A:48:2E:15:96:29:CA:3A:17:6B:2E:BF:4D:E0:AF:36:E5:07:80:CE:43:CA:2B:42:A2:F0:4E:73:08:EC:54:8B:1E:6A:CE:8E:1D:EF:DE:FC:F1:CF:5E:13:50:C8:62 69:90:CC:82:79:85:F3:12:E9:5D:F7:7D:E2:94:62:28:91:41:5F:80:1C:FA:F2:FD:72:9D:BF:E3:FE:B2:72:3E:96:20:7A:61:88:CA:10:D9:A1:CC:E0:E9:FC:8C:A2:35:C5:2B:CF:C3:E6:97:6 D:11:40:80:7C:EA:D4:1E:C3:1C:90:83:82:FE:12:E9:4D:55:26:06:49:8D:88:E5:71:0D:5B:6C:FC:1F:84:A6:3C:21:8C:F9:1A:1B:8B:0E:C7:E3:EC:7A:04:D4:5A:12:BA:FB:FB:04:E0:29:F2:97 58:9A:15:3E:31:E4:19:D6:34:13:07:41:AD:BA:1C:86:73:9A:49:21:D9:E7:BC:AB:F2:C4:3A:0D:01:53:7D:FB:02:17:61:29:C3:C3:08:18:8C:D2:9A:E3:53:CF:F0:8C:1A:12:43:24:C8:FE:B4:8 2:E2:5A:65:66:6C:20:FF:17:87:F4:FE:08:B5:96:00:C5:5F:80:78:E1:20:06:B1:0F:5D:F0:8C:4E:17:D7:C4:06:95:51:9F:DA:8E:10:11:99:D6:6F:6D:40:CD:41:49:97:22:49:E3:3B:37:8B:4E:3 A:69:71:13:02:03:01:00:01 </pre>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401</i> <i>CPS pointer: http://policy.eadtrust.eu</i> <i>CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Subject Key Identifier	<i>8C:48:A3:F4:BF:0A:56:40:CA:CE:93:5D:7A:3D:26:D8:14:94:A6:CF</i>
Issuer Alternative Name	<i>ca@eadtrust.eu</i>
Subject Alternative Name	<i>ca@eadtrust.eu</i> <i>http://www.eadtrust.eu</i> <i>http://ca.eadtrust.eu</i> <i>http://policy.eadtrust.eu</i>
Authority Key Identifier	<i>06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB</i>
CRL Distribution Points	<i>http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl</i>

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *22:E4:1B:48:79:FA:A2:11:61:D4:65:02:C7:FC:14:39:E5:49:0E:CC:FF:43:42:1F:6E:9C:08:61:42:70:81:96*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *jEij9L8KVkDKzpNdej0m2BSUps8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.8.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

40.9 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP

Service Type Identifier<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description** [en]*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es]

*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.***Service Name****Name** [en]*Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP***Name** [es]*Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP***Service digital identities****Certificate fields details****Version:** 3**Serial Number:** 330884354597339267**X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIIE5CCBlugAwIBAgIBjEjKUGCQIMwCgYIKoZlZjOEAwIwQZsQTA/BgNVBAMMOEVBRFRydXN0
IEVDO2YyNTYyUm9ydCB0QSB0b3JpUXVibG5maWwvIElicnR2m1YXRlc3AyMDE5MSBwL0YDVQOQK
DCZFRXVjYVh0b2ZzY3kqb2YgRGlnaXRhcCBUCnVzdCwglUy5MLjEELMAKGA1UEBhMCVRVxgDAW
BgNVBGEtMDIzBEVYTLUjH4NTYyYjE0MDAeFw0xOTAzMDYxMTIzMTJlFw0zNTA2MDIxMTIzMTJlMIGw
MTIwPQYDVQODDZFRUkucnVzdCB0QSB0b3JpUXVibG5maWwvIElicnR2m1YXRlc3AyMDE5MSBwL0YDVQOQK
dGVzZDlwMTkxLzAtBgNVBAoAMjY1cm9wZWVudEFnZW5jeS8vZiBEaWdpdGFSFRydXN0LDBTLkww
MQswCQYDVQOGEWJFZiEYMBYGA1UEYDwPVkFURVMT0j1Nj2MjQwMRUwEwYDVQQLDAXMzWdhhCBQ
ZjZzZ4wWTABoqhkiOPOiBggqhkjOPQMBBwCAATWu018jPjCtFztbystqBRSY2B6sMGg
HRYPeJommoO6orLRmzV9cGF8BjDjfhfRNOwBYEigucSELa6nduo4iCoDCCApwwagGA1UdIASB
oDCBnTAGBgRVHSAAMIGSBgqRbGEAYN1AgEBAYMRMIGAMCUGCCsGAQUFBwIBFh0dHRwOi8vcG9s
aWNSLmVhZHRydXN0LmV1MFCGCCsGAQUFBwICMES5VM1Ym9yZGluYXRiElicnR2m1YXRlc3Ay
dGhvcml0eS4gRXVyb3B0YVY4QWdlbmN5IG9mIERpZ20YVWwVHj1c3QsIFMuTC4wEgYDVROTAQH/
BgwvBgEB/wIBADA0BgNVhQBA8BA8BAMCAYYwHQYDVRO0BBYEFNNM5Dq9N5whyOH0u49kM/Lm/ch
McMAA1UdEgRmFRB0mMmGvH2HRydXN0LmV1hZodHRwOi8vd3d3LnVhZHRydXN0LmV1hZodHRw
Oi8vY2EuZWVkdHJ1c3QzZXVWGGWh0dHA6Ly9wb2xp3kuZWVkdHJ1c3QzZXUwYwYDVRO0BFwwWoeO
Y2FAZWVkdHJ1c3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXUwYwYDVRO0BFwwWoeO
d3d3Y2EuZWVkdHJ1c3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXUwYwYDVRO0BFwwWoeO
rySj115BDBIBgNVHR8EQTAjMDZgOBA5hdodHRwOi8vY3JsLmVhZHRydXN0LmV1L2VhZHRydXN0
LXlvb3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXUwYwYDVRO0BFwwWoeO
cDovL2NhbmVhZHRydXN0LmV1L2VhZHRydXN0LXlvb3QzZXVWGGWh0dHA6Ly93d3cuZWVkdHJ1c3QzZXUwYwYDVRO0BFwwWoeO
AQUF8ZABhhdodHRwOi8vbnZncC5iYWR0cnVzdC5ldAKBggqhkjOPQDAgNjADBGAIEAo3kVg5X
A0kxZV5H86QV1mB0g4mizN1xrt75QV+8ggUCIQCOjpmf3+3shotYYNzkUlv0aWfjV//5lps4eXGP
qoeaQ==

```

-----END CERTIFICATE-----

Signature algorithm: SHA256withECDSA**Issuer 2.5.4.97:** VATES-B85626240**Issuer C:** ES**Issuer O:** European Agency of Digital Trust, S.L.**Issuer CN:** EADTrust ECC 256 Root CA For Qualified Certificates 2019**Subject OU:** Legal Person**Subject 2.5.4.97:** VATES-B85626240**Subject C:** ES**Subject O:** European Agency of Digital Trust, S.L.**Subject CN:** EADTrust ECC 256 SubCA For Qualified Certificates 2019**Valid from:** Thu Jun 06 13:23:12 CEST 2019

Valid to: *Sat Jun 02 13:23:12 CEST 2035*

Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:D6:B8:E9:75:F0:93:C9:71:3C:45:DA:DB:5B:CA:DB:2D:A8:14:46:61:90:7A:B0:C1:AA:1D:16:11:A4:42:68:9A:6A:0E:EA:8A:CB:46:6C:D5:F5:C1:85:23:C9:43:8D:F7:E1:7D:13:74:C0:16:04:8A:08:9C:B0:42:DA:EA:7D:2E*

Certificate Policies *Policy OID: 2.5.29.32.0*
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: http://policy.eadtrust.eu
CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *D3:4C:6C:3A:BD:36:FE:70:87:23:87:3A:EE:3D:90:CF:CB:9B:F7:21*

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
http://www.eadtrust.eu
http://ca.eadtrust.eu
http://policy.eadtrust.eu

Authority Key Identifier *01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *36:09:93:59:34:06:E5:AA:31:16:63:ED:FF:5A:34:09:A8:DD:1E:30:70:8C:9C:AB:E3:4E:FD:8E:53:92:73:3D*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *00xsOr02/nCHI4c67j2Qz8ub9yE=*

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.9.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

40.10 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019-LP**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019-LP

Name [es] Certificados cualificados emitidos por ECC 384 SubCA For Qualified Certificates 2019-LP

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 6351802085939901953

Subject Alternative Name *ca@eadtrust.eu*
http://www.eadtrust.eu
http://ca.eadtrust.eu
http://policy.eadtrust.eu

Authority Key Identifier *78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt*
http://ocsp.eadtrust.eu

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *04:14:B9:54:12:A9:8B:2D:9C:8B:DD:67:16:72:19:9D:7A:9C:E5:B9:7F:69:07:38:01:AD:CB:E0:DE:D9:7B:41*

X509SubjectName

Subject OU: *Legal Person*

Subject 2.5.4.97: *VATES-B85626240*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

X509SKI

X509 SK I *XBniqx22uD1FEpGSG4wUcdjo9fY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from: *Thu Jun 06 13:37:02 CEST 2019*

Valid to: *Tue Jun 03 13:37:02 CEST 2031*

Public Key:
30:82:02:22:30:0D:06:09:2A:96:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CA:5E:F2:49:EC:A3:02:BD:8C:4E:F2:57:A5:68:33:4E:AA:27:C7:F9:37:48:95:58:AF:3E:F4:28:6F:0E:82:6E:7B:A2:30:94:00:7A:0C:5F:B6:C9:B5:DC:80:BA:35:94:63:E6:9F:C8:66:43:6D:57:D8:A1:4F:CA:8D:9F:28:BA:29:AD:5F:67:13:FC:02:3D:DC:A1:63:45:4E:08:77:50:1D:AF:EE:CA:88:4E:A2:8A:1D:E3:0A:7C:27:B3:0E:D6:9C:62:40:FB:36:AB:A8:4C:43:A9:3B:17:24:E0:DD:5A:C5:73:82:B1:3B:BD:A5:AA:1A:6C:77:41:56:85:E4:07:A7:DF:54:1A:74:A0:52:94:F8:99:FC:18:D1:94:49:D4:08:DD:AF:AC:C3:63:4F:35:44:DA:C1:90:20:F7:7A:C5:50:78:6D:05:6F:81:92:06:6C:7E:31:91:15:D2:51:05:B3:F6:6F:F0:B8:8F:A8:9A:25:26:C4:C5:00:63:F2:C2:A1:E0:4A:9C:D8:8E:C3:0A:DA:27:1C:DB:A8:9B:8F:D8:71:8C:E6:2F:71:55:58:D1:01:39:AF:98:A3:CF:76:01:A9:65:01:4C:A7:6F:CE:02:15:2A:CD:2C:4B:A0:22:D4:87:95:8C:61:42:E8:90:91:D3:15:94:22:A6:95:F4:D4:30:7F:89:4F:E5:47:CD:2F:1E:2A:5A:59:D0:10:C9:C8:2C:E5:EC:FF:E7:8D:05:98:AF:62:14:50:C8:1C:4A:F4:93:9F:A5:4B:10:88:8E:57:64:10:68:83:CE:69:83:C9:54:5C:F6:D1:35:1A:2B:2C:A7:9D:DE:B1:F1:23:EE:D5:D7:98:7E:F8:D3:7D:AB:38:9C:F4:C9:C1:95:B3:9D:4A:68:C3:42:97:23:47:79:43:80:4A:C6:2F:69:E8:40:98:6D:DF:5A:5E:D9:F8:FF:52:05:A7:3A:76:51:21:F0:89:A2:A7:68:1A:82:62:E2:40:82:AC:F8:27:E5:53:A3:7E:AE:49:97:ED:7:8E:33:A8:6C:74:90:E7:1E:C5:C1:FD:68:41:9B:C8:01:8E:55:AE:5F:87:67:92:3B:3A:EC:72:BA:30:AB:7F:14:6A:0C:0B:28:A1:21:23:4D:F4:F3:05:25:03:8C:18:8C:B5:2E:FC:3B:53:52:DD:97:17:09:7F:0A:A6:4F:8A:F3:52:25:CD:2F:70:DC:1D:AF:40:8F:E4:1D:ED:21:06:C3:44:63:CF:4A:16:BA:CB:44:74:B3:EA:7D:95:D5:B2:FC:C9:0C:87:29:7E:14:E7:CD:CD:BD:3A:DB:CF:68:CB:A9:A5:D2:D7:91:50:06:B8:7A:13:9A:F9:02:03:01:00:01

Certificate Policies
Policy OID: 2.5.29.32.0
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: <http://policy.eadtrust.eu>

Basic Constraints
IsCA: true - Path length: 0

Subject Key Identifier
84:CE:F3:6B:AA:A6:57:30:27:F7:C3:12:99:20:E5:E0:9B:5A:1E:44

Authority Key Identifier
B4:1E:28:D4:EA:AA:60:0F:10:04:74:CB:77:94:69:4C:11:87:E2:44

CRL Distribution Points
<http://crl.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22019.crl>

Authority Info Access
<http://ca.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22019.crt>
<http://ocsp.eadtrust.eu>

Extended Key Usage
id_kp_serverAuth

Key Usage:
digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:
SHA-256

Thumbprint:
00:9D:BA:D6:86:CE:CD:81:D1:3A:CA:C4:F6:73:DC:BA:5E:EB:78:9E:63:17:3C:DE:13:6C:B2:88:0C:1D:CE:79

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I *hM7za6qmVzAn98MSmSDI4JtaHkQ=*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] undefined.

[es] undefined.

Status Starting Time*2020-10-05T00:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.11.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.12 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

Name [es] *Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 8543911274838307584

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crt*
http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:4A:80:6A:46:D7:B7:97:25:B9:2C:EA:06:85:54:15:D9:24:E7:6D:C5:D5:1E:4E:D5:CA:39:55:CB:6E:C8:5D*

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I *DmLLaHy9Yxsoi1Qhrg+NpHENll4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.12.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name [en]

Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web
EV/PSD2 Cert 2019

Name [es]

Certificados cualificados emitidos por EADTrust ECC 256 SubCA For
Qualified Web EV/PSD2 Cert 2019

Certificate fields details

Version: 3

Serial Number: 3612576674077687876

[illegible]

Signature algorithm: *SHA256withECDSA*

Issuer C: *FS*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019*

Subject C: ES

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from: *Thu Jun 06 13:49:24 CEST 2019*

Valid to: Tue Jun 03 13:49:24 CEST 2031

Public Key: 30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2A:03:D0:A5:62:9C:0D:32:13:9F:0F:2B:D8:ED:0E:1A:76:E1:AA:35:EF:B5:C8:FA:E1:0D:D5:E9:3E:3D:86:61:80:36:59:78:3E:53:92:30:EB:18:80:B6:51:C8:57:87:0D:B8:53:5F:E9:94:C3:18:64:D5:55:7F:82:A1:07:35

Certificate Policies*Policy OID: 2.5.29.32.0**Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401**CPS pointer: http://policy.eadtrust.eu***Basic Constraints***IsCA: true - Path length: 0***Subject Key Identifier***09:75:1E:59:AD:00:68:B1:14:92:55:41:06:6F:B3:66:30:39:20:73***Authority Key Identifier***D3:77:CD:5A:DA:A3:93:5C:8B:4A:4C:65:D2:9A:0C:01:D5:99:3F:13***CRL Distribution Points***http://crl.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crl***Authority Info Access***http://ca.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crt**http://ocsp.eadtrust.eu***Extended Key Usage***id_kp_serverAuth***Key Usage:***digitalSignature - keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***B7:69:11:A3:35:2D:1A:27:B3:C3:55:F0:49:CF:6F:BF:C5:E3:E4:97:5B:FD:BD:BC:1F:A0:41:32:7F:C7:6D:7C***X509SubjectName****Subject C:***ES***Subject O:***European Agency of Digital Trust, S.L.***Subject CN:***EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019***X509SKI****X509 SK I***CXUeWa0AaLEUKIVBBm+zZjA5IHM=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2020-10-05T00:00:00Z***Scheme Service Definition URI****URI***[en]**https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx***URI***[es]**https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

Valid from: *Thu Jun 06 13:49:26 CEST 2019*

Valid to: *Tue Jun 03 13:49:26 CEST 2031*

Public Key: *30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:0F:C4:FC:C6:62:A7:C9:10:61:80:9D:E9:42:D2:D3:66:45:1E:8D:E6:31:65:CD:3D:7D:93:80:A3:F3:1E:59:11:8C:43:8A:5B:6E:57:3D:3E:E4:1E:06:89:42:40:57:6C:DD:EB:BA:75:92:AD:DD:23:3B:E5:4E:4E:95:D9:46:2C:CB:32:BC:29:C0:BE:1F:1E:A3:BF:08:36:4D:8A:BC:B1:77:40:6C:4A:C7:13:0C:0C:2C:75:29:4D:F9:CD:DA:A5*

Certificate Policies *Policy OID: 2.5.29.32.0*
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: http://policy.eadtrust.eu

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *71:BB:58:A0:3C:2F:54:87:5D:0B:7B:51:48:38:AB:60:D7:AA:A9:E3*

Authority Key Identifier *EA:E9:50:E4:B3:93:49:3F:05:04:35:A5:F0:47:57:11:7E:5E:11:19*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-ecc384eadevpsd22019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-ecc384eadevpsd22019.crt*
http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C8:79:2B:47:35:5F:A3:D1:52:AA:5E:86:F3:7C:27:65:0B:E1:E0:51:37:BD:36:E8:77:8A:CF:27:0B:B1:8B:54*

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

X509SKI

X509 SK I *cbtYoDwwVlddC3tRSDirYNeqqeM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-10-05T00:00:00Z*

Issuer O: *European Agency of Digital Trust, S.L.*
Issuer CN: *EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019*
Subject C: *ES*
Subject O: *European Agency of Digital Trust, S.L.*
Subject CN: *EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*
Valid from: *Thu Jun 06 13:35:52 CEST 2019*
Valid to: *Tue Jun 03 13:35:52 CEST 2031*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:42:6A:8F:D9:82:72:24:00:9A:3E:3F:4C:BB:51:5E:1F:65:13:0C:AE:54:EB:3A:D7:A0:FA:FF:FB:57:00:D1:56:B2:6A:00:BD:24:50:74:DA:0F:F1:7A:3D:D7:F6:DB:F9:E5:CF:55:F2:25:1F:C3:92:C0:EF:45:68:15:B3:4C:8D*
Certificate Policies *Policy OID: 2.5.29.32.0*
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401
CPS pointer: http://policy.eadtrust.eu
Basic Constraints *IsCA: true - Path length: 0*
Subject Key Identifier *E0:9B:82:F0:4B:7F:B6:68:88:EA:9F:B7:A0:2F:FE:15:A5:AC:95:64*
Authority Key Identifier *BC:2B:C7:5B:E3:6A:DA:7D:D1:A8:46:AD:47:DE:E3:45:C0:C3:FD:B2*
CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crl*
Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crt*
http://ocsp.eadtrust.eu
Extended Key Usage *id_kp_serverAuth*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *0E:1F:3A:20:04:0E:D5:B2:72:DC:C9:39:E7:B8:D5:B0:F4:BE:D7:64:C9:5C:E1:6C:B0:A4:7C:A4:56:0A:36:95*

X509SubjectName

Subject C: *ES*
Subject O: *European Agency of Digital Trust, S.L.*
Subject CN: *EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*

X509SKI

X509 SK I

4JuC8Et/tmil6p+3oC/+FaWsIWQ=

Service Status<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time

2020-10-05T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.15.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.16 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

Name [es] Certificados cualificados emitidos por EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 5773670184699650920

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIID1zCCA16gAwIBAgIUCAycVlly2gwCgYIKoZIzj0EAwMwYmYxOzBBBgNVBAMMOKVBRFRydXN0
IEVDQyAzODQgUm9vdCB0OSBgb3lqUXVhbGlnaWVkdjYiBEV9PVIbDZlXj0iDWMtKxLzAtBgNV
BAQMDjVlcn9wZWZuZWZlbnZ5eSBzZjBlaW9pdGZ3P3RyZXR0eXN0LmVudC0yODQyODQyODQy
Fw0xOTAzMDYxMTM1NTVafw0xOTAzMDYxMTM1NTVafw0xOTAzMDYxMTM1NTVafw0xOTAzMDYxMTM1
Mz00fjN1YkNBIEZvcjBRdWVsaWZzZW9vZVJlIERWLD9WIENicnQpMjA0OTVlMjA0OTVlMjA0OTVl
b3B1W4p0W0l0mN5lG9mIEr0Zj0YVW9vVHJlC30fPm0TC4xZjBBBgNVBAYTAkVMMHYwEAYkoZi
zj0CAQYFK4EEACIDYgE6o4kOzPzH2H9Wk476vEY6nkC3Giyoml.9YSRu0zdzl2o5lm8zCzGEUD
7pe0Gd3Y8JL7A1ygrZlJa+TJufpB4MwLz79VchZCRxFZxRuesh4Hn61haPkk7f5UXo4lB
nTCCAZKswYDVROg9EOWQACgRVRVSAAMDgCDSsGAQOB93UCAQESBghEwJzAlB9grB9E7BQCARYZ
aHR0CDovL3BvbGJleS5lYWR0cnVzdC5ldTASBgNVHRMBAf8ECDAGAQHAgEAMAA4GA1UdDwEB/wQE
AwIBhAdBgNVHQ4EFgQUZjV6yYw0Ckc+YKwgJfc+pv9k0wHwYDVROjBBgwFoAUHjTYEpRf9et
Q3G7LK689LA9EYwSwYDVROjBEOWQACgRVRVSAAMDgCDSsGAQOB93UCAQESBghEwJzAlB9grB9E7BQCARYZ
cnVzdC1yb290LWViyZM4NGVhZGR2b3YyMDE5LnNyDB6B8grB9E7BQCARYZMgwwRQYKwYBBQUH
MAKGOWh0dHAg6ly9jY5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LWViyZM4NGVhZGR2b3YyMDE5
LnNyDB6B8grB9E7BQCARYZaHR0CDovL3BvbGJleS5lYWR0cnVzdC5ldS9lYWR0cnVzdC1yb290LWViyZM4NGVhZGR2b3YyMDE5
BQUHAWECcSsGAQUBBMCMMAoGCCqGSM49BAMDA2CAMGQCMFgnk4ZwSc55l+6abjGjHJRlkaGeCj
zs7CXXWBDfEF3Wc9b1zKCjZlZb8hKLZAWRDNBSURCknoZ1GgWrmW/dazQklc+VTQ7t15/sSrm
czCUmbTj03iicWfBm/Hg5

```

-----END CERTIFICATE-----

Signature algorithm:

SHA384withECDSA

Issuer C:

ES

Issuer O:

European Agency of Digital Trust, S.L.

Issuer CN:

EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019

Subject C:

ES

Subject O:

European Agency of Digital Trust, S.L.

Subject CN:

EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

Valid from:

Thu Jun 06 13:35:55 CEST 2019

Valid to:

Tue Jun 03 13:35:55 CEST 2031

Public Key:

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:EA:8E:31:3B:33:F3:1F:61:ED:F5:62:B8:EF:A8:C4:62:3E:A7:90:2D:C6:89:8A:26:2F:D6:12:46:ED:20:CD:D8
 :B6:A1:29:66:F1:E6:5C:18:4B:83:EE:97:B4:19:DD:D8:F0:92:FB:03:5C:A0:47:32:14:6B:E4:D4:89:FB:4F:8C:1E:0C:7D:62:F3:EF:D5:5C:1D:90:91:C6:D1:59:AF:14:6E:7A:C8:78:1C:DE:B5:
 85:A3:EA:92:4E:EC:15:25:31

Certificate Policies

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: <http://policy.eadtrust.eu>**Basic Constraints**

IsCA: true - Path length: 0

Subject Key Identifier

66:3F:D5:EB:2C:B0:D1:CF:E4:73:E6:17:C0:68:C5:73:EA:6F:F6:4A

Authority Key Identifier

1C:94:D8:12:94:49:7F:D7:AD:43:71:BB:2E:B2:BA:33:D2:C0:F4:46

CRL Distribution Points<http://crl.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crl>**Authority Info Access**<http://ca.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crt><http://ocsp.eadtrust.eu>**Extended Key Usage**

id_kp_serverAuth

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint: 80:AB:1B:AA:C5:CA:A2:36:E8:80:17:92:FF:C8:8D:DC:CE:45:A9:30:FA:30:E5:78:D
B:94:4D:51:28:2E:15:70

X509SubjectName

Subject C: ES

Subject O: European Agency of Digital Trust, S.L.

Subject CN: EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019

X509SKI

X509 SK I Zj/V6yyw0c/kc+YXwGjFc+pv9ko=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2020-10-05T00:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.16.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.17 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019

Subject Key Identifier *50:6A:EE:F1:D7:1F:A5:AE:28:0F:A5:B9:00:C0:27:F3:CE:2E:AC:B7*

Authority Key Identifier *B6:C5:79:9E:16:1C:85:D9:52:1D:CB:1C:D2:88:C5:2C:C9:AF:0D:47*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crl*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crt*
http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *07:2C:23:9E:48:EE:41:17:F2:79:35:1A:1F:39:E2:B2:C8:5A:34:DA:65:52:43:EF:FF:18:D9:9B:CB:10:F9:14*

X509SubjectName

Subject C: *ES*

Subject O: *European Agency of Digital Trust, S.L.*

Subject CN: *EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019*

X509SKI

X509 SK I *UGru8dcfpa4oD6W5AMAn884urLc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2020-10-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.17.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

Subject O:	European Agency of Digital Trust, S.L.
Subject CN:	EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019
Valid from:	Thu Jun 06 13:33:34 CEST 2019
Valid to:	Tue Jun 03 13:33:34 CEST 2031
Public Key:	<pre> 30:82:04:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:B1:D5:D4:91:7F:C7:D3:FD:43:4C:4C:B0:2E:21:24:3D:8B:DC:CB:AD:40:D1:A E:A5:51:54:99:89:C9:D2:28:7C:8F:13:48:80:24:4B:43:87:13:56:A2:D5:02:D9:FD:85:89:AB:02:3C:33:32:C6:8A:CA:7E:68:C4:06:06:59:00:A6:A2:74:58:7A:E0:FD:75:F4:B4:CC:9E:E7:82: B4:83:C1:8B:3D:1B:75:0F:02:AF:F4:A3:E5:B6:2E:B7:10:AA:C1:4E:1E:DA:D0:E9:64:CC:48:45:22:18:6F:CE:06:EF:2C:17:63:69:F2:3D:CB:BC:FD:20:E0:3F:9A:79:AE:EC:AB:3F:33:37:6E:3 9:39:FD:03:82:37:01:37:55:EA:8B:04:DA:F2:24:99:2F:9F:02:2A:28:1D:EE:24:A0:20:5B:4B:E8:8A:50:79:C3:EF:1D:1D:C6:DA:BB:CA:DC:0F:D0:51:7F:5A:AC:93:EB:86:D7:F2:EA:20:9D:39 2B:44:1C:DF:E3:C0:6F:87:F7:9B:97:57:E8:AC:44:61:F6:0E:38:57:3B:68:93:B4:C6:7D:C1:84:1F:FC:2D:34:A2:B0:BC:C4:41:4E:62:0C:E2:7F:CB:A9:C9:7C:F0:EB:FD:90:89:F7:B9:E4:22:3 0:52:E2:07:4A:6A:8A:E7:AF:9A:39:64:86:7E:19:86:5D:76:D5:77:75:AD:94:A0:F2:A0:E1:D5:D0:80:04:5C:1A:A8:DA:73:85:A7:81:29:D5:62:13:79:83:0E:13:89:2B:2C:01:DB:32:13:7F:FA CD:51:2C:A3:D9:0C:FE:D7:D4:80:B5:9F:D6:A5:2D:C5:91:8A:7B:D4:49:AB:4C:06:27:43:BB:DD:A9:E6:3F:E0:48:82:10:B1:06:AC:93:FE:C9:BD:FA:50:F6:D8:08:9D:84:8A:91:F6:D3:31:F5 3E:60:B1:C0:D5:DB:E4:EE:99:6F:46:6B:23:B9:C1:E3:10:59:16:82:B2:29:6B:FC:A3:69:6F:83:72:A1:72:4C:AA:00:50:D2:58:7F:35:BC:8D:E0:B9:7C:68:84:AB:7B:3B:F3:03:CC:92:8A:4F:3 B:B6:76:F7:15:4A:09:5A:D8:46:2B:E9:2A:B9:17:E6:98:F3:43:13:14:51:6E:C4:E6:8F:F8:3B:23:35:D2:09:06:27:2C:76:9F:16:7E:85:5A:87:7C:AB:2D:A1:DA:9F:85:DD:A8:51:D1:5B:44:9D 06:12:BE:C9:14:60:51:27:63:37:FE:22:0C:30:EF:83:E6:E9:19:F6:85:6E:67:C6:B7:AS:37:DA:12:82:4E:88:F8:9C:D3:A3:44:64:F9:F0:9F:DB:7D:29:B2:EF:0C:42:9D:89:E3:9C:A4:0B:B3:C 9:C6:70:BC:47:74:8B:E2:CF:31:C3:25:87:F5:C2:77:88:EA:CD:82:8B:08:43:E4:8D:52:AC:7F:39:62:BE:65:19:56:49:53:45:72:61:08:3A:59:0D:19:16:8C:40:D5:3B:82:C0:04:21:82:0C:7B 3F:E3:DF:27:94:F1:90:58:45:01:C1:74:06:F7:9B:D2:A4:FA:47:0F:0D:FC:7B:C3:B6:07:B7:52:93:7C:E3:C7:D4:D6:D6:E2:D7:8D:F8:2B:9F:38:A6:A2:47:4E:A1:21:11:F4:4F:F5:9A:81:A2:0C B5:8F:E4:D1:3D:75:F6:DF:86:80:D7:8E:EB:01:83:0E:F8:5B:5E:7A:D5:4F:03:17:99:6D:FF:9C:5B:38:F6:8A:51:0F:51:84:9A:D8:39:78:0C:9E:CB:5C:12:33:75:12:7C:DD:B1:A8:2A:F6:5E:4 8:F8:8F:C6:0D:46:8D:0E:85:29:3D:0D:E4:B4:4B:8B:80:58:97:98:15:52:6E:F2:12:00:1D:34:5A:BB:5B:1F:2C:6A:25:8A:F2:8B:B1:CD:69:F2:2C:BD:DC:3B:AC:86:3B:88:0F:8F:91:8D:4E 45:37:FE:9C:A2:AF:E9:A6:BC:4D:EA:AC:27:85:65:BB:29:D9:20:C9:13:49:C5:AF:2B:3F:DF:DF:5B:8B:D0:8B:8F:BB:91:FA:85:18:CF:23:D7:B6:FF:88:7A:57:CE:88:87:6E:85:CF:33:E8:06:5 B:26:59:FC:C2:65:4E:87:45:2C:DA:B9:8D:9B:AF:FB:AF:B5:4B:6F:B1:80:61:02:5F:1F:00:CE:BB:28:D0:EC:B4:ED:3C:56:41:A9:5E:34:87:20:99:BA:40:0E:29:C1:C2:CB:84:27:76:68:29 73:C1:D1:16:3B:7D:3E:C3:08:92:FB:BB:69:9D:E3:F8:3F:8F:2B:D4:40:8D:9E:80:20:A5:40:55:60:A1:7B:17:ED:A1:EF:13:A2:66:EE:88:66:27:C0:D1:18:B5:4C:A7:F1:54:F1:94:54:6F:F9:C0 AA:C5:CD:4B:C4:CA:CD:92:31:A0:FF:FA:2F:69:A0:A8:AB:63:F9:9A:06:33:4C:1E:74:E2:2C:7C:2C:A5:2E:53:41:A5:00:77:48:25:51:7C:08:28:96:8B:8F:59:DC:B2:7E:63:9E:D0:2F:F8:E0:B 3:BD:E4:92:64:EC:43:D8:F6:9A:4A:D4:0D:AF:40:66:E8:F7:9C:52:F5:25:BB:58:66:F2:C7:BB:61:35:E5:42:72:6D:18:FF:2E:B3:78:9F:16:AD:65:5D:12:15:F1:1A:87:3D:20:7A:28:B9:48:00: 87:E3:02:03:01:00:01 </pre>
Certificate Policies	Policy OID: 2.5.29.32.0 Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401 CPS pointer: http://policy.eadtrust.eu
Basic Constraints	IsCA: true - Path length: 0
Subject Key Identifier	51:CE:86:38:39:E0:57:A2:35:99:B1:8C:63:57:65:8A:CA:7E:7B:15
Authority Key Identifier	9E:ED:0C:41:81:6A:6F:FA:66:09:FA:7C:7F:8C:48:63:08:36:7D:00
CRL Distribution Points	http://crl.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crl
Authority Info Access	http://ca.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crt http://ocsp.eadtrust.eu
Extended Key Usage	id_kp_serverAuth
Key Usage:	digitalSignature - keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	A1:46:16:D1:E8:C0:B4:9E:0E:21:CA:E2:B5:42:A8:35:1A:26:74:7D:3A:18:A4:59:9 9:C3:8B:A1:D0:78:B6:CB
X509SubjectName	
Subject C:	ES
Subject O:	European Agency of Digital Trust, S.L.
Subject CN:	EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019
X509SKI	
X509 SK I	Uc6GODngV6l1mbGMY1dlisp+exU=

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time*2020-10-05T00:00:00Z***Scheme Service Definition URI**

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.18.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.19 - Service (withdrawn): Qualified timestamps issued by QTSU ALPHA EADTrust**Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by QTSU ALPHA EADTrust*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por QTSU ALPHA EADTrust*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *1199784883094980787842*

Subject Alternative Name *ca@eadtrust.eu*
https://ca.eadtrust.eu
https://www.eadtrust.eu
https://policy.eadtrust.eu

Certificate Policies *Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421*
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.3
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

Subject Key Identifier *E2:60:19:10:A9:F9:70:75:60:4D:EB:35:84:A7:91:F7:28:9B:80:81*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *92:E7:2C:68:F6:B8:4E:8C:71:4F:A6:A0:54:13:C8:D5:0B:8F:1A:97:73:EF:24:0A:17
:B3:B0:B5:CA:59:8D:79*

X509SubjectName

Subject C: *ES*
Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97: *VATES-B85626240*
Subject OU: *Entity Seal Certificate*
Subject CN: *QTSU ALPHA EADTrust*

X509SKI

X509 SK I *4mAZEKn5cHVgTes1hKeR9yibgIE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time 2024-01-24T02:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

40.19.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [en] Qualified timestamps issued by QTSU ALPHA EADTrust

Name [es] Sellos electrónicos cualificados de tiempo emitidos por QTSU ALPHA EADTrust

Service digital identities

X509SubjectName

Subject C: ES

Subject O: EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL

Subject 2.5.4.97: VATES-B85626240

Subject OU: Entity Seal Certificate

Subject CN: QTSU ALPHA EADTrust

X509SKI

X509 SK I 4mAZEKn5cHVgTes1hKeR9yibgIE=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2020-10-05T00:00:00Z

40.20 - Service (withdrawn): Qualified time stamps issued by QTSU DELTA EADTrust

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.

[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Valid to: *Sun Nov 05 12:03:26 CET 2023*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:82:58:09:00:8A:F0:38:0B:6A:CD:3B:82:4D:20:B8:71:87:01:4B:83:20:05:2C:E4:68:2D:A0:22:8D:2F:68:AF:85:C5:73:42:DC:B4:E6:6F:8C:F5:8C:D8:76:1D:CC:95:0A:65:1B:40:DB:26:EF:81:1E:50:D6:C1:18:AB:CF:F7:5D:AC:C6:C9:A9:35:24:C8:6F:67:B1:78:A7:7A:A3:DC:23:01:32:FC:85:03:DE:DE:74:1E:8B:2A:F8:7E:69:3B:A2:47:94:32:56:8C:E7:2A:3B:5C:22:88:94:8A:60:9A:3E:11:49:2B:5A:50:96:CC:3B:39:13:41:2E:A5:7F:53:C6:02:82:D6:B8:EE:59:99:08:0A:5B:6C:30:96:A6:27:A2:36:A0:3A:84:5A:A6:45:C0:9B:45:A4:8A:98:1C:B4:AB:4B:5F:38:CC:CE:9D:EA:CB:AC:49:4C:72:DF:2B:DE:09:B2:01:E5:D6:37:66:36:91:E5:75:F4:0E:23:06:FE:81:4B:6A:77:AB:A1:F4:9A:6C:72:BA:70:41:D9:AE:D9:F2:D0:D8:37:F8:CE:37:F3:33:7F:E6:9A:94:CB:3A:50:F8:70:FD:BB:E8:E6:93:5A:D7:85:70:62:3D:E8:32:11:61:03:27:42:2F:EB:DA:20:01:72:7D:8F:12:55:02:03:01:00:01*

Authority Key Identifier *31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt*
http://ocsp.eadtrust.eu

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
http://ca.eadtrust.eu
http://www.eadtrust.eu
http://policy.eadtrust.eu

Certificate Policies *Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.1
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

Subject Key Identifier *AA:8A:D3:74:92:7B:8F:F8:11:44:C0:EC:91:27:CE:27:8D:15:43:42*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8F:04:72:62:CF:62:25:7E:BF:C8:85:E6:3F:65:11:12:31:35:13:3D:E2:8D:2A:8C:F1:03:4F:CC:B4:EA:7C:DA*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU DELTA EADTrust*

X509SKI

X509 SK I *qorTdJJ7j/gRRMDskSfOJ40VQ0I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2024-01-24T02:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.20.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified time stamps issued by QTSU DELTA EADTrust*

Name *[es] Sellos electrónicos cualificados de tiempo emitidos por QTSU DELTA EADTrust*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU DELTA EADTrust*

X509SKI

X509 SK I *qorTdJJ7j/gRRMDskSfOJ40VQ0I=*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU EPSILON EADTrust*

Valid from: *Wed Nov 06 12:04:13 CET 2019*

Valid to: *Sun Nov 05 12:04:13 CET 2023*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D3:5B:F8:8A:32:AF:34:6B:EF:68:D0:73:0C:19:14:6F:F9:55:03:30:49:D5:7F:C1:4D:37:75:A0:2A:AF:40:5E:9D:E2:87:32:C4:F8:1E:7D:8E:09:BF:3C:12:FC:A3:A3:1E:85:04:A3:11:85:7F:24:59:B1:8B:50:C1:52:8E:1D:A8:9A:BC:8F:CD:7C:D3:8C:6F:AB:A2:80:E7:77:78:05:68:96:98:4F:C7:50:CD:73:0B:35:87:37:AF:D7:B3:E6:D1:17:DA:D3:FD:7E:CF:25:F2:DE:A6:5E:EE:98:83:60:39:84:ED:49:7B:CB:7B:86:F6:5D:75:EC:50:A6:D6:C2:01:87:79:F1:04:8D:4D:0C:39:CD:F7:56:FC:3B:C4:7F:91:4D:9A:E5:6D:D8:80:3D:E6:33:9A:30:9E:63:83:55:D1:8F:F0:F4:75:7E:40:4B:5C:8C:7E:7C:32:DE:8F:1E:42:5D:A0:9A:BF:4B:FF:36:C4:AC:E1:33:7F:8B:92:A1:B3:01:5C:50:13:34:EB:13:2E:10:65:E6:85:21:E9:3C:78:09:E3:A8:3F:13:8A:45:16:C0:B3:81:C5:87:5D:CB:33:17:ED:A0:E3:14:D6:54:A0:D0:6A:53:4F:28:73:BC:F2:1B:93:D1:C5:99:D0:E5:32:62:EC:DD:D0:D8:CB:A7:02:03:01:00:01

Authority Key Identifier *E7:EB:E9:2F:72:EB:F9:59:BD:7D:50:E9:4E:18:D0:CF:28:59:17:22*

Authority Info Access
http://ca.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crt
http://ocsp.eadtrust.eu

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name
ca@eadtrust.eu
http://ca.eadtrust.eu
http://www.eadtrust.eu
http://policy.eadtrust.eu

Certificate Policies
Policy OID: 1.3.6.1.4.1.501.2.1.1.0.3161
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crl*

Subject Key Identifier *E7:BF:CC:78:34:8F:77:61:9E:4C:5D:61:99:C6:B7:58:33:23:F1:74*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:61:40:20:33:60:08:6C:45:F0:73:77:B8:9C:51:35:C3:AB:5A:C2:C0:09:10:D9:20:1C:92:E8:DB:68:3F:61*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU EPSILON EADTrust*

X509SKI

X509 SK I *57/MeDSPd2GeTF1hmca3WDMj8XQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2024-01-24T02:00:00Z*

Scheme Service Definition URI

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

40.21.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified time stamps issued by QTSU EPSILON EADTrust*

Name *[es] Sellos electrónicos cualificados de tiempo emitidos por QTSU EPSILON EADTrust*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Entity Seal Certificate*

Subject CN: *QTSU EPSILON EADTrust*

X509SKI

X509 SK I	57/MeDSPd2GeTF1hmca3WDMj8XQ=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Status Starting Time	2020-10-05T00:00:00Z

40.22 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 2048

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST
Service type description	[en] A time-stamping generation service creating and signing qualified time-stamps tokens. [es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en] Qualified timestamps issued by EADT QTSU 2023 RSA 2048
Name	[es] Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 RSA 2048

Service digital identities

Certificate fields details

Version:	3
Serial Number:	1776818162991950082017

X509 Certificate	-----BEGIN CERTIFICATE----- MIIRTCB2gAwIBAgIJYFJOMUFNTI/hMA0GCsqGSIb3DOEBCwUAMIGxMUAWPqYDVQOQDDdFQURU cnVzCBU0EgNDAsNi8tdWJDOS8Gbz3gUUVhbGlnaWkiEiNcnR2mijYXRlcjYvMDE5MS8wLQYD VOOKDCZFRjY3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMx GDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEw MjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAy MDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYy Nj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNU IFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyo WGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0 KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8 +IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sg OAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0 LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRw OibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3 dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRy dXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1 hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoET BgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2 BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3 MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBU DBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwv RUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEw IFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwMz0xDTI3MTZmNTYNTkwwMfowgaExDAeBgNVBAMMF0VBRFQvUVRVTSYyMDZlFTQSAyMDQAMH4wHAYDVQDBUDBVSW113RnBKAQO2YyZGltYWNoG0xkGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEZMDQGA1UECwwvRUFETFRSVCVUUEVU9KORUFOIEFRHRSU5DWSBPRBESUDjVEFMFRSVVNUIFNMMSQswCQYDVQOGEwIFUzCCASiWDOYjKozhvcNAOE8BQADgEPADCAQoCgqEBANVWGEpWfyoWGU8vukIurDovksu5S3Me3F8ASISKcr83eivXvU2XXLNMWpjl5mrcTHeIDY8FueGdPvYn h6e69nZ76dRAokpVTFH2fdkPL135mxx44W8t8wxMvdZMrxcidWFDHW+KOY4Kp9BIOUgPVL0KSZzvCY1Yg9o2eTIG3di9THarcljV7v6aSLGxylUirGymBvj1OfT2NjINjWEyPfyEugP57SwV8+IUY4NtATsYWFLv75ZjSw3p0W8WRagBxfxyu5X4htms+M7T73a+J8zSPwSVTbuRwUE DHIDxp6hwkAk72PtnMjDTxOMkCAwEAaOAZwwgoNoMB8GA1UdlwOYMBaAFDEuV+9pL9nrl9sgOAnjhKcsf9FMHoGCCsGAOUFBwEBBG4wdbFBggrBgEFBQcwAqY5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRydXN0LmV1YmN1L2Y2OTZlYWRCdWwTKuY3J0MCMGCSGAOUFBzABhhododHRwOibvZnZccC5IYWR0cnVzdC5ldTBjBgNVHRIEXDBaQ05IYUBIYWR0cnVzdC5ldYYaHR0cDovL3d3dy5IYWR0cnVzdC5ldYYaHR0cDovL2NhLmVhZHRydXN0LmV1hhodHRwOi8vcG9saWN5LmVhZHRydXN0LmV1MGMGA1UdEQRmFzBDMmMQCvZHRydXN0LmV1hhodHRwczovL2NhLmVhZHRydXN0LmV1hhodHRwczovL3d3dy5IYWR0cnVzdC5ldYYaHR0cHM6Ly9wb2xpY3kuZWZkdHJ1c3QuZXUwgoETBgNVHSAEggEKMIIBBjCBkgYNkwYBBAQDQOIBAQCJTCBgDBBggrBgEFBQcCAjBLDElFdxjvcGv bB8Z2Yy3kqb2Y9RGlmaXNkY3B1cnVzCmguY5MjELMAKGA1UEBhMCBVMxGDAWBgNVBGEtMDE2BVEVLU4NTYyNj0MDEVMEMGA1UECwwvMTG5bnVwqUGVyc29uMBA4XDTZMDEwMjE4MDAwM

Issuer CN: *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 RSA 2048*

Valid from: *Mon Jan 02 19:00:00 CET 2023*

Valid to: *Fri Dec 31 23:59:00 CET 2027*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D5:56:18:4A:56:B5:FC:A8:59:05:01:BE:E1:DC:8A:EA:C3:A3:29:2C:B9:2D:D2:37:AD:C5:F0:04:89:49:10:44:AF:C7:12:7A:2F:F1:95:5B:83:95:75:CB:85:63:29:26:14:8D:AE:B0:87:B0:47:C3:63:CA:D4:78:60:E9:15:53:68:87:A7:BA:F6:76:57:EF:A7:51:03:FA:24:A5:54:C5:1F:67:DD:92:92:E5:D7:74:A6:C7:1E:00:5B:CB:7C:C3:13:15:75:93:2B:C4:28:9C:75:61:43:1D:6F:8A:39:8E:0A:A7:D0:62:42:ED:20:3D:52:E8:29:26:73:BC:26:35:62:0F:68:D9:E4:C8:1B:77:48:F5:31:EA:AD:C2:09:57:B8:FA:A9:22:C6:C5:88:94:22:B1:98:98:1B:E3:D4:E7:EB:4F:63:49:24:D2:56:13:2A:45:93:21:14:A8:FE:78:48:05:7C:FA:25:18:C4:DB:78:4D:A6:16:14:8B:FB:E4:96:63:4A:2B:D2:A7:45:BC:59:F4:62:83:A1:71:17:1C:AE:C5:25:F8:86:19:E7:4B:E3:3B:EF:BD:DA:F8:9F:1F:CE:34:8F:C3:D5:53:6E:DB:91:FF:03:04:0C:77:C3:FF:1A:7A:87:09:00:93:8D:8F:4E:73:23:75:35:F3:40:C9:02:03:01:00:01*

Authority Key Identifier *31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*

Authority Info Access *http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt*
http://ocsp.eadtrust.eu

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
https://ca.eadtrust.eu
https://www.eadtrust.eu
https://policy.eadtrust.eu

Certificate Policies *Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.1
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

Subject Key Identifier *A1:2F:86:A4:50:43:86:C6:22:1F:57:A1:63:AB:64:A0:02:F4:3D:05*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2B:B1:B5:AA:39:76:B7:70:E8:74:D9:26:3A:39:6B:ED:F7:04:6C:B7:95:54:70:DA:E
E:DB:37:B9:9D:82:91:67*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 RSA 2048*

X509SKI

X509 SK I *oS+GpFBDhsYiH1ehY6tkoAL0PQU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2023-02-15T00:00:00Z*

40.23 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 3072 ENS alto

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by EADT QTSU 2023 RSA 3072 ENS alto*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 RSA 3072 ENS alto*

Service digital identities**Certificate fields details**

Version: *3*

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name *ca@eadtrust.eu*
https://ca.eadtrust.eu
https://www.eadtrust.eu
https://policy.eadtrust.eu

Certificate Policies *Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.1
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

Subject Key Identifier *B4:D9:8A:48:9A:0F:5C:2B:86:CF:95:B6:76:45:8E:BE:02:8B:1A:E8*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *56:CA:F8:F0:7F:F8:F7:AB:8A:B5:C3:C6:37:AB:24:A9:93:C4:14:C4:9F:B7:FA:5B:D8:F2:6B:44:12:7D:A6:92*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 RSA 3072 ENS alto*

X509SKI

X509 SK I *tNmKSJoPXCuGz5W2dkWOvgKLGug=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*

40.24 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 4096
QSCD ENS alto

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023*
RSA 4096 QSCD ENS alto

Issuer CN:	<i>EADTrust RSA 4096 SubCA For Qualified Certificates 2019</i>
Subject C:	<i>ES</i>
Subject O:	<i>EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL</i>
Subject 2.5.4.97:	<i>VATES-B85626240</i>
Subject OU:	<i>Timestamp Certificate</i>
Subject CN:	<i>EADT QTSU 2023 RSA 4096 QSCD ENS alto</i>
Valid from:	<i>Mon Jan 02 19:00:00 CET 2023</i>
Valid to:	<i>Fri Dec 31 23:59:00 CET 2027</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BB:31:84:5F:30:59:BF:7C:23:AD:A9:3D:F4:A6:94:57:82:E0:6C:07:BC:9C:78: EA:AF:5A:AD:53:96:14:14:AA:04:93:E2:79:09:0F:40:A2:89:9A:D8:3E:E1:BC:BA:FA:16:7D:C1:65:D7:64:08:F3:D7:16:FC:D0:45:60:3D:BD:C8:33:05:6C:64:5B:83:05:00:5D:87:F7:D5:38: 65:C7:26:60:AF:ED:5D:9B:22:11:92:EC:6A:F7:D8:5C:7E:1F:07:79:EA:FD:B4:15:B5:67:5C:C1:4E:3C:CE:D9:C4:7F:88:E9:E8:21:21:2C:43:11:1C:00:E9:0A:7A:7C:3A:5C:F0:01:A0:2F:00:4 2:5F:2F:B4:3F:15:A1:1C:B1:1B:A3:04:92:BD:70:B2:70:43:39:26:CD:AA:CD:AD:28:10:AB:75:AA:13:F1:16:92:26:F9:7F:AD:77:FE:DE:83:82:CE:04:F9:28:48:BA:53:FA:E0:B7:F2:36:BC:BE: F2:6A:77:35:03:80:0B:9F:7E:83:E4:A6:0F:63:CC:DA:45:6A:DA:19:12:CE:8A:0C:DE:45:71:58:5B:A2:3A:B7:4F:C5:FC:43:D3:BD:AB:C6:C0:81:48:5F:CA:0A:4D:33:AB:A5:F3:48:18:52:80: 17:9B:0F:28:1C:69:3D:C0:6C:27:58:20:EA:D0:01:7C:5B:49:A5:96:19:31:D0:F5:5B:01:86:E9:3D:24:C9:24:3B:FE:D8:E0:10:FE:AD:5C:89:5D:D2:A7:70:DE:53:C4:A0:C9:58:C5:5E:D6:B2: 66:FF:BB:FD:F1:3F:D4:A0:85:59:84:8E:AD:15:87:78:3B:C7:91:7A:19:80:63:5C:66:59:18:CA:B0:F3:E4:66:E3:15:4D:4D:36:A5:8D:4A:44:FA:75:68:68:1B:34:34:49:1C:28:52:85:CF:5B:D 8:25:FE:6F:79:4E:6B:FF:ED:8E:BF:5A:51:72:51:53:05:E1:EF:27:8B:8B:86:CB:9B:3E:13:C7:30:E3:66:8B:FE:15:8B:C5:0E:AE:65:28:3D:99:D8:33:06:7B:91:FD:02:57:76:97:9A:87:05:F3:8 8:B4:BF:2E:2A:3D:EB:3D:B3:BD:14:03:D7:91:D7:60:F2:44:9F:C9:28:5B:59:AD:15:BF:19:F1:4C:33:AB:66:07:DD:91:FD:F4:33:5A:43:89:0B:99:85:E9:A5:68:77:AA:A5:73:79:E8:A4:28:E8 :CF:ED:FF:29:27:94:F7:F8:8F:ED:45:2A:13:C7:90:0E:20:7E:84:45:66:7E:F8:AA:5D:A6:3D:60:25:39:36:76:45:B6:12:C1:7A:7A:5A:60:C2:05:FA:5A:A4:43:02:03:01:00:01 </pre>
Authority Key Identifier	<i>31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45</i>
Authority Info Access	<i>http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt</i> <i>http://ocsp.eadtrust.eu</i>
Issuer Alternative Name	<i>ca@eadtrust.eu</i>
Subject Alternative Name	<i>ca@eadtrust.eu</i> <i>https://ca.eadtrust.eu</i> <i>https://www.eadtrust.eu</i> <i>https://policy.eadtrust.eu</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421</i> <i>CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]</i> <i>CPS pointer: http://policy.eadtrust.eu</i> <i>Policy OID: 0.4.0.194112.1.3</i> <i>CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_RetentionPeriod: 15</i> <i>id_etsi_qcs_QcSSCD</i>
CRL Distribution Points	<i>http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl</i>

Subject Key Identifier *DF:4B:77:3C:A1:3C:FC:14:2C:CF:AD:54:34:AB:84:B3:D2:B2:09:76*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *77:B8:F4:FA:24:32:0E:AB:C0:FB:D1:4A:F7:B5:5C:C7:89:55:FA:82:EF:94:36:B5:ED:A4:AF:3F:BE:4D:CD:C6*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 RSA 4096 QSCD ENS alto*

X509SKI

X509 SK I *30t3PKE8/BQsz61UNKuEs9KyCXY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2023-02-15T00:00:00Z*

40.25 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 ECC 256 ENS alto

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified timestamps issued by EADT QTSU 2023 ECC 256 ENS alto*

Name *[es]* *Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 ECC 256 ENS alto*

Service digital identities**Certificate fields details**

[illegible]

Subject Alternative Name *ca@eadtrust.eu*
https://ca.eadtrust.eu
https://www.eadtrust.eu
https://policy.eadtrust.eu

Certificate Policies *Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.1
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-ecc256eadlp2019.crl*

Subject Key Identifier *33:10:30:38:C8:64:4A:51:4E:B0:0D:08:E6:01:69:66:73:AA:CC:DD*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *03:42:82:8B:B5:28:1C:F3:0B:D9:AF:F5:09:2A:76:1A:8A:FB:E2:1D:37:07:86:6C:28:94:57:19:87:99:2C:48*

X509SubjectName

Subject C: *ES*
Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*
Subject 2.5.4.97: *VATES-B85626240*
Subject OU: *Timestamp Certificate*
Subject CN: *EADT QTSU 2023 ECC 256 ENS alto*

X509SKI

X509 SK I *MxAwOMhkSIFOsA0I5gFpZnOqzN0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

40.26 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 ECC 384
QSCD ENS alto

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by EADT QTSU 2023 ECC 384 QSCD ENS altc

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023
ECC 384 QSCD ENS alto*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 133127642285963800762

[illegible]

Signature algorithm: *SHA384withECDSA*

Issuer OU: *Legal Person*

Issuer 2.5.4.97: *VATES-B85626240*

Issuer C: *ES*

Issuer O: *European Agency of Digital Trust, S.L.*

Issuer CN: *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

Subject C: *ES*

Subject 0: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 ECC 384 QSCD ENS alto*

Valid from: *Mon Jan 02 19:00:00 CET 2023*

Valid to: *Fri Dec 31 23:59:00 CET 2027*

Public Key:
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:D5:FF:FC:3A:D5:6D:AE:4C:9D:62:00:36:EA:B3:48:A0:4F:86:5C:BE:44:F0:60:68:0D:3D:B2:0E:F3:3A:57:7F:37:66:7A:E5:17:5B:9F:36:F8:B9:D2:C4:D4:A3:6C:A8:8E:2B:1A:C0:CC:C3:B4:33:2A:4B:57:20:58:ED:FC:AE:D8:46:3D:F1:92:E5:A2:C3:96:18:4F:9B:4C:DC:22:3A:FB:C0:E2:06:C9:B6:4A:58:8B:68:C0:B9:FE:55:F8:3A

Authority Key Identifier *5C:19:E2:AB:1D:B6:B8:3D:45:12:91:92:1B:8C:14:71:D8:E8:F5:F6*

Authority Info Access
http://ca.eadtrust.eu/eadtrust-subca-ecc384eadlp2019.crt
http://ocsp.eadtrust.eu

Issuer Alternative Name *ca@eadtrust.eu*

Subject Alternative Name
ca@eadtrust.eu
https://ca.eadtrust.eu
https://www.eadtrust.eu
https://policy.eadtrust.eu

Certificate Policies
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]
CPS pointer: http://policy.eadtrust.eu
Policy OID: 0.4.0.194112.1.3
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false
id_etsi_qcs_QcCompliance
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.eadtrust.eu/eadtrust-subca-ecc384eadlp2019.crl*

Subject Key Identifier *ED:42:4A:85:DC:AF:F7:17:91:DE:8C:E8:C9:9C:4B:5D:9D:64:32:12*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *3E:A4:70:EB:D9:06:AB:C6:F0:15:7E:6C:63:06:A2:7D:F6:AB:03:8A:82:63:79:21:11:3A:C6:F1:4A:87:53:CB*

X509SubjectName

Subject C: *ES*

Subject O: *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

Subject 2.5.4.97: *VATES-B85626240*

Subject OU: *Timestamp Certificate*

Subject CN: *EADT QTSU 2023 ECC 384 QSCD ENS alto*

X509SKI

X509 SK I *7UJKhdyv9xeR3ozoyZxLXZ1kMhl=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2023-02-15T00:00:00Z

40.27 - Service (granted): Qualified Certificates issued by EAD Trust ECC 256 SubCA For Qualified Web DV/OV Cert 2024

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by EAD Trust ECC 256 SubCA For Qualified Web DV/OV Cert 2024*

Name [es] *Certificados cualificados emitidos por EAD Trust ECC 256 SubCA For Qualified Web DV/OV Cert 2024*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *8468024348210595411*

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDzCCAs2gAwIBAgIdYR3R3hzhIMwCgYIKoZIzj0EAwIwZELMAkGA1UEBhMCRVVMEjAQBQNV
BAoMClVBRCBKcnVzdDFEMEIGA1UEAw7RUFEFRydXN0IEVDQyAyNTYgUm9vdCBDO5BGB3lgUXVh
bGlnaWVkdFdyBE9PVlBDO2XlODIwMjQwMjYxMTE0MTE0MTE0MTE0MTE0MTE0MTE0MTE0MTE0
WlBIMQswCOYDVOQGEWJFUEZSMBAG1UECgwlRUFEFRydXN0MjYxMTE0MTE0MTE0MTE0MTE0MTE0
RUNDID11NiBtdWIDQ5BGB3lgUXVhbnGlnaWVkdFdyBE9PVlBDO2XlODIwMjQwMjYxMTE0MTE0
POlBBGgqkIOPOMBwNCAAD3ggU+YHs4I8kqF9ds9pToSdLLJEVC3c8DeisXk2TRTbNi8j
u56RYTCAIng06aO+P47OFLpXSpDca4l8YCCAV8wEQYDVR0gBAowCDAGBGRVHSAAMBIGA1Ud
EwEbiwQIMAYBARCAQAwDgYDVDR0PAAQIBAQDApGGMBOGA1UdDgQWBBOIYNslydBJPLY2SC9hoOej
edima2fBgIWNISMEDAwgBQXnzW946b8KuhmWu1gTV5d1YcB8L8gNVHRBERDCCMECgPgA8hjp0
dHRwOi8vY3JslmVhZHRydXN0LmV1L2VhZHRydXN0LXljb3QZWNjMjU2ZWZkZHZydjIwMjY3Is
MHoGCCsGAQUFBwEBBgG4wbDBFgggrBgEFFBQcAwAcy5aHR0cDovL2NhLmVhZHRydXN0LmV1L2VhZHRy
dXN0LXljb3QZWNjMjU2ZWZkZHZydjIwMjY3Ij0MCMGCCsGAQUFBzABhndodHRwOi8vbnV5Z2ZzcSI
YWR0cnVzdC5ldAdBgNVHSEUFEJAUBggrBgEFFBQcDAQYIKwYBBQUHAwIwCgYIKoZIzj0EAwIDSAAw
ROlgFw9GEM61s04HDSYJQhlgB7HFPZK/kUsJNUc+V7zxcCIQDpKqFbiUR8bRK04vMQKwcE+7ii
FhA0K9xNASj9I5kLQ==

```

-----END CERTIFICATE-----

Signature algorithm:

SHA256withECDSA

Issuer CN:

EAD Trust ECC 256 Root CA For Qualified Web DV/OV Cert 2024

Issuer O:

EAD Trust

Issuer C:

ES

Subject CN:

EAD Trust ECC 256 SubCA For Qualified Web DV/OV Cert 2024

Subject O:

EAD Trust

Subject C:

ES

Valid from:

Fri Nov 22 12:42:10 CET 2024

Valid to:

Wed Nov 19 12:42:10 CET 2036

Public Key:

```

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:37:A6:0D:21:FB:21:EC:1F:C8:24:A8:5F:5D:49:EA:53:A3:F4:9D:FC:B2:C9:11:50:B7:73:C6:83:7A
:36:31:2B:34:DF:45:36:CD:88:18:C8:B8:9E:91:61:85:42:00:D9:E0:D3:A6:8E:F8:F8:B8:EF:F4:05:2C:5A:97:4A:00:DC

```

Certificate Policies

Policy OID: 2.5.29.32.0

Basic Constraints

IsCA: true - Path length: 0

Subject Key Identifier

08:60:D4:8B:61:D0:63:3C:B6:33:48:2F:61:A0:E7:A3:79:D8:A7:8B

Authority Key Identifier

17:87:35:BD:03:A6:C1:91:1B:87:99:6B:B5:81:35:79:76:B6:1C:06

CRL Distribution Points

http://crl.eadtrust.eu/eadtrust-root-ecc256eaddvov2024.crl

Authority Info Access

http://ca.eadtrust.eu/eadtrust-root-ecc256eaddvov2024.crt

http://ocsp.eadtrust.eu

Extended Key Usage

id_kp_serverAuth

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

```

45:9E:0F:12:A7:72:3F:40:C7:18:A3:72:18:62:74:7C:9A:28:94:A8:72:1D:50:FE:6B
:A4:E2:2B:EC:49:31:3C

```

X509SubjectName

Subject CN: EAD Trust ECC 256 SubCA For Qualified Web DV/OV Cert 2024

Subject O: EAD Trust

Subject C: ES

X509SKI

X509 SK I CGDUI2HQYzy2M0gvYaDno3nYp4s=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2026-02-26T03:00:00Z

40.27.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.28 - Service (granted): Qualified Certificates issued by EAD Trust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2024

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EAD Trust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2024

Name [es] Certificados cualificados emitidos por EAD Trust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 3835103727180920937

[illegible]

-----END CERTIFICATE-----

SHA256withECDSA

EAD Trust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2024

EAD Trust

ES

EAD Trust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2024

FAD Trust

ES

Fri Nov 22 12:58:13 CET 2024

Wed Nov 19 12:58:13 CET 2036

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:77:82:63:66:01:EE:D3:D4:8B:E2:FE:33:9A:2D:93:C1:3B:42:C1:2F:50:75:DC:88:49:60:F0:8B:C8:1B:F7:C8:8F:F0:F0:19:31:C7:D9:94:1F:74:27:F0:A3:0F:3A:84:F2:CC:47:77:57:56:CE:C7:38:45:02:1F:90:25:65:3F

Policy OID: 2.5.29.32.0

IsCA: true - Path length: 0

D1:94:6B:39:01:6D:AF:B4:D1:8E:04:D0:11:02:BC:4A:95:F7:D0:EB

52:A7:11:29:2E:DB:62:4B:4D:94:A0:65:C7:E5:D1:96:87:9B:8D:A7

<http://crl.eadtrust.eu/eadtrust-root-ecc256eadevpsd22024.crl>

<http://ca.eadtrust.eu/eadtrust-root-ecc256eadevpsd22024.crt>

<http://ocsp.eadtrust.eu>

```
id kp serverAuth
```

digitalSignature - *keyCertSign* - *cRLSign*

SHA-256

62:84:C3:D2:BB:5E:4A:6A:55:51:13:5E:8F:54:C6:25:85:44:5C:1A:56:27:24:C7:C0
:D5:07:38:9B:A5:57:C2

Subject CN: EAD Trust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2024

Subject O: EAD Trust

Subject C: ES

X509SKI

X509 SK I 0ZRrOQFtr7TRjgTQEQK8SpX30Os=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2026-02-26T03:00:00Z

40.28.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.29 - Service (granted): Qualified Certificates issued by EAD Trust ECC 384 SubCA For Qualified Web DV/OV Cert 2024

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EAD Trust ECC 384 SubCA For Qualified Web DV/OV Cert 2024

Name [es] Certificados cualificados emitidos por EAD Trust ECC 384 SubCA For Qualified Web DV/OV Cert 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 180514071555089543

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIDZCCAuggAwIBAgIIAoFQl3gAlIcwCgYIKoZIzj0EAwMwZzELMAkGA1UEBhMCRVVMEjAQBQNV
BAQMCUVBRCBKcnVzdDFEMEIGA1UEAww7RUFEFRydXN0IEVDQyAzODQgUm9vdCBQDQSGb3IglUUVh
bGimaWVvFdyBEV9PVjBDZXI0IDlwMjQwMjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
WjBIMCswCQYDVOQGEWjFUEZSMBAUUECgWjRUEFRydXN0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
RUNDIDM4NCBtdWJ0QSBGbz3IglUUVhGimaWVvFdyBEV9PVjBDZXI0IDlwMjQwMjE0MjE0MjE0MjE0
POBBBgUigQQAgnIAAOh9UHV0L+xtHfGwykucEmhBOM4C84ZLvJLB962Ph6d9VnAdq
Fm1UATUBXg+RrEFNDLRq+U3A1TtNCZ+JagQo7y7ZR8mvXktY13k6aDeO5ALC5Hr+Jggf
MIIBZARBgNVHSAECAIMAYGBFUDIAAwEgYDVROTAQHBAQw8gEB/wBADAQBgNVHQ8BAQEBAQMC
ATYWHQYDVRO0BBEFGGdR2ikuj9JwLtwVGFjOTB249ZMB8GA1UdHwQIMBAFlnR0R0loxt+3Z2b
YtaotU/N5OwmMEGA1UdHwREMEIwQK+cdYgOmh0dHA6Ly9icmwwZWZkdHJlC3QzXUZXVWZWFkdHJl
C30tm9vdC1Y2MzODRlYWRkd92MjA5NC5jcmwwegYKwYBBQUHAEQEBjBsMEUGCCsGAOUFBzAC
hJodHRwOi8vY2EuzWFKdHJlC3QzXUZXVWZWFkdHJlC30tm9vdC1Y2MzODRlYWRkd92MjA5NC5j
cmwwYKwYBBQUHMAAGCF2hd0HA6Ly9vY3NwLmVhZHRydXN0LmV1MB0GA1UdJQQOMW0GCCsGAQUF
BwMBBggrBgEFBQcDAjAKBggghkiOPOODAwNoADBlAEArMpgtr+y3wUTAF+IEGn0b0oVw+ezd8
NC2xdlWgpmEHGx25EIAWICOhZZYIAjBEY6XwNodTzR2R0YCTHlPhsYzJrwi+Q3IH0Y18
sMnQGM5UBShmwOm2dsG7Gbk=

```

-----END CERTIFICATE-----

Signature algorithm:*SHA384withECDSA***Issuer CN:***EAD Trust ECC 384 Root CA For Qualified Web DV/OV Cert 2024***Issuer O:***EAD Trust***Issuer C:***ES***Subject CN:***EAD Trust ECC 384 SubCA For Qualified Web DV/OV Cert 2024***Subject O:***EAD Trust***Subject C:***ES***Valid from:***Fri Nov 22 12:42:20 CET 2024***Valid to:***Wed Nov 19 12:42:20 CET 2036***Public Key:**

```

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:28:81:04:00:22:03:62:00:04:07:F5:48:67:FE:87:D0:20:BF:B1:9F:87:E0:58:2C:6E:BD:C1:26:84:14:0C:23:80:BC:E1:91:AF:24:80:7D:E9:
93:E1:FF:A7:62:F6:D5:66:00:38:AA:16:6D:62:01:35:01:C5:78:3E:69:18:44:14:D0:CB:46:A8:FE:53:70:35:7C:9B:4D:73:32:3E:D9:A1:90:A3:88:B2:ED:94:41:9A:F5:E4:B5:8D:79:93:A6:8
3:78:EB:00:2D:CE:5F:1E:BF

```

Certificate Policies*Policy OID: 2.5.29.32.0***Basic Constraints***IsCA: true - Path length: 0***Subject Key Identifier***61:9D:47:69:64:B8:9F:49:C0:B9:F0:BC:61:63:FC:34:FC:CF:8F:59***Authority Key Identifier***B9:D1:45:08:65:A3:14:FE:75:96:5B:61:36:A8:7E:EF:CD:E5:0C:26***CRL Distribution Points***http://crl.eadtrust.eu/eadtrust-root-ecc384eaddvov2024.crl***Authority Info Access***http://ca.eadtrust.eu/eadtrust-root-ecc384eaddvov2024.crt**http://ocsp.eadtrust.eu***Extended Key Usage***id_kp_serverAuth***Key Usage:***digitalSignature - keyCertSign - cRLSign***Thumbprint algorithm:***SHA-256***Thumbprint:***14:85:B4:A7:DE:D0:10:28:14:02:A5:43:DE:B6:4E:77:F6:65:5D:E0:8F:FD:E3:8B:6
6:16:E2:6B:20:25:FA:1F***X509SubjectName**

Subject CN: EAD Trust ECC 384 SubCA For Qualified Web DV/OV Cert 2024

Subject O: EAD Trust

Subject C: ES

X509SKI

X509 SK I YZ1HaWS4n0nAufC8YWP8NPzPj1k=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2026-02-26T03:00:00Z

40.29.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.30 - Service (granted): Qualified Certificates issued by EAD Trust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2024

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EAD Trust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2024

Name [es] Certificados cualificados emitidos por EAD Trust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1384859187924174929

[illegible]

-----END CERTIFICATE-----

SHA384withECDSA

EAD Trust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2024

EAD Trust

ES

EAD Trust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2024

EAD Trust

ES

Fri Nov 22 12:58:20 CET 2024

Wed Nov 19 12:58:20 CET 2036

30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:1D:40:02:AA:7C:B3:7D:8B:80:85:45:1A:09:0B:7B:F9:D9:71:7A:72:A5:5E:0E:7A:22:20:CE:73:97:AF:EB:35:EB:02:3B:9A:94:8A:14:CB:03:A3:8A:12:48:B4:04:6C:8E:24:CD:BD:B1:45:60:4F:3B:5F:42:F6:58:3A:AF:5B:1F:48:E1:C3:02:D7:03:A3:08:BE:52:CD:07:36:BF:D9:4E:32:BD:6D:4A:44:0F:0A:A9:96:9E:03:2F:15:24

Policy OID: 2.5.29.32.0

IsCA: true - Path length: 0

0B:93:22:F1:EF:DF:60:EF:65:F3:11:13:36:47:6F:87:43:FB:23:D5

F3:1D:CF:8F:AA:5C:06:D1:17:29:EA:F5:A6:C3:77:BD:F2:5E:74:F5

<http://crl.eadtrust.eu/eadtrust-root-ecc384eadevpsd22024.crl>

<http://ca.eadtrust.eu/eadtrust-root-ecc384eadevpsd22024.crt>

<http://ocsp.eadtrust.eu>

```
id kp serverAuth
```

digitalSignature - *keyCertSign* - *cRLSign*

SHA-256

38:45:F5:6E:3F:6C:15:0E:2F:B5:72:D6:2F:8C:61:BA:7D:9A:16:4E:45:67:7E:B7:19
98:C4:71:B7:58:C3:9F

Subject CN: EAD Trust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2024

Subject O: EAD Trust

Subject C: ES

X509SKI

X509 SK I C5Mi8e/fYO9l8xETNkdvh0P7l9U=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2026-02-26T03:00:00Z

40.30.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

40.31 - Service (granted): Qualified Certificates issued by EAD Trust RSA 4096 SubCA For Qualified Web DV/OV Cert 2024

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by EAD Trust RSA 4096 SubCA For Qualified Web DV/OV Cert 2024

Name [es] Certificados cualificados emitidos por EAD Trust RSA 4096 SubCA For Qualified Web DV/OV Cert 2024

Service digital identities

Certificate fields details

Version: 3

Serial Number: 8581064901047513491

Thumbprint algorithm: *SHA-256*

Thumbprint: *F5:6A:99:F8:A7:B4:DC:80:7F:23:C7:23:EB:62:0A:C2:96:D9:80:BD:E1:43:E3:17:E1:8E:B6:4E:B5:6F:F6:CE*

X509SubjectName

Subject CN: *EAD Trust RSA 4096 SubCA For Qualified Web DV/OV Cert 2024*

Subject O: *EAD Trust*

Subject C: *ES*

X509SKI

X509 SK I *hkmNXNRzGyDmvCmk4m33YcCUKgo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2026-02-26T03:00:00Z*

40.31.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.32 - Service (granted): Qualified Certificates issued by EAD Trust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2024

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name [en] *Qualified Certificates issued by EAD Trust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2024*

Name [es] *Certificados cualificados emitidos por EAD Trust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2024*

Service digital identities

Authority Info Access *http://ca.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22024.crt*
http://ocsp.eadtrust.eu

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C3:B2:8B:A9:15:38:23:BD:E1:98:A6:65:EB:35:C3:DD:F8:D3:DF:FA:F7:37:10:95:1C:E3:AF:97:BA:8D:1B:3A*

X509SubjectName

Subject CN: *EAD Trust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2024*

Subject O: *EAD Trust*

Subject C: *ES*

X509SKI

X509 SK I *b/ltZtjaDJqpFkarQH0VenJVuz0=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2026-02-26T03:00:00Z*

40.32.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

40.33 - Service (granted): Qualified Certificates issued by EAD Trust RSA 8192 SubCA For Qualified Web DV/OV Cert 2024**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Certificate fields details

Serial Number: 1266733156385493048

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *EAD Trust RSA 8192 Root CA For Qualified Web DV/OV Cert 2024*

Issuer 0: *EAD Trust*

Issuer C: *ES*

Subject CN: *EAD Trust RSA 8192 SubCA For Qualified Web DV/OV Cert 2024*

Subject O: *EAD Trust*

Subject C: *ES*Valid from: *Fri Nov 22 12:41:57 CET 2024*

Valid to: Wed Nov 19 12:41:57 CET 2036

Public Key:	30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:D7:F8:DF:FD:DB:C3:80:55:94:CF:F2:71:3A:28:C2:16:0A:01:33:E6:61:AA:F7:7C:54:90:E3:78:70:D1:9F:CA:74:61:54:0C:D8:7A:18:EE:1F:D6:19:C5:03:98:F7:99:6C:18:93:17:00:AA:D0:88:D8:D8:C3:02:29:04:03:71:7E:92:79:55:9A:9F:F7:EA:CB:7C:A2:2A:78:59:4E:4F:7C:E1:19:23:A6:AE:07:E1:93:2F:3F:86:FC:58:63:44:8E:C5:D7:70:80:34:C6:07:6C:92:19:80:D5:52:E2:98:6D:63:D1:6A:40:1D:32:FC:2A:6A:18:20:60:11:40:66:7E:78:C6:1A:74:4B:67:15:97:9A:BA:A2:14:0C:8E:C4:CF:91:CC:34:DD:27:C4:7B:1E:FC:DA:D1:C5:51:E7:06:C4:F5:95:83:42:0E:FE:B2:70:55:29:F8:D8:A3:EF:3D:0B:B2:A8:C8:23:14:7D:00:F8:B4:95:0B:74:0C:05:22:15:90:56:1F:51:A1:26:58:F8:9F:6C:23:06:E4:ED:6D:08:A0:D5:01:F8:1B:43:00:D8:52:C0:56:C6:16:AB:0A:DA:B4:18:DB:81:96:D1:8E:A7:A3:A6:EA:FF:F3:9C:E4:82:EC:46:9A:8F:29:2D:E4:8A:91:E1:2F:00:5E:58:EC:24:DF:FF:E5:91:05:EE:2D:58:4A:95:7C:D6:43:E0:42:44:82:6E:77:8C:6F:DE:A6:E6:01:BE:11:48:08:40:6C:F0:C3:9F:58:9C:4C:74:2B:1F:F0:0A:3A:D7:86:54:E3:A7:F0:A2:20:7F:55:9E:4E:C4:39:63:45:87:78:C2:68:58:91:CF:26:31:DB:EB:F7:BA:A8:52:A5:AF:3F:05:01:53:36:E6:CB:1A:AB:C8:C8:0D:3E:38:45:F5:04:24:21:E8:C0:77:75:0A:F3:45:EA:73:63:6F:EF:55:70:CE:89:15:53:3A:99:AA:59:1E:29:D8:E2:64:E2:A2:20:3C:9E:98:98:35:A0:5D:D4:29:CF:20:3F:8B:5A:C5:10:C3:B6:AF:65:A9:5F:83:78:95:91:9F:2E:40:36:C6:8A:7D:0C:A4:8A:FB:08:9F:8C:B9:6A:A8:67:DC:36:6D:8C:48:8C:17:9A:0C:93:AC:0A:74:2C:59:32:0D:45:4B:DB:E9:0A:D1:CF:B2:A5:68:7D:56:75:FA:BE:47:01:3B:FF:08:AF:C2:00:6D:F6:BE:28:9F:79:81:16:63:DC:89:03:4F:3E:8B:C6:68:27:57:72:89:C6:CA:F9:57:3B:39:97:E5:E0:05:14:EE:7F:F5:FF:7D:F4:8B:8A:D3:A3:6F:4B:E2:30:71:C4:55:BF:20:79:BA:85:3C:F3:1A:15:FE:93:C1:78:F4:31:FA:1C:CF:EC:32:B8:AE:D2:CF:1B:52:A0:D5:42:85:74:C3:CA:74:C5:B8:20:23:A2:48:FE:7A:A7:55:9E:D8:A9:15:CC:3C:76:4F:BA:56:03:10:D7:01:64:24:C4:E1:5A:DD:55:06:11:CF:D0:18:89:54:ED:B8:E0:A4:D4:DF:C2:86:A3:A0:1A:1A:38:6D:01:58:0F:F5:2A:05:19:90:78:71:D4:34:0A:68:78:29:2D:99:B8:EF:0B:87:0D:B7:F9:83:54:F8:E6:C5:5F:B6:D4:49:15:A1:0C:E7:E6:68:10:59:AC:1F:88:B8:DA:07:D2:F4:E0:EC:4B:48:78:D4:88:EB:7A:7B:3B:9A:42:FA:02:CC:EE:73:D9:F2:0D:69:17:53:1E:52:40:C2:6B:87:C5:A8:2C:60:24:C3:94:72:8F:2E:FC:BF:89:3D:51:49:A6:94:BC:A4:6C:0E:48:3D:5F:DA:7D:D1:3E:87:73:44:0E:2F:EF:7A:72:5E:BD:76:60:0E:3B:06:84:59:DE:A3:65:37:E0:C2:5E:18:9D:32:57:CC:5A:5C:A9:49:60:73:FA:7D:77:26:19:0C:DF:C0:33:95:63:75:A9:15:23:F9:2F:B0:33:78:0E:46:78:75:7E:5C:E4:06:47:8E:C5:37:11:B1:C8:6F:12:69:2D:55:1C:62:D3:60:C3:1B:BF:13:7E:27:F9:E0:4D:02:2A:C9:A1:D4:47:BE:35:79:19:70:A1:21:81:4E:70:8C:AA:DC:E3:15:E1:97:EC:0F:82:12:A3:38:FC:01:FA:EF:34:DC:75:C2:3F:6E:16:77:CABF:7D:5D:58:F4:FD:CA:05:1F:09:AA:23:EF:8E:AA:B4:FC:91:36:FA:EA:A3:E7:72:82:D6:1D:8B:8B:EF:EF:E3:DE:61:D7:FD:8D:94:5D:68:49:FD:6B:E7:EE:4D:F0:84:20:F7:B2:41:7A:C1:45:7A:16:76:8F:95:6F:0C:1F:68:6D:4B:69:8F:56:71:F2:B8:F1:B6:97:59:B2:62:28:2A:D2:79:CF:F8:A2:D8:FA:58:93:D9:F3:18:F8:66:65:D9:79:64:21:81:AD:C9:3E:87:6B:9B:5C:F8:59:9F:E7:61:57:6D:A9:9F:4A:BE:2D:09:4D:29:F2:37:15:01:F4:F2:9C:AA:9A:67:63:71:7A:80:44:1A:FF:96:2F:37:0D:91:45:F1:16:D5:20:4A:2B:5C:EE:20:AB:DC:AF:54:3C:42:1A:0C:A7:6E:D8:1C:26:9C:F7:41:C2:62:58:03:84:1A:7C:C3:23:EF:6D:14:C8:02:03:01:00:01
Certificate Policies	Policy OID: 2.5.29.32.0
Basic Constraints	IsCA: true - Path length: 0
Subject Key Identifier	B5:EF:AE:01:35:E2:50:E7:B7:E5:B8:25:99:13:B4:33:87:90:06:07
Authority Key Identifier	2B:BC:08:72:2B:4C:0A:57:9A:FB:A9:AE:39:CC:E4:52:88:EA:BD:6E
CRL Distribution Points	http://crl.eadtrust.eu/eadtrust-root-rsa8192eaddvov2024.crl
Authority Info Access	http://ca.eadtrust.eu/eadtrust-root-rsa8192eaddvov2024.crt http://ocsp.eadtrust.eu
Extended Key Usage	id_kp_serverAuth
Key Usage:	digitalSignature - keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256
Thumbprint:	4B:4C:8E:AC:32:77:60:E8:7F:C9:25:66:C9:06:5A:7C:C6:10:9F:DD:E0:2B:A1:72:66:21:CE:37:30:13:20:80
X509SubjectName	
Subject CN:	EAD Trust RSA 8192 SubCA For Qualified Web DV/OV Cert 2024
Subject O:	EAD Trust
Subject C:	ES
X509SKI	
X509 SK I	te+uATXiUOe35bglmR00M4eQBgc=
Service Status	
Service status description	[en] undefined. [es] undefined.
Status Starting Time	2026-02-26T03:00:00Z
40.33.1 - Extension (critical): additionalServiceInformation	

Issuer C: *ES*

Subject CN: *EAD Trust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2024*

Subject O: *EAD Trust*

Subject C: *ES*

Valid from: *Fri Nov 22 12:57:59 CET 2024*

Valid to: *Wed Nov 19 12:57:59 CET 2036*

Public Key:

```

30:82:04:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:04:0F:00:30:82:04:0A:02:82:04:01:00:D1:97:A8:22:5F:68:C6:93:A2:29:BD:D3:38:3A:D2:58:F0:2C:F0:23:FF:C4:84:
63:F4:31:7A:2A:48:03:9A:06:72:E8:DC:AC:C1:AA:F8:35:8D:5B:C9:0F:83:EB:85:18:B4:AE:DD:94:7D:EE:D7:5A:7D:C3:93:9B:50:4F:7B:E0:24:23:9F:E8:CA:9A:43:89:AE:59:01:5C:E0:A9:
AA:AD:4A:27:96:99:13:28:85:AA:70:4D:AD:58:F8:CF:D4:FA:DC:3E:5B:0E:0D:A9:87:70:F7:5B:66:FC:84:0E:FA:F3:4E:9F:10:52:9A:55:E5:25:80:F3:93:E9:41:A7:2D:20:53:E9:D1:38:F2:08
:47:A3:9A:3A:9C:4D:6C:BD:19:2C:59:CA:A2:C6:5E:CA:68:2E:F6:F9:5B:9C:6C:AC:6C:E1:96:BB:C7:32:A7:E0:94:E8:6A:04:C3:31:7E:1E:26:28:9C:8E:C6:EA:0C:D6:6C:9F:C7:82:60:1C:D1:
E0:3E:F8:0D:F0:A5:9F:07:53:55:46:FE:32:62:18:C2:E7:93:CC:83:D8:E3:43:CD:44:23:20:30:87:7D:05:BD:DE:3A:E6:EE:D6:2A:F3:A5:41:88:84:7D:AD:FF:8C:80:DD:DB:C4:1B:25:07:DD:
AA:E7:8C:30:53:76:5F:70:C5:4D:DD:5C:0F:F2:04:92:50:D9:B9:23:9D:41:CA:BE:23:59:D5:EA:E4:08:7D:DB:45:19:70:C1:11:0C:8C:7F:15:A1:E7:7F:D9:E3:09:3F:A8:37:13:A5:17:80:27:A
D:F7:DE:C7:37:8A:A2:9C:38:B6:BD:D1:EE:CF:F7:6C:53:06:38:44:0B:4F:27:29:D5:48:F3:AF:78:CC:03:49:C6:64:37:81:B6:AA:C5:51:51:29:33:21:C9:FE:7B:F7:3D:CD:94:6A:2C:A2:A2:AB
:24:20:3C:D1:A4:08:EB:7A:E6:DF:04:51:1E:BB:7A:53:F2:25:94:CA:02:16:5D:F3:CC:60:8F:99:67:00:8A:08:07:D6:B8:E5:0E:B3:81:3A:46:82:C5:2E:CB:48:0A:A3:32:9A:3F:68:B5:D2:FE
B2:38:BD:28:5F:B1:9C:A0:42:25:8E:B1:A7:51:13:83:D2:06:70:DD:CB:73:D6:22:B8:E3:87:6A:0C:5A:04:DB:60:EB:38:25:E5:BD:73:87:39:B9:9F:4E:88:43:C4:CC:98:8E:EF:47:70:38:F2:8
1:C3:6A:18:D6:E3:A8:48:5C:E2:98:2A:60:1C:73:9F:C9:D5:DF:CB:0E:A0:48:C5:6D:95:D3:56:A7:95:5E:A9:0C:EB:8E:58:88:B5:67:E1:7B:0E:11:C4:C6:CC:80:8F:57:79:48:55:7E:89:15:C5
:17:EB:73:3C:34:6D:F3:19:FA:6B:F9:81:EB:08:E2:EE:AF:98:3E:90:C7:04:55:1E:92:E9:DC:88:C7:0A:0B:6E:2C:1C:66:33:CF:88:A3:61:34:78:1B:E9:98:59:29:07:7A:F6:2C:3C:8A:44:82:6
A:85:50:26:50:BE:F2:A8:6C:83:CE:AC:2D:BE:AC:12:8F:80:C9:2B:A3:F2:9D:E4:00:49:F6:86:22:82:45:5C:8E:A3:4E:F8:98:D0:73:5C:A3:1A:88:4E:33:32:C3:67:91:58:23:1A:35:76:38:
F3:33:4F:68:E7:25:5A:0F:D2:35:ED:76:80:ED:FE:DB:98:13:4E:FC:D8:9A:3A:3F:EB:8D:B2:4C:1D:27:61:45:9F:D1:E0:2D:8E:28:5E:3B:78:97:1D:2A:02:05:9A:25:10:DB:22:DF:AD:F9:87:0
D:09:76:31:27:B9:48:05:F7:63:7E:1A:66:33:24:47:2B:5E:5A:28:04:79:00:41:7F:2D:6E:51:68:67:04:A9:C2:62:C9:AD:77:16:29:A2:DB:56:54:04:5F:A4:3C:69:F7:63:C5:A4:3C:02:4B:23:
D8:A9:DB:98:81:A4:9C:E4:89:20:70:95:F0:FD:52:4E:4E:B6:D2:5F:A8:9E:68:13:6E:8F:0C:90:30:F7:4E:75:4D:2A:C1:6E:67:D0:81:2D:B7:77:D8:A0:8B:4A:F2:A2:B5:01:5C:37:50:8E:77:5
5:66:D0:DD:3C:81:A9:DC:53:4F:86:66:B9:01:95:07:EC:A3:65:24:2E:A1:0E:62:2E:CA:F1:2A:98:85:D7:E9:F9:35:C8:C1:DF:98:8D:20:18:AB:26:C5:45:E1:98:34:8D:D0:B9:E1:54:49:78:A9
:58:45:C0:37:F2:87:7F:55:5B:0F:B8:29:F1:3D:01:E5:6E:8D:6E:6C:1B:5A:AE:A8:99:76:64:EB:80:6F:D3:6F:69:C8:09:CD:F7:C2:CB:6A:9A:C3:31:F8:8F:1E:4F:92:A1:0C:36:4B:E6:91:81:C
2:0E:E3:FD:3D:8E:7C:7F:FE:04:A8:74:47:80:6F:CD:DF:2F:FA:6A:31:BA:64:6F:AE:37:73:08:33:4C:32:C0:3C:42:64:B9:F5:41:58:31:13:13:54:9F:0F:17:36:54:03:72:6C:D6:DE:AA:94:AE:9
0:F4:D8:63:F1:DC:93:DE:F5:01:CB:DA:60:15:16:C2:78:E7:27:42:46:FE:54:D4:F4:80:A7:9F:BD:20:CA:35:37:5B:86:39:5C:5E:FF:53:32:F0:80:09:78:E6:F9:9D:8C:5E:5D:FD:11:DB:1E:6D:
8A:38:59:02:03:01:00:01

```

Certificate Policies *Policy OID: 2.5.29.32.0*

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *1A:C1:7A:4D:1A:FB:EB:8D:95:6C:3A:A5:98:43:A6:6A:41:84:A6:51*

Authority Key Identifier *11:7F:B5:2B:07:48:10:B8:ED:48:09:94:AF:24:B9:F1:3B:07:43:D7*

CRL Distribution Points *<http://crl.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22024.crl>*

Authority Info Access *<http://ca.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22024.crt>
<http://ocsp.eadtrust.eu>*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8F:54:0A:B3:E8:9D:71:E9:D2:F7:12:86:F5:D8:40:45:26:F4:FE:41:EB:FE:E5:4D:18:B5:E0:2D:F0:D3:88:DA*

X509SubjectName

Subject CN: *EAD Trust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2024*

Subject O: *EAD Trust*

Subject C: *ES*

X509SKI

X509 SK I

GsF6TRr7642VbDqImEOmakGEplE=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time

2026-02-26T03:00:00Z

40.34.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

41 - TSP: Bewor tech, S.L.**TSP Name**

Name [en] *Bewor tech, S.L.*

Name [es] *Bewor tech, S.L.*

TSP Trade Name

Name [en] *Bewor tech*

Name [es] *Bewor tech*

Name [en] *VATES-B19603968*

Name [es] *VATES-B19603968*

PostalAddress

Street Address [en] *Polígono La Ermita, calle Abeto s/n, Edificio CEG oficina 17-19*

Locality [en] *Atarfe*

State Or Province [en] *Granada*

Postal Code [en] *18230*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Polígono La Ermita, calle Abeto s/n, Edificio CEG oficina 17-19*

Locality [es] *Atarfe*

State Or Province [es] *Granada*

Postal Code [es] *18230*

Country Name [es] *ES*

ElectronicAddress

URI [en] *http://bewor.com*

URI [es] *http://bewor.com*

URI [en] *mailto:info@bewor.com*

URI [en] *<http://www.bewor.com>*

URI *[es]* *http://www.bewor.com*

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificates issued by BEWOR TECH CA1

Name [es] *Certificados cualificados emitidos por BEWOR TECH CA1*

Version: 3

Serial Number: 4955006823150501412

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATFS-A66721499*

Issuer CN: UANATACA ROOT 2016

Issuer OU: *TSP-UANATACA*

Issuer O:	UANATACA S.A.
Issuer L:	Barcelona (see current address at www.uanataca.com/address)
Issuer C:	ES
Subject 2.5.4.97:	VATES-B19603968
Subject CN:	BEWOR TECH CA1
Subject OU:	PSC-BEWOR
Subject O:	Bewor tech SL
Subject L:	GRANADA
Subject C:	ES
Valid from:	Tue May 12 10:46:35 CEST 2020
Valid to:	Thu May 12 10:46:35 CEST 2033
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9C:53:DE:96:E2:5C:48:BC:23:49:FF:1B:4B:CE:8F:33:93:E1:46:A4:54:B4:3A: 6E:D1:4E:B9:9D:BA:EC:84:09:AE:E9:46:14:EA:25:F7:D1:C6:33:62:92:5D:D5:E2:FF:13:C0:57:DF:67:6E:4D:6E:0D:98:83:64:73:7D:27:65:3D:37:74:59:98:8C:FA:F2:5D:30:5C:60:9F:ED:A 1:DA:4C:0A:73:AC:A8:73:D9:C2:DB:05:D0:A5:43:0A:2F:2F:F8:D8:0C:26:15:A4:B9:22:8E:F2:7C:86:F5:22:2E:B5:CA:C5:90:FD:2D:6E:97:E5:3A:34:A1:26:12:30:19:72:B2:5E:27:14:F7:4E: 97:8E:C5:C4:8C:2C:9C:8F:75:8F:7F:94:08:8B:3B:D7:CF:2C:EE:09:82:FC:B7:7E:7B:72:B2:1E:64:66:81:E4:EF:62:86:B6:6E:FC:43:DC:C8:20:5E:E9:15:EB:5A:2F:07:A6:24:6C:BB:EA:7E:82: 6D:E4:39:D5:C0:DD:CD:2A:08:35:E5:CA:E5:2C:50:D1:BE:D5:29:88:83:07:04:26:CD:5E:6E:5F:98:2A:11:89:D6:95:89:FE:F6:FF:86:BA:37:7D:82:C4:99:4E:B9:B1:0D:BA:DA:4C:FC:8F:A2: 54:47:E1:DC:E1:32:98:47:C6:2B:30:79:0C:7F:28:64:2F:A6:3B:25:93:93:C9:19:C9:88:F9:A7:1A:3C:C9:5D:E3:90:96:93:9D:EF:0C:68:25:E4:CD:58:9B:ED:52:A5:F8:7A:69:2E:14:0C:CC:8 9:21:13:B7:DA:14:45:EC:41:58:DF:96:D1:94:DB:D8:65:BC:3E:A3:CB:A8:F7:DD:37:B1:DA:E5:D0:BA:86:98:95:EA:06:B1:4F:E1:BB:60:FC:05:B9:BA:D7:C8:42:6F:AA:AE:AB:AD:B3:79:CC: 53:11:8B:9A:48:86:40:A9:72:A7:C5:3B:F8:26:B9:D7:84:97:29:8B:A9:E2:FA:E2:06:1C:7D:E6:78:64:91:9A:08:57:81:58:28:96:CD:C8:07:48:95:AD:21:0C:01:FA:04:29:7D:BA:12:34:7D:B 2:80:3A:30:9A:33:32:DB:5B:30:94:CC:9E:BC:AC:E9:03:52:42:60:22:3E:F6:E9:86:03:5B:17:60:30:AF:D7:53:77:2C:29:E6:06:8C:5F:8F:2C:F9:17:D3:06:27:A4:F9:A9:4C:89:AE:2F:EB:5D: C7:B0:C8:E3:44:14:64:0C:A5:67:31:AA:51:B9:06:2A:A8:82:F7:64:7D:D0:94:7B:12:4D:E0:69:73:81:16:CA:2F:57:7D:1E:31:25:13:72:DB:57:0D:2C:CE:6D:02:03:01:00:01 </pre>
Authority Info Access	http://ocsp1.uanataca.com/public/pki/ocsp/ http://ocsp2.uanataca.com/public/pki/ocsp/
Subject Key Identifier	36:02:5A:C1:64:B4:F9:29:F1:03:09:16:94:B3:D9:A6:BD:7A:13:42
Basic Constraints	IsCA: true - Path length: 0
Authority Key Identifier	55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C
Issuer Alternative Name	info@uanataca.com
Certificate Policies	Policy OID: 2.5.29.32.0 CPS pointer: https://bewor.com/dpc CPS text: [Certificado de la Autoridad de Certificación Subordinada de Bewor tech - https://bewor.com/proveedor-de-firma]
CRL Distribution Points	http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl
Subject Alternative Name	info@bewor.com
Key Usage:	keyCertSign - cRLSign
Thumbprint algorithm:	SHA-256

Thumbprint: *8A:38:6E:D1:C0:93:26:03:D3:B5:F4:78:9B:7F:CB:33:CF:09:C8:1A:56:DE:97:FC:82:67:47:95:6C:2E:78:6D*

X509SubjectName

Subject 2.5.4.97: *VATES-B19603968*

Subject CN: *BEWOR TECH CA1*

Subject OU: *PSC-BEWOR*

Subject O: *Bewor tech SL*

Subject L: *GRANADA*

Subject C: *ES*

X509SKI

X509 SK I *NgJawWS0+SnxAwkWILPZpr16E0I=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time *2020-10-23T02:00:00Z*

41.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

42 - TSP: SIGNICAT S.L.U.**TSP Name**

Name [en] *SIGNICAT S.L.U.*

Name [es] *SIGNICAT S.L.U.*

TSP Trade Name

Name [en] *SIGNICAT SPAIN*

Name [en] *Electronic Identification S.L.*

Name [en] *VATES-B86681533*

PostalAddress

Street Address [en] *Avenida Ciudad de Barcelona, 81. 4ª Planta.*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28007*

Country Name [en] *ES*

ElectronicAddress

URI [en] *<https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>*

URI [en] *<mailto:eIDLegal@signicat.com>*

TSP Information URI

URI [en] *<https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>*

42.1 - Service (granted): Qualified Certificates issued by ELECTRONIC IDENTIFICATION CA1**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Subject C: *ES*

Valid from: *Tue Feb 25 11:57:13 CET 2020*

Valid to: *Thu Feb 24 11:57:13 CET 2033*

Public Key:
 30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C0:14:E4:D2:C2:71:01:25:20:0C:EA:1F:45:4F:91:13:89:51:C0:B4:8D:4A:F3:CE:6A:18:2E:81:77:EE:62:50:C8:54:98:75:1E:93:99:85:3D:9C:49:CD:4B:0C:5D:09:DD:3C:17:DA:44:88:B6:A2:CE:2E:A4:E9:F0:AF:03:6C:93:46:CE:7D:D4:CA:87:AA:B0:98:DE:54:AA:CB:5B:2F:D4:07:D9:6D:DE:2D:87:94:64:71:F5:D5:D6:3F:6D:ED:CF:65:25:08:0A:B3:19:65:15:13:FD:83:F9:18:18:61:25:1F:AE:CB:AF:40:60:9F:15:CD:E2:F0:8C:CB:65:82:EB:1E:F3:8D:10:05:10:0B:B8:F4:4F:ED:0E:14:D8:FF:FF:85:F1:6F:C3:6B:E5:64:01:29:9C:01:5E:3B:8A:4A:E8:4C:BD:77:35:DC:89:9A:4F:B5:E2:FF:F4:26:1F:D4:29:78:F1:F3:69:16:CF:39:3E:3B:25:FF:6C:4A:C9:CA:D1:21:87:34:74:24:DE:E8:20:93:97:31:4F:6D:95:F9:C6:C2:A2:70:CC:EF:15:08:0D:FF:FE:81:15:C9:18:FF:57:FC:85:6E:F2:C1:99:20:04:75:1F:BA:F3:64:2E:82:F8:2D:F0:DD:BD:87:46:33:CB:F3:7D:2E:4E:CF:3E:E3:FA:75:C5:B3:53:18:73:48:38:88:8B:A6:CA:78:69:86:6A:64:47:59:FF:F8:90:CC:35:FD:EE:4C:55:A5:5D:46:4E:F5:DC:B8:71:FA:FB:CE:A2:E6:F9:8F:9A:F9:A0:11:B9:DF:0A:F1:A2:91:08:75:05:A8:E1:0C:58:A2:41:E1:3E:C2:D5:AD:7E:FE:89:8F:BD:77:80:1E:30:7C:9E:DD:44:A8:0E:2D:00:24:10:85:B0:77:00:76:DD:77:96:E7:C2:9E:26:C6:EF:E8:F7:B9:2F:7C:8D:13:08:4E:5C:F8:8A:9A:70:B6:56:5B:C4:97:0E:64:47:BF:66:50:4E:40:80:D4:68:5E:E6:A2:4B:9C:2F:CC:D1:A5:9B:C9:DD:17:16:4E:23:F5:78:F3:A1:AE:24:D2:86:12:44:8F:B4:C1:B2:AB:85:39:58:42:EF:2D:D7:87:4B:BC:EC:6E:8D:F4:65:3B:1D:59:65:F4:30:54:4A:8F:BC:82:63:37:CB:79:2B:DE:CF:38:8D:A4:C9:AA:0E:70:51:B9:8B:00:28:D3:A6:EF:2D:F4:48:82:AE:E4:0D:4D:39:39:9D:14:C5:9B:AD:E5:0E:D2:50:1F:5F:F6:59:00:F5:B1:64:7A:0F:BD:45:0B:41:48:D5:1D:8F:B0:42:A2:CB:C9:99:A3:90:D3:02:03:01:00:01

Authority Info Access
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *85:15:64:CD:9B:07:48:9D:F7:E6:9A:44:07:9C:79:0A:8C:A1:96:3F*

Basic Constraints
IsCA: true - Path length: 0

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://www.electronicid.eu/certification-practice-statement-cpd/>
CPS text: [Certificado de la Autoridad de Certificación Subordinada de Electronic Identification. - www.electronicid.eu]

CRL Distribution Points
http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

Subject Alternative Name *info@electronicid.eu*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EE:DC:F3:16:33:60:9A:CB:49:28:95:FD:55:AA:59:1A:10:9C:44:D3:B0:FC:1D:06:21:E0:FB:41:A2:CB:49:2B*

X509SubjectName

Subject 2.5.4.97: *VATES-B86681533*

Subject CN: *ELECTRONIC IDENTIFICATION CA1*

Subject OU: *PSC-EID*

Subject O: *Electronic Identification S.L.*

Subject L: *MADRID*

Subject C: ES

X509SKI

X509 SK I hRVkzZsHSJ335ppEB5x5Coyhlj8=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2020-11-18T22:00:00Z

Scheme Service Definition URI

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

42.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

42.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.55193.1.1.2

Description

43 - TSP: Sectigo (Europe) SL

TSP Name

Name [en] *Sectigo (Europe) SL*

Name [es] *Sectigo (Europe) SL*

TSP Trade Name

Name [en] *SECTIGO*

Name [es] *SECTIGO*

Name [en] *VATES-B01683580*

PostalAddress

Street Address [en] *Rambla Catalunya 33, 3^a*

Locality [en] *Barcelona*

State Or Province [en] *Barcelona*

Postal Code [en] *08007*

Country Name [en] *ES*

ElectronicAddress

URI [en] *https://www.sectigo.com*

URI [en] *mailto:inigo.barreira@sectigo.com*

TSP Information URI

URI [en] *https://www.sectigo.com*

43.1 - Service (granted): Qualified Certificates issued by "Sectigo Qualified Website Authentication CA E35"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Name	[en]	Qualified Certificates issued by “Sectigo Qualified Website Authentication CA E35”
Name	[es]	Certificados cualificados emitidos por “Sectigo Qualified Website Authentication CA E35”

Service digital identities

Certificate fields details

Version:	3
Serial Number:	210467423367101675439552997939815733505
X509 Certificate	-----BEGIN CERTIFICATE----- MIIDbCCAvSgAwIBAgIRAJ5W5He2JMHw0CAy2ZWQEWGQYKozlZj0EAWMwgYqxCzAJBgNVBAYT AIVTMRMEQYDVQQEwPOZXRz3b3jrmS4wLAYDVOODEYyVU0VSVHJ1c3QgRUNDIENicnRp2mjiYXRp b24gQXV0aG9yaXR5MB4XDjE1MTAwMTAwMDAwMFoXDTE1MTAwNDIeNTR1OVVwZTElMAkGA1UEBhMC RVh0AABgNVBAQoTE1NY3Rpb28gKEV1cm9wZSkgU0wxODAA2BgNVBAMTL1NY3Rpb28gUUVhbGlm aWVkfDIYnNpdGUgQXV0aGVudGUiYXRpb24gOGEgRTM1MkFkewYHkZlZj0CAOYKozlZj0DAQcD QgAeZlmaXB18Y0Y6aF0kuyZTQl0wxxwijnR28uVLF3L4B1NgZAINTwCR1QULYgC0BZX2k8 c8r+E4w53gARlaOCAV8wggFbMB8CA1UdlwQYMBAAFDmCYbUzxmClnZOSXbc4DXGY20aMB0GA1Ud DgQWB8Q8ELB9TETSoLg+ejafluK56vWTA0BgNVHQB8BEBAMCAyYwEgYDVROTAQH/BAQwBgEB /wBAAQABgNVHSEETjAUBgggBgEFBQcDAQYIKwYBBQUHAWMEQYDVROgBAAwCAAGBgRVHSAAMFAG A1UdHwRjMEcwRABDQEGCP2h0dHA6Ly9jcmwudXNlcncydnXN0LmNvbS9VU0VSVHJ1c3RFOQNDZXJ0 aWZpY2F0aW9uQXV0aG9yaXR5LmNybDBx8ggrBgEFBQcBAQRIMGMwOgyIkwyBBQUHMAKGLmh0dHA6 Ly9icm0uZnNlcncydnXN0LmNvbS9VU0VSVHJ1c3RFOQNBQURDQ55icm0wOgyIkwyBBQUHMAKGLmh0dHA6 dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wCgYKozlZj0EAWMDaAAWZQixAPdGdzU3wUj6nUMuGR88 wpKNe8anIep+ilkEqg9E4TrbVsi+DKza3bZXD1+TpLXiwiwSn26MmiP43/g/EVOPLSG/jw9EEod K6gdSABirrkW75mhFPLMduOCbAGR7MvBVbV -----END CERTIFICATE-----
Signature algorithm:	SHA384withECDSA
Issuer CN:	USERTrust ECC Certification Authority
Issuer O:	The USERTRUST Network
Issuer L:	Jersey City
Issuer ST:	New Jersey
Issuer C:	US
Subject CN:	Sectigo Qualified Website Authentication CA E35
Subject O:	Sectigo (Europe) SL
Subject C:	ES
Valid from:	Mon Oct 05 02:00:00 CEST 2020
Valid to:	Fri Oct 05 01:59:59 CEST 2035
Public Key:	30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:A1:9F:E6:6A:25:C1:D7:C6:28:63:AB:08:16:2D:24:BB:26:53:42:5B:60:C3:1C:23:9E:58:D1:67:C B:8F:34:81:77:2F:86:F3:36:06:40:94:D4:F0:19:1D:50:2C:86:20:18:E0:59:C7:89:3C:73:CA:FE:13:8C:12:DE:00:11:95
Authority Key Identifier	3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
Subject Key Identifier	01:10:B0:7D:4C:44:D2:A0:B2:60:F9:E8:DA:7D:FB:8A:AF:9E:AF:59
Basic Constraints	IsCA: true - Path length: 0
Extended Key Usage	id_kp_serverAuth

Certificate Policies	<i>Policy OID: 2.5.29.32.0</i>
CRL Distribution Points	<i>http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl</i>
Authority Info Access	<i>http://crt.usertrust.com/USERTrustECCAAACA.crt http://ocsp.usertrust.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>56:2D:6A:5B:4B:06:74:65:FF:D0:FB:FC:9B:B0:57:55:CD:AC:F5:5B:5E:E5:C6:F9:10:B8:B5:3D:B1:28:F5:7A</i>

X509SubjectName

Subject CN:	<i>Sectigo Qualified Website Authentication CA E35</i>
Subject O:	<i>Sectigo (Europe) SL</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>ARCwfUxE0qCyYPno2n37iq+er1k=</i>

Service Status

	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description [en]	<i>undefined.</i>
[es]	<i>undefined.</i>

Status Starting Time	<i>2021-05-05T01:00:00Z</i>

43.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

43.2 - Service (granted): Qualified Certificates issued by "Sectigo Qualified Website Authentication CA R35"**Service Type Identifier**

	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
Service type description [en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Authority Key Identifier	<i>53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB</i>
Subject Key Identifier	<i>EB:35:25:2A:06:36:E8:D6:01:E5:69:93:84:D2:F3:2C:3B:AC:DE:AF</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i>
CRL Distribution Points	<i>http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl</i>
Authority Info Access	<i>http://crt.usertrust.com/USERTrustRSAAAACA.crt</i> <i>http://ocsp.usertrust.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>00:23:93:FA:0A:68:25:F7:7E:F6:86:E2:08:62:0B:97:17:77:91:F0:2F:07:DB:25:18:48:0F:BE:37:CE:7B:D8</i>

X509SubjectName

Subject CN:	<i>Sectigo Qualified Website Authentication CA R35</i>
Subject O:	<i>Sectigo (Europe) SL</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>6zUIKgY26NYB5WmThNLzLDus3q8=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2021-05-05T01:00:00Z</i>

43.2.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified Certificates issued by “Sectigo Qualified Time Stamping CA R35”
Name	[es]	Certificados cualificados emitidos por “Sectigo Qualified Time Stamping CA R35”

Version: 3

Serial Number: 17085313805061118988539507999818040923

Signature algorithm:	<i>SHA384withRSA</i>
Issuer CN:	<i>Sectigo Qualified Time Stamping Root R45</i>
Issuer O:	<i>Sectigo (Europe) SL</i>
Issuer C:	<i>ES</i>
Subject CN:	<i>Sectigo Qualified Time Stamping CA R35</i>
Subject O:	<i>Sectigo (Europe) SL</i>
Subject C:	<i>ES</i>
Valid from:	<i>Mon Oct 05 02:00:00 CEST 2020</i>
Valid to:	<i>Fri Oct 05 01:59:59 CEST 2035</i>

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:81:97:8E:E6:38:6C:C7:07:E3:37:CC:9C:AC:A2:23:C6:DC:D5:81:B5:AF:C9:0C:CC:A1:C6:15:4B:FF:39:48:9B:E3:0A:F3:2D:03:00:B4:8C:18:B2:25:87:3E:98:96:9B:93:02:CC:A4:9E:BA:40:C6:A9:AB:38:AA:05:25:17:FE:A1:B9:B1:FA:A1:38:05:D9:04:22:91:11:30:DA:74:2B:57:C3:C5:4D:92:15:13:C9:4E:6D:A6:42:BA:BC:30:9F:89:69:A4:99:94:2F:55:A8:A8:BC:47:64:29:68:BD:34:84:51:89:6C:17:56:55:A8:35:DE:E6:3C:8A:4B:83:C1:73:CD:DD:2E:BA:04:9F:A9:EE:21:30:61:13:EC:F9:0C:60:AF:F7:B1:D5:DD:48:4C:70:82:4C:88:A4:D9:99:0A:ED:89:48:C7:D2:8C:E0:DE:59:F3:54:F2:36:4F:CC:B7:03:5E:C0:3F:25:89:6C:B9:AC:7F:7C:1A:63:9E:2F:20:6A:84:AC:07:4B:2D:86:F0:3D:15:06:59:81:D9:53:85:BB:9E:48:09:7C:88:88:40:87:DA:F9:DD:13:FF:51:46:E3:23:C9:5D:35:8A:D7:09:CB:64:2E:A5:0D:75:18:7D:94:8E:C6:83:F6:79:00:86:D2:0E:CC:CF:A8:D1:94:63:DD:61:02:6A:55:A2:06:6A:33:EB:11:46:2E:88:D2:7E:02:E6:10:9C:C0:CC:22:DC:0C:AA:BB:FC:06:3C:A0:B4:49:60:FF:09:BD:96:0D:46:04:AE:09:DA:06:EC:65:8E:0F:62:66:55:90:54:DE:72:87:24:02:C1:74:4D:D7:FB:9E:C7:4C:6D:3C:39:4D:AE:DF:17:23:43:A2:17:52:AB:48:E0:07:72:F5:F5:7F:12:8D:34:18:0B:DF:58:78:26:35:44:F5:37:07:D6:46:D3:66:68:97:AC:A2:3D:53:91:2D:B6:D4:2E:2A:16:6A:FC:0A:E7:A2:F4:4C:B7:43:CB:02:03:01:00:01

Authority Key Identifier

59:81:A8:C3:85:64:E7:E3:44:A4:69:52:26:94:53:F6:3B:0D:EE:DE

Subject Key Identifier

61:00:3F:77:D9:FF:EA:39:D2:91:A5:1C:BE:9D:35:C7:78:5E:A4:67

Basic Constraints

IsCA: true - Path length: 0

Extended Key Usage

id_kp_timeStamping

Certificate Policies

Policy OID: 2.5.29.32.0

CRL Distribution Points

<http://crl.sectigo.com/SectigoQualifiedTimeStampingRootR45.crl>

Authority Info Access

<http://crt.sectigo.com/SectigoQualifiedTimeStampingRootR45.crt>
<http://ocsp.sectigo.com>

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

CD:0A:3E:00:A1:BD:AE:3A:15:9F:A9:E3:D7:0F:8E:66:4F:56:0F:DC:E1:63:57:CB:E4:40:ED:0B:0D:88:24:4F

X509SubjectName**Subject CN:**

Sectigo Qualified Time Stamping CA R35

Subject O:

Sectigo (Europe) SL

Subject C:

ES

X509SKI**X509 SK I**

YQA/d9n/6jnSkaUcvp01x3hepGc=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2021-05-05T01:00:00Z

Scheme Service Definition URI**URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name [en]

Qualified Certificates issued by "Sectigo Qualified Natural Person CA E35"

Name [es]

Certificados cualificados emitidos por "Sectigo Qualified Natural Person CA F35"

Certificate fields details

Version: 3

Serial Number: 255804324125549905159335600213648333605

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA384withECDSA*

Issuer CN: *Sectigo Qualified Natural Person Root E45*

Issuer O: *Sectigo (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Natural Person CA E35*

Subject O: *Sectigo (Europe) SL*

Subject C: *FS*

Valid from: Mon Oct 05 02:00:00 CEST 2020

Valid to: *Fri Oct 05 01:59:59 CEST 2035***Public Key:**

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:28:40:8F:7E:85:93:B1:0F:FA:99:09:99:D8:C3:F5:0F:4C:FC:70:16:F1:93:80:F7:57:1A:E6:60:18:90:83:72:44:20:9F:89:6A:C3:68:B9:85:C9:5E:F2:88:75:D0:51:DD:8F:83:E4:20:00:36:E2:F9:36:FF:E0:33:EA:F8:11

Authority Key Identifier	<i>C7:E1:52:9C:DC:66:31:F4:0C:4F:FD:0A:A7:28:3A:6C:D5:EE:10:CB</i>
Subject Key Identifier	<i>C4:6E:19:01:62:AD:55:4B:C4:84:D5:87:C9:46:CB:30:79:83:68:6A</i>
Basic Constraints	<i>IsCA: true - Path length: 0</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i>
CRL Distribution Points	<i>http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crl</i>
Authority Info Access	<i>http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crt http://ocsp.sectigo.com</i>
Key Usage:	<i>digitalSignature - keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>53:B2:40:05:FD:13:67:1F:54:99:89:C8:C6:69:05:9E:AB:E7:7A:D1:9D:DE:E1:E7:0F:72:C9:FB:B3:C0:D9:F9</i>

X509SubjectName

Subject CN:	<i>Sectigo Qualified Natural Person CA E35</i>
Subject O:	<i>Sectigo (Europe) SL</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>xG4ZAWKtVUvEhNWHyUbLMHmDaGo=</i>

Service Status

Service status description	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<i>[en]</i>	<i>undefined.</i>
<i>[es]</i>	<i>undefined.</i>

Status Starting Time	<i>2021-05-05T01:00:00Z</i>

43.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key: *30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:A0:01:03:50:08:DF:43:BB:6E:4F:E0:7D:EB:90:D8:78:B3:17:F3:31:74:E3:3B:E5:29:BE:38:A1:91:71:16:AE:E8:05:0B:08:C1:E0:B6:4C:92:4D:0F:FE:45:2E:53:C4:CC:78:E6:A6:00:6C:27:8E:73:14:A8:76:99:17:9E:D6:D8:67:85:ED:B3:01:ED:68:C8:CC:98:C0:38:2A:98:D4:BF:8B:51:95:14:BF:62:E1:C3:15:0D:13:0E:D6:5B:03:8E:05:9B:F4:CD:39:CA:37:1E:60:38:97:7C:17:A4:9B:BA:D3:38:44:50:90:49:B8:79:1E:DE:6D:84:64:80:19:08:E3:5D:7D:7D:88:04:92:7A:7A:72:22:5E:DB:2B:1A:DD:FA:39:CF:F2:C8:1E:C7:A7:18:61:29:5C:64:65:A5:D4:DF:68:6D:50:C0:78:0B:E0:7E:43:2E:58:D4:45:F8:E9:EF:89:EB:BA:93:BF:BA:40:4D:C1:70:27:0C:DA:30:4D:C3:5E:8F:72:14:40:C3:D6:1E:F5:50:23:86:B9:09:BF:42:57:5A:37:22:64:08:75:21:5F:DD:87:1C:E4:88:81:A0:ED:33:37:7A:75:A1:D7:29:08:AC:BE:86:93:93:F8:76:F8:B E:D9:4F:60:89:74:AF:57:05:C4:BF:F4:AB:E9:D5:83:8E:F1:F2:ED:16:A5:11:E0:85:7C:19:A4:9E:2A:06:4B:2D:94:47:0C:4C:37:F3:10:A7:EF:38:91:AD:AF:76:DA:8F:B6:AD:F7:8B:A2:35:94:A6:35:CA:8C:CD:BF:59:0F:CB:0C:CF:76:3C:16:0A:0D:9F:E8:3C:CC:2D:5A:13:E2:77:C6:BA:87:93:8D:89:61:37:B7:64:87:64:43:AB:33:38:C2:EE:3B:84:B0:07:0C:A6:BC:73:95:13:D2:F1:AE:37:5F:5F:ED:3D:E7:F3:D7:8F:AF:F9:F3:AB:7D:D5:3D:FF:F2:1F:18:3A:A3:35:35:1F:93:88:A7:02:03:01:00:01*

Authority Key Identifier *E4:EA:E1:45:46:3B:0B:48:F5:78:F4:C2:49:09:B2:42:92:84:06:B9*

Subject Key Identifier *E7:BF:64:10:52:01:3C:A6:83:09:B0:FC:A3:4D:A3:68:40:52:8D:00*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crl*

Authority Info Access *http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crt
http://ocsp.sectigo.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AC:86:68:30:D7:B8:D7:12:73:C7:CD:E0:57:A8:D5:3E:93:4C:4E:6F:16:94:7D:13:8A:12:3C:BE:C8:C6:3B:DE*

X509SubjectName

Subject CN: *Sectigo Qualified Natural Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *579kEFIBPKaDCbD8o02jaEBSjQA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.
[es] undefined.*

Status Starting Time *2021-05-05T01:00:00Z*

43.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

Public Key:

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2E:CD:64:81:35:FF:1D:56:82:41:CE:00:C7:F0:9B:2D:A9:C6:9A:CE:91:D0:74:53:1B:8B:D4:B8:71:9B:33:F1:A9:56:6B:F1:96:38:B1:E9:97:A7:E6:58:50:47:D8:66:E0:1E:32:21:35:C4:1B:76:2C:5D:2E:84:56:3C:FE:DD

Authority Key Identifier

0E:C9:9E:2D:8C:F8:67:78:9B:E9:8C:FE:30:D8:40:80:B3:44:4A:2A

Subject Key Identifier

74:3F:73:35:63:94:96:1B:8E:F1:CD:77:A8:A8:0B:75:72:BB:15:63

Basic Constraints

IsCA: true - Path length: 0

Extended Key Usage

id_kp_clientAuth

Certificate Policies

Policy OID: 2.5.29.32.0

CRL Distribution Points

http://crl.sectigo.com/SectigoQualifiedLegalPersonRootE45.crl

Authority Info Access

http://crt.sectigo.com/SectigoQualifiedLegalPersonRootE45.crt
http://ocsp.sectigo.com

Key Usage:

digitalSignature - keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

D1:1D:91:67:B7:6C:CF:32:AF:9F:FE:0D:5B:F6:6A:82:BB:56:85:40:AE:39:F5:96:54:41:FB:BD:55:E1:D9:D8

X509SubjectName**Subject CN:**

Sectigo Qualified Legal Person CA E35

Subject O:

Sectigo (Europe) SL

Subject C:

ES

X509SKI**X509 SK I**

dD9zNWOUlhuO8c13qKgLdXK7FWM=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2021-05-05T01:00:00Z

43.6.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI**

[en]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name [en]

Qualified Certificates issued by "Sectigo Qualified Legal Person CA R35"

Name [es]

Certificados cualificados emitidos por "Sectigo Qualified Legal Person CA R35"

Version: 3

Serial Number: 281853815834614069450094829868643163637

X509 Certificate

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *Sectigo Qualified Legal Person Root R45*

Issuer O: *Sectiao (Europe) SL*

Issuer C: *ES*

Subject CN: *Sectigo Qualified Legal Person CA R35*

Subject 0: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: Mon Oct 05 02:00:00 CEST 2020

Valid to: *Fri Oct 05 01:59:59 CEST 2035*

Public Key: *30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:C8:9C:66:4E:69:FE:69:9A:20:C0:F8:DD:85:B6:B0:91:C6:18:89:BF:F6:88:62:F5:CA:B2:22:67:30:7C:3E:61:9F:84:86:19:9E:F4:2E:9C:89:92:FF:E1:68:E5:07:95:FC:E7:0F:9E:5F:95:8F:3E:07:89:DA:DC:F7:EC:71:E5:94:6D:1C:07:2A:F8:9A:3F:17:58:55:7D:63:FA:76:81:3D:F3:15:D6:7D:5E:A5:8E:D6:B3:E5:E2:D3:75:6A:B2:21:6A:73:B9:EA:05:88:8D:9D:7C:DC:28:2D:8D:12:53:CC:AD:5D:DB:22:99:75:0E:E2:48:98:CA:D2:05:D8:A3:6A:4F:29:7C:13:0B:ES:18:26:D6:3C:3C:00:3D:73:87:22:EF:D7:C7:7B:13:64:00:8C:8C:6D:27:C1:9E:8C:28:C6:E6:D9:15:23:23:41:9D:2C:D0:70:83:D2:09:32:F1:6F:87:44:83:0C:E5:5D:DF:17:BA:1D:0A:7E:0B:9D:BC:1E:89:D9:C8:D8:58:4E:49:78:B0:01:52:D5:53:EF:ED:5B:C2:83:B0:4F:86:A3:59:8D:D8:34:58:CE:44:CB:24:67:D6:8F:B5:38:99:BC:83:14:A7:1D:88:D1:E6:A6:BC:AD:14:06:84:25:D7:89:A9:F9:12:AC:9D:93:17:60:92:C8:76:7A:5E:8E:70:E1:8C:73:0B:F1:54:45:B5:96:F9:00:91:BF:99:1F:57:1F:A8:8E:9B:29:CB:1D:AC:C4:69:FA:D6:88:48:85:FD:C6:5A:42:4B:58:36:1A:F8:A0:E7:34:65:87:CA:99:89:28:A0:4E:C6:C0:7C:4D:3E:7E:9D:CD:EC:66:2D:2F:FD:29:47:D7:EE:B9:6D:B5:C5:C5:23:09:AA:42:9E:89:87:FF:2A:82:A1:39:9D:5A:CA:4F:FE:2B:AA:C4:7A:44:5E:B2:3E:11:51:EA:E8:18:F0:2E:18:69:DC:35:C1:51:10:55:40:7D:33:FE:B0:7D:51:BD:ED:02:03:01:00:01*

Authority Key Identifier *07:4B:74:2F:D7:70:4A:79:E2:CF:C8:AA:A6:69:05:80:08:83:07:6A*

Subject Key Identifier *AC:EE:22:F8:B9:8B:F1:EE:72:13:1A:91:6F:A4:E2:4D:F2:14:EC:14*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.sectigo.com/SectigoQualifiedLegalPersonRootR45.crl*

Authority Info Access *http://crt.sectigo.com/SectigoQualifiedLegalPersonRootR45.crt
http://ocsp.sectigo.com*

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *33:95:96:69:16:F8:D3:9D:CE:B5:F7:5C:FF:8B:8E:F4:ED:CB:36:2B:1C:0C:27:92:4D:A4:2D:07:DD:18:F1:59*

X509SubjectName

Subject CN: *Sectigo Qualified Legal Person CA R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *rO4i+LmL8e5yExqRb6TiTfIU7BQ=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.
[es] undefined.*

Status Starting Time *2021-05-05T01:00:00Z*

43.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

Subject C: *ES*
Valid from: *Tue Nov 17 01:00:00 CET 2020*
Valid to: *Sat Nov 17 00:59:59 CET 2035*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:24:33:11:92:8A:7B:AE:1F:F5:F7:2F:E1:59:B9:D7:EF:BC:44:AB:73:66:DF:53:02:98:1C:5B:EC:D5:34:80:4C:E4:DD:D8:06:F9:A3:6F:8D:6C:EF:4F:01:89:53:5B:FB:94:55:8F:44:8E:38:50:00:67:5F:87:4A:97:16:E8:D1*
Authority Key Identifier *3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A*
Subject Key Identifier *57:2D:B9:6D:D4:5F:FB:E6:93:23:66:F5:37:EB:3F:1E:60:07:1D:A0*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CRL Distribution Points *http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl*
Authority Info Access *http://crt.usertrust.com/USERTrustECCAAACA.crt*
http://ocsp.usertrust.com
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *A9:84:1D:2E:47:CB:E6:D7:1D:8F:AF:DF:38:38:7F:93:F4:3D:76:D7:92:50:4E:FB:17:A2:10:20:C5:8C:0B:89*

X509SubjectName

Subject CN: *Sectigo Qualified Website Authentication CA Natural E35*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*

X509SKI

X509 SK I *Vy25bdRf+ +aTI2b1N+s/HmAHHaA=*

Service Status

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2021-05-05T01:00:00Z*

43.8.1 - Extension (critical): additionalServiceInformation

Issuer C: *US*

Subject CN: *Sectigo Qualified Website Authentication CA Natural R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

Valid from: *Tue Nov 17 01:00:00 CET 2020*

Valid to: *Sat Nov 17 00:59:59 CET 2035*

Public Key:
 30:82:01:A2:30:0D:06:09:2A:86:4B:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:92:E0:B2:D5:0E:F6:EC:80:94:86:3F:07:92:8B:1B:DF:08:11:9A:CD:0E:D3:CE
 74:CD:2B:DD:B2:FE:E8:18:08:C0:F9:AD:F6:55:78:16:DA:02:0F:28:DD:AA:CF:E6:71:86:37:68:88:25:57:4D:A0:AA:56:72:A4:96:2A:EE:2A:57:C0:CC:F2:0E:93:FE:01:53:FF:D3:1B:6D:98:
 FA:88:6F:A9:36:AB:70:BF:95:86:88:E9:E8:CF:14:59:7D:A4:74:4F:EF:4E:06:CE:92:F2:24:AB:96:56:CF:5A:9A:E7:05:CC:A9:A7:67:87:2B:8A:96:95:73:2F:FA:AA:83:34:42:66:FA:69:52:12:
 43:22:87:37:08:FE:21:AF:BC:68:7C:A7:AB:01:A4:60:03:4B:AD:7F:7E:F4:14:CC:13:37:21:54:E5:5F:81:12:8F:80:D9:A7:35:FE:D6:9F:ED:C8:F9:9E:7C:29:FA:DF:D2:A2:74:7C:C8:2C:6D:25:
 19:6D:4A:62:40:97:89:F6:C7:65:84:11:DE:E0:53:17:7B:1D:EA:C7:F2:8F:B4:DF:C2:27:48:8F:C9:88:DF:A7:81:A6:31:98:32:39:42:43:69:F6:E3:87:1F:DA:0F:7B:E7:00:F5:87:F8:77:66:55:
 A9:5D:A9:DC:84:FC:48:46:A1:3A:9E:9C:DA:DA:65:C5:B9:A3:80:AA:A7:F6:1D:08:09:D7:00:CD:E3:05:79:31:4E:52:59:2D:34:F5:B5:35:CB:DD:6D:67:AC:85:F4:C5:F4:DF:C7:8B:C6:8A:A
 6:D9:41:B3:5B:3C:74:03:99:C2:AB:86:4B:19:DD:27:82:D6:0E:0F:5D:CC:12:03:DE:8A:08:71:28:18:F7:83:C1:C4:AA:C5:07:3C:87:CE:D8:04:41:C3:5A:EF:01:05:5E:2E:FE:55:40:A7:24:93
 9F:2E:70:06:8B:CC:63:9D:E6:A9:B6:76:4A:95:85:78:2F:41:C9:5D:4E:17:27:5D:E9:68:79:B7:02:03:01:00:01

Authority Key Identifier *53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB*

Subject Key Identifier *E5:D6:D0:41:C2:47:C0:C4:72:81:A5:3E:2D:19:58:E9:5B:25:29:38*

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_serverAuth*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl*

Authority Info Access *http://crt.usertrust.com/USERTrustRSAAAACA.crt*
http://ocsp.usertrust.com

Key Usage: *digitalSignature - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *33:9E:6B:92:BE:54:59:F2:6A:8D:C3:C5:F3:72:09:33:C8:38:E2:36:60:1B:05:00:48
 :C0:47:A1:23:E6:F8:E7*

X509SubjectName

Subject CN: *Sectigo Qualified Website Authentication CA Natural R35*

Subject O: *Sectigo (Europe) SL*

Subject C: *ES*

X509SKI

X509 SK I *5dbQQcJHwMRygaU+LRIY6VsIKTg=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

43.9.1 - Extension (critical): additionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name	[en]	Qualified Certificates issued by Sectigo Qualified Website Authentication CA E39
Name	[es]	Certificados Cualificados emitidos por Sectigo Qualified Website Authentication CA E39

Version: 3

Serial Number: 88805007699422138726469398921566811023

[illegible]

Page 1382

Issuer C: *GB*
Subject CN: *Sectigo Qualified Website Authentication CA E39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
Valid from: *Wed Sep 18 02:00:00 CEST 2024*
Valid to: *Sun Sep 18 01:59:59 CEST 2039*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2B:02:09:3C:EC:F8:82:C7:8E:CD:25:08:06:AC:8A:D0:95:5A:1E:23:C1:0E:E2:C3:D6:5A:CA:31:2A:D4:6C:D4:04:72:01:D8:9D:82:5F:FE:2C:07:58:46:83:BB:D5:EA:CD:E7:5E:8F:A2:37:74:E2:C8:C8:32:44:30:2E:45:97*
Authority Key Identifier *D1:22:DA:4C:59:F1:4B:5F:26:38:AA:9D:D6:EE:EB:0D:C3:FB:A9:61*
Subject Key Identifier *EE:4E:E1:B1:E1:13:8F:69:CB:9A:EE:D9:C4:C0:E4:DC:A7:2B:B1:E3*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CRL Distribution Points *http://crl.sectigo.com/SectigoPublicServerAuthenticationRootE46.crl*
Authority Info Access *http://crt.sectigo.com/SectigoPublicServerAuthenticationRootE46.p7c*
http://ocsp.sectigo.com
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *05:46:16:34:19:58:49:A1:BC:CC:99:26:49:12:05:4F:DE:B9:87:A5:2E:66:13:12:AE:9C:CA:3E:3E:D8:D3:18*

X509SubjectName

Subject CN: *Sectigo Qualified Website Authentication CA E39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*

X509SKI

X509 SK I *7k7hseETj2nLmu7ZxMDk3KcrseM=*

Service Status

Service status description *[en] undefined.* <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

[es] undefined.

Status Starting Time *2025-06-10T00:00:00Z*

43.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

43.11 - Service (granted): Qualified Certificates issued by Sectigo Qualified Website Authentication CA R39

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	<i>[en]</i> <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i> <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	Qualified Certificates issued by Sectigo Qualified Website Authentication CA R39

Name [es] *Certificados Cualificados emitidos por Sectigo Qualified Website Authentication CA R39*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 190915774391050142477667018687804850969

[illegible]

Signature algorithm: *SHA384withRSA*

Issuer CN: *Sectigo Public Server Authentication Root R46*

Issuer O: *Sectigo Limited*
Issuer C: *GB*
Subject CN: *Sectigo Qualified Website Authentication CA R39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
Valid from: *Wed Sep 18 02:00:00 CEST 2024*
Valid to: *Sun Sep 18 01:59:59 CEST 2039*
Public Key:

```

30:82:01:A2:30:0D:06:09:2A:86:4B:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:C8:EE:D6:7A:ED:08:0C:F7:00:DF:81:02:D2:A5:2E:25:C1:FA:2C:19:C7:D1:6C
54:34:56:CC:04:F4:8C:6D:DA:A1:E8:62:E3:A1:A5:AE:6F:9D:09:F8:F3:D4:82:88:55:D8:0E:6C:8F:86:E1:E6:F2:38:A3:52:9E:9B:A1:27:DF:2A:BF:46:CF:EF:25:CF:48:E3:F4:DD:00:82:94:D
2:68:EC:40:C5:8B:D1:0A:C0:68:4E:F7:5C:9C:3B:DE:6F:4F:B5:8D:16:66:1E:3E:37:06:3B:A0:A8:90:AC:71:0B:8F:A0:83:E2:BE:3B:0A:05:72:E4:6A:85:AB:65:49:7B:17:D7:34:D3:6F:24:93:
1E:4A:84:9D:DC:03:F0:92:EB:0F:93:DC:E1:C5:17:D8:E8:23:D6:3F:97:D1:1D:64:2F:92:F5:13:FF:8F:DB:1B:6D:DA:29:AC:0A:26:05:8F:DF:D2:17:7F:5D:6E:14:AE:06:4A:36:50:50:B2:4A:6
8:40:F2:12:89:E6:E6:2A:60:72:14:50:DD:AD:86:30:79:DF:F5:9A:E6:CF:DF:77:5B:5A:23:33:9F:07:44:8F:31:A0:89:14:5E:34:65:3C:64:0D:59:EC:49:68:81:27:E0:19:68:1A:C9:19:6A:AF
7E:97:90:27:3F:A7:10:6E:28:48:B3:82:29:D7:AD:2D:3B:2B:7B:CE:29:98:3F:C1:7E:68:F0:43:2D:2C:1F:00:ED:16:77:E7:86:C8:0D:E4:71:C8:16:4B:77:77:7B:AF:DC:21:23:58:90:2E:3B:7
7:B2:FB:6E:24:9C:12:F4:02:D6:80:34:A1:E2:66:75:1B:F3:C9:ED:46:54:55:BE:1E:15:2C:FD:B8:99:2D:72:64:7F:43:ED:9A:B3:92:A4:F6:A0:53:20:8F:97:49:95:7B:AE:1F:63:CC:F0:71:47:C
A:FE:6E:1E:6E:AB:D0:72:8F:ED:C1:FA:1E:79:20:DB:60:3E:38:B5:15:5D:46:5B:49:EF:06:2B:02:03:01:00:01

```

Authority Key Identifier *56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49*
Subject Key Identifier *2A:64:DA:5B:61:4B:84:BD:6C:2C:C1:25:4E:A4:15:E1:8C:65:10:63*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CRL Distribution Points *http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl*
Authority Info Access *http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c*
http://ocsp.sectigo.com
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *AC:8C:7E:F9:6E:B4:B5:35:FB:FB:4E:75:21:F1:30:53:61:98:A6:0D:FF:71:63:12:B2:2D:4A:CC:4A:FE:9A:7D*
X509SubjectName
Subject CN: *Sectigo Qualified Website Authentication CA R39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
X509SKI
X509 SK I *KmTaW2FLhL1sLMEITqQV4YxIEGM=*

Issuer O: *Sectigo Limited*
Issuer C: *GB*
Subject CN: *Sectigo Qualified Website Authentication CA Natural E39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
Valid from: *Wed Sep 18 02:00:00 CEST 2024*
Valid to: *Sun Sep 18 01:59:59 CEST 2039*
Public Key: *30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:F8:8C:23:AD:99:C4:35:79:17:92:5F:3A:8C:31:2B:AB:F6:9D:8A:2E:B7:DA:C7:B1:80:AD:33:4F:B
D:33:1D:02:C6:9E:E6:B0:34:89:77:9D:DF:BF:D1:B6:A9:E8:FC:ED:12:B7:6D:4A:F8:1D:54:EC:F6:31:29:C0:B0:11:8D:72*
Authority Key Identifier *D1:22:DA:4C:59:F1:4B:5F:26:38:AA:9D:D6:EE:EB:0D:C3:FB:A9:61*
Subject Key Identifier *D3:0E:2F:79:83:74:6D:3C:2D:6F:BA:F0:C1:CA:6E:70:20:02:39:3A*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CRL Distribution Points *http://crl.sectigo.com/SectigoPublicServerAuthenticationRootE46.crl*
Authority Info Access *http://crt.sectigo.com/SectigoPublicServerAuthenticationRootE46.p7c
http://ocsp.sectigo.com*
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *00:C3:67:A7:74:B7:CE:9A:0F:79:13:42:38:3F:86:5F:2A:F6:CD:37:67:4B:85:16:7E
:6F:23:9E:31:3D:60:BB*
X509SubjectName
Subject CN: *Sectigo Qualified Website Authentication CA Natural E39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
X509SKI
X509 SK I *0w4veYN0bTwtb7rwwcpucCACOTo=*
Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

43.12.1 - Extension (critical): additionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

Service type description	<i>[en]</i> A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	<i>[es]</i> Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Name	[es]	Certificados Cualificados emitidos por Sectigo Qualified Website Authentication CA Natural R39

[illegible]

Page 1388

Issuer O: *Sectigo Limited*
Issuer C: *GB*
Subject CN: *Sectigo Qualified Website Authentication CA Natural R39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
Valid from: *Wed Sep 18 02:00:00 CEST 2024*
Valid to: *Sun Sep 18 01:59:59 CEST 2039*
Public Key:

```

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:E5:EC:0E:02:A4:FD:F3:14:07:79:B0:96:65:65:E4:7D:7F:18:BD:89:E1:F2:DB:
33:30:16:0D:E1:22:83:33:08:0E:54:73:01:08:69:E8:2A:88:22:EC:E3:A6:D6:15:94:D3:65:CD:09:61:19:35:46:47:05:49:53:0C:C4:F8:6F:08:DC:D8:2C:64:DE:01:1B:D9:08:39:30:1E:56:
4B:D8:CE:E0:A3:15:7E:9D:E8:88:B4:80:1E:A2:C6:B1:B1:3F:E8:EC:D4:2B:A9:89:01:E1:D9:FD:26:62:70:C8:CA:66:57:51:D3:08:08:82:DF:36:BC:89:65:8A:FC:49:89:37:8F:C3:A6:83:FF:D
C:98:BB:0B:40:77:E6:29:04:03:5E:3C:6D:C7:20:EB:29:B6:43:97:C0:9C:5C:75:8D:4A:AC:78:25:44:56:B0:71:81:D6:33:00:16:31:2D:46:BA:4C:98:C0:4F:DA:81:C4:7F:B5:87:30:F0:92:0E
DD:64:7C:38:89:AA:22:6F:65:06:C0:96:83:5E:E4:43:47:FD:F8:F0:66:18:38:3F:A1:60:69:CA:34:34:9F:8C:68:8F:D4:E8:0F:41:FD:D6:54:41:8E:50:DF:FE:EB:6C:F3:8F:BA:8B:9E:88:09:B
A:FE:97:4E:35:F8:5F:F9:C4:0D:7D:52:86:5F:23:5B:37:0A:55:B4:98:12:79:F8:38:9E:E5:04:38:12:C2:87:98:F5:44:31:B4:86:34:4A:05:1F:10:FD:21:98:08:E1:40:95:9C:BC:A6:68:88:3A:0
9:A8:92:4C:DE:31:F9:48:0E:90:1A:A0:2B:75:78:1F:31:EC:C5:77:CB:32:E6:01:EB:C7:AF:0D:0F:75:31:E8:4D:8E:98:03:85:DE:CD:EC:ED:46:06:0B:5B:48:41:13:A5:B3:FF:F3:3B:80:BD:5F:
BC:BD:6E:E5:30:D6:07:07:B8:F0:04:43:2A:69:1F:C9:AA:36:76:EF:56:2B:FA:AE:C4:2C:E5:59:02:03:01:00:01

```

Authority Key Identifier *56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49*
Subject Key Identifier *15:4F:67:3A:28:A0:6B:C5:7A:34:DB:8A:B4:F1:C2:E6:39:F4:D9:5B*
Basic Constraints *IsCA: true - Path length: 0*
Extended Key Usage *id_kp_serverAuth*
Certificate Policies *Policy OID: 2.5.29.32.0*
CRL Distribution Points *http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl*
Authority Info Access *http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c*
http://ocsp.sectigo.com
Key Usage: *digitalSignature - keyCertSign - cRLSign*
Thumbprint algorithm: *SHA-256*
Thumbprint: *3C:CF:03:06:BE:D8:C9:10:B3:27:A1:5F:21:59:FD:D1:E4:14:47:4F:77:69:6C:3D:98:78:1B:11:60:27:7B:CA*
X509SubjectName
Subject CN: *Sectigo Qualified Website Authentication CA Natural R39*
Subject O: *Sectigo (Europe) SL*
Subject C: *ES*
X509SKI
X509 SK I *FU9nOiiga8V6NNuKtPHC5jn02Vs=*

Service Status			<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>	
	<i>[es]</i>	<i>undefined.</i>	

Status Starting Time *2025-06-10T00:00:00Z*

43.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuth entication</i>

44 - TSP: Docuten Tech SL

TSP Name

Name [en] Docuten Tech SL

Name [es] Docuten Tech SL

TSP Trade Name

Name [en] Docuten

Name [es] DOCUTEN TECH SL

Name [en] VATES-B85630978

PostalAddress

Street Address [en] AV/ PORTO DA CORUÑA, 3, PLANTA BAJA

Locality [en] A CORUÑA

Postal Code [en] 15008

Country Name [en] ES

ElectronicAddress

URI [en] mailto:administracion@docuten.com

URI [en] https://docuten.com/en

URI [es] https://docuten.com/es

TSP Information URI

URI [en] https://docuten.com/en/pcsc/

44.1 - Service (granted): Certificados cualificados emitidos por "DOCUTEN TECH CA1"

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Certificate fields details

Version: 3

Serial Number: 3425867390684835747

[illegible]

Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-A66721499
Issuer CN:	UANATACA ROOT 2016
Issuer OU:	TSP-UANATACA
Issuer O:	UANATACA S.A.
Issuer L:	Barcelona (see current address at www.uanataca.com/address)
Issuer C:	ES
Subject 2.5.4.97:	VATES-B85630978
Subject CN:	DOCUTEN TECH CA1
Subject OU:	TSP-PSC-DOCUTEN
Subject O:	Docuten Tech SL
Subject L:	A CORUÑA
Subject C:	ES

Valid from: *Fri Sep 18 10:52:21 CEST 2020*

Valid to: *Sun Sep 18 10:52:21 CEST 2033*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AD:19:04:5F:26:53:B1:FA:3A:C9:A6:27:B1:D4:28:B8:FD:DD:54:F4:C5:26:3B:10:41:2A:35:AE:E0:61:28:0E:C8:10:08:CA:DC:50:75:F1:95:BC:D4:32:6F:E1:F4:41:8D:33:AB:8A:98:90:DD:80:E9:DE:69:8D:EC:3E:A9:4A:04:2F:18:90:06:DA:E9:9C:B5:23:DA:43:56:7F:3E:FD:15:16:D8:58:97:F8:6C:AB:F2:8E:04:FE:8D:6D:AC:55:DF:0F:7B:DC:7C:FA:94:16:F0:97:3D:37:18:8A:76:75:F1:A0:0D:CC:EA:5E:CC:79:7B:4D:92:22:23:93:F8:0F:56:A8:5E:6F:66:3C:14:63:12:F0:5B:A0:8D:42:A4:40:CA:A2:2B:35:A9:77:03:B5:6B:0D:87:18:D2:03:10:67:5E:93:B9:A7:B4:A3:8B:6D:46:71:80:03:86:EA:77:3F:EC:38:C8:F6:9D:85:FC:BE:A4:59:E9:12:ED:3C:A9:91:9E:73:01:E7:0C:89:27:A1:E6:D5:E4:CB:D3:F4:4A:CE:E9:C3:4F:03:1F:41:35:94:E0:3D:B3:3F:07:DE:B6:E2:40:7E:D1:05:F2:4C:C7:23:6A:55:52:80:85:1F:CD:65:78:17:33:F0:93:7B:06:19:5A:EA:A3:24:E0:E5:9F:BE:91:B3:25:73:CB:00:65:78:D4:F6:D4:46:EF:F9:60:A1:28:C4:5E:C1:8F:8D:A6:A4:71:01:46:0F:0F:25:2F:1E:47:D3:54:2B:9E:A1:FE:F6:C2:11:5A:1B:97:D9:37:E8:F4:32:D5:22:41:29:11:0E:0E:93:EA:0E:E3:DD:43:00:20:33:B6:10:2F:3F:CS:61:5E:B6:F4:8D:11:BE:01:0E:7B:89:EE:76:D8:14:16:E8:2A:39:80:11:2F:8B:0B:05:01:B0:F2:E0:04:46:87:0A:90:FE:AF:11:99:85:3A:26:3B:A3:EB:E5:CE:DD:00:7B:67:64:16:F8:61:38:ED:D3:9C:7D:81:64:A8:63:02:DF:68:6E:03:02:32:28:A5:E4:ED:50:DC:77:24:EE:78:42:6A:24:5C:0F:60:30:EF:51:63:0A:88:6A:35:DB:03:E0:ED:3E:E0:B2:7B:1F:3C:6A:DC:B8:85:3F:2B:47:6F:AB:70:F8:38:16:26:63:A1:E8:12:53:F8:CC:35:EA:48:3C:F7:F8:15:00:F0:ED:0A:9D:5E:0A:6E:43:D1:5C:02:17:1E:8B:27:A2:3E:78:A0:41:D0:23:5B:08:8F:E5:31:F8:ED:F7:C1:36:80:67:8F:0D:BF:36:AF:3F:F5:43:60:69:17:1A:90:68:CD:C7:E8:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS pointer: https://www.docuten.com/es/pcsc/cps/
CPS text: [Subordinate Certification Authority Certificate of / Certificado de la
Autoridad de Certificación Subordinada de / Docuten tech - www.docuten.com]*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*

Subject Alternative Name *info@docuten.com*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B0:CD:0C:09:3E:A1:D6:52:75:40:14:C6:AF:2E:2B:B2:1B:E1:83:8E:95:8E:90:6B:05:50:5E:CB:AD:60:BD:97*

X509SubjectName

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN TECH CA1*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *Docuten Tech SL*

Subject L: *A CORUÑA*

Subject C: *ES*

X509SKI**X509 SKI***cOM/c2pcj9RgNYiekdikmYuv1g=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2021-07-01T01:00:00Z***44.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI**

[en]

*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***44.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI**

[en]

*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals***44.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]****Qualifier type description** [en]*undefined.*

[es]

*undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.56098.1.1.2***Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.56098.1.2.2.2***Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.56098.1.3.2***Policy Identifier:****Identifier**

[OIDASURN]

*urn:oid:1.3.6.1.4.1.56098.1.4.2***Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.56098.1.5.2
Description		

44.2 - Service (granted): Qualified electronic time stamps issued by “DOCUTEN timestamping electronic certificate - TSU01”

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST	
Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name		
Name	[en]	Qualified electronic time stamps issued by “DOCUTEN timestamping electronic certificate - TSU01”
	[es]	Sellos electrónicos cualificados de tiempo emitidos por “DOCUTEN timestamping electronic certificate - TSU01”

Service digital identities

Certificate fields details

Version:	3
Serial Number:	2726984659801151553
X509 Certificate	

-----BEGIN CERTIFICATE-----
MIHhCCBQugAwIBAgIJldyGZNIjGEEwDQYJKoZIhvcNAQELBQAwYoxCzAJBgNVBAYTAkVTMRkwEAYDVQQDDAIBIENPUJXODkUEXGDAWBgNVBAoMD0RvY3V0ZW4gVGVjaCBTDDYMBYGA1UECwwPVFNQ
LVBTQy1ET0NVVEVOMRkwFwYDQ0ODBBETONVVEVOIRFQ0gqOQExMRgwFgYDQORhDA9WQVRfUy1C
ODU2MzAsNzgwMjYhbnhNMAkMDAAMTAAODU0WkxMRgwFgYDQORhDA9WQVRfUy1C
EJA0BgNVBACMCUEgO095VcORQTEYMBYGA1UECgwPRE9DVRFTIBURUNIFNMMMRgwFgYDQORhDA9U
U1A0UFRDLURPQ1VURU4xPjA8BgNVBAMNURPQ1VURU4gdGltZXN0YX1waW5nIGVsZWNOcm9uaWMg
Y2YyYyGtmaWNoGUp4cTFRVTAxMRgwFgYDQORhDA9WQVRfUy1C
ODU2MzAsNzgwMjYhbnhNMAkMDAAMTAAODU0WkxMRgwFgYDQORhDA9WQVRfUy1C
Sib3DOEBAQUAA4IBDwAwggEKAoIBAQCyOLdZ8fdoSediOYfXaz1Db6QlfzyADUHTlze/Rf3Me
QITm7E0T4conOfixysbft5ZfNHEKzj8ShZtY3GujzskstfMocRfImvmbIVLhTClalmdR
uRzNCAq1UELO1LF+z3xyflumL6BjhhbEiem61d3dSLKZxe4TegoxDTKQ8MRwStc480yoE
LLFVZHaGRZQUBj39LCmEGOR64jGWIZ1jfgDFDU+2DRemHvhOtqwy6K3HBj3Ca0+qJlCW3Aai
MpwCWRKKmbH2i00KwF4pRcoGTgaeqy576jllKtCnXN0DWerhXyDiCaxZXva0+x3AgMBAAGj
ggJkMIICYD+BggrBgEFBQcBAQoRMHAAwNgYknYBBQUHAGGKmtHdHABLy9vY3NwMSS1YWSdGfj
Y55jb2V0cHVibGllL3BraS9vY3NwLzA2BggrBgEFBQcWAwYygaHR0CDovL29jc3AyLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQWBBOBQBr4jVB0gWFRUAISgw6gNlaCsyfjAIBgNV
HRME4AAMBGA1UdIwQIMBsaFH0j3NqXUUYDWinp1YjmlL9tMbsGA1UdeGQUmBKGluZm9A
ZG9jdXRib5ib20wga8GA1UdIASBncCpDpCBlwyKkwyBBAGDtlCjCBiDAwBggrBgEFBQcCARYk
aHR0cHM6Ly93d3cuZG9jdXRib5ib20vZXN0YX1waW5nIGVsZWNOcm9uaWMgY2YyYyGtmaWNoGUp4cTFRVTAxMRgwFgYDQORhDA9WQVRfUy1C
AGMAyOBAQAwCAYBACPEgECMH8GA1UdHwR4MHYwOaA3oDWGM2h0dHA6Ly9jcmwLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL2NybC9kb2N1dGVuLmNybDA5oDegN1YzaHR0CDovL2NybDludWfuYXRh
Y2Euf29RL3B1YmNpYy9wa2kYy3jL2RvY3V0ZW4uY3NwMGA1UdeGQUmBKGluZm9A
AFBEDDAKBgrBgEFBQcDCDABBgNVHREFFDASgRpbmZVQGRvY3V0ZW4uY29tMAOGCSqSib3DOEB
CwIAA4CAQCdyvKj1wnCBrr7oF6Mowcy3vkp6kcoinh20cxfekMY+B4nozJg+ntPgT6cCPad
re8BwL0EVTSw511tpw6QRC5+0c75OK4gknK8lieTwr+d3abWMutH4w3Q3MRH56+tsSHde
rYmhz2lm1SjAgBZgRqIXF7O6VGTKSPD7CmXR4sB4/O8BAJONmNDX6243Y3NUJ85xfTsToQl8efC
U4n6w9Zt9K7U95McSgyJthwdFnr+4c0Jl4QqmmDixqphwmeUW6gklbbX57ySMMDd/WaCQKxxT3
NB+AyX9DPYSDwZ25r0t0Tt+Zn0m8CsX73VavTczy8GjRTRnASjeso+YX4ueVMeM0uKdb1
13acJtp1bUVPDg4tM0wBaRK3p266DnHNIQe5YvYbSLuiddPIZmPcCQ9CDsAfteqNpxqr981NO
qKtMG+I04iyu1BpqXZPANfIL7Bx0hRtwzVFWTBKaOUVeND+jx1VLvxo/YvtA9mixg85F78wdRmB
L4vtG5Fm3zPp0p010adQOSN7UGdevBes2t5EL7AF3KJUNqUwE89OCBBPqCaCMdeV
GUHclgflrPxHAbPlbRxl+vEh1B0IZ8m0y0cRigY75mpejQWzLRe7LlUa0935TYE5YK1ejPAVnT
ZyPMgFFf5A==
-----END CERTIFICATE-----

Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-B85630978
Issuer CN:	DOCUTEN TECH CA1
Issuer OU:	TSP-PSC-DOCUTEN
Issuer O:	Docuten Tech SL
Issuer L:	A CORUÑA

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN timestamping electronic certificate - TSU01*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *DOCUTEN TECH SL*

Subject L: *A CORUÑA*

Subject C: *ES*

Valid from: *Thu Oct 08 12:18:54 CEST 2020*

Valid to: *Sun Oct 08 12:18:54 CEST 2028*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:38:B7:59:F0:57:68:49:E7:48:39:81:6D:5D:A6:75:0D:BE:90:95:FC:F2:00:35:07:B5:38:A2:CD:EF:D1:17:73:1E:42:24:E6:EC:4D:13:E1:CA:27:38:52:1F:C5:84:98:7E:DE:76:CC:5A:CD:1C:49:33:27:C4:A1:87:68:58:DC:91:AE:27:3B:10:2A:C7:CC:41:C4:45:21:F9:AF:99:B9:55:10:B8:53:0A:56:A5:96:67:51:B9:1C:CD:6C:20:2A:D5:41:0B:43:52:C5:F8:3D:F1:C9:F9:6E:9A:F2:FA:04:96:E1:85:B1:22:7A:6E:B5:B6:57:77:75:22:CA:65:77:B8:4D:E1:A8:C4:34:C9:29:0F:0C:47:08:D2:B5:CE:3C:3B:2A:04:2C:BB:45:57:61:DA:81:1F:D9:41:40:49:DF:D2:C2:12:61:06:41:1E:BB:24:65:88:67:52:5F:7E:00:C5:0D:4F:B6:0D:17:A6:1E:F8:4E:B6:0C:18:E8:AD:C7:06:2D:C2:68:4F:AA:24:80:96:DC:06:A2:32:9C:02:59:12:8A:99:F6:C7:64:8D:34:2B:01:78:A5:17:28:1A:D1:9A:7B:FA:B2:E7:BE:89:8A:59:13:72:78:B1:37:40:D6:7A:B8:57:95:80:E2:0A:AC:59:5E:58:DA:D3:EC:77:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *01:AF:82:55:07:48:16:15:15:00:95:28:30:EA:03:48:68:2B:32:16*

Basic Constraints *IsCA: false*

Authority Key Identifier *70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58*

Issuer Alternative Name *info@docuten.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.56098.2.10
CPS pointer: https://www.docuten.com/es/pcsc/cps/
CPS text: [Timestamping electronic certificate]
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/docuten.crl
http://crl2.uanataca.com/public/pki/crl/docuten.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@docuten.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *64:B2:6E:B2:72:6D:47:CA:A4:95:2F:E1:C2:88:E0:59:9E:94:5B:C7:DC:56:03:16:16:85:0B:4A:FB:39:A7:E6*

X509SubjectName

Subject 2.5.4.97: *VATES-B85630978*

Subject CN: *DOCUTEN timestamping electronic certificate - TSU01*

Subject OU: *TSP-PSC-DOCUTEN*

Subject O: *DOCUTEN TECH SL*

Subject L: *A CORUÑA*

Subject C: *ES*

X509SKI

X509 SK I *Aa+CVQdIFhUVAJUoMOoDSGgrMhY=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2021-07-01T01:00:00Z*

45 - TSP: MAILTECK, S.A.**TSP Name**

Name [es] MAILTECK, S.A.

Name [en] MAILTECK, S.A.

TSP Trade Name

Name [en] Mailteck, SA

Name [en] VATES- A31501901

Name [es] Mailteck SA

PostalAddress

Street Address [en] Polígono Industrial La Laguna, Avenida de la Recomba 14

Locality [en] Leganés

State Or Province [en] Madrid

Postal Code [en] 28914

Country Name [en] ES

PostalAddress

Street Address [es] Polígono Industrial La Laguna, Avenida de la Recomba 14

Locality [es] Leganés

State Or Province [es] Madrid

Postal Code [es] 28914

Country Name [es] ES

ElectronicAddress

URI [en] mailto:infomadrid@mailteck.com

URI [en] https://comunicaciones-legales.mailteck.com/

URI [es] https://comunicaciones-legales.mailteck.com/

TSP Information URI

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</i>
Service type description	<i>[en]</i>	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	<i>[es]</i>	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>

Service Name		
Name	[es]	Servicio cualificado de entrega electrónica certificada emitido para "CertySign MAILTECK"
Name	[en]	Qualified electronic certified delivery service issued for "CertySign MAILTECK"

Certificate fields details

Version: 3

Serial Number: 8514469021950128893

Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-A667214
Issuer CN:	UANATACA CA1
Issuer OU:	TSP-UANATACA
Issuer O:	UANATACA S.A.

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-A31501901*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *A31501901*

Subject O: *Mailteck SA*

Subject C: *ES*

Valid from: *Fri Feb 12 14:23:00 CET 2021*

Valid to: *Wed Feb 11 14:23:00 CET 2026*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:4B:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9F:62:8C:7D:9B:C3:72:C3:C7:C4:D4:70:02:53:49:9D:8C:37:AE:DB:0E:DE:03:85:6A:F0:9D:C7:56:AD:E7:BE:6F:3F:B2:F4:76:F0:82:37:5D:47:6C:8E:9B:6F:97:E1:3D:17:76:4B:49:EE:6D:6E:83:89:89:4E:EB:29:CF:C6:9F:36:B7:94:E9:29:78:3D:CE:57:82:B2:7A:F0:C8:F5:A3:0C:1E:3D:08:C5:F5:72:DA:89:22:E8:FF:E3:A2:6D:84:B9:B1:7A:62:01:49:9F:26:6F:F8:AF:80:09:DA:33:C2:37:D2:CE:7D:10:0F:C6:8B:F0:DD:E9:F7:F5:77:4B:7A:78:9C:BF:37:52:C6:B7:B6:78:64:F3:56:5F:8E:67:7D:7B:0B:68:75:EE:A0:1C:A1:0E:E8:65:41:50:D9:04:63:AE:3D:26:79:20:9E:E4:5E:C3:D6:44:3E:EE:40:C4:6F:31:70:39:AE:CB:DA:3B:A9:74:2F:C2:15:31:3A:58:00:41:B3:3B:E8:82:39:0F:11:82:14:CD:44:5C:CA:F4:CE:DB:E1:92:6C:A3:D1:C7:B4:00:B3:B2:45:74:EA:46:DB:55:AE:79:2E:2D:DE:3B:78:51:23:70:4C:CA:C2:11:0A:80:18:E2:A8:73:EE:01:BE:1B:B2:F9:FA:3F:EA:C3:02:03:01:00:01*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt*
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *87:DB:A5:98:1F:19:9C:48:9A:F8:02:38:F1:8C:BA:AD:5F:13:16:87*

Basic Constraints *IsCA: false*

Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points *<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>*
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *comunicacionescertificadas@mailteck.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *46:3B:20:D1:F6:C5:71:8A:4E:5D:22:A5:FC:3D:09:DC:83:2E:2A:2C:C7:50:1F:AE:6D:5B:EE:B8:2B:2B:1D:B5*

X509SubjectName

Subject 2.5.4.97: *VATES-A31501901*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *A31501901*

Subject O: *Mailteck SA*

Subject C: *ES*

X509SKI

X509 SK I *h9ulmB8ZnEia+Al48Yy6rV8TFoc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2026-03-26T02:00:00Z*

45.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada emitido para "CertySign MAILTECK"*

Name [en] *Qualified electronic certified delivery service issued for "CertySign MAILTECK"*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-A31501901*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *A31501901*

Subject O: *Mailteck SA*

Issuer CN: *UANATACA CA1 2021*
Issuer OU: *TSP-UANATACA*
Issuer O: *UANATACA S.A.*
Issuer L: *Barcelona*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-A31501901*
Subject CN: *CertySign*
Subject SERIAL NUMBER: *A31501901*
Subject O: *Mailteck, SA*
Subject C: *IT*
Valid from: *Wed Jul 09 10:07:00 CEST 2025*
Valid to: *Mon Jul 08 10:07:00 CEST 2030*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9D:13:9F:D4:7B:95:5E:7C:60:C2:2E:7F:38:31:46:BC:D4:8D:C5:81:2D:49:3C:2C:93:50:B7:1D:44:8E:E3:9B:13:61:C9:7E:92:A1:CE:37:08:32:2B:19:38:2B:62:75:F4:3B:34:E9:83:E7:60:AA:3B:51:E7:CA:1B:6A:1B:4D:68:FD:A7:F1:65:2F:F2:E9:FD:0F:98:9E:A0:54:3D:A1:04:C4:61:83:89:DD:0B:8F:B8:68:45:D9:7D:15:76:8F:27:8E:03:C7:74:25:1E:26:94:66:5F:A1:FD:CC:2F:BF:0B:40:17:D7:96:E5:A8:DE:A9:DE:FF:D8:87:20:2A:B6:BD:49:35:ED:79:12:7E:8C:72:84:FF:4A:28:89:C9:93:6B:3F:EA:4F:AC:37:5C:4B:EC:BE:4C:57:F3:54:94:93:52:FD:AA:E0:88:C3:11:59:6D:ED:E7:06:60:57:A5:11:31:48:29:BF:58:DF:30:9F:FA:6B:20:17:7C:C8:48:39:33:FF:0C:08:73:01:E9:96:9F:FA:9C:C3:62:F2:2D:25:C2:90:F9:80:1D:44:57:7D:AF:80:9E:29:AA:F4:73:15:D7:E6:91:65:F0:77:EA:E8:E6:AC:DA:E3:D6:27:E2:83:2D:03:72:21:72:F9:18:85:65:C4:EA:6B:F7:C6:9E:73:02:03:01:00:01*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD
Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/
Subject Key Identifier *36:E1:56:99:7B:8F:69:97:7B:70:AA:E5:C7:0A:CA:1F:92:B2:3D:7C*
Basic Constraints *isCA: false*
Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*
Issuer Alternative Name *info@uanataca.com*
Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage
id_kp_clientAuth

Subject Alternative Name
rpastor@mailteck.com

Key Usage:
digitalSignature - nonRepudiation - keyEncipherment

Thumbprint algorithm:
SHA-256

Thumbprint:
99:20:79:17:3B:30:03:4E:6D:C1:71:0C:41:EE:F0:05:59:45:D0:11:0B:06:4F:DF:FA:0D:EE:7C:2F:53:88:93

X509SubjectName

Subject 2.5.4.97:
VATES-A31501901

Subject CN:
CertySign

Subject SERIAL NUMBER:
A31501901

Subject O:
Mailteck, SA

Subject C:
IT

X509SKI

X509 SK I
NuFWmXuPaZd7cKrlxwrKH5KyPXw=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] *undefined.*
 [es] *undefined.*

Status Starting Time
2026-03-26T02:00:00Z

45.3 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals CertySign MAILTECK

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

Service type description [en] *A preservation service for qualified electronic signatures.*
 [es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name [en] *Qualified preservation service for qualified electronic signatures and qualified electronic seals CertySign MAILTECK*

Public Key:

30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9D:13:9F:D4:78:95:5E:7C:60:C2:2E:7F:38:31:46:BC:D4:8D:C5:81:2D:49:3C:2C:93:50:87:1D:44:8E:E3:98:13:81:C9:7E:92:A1:CE:37:08:32:2B:18:38:28:62:75:F4:38:34:E9:83:E7:60:AA:36:51:E7:CA:18:8A:1B:4D:68:FD:A7:F1:65:2F:F2:E9:FD:0F:98:9E:A0:54:3D:A1:04:C4:61:83:89:DD:0B:8F:86:68:45:D9:7D:15:76:8F:27:8E:03:C7:74:25:1E:26:94:66:5F:A1:FD:CC:2F:BF:0B:40:17:D7:96:E5:A8:DE:A9:DE:EF:D8:87:20:2A:B6:BD:49:35:ED:79:12:7E:8C:72:84:FF:4A:28:89:C9:93:6B:3F:EA:4F:AC:37:5C:4B:EC:BE:4C:57:F3:54:94:93:52:FD:AA:E0:88:C3:11:59:6D:ED:E7:06:60:57:A5:11:31:48:29:BF:58:DF:30:9F:FA:6B:20:17:7C:C8:48:39:33:FF:0C:08:73:01:E8:96:9F:FA:9C:C3:62:F2:2D:25:C2:90:F9:80:1D:44:57:7D:AF:80:9E:29:AA:F4:73:15:D7:E6:91:65:F0:77:EA:E8:E6:AC:DA:E3:D6:27:E2:83:2D:03:72:21:72:F9:18:85:65:C4:EA:68:F7:C6:9E:73:02:03:01:00:01

QCStatements - crit. = false*id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15**id_etsi_qcs_QcSSCD***Authority Info Access***http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c**http://ocsp1.uanataca.com/public/pki/ocsp/**http://ocsp2.uanataca.com/public/pki/ocsp/***Subject Key Identifier***36:E1:56:99:7B:8F:69:97:7B:70:AA:E5:C7:0A:CA:1F:92:B2:3D:7C***Basic Constraints***IsCA: false***Authority Key Identifier***81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68***Issuer Alternative Name***info@uanataca.com***Certificate Policies***Policy OID: 0.4.0.194112.1.3**Policy OID: 1.3.6.1.4.1.47286.1.9.6**CPS pointer: https://www.uanataca.com/public/cps/**CPS text: [Qualified certificate for e-seal in Remote QSCD]***CRL Distribution Points***http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl**http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl***Extended Key Usage***id_kp_clientAuth***Subject Alternative Name***rpastor@mailteck.com***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***99:20:79:17:3B:30:03:4E:6D:C1:71:0C:41:EE:F0:05:59:45:D0:11:0B:06:4F:DF:FA:0D:EE:7C:2F:53:88:93***X509SubjectName****Subject 2.5.4.97:***VATES-A31501901***Subject CN:***CertySign***Subject SERIAL NUMBER:***A31501901***Subject O:***Mailteck, SA***Subject C:***IT*

46 - TSP: CUSTOMER COMMUNICATIONS TECKNALIA, S.L.**TSP Name**

Name [es] *CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*

Name [en] *CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*

TSP Trade Name

Name [en] *Customer Communications Tecknalia, SL*

Name [en] *VATES-B86414000*

Name [es] *CUSTOMER COMMUNICATIONS TECKNALIA SL*

PostalAddress

Street Address [en] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

Locality [en] *Leganés*

State Or Province [en] *Madrid*

Postal Code [en] *28914*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

Locality [es] *Leganés*

State Or Province [es] *Madrid*

Postal Code [es] *28914*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:info@customercomms.com*

URI [en] *https://www.customercomms.com*

URI [es] *https://www.customercomms.com*

URI [es] *mailto:info@customercomms.com*

Issuer O: UANATACA S.A.
Issuer L: Barcelona (see current address at www.uanataca.com/address)
Issuer C: ES
Subject 2.5.4.97: VATES-B86414000
Subject CN: CertySign
Subject SERIAL NUMBER: B86414000
Subject O: CUSTOMER COMMUNICATIONS TECKNALIA SL
Subject C: ES
Valid from: Fri Feb 12 14:21:00 CET 2021
Valid to: Wed Feb 11 14:21:00 CET 2026
Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:07:78:5F:9D:D3:8A:04:A0:C1:84:9D:EC:9C:90:36:8A:E1:24:A2:EE:2F:D0:90:01:DD:22:65:E4:29:8C:AD:4D:9A:F0:01:37:6E:13:20:2D:08:9D:2C:BA:85:D5:0C:42:EE:AA:E6:E9:60:AE:28:FF:D7:22:47:BA:8C:90:10:82:1F:A3:79:99:CB:92:0D:52:B0:17:AF:AA:DE:DA:E8:47:8B:85:4B:25:FA:4D:CD:DA:9C:AE:E6:39:01:59:AC:F8:78:51:73:AE:2F:3B:AA:FC:04:40:99:C0:E1:27:FF:88:E3:97:F5:34:7E:B1:32:AC:34:7D:7A:3E:DA:76:4F:D1:00:E6:4B:6E:9:9:59:6A:F6:72:4B:7F:DF:C0:79:A9:7C:5E:EF:14:E5:1B:E0:F8:DD:2C:38:06:74:6D:04:14:F4:AE:AF:D3:C1:F8:26:D1:B7:FF:14:79:30:02:D8:48:87:67:34:94:4D:BD:AC:9C:88:BA:F7:59:7C:E5:1B:18:B8:73:FA:23:D1:41:8D:C3:09:11:84:05:77:26:85:64:8A:D0:FC:AF:D1:DF:82:1D:DD:A7:54:66:AE:90:BA:7D:7C:9B:8C:E0:D2:E1:DD:19:45:22:FD:9D:9F:7F:37:28:5D:D2:84:39:2E:EF:B1:64:F1:65:37:95:D7:CE:F6:C9:02:03:01:00:01
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD
Authority Info Access http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>
Subject Key Identifier DE:AA:E3:DC:09:D0:D0:F0:A4:9B:80:1A:80:EA:64:26:AF:12:1B:D0
Basic Constraints *IsCA: false*
Authority Key Identifier 2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5
Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Qualified certificate for e-seal in Remote QSCD]
CRL Distribution Points <http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>
Extended Key Usage *id_kp_clientAuth*
Subject Alternative Name *comunicacionescertificadas@customercomms.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *04:2B:A1:E7:60:3B:28:12:F8:C1:25:2B:D1:29:D0:E5:21:F6:A2:A5:28:9A:08:36:89:F3:A5:EF:A5:28:5A:8C*

X509SubjectName

Subject 2.5.4.97: *VATES-B86414000*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *B86414000*

Subject O: *CUSTOMER COMMUNICATIONS TECKNALIA SL*

Subject C: *ES*

X509SKI

X509 SK I *3qrj3AnQ0PCkm4AagOpkJq8SG9A=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2026-03-26T02:00:00Z*

46.1.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada emitido para "CertySign CUSTOMERSCOMMS"*

Name *[en]* *Qualified electronic certified delivery service issued for "CertySign CUSTOMERSCOMMS"*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B86414000*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *B86414000*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA1 2021*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B86414000*

Subject CN: *CertySign*

Subject SERIAL NUMBER: *B86414000*

Subject O: *Customer Communications Tecknalia, SL*

Subject C: *IT*

Valid from: *Wed Jul 09 10:04:00 CEST 2025*

Valid to: *Mon Jul 08 10:04:00 CEST 2030*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A4:10:96:D6:E6:B0:4A:F4:F7:C6:26:9D:92:F3:CE:7A:C7:FE:84:9E:A1:42:1A:6C:6B:0C:A5:E6:30:74:34:C4:70:D2:E2:13:59:8C:2A:F6:0B:25:95:11:8F:A0:0F:9D:90:46:01:69:81:F9:1C:11:6F:84:D8:DF:F3:B7:93:47:DB:52:68:D5:B5:3B:D7:9C:1B:2B:E7:65:52:C4:59:5C:8F:E3:57:6D:8B:C8:06:80:68:81:E6:EF:7E:60:CF:C4:67:21:B9:57:A7:9C:DA:4C:A8:C7:9C:05:20:AB:3B:D1:12:09:95:4F:86:85:EE:B5:E8:14:E6:E2:11:85:19:89:B4:1E:03:15:48:11:A0:41:FB:C7:84:67:C8:4C:8A:23:8C:A2:A3:5D:F7:27:07:F0:48:41:36:63:2B:FE:D0:E4:47:62:AE:A5:2C:4C:E2:DC:F2:4B:CF:32:7D:00:4F:7F:43:D5:D6:53:08:69:39:57:95:F0:CD:AE:3C:CE:0A:9E:FE:F4:CD:A6:BB:AB:CE:5E:6A:91:75:BF:F8:61:73:E6:79:2B:C4:41:A2:32:11:2C:48:1A:B8:92:37:FA:26:96:A2:9E:00:0F:88:C2:B8:59:F8:45:1B:D1:D2:22:DD:74:47:49:F3:26:86:5A:55:2D:19:F1:F6:A0:AA:D9:36:B5:02:03:01:00:01

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Authority Info Access
http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *4A:62:CA:5F:98:83:F7:3F:E4:1E:4D:3A:8E:F3:29:C9:F1:8D:26:5F*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 0.4.0.194112.1.3
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage
id_kp_clientAuth

Subject Alternative Name
rpastor@mailteck.com

Key Usage:
digitalSignature - nonRepudiation - keyEncipherment

Thumbprint algorithm:
SHA-256

Thumbprint:
*37:3B:49:D7:B3:14:B2:83:2C:D7:CB:39:33:8D:DC:83:C7:CA:EF:E8:87:F6:74:1F:E
F:13:F1:6F:97:C1:86:2B*

X509SubjectName

Subject 2.5.4.97:
VATES-B86414000

Subject CN:
CertySign

Subject SERIAL NUMBER:
B86414000

Subject O:
Customer Communications Tecknalia, SL

Subject C:
IT

X509SKI

X509 SK I
SmLKX5iD9z/kHk06jvMpyfGNJI8=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time
2026-03-26T02:00:00Z

46.3 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals CertySign CUSTOMERSCOMMS

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

Service type description [en] *A preservation service for qualified electronic signatures.*
[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name [en] *Qualified preservation service for qualified electronic signatures and qualified electronic seals CertySign CUSTOMERSCOMMS*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A4:10:96:D6:E6:80:4A:F4:F7:C6:26:9D:92:F3:CE:7A:C7:FE:84:9E:A1:42:1A:6C:6B:0C:A5:E6:30:74:34:C4:70:D2:E2:13:59:8C:2A:F6:0B:25:95:11:8F:A0:0F:9D:90:46:01:89:B1:F9:1C:11:6F:84:D8:DF:F3:B7:93:47:D8:52:68:D5:3B:B7:9C:1B:28:E7:65:52:C4:59:5C:8F:E3:57:6D:8B:C8:06:80:68:81:E6:EF:7E:60:CF:C4:67:21:89:57:A7:9C:DA:4C:A8:C7:9C:05:2D:AB:3B:D1:12:09:95:4F:86:85:EE:B5:E8:14:E6:E2:11:85:19:89:84:1E:03:15:48:11:A D:41:FB:C7:84:67:C8:4C:8A:23:8C:A2:A3:5D:F7:27:07:F0:48:41:36:63:2B:FE:D0:E4:47:62:AE:A5:2C:4C:E2:DC:F2:4B:CF:32:7D:00:4F:7F:43:D5:D6:53:08:69:39:57:95:F0:CD:AE:3C:CE:0A:9E:FE:F4:CD:A6:8B:AB:CE:5E:6A:91:75:BF:F8:81:73:E6:79:2B:C4:41:A2:32:11:2C:48:1A:B8:92:37:FA:26:96:A2:9E:00:0F:88:C2:88:59:F8:45:1B:D1:D2:22:DD:74:47:49:F3:26:86:5A :55:2D:19:F1:F6:A0:AA:D9:36:B5:02:03:01:00:01

QCStatements - crit. = false*id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15**id_etsi_qcs_QcSSCD***Authority Info Access***http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c**http://ocsp1.uanataca.com/public/pki/ocsp/**http://ocsp2.uanataca.com/public/pki/ocsp/***Subject Key Identifier***4A:62:CA:5F:98:83:F7:3F:E4:1E:4D:3A:8E:F3:29:C9:F1:8D:26:5F***Basic Constraints***IsCA: false***Authority Key Identifier***81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68***Issuer Alternative Name***info@uanataca.com***Certificate Policies***Policy OID: 0.4.0.194112.1.3**Policy OID: 1.3.6.1.4.1.47286.1.9.6**CPS pointer: https://www.uanataca.com/public/cps/**CPS text: [Qualified certificate for e-seal in Remote QSCD]***CRL Distribution Points***http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl**http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl***Extended Key Usage***id_kp_clientAuth***Subject Alternative Name***rpastor@mailteck.com***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***37:3B:49:D7:B3:14:B2:83:2C:D7:CB:39:33:8D:DC:83:C7:CA:EF:E8:87:F6:74:1F:E F:13:F1:6F:97:C1:86:2B***X509SubjectName****Subject 2.5.4.97:***VATES-B86414000***Subject CN:***CertySign***Subject SERIAL NUMBER:***B86414000***Subject O:***Customer Communications Tecknalia, SL***Subject C:***IT*

47 - TSP: Iberexaminis Consulting S.L.

TSP Name

Name	[en]	Iberexaminis Consulting S.L.

Name	[es]	Iberexaminis Consulting S.L.

TSP Trade Name

Name	[en]	EXAMINIS

Name	[es]	EXAMINIS

Name	[en]	VATES-B39877915

Name	[en]	Iberexaminis Consulting SL

PostalAddress

Street Address	[en]	CALLE JOAQUIN CAYON 14 4ªA

Locality	[en]	TORRELAVEGA

State Or Province	[en]	CANTABRIA

Postal Code	[en]	39300

Country Name	[en]	ES

PostalAddress

Street Address	[es]	CALLE JOAQUIN CAYON 14 4ªA

Locality	[es]	TORRELAVEGA

State Or Province	[es]	CANTABRIA

Postal Code	[es]	39300

Country Name	[es]	ES

ElectronicAddress

URI	[en]	mailto:info@iberexaminis.com

URI	[en]	https://www.iberexaminis.com

TSP Information URI

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified electronic time stamps issued by "Examinis TSU01"

Name [es] *Sellos electrónicos cualificados de tiempo emitidos por “Examinis TSU01”*

Certificate fields details

Version: 3

Serial Number: 8182055068043534744

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: UANATACA CA2 2016

Issuer OU: TSP-UANATACA

Issuer O: UANATACA S.A

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B39877915*

Subject CN: *Examinis TSU01*

Subject OU: *IBEREXAMINIS TSP*

Subject O: *Iberexaminis Consulting SL*

Subject L: *Torrelavega*

Subject C: *ES*

Valid from: *Thu Jan 14 13:18:01 CET 2021*

Valid to: *Sun Jan 14 13:18:01 CET 2029*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F3:E7:3E:D8:1D:09:32:D8:F6:3F:43:8F:A1:F3:8F:56:5C:E8:1F:A3:83:40:D4:0E:CF:5D:0D:8B:25:22:C4:1E:57:81:5A:2A:2E:D7:D4:A2:99:44:D0:F4:68:7E:5A:F9:33:C3:1F:AD:20:8B:09:10:0B:60:BC:BA:F7:52:F2:45:7E:83:1E:8A:84:3B:3D:FB:07:19:BF:89:D8:E0:D F:55:44:0E:80:EE:A1:41:25:B3:AD:1D:C5:6F:08:46:B8:3E:33:D2:4B:96:9F:40:3D:C4:AE:F7:E0:54:C0:6B:70:38:6F:C0:78:2F:CF:C7:28:38:F7:F0:5A:62:C9:85:78:FF:A0:8F:EB:F8:8A:0D:D B:39:D8:B4:7B:F3:C9:92:1F:26:2C:98:44:1E:03:93:EC:B7:2C:11:D1:21:65:1B:2C:CF:1F:56:86:0C:B5:E3:47:0E:76:5F:08:4E:47:79:CB:EB:62:70:5F:C0:A4:87:31:87:D8:39:6B:03:89:86: 14:77:18:5C:00:B1:C2:B7:A5:29:C8:44:0B:C6:30:F1:19:E1:AB:1A:C0:C3:F0:78:AC:DE:CA:65:78:AF:74:1D:2A:03:56:D6:E9:35:A6:49:95:07:F7:A0:2A:BE:56:7F:97:2C:C2:25:E4:F0:AD:0 D:DB:F0:3F:44:6E:42:76:45:45:77:02:03:01:00:01

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *79:D2:C4:CF:54:E0:99:39:45:7D:D3:1B:E1:67:DE:6E:16:C2:DC:46*

Basic Constraints *IsCA: false*

Authority Key Identifier *7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@iberexaminis.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *54:A9:49:39:DE:E1:89:3D:A5:74:AD:98:DB:46:B4:58:C0:22:82:1B:BE:AA:7A:78:0 2:47:2F:A3:46:75:2A:12*

X509SubjectName

Subject 2.5.4.97: *VATES-B39877915*

Subject CN: *Examinis TSU01*

Subject OU: *IBEREXAMINIS TSP*

Subject O: *Iberexaminis Consulting SL*

Subject L: *Torrelavega*

Subject C: *ES*

X509SKI

X509 SK I *edLEz1TgmTIFdMb4WfebhbC3EY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2023-11-08T00:00:00Z*

47.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en] Qualified electronic time stamps issued by "Examinis TSU01"*

Name *[es] Sellos electrónicos cualificados de tiempo emitidos por "Examinis TSU01"*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B39877915*

Subject CN: *Examinis TSU01*

Subject OU: *IBEREXAMINIS TSP*

Subject O: *Iberexaminis Consulting SL*

Subject L: *Torrelavega*

Subject C: *ES*

X509SKI

X509 SK I*edLEz1TgmTIFfdMb4WfebhbC3EY=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Status Starting Time***2021-10-04T01:00:00Z*

48 - TSP: Lleidanet PKI S.L.**TSP Name**

Name [en] *Lleidanet PKI S.L.*

Name [es] *Lleidanet PKI S.L.*

TSP Trade Name

Name [en] *VATES-B97458996*

Name [en] *INDENOVA*

Name [en] *inDenova SL*

Name [en] *Indenova S.L.*

Name [en] *Lleidanet PKI*

Name [en] *Lleidanet PKI SLU*

PostalAddress

Street Address [en] *Calle Andarella nº 2, escalera 2, piso 3º, puerta 8*

Locality [en] *Xirivella*

State Or Province [en] *Valencia*

Postal Code [en] *46950*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Calle Andarella nº 2, escalera 2, piso 3º, puerta 8*

Locality [es] *Xirivella*

State Or Province [es] *Valencia*

Postal Code [es] *46950*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:indenova@indenova.com*

URI	[en]	https://www.indenova.com
URI	[es]	https://www.indenova.com

Page 1424

Issuer CN:	<i>Certification Authority Root Indenova SL</i>
Issuer O:	<i>Indenova SL</i>
Issuer SERIAL NUMBER:	<i>B97458996</i>
Issuer OU:	<i>Certification Authority Indenova SL</i>
Issuer L:	<i>Valencia</i>
Issuer C:	<i>ES</i>
Subject 2.5.4.13:	<i>inDenova Subordinate CA 003</i>
Subject CN:	<i>inDenova SUB CA 003</i>
Subject O:	<i>inDenova SL</i>
Subject 2.5.4.97:	<i>VATES-B97458996</i>
Subject SERIAL NUMBER:	<i>B97458996</i>
Subject OU:	<i>Certification Authority inDenova SL</i>
Subject T:	<i>Subordinate Certificate Authority inDenova SL</i>
Subject L:	<i>VALENCIA</i>
Subject C:	<i>ES</i>
Valid from:	<i>Mon May 31 10:32:46 CEST 2021</i>
Valid to:	<i>Fri May 31 10:32:46 CEST 2041</i>
Public Key:	<i>30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B7:2F:A2:17:D4:C4:A2:22:5F:21:D8:C5:F1:FC:00:9F:16:58:A0:59:E6:8B:1F:71:D8:09:9A:48:11:CE:92:CF:29:4B:D7:CC:56:8E:05:98:B3:09:AD:61:A9:5C:B8:2F:A6:23:0F:79:E6:2F:5E:3C:62:0E:6E:70:42:14:4E:9F:0F:06:D1:E8:01:82:3E:4B:81:7F:A2:9D:21:15:BC:13:82:57:7F:24:5D:AE:BC:86:B4:8D:83:A8:A1:37:50:3C:91:86:57:A9:4B:4E:4A:28:25:6A:11:4B:D8:90:7C:8F:F6:1B:59:DF:BC:93:20:DF:0B:52:F0:3F:35:35:44:E6:16:7E:E3:65:07:E7:76:03:0A:33:CF:55:85:44:8C:B8:3D:EC:76:95:43:5F:36:F9:F1:EA:16:EA:BB:6B:EA:38:AD:C3:62:4D:A7:0B:18:40:A6:98:16:FD:57:A1:F6:0D:C4:8A:DA:2F:5C:A8:C4:4C:F8:D2:5D:A0:8F:5F:7D:55:E7:EA:4A:80:38:DE:64:95:8F:FE:58:23:1C:90:BE:55:CB:51:B4:D9:E2:D3:8A:43:F7:0F:67:65:5A:A2:16:68:91:24:49:11:2D:35:71:86:14:3D:5F:C0:AF:6D:62:1B:EB:8A:1D:49:C9:9CA7:8F:EE:F8:D8:64:AA:2A:BC:2C:02:1F:7E:BD:28:3C:1D:CF:1F:D5:F3:BA:71:85:80:DC:32:A3:90:3F:5D:80:5E:A9:F5:E5:67:DE:76:0E:E9:5E:1E:43:1E:F8:9E:80:38:B9:EE:7A:DB:06:E9:1C:55:9A:92:4B:59:E2:F6:98:2E:2A:46:79:15:67:70:D4:3A:20:B6:79:D0:7B:31:58:41:72:60:85:09:29:D7:21:5F:F7:85:34:94:86:BB:86:3C:11:84:23:11:3B:E8:91:A7:2B:73:71:DB:AB:EA:EC:88:68:18:0B:A2:29:4B:5A:F7:95:36:F8:00:AC:95:37:DC:D1:17:89:62:14:51:B1:A5:46:48:9B:D2:23:22:B0:53:8A:E9:F8:BA:84:5D:36:31:D1:49:11:DC:27:13:A4:DD:30:BE:47:40:69:24:FD:24:1C:33:39:02:3E:19:30:D2:D6:B8:CD:60:03:B4:D3:7F:B8:90:1A:F2:04:C9:87:8F:C0:E9:6F:53:EC:11:AB:09:14:D5:C7:0B:8E:22:9C:40:D9:91:88:EC:56:C0:30:10:E0:0A:F2:55:E3:D4:C8:52:E6:74:57:38:8B:C7:93:B4:C6:4E:09:09:FB:30:C4:C6:43:04:1C:48:6F:C4:2B:13:5A:18:2D:50:F1:2C:1B:34:9E:DF:94:1C:A3:20:96:19:3F:02:03:01:00:01</i>
Subject Key Identifier	<i>C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46</i>
Authority Key Identifier	<i>B9:A1:B7:83:14:F5:DA:D8:BC:10:89:01:C0:E2:D2:C5:F7:A0:3F:1B</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://cps.esigna.es/sub/cps_sub003_ca.pdf</i>
Authority Info Access	<i>http://certs.esigna.es/root/ca_root_indenova_sl.crt</i> <i>http://ocsp2.esigna.es</i>

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.esigna.es/root/ca_root_indenova_sl.crl*
http://crl1.esigna.es/root/ca_root_indenova_sl.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *34:52:E9:67:43:44:26:07:F2:1D:85:08:4C:3D:B8:97:E3:75:49:FE:D2:3F:13:5C:DB:D2:02:E6:90:D5:2E:25*

X509SubjectName

Subject 2.5.4.13: *inDenova Subordinate CA 003*

Subject CN: *inDenova SUB CA 003*

Subject O: *inDenova SL*

Subject 2.5.4.97: *VATES-B97458996*

Subject SERIAL NUMBER: *B97458996*

Subject OU: *Certification Authority inDenova SL*

Subject T: *Subordinate Certificate Authority inDenova SL*

Subject L: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *w5x0XdAiqO3y7lC+r617aymAbEY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*
[es] *undefined.*

Status Starting Time

2024-06-05T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

48.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

48.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

48.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.2

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.1

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.2

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.3

Policy Identifier:

Identifier	[OIDA sURN]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.1

Policy Identifier:

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.3.2</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.3.3</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.4.3</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.4.4</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.5.3</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.5.4</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.5.5</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.6.3</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.6.4</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.6.5</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.7.3</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.7.4</i>
Policy Identifier:		
Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.49959.1.1.3.7.5</i>

Description

48.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[es]* *Servicio de expedición de certificados electrónicos cualificados expedidos por «inDenova SUB CA 003»*

Name *[en]* *Qualified certificates issued by «inDenova SUB CA 003»*

Service digital identities**X509SubjectName**

Subject 2.5.4.13: *inDenova Subordinate CA 003*

Subject CN: *inDenova SUB CA 003*

Subject O: *inDenova SL*

Subject 2.5.4.97: *VATES-B97458996*

Subject SERIAL NUMBER: *B97458996*

Subject OU: *Certification Authority inDenova SL*

Subject T: *Subordinate Certificate Authority inDenova SL*

Subject L: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *w5x0XdAiqO3y7lC+r617aymAbEY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-12-13T02:00:00Z*

48.1.4.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

48.1.4.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

48.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[en]	undefined.
	[es]	undefined.

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.2

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.2

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.3

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.1

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.2

Policy Identifier:

Identifier	[OIDsURN]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.3

Issuer T: *Service Timestamping inDenova SL*
Issuer L: *VALENCIA*
Issuer C: *ES*
Subject 2.5.4.13: *inDenova SL Timestamping Certificate 003*
Subject CN: *inDenova TSU 003*
Subject O: *inDenova SL*
Subject 2.5.4.97: *VATES-B97458996*
Subject SERIAL NUMBER: *B97458996*
Subject OU: *Trusted Timestamp Service inDenova SL*
Subject T: *Service Timestamping inDenova SL*
Subject L: *VALENCIA*
Subject C: *ES*
Valid from: *Mon May 31 10:53:49 CEST 2021*
Valid to: *Sat May 31 10:53:49 CEST 2031*
Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B6:D9:EE:E8:47:B3:AD:82:3E:88:43:83:8D:05:C0:2A:F8:88:3B:EA:52:2C:DF:4B:68:7B:F4:6F:32:65:EF:AE:32:57:D6:57:72:2B:DA:3F:C3:A3:22:06:59:F6:39:74:6C:D1:EE:8A:80:91:5E:72:2B:74:0C:D5:1E:0C:54:98:45:5D:07:85:83:1F:DE:AD:AE:06:03:1E:E7:6C:53:34:99:74:13:BE:AB:12:A5:BF:BF:29:91:73:66:78:83:5F:2A:CA:D0:CE:C6:02:F5:D5:80:36:64:CC:DE:DE:41:73:8B:E2:76:3E:0A:2B:E3:72:C3:33:80:FB:20:4D:72:2A:CE:57:08:6D:73:49:3F:D1:A3:BE:E6:33:33:7E:06:D8:81:BD:6D:C1:BF:DA:02:38:55:05:8F:B8:35:5B:AB:3A:D8:06:D5:CE:85:39:05:47:56:E6:EF:0C:A2:0C:78:D2:04:AF:F2:81:C1:D2:34:9F:6F:BC:36:E0:1A:1C:80:5B:2B:34:A1:C8:81:00:89:21:22:FE:0E:26:CC:49:5D:58:B3:1C:C8:E1:E8:69:A6:C0:CF:0D:4A:8B:1E:80:45:2E:D2:1D:30:0A:B4:2D:E2:C0:1D:07:9F:79:46:9F:A0:4E:28:80:DA:F8:2C:21:FD:A2:F8:9E:94:74:E5:31:D5:85:18:66:F8:65:C4:E1:9F:18:F8:71:9E:94:E3:CB:7D:26:CB:B4:19:E3:31:14:37:9A:C8:E2:1E:7A:39:B6:07:E8:33:62:1E:84:E8:80:5B:0A:16:C1:6E:79:7B:DA:25:6E:17:43:EE:7C:2C:8F:E8:A7:C3:97:4A:D3:F1:01:7C:64:ED:8E:D3:80:4A:4E:FE:DE:C0:A9:5D:52:9F:BB:01:70:79:FF:E2:F4:A6:D8:C6:48:21:53:74:3D:69:BB:16:8C:CC:2F:72:8C:7B:EF:22:A1:AA:00:FE:94:8A:2F:56:E4:96:D3:82:2D:7C:6C:F7:9D:DD:9B:4B:2F:30:98:0E:C3:BF:5C:7F:2F:1A:5B:3B:48:1D:AD:50:97:41:23:34:85:FF:A5:93:AE:71:7A:7E:52:A4:26:DA:9A:1E:7E:40:85:C1:94:21:C3:C2:17:EC:6A:75:88:AE:A5:83:40:7F:18:0C:95:2D:88:A5:43:43:49:94:98:F9:3B:E9:29:40:72:C1:1E:A4:DE:80:BF:E9:DC:EF:8A:D5:6B:24:AC:DE:6A:05:86:B D:07:0D:F2:56:FE:29:4F:F3:18:3B:11:C4:96:35:FE:FA:35:A0:F6:99:B6:4A:C5:22:68:70:65:89:4D:11:92:E8:7C:64:EE:BD:30:25:C9:49:73:C6:DF:F9:02:03:01:00:01
Subject Key Identifier *90:69:12:08:5C:DA:C0:64:CE:86:0D:60:EF:FA:7A:34:75:2C:EB:B8*
Authority Key Identifier *2B:6E:5E:F1:DA:66:7D:B6:E7:AE:1F:60:6E:9E:DA:3A:3F:B3:EF:B1*
Extended Key Usage *id_kp_timeStamping*
Certificate Policies *Policy OID: 1.3.6.1.4.1.49959.1.1.5*
CPS pointer: http://cps.esigna.es/tsa/cps_tsa003.pdf
CPS text: [Warranty limitations of this certificate can be found in the CPS]
Authority Info Access *http://certs.esigna.es/tsa/indenova_tsa_003.crt*
<http://ocsp2.esigna.es>
Basic Constraints *IsCA: false*
CRL Distribution Points *http://crl.esigna.es/tsa/indenova_tsa_003.crl*
http://crl1.esigna.es/tsa/indenova_tsa_003.crl

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *83:77:19:18:FB:57:38:FC:75:5A:43:90:41:67:C2:21:9D:D9:3A:C4:69:81:7B:14:33:D0:14:9E:65:B0:23:6D*

X509SubjectName

Subject 2.5.4.13: *inDenova SL Timestamping Certificate 003*

Subject CN: *inDenova TSU 003*

Subject O: *inDenova SL*

Subject 2.5.4.97: *VATES-B97458996*

Subject SERIAL NUMBER: *B97458996*

Subject OU: *Trusted Timestamp Service inDenova SL*

Subject T: *Service Timestamping inDenova SL*

Subject L: *VALENCIA*

Subject C: *ES*

X509SKI

X509 SK I *kGkSCFzawGTOhg1g7/p6NHUs67g=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2021-12-13T02:00:00Z

Scheme Service Definition URI

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

48.3 - Service (withdrawn): Servicio de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados del proveedor «LLEIDANET PKI S.L.»

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

[illegible]

Subject 2.5.4.97: *B97458996*

Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

Subject CN: *(B97458996) Indenova S.L.*

Subject OU: *Dirección*

Subject O: *Indenova S.L.*

Subject SERIAL NUMBER: *44864081M*

Subject ST: *VALENCIA*

Subject L: *VALENCIA*

Subject E: *equipocrypto@indenova.com*

Subject C: *ES*

Valid from: *Fri Jul 09 11:08:44 CEST 2021*

Valid to: *Mon Jul 08 11:18:44 CEST 2024*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A0:BA:2F:CC:1C:A5:81:CD:F4:00:71:73:73:68:05:96:41:8C:55:0E:78:46:A1:
E4:19:33:91:C7:4E:D8:54:E8:6F:82:2B:31:A5:4B:04:1E:01:65:C8:2C:0C:25:E0:05:5A:E2:80:90:03:86:03:45:6B:83:EE:88:FC:E8:D5:6A:8B:CD:4C:D2:2B:97:94:2B:EC:D8:59:18:83:EF:6
A:FB:DD:22:EB:A8:36:EC:3F:EF:F5:B5:65:CC:FE:B4:8D:E5:92:5C:5D:AD:7C:B1:FB:67:56:98:C1:52:A4:07:4F:EA:AB:2E:2F:79:5A:A8:49:F2:0F:2C:5A:4A:9C:EF:15:70:0B:42:5F:CB:2D:B1:
99:B2:9E:36:E8:81:8F:A3:9C:4E:CD:07:79:D8:21:E6:21:52:A9:13:67:C6:58:F9:6D:8B:87:8A:28:B3:E3:41:7C:F2:BA:4A:2C:D1:4E:34:A5:93:05:DD:72:26:5A:E4:08:F1:04:AF:B9:82:75:5
5:9C:94:A9:EB:74:7C:B7:AE:3C:1A:85:5E:6B:1E:01:68:AE:65:5C:9D:BC:E8:29:42:E7:28:AF:D5:30:BC:43:1E:6B:C9:8C:64:3F:47:F8:5D:EE:DF:7A:2D:EE:D5:96:B8:51:78:D3:84:E3:C5:4E
:45:1A:21:99:89:3F:94:35:E0:CF:8F:02:03:01:00:01

Basic Constraints *IsCA: false*

Extended Key Usage *Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id_kp_clientAuth - id_kp_smartcardlogon*

Subject Key Identifier *56:BF:03:6B:D1:B8:A3:B7:10:98:40:37:51:7F:14:44:A4:5C:18:E9*

Authority Info Access *http://ocsp2.esigna.es
http://certs.esigna.es/ca/indenova_pki_003.crt*

Authority Key Identifier *C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46*

CRL Distribution Points *http://crl1.esigna.es/sub/indenova_pki_003.crl
http://crl.esigna.es/sub/indenova_pki_003.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.1
CPS pointer: http://cps.esigna.es/sub/cps_sub003_ca.pdf
CPS text: [Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf]
Policy OID: 0.4.0.194112.1.1*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance
id_etsi_qcs_RetentionPeriod: 15*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:FC:B0:0B:7B:B7:1E:8C:6D:6F:0A:23:24:9E:E0:BF:F3:59:85:C8:C2:AD:7E:8A:B9:8A:D2:DE:DA:60:82:99*

X509SubjectName

Subject 2.5.4.97: *B97458996*

Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

Subject CN: *(B97458996) Indenova S.L.*

Subject OU: *Dirección*

Subject O: *Indenova S.L.*

Subject SERIAL NUMBER: *44864081M*

Subject ST: *VALENCIA*

Subject L: *VALENCIA*

Subject E: *equipocrypto@indenova.com*

Subject C: *ES*

X509SKI

X509 SK I *Vr8Da9G4o7cQmEA3UX8URKRcGOk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2025-02-05T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

48.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

48.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

48.3.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service Name

Name [es] *Servicio de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados del proveedor «LLEIDANET PKI S.L.»*

Name [en] *Validation service of qualified electronic signatures and qualified electronic seals of the TSP «LLEIDANET PKI S.L.»*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *B97458996*

Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

Subject CN: *(B97458996) Indenova S.L.*

Subject OU: *Dirección*

Subject O: *Indenova S.L.*

Subject SERIAL NUMBER: *44864081M*

Subject ST: *VALENCIA*

Subject L: *VALENCIA*

Subject E: *equipocrypto@indenova.com*

Subject C: *ES*

X509SKI

X509 SK I *Vr8Da9G4o7cQmEA3UX8URKRcGOk=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2023-11-08T00:00:00Z

48.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

48.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

48.3.4 - History instance n.2 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service Name

Name [es] *Servicio de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados del proveedor «Indenova S.L.»*

Name [en] *Validation service of qualified electronic signatures and qualified electronic seals of the TSP «Indenova S.L.»*

Service digital identities

X509SubjectName

Subject 2.5.4.97: B97458996

Subject 2.5.4.13: Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003

Subject CN: (B97458996) Indenova S.L.

Subject OU: Dirección

Subject O: Indenova S.L.

Subject SERIAL NUMBER: 44864081M

Subject ST: VALENCIA

Subject L: VALENCIA

Subject E: equipocrypto@indenova.com

Subject C: ES

X509SKI

X509 SKI Vr8Da9G4o7cQmEA3UX8URKRcGOk=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-12-13T02:00:00Z

48.3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

48.3.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

48.4 - Service (granted): Qualified validation service for qualified electronic signatures and qualified electronic seals of the TSP «LLEIDANET PKI S.L. 2024»

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service type description [en] undefined.
[es] undefined.

Service Name

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals of the TSP «LLEIDANET PKI S.L. 2024»

Name [es] Servicio de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados del proveedor «LLEIDANET PKI S.L. 2024»

Service digital identities

Certificate fields details

Version: 3

Serial Number: 5276391985995457489

Subject GIVEN NAME: FRANCISCO JOSE
Subject SERIAL NUMBER: IDCES-40897755Y
Subject SURNAME: SAPENA SOLER
Subject E: sisco@lleida.net
Subject C: ES
Valid from: Mon Jul 08 12:01:17 CEST 2024
Valid to: Sat Jul 07 12:11:17 CEST 2029
Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B4:AC:6A:B7:02:EA:94:22:95:3F:07:2E:90:91:90:62:BC:CB:29:63:AC:E5:DB:F4:E5:1C:63:46:81:02:68:A3:AB:05:55:D1:10:73:45:47:6D:29:1D:C5:B2:E8:FD:2A:D3:FC:02:A7:96:01:3D:52:8B:8F:54:88:62:2E:71:47:73:A3:F7:48:0F:31:50:AF:3C:37:EE:81:85:D3:93:50:B8:27:A1:B7:CF:F4:40:FF:A1:42:FF:CA:64:A2:CF:44:2C:75:8F:2B:03:4D:87:20:B7:7E:FB:62:A7:FB:9F:F1:54:91:9A:5B:C9:CF:89:33:D8:C0:0B:83:A5:9F:4B:52:A5:9C:27:8A:D8:E6:F9:59:E9:07:76:33:EC:57:DF:75:30:C8:89:ED:9E:7C:DD:E1:15:1E:05:56:94:46:66:79:2E:38:5F:48:40:CD:88:DD:35:92:9B:16:38:0D:80:64:6B:34:C6:9A:C2:DC:87:F3:09:DD:2E:DD:8D:E3:8F:AA:0E:18:1A:80:AA:B0:31:77:64:9A:6F:56:94:70:3B:5A:88:59:2B:C6:88:4E:C1:30:02:10:93:37:FC:45:6A:B0:06:10:55:E0:2E:C0:B8:74:D7:AB:CC:7B:80:0B:CB:74:00:C4:0C:43:D4:EE:7F:E8:6B:57:49:6F:1D:26:71:39:02:03:01:00:01
Basic Constraints *IsCA: false*
Extended Key Usage *Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id_kp_clientAuth - id_kp_smartcardlogon*
Subject Key Identifier 3E:36:A6:00:2E:99:9A:5E:35:AC:00:9E:65:B1:1D:0F:50:B6:E7:12
Authority Info Access *http://ocsp2.esigna.es*
http://certs.esigna.es/ca/indenova_pki_003.crt
Authority Key Identifier C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46
CRL Distribution Points *http://crl1.esigna.es/sub/indenova_pki_003.crl*
http://crl.esigna.es/sub/indenova_pki_003.crl
Subject Alternative Name *sisco@lleida.net*
OID.2.16.724.1.3.5.6.1.2=Lleidanet PKI SLU
OID.2.16.724.1.3.5.6.1.9=sisco@lleida.net
OID.2.16.724.1.3.5.6.1.8=SOLER
OID.2.16.724.1.3.5.6.1.6=FRANCISCO JOSE
OID.2.16.724.1.3.5.6.1.1=SELLO ELECTRONICO DE NIVEL ALTO
OID.2.16.724.1.3.5.6.1.7=SAPENA
OID.2.16.724.1.3.5.6.1.3=B97458996
OID.2.16.724.1.3.5.6.1.4=40897755Y

Certificate Policies*Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.4**CPS pointer: http://cps.esigna.es/sub/cps_sub003_ca.pdf**CPS text: [Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en http://cps.esigna.es/sub/cps_sub003_ca.pdf]**Policy OID: 0.4.0.194112.1.3**Policy OID: 2.16.724.1.3.5.6.1***QCStatements - crit. = false** *id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15**id_etsi_qcs_QcSSCD***Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:** *SHA-256***Thumbprint:** *B4:9C:3C:5E:AB:F3:98:4E:F6:59:0B:07:D5:3C:DF:1A:27:25:2E:C5:F0:DE:E4:39:86:8D:28:6E:55:53:C0:C6***X509SubjectName****Subject 2.5.4.97:** *VATES-B97458996***Subject 2.5.4.13:** *Certificado de Sello Electrónico Centralizado UP (QSCD) - Emitido por inDenova SUB CA 003***Subject T:** *Ceo***Subject CN:** *(B97458996) Lleidanet PKI SLU***Subject OU:** *SELLO ELECTRÓNICO***Subject OU:** *Gerencia***Subject O:** *Lleidanet PKI SLU***Subject GIVEN NAME:** *FRANCISCO JOSE***Subject SERIAL NUMBER:** *IDCES-40897755Y***Subject SURNAME:** *SAPENA SOLER***Subject E:** *sisco@lleida.net***Subject C:** *ES***X509SKI****X509 SK I** *PjamAC6Zml41rACeZbEdD1C25xl=*

Service Status*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] undefined.
[es] undefined.

Status Starting Time*2025-02-05T00:00:00Z***Scheme Service Definition URI**

URI [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

48.4.1 - Extension (not critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

48.4.2 - Extension (not critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

49 - TSP: BTP ONETEC, S.L.**TSP Name**

Name *[en]* *BTP ONETEC, S.L.*

Name *[es]* *BTP ONETEC, S.L.*

TSP Trade Name

Name *[en]* *VATES-B33943564*

Name *[es]* *VATES-B33943564*

Name *[en]* *BTP ONETEC*

PostalAddress

Street Address *[en]* *C/ La Mecánica, 305. Polígono Industrial La Peñona*

Locality *[en]* *GIJÓN*

State Or Province *[en]* *ASTURIAS*

Postal Code *[en]* *33211*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *C/ La Mecánica, 305. Polígono Industrial La Peñona*

Locality *[es]* *GIJÓN*

State Or Province *[es]* *ASTURIAS*

Postal Code *[es]* *33211*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:info@btponetec.es*

URI *[en]* *https://www.btponetec.es*

URI *[es]* *mailto:info@btponetec.es*

URI *[es]* *https://www.btponetec.es*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B33943564*

Subject CN: *BTP QUALIFIED TSU01*

Subject OU: *BTP TSP*

Subject O: *BTP ONETEC, S.L.*

Subject L: *GIJON*

Subject C: *ES*

Valid from: *Tue Sep 21 18:37:09 CEST 2021*

Valid to: *Fri Sep 21 18:37:09 CEST 2029*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A5:3E:58:21:C8:8F:61:26:8B:44:97:E0:AD:4F:A8:18:24:B0:91:72:D0:97:3A:27:BE:67:0A:C9:52:9C:24:F8:22:27:6E:9F:9A:EC:F2:33:CD:11:62:B7:C9:5E:23:26:C6:11:C8:8D:48:59:B0:E0:E0:C8:3F:3D:A9:5F:F7:53:12:1B:4B:24:60:CC:B9:CB:A4:B7:A9:DC:74:05:C B:0A:B5:C1:CB:DC:E1:04:32:6F:C2:F5:DB:F2:18:55:5C:24:DB:41:2F:16:2B:6E:02:D4:E7:E1:61:72:D0:EB:13:24:F2:95:8E:42:ED:FB:29:9F:C7:BB:8B:68:E6:F7:2B:A5:D0:82:BB:24:7D:B1 :AD:EB:14:8E:D4:EA:BB:13:9B:80:A5:1E:86:2D:69:31:1C:DB:87:3F:CC:31:23:BF:BA:3B:4D:31:BE:28:5F:23:6F:ED:3D:00:28:62:68:56:62:A9:C6:0F:F3:5F:43:A8:FF:A5:B4:40:A6:69:D9: 7B:8A:75:03:D9:36:AC:C9:1D:07:D0:BB:91:C7:D9:C3:49:34:CA:FF:D4:86:FF:E8:48:B1:D1:85:70:BA:74:0D:53:A1:96:24:21:A4:F5:7A:4D:C1:50:0D:88:FA:0A:10:2D:B6:4C:99:1D:08:EB: C2:BB:2E:E0:D2:2E:12:F0:86:36:96:89:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/*
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *2C:64:0F:E5:8E:29:B0:8A:5A:2A:73:7D:E4:09:41:A2:C0:62:A8:AB*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@btponetec.es*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: 09:91:3A:8F:69:B5:42:55:93:4A:40:E1:27:12:AF:D1:D5:B9:9A:95:C0:EC:23:12:7F:3B:32:99:40:29:1A:0D

X509SubjectName

Subject 2.5.4.97: VATES-B33943564

Subject CN: BTP QUALIFIED TSU01

Subject OU: BTP TSP

Subject O: BTP ONETEC, S.L.

Subject L: GIJON

Subject C: ES

X509SKI

X509 SK I LGQP5Y4psIpaKnN95AlBosBiqKs=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2026-01-22T02:00:00Z

49.1.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service Name

Name [es] Sellos de tiempo cualificados emitidos por BTP QUALIFIED TSU01

Name [en] Qualified timestamps issued by BTP QUALIFIED TSU01

Service digital identities

X509SubjectName

Subject 2.5.4.97: VATES-B33943564

Subject CN: BTP QUALIFIED TSU01

Subject OU: BTP TSP

Subject O: BTP ONETEC, S.L.

Issuer CN: UANATACA CA1 2021
Issuer OU: TSP-UANATACA
Issuer O: UANATACA S.A.
Issuer L: Barcelona
Issuer C: ES
Subject 2.5.4.97: VATES-B33943564
Subject CN: BTP QUALIFIED TSU 02
Subject OU: BTP TSP
Subject O: BTP ONETEC, S.L.
Subject L: GIJON
Subject C: ES
Valid from: Wed Oct 08 12:38:24 CEST 2025
Valid to: Sat Oct 08 12:38:24 CEST 2033
Public Key: 30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:A6:7A:C1:02:5D:36:C6:66:5E:C7:A3:07:2E:59:A7:10:3F:15:32:3E:62:58:2E:70:92:EF:1D:32:56:7E:71:44:97:57:84:A1:77:78:7F:62:E4:E5:0E:45:59:CF:FC:D7:64:4D:D5:76:EE:9B:F9:C7:C1:96:96:9E:40:4A:CC:9B:47:5C:66:22:9C:39:59:1D:58:02:F4:01:EF:6E:0C:CF:39:1D:2C:A9:B9:1F:35:54:24:85:89:EA:91:B4:A7:CE:20:51:25:F9:DF:9B:CB:5F:BE:92:CC:D9:DE:59:EA:4C:4A:66:64:29:09:4F:F7:55:2F:22:59:B6:56:B1:F9:16:A6:6A:6F:58:E4:76:A8:A1:F8:9F:F2:07:46:C4:DC:E4:42:97:8E:EE:D6:E7:7A:34:12:ED:B1:B3:09:82:21:6A:43:49:48:A3:25:23:1A:2F:0E:52:02:A7:48:68:2F:15:CD:D3:B5:60:65:57:78:36:E6:DC:76:A9:66:FB:C5:DA:86:68:95:50:4D:01:D5:F9:24:E8:1D:B9:F4:D7:6C:BA:09:98:42:D4:CF:5A:9B:EF:D0:0C:FD:2A:3E:75:F4:4C:04:96:78:45:11:B1:11:A2:10:83:97:14:12:F2:99:45:A5:6D:5D:C0:94:0D:F3:89:52:47:96:AD:8A:34:CD:01:28:7E:F0:BA:49:98:E7:30:CF:2F:6A:C2:F5:43:0C:F4:F1:44:A4:7F:B1:2C:D6:A9:D9:F5:89:1C:B2:B0:CB:EA:25:59:53:9C:A1:25:C3:7A:5F:D6:9B:82:1F:A7:8D:CC:C4:FF:7D:D9:35:CD:98:A1:19:D2:86:46:5E:55:D0:B4:2C:AA:19:FD:2E:DA:84:8A:80:AC:5A:68:6A:E7:6B:FF:D8:E3:5D:7A:B3:3E:83:95:E2:26:B5:44:D9:B7:64:1A:77:19:5F:70:23:28:93:C6:F6:EE:27:C3:37:41:33:4A:44:37:64:05:84:58:B1:23:8B:5C:D3:68:4D:33:CE:6F:02:03:01:00:01
Authority Info Access
https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer
<http://ocsp1.modernpki.com/public/pki/ocsp/>
<http://ocsp2.modernpki.com/public/pki/ocsp/>
Subject Key Identifier 3C:A9:1F:E0:C2:92:8B:A7:45:19:47:82:85:D6:98:64:BC:D7:92:2C
Basic Constraints IsCA: false
Authority Key Identifier 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68
Issuer Alternative Name info@uanataca.com
Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
<http://crl1.modernpki.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.modernpki.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage
id_kp_timeStamping

Subject Alternative Name
info@btponetec.es

Key Usage:
digitalSignature

Thumbprint algorithm:
SHA-256

Thumbprint:
9C:BD:C8:70:BA:9F:46:63:50:A4:25:D4:AC:BB:6D:64:69:EF:3E:00:EE:ED:8F:8C:75:89:09:28:5A:0C:84:F2

X509SubjectName

Subject 2.5.4.97:
VATES-B33943564

Subject CN:
BTP QUALIFIED TSU 02

Subject OU:
BTP TSP

Subject O:
BTP ONETEC, S.L.

Subject L:
GIJON

Subject C:
ES

X509SKI

X509 SK I
PKkf4MKSi6dFGUeChdaYZLzXkiw=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]*
undefined.

[es]
undefined.

Status Starting Time
2026-01-22T02:00:00Z

50 - TSP: AVIVA VOICE SYSTEMS AND SERVICES, S.L.**TSP Name**

Name [es] AVIVA VOICE SYSTEMS AND SERVICES, S.L.

Name [en] AVIVA VOICE SYSTEMS AND SERVICES, S.L.

TSP Trade Name

Name [en] VATES-B84216142

Name [en] Aviva Voice Systems and Services SL

PostalAddress

Street Address [en] C/ Golfo de Salónica 27 Planta 5ª puerta B

Locality [en] MADRID

State Or Province [en] MADRID

Postal Code [en] 28033

Country Name [en] ES

PostalAddress

Street Address [es] C/ Golfo de Salónica 27 Planta 5ª puerta B

Locality [es] MADRID

State Or Province [es] MADRID

Postal Code [es] 28033

Country Name [es] ES

ElectronicAddress

URI [en] mailto:info@avivavoice.com

URI [en] http://www.avivavoice.com/

URI [es] http://www.avivavoice.com/

URI [es] mailto:info@avivavoice.com

TSP Information URI

URI [en] <http://www.avivavoice.com/>

50.1 - Service (withdrawn): Sellos de tiempo cualificados emitidos por AVIVA VOICE QUALIFIED TSU01

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por AVIVA VOICE QUALIFIED TSU01*

Name [en] *Qualified timestamps issued by AVIVA VOICE QUALIFIED TSU01*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 542405915439744316

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIHBTCCBO2gAwIBAgIIB4cDTmnbrTwwDOYJKoZIhvcNAQELBQAwYXZlbnVBAWYAKVtMRWwE
EAYDVQODDAICYXJzWxvbmExFjAUBgNVBAoMDVVBTKFUGUUNBIFMuOS4xFTATBgNVBAAsMDFRTUC1V
QUJ5BEFDD0TEaM9GGA1UEAwwRVUFOOVRBODQgODExIDlwMjEwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MTQ5OT0AeWdybWl0eXNDMwNjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZm
A1UEBmVwGTFUFEUKIEMswK9YDVOQKDCNbdm1Y29hZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZmZjZm
TDEYMBYGA1UECwwPOVZjVjEgYVZjVjEgYVZjVjEgYVZjVjEgYVZjVjEgYVZjVjEgYVZjVjEgYVZj
RUQGVFVNMDEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
ADCCAQoCggEBAAKqPbLSQWxz4qnvNaLdylqzWFLCuhMjWxooQg0e3YlOmGNRT5cIM3LF
rfqW6u+KOCuthppzgn5ZhrZ+NySx0NefKx0FzPg8dypXMST/8QlanOKQIn4N6CwhjDcZ28f+
Zx4dT7TCdztOnas8ZkE8KyybK0ksdWwuc4A9KqzbWCSmjT54N+PzNjHeTW65pKb6fWwd
QKdRcobUn9MfhzP4vu+20Ffp3WISRIEKCjMOHLM0ZuVnlgwJQA75fyobj+IaPg2NGNKYKLU
71NN3av61YmVlnMXZagCr73Kw7zbdKj6CvOz02ebjGSYHFFPCAwEAAaOCAlMwggPMH4GCCsG
AOUBwEBBhwDAZBggrBgEFBQcwAYYgaHR0cDovLz9ic3AkLnVhbmF0YWNhLnV5bS9wdWJsaWMy
cGtpL29ic3AvMDYGCCSGAUFBzABhipodHrwOibv2NzcDludWfuYXRhY2Euy29hL3B1YmVwYy9w
a2kvb2NzcC8wHQYDVR0OB8YEFkTRlRlgVvd/18evKluVhtnT+VeMAKGA1UdEwQCMAAwHwYDVR0j
BBgwFoAUGc+QWTS7arctGcUob8bz8fWpwhIAYDVR0SB8uWEERAw5mb0B1YW5hdGFYYS5jb2w
gZMGA1UdIASBzCBIDB8BgorBgEEAYLXNgtFMGAwMAYIKwYBBQUHAgEWWGh0dHBzOibv2NzcDludW
bmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxs
by8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0
dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fk
by8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0a
WZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+
MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAu
DCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1
UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEF
BQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI
96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3Bz
L2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7mua
WNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9w
dWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZm
ZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0
YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8kZS8Z2Wxsby8k
ZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6oDGNmh0dHA6L9j
cmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj0aWZpY2Fkby8k
ZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1UdHwR+MhwwKA6o
DGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQcCAjAuDCx0Zj
0aWZpY2Fkby8kZS8Z2Wxsby8kZS80aWwteGZmZWx1f3Ry7muaWNL1AibgYEAI96AQwYUGA1Ud
HwR+MhwwKA6oDGNmh0dHA6L9jcmwXLnVhbmF0YWNhLnV5bS9wdWJsaWMyV3BzL2A6BgrBgEFBQ
cCA
```

Subject 2.5.4.97: *VATES-B84216142*

Subject CN: *AVIVA VOICE QUALIFIED TSU01*

Subject OU: *AVIVA VOICE TSP*

Subject O: *Aviva Voice Systems and Services SL*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Wed Nov 03 17:23:26 CET 2021*

Valid to: *Mon Nov 05 17:23:26 CET 2029*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A0:04:96:03:D8:2D:24:16:5E:7C:FF:E2:09:EF:36:A2:DD:C8:8A:B3:58:41:48:2C:25:21:32:22:56:C6:8A:0E:83:47:B7:C8:84:26:18:D4:53:88:97:08:33:72:C5:AD:FF:EA:5B:AB:BE:28:E0:AE:B6:1A:69:CE:E8:27:E5:98:6B:67:E3:72:49:7D:0D:78:59:31:D0:5C:CF:1B:C7:7F:CA:95:CC:49:3F:FC:42:56:A1:38:A4:08:AC:9E:0D:E8:2C:21:24:3B:76:67:C7:FE:67:1E:1D:4D:8E:DC:0F:37:D5:0E:76:AC:F3:62:A5:13:CB:4A:CB:20:64:3A:48:AC:74:3C:2E:72:3E:00:F4:AB:63:CD:B2:56:09:29:A3:7D:2E:0D:F8:FC:FF:36:31:DE:ED:6E:89:A4:72:BA:7D:5C:1D:40:A7:51:08:46:D4:9F:D3:1F:22:1C:CF:E2:F8:BE:08:E1:45:A7:72:56:95:24:62:12:D4:1C:24:C4:07:7C:B9:90:66:E5:67:26:AC:09:89:00:3B:E5:FC:A0:6C:9F:88:68:F8:36:34:63:4A:60:AB:54:EF:53:4D:DD:AB:FA:D5:89:95:22:73:17:64:08:02:AF:BD:D7:C3:BC:73:6C:39:09:97:A0:AF:42:83:86:79:B2:46:E5:81:C5:14:F7:02:03:01:00:01

Authority Info Access
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *B8:AD:4D:19:60:55:57:7F:D7:C7:95:2A:5B:A5:54:7B:67:4F:E5:5E*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@avivavoice.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *95:42:8E:4B:2F:9C:AD:1F:59:44:D7:CA:D8:E7:E7:F9:75:71:84:CE:65:09:86:9D:E8:F8:DE:33:18:D4:26:AE*

X509SubjectName

Subject 2.5.4.97: *VATES-B84216142*

Subject CN: *AVIVA VOICE QUALIFIED TSU01*

Subject OU: *AVIVA VOICE TSP*

Subject O: *Aviva Voice Systems and Services SL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *uK1NGWBVV3/Xx5UqW6VUe2dP5V4=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2026-03-26T02:00:00Z*

50.1.1 - History instance n.1 - Status: granted

Service Type Identifier *<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>*

Service Name

Name *[es]* *Sellos de tiempo cualificados emitidos por AVIVA VOICE QUALIFIED TSU01*

Name *[en]* *Qualified timestamps issued by AVIVA VOICE QUALIFIED TSU01*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B84216142*

Subject CN: *AVIVA VOICE QUALIFIED TSU01*

Subject OU: *AVIVA VOICE TSP*

Subject O: *Aviva Voice Systems and Services SL*

Subject L: *MADRID*

Subject C: *ES*

Issuer O: UANATACA S.A.

Issuer L: Barcelona

Issuer C: ES

Subject 2.5.4.97: VATES-B84216142

Subject CN: AVIVA VOICE QUALIFIED TSU 02

Subject OU: AVIVA VOICE TSP

Subject O: Aviva Voice Systems and Services SL

Subject L: MADRID

Subject C: ES

Valid from: Wed Oct 15 17:43:20 CEST 2025

Valid to: Mon Oct 17 17:43:20 CEST 2033

Public Key:
30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:CB:19:F8:27:0E:64:67:33:A5:F1:2A:56:21:10:E4:9A:70:51:81:B6:88:96:66:88:02:84:C5:B7:2E:99:D4:23:F5:FF:83:DA:CA:AC:B8:18:D5:98:EE:17:57:C2:C1:F0:0A:99:ED:F8:DE:CD:DF:28:C7:AD:58:69:D8:94:69:06:55:CC:9A:69:9A:4A:81:1C:86:24:EF:40:66:36:87:00:5B:8C:C2:6D:0F:D7:7E:9A:B9:9E:29:62:40:9F:86:12:B3:5D:36:3A:7F:6A:AC:1C:56:7E:6D:48:71:B0:91:5D:48:48:7D:CF:44:18:29:6E:91:78:6E:64:73:35:F7:C4:FD:D2:32:97:D4:74:D1:E8:A0:98:35:26:74:28:88:6A:EF:46:CD:AF:DF:86:74:EB:9E:8E:CD:B8:6E:BC:11:03:97:34:2F:BF:42:68:B2:22:9D:A3:9F:AF:33:66:99:B7:48:D6:69:DA:A2:8C:20:CD:DF:7F:A5:78:8D:00:AF:61:B6:A9:8D:8D:27:51:82:A5:A7:3D:9F:DB:F1:E5:A8:CE:7A:79:92:0D:1F:66:63:54:3A:D9:15:52:27:74:63:79:23:58:A9:57:15:1E:FC:CF:83:2C:3B:0F:26:67:B2:A3:71:E5:7D:48:61:D5:30:C2:DF:2E:9E:94:F7:17:4B:05:50:08:68:6C:14:FD:59:42:68:2F:A5:4A:7E:15:04:BB:9B:B2:F2:B0:81:17:1D:8D:16:71:FA:3B:36:36:5F:7D:84:63:D6:AD:7C:F2:DA:EB:BE:95:A2:80:A0:32:1C:79:D9:4D:61:12:52:3D:5E:6B:BC:9C:52:CB:4A:49:02:8C:B1:A3:27:8F:0C:E3:29:45:0E:85:E0:6A:FE:0B:97:8D:41:30:53:DB:FF:48:78:6B:BC:53:04:C0:3B:F8:5B:B4:B5:39:43:3A:D0:EF:DE:22:E0:50:1E:58:2D:97:1A:26:DE:59:05:17:A1:19:00:F5:7F:95:00:A6:E7:F0:F9:8D:02:03:01:00:01

Authority Info Access
https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier 4B:2C:A1:17:A6:B1:5F:32:54:E3:71:F9:87:07:35:57:32:06:90:26

Basic Constraints *IsCA: false*

Authority Key Identifier 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@avivavoice.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D1:C0:1E:A7:37:7C:CA:51:90:E0:29:83:5A:0E:0C:ED:1C:0A:A8:8D:33:02:BD:3E:2A:EC:DF:7C:BD:0E:E3:68*

X509SubjectName

Subject 2.5.4.97: *VATES-B84216142*

Subject CN: *AVIVA VOICE QUALIFIED TSU 02*

Subject OU: *AVIVA VOICE TSP*

Subject O: *Aviva Voice Systems and Services SL*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *SyyhF6axXzJU43H5hwc1VzIGkCY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-03-26T02:00:00Z*

51 - TSP: ASETEC INGENIERIA DE SISTEMAS, S.L.**TSP Name**

Name [es] ASETEC INGENIERIA DE SISTEMAS, S.L.

Name [en] ASETEC INGENIERIA DE SISTEMAS, S.L.

TSP Trade Name

Name [en] VATES-B82149139

Name [en] ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK

PostalAddress

Street Address [es] Calle Jaenar nº 27

Locality [es] Madrid

State Or Province [es] Madrid

Postal Code [es] 28043

Country Name [es] ES

PostalAddress

Street Address [en] Calle Jaenar nº 27

Locality [en] Madrid

State Or Province [en] Madrid

Postal Code [en] 28043

Country Name [en] ES

ElectronicAddress

URI [en] mailto:pscc@mensatek.com

URI [en] https://www.mensatek.com

URI [es] https://www.mensatek.com

URI [es] mailto:pscc@mensatek.com

TSP Information URI

Page 1459

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B82149139*

Subject CN: *MENSATEK QUALIFIED TSU01*

Subject OU: *MENSATEK TSP*

Subject O: *ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Tue Sep 21 19:19:13 CEST 2021*

Valid to: *Fri Sep 21 19:19:13 CEST 2029*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E2:6E:5F:7E:E1:7B:DF:CC:1E:3F:36:9C:89:23:0D:31:45:DA:2F:30:04:DD:B1:0C:7D:E8:C6:D4:D5:83:44:63:91:F0:BC:CE:52:83:AC:08:A7:13:53:73:19:80:D5:53:3F:A6:63:E8:AB:9D:57:F5:56:94:D0:95:AE:46:3F:1A:CE:CD:DD:E8:1A:C1:FE:2D:00:C6:48:20:DD:CC:49:29:7F:CB:42:2D:A9:E0:3B:4A:64:48:25:6B:5B:63:79:86:A7:AB:4E:88:B9:7B:8E:07:C4:44:27:12:09:DE:17:9B:D4:83:F3:75:94:EB:B7:2D:75:44:A0:50:93:CD:7B:8B:38:30:F1:6C:E7:D7:CA:33:79:9D:CD:D8:93:8A:12:49:AD:51:37:7B:41:D7:F2:9F:7B:F3:4E:7B:D1:58:01:61:60:EC:84:00:F4:6A:91:3B:D7:22:59:32:AA:F9:68:84:0B:C4:CB:AA:88:8E:1A:3C:96:F4:CC:7B:A2:4B:90:3E:DE:61:2F:1D:CA:75:D4:59:F3:F4:20:1F:80:C1:CF:90:06:51:A0:4F:7D:E0:C4:DC:57:B2:95:E3:6C:A6:9B:8A:F4:8D:17:C4:E6:EE:7B:A1:20:D4:1E:BC:00:33:C8:5B:2C:52:28:97:66:07:6F:25:5B:3C:D7:5E:F4:62:AD:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *CC:35:F5:32:59:05:A6:71:E7:48:5A:3C:B6:AB:37:62:AF:75:18:AB*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *tsa@mensatek.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint:

EC:C7:39:8F:DF:BC:16:E3:14:45:47:E2:E8:0A:64:F8:1F:9B:F7:50:23:EA:F9:4F:F9:70:B2:B1:E0:6F:16:A8

X509SubjectName**Subject 2.5.4.97:**

VATES-B82149139

Subject CN:

MENSATEK QUALIFIED TSU01

Subject OU:

MENSATEK TSP

Subject O:

ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK

Subject L:

MADRID

Subject C:

ES

X509SKI**X509 SK I**

zDX1MlkFpnHnSFo8tqs3Yq91GKs=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]*

undefined.

[es]

undefined.

Status Starting Time

2022-05-31T00:00:00Z

52 - TSP: 3G SOLUCIONES MOVILIDAD, S.L.**TSP Name**

Name [es] 3G SOLUCIONES MOVILIDAD, S.L.

Name [en] 3G SOLUCIONES MOVILIDAD, S.L.

TSP Trade Name

Name [en] VATES-B09444431

Name [en] 3G MOBILE GROUP

Name [en] 3G SOLUCIONES MOVILIDAD SL

PostalAddress

Street Address [en] Pasaje Gutiérrez, 3, 1º

Locality [en] Valladolid

State Or Province [en] Valladolid

Postal Code [en] 47002

Country Name [en] ES

PostalAddress

Street Address [es] Pasaje Gutiérrez, 3, 1º

Locality [es] Valladolid

State Or Province [es] Valladolid

Postal Code [es] 47002

Country Name [es] ES

ElectronicAddress

URI [en] mailto:soporte@3gmg.com

URI [en] https://www.3gmg.com

TSP Information URI

URI [en] https://www.3gmg.com/

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por 3G QUALIFIED TSU01*

Name	[en]	Qualified timestamps issued by 3G QUALIFIED TSU01

Certificate fields details

Version: 3

Serial Number: 9155928350612378749

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA1 2021

Issuer OU: *TSP-UANATACA*

Issuer O: UANATACA S.A.

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B09444431*

Subject CN: *3G QUALIFIED TSU01*

Subject OU: *3G TSP*

Subject O: *3G SOLUCIONES MOVILIDAD SL*

Subject L: *VALLADOLID*

Subject C: *ES*

Valid from: *Tue Sep 21 18:53:11 CEST 2021*

Valid to: *Fri Sep 21 18:53:11 CEST 2029*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:51:03:7A:CF:50:8C:B5:F3:5D:47:6C:9F:67:29:9F:C1:53:50:DC:68:A2:1A:70:18:9B:49:31:37:F5:DD:B7:A4:98:E3:A6:64:06:CD:C1:32:F0:C0:A4:74:F3:7D:B8:B5:5E:19:D8:98:C6:F4:11:A4:B6:8B:60:F6:28:1D:C6:DA:80:36:DD:09:A3:84:FC:D0:B9:51:81:9E:89:1D:8E:F9:AB:C0:01:15:86:DA:91:48:DF:73:F0:F9:EE:00:FB:A8:D9:AE:9C:4A:00:34:C9:18:1A:95:3F:37:40:5E:08:B3:E7:67:CC:20:9F:45:F6:05:F0:66:B3:BF:03:64:9B:65:07:92:4F:6F:13:94:08:76:60:07:4C:04:A3:22:AB:CF:07:5E:6C:D3:8C:EC:87:10:AE:1B:A8:08:08:D8:77:60:02:31:15:80:C2:37:5A:5A:13:88:9F:44:80:59:AA:9C:5F:73:ED:38:A2:EF:DA:2D:98:EF:ED:37:2A:36:87:07:71:D6:AC:15:2D:0B:C3:8C:37:64:E8:1E:FA:20:5B:E3:B3:71:8E:EC:66:22:70:A1:51:19:81:E0:29:59:9A:4A:13:B2:FC:F1:67:88:B3:B0:94:36:E9:9F:B2:6B:F9:D1:84:F9:40:E8:68:96:7A:0B:18:8F:86:DC:F9:7D:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *85:B5:92:7B:68:4C:CB:E1:C2:11:1D:96:40:C3:D1:B6:2F:EC:D5:43*

Basic Constraints *isCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *soporte@3gmg.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *07:0E:12:83:52:CC:3F:65:BB:BA:3C:4D:BF:B4:B0:CE:FC:F9:75:1C:3B:FE:EF:15:11:4A:A5:10:13:D3:1D:FA*

X509SubjectName

Subject 2.5.4.97: *VATES-B09444431*

Subject CN: *3G QUALIFIED TSU01*

Subject OU: *3G TSP*

Subject O: *3G SOLUCIONES MOVILIDAD SL*

Subject L: *VALLADOLID*

Subject C: *ES*

X509SKI

X509 SK I *hbWSe2hMy+HCER2WQMPRTi/s1UM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2026-01-22T02:00:00Z

52.1.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name [es] *Sellos de tiempo cualificados emitidos por 3G QUALIFIED TSU01*

Name [en] *Qualified timestamps issued by 3G QUALIFIED TSU01*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B09444431*

Subject CN: *3G QUALIFIED TSU01*

Subject OU: *3G TSP*

Subject O: *3G SOLUCIONES MOVILIDAD SL*

Subject L: *VALLADOLID*

Subject C: *ES*

Issuer O: *UANATACA S.A.*
Issuer L: *Barcelona*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-B09444431*
Subject CN: *3G QUALIFIED TSU01*
Subject OU: *3G TSP*
Subject O: *3G SOLUCIONES MOVILIDAD SL*
Subject L: *VALLADOLID*
Subject C: *ES*
Valid from: *Wed Jul 30 16:49:47 CEST 2025*
Valid to: *Sat Jul 30 16:49:47 CEST 2033*
Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BF:FD:68:11:C2:63:A0:64:88:76:7B:E2:AB:F1:AA:A4:CB:BF:CC:4E:71:63:1B:1B:0F:97:B2:03:CC:4F:58:47:C6:2D:8A:E5:9B:11:EC:0C:88:1E:7E:5A:F3:05:CF:2C:56:5D:8C:CC:9D:DE:F2:92:E1:38:4D:01:4F:87:07:CE:2A:FF:FE:60:12:95:C0:FE:F1:98:60:AA:41:2D:E2:88:20:26:61:10:81:18:E6:75:D9:28:47:38:9B:5F:6A:3F:99:55:76:39:23:DE:3C:E1:5C:75:39:FF:B8:79:58:02:39:B5:61:D8:2B:70:87:F9:4E:68:FC:E1:03:56:47:60:DA:22:FA:CC:E1:B3:14:54:2E:FA:C4:B3:ED:E3:E3:FD:ED:E0:51:7B:C0:8C:76:15:54:5D:D9:56:FB:61:4F:C8:2D:23:24:C0:7B:7B:7E:7B:E0:BD:ED:E6:B4:BE:6B:D4:09:B5:8D:E7:92:E3:EE:6D:22:8A:7B:0A:72:20:08:62:51:00:78:1F:14:2B:7F:87:F0:EF:7F:56:96:F9:34:1D:2D:42:09:A6:9A:54:68:C5:F4:69:AE:FF:A6:AC:1F:82:80:45:2B:B7:EC:F1:F2:18:6C:27:ED:F8:38:A3:A9:33:20:88:7E:52:B5:6E:3C:43:8C:E5:FB:E7:99:3E:21:02:03:01:00:01*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
Authority Info Access *https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/
Subject Key Identifier *33:8C:BC:A2:D1:D7:B7:C3:58:02:3A:11:A5:0B:3E:D6:7E:59:60:DA*
Basic Constraints *IsCA: false*
Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*
Issuer Alternative Name *info@uanataca.com*
Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2
CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *soporte@3gmg.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9B:0B:DC:E2:8D:F3:AB:67:2C:85:68:23:5C:28:F3:86:B0:7F:F8:41:1F:8F:BC:24:52
:15:7B:46:96:1C:C4:7B*

X509SubjectName

Subject 2.5.4.97: *VATES-B09444431*

Subject CN: *3G QUALIFIED TSU01*

Subject OU: *3G TSP*

Subject O: *3G SOLUCIONES MOVILIDAD SL*

Subject L: *VALLADOLID*

Subject C: *ES*

X509SKI

X509 SK I *M4y8otHXt8NYAjoRpQs+1n5ZYNo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-01-22T02:00:00Z*

53 - TSP: WISE SECURITY GLOBAL S.L.**TSP Name**

Name [en] *WISE SECURITY GLOBAL S.L.*

Name [es] *WISE SECURITY GLOBAL S.L.*

TSP Trade Name

Name [en] *WISE SECURITY GLOBAL*

Name [en] *VATES-B95732087*

Name [en] *"WISE SECURITY GLOBAL, S.L."*

PostalAddress

Street Address [en] *Alameda de Recalde, 34, 2º izq*

Locality [en] *Bilbao*

State Or Province [en] *Vizcaya*

Postal Code [en] *48009*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Alameda de Recalde, 34, 2º izq*

Locality [es] *Bilbao*

State Or Province [es] *Vizcaya*

Postal Code [es] *48009*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:administracion@wsg127.com*

URI [en] *http://wsg127.com*

TSP Information URI

URI [en] *https://erds-mee.com/*

Issuer ST: MADRID
Issuer L: MADRID
Issuer C: ES
Subject C: ES
Subject O: WISE SECURITY GLOBAL S.L.
Subject OU: TRUST
Subject 2.5.4.97: VATES-B95732087
Subject CN: WISE - FIRMA Y CUSTODIA DE EVIDENCIAS DE TERCEROS
Valid from: Wed Mar 25 14:08:47 CET 2020
Valid to: Sun Mar 24 14:08:47 CET 2024
Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:DD:79:DB:43:13:79:A6:75:88:39:6F:08:FD:13:58:32:EB:97:67:FA:03:57:80:71:60:21:A4:32:46:AF:84:93:F3:E5:19:81:80:E7:53:AB:61:00:38:39:E0:F9:78:E9:79:87:2B:59:4F:2E:26:B1:BF:E6:F5:BE:A1:4F:FC:6D:4A:49:1A:F8:85:37:0F:57:C2:6F:FC:18:49:01:D2:0A:A0:24:96:9F:0F:71:77:88:44:9D:12:B5:4A:1A:94:08:20:C5:C5:08:FA:7D:20:3E:84:4E:F1:08:47:D1:5A:F3:C0:23:08:55:B5:20:4B:7B:B2:8D:62:FF:C6:F4:72:CF:92:FC:E7:58:37:D9:17:E9:B0:0A:0E:E7:00:29:20:9C:48:A4:E6:AD:82:DF:06:5F:D3:CA:D9:3E:16:A0:97:EF:1C:48:73:BD:2B:0C:7E:0B:A4:D6:66:C7:CE:F9:99:BC:E2:58:F9:45:A7:CC:30:DE:46:3F:F8:92:ED:F7:EF:26:25:CB:63:0F:1A:65:38:86:86:14:8C:26:2F:DF:BD:1D:6:75:56:07:CB:1C:2B:58:68:79:A4:86:A8:39:18:B1:2D:F6:CA:33:94:26:6C:D7:4D:0D:43:8C:42:B5:59:C8:9B:C1:C7:F2:55:0A:76:2C:FB:A7:20:9A:9F:44:FB:02:03:01:00:01
Basic Constraints *IsCA: false*
Extended Key Usage *id_kp_clientAuth*
Subject Key Identifier 51:31:82:76:E1:CE:ED:86:AC:AF:F3:5B:F7:71:8A:F4:C4:DD:A0:C6
Authority Info Access http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt
<http://ocsp.camerfirma.com>
Authority Key Identifier C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42
CRL Distribution Points http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl
http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl
Subject Alternative Name *info@wsg127.com*
OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO
Issuer Alternative Name *ca@camerfirma.com*
Certificate Policies *Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2*
CPS pointer: https://policy.camerfirma.com
CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *92:77:34:57:D7:E5:13:93:BF:A4:06:B1:81:AF:A1:39:18:62:25:C2:AF:CF:78:23:F8:7B:D3:C9:46:44:10:76*

X509SubjectName

Subject C: *ES*

Subject O: *WISE SECURITY GLOBAL S.L.*

Subject OU: *TRUST*

Subject 2.5.4.97: *VATES-B95732087*

Subject CN: *WISE - FIRMA Y CUSTODIA DE EVIDENCIAS DE TERCEROS*

X509SKI

X509 SK I *UTGCduHO7Yasr/Nb93GK9MTdoMY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*
 [es] *undefined.*

Status Starting Time

2024-10-16T00:00:00Z

53.1.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name [en] *Qualified electronic certified delivery service issued for WISE (ERDS MEE)*

Name [es] *Servicio cualificado de entrega electrónica certificada emitido para WISE (ERDS MEE)*

Service digital identities**X509SubjectName**

Subject C: *ES*

Subject O: *WISE SECURITY GLOBAL S.L.*

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</i>
Service type description	[en]	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	[es]	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>

Service digital identities

Certificate fields details

Version:	3
Serial Number:	1781426108004462799286
X509 Certificate	-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer O: *AC CAMERFIRMA S.A.*

Issuer 2.5.4.97: *VATES-A82743287*

Issuer SERIAL NUMBER: *A82743287*

Issuer OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer OU: *see current address at <https://www.camerfirma.com/address>*

Issuer ST: *MADRID*

Issuer L: *MADRID*

Issuer C: *ES*

Subject C: *ES*

Subject O: *WISE SECURITY GLOBAL, S.L.*

Subject OU: *ADMINISTRACION*

Subject 2.5.4.97: *VATES-B95732087*

Subject CN: *CERTIFICADO DE SELLO ELECTRÓNICO*

Valid from: *Fri Mar 22 14:38:01 CET 2024*

Valid to: *Tue Mar 21 14:38:01 CET 2028*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CC:1A:2C:8B:1C:FC:DD:7B:24:40:56:AC:FF:E5:A6:F1:43:4A:D3:F1:8C:E8:62:F0:83:3E:7E:07:3A:A4:83:74:4F:CA:69:F7:F5:25:68:C0:C8:CA:EE:44:EF:0B:8D:79:CE:E9:01:D2:93:0A:16:89:D2:A3:34:E7:6D:2F:22:F1:0D:B7:4A:BE:FB:BF:D4:5E:58:80:EE:23:23:ED:0B:0D:ED:1D:9F:40:45:79:85:EA:51:68:1A:19:9C:4D:E2:B5:88:EF:41:29:E2:30:75:49:6F:0F:5C:B7:53:AC:37:53:24:0B:E0:DB:28:44:54:D0:DC:03:E8:5B:38:10:A2:FF:7A:C1:26:79:DB:5C:74:BA:6A:5E:0F:93:D9:8E:82:81:7F:D5:E7:27:37:06:AA:13:EF:81:4D:CD:1C:82:2F:44:78:7F:9B:03:63:1A:2B:DC:63:63:1F:65:1A:76:C5:9D:10:4E:BE:0B:8F:53:45:EB:42:1C:4E:47:3B:F2:18:AF:F4:44:5D:14:81:5E:13:75:0E:C9:CA:87:0F:7E:16:0D:EB:87:62:BA:9C:5E:80:7C:98:04:3D:E3:5E:A9:BA:C6:90:4C:F0:A9:61:84:6D:8C:CA:61:E5:57:A1:36:A8:6E:3D:33:35:C9:51:ED:57:EB:27:8D:EC:C5:95:93:72:4B:02:03:01:00:01*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_clientAuth*

Subject Key Identifier *3C:84:EE:84:93:F2:AB:04:5F:EA:94:EF:C4:9B:ED:AA:59:5B:57:9E*

Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt
<http://ocsp.camerfirma.com>*

Authority Key Identifier *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl
http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl*

Subject Alternative Name *administracion@wsg127.com*
OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO

Issuer Alternative Name *ca@camerfirma.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2*
CPS pointer: https://policy.camerfirma.com
CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]
Policy OID: 0.4.0.194112.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *74:B0:F3:4E:D0:33:B9:2C:1B:19:60:EB:16:DA:4B:8C:22:E6:C8:28:89:B9:1D:BD:5E:FD:83:32:D1:58:36:3E*

X509SubjectName

Subject C: *ES*

Subject O: *WISE SECURITY GLOBAL, S.L.*

Subject OU: *ADMINISTRACION*

Subject 2.5.4.97: *VATES-B95732087*

Subject CN: *CERTIFICADO DE SELLO ELECTRÓNICO*

X509SKI

X509 SK I *PITuhJPyqwRf6pTvxJvtqllbV54=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2024-10-16T00:00:00Z*

54 - TSP: COGNICASE MANAGEMENT CONSULTING, S.L.**TSP Name**

Name *[en]* *COGNICASE MANAGEMENT CONSULTING, S.L.*

Name *[es]* *COGNICASE MANAGEMENT CONSULTING, S.L.*

TSP Trade Name

Name *[en]* *VATES-B80440795*

Name *[en]* *CMC*

Name *[es]* *CMC*

Name *[en]* *COGNICASE MANAGEMENT CONSULTING SL*

Name *[es]* *COGNICASE MANAGEMENT CONSULTING SL*

PostalAddress

Street Address *[en]* *Avenida de Manoteras, 10*

Locality *[en]* *MADRID*

State Or Province *[en]* *MADRID*

Postal Code *[en]* *28050*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Avenida de Manoteras, 10*

Locality *[es]* *MADRID*

State Or Province *[es]* *MADRID*

Postal Code *[es]* *28050*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *http://www.grupocmc.es*

URI *[en]* *mailto:psc.es@cgi.com*

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B80440795*

Subject CN: *CMC Prestador Servicios Electrónicos Confianza*

Subject SERIAL NUMBER: *B80440795*

Subject O: *COGNICASE MANAGEMENT CONSULTING SL*

Subject C: *ES*

Valid from: *Mon Jun 28 15:53:00 CEST 2021*

Valid to: *Wed Jun 28 15:53:00 CEST 2023*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:02:01:01:00:CF:CD:46:69:4C:8E:10:69:4B:AA:D1:C8:64:AA:79:FD:85:A2:D0:DD:BB:F0:D8:74:AE:DC:76:7E:A3:00:A1:9A:9A:1A:22:02:CC:D3:4B:06:BF:93:85:B5:D4:06:25:9D:B6:BF:BB:F3:74:9F:D3:E4:99:30:FF:B4:53:D1:76:7E:E3:80:30:CA:1F:76:9F:D7:6C:EF:31:CC:7F:47:74:18:E7:8D:34:A1:EF:22:C8:73:88:11:7F:29:22:17:50:9F:0D:F3:78:57:B2:0D:38:E0:D3:F4:07:97:76:15:80:B1:99:28:5C:25:5B:A5:AD:6B:C2:87:11:6C:8E:48:63:85:09:4E:84:B1:44:99:5B:74:B3:A2:A8:68:1D:B7:C8:25:4A:A8:8A:42:F1:2F:C3:9B:E0:27:38:49:B9:A1:0D:48:40:79:84:FB:5E:C8:82:21:35:8A:87:AD:1E:1C:72:34:40:05:4B:3E:75:65:83:86:9D:79:1D:DD:61:8B:80:70:8B:9C:E8:8F:38:6C:3B:0F:AB:F2:48:42:9E:49:BB:52:3A:67:C0:9E:72:27:1C:4D:46:AF:82:1E:5E:34:3A:6D:97:15:81:E6:3E:26:3E:C1:F4:1C:D7:1D:AC:88:80:48:68:47:92:E6:1B:74:27:1F:85:CB:ED:48:70:38:22:13:02:03:01:00:01*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt*
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *28:15:B4:76:8C:73:25:4D:C2:A4:9A:0B:30:3C:03:1B:2D:F1:65:7E*

Basic Constraints *IsCA: false*

Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.1.9.5*
CPS text: [Certificado cualificado de Sello Electrónico en HSM centralizado.]
CPS pointer: <https://www.uanataca.com/public/cps/>
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points *<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>*
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *info@grupocmc.es*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6D:62:6F:7C:1C:5E:9D:8F:66:E8:54:48:92:7B:A6:CA:18:97:7E:8C:6E:7F:B1:25:D
E:BF:63:2E:18:D4:12:B6*

X509SubjectName

Subject 2.5.4.97: *VATES-B80440795*

Subject CN: *CMC Prestador Servicios Electrónicos Confianza*

Subject SERIAL NUMBER: *B80440795*

Subject O: *COGNICASE MANAGEMENT CONSULTING SL*

Subject C: *ES*

X509SKI

X509 SK I *KBW0doxzJU3CpJoLMDwDGy3xZX4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time *2024-03-26T01:00:00Z*

54.1.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name [en] *Qualified electronic registered delivery service "CMC Prestador Servicios Electrónicos Confianza"*

Name [es] *Servicio cualificado de entrega electrónica certificada "CMC Prestador Servicios Electrónicos Confianza"*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATES-B80440795*

Subject CN: *CMC Prestador Servicios Electrónicos Confianza*

Subject SERIAL NUMBER: *B80440795*

Subject O: *COGNICASE MANAGEMENT CONSULTING SL*

Subject C: *ES*

X509SKI

X509 SK I *KBW0doxzJU3CpJoLMDwDGy3xZX4=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Status Starting Time *2022-09-13T00:00:00Z*

55 - TSP: SERVICIOS DE MAILCERTIFICADO SL

TSP Name

Name [en] *SERVICIOS DE MAILCERTIFICADO SL*

Name [es] *SERVICIOS DE MAILCERTIFICADO SL*

TSP Trade Name

Name [en] *CODICERT*

Name [es] *CODICERT*

Name [en] *VATES-B85804532*

PostalAddress

Street Address [en] *Embajadores 181B Local 9*

Locality [en] *Madrid*

State Or Province [en] *MADRID*

Postal Code [en] *28045*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Embajadores 181B Local 9*

Locality [es] *Madrid*

State Or Province [es] *MADRID*

Postal Code [es] *28045*

Country Name [es] *ES*

ElectronicAddress

URI [en] *http://codicert.io*

URI [es] *http://codicert.io*

URI [en] *mailto:administracion@codicert.io*

URI [es] *mailto:administracion@codicert.io*

Issuer OU: *ANF Autoridad Intermedia de Identidad*
Issuer O: *ANF Autoridad de Certificacion*
Issuer L: *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*
Issuer ST: *Barcelona*
Issuer C: *ES*
Subject 2.5.4.97: *VATES-B85804532*
Subject CN: *CODICERT-SEC*
Subject OU: *Certificado Cualificado de Sello Electronico*
Subject O: *SERVICIOS DE MAILCERTIFICADO SL*
Subject L: *MADRID*
Subject ST: *MADRID*
Subject C: *ES*
Subject SERIAL NUMBER: *B85804532*
Valid from: *Fri Apr 29 14:00:10 CEST 2022*
Valid to: *Wed Apr 29 14:00:10 CEST 2026*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D2:5B:1B:F1:0E:6E:E1:34:DA:FC:8F:62:93:19:0E:73:F5:89:5A:F2:6E:0B:70:E5:96:4D:38:2C:6B:AE:28:AD:0F:03:49:22:3E:A2:98:44:A3:FD:35:5A:8E:35:E9:E3:6E:8D:7E:A5:BE:86:EC:FB:28:65:A8:C8:3B:46:EE:F9:CD:12:9C:4E:A6:E6:55:CB:41:82:EF:22:16:AD:4C:86:B6:D8:A0:40:AD:6A:4C:A7:1A:BC:D0:93:38:14:52:97:D9:3C:D8:81:75:C6:E6:ED:BD:18:43:35:DD:6F:D5:36:A3:9A:49:A6:3D:99:E6:53:B8:F4:EF:D6:72:0B:0B:B3:88:93:BF:E7:A3:8A:7C:71:EC:D2:46:00:CF:3D:0C:4B:A2:37:9F:71:3E:98:38:E0:8E:67:37:73:25:24:42:3C:49:E6:22:E2:6F:68:0D:80:70:43:A7:F0:58:99:29:16:80:24:5A:40:05:89:94:58:B6:15:43:18:85:70:AB:43:80:94:0F:70:8D:78:72:E5:15:65:4C:85:D5:DC:63:25:84:F6:16:38:78:40:F2:D9:9A:23:A7:81:B9:88:CD:36:01:0B:59:3B:6D:F6:1E:A2:20:C0:73:D0:EA:54:45:0A:93:46:47:46:C3:40:C7:17:FE:41:AA:BB:CA:71:27:E1:02:03:01:00:01*
Authority Key Identifier *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*
Subject Key Identifier *EF:23:D4:C3:48:B4:60:2D:70:42:E0:4E:1E:25:8E:D7:7C:76:8F:8B*
Subject Alternative Name *no-reply@codicert.net*
Extended Key Usage *id_kp_clientAuth*
CRL Distribution Points *http://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl*
Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.1*
CPS pointer: <https://www.anf.es/documentos>
Policy OID: 0.4.0.194112.1.1
Authority Info Access *<http://ocsp.anf.es/spain/AV>*
http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer

Basic Constraints	<i>IsCA: false</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i>
Key Usage:	<i>digitalSignature - nonRepudiation - keyEncipherment</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>26:60:06:51:7C:8D:5A:21:76:34:2A:C3:6E:60:8A:8B:9E:0B:D0:05:80:AA:20:90:96:D5:19:E8:DB:E4:82:63</i>

X509SubjectName

Subject 2.5.4.97:	<i>VATES-B85804532</i>
Subject CN:	<i>CODICERT-SEC</i>
Subject OU:	<i>Certificado Cualificado de Sello Electronico</i>
Subject O:	<i>SERVICIOS DE MAILCERTIFICADO SL</i>
Subject L:	<i>MADRID</i>
Subject ST:	<i>MADRID</i>
Subject C:	<i>ES</i>
Subject SERIAL NUMBER:	<i>B85804532</i>

X509SKI

X509 SK I	<i>7yPUw0i0YC1wQuBOHiWO13x2j4s=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2024-05-13T00:00:00Z</i>

55.1.1 - History instance n.1 - Status: granted

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</i>

Service Name

Name	<i>[en]</i>	<i>Qualified electronic certified delivery service issued for SERVICIOS DE MAILCERTIFICADO SL</i>
Name	<i>[es]</i>	<i>Servicio cualificado de entrega electrónica certificada emitido para SERVICIOS DE MAILCERTIFICADO SL</i>

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B85804532*

Subject CN: *CODICERT-SEC*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *SERVICIOS DE MAILCERTIFICADO SL*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

Subject SERIAL NUMBER: *B85804532*

X509SKI

X509 SK I *7yPUw0i0YC1wQuBOHiWO13x2j4s=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2022-10-10T00:00:00Z*

55.2 - Service (granted): Servicio cualificado de entrega electrónica certificada emitido para CODICERT

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en]* *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name *[es]* *Servicio cualificado de entrega electrónica certificada emitido para CODICERT*

Name *[en]* *Qualified electronic certified delivery service issued for CODICERT*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *1011050006865618235616041291*

Subject Alternative Name *no-reply@codicert.net*
OID.1.3.6.1.4.1.18332.10.4=B85804532

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_AC_Qualified_Certificates_for_eSeal.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.18332.25.1.1.1*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.1

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AC:4B:2C:5B:C6:18:62:2D:5B:C4:B8:10:AF:4F:40:46:1D:6E:88:4C:55:7B:F3:92:C3:17:2B:F7:3B:9F:87:E3*

X509SubjectName

Subject L: *MADRID*

Subject ST: *MADRID*

Subject 2.5.4.97: *VATES-B85804532*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *SERVICIOS DE MAILCERTIFICADO SL*

Subject CN: *CODICERT*

Subject SERIAL NUMBER: *B85804532*

Subject C: *ES*

X509SKI

X509 SK I *mOwz0SFU06WmytVfq0P8vuA4EzY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	[en]	undefined.
	[es]	undefined.

Status Starting Time	2024-05-13T00:00:00Z

56 - TSP: FACTORYNET AUGUSTA, S.L.**TSP Name**

Name [en] *FACTORYNET AUGUSTA, S.L.*

Name [es] *FACTORYNET AUGUSTA, S.L.*

TSP Trade Name

Name [en] *FACTORYMAIL*

Name [en] *VATES- B50980804*

Name [en] *FACTORYNET AUGUSTA SL*

PostalAddress

Street Address [en] *C/ VELAZQUEZ, 10, 1º A*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28001*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/ VELAZQUEZ, 10, 1º A*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Postal Code [es] *28001*

Country Name [es] *ES*

ElectronicAddress

URI [en] *<https://www.factorymail.es>*

URI [en] *<mailto:admon@factorymail.es>*

TSP Information URI

URI [en] *<https://www.factorymail.es/politicas-factorymail>*

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description	<i>[en]</i>	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	<i>[es]</i>	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>

Service Name

Name [es] Servicio cualificado de entrega electrónica certificada emitido para
FACTORYNET AUGUSTA S.L.

Name	[en]	Qualified electronic certified delivery service issued for FACTORYNET AUGUSTA S.L.

Service digital identities

Certificate fields details

Version: 3

Serial Number: 8760835572502450359

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA1 2016

Issuer OU: *TSP-UANATACA*

Issuer O: UANATACA S.A.

Issuer L: *Barcelona (see current address at www.uanataca.com/address)*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B50980804*

Subject CN: *Firma de documentos*

Subject SERIAL NUMBER: *B50980804*

Subject O: *FACTORYNET AUGUSTA SL*

Subject C: *ES*

Valid from: *Thu Dec 16 09:47:00 CET 2021*

Valid to: *Sat Dec 16 09:47:00 CET 2023*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:7C:CD:BC:F4:CE:18:D5:23:8F:E2:42:F3:6A:28:68:C3:53:7E:45:8D:CE:94
:31:98:8A:4B:AC:89:8E:1C:58:AA:DC:1D:0F:E2:E7:E4:42:2C:F0:95:26:7A:34:32:1E:F7:9F:CD:BC:6D:29:BF:3C:A5:49:0E:E8:86:76:C9:FC:EF:E1:95:7C:24:38:8A:EF:E8:5D:78:F0:67:83:1
4:8D:84:00:D4:99:C8:B2:AC:41:A7:F2:70:C7:FB:67:AF:DE:DF:EF:67:DB:AA:1C:5D:8F:88:8E:23:91:67:BB:35:46:86:A5:6A:E7:A0:89:C3:FD:1F:8F:C3:AC:8C:31:90:21:71:C4:1A:3C:97:44
:F0:D6:DD:47:AC:92:C4:6F:D6:DC:15:03:5A:1C:D5:9E:E2:56:D6:F0:97:13:E3:91:0F:80:EE:09:11:F3:11:83:A9:EA:AF:15:27:72:76:65:F7:56:4F:B1:40:43:99:C1:DF:6A:F1:F9:67:95:5
0:8F:B6:81:18:A7:7C:C6:29:32:F1:5B:C8:1D:29:FC:F9:02:91:81:5E:09:5F:F3:E8:48:F3:B2:C0:47:DD:01:A6:92:30:BD:DD:99:3D:46:23:62:FA:92:83:BF:36:D1:56:79:41:DB:7B:DB:11:ED
:D4:06:0A:AA:67:F6:FC:F4:C8:46:03:02:03:01:00:01

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *AE:47:E1:2C:1B:F9:8B:F5:41:4B:8F:4C:EA:65:68:5F:46:1D:9F:A7*

Basic Constraints *IsCA: false*

Authority Key Identifier *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl*
http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *admon@factorymail.es*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *14:28:B7:9E:5B:9B:E1:4A:C6:76:1B:36:C3:F5:FF:16:DE:E6:4D:20:BB:83:48:7C:E3
:19:C3:B4:47:A7:15:E4*

X509SubjectName

Subject 2.5.4.97: VATES-B50980804

Subject CN: Firma de documentos

Subject SERIAL NUMBER: B50980804

Subject O: FACTORYNET AUGUSTA SL

Subject C: ES

X509SKI

X509 SK I rkfhLBv5i/VBS49M6mVoX0Ydn6c=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2024-09-30T00:00:00Z

56.1.1 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service Name

Name [es] Servicio cualificado de entrega electrónica certificada emitido para FACTORYNET AUGUSTA S.L.

Name [en] Qualified electronic certified delivery service issued for FACTORYNET AUGUSTA S.L.

Service digital identities

X509SubjectName

Subject 2.5.4.97: VATES-B50980804

Subject CN: Firma de documentos

Subject SERIAL NUMBER: B50980804

Subject O: FACTORYNET AUGUSTA SL

Subject C: ES

X509SKI

Issuer O: UANATACA S.A.
Issuer L: Barcelona (see current address at www.uanataca.com/address)
Issuer C: ES
Subject 2.5.4.97: VATES-B50980804
Subject CN: FactoryMail-firma electronica de evidencias
Subject SERIAL NUMBER: B50980804
Subject O: FACTORYNET AUGUSTA SL
Subject C: ES
Valid from: Fri Dec 15 18:06:00 CET 2023
Valid to: Sun Dec 14 18:06:00 CET 2025
Public Key: 30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:FA:F6:4A:A2:5F:57:38:9E:37:00:E9:F6:88:1D:12:51:1E:DD:69:F2:C5:82:C0:45:D1:F6:CA:1E:63:09:96:80:DE:C7:81:1D:74:56:AD:85:FF:EC:78:24:FF:4E:94:6C:DA:B9:DE:A7:42:9D:13:48:80:F9:A0:BD:8C:59:6F:B1:5E:A5:F2:2D:0C:5B:D0:E4:4D:A8:F7:61:14:AD:85:7D:65:92:12:28:86:1C:CC:EA:38:D7:35:57:C8:E3:66:76:45:82:93:65:3A:7C:CS:15:27:33:F0:E0:A1:7D:18:A0:F7:5C:3C:24:A7:E0:C8:A9:5F:A5:1C:7A:3C:C5:6E:89:BC:A2:3B:AE:30:08:91:60:16:79:40:04:19:3D:03:87:5C:CE:98:FD:14:5E:DB:C8:91:88:73:93:8E:0F:E7:38:AE:3E:F7:02:D9:53:67:0E:21:FB:43:9C:44:A4:A1:E1:3F:F1:F3:5C:F3:6A:3D:26:A7:B8:7C:F4:79:DA:18:76:CE:FC:81:93:67:02:C9:F1:7D:AB:56:A9:55:16:90:57:73:63:F2:2C:E4:6D:49:8E:49:92:04:38:5B:A2:11:E5:94:6C:15:76:AC:84:6D:7F:98:A9:64:E4:4B:FF:A0:53:A5:ED:8E:0F:BF:B6:CC:0C:46:EB:34:CA:0D:6D:CF:02:03:01:00:01
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD
Authority Info Access http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>
Subject Key Identifier CD:26:83:DE:C0:F2:1C:66:06:F7:B8:8D:DE:DE:3B:C3:74:04:22:06
Basic Constraints *IsCA: false*
Authority Key Identifier 2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5
Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Qualified certificate for e-seal in Remote QSCD]
CRL Distribution Points <http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>
Extended Key Usage *id_kp_clientAuth*
Subject Alternative Name *admon@factorymail.es*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A0:43:67:73:2A:AF:03:82:AF:6D:02:B4:80:6C:F3:D4:1D:E6:5F:61:A3:0A:B9:E6:51:A3:8A:F8:D7:B5:EE:AE*

X509SubjectName

Subject 2.5.4.97: *VATES-B50980804*

Subject CN: *FactoryMail-firma electronica de evidencias*

Subject SERIAL NUMBER: *B50980804*

Subject O: *FACTORYNET AUGUSTA SL*

Subject C: *ES*

X509SKI

X509 SK I *zSaD3sDyHGYG97iN3t47w3QEIgY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2026-02-19T03:00:00Z*

56.2.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service Name

Name *[en]* *Qualified electronic registered delivery service for FACTORYNET AUGUSTA S.L. (2024)*

Name *[es]* *Servicio cualificado de entrega electrónica certificada para FACTORYNET AUGUSTA S.L. (2024)*

Service digital identities**X509SubjectName**

Subject 2.5.4.97: *VATES-B50980804*

Subject CN: *FactoryMail-firma electronica de evidencias*

Subject SERIAL NUMBER: *B50980804*

56.3 - Service (granted): Qualified electronic registered delivery service for FACTORYNET AUGUSTA S.L. (2026)

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</i>
Service type description	<i>[en]</i>	<i>An electronic delivery service providing qualified electronic deliveries.</i>
	<i>[es]</i>	<i>Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.</i>
Service Name		
Name	<i>[en]</i>	<i>Qualified electronic registered delivery service for FACTORYNET AUGUSTA S.L. (2026)</i>
	<i>[es]</i>	<i>Servicio cualificado de entrega electrónica certificada para FACTORYNET AUGUSTA S.L. (2026)</i>

Certificate fields details

```
Version: 3
Serial Number: 1247443700873592154
X509 Certificate -----BEGIN CERTIFICATE-----
```

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: *UANATACA CA1 2021*

Issuer OU: *TSP-UANATACA*

Issuer O: *UANATACA S.A.*

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B50980804*

Subject CN: *FactoryMail-firma electronica de evidencias*

Subject SERIAL NUMBER: *B50980804*

Subject O: *FACTORYNET AUGUSTA SL*

Subject C: *ES*

Valid from: *Thu Dec 11 15:44:00 CET 2025*

Valid to: *Sat Dec 11 15:44:00 CET 2027*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:5C:F9:BE:8F:0F:9D:7B:48:65:40:D4:DD:4B:10:BB:7B:DB:84:0D:8A:7D:A
7:41:E1:A7:C9:8E:60:89:5C:3A:FC:10:8F:22:71:1E:63:20:33:0F:12:09:6D:CC:6A:51:78:25:78:78:DA:02:67:B1:9C:52:89:30:09:C5:EF:35:BA:C5:84:7B:F5:5D:56:FD:2C:EC:4A:28:90:A0:
24:25:A6:F5:D7:60:2F:82:E5:13:78:FD:6A:D6:5E:92:F5:B3:7A:B9:1D:BE:7F:14:C4:30:A3:4F:93:01:63:FA:1F:06:55:DC:C4:0D:24:DD:A6:0A:CA:41:89:4C:5D:37:55:32:91:15:83:98:79:A
5:A7:E7:53:A1:0C:33:E0:DE:E1:18:9A:85:A6:F1:F2:69:82:FD:42:16:ED:CE:E1:1F:38:29:A3:B3:21:A0:BC:75:9B:7F:0F:13:C7:08:1B:D6:7F:B4:6C:B1:94:62:52:66:F1:55:A6:E8:A2:55:A7:
C2:9E:BD:32:EC:F7:CB:C6:44:D0:E0:0A:03:16:69:BA:5A:00:9B:F7:DA:2A:A3:95:07:B7:31:2A:B7:4C:35:82:A5:94:8C:D2:A6:B5:7F:AD:E6:4D:C6:3E:88:2C:55:9D:BC:89:65:F9:DF:E2:F8:
97:23:7E:6C:8B:DD:A6:E6:FA:16:BB:88:02:03:01:00:01

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Authority Info Access
http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *6C:AD:5A:C1:E8:F7:B6:89:FC:67:32:18:34:FB:39:38:AE:7C:E9:A4*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 0.4.0.194112.1.3
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *admon@factorymail.es*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *89:9A:D3:C7:FD:E3:EA:7F:E0:5D:D3:0C:F4:57:A5:14:F4:91:91:3D:AE:49:6C:BF:C3:34:14:E1:75:37:EA:FE*

X509SubjectName

Subject 2.5.4.97: *VATES-B50980804*

Subject CN: *FactoryMail-firma electronica de evidencias*

Subject SERIAL NUMBER: *B50980804*

Subject O: *FACTORYNET AUGUSTA SL*

Subject C: *ES*

X509SKI

X509 SK I *bK1awej3ton8ZzIYNPs5OK586aQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-02-19T03:00:00Z*

57 - TSP: FULL CERTIFICATE S.L.**TSP Name**

Name *[en]* *FULL CERTIFICATE S.L.*

Name *[es]* *FULL CERTIFICATE S.L.*

TSP Trade Name

Name *[en]* *FULL CERTIFICATE, WEVOTE, AVISOS CERTIFICADOS*

Name *[es]* *FULL CERTIFICATE, WEVOTE, AVISOS CERTIFICADOS*

Name *[en]* *VATES- B87336178*

Name *[en]* *FULL CERTIFICATE SL*

Name *[en]* *FULL CERTIFICATE*

PostalAddress

Street Address *[en]* *BOIX Y MORER 6, 9*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28003*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *BOIX Y MORER 6, 9*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28003*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *https://www.fullcertificate.com*

URI *[en]* *mailto:admin@fullcertificate.com*

Issuer OU: *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Issuer OU: *see current address at <https://www.camerfirma.com/address>*

Issuer ST: *MADRID*

Issuer L: *MADRID*

Issuer C: *ES*

Subject C: *ES*

Subject O: *FULL CERTIFICATE SL*

Subject OU: *DIRECCIÓN*

Subject OU: *IT*

Subject 2.5.4.97: *VATES-B87336178*

Subject CN: *FULL CERTIFICATE*

Valid from: *Thu Mar 26 13:31:56 CET 2020*

Valid to: *Mon Mar 25 13:31:56 CET 2024*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DF:43:02:3E:71:22:A0:6D:4F:5B:18:02:36:84:47:9D:31:47:5F:5B:BF:41:67:EC:C7:32:8A:F8:83:38:FA:60:A6:84:AD:3A:38:82:DF:EA:E6:0B:C4:84:62:64:F8:7D:65:E5:22:DE:7C:9B:E0:56:6B:4C:F4:09:23:C4:65:4B:0C:24:F6:0D:85:E3:95:78:C8:E4:1E:AD:E2:50:F3:07:8D:A4:48:DC:11:7F:48:30:3C:B2:AD:3E:36:E4:C9:38:E2:C7:9A:C0:28:DD:DC:A6:50:A3:FF:38:3A:DC:39:69:7C:25:20:BE:A3:BF:83:65:D7:BF:FA:DF:4E:2C:DE:A6:81:EB:7D:91:A3:D3:D3:90:4D:07:31:02:D5:F8:36:4D:B6:E1:01:7E:6C:10:98:F8:79:5B:AA:6A:46:2F:45:91:CF:0C:9F:60:FF:0F:EA:F5:4F:A9:BE:BD:2D:BA:31:A1:EC:03:31:A7:83:D6:CD:A4:89:A1:90:5E:DE:3A:D9:31:12:BA:80:96:0C:6B:9A:E4:C3:F9:8D:85:21:8D:76:49:A4:8D:A9:50:FA:5E:39:DC:A3:0F:34:CA:AD:DB:3D:04:9A:21:BA:42:7E:26:4A:66:76:BC:14:EF:45:56:04:D7:95:A8:64:F2:98:C5:75:B1:A6:60:E3:04:AB:FD:3D:9D:02:03:01:00:01*

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_clientAuth*

Subject Key Identifier *7D:DF:5F:7F:C2:E7:DF:49:2A:45:77:EE:5C:3D:E4:44:53:64:22:64*

Authority Info Access *http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt
<http://ocsp.camerfirma.com>*

Authority Key Identifier *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

CRL Distribution Points *http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl
http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl*

Subject Alternative Name *certificate@fullcertificate.com
OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO*

Issuer Alternative Name *ca@camerfirma.com*

Certificate Policies*Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2**CPS pointer: <https://policy.camerfirma.com>**CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en <https://policy.camerfirma.com>]**Policy OID: 0.4.0.194112.1.1***QCStatements - crit. = false***id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***5A:FD:53:AA:CF:4C:A4:0E:E4:03:A0:C2:71:83:7E:A5:3F:30:77:19:12:29:CA:B6:0B:AC:E3:97:AF:5A:41:4E***X509SubjectName****Subject C:***ES***Subject O:***FULL CERTIFICATE SL***Subject OU:***DIRECCIÓN***Subject OU:***IT***Subject 2.5.4.97:***VATES-B87336178***Subject CN:***FULL CERTIFICATE***X509SKI****X509 SK I***fd9ff8Ln30kqRXfuXD3kRFNklmQ=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2025-07-17T02:00:00Z***57.1.1 - History instance n.1 - Status: granted****Service Type Identifier***<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>***Service Name****Name***[es]**Servicio cualificado de entrega electrónica certificada emitido para FULL CERTIFICATE*

Name [en] *Qualified electronic certified delivery service issued for FULL CERTIFICATE*

Service digital identities

X509SubjectName

Subject C: *ES*

Subject O: *FULL CERTIFICATE SL*

Subject OU: *DIRECCIÓN*

Subject OU: *IT*

Subject 2.5.4.97: *VATES-B87336178*

Subject CN: *FULL CERTIFICATE*

X509SKI

X509 SK I *fd9ff8Ln30kqRXfuXD3kRFNkImQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2023-02-15T00:00:00Z*

57.2 - Service (granted): Servicio cualificado de entrega electrónica certificada emitido para FULL CERTIFICATE 2025

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description [en] *An electronic delivery service providing qualified electronic deliveries.*

[es] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada emitido para FULL CERTIFICATE 2025*

Name [en] *Electronic delivery services providing qualified electronic deliveries for FULL CERTIFICATE 2025*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *770966684301235998123*

Basic Constraints	<i>IsCA: false</i>
Extended Key Usage	<i>id_kp_clientAuth</i>
Subject Key Identifier	<i>1D:CB:84:43:1A:E1:00:BB:B6:2C:DC:38:50:2A:DC:C6:A9:63:CC:2F</i>
Authority Info Access	<i>http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt http://ocsp.camerfirma.com</i>
Authority Key Identifier	<i>C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42</i>
CRL Distribution Points	<i>http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl</i>
Subject Alternative Name	<i>certificate@fullcertificate.com OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO</i>
Issuer Alternative Name	<i>ca@camerfirma.com</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2 CPS pointer: https://policy.camerfirma.com CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com] Policy OID: 0.4.0.194112.1.1</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance id_etsi_qcs_RetentionPeriod: 15</i>
Key Usage:	<i>digitalSignature - nonRepudiation - keyEncipherment</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>67:7E:D4:30:45:33:FE:4C:4F:F4:5B:AB:7E:3D:E2:A8:77:A3:15:FD:71:2E:01:B9:5A :5F:1A:B1:50:BA:8D:5B</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject O:	<i>FULL CERTIFICATE</i>
Subject OU:	<i>IT</i>
Subject 2.5.4.97:	<i>VATES-B87336178</i>
Subject CN:	<i>FULL CERTIFICATE</i>

X509SKI

X509 SK I		<i>HcuEQxrhALu2LNw4UCrcxqljzC8=</i>
Service Status		<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time		<i>2025-07-17T02:00:00Z</i>

58 - TSP: DEH NOTIFICACION ELECTRONICA HABILITADA S.L.**TSP Name**

Name [en] *DEH NOTIFICACION ELECTRONICA HABILITADA S.L.*

Name [es] *DEH NOTIFICACION ELECTRONICA HABILITADA S.L.*

TSP Trade Name

Name [en] *VATES-B86198306*

Name [en] *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

Name [en] *DEH ONLINE*

Name [en] *DEH NOTIFICACION ELECTRONICA HABILITADA SL*

PostalAddress

Street Address [en] *C/ Sierra de Cazorla, 1, Entreplanta, Oficina H, Edificio Cimaga*

Locality [en] *Las Matas - Las Rozas*

State Or Province [en] *Madrid*

Postal Code [en] *28290*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/ Sierra de Cazorla, 1, Entreplanta, Oficina H, Edificio Cimaga*

Locality [es] *Las Matas - Las Rozas*

State Or Province [es] *Madrid*

Postal Code [es] *28290*

Country Name [es] *ES*

ElectronicAddress

URI [en] *https://www.dehonline.es/*

URI [en] *mailto:atencionalcliente@dehonline.es*

TSP Information URI

URI	[en]	https://www.dehonline.es/

58.1 - Service (granted): Sellos de tiempo cualificados emitidos por DEH QUALIFIED
TSU01

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</i>	
Service type description	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Service Name

Name	[es]	Sellos de tiempo cualificados emitidos por DEH QUALIFIED TSU01
Name	[en]	Qualified timestamps issued by DEH QUALIFIED TSU01

Service digital identities

Certificate fields details

```

Version:                               3

Serial Number:                          2014633181964808981

X509 Certificate                        -----BEGIN CERTIFICATE-----

```

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA1 2021

Issuer OU: *TSP-UANATACA*

Issuer 0: UANATACA S.A.

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B86198306*

Subject CN: *DEH QUALIFIED TSU01*

Subject OU: *DEH TSP*

Subject O: *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Tue Sep 21 18:47:29 CEST 2021*

Valid to: *Fri Sep 21 18:47:29 CEST 2029*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:90:3C:AB:D1:3E:C2:F4:63:64:ED:F1:E9:CD:7E:48:3C:C2:CD:0F:C4:93:3E:46
15:A6:40:80:07:29:03:E9:DD:A4:F7:6C:2D:36:FC:1F:CA:F0:A2:A4:E2:A1:27:81:82:82:CF:E7:9F:34:F8:63:47:2B:63:2D:CE:A5:5B:AE:88:03:24:7D:58:E3:8B:8F:DE:97:EB:F5:B6:AB:12:4
0:A2:D4:B2:61:F2:A2:F6:2A:80:3B:E8:DF:27:BD:45:EE:C7:98:10:49:55:88:6F:31:75:99:A1:B3:AC:59:40:1D:B4:EC:5C:DA:7F:D4:FE:05:DF:E0:8C:7C:8E:54:79:7E:2E:20:4D:7A:2D:B4:C7
:E5:5E:40:9B:AA:E7:75:8A:20:6C:DA:74:21:C8:CD:E8:F6:69:EA:58:47:B1:04:C8:73:FE:4D:61:CE:5A:2B:F4:CC:E1:5D:64:B1:49:08:80:B7:B6:CC:75:41:D3:77:78:01:11:74:3E:AD:B8
9D:34:CF:4D:53:2E:30:03:5D:81:57:0A:24:56:BC:E5:0D:C1:68:14:60:EF:1F:7D:E2:5D:6D:5C:54:65:45:BE:1C:BF:8E:0D:F3:7C:D1:13:98:BF:7A:31:EE:85:65:DE:69:AC:26:68:4F:E6:27:0
A:0D:C4:F7:1C:A8:A1:BF:5F:2B:92:87:02:03:01:00:01

Authority Info Access
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *80:C0:E2:57:C7:6B:A2:91:B4:E6:FC:09:36:FE:7A:0F:82:B2:39:1D*

Basic Constraints *isCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *atencionalcliente@dehonline.es*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *89:BF:44:87:9E:D7:B5:11:8A:90:00:E7:10:98:2E:53:6A:BA:AA:BD:E4:F9:34:AA:D
C:67:68:84:C2:4E:CD:E0*

X509SubjectName

Subject 2.5.4.97: *VATES-B86198306*

Subject CN: *DEH QUALIFIED TSU01*

Subject OU: *DEH TSP*

Subject O: *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

Subject L: *MADRID*

Subject C: *ES*

X509SKI

X509 SK I *gMDiV8dropG05vwjNv56D4KyOR0=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time

2023-02-28T00:00:00Z

58.2 - Service (granted): Qualified electronic time stamps issued by DEH QUALIFIED TSU02

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name *[en]* *Qualified electronic time stamps issued by DEH QUALIFIED TSU02*

Name *[es]* *Sellos cualificados de tiempo electrónicos emitidos por DEH QUALIFIED TSU02*

Service digital identities**Certificate fields details**

Version: *3*

Serial Number: *7723086734428710963*

Authority Info Access	https://www.dehonline.es/ca/certificates http://ocsp1.uanataca.com/tsp/ocsp/ http://ocsp2.uanataca.com/tsp/ocsp/
Issuer Alternative Name	<i>canotises@dehonline.es</i>
Subject Alternative Name	<i>atencionalcliente@dehonline.es</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.57853.2.5</i> <i>CPS pointer: https://www.dehonline.es/ca/dpc/</i> <i>CPS text: [Certificado de sello de tiempo electrónico.]</i> <i>Policy OID: 0.4.0.2042.1.2</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	http://crl1.uanataca.com/public/pki/crl/DEHCA1.crl http://crl2.uanataca.com/public/pki/crl/DEHCA1.crl
Subject Key Identifier	<i>30:56:42:F8:0F:1C:36:79:EE:F3:A1:26:78:49:BF:1E:62:F0:4A:ED</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>95:75:5D:40:AC:28:27:63:DB:4D:5B:E7:0E:75:9F:CC:70:09:70:16:C0:33:18:C4:1A:A0:44:2D:2F:2F:C5:29</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>MADRID</i>
Subject O:	<i>DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.</i>
Subject 2.5.4.97:	<i>VATES-B86198306</i>
Subject OU:	<i>TSP - CERTIBOX</i>
Subject CN:	<i>DEH QUALIFIED TSU02</i>

X509SKI

X509 SK I	<i>MFZC+A8cNnnu86EmeEm/HmLwSu0=</i>

Service Status

Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

58.3 - Service (granted): Qualified certificates issued by CERTIBOX SA Subordinada 01

Service Type Identifier	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>

Service type description	[en] <i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es] <i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name	[en]	Qualified certificates issued by CERTIBOX SA Subordinada 01

Name	[es]	Certificados cualificados emitidos por CERTIBOX SA Subordinada 01

Service digital identities

Certificate fields details

Version: 3

Serial Number: 5447506823635472276

X509 Certificate

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *ES*

Issuer L: *Madrid*

Issuer O: *DEH NOTIFICACION ELECTRONICA HABILITADA SL*

Issuer 2.5.4.97: *VATES-B86198306*

Issuer OU: TSP-CERTIBOX

Issuer CN: CERTIBOX ROOT CA

Subject C: *ES*

Subject L: *Madrid*

Subject O: *DEH NOTIFICACION ELECTRONICA HABILITADA SL*

Subject 2.5.4.97: *VATES-B86198306*

Subject OU: *TSP-CERTIBOX*

Subject CN: *CERTIBOX CA Subordinada 01*

Valid from: *Mon Mar 06 12:43:15 CET 2023*

Valid to: *Wed Mar 05 12:43:15 CET 2036*

Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A5:25:25:34:FD:77:69:ED:28:DE:61:5A:42:D3:59:82:2A:88:A6:14:40:DF:E9:8D:13:48:48:82:6C:5B:6A:C0:8C:F8:A8:79:2D:A2:BA:26:88:48:8C:D5:A9:84:E9:8A:44:6E:2D:EC:A6:14:EE:72:76:60:69:88:61:83:7B:33:F5:B4:5E:73:1E:71:C9:FF:DE:29:CC:28:31:AF:57:D3:EA:16:19:60:FA:A8:F8:E9:D5:C3:AF:A1:07:BE:85:81:AB:99:92:01:C7:B0:DA:46:0F:2E:C3:F9:72:46:34:81:82:6D:B1:CD:1C:FB:D6:01:99:80:24:82:83:EB:A8:4F:FD:BF:EA:C1:E7:94:56:C3:C9:56:BF:0D:14:3E:69:A3:06:40:4F:E6:14:4D:85:F1:5A:68:F5:85:97:A3:57:38:AC:8C:7F:F9:B3:47:2E:12:2C:55:FC:90:E3:93:3A:F7:58:6E:EF:C4:77:48:11:E7:EC:5F:59:F9:01:6E:34:60:9D:13:23:CF:2F:47:16:EB:3A:07:CD:98:77:92:56:47:25:02:1C:34:C0:E9:49:3F:49:4A:8E:CF:BA:22:AC:97:0C:1A:7F:E1:9C:71:05:0B:CF:6A:18:C9:24:CD:B7:21:EB:78:7E:58:C1:E4:67:AA:7E:4D:8D:24:C2:EF:D7:2F:5E:57:61:09:1E:F1:AD:F5:81:70:CB:2E:A3:38:69:90:E9:51:86:0F:15:30:2F:67:F4:00:05:62:3C:AC:77:38:14:F6:8F:3D:C6:62:10:0D:3C:A2:86:1F:2F:C4:C0:3E:77:0E:CF:D0:83:B3:07:1C:4C:C9:1F:72:98:67:CD:DB:81:43:92:2D:CD:F6:8C:AF:6F:C7:3A:68:26:D2:53:0C:51:32:4C:D6:DF:4D:47:2E:44:5A:FB:C2:85:88:D3:5D:13:96:96:23:B7:66:A4:14:68:01:68:67:86:39:F0:8C:9A:EC:3C:92:AF:64:62:45:5E:85:6A:43:97:F6:54:19:B1:10:E7:52:73:E3:9D:88:D0:30:D6:11:01:29:08:03:D8:07:30:D7:D0:CE:72:03:15:47:12:90:A6:0A:70:8A:33:B1:A0:01:32:D3:94:72:C4:56:85:42:89:86:8C:3D:F5:57:55:61:07:39:79:D9:D7:00:9F:F9:21:03:DA:45:46:17:21:F3:4A:48:66:06:EA:57:54:DA:CC:19:B4:6F:B2:06:60:2F:83:2A:55:E7:B2:93:94:8C:B9:86:F1:C5:81:B8:53:1F:12:99:3F:16:10:22:B8:62:8F:39:22:B3:CD:7D:0E:BB:6D:AF:6F:8D:31:28:9E:00:0B:90:D2:37:02:03:01:00:01*

Basic Constraints *IsCA: true*

Authority Key Identifier *20:16:43:D9:F8:6C:6B:52:D4:8F:ED:29:33:7E:84:9C:5B:6C:4D:F2*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Issuer Alternative Name *canotises@dehonline.es*

Subject Alternative Name *canotises@dehonline.es*

Certificate Policies *Policy OID: 2.5.29.32.0
CPS text: [Certificado de la Autoridad de Certificación Subordinada de DEH Online - https://www.dehonline.es/]
CPS pointer: https://www.dehonline.es/ca/dpc/*

CRL Distribution Points *http://crl1.uanataca.com/tsp/crl/arl_deh.crl
http://crl2.uanataca.com/tsp/crl/arl_deh.crl*

Subject Key Identifier *6B:BA:86:25:B6:62:33:98:64:47:EA:B2:37:DF:F5:13:1B:0C:90:7F*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E9:48:5E:07:62:81:B7:83:84:6F:4C:03:E9:29:1D:02:CD:22:FD:1A:0D:A2:C5:5F:05:1D:D4:86:73:44:0A:E8*

X509SubjectName

Subject C: ES

Subject L: Madrid

Subject O: DEH NOTIFICACION ELECTRONICA HABILITADA SL

Subject 2.5.4.97: VATES-B86198306

Subject OU: TSP-CERTIBOX

Subject CN: CERTIBOX CA Subordinada 01

X509SKI

X509 SK I a7qGJbZiM5hkR+qyN9/1ExsMkH8=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2026-03-26T02:00:00Z

58.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

58.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

58.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.57853.1.1.3

Description

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.57853.1.2.3*

Description

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.57853.1.3.3*

Description

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.57853.1.4.3*

Description

Description

59 - TSP: TECALIS SOTWARE S.L.**TSP Name**

Name *[en]* *TECALIS SOTWARE S.L.*

Name *[es]* *TECALIS SOTWARE S.L.*

TSP Trade Name

Name *[en]* *TECALIS*

Name *[en]* *VATES-B70186184*

PostalAddress

Street Address *[en]* *Rúa Oliveira 96 B - Parque empresarial Novo Milladoiro*

Locality *[en]* *Milladoiro (Ames)*

State Or Province *[en]* *A CORUÑA*

Postal Code *[en]* *15895*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Rúa Oliveira 96 B - Parque empresarial Novo Milladoiro*

Locality *[es]* *Milladoiro (Ames)*

State Or Province *[es]* *A CORUÑA*

Postal Code *[es]* *15895*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *https://www.tecalis.com/es*

URI *[en]* *mailto:hello@tecalis.com*

TSP Information URI

URI *[es]* *https://www.tecalis.com/es*

URI *[en]* *https://www.tecalis.com*

Subject OU: *TECALIS TSP*

Subject O: *TECALIS SOFTWARE S.L.*

Subject L: *A CORUÑA*

Subject C: *ES*

Valid from: *Fri May 06 16:26:36 CEST 2022*

Valid to: *Mon May 06 16:26:36 CEST 2030*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D6:2D:34:5E:EC:99:F7:7A:80:E2:23:E1:12:0B:D6:86:95:82:D5:63:96:50:D1:80:29:1A:3C:3C:D4:E4:9F:D7:69:CE:B9:7D:AD:2D:E7:0C:D8:E6:68:29:C9:66:9B:18:E8:7C:7C:D0:38:D8:D1:C2:F2:98:67:DC:9A:F9:FC:96:7A:5F:CD:70:D8:E2:67:09:07:7C:1D:D9:84:D:D:EE:C5:47:EC:2A:1B:9C:87:79:7C:F8:FB:38:AC:B6:85:80:F6:0B:20:FF:39:0F:67:7E:DB:67:48:84:05:BF:E2:4A:B6:2B:99:12:96:FF:3A:19:1D:7B:09:D7:A0:3E:C5:3A:A8:2F:9A:A0:45:7B:E3:CA:42:73:1A:1D:63:97:4D:3F:C2:A1:34:EF:ED:C6:75:19:26:8D:49:78:E8:1B:D7:57:62:78:25:C7:BF:74:58:BC:FF:68:D7:BE:44:8E:26:E3:DF:09:BC:7C:AB:0E:CC:FD:10:37:B2:3C:4B:72:AA:81:07:08:2B:44:C8:FE:2B:3B:A7:1D:B4:FA:59:56:20:F0:0B:16:30:2E:FF:D7:2F:7D:B5:13:19:44:45:A2:3E:55:75:D3:0C:E1:43:3C:C3:57:C0:60:58:5F:17:EF:83:F3:57:7C:12:BD:E0:B9:D5:34:55:EA:F2:E8:7B:D6:E4:D5:31:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *3A:B4:DA:09:58:EA:D4:9B:5E:01:48:9C:29:D9:A1:72:41:C5:0B:30*

Basic Constraints *isCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2*

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl*

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *info@tecalis.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1D:5F:95:13:A7:E4:75:F4:07:E1:46:81:37:B1:58:38:D9:8E:10:28:83:20:E6:58:03:1F:34:A0:4C:A7:0D:B7*

X509SubjectName

Subject 2.5.4.97: *VATES-B70186184*

Subject CN: *TECALIS QUALIFIED TSU01*

Subject OU: *TECALIS TSP*

Subject O: *TECALIS SOFTWARE S.L.*

Subject L: *A CORUÑA*

Subject C: *ES*

X509SKI

X509 SK I *OrTaCVjq1JteAUicKdmhckHFCzA=*

Service Status *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2023-03-28T00:00:00Z*

60 - TSP: INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.**TSP Name**

Name [en] *INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.*

Name [es] *INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.*

TSP Trade Name

Name [en] *INDIZE*

Name [en] *VATES-A18962399*

Name [en] *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

PostalAddress

Street Address [en] *Camino de la Torrecilla N.º 30, Edificio Educa Edtech, Oficina 11*

Locality [en] *Maracena*

State Or Province [en] *GRANADA*

Postal Code [en] *18200*

Country Name [en] *ES*

PostalAddress

Street Address [es] *Camino de la Torrecilla N.º 30, Edificio Educa Edtech, Oficina 11*

Locality [es] *Maracena*

State Or Province [es] *GRANADA*

Postal Code [es] *18200*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:empresa@indize.es*

URI [en] *https://indize.es/*

TSP Information URI

URI [en] *https://indize.es/*

Subject CN: *INDIZE CA Subordinada 01*

Subject OU: *TSP - INDIZE*

Subject O: *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

Subject L: *Granada*

Subject C: *ES*

Valid from: *Wed Nov 24 13:00:15 CET 2021*

Valid to: *Fri Nov 24 13:00:15 CET 2034*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AD:F7:F9:A6:40:47:60:3F:DE:2A:62:50:14:B3:27:61:D8:A0:DE:60:55:84:6A:
47:3D:A3:05:15:74:5F:73:6F:E8:7C:3D:D6:79:A3:D5:D3:87:68:FD:CE:81:B5:9A:F3:74:20:86:89:2C:5B:C8:28:BA:C4:F8:64:D7:05:28:CA:9E:07:A3:C5:1C:CE:E2:F5:65:A0:68:21:E3:C8:3
4:59:66:D3:69:97:44:D5:80:AC:90:13:FA:99:32:E2:62:AE:8C:30:17:88:E4:3D:70:B5:ED:E5:A6:FA:24:E4:75:2E:92:DB:B9:A1:48:DD:7E:12:7E:DA:98:A3:C6:B7:ED:37:76:C1:33:31:54:25
2F:5D:13:E5:66:E7:20:47:3F:BB:ED:ED:E5:FC:77:0C:6C:8D:BA:67:A6:7E:83:31:98:22:C5:3A:A2:D5:AD:38:AE:DA:4B:67:50:4C:A4:88:AF:DB:C7:85:FF:E1:91:77:60:FE:8A:EB:21:E5:DD:
82:17:21:82:CE:53:D9:F9:98:74:E6:61:41:9A:F2:1C:03:2F:89:36:56:93:E9:19:91:E1:8A:86:76:97:5A:0C:8B:FA:76:88:89:49:D3:90:9B:1E:F3:43:7D:A6:EE:06:6C:24:26:08:C5:67:AC:36
:03:60:1D:05:E2:A0:80:BC:97:27:DC:A0:16:D9:6A:C6:B4:0C:03:DB:58:95:2A:F3:CF:C1:45:3D:98:F9:A4:89:49:D3:80:91:6F:8E:C7:97:C4:59:AB:DD:4C:A2:D4:81:55:70:93:AB:32:53:E1
:AB:08:CD:B1:AB:BC:8C:D9:FF:AD:88:5E:BC:AC:D4:0C:92:96:80:77:A2:81:A1:E9:EE:0F:FA:53:10:D6:8B:DE:FE:6D:EE:05:C3:3F:DD:A8:8E:98:3D:58:F3:C2:4F:1C:0D:3:83:68:DA:21:2F
:E2:7C:0C:16:F7:8E:1E:4E:9F:34:82:4E:15:B5:0C:60:F0:10:8C:3C:DF:36:2A:D9:A0:7C:A5:8B:1E:B5:EF:D2:06:71:A0:E6:12:84:05:0C:8D:51:65:17:37:03:A8:5F:44:C3:80:4D:86:92:45:A
0:34:6A:04:99:48:7D:58:2A:32:42:12:77:92:42:7C:4B:E7:8C:14:70:DC:72:BA:E2:73:58:B5:79:37:59:DF:29:92:6F:8A:37:07:47:87:0C:30:E1:D0:D6:E0:1A:10:97:44:1A:72:0D:AB:95:C1:
6A:2D:AB:B1:7E:50:84:09:1C:13:89:04:C2:DD:0F:30:8B:EE:F0:D4:B0:64:9C:5E:64:B7:BB:7A:B1:E2:AE:8A:F7:EC:C8:E7:78:9D:D4:21:A7:4F:F8:B6:48:8B:02:03:01:00:01

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/*
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *E6:33:F2:3A:87:94:F5:B0:36:7C:2E:DE:14:A9:8C:F2:D9:11:7A:F5*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://indize.es/prestador-cualificado-servicios-de-confianza/politicas-practicas
CPS text: [Certificado de la Autoridad de Certificación Subordinada de INDIZE - https://indize.es/]

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/ar1_uanataca.crl*
http://crl2.uanataca.com/public/pki/crl/ar1_uanataca.crl

Subject Alternative Name *EMPRESA@INDIZE.ES*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:6D:A0:04:80:EB:C8:14:82:E3:DC:20:3C:BD:D4:3D:69:5F:F1:22:12:7A:DD:98:6F:28:79:B6:29:D1:F0:62*

X509SubjectName

Subject 2.5.4.97: *VATES-A18962399*

Subject CN: *INDIZE CA Subordinada 01*

Subject OU: *TSP - INDIZE*

Subject O: *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

Subject L: *Granada*

Subject C: *ES*

X509SKI

X509 SK I *5jPyOoeU9bA2fC7eFKmM8tkRevU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-03-28T00:00:00Z*

60.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

60.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

60.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*
[es] *undefined.*

Criteria list assert=*atLeastOne*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.57967.1.1.2*

Policy Identifier:

Identifier [OIDASURN] *urn:oid:1.3.6.1.4.1.57967.1.2.2*

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.57967.1.3.2

Policy Identifier:

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.57967.1.4.2

60.2 - Service (granted): Qualified timestamps issued by INDIZE Qualified TSU01

Service Type Identifier	http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST	
Service type description	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name	[en]	Qualified timestamps issued by INDIZE Qualified TSU01
Name	[es]	Sellos de tiempo cualificados emitidos por INDIZE Qualified TSU01

Service digital identities

Certificate fields details

Version:	3
Serial Number:	1959589763653621775
X509 Certificate	

-----BEGIN CERTIFICATE-----
MIHfDCCBWSgAwIBAgIIg2hcgfgoQ2ABwDOYIKoZihvcNAQELBQAwgasxCzAJBgNVBAYTAkVTMRAw
DgYDVQHDADhcmF1WWhMTYwAYDVOQKDC1JTNUSVVRVWBgUEFSOSBMSQBSUSBTUaQUJNT04g
RUNPRTk9NSUNBIFMuQ54xFTATBGNVBAaMDFRtUCAtEiORElaRTEhMB8GA1UEAwYUSUSESVpFIENB
IFh1Ym9yZGluYWRhIDAxMRgwFgYDVORhDA9wQVRFUy1BMTh5NjZpOTkwHhcnMjExMTI1MTQyNE1
WncMMkxMTSMTOyNjE1WjBqTElMAkGA1UEBnMCRVhEADA0BGNVBAcMBDdyYW51ZGExNA0BgaNV
BAoMLiUOU1RJVFVUTyBQOVBjEiERJTKFN5vpBQOIPTBF009OT01JQ0EgUys8LjEVMBMGA1UE
CwwMVFNQIC0gSUSESVpFMR8wHOYDVQDDDBZJTKRJKWUgUVVBTEIGSUVEIFRTVTAxMRgwFgYDVORh
DA9wQVRFUy1BMTh5NjZpOTkwHhcnMjExMTI1MTQyNE1WncMMkxMTSMTOyNjE1WjBqTElMAkGA1UEBnMCRVhEADA0BGNVBAcMBDdyYW51ZGExNA0BgaNV
BEZAVWITfTord0FFGjQ0ObdKNTtmbJATY3WuZekJzPL2CRQDZvbEYzN7Dme5c5D60LhyP5kP60A
Q8x25tjGtjGtektY5yAgZlaNI+KQuog2X/DWSlma9tzi862KT9NxsG58wfaJEpThvzj7svNlmo
3UeawPZ0yJgEIToxsJ0az27TgsiebeerhTUUDorqmiZhoHw8B13LmFW38BZAAtL7fImK
2xLZJ4IRvPE09Qw0P9kO3ys4xglpdy2YetQXVsGo4LIDGw0ldkh5pmemg6xmbKe5qTdYioYN
6GyF01hP+rt7JK26xUanPx7SDhVAgMBAAAGggKMIICnJB+BgggrBgEBQCBARyMHAwNgYIKwYB
BQUIMAGCKmhndAaLysyYvNWS51YV5hdFj7SSjB20vcHf0dGIL3Bqa59Y3NwLZA2BgrBgEB
BQcWAYgaHR0CDovL29jC3AyLnVhbmF0YWNhLnNvb59wdWJsaWMvcGtpL29jC3AvMB0GA1UdDgQW
BBTmYXwX+CKYAS3hgz8THWgsYXosLDAJbG9VHRMEAJAAMB8GA1UdIwQYMBaAF0Yz8jgHlPwWnmu
3hSpPLZEX1rMBwC1UdeGQVMB0BUVNUFjU0FASUSSEVpLJATVMThtBgNVHSAEglwgelwGUJ
CisGAQOBgRvAgIwgcYwZAYIKwYBBQUHAgIwB5WAEMAZOBvAHQAa0BmAGkAYwBhAQABwAgAQAA
Z0AGAHMAZOBsAGwAbwAgAQAZQAgAHQAa0BIAgACABvACAQZOBsAGUAyWbDAHABwBuAGkAYwBv
AC4kYkYkYwB6QUHAgEwUlmhndR6oD8vaWSkXpLmVz13By2XMOYWRwcljldWFSaIZoY2FkbyIz
ZXJ2aWwPb3MtZGUTY29uZmlhbnphL3BvbG0aWWhncy1wcmFjdGllYXNwCAyCBACPEgECMH0GA1Ud
HwRZMHQwOKAZoDSGMmh0dHA6Ly9jcmwXLnVhbmF0YWNhLnNvb59wdWJsaWMvcGtpL2NybcC9pbmRm
emUuY3JsMDp0Ag0dhjodRwOibv73jM651YWSHdGFYS5B20vcHf0dGIL3Bqa59Y3NwLZA2BgrBgEB
aXpLmYBdA0BGNVhQBBAT8EBAMCB4AwfYDVR0IAQH/BAwwCgYIKwYBBQUHAgwWHAYDVOR0BBUw
E4ERZWIwcmVzYUUpbmRlcmUuZXNwDOYIKoZihvcNAQELBQADggIBAJbBAhnxUbmtoVajAreRCaSi
N4SRAG33MZT0RnWanWnUjUqVtCDvK9BgMR9YNINWjzsm7uxof8RRFmleH3mqcHq60Ttx56
nDr2YCW6rImx8RwkbqN+U6sZaNH/GeeOp3zoxzO2t8cpM4q+ckA/CBEVGN1QuddhNB8ybcz3Juw
pps++3BQ3zc8kbsxE7fmYQ8aXs4HEZ2IPfxg6DRh82G1YizdF7ELTjmH826Woz2NC4QPu6bEPs
Kktv4V6pKQvac9P1cYDRTPMeGluMhms7V6L8UL1DtWcGRyoYsLoqNYL4LFF56C2zarnYRV
Fxi2OULtAtxs+pq6a3a0ZniocITUMvs6p6j+pBewOc+W32H07IPtSmVPT6oz3Owlmcz7fgB4jr
hsXJhXU6lbZWta0hQ0KrdynBMwLYgY2Pyj1W5pEuBVUAWCZif77BwtsGRV+uYFHQ9KAvsU
aQ1Bmg5c4mpWdJl/mh8cQLGrg6UdTrn58QvNMhYx+70MUAfSKZdmx98WHRMgscowZBNH+Tw
lJUSnsRsbns5bIL4Ujy28x3t8JnXuKpHAM+6TDJgxofpp8NaDEWJpg2Duoc0A4IKm8qnYl+EstX
f00tx5hX4JtpdyCTTzInWnk+4xxSE2kOEtCuXmIAB49XepTN3
-----END CERTIFICATE-----

Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-A18962399
Issuer CN:	INDIZE CA Subordinada 01
Issuer OU:	TSP - INDIZE
Issuer O:	INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.

Issuer L: Granada
Issuer C: ES
Subject 2.5.4.97: VATES-A18962399
Subject CN: INDIZE QUALIFIED TSU01
Subject OU: TSP - INDIZE
Subject O: INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.
Subject L: Granada
Subject C: ES
Valid from: Thu Nov 25 15:26:15 CET 2021
Valid to: Tue Nov 27 15:26:15 CET 2029
Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D9:43:58:14:6C:9F:F4:04:4C:C0:55:62:13:AD:3A:2B:77:41:45:18:94:0E:6D:D2:8D:4E:D9:81:24:04:08:DD:68:BF:65:E2:89:CC:FB:4B:D8:24:50:0D:96:D6:11:8C:CD:EC:39:9E:E5:CE:43:E8:E2:E1:C8:FE:64:3D:B0:00:43:CC:76:E4:9B:68:24:62:6D:D1:E9:2D:63:9C:80:81:92:28:36:2F:8A:42:EA:20:D9:7F:C3:59:29:60:99:AF:6D:CE:2F:3A:D8:A4:FD:37:11:AC:E7:CC:1F:6A:31:29:62:1B:F3:8F:BB:2F:34:89:B4:DD:47:A8:AE:2C:0F:67:4C:88:80:48:93:E8:18:09:17:46:B3:AF:64:E5:81:28:9E:89:B7:9E:AC:8C:13:51:40:E8:AE:A9:A5:66:1A:07:E3:08:01:D7:72:E6:3D:6D:FC:07:30:00:B5:B2:FF:62:59:8A:DB:12:D9:27:89:51:BC:FB:C4:D3:D3:AF:FF:43:FD:91:0D:F2:83:8C:60:22:97:72:09:87:AD:41:75:6C:B0:6A:38:2E:20:C6:C3:48:9D:92:38:79:A6:67:A6:AB:AC:66:6C:A7:B9:A9:37:58:8A:86:0D:E8:6C:85:D3:58:4F:FA:BB:7B:24:AD:BA:C5:46:A7:3F:1E:D2:0E:15:F7:02:03:01:00:01
Authority Info Access <http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>
Subject Key Identifier CC:FD:8C:17:F8:29:18:03:9D:E1:83:3F:13:1D:6A:AC:61:7A:2C:2C
Basic Constraints *IsCA: false*
Authority Key Identifier E6:33:F2:3A:87:94:F5:B0:36:7C:2E:DE:14:A9:8C:F2:D9:11:7A:F5
Issuer Alternative Name EMPRESA@INDIZE.ES
Certificate Policies Policy OID: 1.3.6.1.4.1.57967.2.2
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: <https://indize.es/prestador-cualificado-servicios-de-confianza/politicas-practicas>
Policy OID: 0.4.0.2042.1.2
CRL Distribution Points <http://crl1.uanataca.com/public/pki/crl/indize.crl>
<http://crl2.uanataca.com/public/pki/crl/indize.crl>
Extended Key Usage *id_kp_timeStamping*
Subject Alternative Name empresa@indize.es
Key Usage: digitalSignature

Thumbprint algorithm: *SHA-256*

Thumbprint: *71:1F:A5:07:FD:AC:69:BB:CC:1B:D1:00:78:C5:1A:AA:F8:C0:8E:FC:58:97:0F:18:8A:06:CF:A8:3D:23:4A:D1*

X509SubjectName

Subject 2.5.4.97: *VATES-A18962399*

Subject CN: *INDIZE QUALIFIED TSU01*

Subject OU: *TSP - INDIZE*

Subject O: *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

Subject L: *Granada*

Subject C: *ES*

X509SKI

X509 SK I *zP2MF/gpGAOd4YM/Ex1qrGF6LCw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*
[es] *undefined.*

Status Starting Time *2023-03-28T00:00:00Z*

60.3 - Service (granted): Qualified electronic time stamp issued by INDIZE QUALIFIED TSU 02

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*
[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified electronic time stamp issued by INDIZE QUALIFIED TSU 02*

Name [es] *Sellos cualificados de tiempo electrónico emitidos por INDIZE QUALIFIED TSU 02*

Service digital identities

Certificate fields details

Version: *3*

Authority Key Identifier	<i>E6:33:F2:3A:87:94:F5:B0:36:7C:2E:DE:14:A9:8C:F2:D9:11:7A:F5</i>
Authority Info Access	<i>https://indize.es/wp-content/themes/indize_theme/assets/certificados/SUBCAINDIZE01.cer</i> <i>http://ocsp1.modernpki.com/public/pki/ocsp/</i> <i>http://ocsp2.modernpki.com/public/pki/ocsp/</i>
Issuer Alternative Name	<i>EMPRESA@INDIZE.ES</i>
Subject Alternative Name	<i>EMPRESA@INDIZE.ES</i>
Certificate Policies	<i>Policy OID: 0.4.0.2042.1.2</i> <i>Policy OID: 1.3.6.1.4.1.57967.2.2</i> <i>CPS text: [Certificado de sello de tiempo electrónico.]</i> <i>CPS pointer: https://indize.es/prestador-cualificado-servicios-de-confianza/politicas-practicas</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	<i>http://crl1.modernpki.com/public/pki/crl/indize.crl</i> <i>http://crl2.modernpki.com/public/pki/crl/indize.crl</i>
Subject Key Identifier	<i>43:25:A4:AD:31:A4:A0:2B:5A:B2:90:2F:CD:00:EB:19:BD:91:43:1D</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>F1:F4:E0:A7:10:05:5D:D4:29:C6:76:C3:56:A6:90:4E:4A:20:B5:14:90:DF:DD:69:84:21:A8:F9:22:ED:5F:11</i>
X509SubjectName	
Subject CN:	<i>INDIZE QUALIFIED TSU 02</i>
Subject OU:	<i>TSP - INDIZE</i>
Subject 2.5.4.97:	<i>VATES-A18962399</i>
Subject O:	<i>INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.</i>
Subject L:	<i>Granada</i>
Subject C:	<i>ES</i>
X509SKI	
X509 SK I	<i>QyWkrTGkoCtaspAvzQDrGb2RQx0=</i>

Service Status		<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
Service status description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
Status Starting Time		<i>2026-05-20T03:00:00Z</i>

61 - TSP: ANF Certification Authority, S.L.**TSP Name**

Name *[en]* *ANF Certification Authority, S.L.*

Name *[es]* *ANF Certification Authority, S.L.*

TSP Trade Name

Name *[en]* *VATES-B87341228*

Name *[en]* *ANF CA*

Name *[es]* *ANF CA*

PostalAddress

Street Address *[en]* *Paseo de la Castellana, 79, 7ª planta*

Locality *[en]* *MADRID*

State Or Province *[en]* *MADRID*

Postal Code *[en]* *28046*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Paseo de la Castellana, 79, 7ª planta*

Locality *[es]* *MADRID*

State Or Province *[es]* *MADRID*

Postal Code *[es]* *28046*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *http://www.anf.ac*

URI *[en]* *mailto:info@anf.es*

TSP Information URI

URI *[en]* *http://www.anf.ac/en/*

Service Type Identifier		http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Name [es] *Certificados cualificados emitidos por ANF Qualified for eSignature CA*

Version: 3

Serial Number: 995739836512566230583025529

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: ANF AC SL Root CA

Issuer 2.5.4.97: *VATES-B87341228*

Issuer O: *ANF Certification Authority, S.L.*

Issuer C: *ES*

Issuer SERIAL NUMBER: *B87341228*

Subject CN: ANF Qualified for eSignature CA
Subject OU: Qualified Certificates for electronic signature
Subject 2.5.4.97: VATES-B87341228
Subject O: ANF Certification Authority, S.L.
Subject C: ES
Subject SERIAL NUMBER: B87341228
Valid from: Fri Oct 07 16:16:18 CEST 2022
Valid to: Mon Oct 04 16:16:18 CEST 2032
Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C4:6C:77:69:3F:9F:8A:99:C2:D6:6C:83:DF:C1:48:D2:53:72:72:D3:38:AF:E0:64:11:BB:21:C1:41:01:75:40:FA:4B:9C:8C:0B:A7:84:A7:A0:9F:1F:4B:A8:C7:6B:97:BF:0C:99:26:8F:2A:63:50:75:37:E2:8A:9F:E5:7F:8E:BE:47:8A:4A:0D:8B:1D:9C:63:8A:EB:6D:63:5C:99:64:A3:4F:1C:A1:A1:7A:69:35:ED:D3:86:64:46:74:CB:3D:CF:E2:BB:73:17:9D:DC:E8:23:60:18:12:80:83:59:7E:77:7E:66:28:2F:6C:71:D2:5D:47:CA:80:98:D8:08:EA:61:CD:8A:8F:E0:D7:60:65:4A:40:6C:32:0A:7E:82:E4:52:80:FF:2D:D0:CA:2A:47:8C:EF:E0:55:7E:24:F2:9D:BA:D4:D1:93:D6:59:E6:51:34:8D:54:7E:F7:7B:C6:6D:A8:1D:C5:E8:54:61:41:DC:0F:6E:E0:2F:7B:0C:2F:FB:5C:0D:81:53:31:D2:F9:91:7F:E5:17:27:A7:4F:7E:13:88:9A:1A:C7:06:6F:85:04:CC:73:17:F8:A0:D4:FF:D4:F7:03:54:2E:D2:9F:E1:8C:77:93:5CA9:90:F1:05:BC:CD:A4:48:AD:F6:25:A4:52:9F:D9:AC:00:38:5C:FF:69:F7:A9:98:40:64:46:8E:28:E3:E6:0D:1D:C1:C5:2F:74:3A:05:8D:D8:88:BE:80:FC:5A:3E:3F:E1:5A:3F:99:C2:88:4F:7B:32:EC:F1:F8:20:79:1B:FC:9F:17:AD:F0:61:52:24:C3:90:FA:A5:46:82:8E:A4:76:BF:FA:1D:65:66:96:45:83:C6:9E:9A:AC:B0:0A:54:C7:75:66:91:6E:BA:6C:27:4E:CF:11:B2:1E:98:76:18:E6:FA:51:75:5C:24:8D:47:73:36:C8:C9:08:F4:89:C5:03:88:D0:52:57:02:2B:91:2A:33:2C:43:FE:82:E1:ED:38:32:6C:44:1C:E6:D1:86:80:44:93:F4:FC:6A:6A:A3:66:7D:AE:82:CD:77:60:4E:78:0A:5A:3D:D3:E1:7C:F7:B9:4E:4C:85:66:0F:B3:B3:56:3F:84:84:5D:BE:E7:A5:0D:2F:89:5E:FE:F9:BD:96:FF:7C:13:5B:A3:E0:40:8E:7B:07:5F:2B:74:B0:D5:B5:9D:81:5C:97:14:6D:30:E1:C9:56:29:55:50:8F:33:92:89:5C:37:4E:37:E5:39:1A:A7:7E:08:89:31:6E:06:45:C5:DA:92:14:AD:0A:85:B7:95:FF:B8:76:B5:E2:50:1C:70:D7:EF:CB:CD:31:C6:42:66:5F:64:DC:AF:55:02:03:01:00:01
Authority Key Identifier 4C:54:D3:CF:6B:65:B7:D2:19:C1:16:BD:9A:F4:27:BD:A9:6B:31:4A
Subject Key Identifier 53:8F:EC:3D:AD:1E:BB:A5:7A:86:14:01:05:58:C9:E7:60:F6:1E:92
CRL Distribution Points http://crl.anf.es/crl/ANF_AC_SL_Root_CA-ar1.crl
Certificate Policies Policy OID: 2.5.29.32.0
CPS pointer: <https://anf.es/repositorio-legal/>
CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]
Authority Info Access <http://ocsp.anf.es/spain/AV>
<http://crl.anf.es/certificates-download/ANFACSLRootCA.cer>
Basic Constraints IsCA: true
Key Usage: keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 59:99:78:9A:17:DF:86:74:D0:98:DB:05:7D:F8:ED:37:64:E9:65:29:D4:A0:EB:56:24:6D:E3:C4:6F:B0:E2:8A

X509SubjectName

Subject CN: ANF Qualified for eSignature CA
Subject OU: Qualified Certificates for electronic signature
Subject 2.5.4.97: VATES-B87341228

Subject O: ANF Certification Authority, S.L.

Subject C: ES

Subject SERIAL NUMBER: B87341228

X509SKI

X509 SK I U4/sPa0eu6V6hhQBBVjj52D2Hpl=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2024-02-08T02:00:00Z

61.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

61.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.2.5.1.13

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.2.5.1.14

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.2.5.1.15

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.3.4.1.5.22

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.3.4.1.8.22

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

[en]

[es]

[es]

[en]

3

[illegible]

-----END CERTIFICATE-----

Subject 2.5.4.97: VATES-B87341228

Subject O: ANF Certification Authority, S.L.

Subject C: ES

Subject SERIAL NUMBER: B87341228

Valid from: Fri Oct 07 16:28:18 CEST 2022

Valid to: Mon Oct 04 16:28:18 CEST 2032

Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A7:74:4E:F9:4A:2C:2A:F8:5B:3A:61:3C:88:79:80:D9:CC:F1:E7:97:35:70:84:92:80:24:68:ED:28:92:EAE:68:3A:87:6F:14:22:E9:78:02:60:5C:32:26:9E:46:20:37:7E:94:9C:26:79:62:3A:07:68:70:E1:B2:60:E3:05:CB:08:6F:20:CA:56:17:98:F4:DE:EB:BA:04:F9:7E:63:88:65:76:C4:E6:E7:37:29:66:7F:10:FA:6F:CC:E0:ED:C9:E4:42:01:93:42:00:1E:73:29:31:C3:A9:EB:53:78:5A:B2:EB:5A:FE:7A:6F:B9:D5:AA:A7:B6:18:01:ED:9F:97:35:E4:39:50:79:A2:82:AC:25:A2:CE:78:47:05:8B:29:AB:32:93:FF:9F:A7:C9:CD:4C:D3:89:91:0C:2A:90:32:AA:EB:8C:58:25:1F:8A:4B:38:22:AA:C8:F3:19:B7:D0:C6:1E:38:29:C0:60:BA:AB:61:67:DC:A6:8B:BE:8F:EA:C1:EE:38:52:AD:50:70:88:7C:19:33:F8:14:A1:97:36:4F:81:91:51:E9:8C:91:85:40:94:8E:A1:23:5E:E8:33:5F:85:66:82:55:C8:8F:BA:86:D6:0F:29:04:99:51:14:34:3C:A4:DD:31:6E:87:73:F2:C8:BE:BA:FC:88:BA:63:80:50:28:A5:A3:C5:E8:65:E1:29:0A:F3:39:81:62:51:9A:5C:4D:42:C3:2D:4A:92:2F:08:51:14:A0:78:8F:22:5D:E0:9F:17:38:3D:85:E2:98:45:F0:7B:93:3C:D4:3F:19:8D:F8:CE:10:81:21:11:6D:AE:7C:90:68:8B:A3:53:0F:CA:A3:5B:2C:45:39:BE:73:A8:94:D7:A6:D0:F2:BA:FF:4E:06:FC:7E:DE:F7:F9:5D:AC:45:14:C5:72:3F:D5:2C:D9:39:8D:17:0A:88:2C:25:87:08:77:01:64:1F:A2:11:B3:DE:98:D2:E2:96:3A:FD:0A:51:09:01:32:6E:04:AD:11:11:04:28:CD:17:E5:BC:DC:BE:49:07:39:AB:89:FD:C0:D6:E0:79:A3:1D:6F:BE:78:F1:5D:48:F8:A9:65:9F:23:94:01:E0:23:87:CE:12:CA:A1:4D:8C:F4:2A:12:EC:5A:19:83:C7:41:98:6E:1D:6E:E7:59:CB:ED:0C:91:06:7E:C5:7D:33:EA:FE:A0:9C:93:6C:22:78:85:E5:8E:E2:EF:F3:12:B8:62:47:38:94:0A:C0:01:53:94:E0:FA:69:39:62:AB:F0:F6:A6:4E:A6:86:8F:02:FE:02:84:EA:6B:EB:AB:C5:DB:49:9D:92:DA:AA:8C:93:89:FD:02:03:01:00:01

Authority Key Identifier 4C:54:D3:CF:6B:65:B7:D2:19:C1:16:BD:9A:F4:27:BD:A9:6B:31:4A

Subject Key Identifier 41:08:13:EB:85:53:73:06:56:3B:9E:D4:7A:8C:05:4F:08:E4:EB:25

CRL Distribution Points http://crl.anf.es/crl/ANF_AC_SL_Root_CA-ar1.crl

Certificate Policies
Policy OID: 2.5.29.32.0
CPS pointer: <https://anf.es/repositorio-legal/>
CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]

Authority Info Access
<http://ocsp.anf.es/spain/AV>
<http://crl.anf.es/certificates-download/ANFACSLRootCA.cer>

Basic Constraints IsCA: true

Key Usage: keyCertSign - cRLSign

Thumbprint algorithm: SHA-256

Thumbprint: 16:AD:38:14:2B:F3:D0:7D:42:1B:73:93:E6:99:44:42:40:B1:78:F9:48:0E:AF:37:E0:ED:A8:33:65:C5:39:CF

X509SubjectName

Subject CN: ANF Qualified for eSeal CA

Subject OU: Qualified Certificates for electronic seal

Subject 2.5.4.97: VATES-B87341228

Subject O: ANF Certification Authority, S.L.

Subject C: ES

Subject SERIAL NUMBER: B87341228

X509SKI

X509 SKI QQgT64VTcwZWO57UeowFTwjk6yU=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2024-02-08T02:00:00Z

61.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

61.2.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.25.1.1.7

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.25.1.1.9

Policy Identifier:

Identifier [OIDASURN] urn:oid:1.3.6.1.4.1.49201.25.1.1.11

61.3 - Service (granted): Certificados cualificados emitidos por ANF Secure SSL CA

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [es] Certificados cualificados emitidos por ANF Secure SSL CA

Subject Key Identifier	<i>45:1F:DA:20:D0:D6:95:9D:20:C7:B3:07:4B:67:DC:1C:D7:B9:F6:CA</i>
Extended Key Usage	<i>id_kp_serverAuth</i>
CRL Distribution Points	<i>http://crl.anf.es/crl/ANF_AC_SL_Root_CA-arl.crl</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: https://anf.es/repositorio-legal/</i>
Authority Info Access	<i>http://ocsp.anf.es/spain/AV</i> <i>http://crl.anf.es/certificates-download/ANFACSLRootCA.cer</i>
Basic Constraints	<i>IsCA: true</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>79:A4:9F:18:EA:13:D9:23:45:7C:3B:9F:63:DD:92:AE:33:25:29:90:E4:DA:28:1B:63:41:20:34:C7:47:B3:B9</i>

X509SubjectName

Subject CN:	<i>ANF Secure SSL CA</i>
Subject 2.5.4.97:	<i>VATES-B87341228</i>
Subject O:	<i>ANF Certification Authority, S.L.</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>RR/aINDWIZ0gx7MHS2fcHNe59so=</i>

Service Status

<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>	
Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2024-02-08T02:00:00Z</i>

61.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</i>

Subject O: ANF Certification Authority, S.L.
Subject C: ES
Subject SERIAL NUMBER: B87341228
Valid from: Wed May 24 14:54:58 CEST 2023
Valid to: Sat May 21 14:54:58 CEST 2033
Public Key:
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CB:DD:46:4D:38:8B:16:E1:17:63:51:BF:F2:DC:ED:16:2E:EF:4A:F2:A9:AB:1B:60:00:FA:01:1D:1D:16:A2:AB:4A:8F:66:AD:E6:79:82:B2:EF:20:CF:A4:A1:BE:EF:11:84:2B:A0:7E:E9:05:E2:B4:84:49:AF:AD:69:1A:80:48:60:32:F7:6A:60:05:F8:05:79:CD:F7:02:48:95:53:C5:76:56:BF:AD:0E:80:C8:87:53:C9:04:3F:14:02:2D:0F:29:C4:08:7A:76:35:B7:82:88:81:B7:C8:07:05:84:B1:90:C0:C8:4B:C7:EA:1D:B6:8D:08:3C:12:6F:A4:D6:C1:ED:83:C8:16:3A:38:4C:F3:CA:BC:BC:AC:1E:EB:A1:8C:94:F4:34:4B:D9:AC:05:F1:80:0B:A4:8D:68:C9:84:0A:E5:E8:C0:A5:75:66:DE:F1:DA:6C:45:5B:18:F1:99:DC:04:41:CF:27:70:17:E4:D9:23:A6:F4:C8:AC:FF:F2:C3:01:E0:88:EC:15:04:7D:6F:44:E1:8A:A2:AE:14:80:F0:AF:CA:A8:7D:85:3A:74:71:1B:79:86:36:FB:59:F1:73:D9:0F:96:10:EE:0D:A9:0D:3D:61:E5:36:5C:EC:05:62:C8:F4:FC:C4:72:D4:E7:5C:0A:E3:80:5A:51:E1:56:8A:6B:C1:E8:98:F3:24:69:1F:01:BA:28:FB:D4:C9:3A:68:97:74:A2:1D:3D:6D:0D:48:D9:B1:11:D1:D5:94:00:55:68:41:07:C1:48:45:42:C0:27:F6:CE:B3:D4:9E:56:44:D8:20:80:30:03:BA:A2:00:F4:6A:14:C0:90:ED:8F:6A:31:5E:62:F3:CC:CA:01:46:85:D5:4C:51:30:5A:D5:EC:F3:BC:45:F4:77:21:D8:A6:06:B4:97:D0:32:CC:29:8A:49:F5:29:2E:D7:AD:19:07:1D:79:04:74:42:8F:A5:CE:06:65:E8:08:00:12:94:AA:56:27:1E:4B:73:38:EC:83:CF:D6:6F:2A:05:DF:BE:25:EC:58:A5:66:54:80:5A:5B:61:6D:1D:C8:01:73:AC:41:D1:B6:2F:3A:22:A6:8A:CA:ED:61:6C:3A:8A:EB:41:BF:7A:01:85:37:8E:E2:1F:F5:07:F7:31:56:3E:C9:53:2C:CA:3C:06:6B:2F:26:5C:CC:18:52:9B:8D:FA:5A:5A:43:8D:1E:65:B0:2E:6A:AB:68:5E:76:D9:85:CB:B7:36:29:B0:6A:11:05:73:46:F5:30:1B:85:80:06:B1:7D:5E:6D:93:5B:A3:78:AB:85:8D:2F:61:E2:2B:75:E9:C8:25:61:A7:31:EB:AB:FF:CE:B0:D5:02:03:01:00:01
Authority Key Identifier 4C:54:D3:CF:6B:65:B7:D2:19:C1:16:BD:9A:F4:27:BD:A9:6B:31:4A
Subject Key Identifier 04:20:1B:21:A4:8D:86:1C:83:8A:E8:0C:DB:F4:CB:40:68:80:D0:19
CRL Distribution Points http://crl.anf.es/crl/ANF_AC_SL_Root_CA-ar1.crl
Certificate Policies Policy OID: 2.5.29.32.0
CPS pointer: <https://anf.es/repositorio-legal/>
CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]
Authority Info Access <http://ocsp.anf.es/spain/AV>
<http://crl.anf.es/certificates-download/ANFACSLRootCA.cer>
Basic Constraints IsCA: true
Key Usage: keyCertSign - cRLSign
Thumbprint algorithm: SHA-256
Thumbprint: 1D:14:93:4F:39:07:6A:B9:84:C5:97:65:F3:1D:A4:0C:BA:05:B0:08:DD:67:EA:35:A9:F9:B9:B6:3E:06:71:CA
X509SubjectName
Subject CN: ANF Qualified TSA
Subject OU: Qualified Certificates for timestamping
Subject 2.5.4.97: VATES-B87341228
Subject O: ANF Certification Authority, S.L.
Subject C: ES
Subject SERIAL NUMBER: B87341228

X509SKI**X509 SK I***BCAblaSNhhyDiugM2/TLQGiA0Bk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description** *[en]**undefined.**[es]**undefined.***Status Starting Time***2024-02-08T02:00:00Z***Scheme Service Definition URI****URI** *[en]**https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF-CA.aspx***URI** *[es]**https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF-CA.aspx***61.5 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/EDS/Q***Service type description** *[en]**An electronic delivery service providing qualified electronic deliveries.**[es]**Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.***Service Name****Name** *[es]**Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"***Name** *[en]**Qualified electronic registered delivery service by "Sign to Sign Delivery Services"***Service digital identities****Certificate fields details****Version:***3***Serial Number:***995917462590293480669943701*

Subject Key Identifier *4D:5B:40:49:DE:FB:D7:75:A7:CD:B2:E4:2F:EF:68:AA:18:B1:B3:7F*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *25:27:31:E3:09:3A:87:75:D1:F6:65:E6:20:05:FF:33:59:28:DB:7C:8F:C5:19:9F:34:90:18:4C:74:B3:97:98*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *Sign to Sign Delivery Services*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I*TVtASd7713WnzbLkL+9oqhixs38=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-05-27T00:00:00Z***61.5.1 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/EDS/Q***Service Name****Name**

[es]

*Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"***Name**

[en]

*Qualified electronic registered delivery service by "Sign to Sign Delivery Services"***Service digital identities****X509SubjectName****Subject L:***BARCELONA***Subject ST:***BARCELONA***Subject 2.5.4.97:***VATES-B87341228***Subject OU:***Certificado Cualificado de Sello Electronico***Subject O:***ANF Certification Authority, S.L.***Subject CN:***Sign to Sign Delivery Services***Subject SERIAL NUMBER:***B87341228***Subject C:***ES***X509SKI****X509 SK I***TVtASd7713WnzbLkL+9oqhixs38=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2024-02-08T02:00:00Z*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF AC Servicio de conservación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

Valid from: *Fri May 26 13:50:31 CEST 2023*

Valid to: *Sun May 25 13:50:31 CEST 2025*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C2:FD:C3:1A:19:16:79:CB:F9:19:DF:2A:54:81:15:00:EA:78:F9:D4:2A:52:16:C5:C1:45:15:86:C4:D2:70:66:8B:F6:13:E7:A7:80:59:94:1F:5E:4B:62:BE:97:74:90:70:D4:15:ED:3E:31:AB:7A:D4:5A:2E:5D:D9:2C:28:C7:38:85:5B:EE:2E:92:77:5B:A1:CA:2C:37:CA:DB:BB:CA:B8:7B:3F:D4:0E:FE:3C:00:6B:BD:36:31:18:24:37:DF:BD:B3:C3:BE:E7:D6:99:4F:32:05:74:1F:6F:69:8A:3A:5D:6B:73:50:CA:7A:70:91:07:B4:8A:FE:96:96:74:03:FF:69:03:FA:27:01:21:49:8A:FC:08:3E:FA:EE:04:44:6D:34:3B:4C:F1:8A:EA:96:E1:DC:45:A8:39:1F:F9:47:A2:86:80:EC:78:01:5B:31:DA:E2:80:0D:23:34:94:D1:DE:7A:4E:57:56:69:E0:18:5B:E1:A7:C4:C5:C2:EF:A1:A2:9B:6B:5B:4E:F8:1C:60:93:8C:8B:2E:BD:7C:63:82:9B:8F:7D:A5:0B:DC:4B:80:83:E8:6B:69:BC:E8:24:2C:2B:90:77:C3:D0:88:31:52:1E:37:06:49:94:B6:7D:3C:23:0D:7A:13:08:97:3A:31:A2:FC:AE:80:E1:1D:4B:02:03:01:00:01*

Authority Key Identifier *41:08:13:EB:85:53:73:06:56:3B:9E:D4:7A:8C:05:4F:08:E4:EB:25*

Subject Key Identifier *FC:46:8D:D5:44:63:8D:F4:EB:CD:33:9A:F1:E7:11:16:A3:06:68:81*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BF:AB:31:3C:85:85:92:43:A5:7E:73:11:21:3E:75:DD:74:76:F9:54:30:07:4B:89:FB:DC:80:D2:7D:75:FA:1B*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF AC Servicio de conservación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I */EaN1URjffTrzTOa8ecRFqMGaIE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-05-27T00:00:00Z*

61.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

61.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

61.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

Service Name

Name	<i>[es]</i>	<i>Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados "ANF CA Servicio de conservación"</i>
Name	<i>[en]</i>	<i>Qualified preservation service for qualified electronic signatures and qualified electronic seals "ANF CA Servicio de conservación"</i>

Service digital identities**X509SubjectName**

Subject L:	<i>BARCELONA</i>
Subject ST:	<i>BARCELONA</i>
Subject 2.5.4.97:	<i>VATES-B87341228</i>
Subject OU:	<i>Certificado Cualificado de Sello Electronico</i>
Subject O:	<i>ANF Certification Authority, S.L.</i>
Subject CN:	<i>ANF AC Servicio de conservación</i>
Subject SERIAL NUMBER:	<i>B87341228</i>
Subject C:	<i>ES</i>

X509SKI

X509 SK I	<i>/EaN1URjffTrzTOa8ecRFqMGaIE=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time	<i>2024-02-08T02:00:00Z</i>

61.6.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

61.6.3.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</i>

Service Name

Service digital identities

Page 1550

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

Valid from: *Fri May 26 13:50:30 CEST 2023*

Valid to: *Sun May 25 13:50:30 CEST 2025*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A1:23:BE:08:1D:29:F9:C1:52:12:FE:51:8B:71:B7:B8:2A:E2:52:55:78:5C:A8:15:C9:05:F8:9E:75:F5:AF:31:84:79:88:74:DC:62:FD:11:11:FA:B6:19:1A:C8:7F:86:EB:CA:90:3B:86:D7:AE:CC:E3:74:51:C2:F9:65:02:BC:C6:B1:1E:F4:9D:D8:CA:FF:7E:06:A4:05:CA:F7:14:82:0C:1D:70:E4:96:0B:7F:D6:8E:AC:BE:52:80:16:1F:26:96:38:58:8D:6B:CA:9B:9E:7F:46:00:D7:EA:9B:65:90:F5:C3:12:70:7B:C7:27:3E:9D:AE:22:A4:0F:1D:89:A1:E0:77:72:EE:41:12:B4:48:0D:43:28:1F:5A:02:8E:5E:8B:CD:FA:12:B8:7A:FF:F8:8D:65:56:03:86:E8:D1:35:E1:E0:36:30:2C:2E:1A:E7:81:6A:A7:13:28:78:75:A1:77:17:7D:99:28:BF:7F:1E:A7:72:FC:9A:A4:69:CD:DA:13:34:BF:BF:EF:8D:E5:35:20:32:50:49:D5:6C:B3:B8:86:7B:B8:E3:17:B2:6A:B6:E4:1C:AE:A6:B5:19:0C:C0:2E:2E:39:CF:84:EC:06:76:55:AF:D7:02:3A:CD:FC:DF:9B:D3:FB:FF:32:8A:08:7F:3F:1E:7F:D7:21:81:92:01:02:03:01:00:01*

Authority Key Identifier *41:08:13:EB:85:53:73:06:56:3B:9E:D4:7A:8C:05:4F:08:E4:EB:25*

Subject Key Identifier *1A:8D:08:20:4E:52:58:C6:53:3C:EF:CE:DC:52:72:6C:45:73:1A:6C*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.9*
CPS pointer: http://www.anf.es/documentos
Policy OID: 0.4.0.194112.1.3

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FC:62:D6:7A:39:4F:64:12:C8:C0:93:1D:14:38:06:C5:72:E9:0C:36:DA:60:1A:8E:EE:C9:FB:2F:26:20:62:C5*

X509SubjectName

Subject L: *BARCELONA*

Subject ST: *BARCELONA*

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF AC Servicio de validación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I *Go0IIE5SWMZTPO/O3FjybEVzGmw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2025-05-27T00:00:00Z*

61.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

61.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

61.7.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service Name

Name	[es]	Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados "ANF CA Servicio de validación"
Name	[en]	Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF CA Servicio de validación"

Service digital identities

X509SubjectName

Subject L:	BARCELONA
Subject ST:	BARCELONA
Subject 2.5.4.97:	VATES-B87341228
Subject OU:	Certificado Cualificado de Sello Electronico
Subject O:	ANF Certification Authority, S.L.
Subject CN:	ANF AC Servicio de validación
Subject SERIAL NUMBER:	B87341228
Subject C:	ES

X509SKI

X509 SK I	Go0IIE5SWMZTPO/O3FjybEVzGmw=

Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time	2024-02-08T02:00:00Z

61.7.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

61.7.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

Service digital identities

Version:	3
Serial Number:	994161039288795441469162831
X509 Certificate	-----BEGIN CERTIFICATE-----

Page 1554

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF Servicio de entrega certificada*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

Valid from: *Thu Mar 06 17:00:03 CET 2025*

Valid to: *Sat Mar 06 17:00:03 CET 2027*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A9:1D:F6:65:C0:3A:B4:D1:98:A4:82:48:E4:40:7A:EE:19:60:08:A7:66:AB:64:8A:8B:1F:39:6A:21:85:33:12:68:7A:AD:AA:67:C9:6F:16:90:AA:82:4E:CC:2E:9F:EC:F1:7F:74:7F:C4:93:3E:2B:7F:23:CE:DE:66:0D:A3:5A:3E:3D:06:61:28:51:F3:F2:10:D8:E5:50:8F:2C:5F:9F:84:DD:86:D2:D4:72:1F:94:90:59:09:3D:7E:19:86:46:16:03:69:85:3F:F1:A0:B0:69:5D:20:A9:6F:BE:84:F8:1D:C0:86:2A:53:E8:3C:CF:9E:75:88:B2:25:6A:D2:01:2E:44:17:7F:F3:08:69:29:52:EE:3C:D4:2A:DE:6E:28:1D:11:A4:44:33:99:63:FF:AE:FC:58:F0:BA:9D:6B:A5:3E:B7:01:A9:DD:58:A1:85:A3:22:F4:4D:6C:DE:DB:D2:9C:DC:5F:AC:A6:02:AF:90:7A:AB:93:E4:04:C E:A4:A2:9C:31:90:4D:86:62:A1:88:E5:F6:2A:09:C7:DC:1D:EC:B2:93:47:DC:0C:0C:0D:21:26:FD:6D:22:DF:60:FD:D9:7D:38:23:19:94:BC:F4:6F:DC:0A:38:62:50:6B:E1:A7:01:B6:0F:2F:15:D7:4D:ED:CD:EE:C7:F4:BA:82:11:BF:02:03:01:00:01

Authority Key Identifier *41:08:13:EB:85:53:73:06:56:3B:9E:D4:7A:8C:05:4F:08:E4:EB:25*

Subject Key Identifier *E8:3F:36:C3:1D:CE:7D:E0:EB:3B:25:A9:B0:0C:F8:03:9D:87:0A:B7*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.1*
CPS pointer: http://www.anf.es/documentos
CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]
Policy OID: 0.4.0.194112.1.1

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BD:77:A6:60:A0:AE:E6:06:F2:BA:A3:F2:2F:75:4B:3F:BD:32:56:A2:C5:0C:71:50:1E:FE:A9:F0:D2:53:4B:EF*

X509SubjectName

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF Servicio de entrega certificada*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I *6D82wx3OfeDrOyWpsAz4A52HCrc=*

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]* *undefined.*

[es] *undefined.*

Status Starting Time *2025-05-27T00:00:00Z*

61.9 - Service (granted): Qualified service for the preservation of qualified electronic signatures and qualified electronic seals from ANF Servicio de conservación

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

Service type description *[en]* *A preservation service for qualified electronic signatures.*

[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

Service Name

Name *[en]* *Qualified service for the preservation of qualified electronic signatures and qualified electronic seals from ANF Servicio de conservación*

Name *[es]* *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados de ANF Servicio de conservación*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *994939800220357870304353033*

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.1*
CPS pointer: http://www.anf.es/documentos
CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]
Policy OID: 0.4.0.194112.1.1

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *64:AF:6A:50:83:E3:F1:C7:95:62:B3:F4:E3:E2:1E:F3:FF:C7:9D:6A:C6:73:67:18:B8:6C:B5:C9:02:03:34:84*

X509SubjectName

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF Servicio de conservación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I *jxwZJX+Moi3A2udKJpfXcO/m1aw=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time 2025-05-27T00:00:00Z

61.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

61.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

61.10 - Service (granted): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF Servicio de validación

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

Service type description [en] undefined.
[es] undefined.

Service Name

Name [en] Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF Servicio de validación
Name [es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados por ANF Servicio de validación

Service digital identities

Certificate fields details

Version: 3

Serial Number: 994730265203450812280335571

Subject Alternative Name *soporte@anf.es*
OID.1.3.6.1.4.1.49201.10.4=B87341228

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://crl.anf.es/crl/ANF_Qualified_for_eSeal_CA.crl*

Certificate Policies *Policy OID: 1.3.6.1.4.1.49201.25.1.1.1*
CPS pointer: http://www.anf.es/documentos
CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]
Policy OID: 0.4.0.194112.1.1

Authority Info Access *http://ocsp.anf.es/spain/AV*
http://crl.anf.es/certificates-download/ANFQualifiedforeSealCA.cer

Basic Constraints *IsCA: false*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *39:07:0F:EE:99:8B:1A:A5:7E:90:9D:D8:6D:A8:DF:ED:BC:FA:A8:24:19:0D:9D:A2:85:88:46:DE:70:8C:44:51*

X509SubjectName

Subject 2.5.4.97: *VATES-B87341228*

Subject OU: *Certificado Cualificado de Sello Electronico*

Subject O: *ANF Certification Authority, S.L.*

Subject CN: *ANF Servicio de validación*

Subject SERIAL NUMBER: *B87341228*

Subject C: *ES*

X509SKI

X509 SK I *NTd0vpWKA/vYgltvEfNVU/SZBI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2025-05-27T00:00:00Z

61.10.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation****URI***[en]**<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>***61.10.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[en]**<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

62 - TSP: CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA

TSP Name

Name	[en]	CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA
Name	[es]	CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA

TSP Trade Name

Name	[en]	CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA
Name	[en]	VATES-A81154197

PostalAddress

Street Address	[en]	Avenida de Manoteras, 10
Locality	[en]	Madrid
Postal Code	[en]	28050
Country Name	[en]	ES

ElectronicAddress

URI	[en]	mailto:psc.es@cgi.com
URI	[en]	https://www.cgi.com/spain/es

TSP Information URI

URI	[en]	https://www.cgi.com/spain/es

62.1 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada "CGI (España)"

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description	[en]	An electronic delivery service providing qualified electronic deliveries.
	[es]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Service Name

Name	[es]	Servicio cualificado de entrega electrónica certificada "CGI (España)"
Name	[en]	Qualified electronic registered delivery service by "CGI (España)"

Service digital identities

Certificate fields details

Version:	3
Serial Number:	2968551839957535095
X509 Certificate	<pre> -----BEGIN CERTIFICATE----- MIITCCBjagAwIBAgIJKTJkS4ASXcwDOYKozIhvcNAOELBQAwbgbxCzAIBgNVBAYTAkVTMUQw OgYDVQHDDECYXJlZWxvbmEgKHNIzSjdXJzW50IGFkZHIjZm9yYXQzS3dLnVhbmF0YUVMNmNm bS9hZGRyZXMzZTEwMBQGA1UECgwwNVUFOQVRBODQGA1UECy5BLiEVMBMGA1UECwwwVFNOLVVTkFQUUNB MR0wGAYDVQODDBFVQUS5VEFODQSDQDEgMAkNJE1TMBYGA1UEYDwPbFURVWMO1Y2NzdkNDk5MB4X DTIzMTcwNzE3NTEwMfoXDTI1MTEwNjE3NTEwMfoWgeOxCzAIBgNVBAYTAkVTMUyRAYDVOQKDD1D R0kgSUSGT1JNOVRJTD4gUjI1TEVNUyBBTKogTUFOQUJFTUVOVCBODT05TVUxUQU5UyUyBFUjI1BBw5FB IFBMRiRWEAYDVOQFEwIBODEXNT0xOtcXZSBgVNBAMMKNHSAORXNWYCOYXSkZW4g1ZTsaWRh ZCBKZSBQcmVzdGfkb3lgZGUgU2VydmljaW9zIGRIENvbmZpYWS6Y59UcnVzdCBTZXI2aWNIIFBy b3ZpZGVyMRgwfGyDVRhDA9WQVRfUy1BODEXNT0xOTcwggEiMA0GCsqG5lb3DQEBQUAA4IBDwAw 9gEKAoiBAQCXNG+awUQ7TD0wMLEYg7TtwGqyHzMx7PejrhvLJlVtSLVetBnmKRL0MktsdA qvjqgkykuCeDwGUVXRX90KUYOBGfnc3QYhDLDesmQKZ4Krh9ujF0SQm/mWae/37+gJSA1I40tr6 hIeOfxgT83BghGksIAmMynXWqXindxP7IRiZz8ytki0XmFuD+tv9zjM1+GvEPWILU+a/HDEy EiNLv6Z2AsdhkacXWG7Wh7Bc3e9OuhSVRLstGx65Xc2Muj9RB8tnc48MUy9Up0k4d6gekU+Hcw QKMP9oLVTwpr+DQmKriuoNjgh/WAS41E4f2vnVuU2fc13AgMBAAGggMsMIDKDBYBggrBgEF BQcBAWRmMGQwCAYGBACORgEBMAsGBgOAjkyBAwiBDZA2BgYEAISGAOUwLDAqFIRodhRwczoVl3d3 dy51YW5hdGFYSS5jb20vcHViGjI1Nwcy8TAkVOMBMGBgOAjkyBAwCAYGBACORgEBMAsGBgOAjky BgEFBQcBAOSbYjC6xz8VBggrBgEFBQcAwZjaHR0cDovL3d3dy51YW5hdGFYSS5jb20vcHViGjI1 L2Rvd25sb2FkL3RzcF9jZjI0aWZpY2F0ZXMvc3Vib3kaW5hdGUxLmNydDA2BggrBgEFBQcAwY1Yq aHR0cDovL29ic3AxlNlVhbmF0YUVMNmNm59wdfWjsaWwvcGpL29ic3AwdYjGCCsGAQUFB2A8hipo dHRwOi8vb2NzcDludWfUYXRhY2EuY29tL3B1Ym9pYy9wa2kvb2NzcC6wHOYDVR0OBBYEFPR9LXT FP5pABX4raZ+Kih0j4MAwGA1UdEwEBwQCMAAWhwYDVR0BBGwFoAULXhvsGN/9f9gy/ER0QO MIFtFeUwpg06K8Hr0Q26wY511gYU3LD30UrpURij/nwifMMA0B1YFC5D0VfmsXkxWWN dGimaWNhZG8gY3VhbGimaWNhZG8gZGUgU2VsbG8gRWwY3RyYw7NuaWNwGjUjEhTTSBjZW50cmFs aXphZG8uMDAGCCsGAOUFBwIBFIRodhRwczoVl3d3dy51YW5hdGFYSS5jb20vcHViGjI1Nwcy8w C0YHBACLTEA8ATCBIwYDVR0BBGIMGECECgPgA8hipodHRwOi8vb3J5MS51YW5hdGFYSS5jb20v CHViGjI13Bra59cmwvQ0Exc3Vib3kaW5hZCeuY3JsMECgPgA8hipodHRwOi8vb3J5MS51YW5h dGFYSS5jb20vcHViGjI13Bra59cmwvQ0Exc3Vib3kaW5hZCeuY3JsMA4GA1UdDwEBwQEAwIf 4DA8BmVnV5UEjAUBggrBgEFBQcDAgYikwYBBQIHAwCwQDVR0RBBIwEIOCHNlbnVzQSNnaS5j b20wDOYKozIhvcNAOELBQADgglBADA5P8PCutGfYafn6YjKCEKXMGufOfhwz9iw+OTD55zDkm PQ0iQDzP16GZGwloF4vg9ZNR+658KMLYpM95nbGSV72dTrBxx1lw08h8AJxOv5e6ta0eZ/I 4vyyed7HLdp6K8Hr0Q26wY511gYU3LD30UrpURij/nwifMMA0B1YFC5D0VfmsXkxWWN qKLUxndAvUmKlMBX7xTnY3Aeye/qRSnLLBDHkjtIbpMvoOTCmJ7YVYVnkrbkoHoPv2CVuk67r iukQG3FrB8H4WizjFiyOxibbpQp7sMgvTzNZX7bktng4izO4VWSZUWom5z16eQcQd8uA6iW AFRi1T2F0cV0nXfHwcey1T52BTJ0GvGZilBLKJ5SDrEdg3K7o/w0oR+SV1KkP5Rr c+dwksXsGokbey77HfnPH4p1ypW7wm9M0qYQzChRAa0Fgzdo+aD9ogDAKInfauksQv8zxf+x9e AsjACNa0Fsiagb8kj8sAygNjz2LThyPE003AamcFIN92nNj/Fmj3z8ahDtbzDNz03GSz/MQZ +isd59lWf8W5GfAE0EgP5nBEDTGeY7PQbLeltKDIWEWpPQ1x1515P4kZvZs+IR3GRtC7HBI OxK9N3KeXjAIT0i6A3SIGT3YrR -----END CERTIFICATE----- </pre>
Signature algorithm:	SHA256withRSA
Issuer 2.5.4.97:	VATES-A66721499
Issuer CN:	UANATACA CA1 2016
Issuer OU:	TSP-UANATACA
Issuer O:	UANATACA S.A.
Issuer L:	Barcelona (see current address at www.uanataca.com/address)
Issuer C:	ES
Subject 2.5.4.97:	VATES-A81154197
Subject CN:	CGI (España) en calidad de Prestador de Servicios de Confianza/Trust Service Provider
Subject SERIAL NUMBER:	A81154197
Subject O:	CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA
Subject C:	ES
Valid from:	Tue Nov 07 18:51:00 CET 2023
Valid to:	Thu Nov 06 18:51:00 CET 2025

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:97:34:68:7E:69:65:0E:17:80:ED:D3:03:2D:97:36:2A:ED:3C:06:AB:21:F3:34:
CC:78:3D:E8:E6:97:F8:4B:53:FB:E5:90:85:5E:87:C9:EF:98:A4:6D:D0:D9:2D:B1:88:80:AA:F8:E8:A9:EC:A4:88:27:83:C0:65:94:55:74:4A:F7:42:94:60:E0:46:97:0D:D0:FD:88:43:0D:EB:2
3:99:09:19:E0:A8:7D:BA:31:74:49:03:3F:99:66:9E:FF:7E:E3:F8:62:52:01:39:78:D2:DA:FA:86:2D:1E:38:5C:60:4F:CD:FC:5C:68:46:92:C9:40:98:C6:27:5E:C5:AA:5E:59:DD:C4:FF:FB:95:
18:99:66:BF:32:7E:48:84:5E:61:6E:0F:EB:6F:F7:38:CC:D7:E1:AF:10:F5:A5:53:E6:BF:1C:31:32:12:D3:4B:55:DE:36:4C:08:1D:86:46:9C:5D:61:BF:ED:68:7B:04:2D:DC:F4:53:9D:1D:25:5
1:92:C9:C6:CA:1E:57:71:93:2F:8F:04:7C:88:69:C2:E3:C3:14:63:D5:29:D2:47:7A:19:E9:1D:F8:77:30:40:A3:0F:F6:82:EF:FD:3C:29:9F:ED:10:9A:D9:11:8A:EA:0D:34:98:07:FD:60:39:E3:
51:38:7F:68:E7:56:E5:36:7D:CD:77:02:03:01:00:01

QCStatements - crit. = false*id_etsi_qcs_QcCompliance**id_etsi_qcs_RetentionPeriod: 15***Authority Info Access***http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt**http://ocsp1.uanataca.com/public/pki/ocsp/**http://ocsp2.uanataca.com/public/pki/ocsp/***Subject Key Identifier***F7:ED:F4:B5:D3:14:F8:92:A4:00:57:E2:B0:33:F8:A8:87:A2:3E:3F***Basic Constraints***IsCA: false***Authority Key Identifier***2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5***Certificate Policies***Policy OID: 1.3.6.1.4.1.47286.1.9.5**CPS text: [Certificado cualificado de Sello Electrónico en HSM centralizado.]**CPS pointer: <http://www.uanataca.com/public/cps/>**Policy OID: 0.4.0.194112.1.1***CRL Distribution Points***<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>**<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>***Extended Key Usage***id_kp_clientAuth***Subject Alternative Name***psc.es@cgi.com***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***B4:04:36:35:58:38:1E:EE:13:47:6B:CB:AA:CE:E9:F9:94:3E:BF:09:B9:BF:30:DC:91
:D3:AF:A3:BC:6A:CF:D4***X509SubjectName****Subject 2.5.4.97:***VATES-A81154197***Subject CN:***CGI (España) en calidad de Prestador de Servicios de Confianza/Trust Service Provider***Subject SERIAL NUMBER:***A81154197***Subject O:***CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA***Subject C:***ES***X509SKI**

X509 SK I*9+30tdMU+JKkAFfisDP4qleiPj8=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** [en]*undefined.*

[es]

*undefined.***Status Starting Time***2025-12-18T00:00:00Z***62.1.1 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/EDS/Q***Service Name****Name** [es]*Servicio cualificado de entrega electrónica certificada "CGI (España)"***Name** [en]*Qualified electronic registered delivery service by "CGI (España)"***Service digital identities****X509SubjectName****Subject 2.5.4.97:***VATES-A81154197***Subject CN:***CGI (España) en calidad de Prestador de Servicios de Confianza/Trust Service Provider***Subject SERIAL NUMBER:***A81154197***Subject O:***CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA***Subject C:***ES***X509SKI****X509 SK I***9+30tdMU+JKkAFfisDP4qleiPj8=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2024-03-13T02:00:00Z***62.2 - Service (granted): Qualified electronic registered delivery service by CGI DigitalTrust360 ERDS****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/EDS/Q***Service type description** [en]*An electronic delivery service providing qualified electronic deliveries.*

[es]

Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

Subject C: *ES*

Valid from: *Tue Oct 21 12:11:00 CEST 2025*

Valid to: *Thu Oct 21 12:11:00 CEST 2027*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:07:DC:69:CF:A0:DC:EB:F9:75:DC:F0:38:64:22:4C:31:06:99:72:10:10:A0:37:FF:88:09:CB:16:F2:8E:43:83:99:D0:A5:0E:CD:28:D4:47:E0:52:7C:CE:0F:87:32:85:34:10:D8:80:60:16:EB:5E:4C:02:FB:19:45:3C:58:06:BC:17:80:AA:53:CC:93:20:0E:D6:DA:5C:1C:F7:2F:B5:55:4B:8F:F9:D9:23:08:99:70:78:48:F9:45:D7:AE:8C:0D:8F:B3:16:A0:53:62:80:B5:F7:EF:08:BC:8D:05:F8:21:93:4C:DC:D8:9F:6F:06:5F:AC:D4:07:40:84:84:37:25:E0:66:CF:98:28:15:8F:A6:34:D6:3A:10:F2:2A:64:C8:2D:63:81:5A:C0:2D:66:3F:37:EC:2C:48:65:8D:67:65:6D:08:E1:32:C3:B1:8F:89:73:8D:23:FA:F0:ED:7A:BC:51:6F:10:25:68:46:FB:95:AC:9F:9A:E4:3:8:D8:EE:11:78:D8:42:A9:95:D1:D3:DC:8F:6C:1E:7D:06:6D:90:5C:6A:90:A1:36:02:83:EA:FC:40:43:9C:73:36:2A:EC:69:31:92:7E:5F:FA:A4:5B:EA:EE:32:EC:7F:3D:AE:9D:F8:41:46:D9:03:74:0A:C2:E2:81:37:1F:E4:03:83:EB:02:03:01:00:01*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *9E:8F:A6:D2:BD:BE:A8:A5:79:47:1C:43:B9:2A:02:65:2F:08:BD:9D*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.1.9.5*
CPS text: [Certificado cualificado de Sello Electrónico en HSM centralizado.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.194112.1.1

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *alberto.anayareig@cgi.com*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8B:B0:41:2D:B7:E4:E2:BE:9A:0F:12:53:23:99:95:EE:7B:FE:88:65:4B:6E:8D:A7:78:FB:6F:FA:81:8A:53:C6*

X509SubjectName

Subject 2.5.4.97: *VATES-A81154197*

Subject CN: *CGI (España) en calidad de Prestador de Servicios de Confianza/Trust Service Provider*

Subject SERIAL NUMBER: *A81154197*

Subject O: *CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA SA*

Subject C: *ES*

X509SKI

X509 SK I *no+m0r2+qKV5RxxDuSoCZS8lvZ0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*

[es] undefined.

Status Starting Time *2025-12-18T00:00:00Z*

63 - TSP: FACTUM IDENTITY SOLUTIONS, S.L.U.**TSP Name**

Name [es] *FACTUM IDENTITY SOLUTIONS, S.L.U.*

Name [en] *FACTUM IDENTITY SOLUTIONS, S.L.U.*

TSP Trade Name

Name [en] *FACTUM ID*

Name [en] *VATES-B09694217*

Name [en] *SealSign*

PostalAddress

Street Address [es] *Calle Doctor Zamenhof, 36 bis, 1ª planta*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Postal Code [es] *28027*

Country Name [es] *ES*

PostalAddress

Street Address [en] *Calle Doctor Zamenhof, 36 bis, 1ª planta*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28027*

Country Name [en] *ES*

ElectronicAddress

URI [en] *mailto:accounts.admin@factumid.com*

URI [en] *https://www.factumidentity.com/*

TSP Information URI

URI [en] *https://www.factumidentity.com/reference/sealsend/politica-servicio*

Page 1571

Subject SERIAL NUMBER: *B09694217*
Subject 2.5.4.97: *VATES-B09694217*
Subject O: *FACTUM IDENTITY SOLUTIONS SL*
Subject ST: *Madrid*
Subject C: *ES*
Valid from: *Thu Feb 01 16:35:25 CET 2024*
Valid to: *Sun Feb 01 16:35:25 CET 2026*
Public Key:

```

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DF:6E:4C:32:92:1C:72:4D:F9:88:61:96:C2:38:58:3E:56:CC:D5:97:E9:21:78:
74:6B:A4:31:D3:70:D7:96:27:86:CA:4E:EF:76:C4:72:33:89:AE:4D:5C:66:C9:2B:E1:E0:FC:BC:0E:A7:89:FA:20:5A:7B:8C:CD:36:67:6E:2F:67:84:A8:D8:40:53:76:69:E8:CD:E7:23:E1:6E:6
1:3F:07:6B:7E:92:FA:3D:F5:11:F5:67:C4:CF:6D:08:9A:22:68:9A:02:0A:3D:B2:3A:D1:D7:D7:4C:E5:33:E3:90:A1:CE:AF:C4:B0:4A:05:C1:C6:9E:58:34:14:26:CE:0D:17:C4:34:B8:5B:6B:13
:99:6F:27:93:3C:D5:2B:C1:48:80:24:D1:25:85:F7:3B:2B:36:83:AD:4E:97:C5:38:6F:9F:1F:CD:94:49:CD:09:83:8A:1D:29:E9:D3:9D:99:A9:80:89:7A:56:F8:17:9C:63:AE:2B:C2:C3:74:37:
40:CE:0D:14:56:28:04:A0:97:ED:99:80:62:DF:93:86:FB:F8:D0:F0:F7:8C:FA:6E:7D:9A:D2:56:12:EE:94:D0:26:AD:37:9A:82:25:E1:09:D8:25:45:3D:6D:27:08:75:DF:5E:7E:59:1A:8E:B9:1
2:F8:92:70:62:DA:80:22:38:2B:EB:FF:02:03:01:00:01

```

Basic Constraints *IsCA: false*
Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*
Authority Info Access
http://crl.firmaprofesional.com/cualificados.crt
http://ocsp.firmaprofesional.com
Subject Alternative Name *saas.support@factumidentity.com*
Certificate Policies
Policy OID: 1.3.6.1.4.1.13177.10.1.10.3
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.3
Extended Key Usage *id_kp_clientAuth*
QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD
CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*
Subject Key Identifier *8F:79:40:7C:23:0E:BB:53:57:16:71:0B:F9:96:B9:3F:5C:35:C7:6A*
Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*
Thumbprint algorithm: *SHA-256*
Thumbprint: *6D:AC:39:37:3D:E9:98:72:24:F3:72:CC:18:2D:03:88:E1:59:48:7D:55:44:E1:22:91:90:FC:81:D8:16:71:C7*

X509SubjectName

Subject E: *saas.support@factumidentity.com*

Subject CN: *SealSign*

Subject SERIAL NUMBER: *B09694217*

Subject 2.5.4.97: *VATES-B09694217*

Subject O: *FACTUM IDENTITY SOLUTIONS SL*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *j3IAfCMOu1NXFnEL+Za5P1w1x2o=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2026-03-26T02:00:00Z

63.1.1 - History instance n.1 - Status: granted**Service Type Identifier**

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service Name

Name [es] *Servicio cualificado de entrega electrónica certificada por "SealSign"*

Name [en] *Qualified electronic registered delivery service by "SealSign"*

Service digital identities**X509SubjectName**

Subject E: *saas.support@factumidentity.com*

Subject CN: *SealSign*

Subject SERIAL NUMBER: *B09694217*

Subject 2.5.4.97: *VATES-B09694217*

Subject O: *FACTUM IDENTITY SOLUTIONS SL*

Service Type Identifier		<i>http://uri.etsi.org/TrstSvc/Svctype/PSES/Q</i>
Service type description	[en]	<i>A preservation service for qualified electronic signatures.</i>
	[es]	<i>Un servicio de la preservación de las firmas electrónicas reconocidas.</i>

Name	[en]	Qualified preservation service for qualified electronic signatures and qualified electronic seals SealSafe
Name	[es]	Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados SealSafe

Version: 3

Serial Number: 99732270889796815617082802965669616243

Signature algorithm: *SHA256withRSA*

Issuer CN: *AC Firmaprofesional - CUALIFICADOS*

Issuer SERIAL NUMBER: *A62634068*

Issuer OU: *Certificados Cualificados*

Issuer O: *Firmaprofesional S.A.*

Issuer C: *ES*

Subject CN: *SealSign*

Subject SERIAL NUMBER: *B09694217*

Subject 2.5.4.97: *VATES-B09694217*

Subject O: *FACTUM IDENTITY SOLUTIONS SL*

Subject ST: *Madrid*

Subject C: *ES*

Valid from: *Wed Jan 28 16:28:05 CET 2026*

Valid to: *Thu Jan 28 16:28:05 CET 2027*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A7:D5:B7:47:F2:AA:A0:49:8C:07:05:88:A8:F9:46:01:8A:10:CF:21:8B:E1:24:01:0D:F7:CA:9C:C0:C9:08:8B:EB:33:18:C2:BE:70:F8:18:AD:B5:C2:2E:64:C7:59:90:F8:94:25:A6:33:80:08:CE:49:D0:98:A8:31:EC:0A:A9:AA:BD:BD:D2:BF:0C:80:30:2E:3A:26:25:83:4F:B9:5E:0C:06:54:88:D9:CB:86:82:03:CF:73:7C:86:D8:C5:45:CE:25:20:CF:F3:21:40:3A:6A:90:78:89:48:E6:E5:50:79:72:30:A9:8B:3B:B6:DD:96:6E:EA:9A:C3:35:45:DC:3A:CD:D2:B5:6D:5B:4F:41:F5:BE:D5:CD:D6:CE:14:BA:A4:CE:7E:47:84:51:D7:A2:82:F7:F7:DF:89:E8:EB:41:49:77:A7:4B:B1:1F:92:F0:49:08:C8:DC:68:DE:7C:E7:F5:28:97:9C:03:CL:7A:22:FC:3D:51:12:5A:9D:78:20:CF:75:F1:F0:08:39:B7:44:7A:0A:1C:E4:15:50:F5:D1:FA:6F:67:80:47:87:EF:64:ED:8E:55:3D:A3:FA:72:02:65:2B:3B:07:08:75:E0:58:A9:12:D2:98:F9:44:13:73:78:9C:D9:11:48:12:2B:1D:1E:CC:5C:F0:EE:F0:07:28:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Authority Info Access
http://crl.firmaprofesional.com/cualificados.crt
http://ocsp.firmaprofesional.com

Certificate Policies
Policy OID: 1.3.6.1.4.1.13177.10.1.10.3
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.3

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false
id_etsi_qcs_QcCompliance
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*

Subject Key Identifier *C8:F3:38:68:09:F7:F5:20:AC:6B:81:A6:E7:A9:88:52:68:56:96:5E*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DF:B5:9B:50:15:8F:20:D7:78:0A:5A:3B:7A:8D:7B:B0:04:0C:91:82:3E:3D:C4:ED:4F:FB:1F:8C:F9:FE:E0:A0*

X509SubjectName

Subject CN: *SealSign*

Subject SERIAL NUMBER: *B09694217*

Subject 2.5.4.97: *VATES-B09694217*

Subject O: *FACTUM IDENTITY SOLUTIONS SL*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *yPM4aAn39SCsa4Gm56mIUmhWII4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time

2026-03-26T02:00:00Z

63.2.1 - Extension (not critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

63.2.2 - Extension (not critical): additionalServiceInformation**AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

63.3 - Service (granted): Qualified electronic registered delivery service by SealSend

Subject C: *ES*

Valid from: *Wed Jan 28 16:28:05 CET 2026*

Valid to: *Thu Jan 28 16:28:05 CET 2027*

Public Key:
30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A7:D5:B7:47:F2:AA:A0:49:8C:07:05:B8:AB:F9:46:01:8A:10:CF:21:8B:E1:24:01:0D:F7:CA:8C:0C:9:08:6B:EB:33:18:C2:BE:70:78:18:AD:85:C2:2E:64:C7:58:90:F8:94:25:AB:33:80:08:CE:49:D0:9B:A8:31:EC:0A:A9:AA:BD:8D:D2:BF:0C:80:30:2E:3A:26:25:B3:4F:B9:5E:0C:06:54:88:D9:CB:86:82:03:CF:73:7C:86:D8:C5:45:CE:25:20:CF:F3:21:40:3A:6A:90:78:89:48:E6:E5:50:79:72:30:A9:8B:3B:B6:DD:96:6E:EA:9A:C3:35:45:DC:3A:CD:D2:B5:6D:5B:4F:41:F5:8E:D5:CD:D6:CE:14:BA:A4:CE:7E:47:84:51:D7:A2:82:F7:F7:DF:89:EB:EB:41:49:77:A7:4B:B1:1F:92:F0:49:08:C8:DC:68:DE:7C:E7:F5:28:97:9C:03:CL:7A:22:FC:3D:51:12:5A:90:78:20:CL:75:F1:F0:08:39:B7:44:7A:0A:1C:E4:15:50:F5:D1:FA:6F:67:80:47:87:EF:64:ED:8E:55:3D:A3:FA:72:02:63:2B:3B:07:08:75:E0:58:A9:12:D2:98:F9:44:13:73:78:9C:D9:11:48:12:28:1D:1E:CC:5C:F0:EE:F0:07:2B:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

Authority Info Access
http://crl.firmaprofesional.com/cualificados.crl
http://ocsp.firmaprofesional.com

Certificate Policies
Policy OID: 1.3.6.1.4.1.13177.10.1.10.3
CPS pointer: http://www.firmaprofesional.com/cps
CPS text: [Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]
Policy OID: 0.4.0.194112.1.3

Extended Key Usage *id_kp_clientAuth*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

CRL Distribution Points *http://crl.firmaprofesional.com/cualificados.crl*

Subject Key Identifier *C8:F3:38:68:09:F7:F5:20:AC:6B:81:A6:E7:A9:88:52:68:56:96:5E*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DF:B5:9B:50:15:8F:20:D7:78:0A:5A:3B:7A:8D:7B:B0:04:0C:91:82:3E:3D:C4:ED:4F:FB:1F:8C:F9:FE:E0:A0*

X509SubjectName

Subject CN: *SealSign*

Subject SERIAL NUMBER: *B09694217*

Subject 2.5.4.97: *VATES-B09694217*

Subject O: *FACTUM IDENTITY SOLUTIONS SL*

Subject ST: *Madrid*

Subject C: *ES*

X509SKI

X509 SK I *yPM4aAn39SCsa4Gm56mlUmhWll4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*
[es] undefined.

Status Starting Time *2026-03-26T02:00:00Z*

64 - TSP: TRUSTCLOUD TECH SL

TSP Name

Name [en] TRUSTCLOUD TECH SL

Name [es] TRUSTCLOUD TECH SL

TSP Trade Name

Name [en] TRUSTCLOUD TECH

Name [es] TRUSTCLOUD TECH

Name [en] VATES-B67693655

Name [en] Trustcloud Tech SL

Name [es] Trustcloud Tech SL

PostalAddress

Street Address [en] C/Buenos Aires, 12

Locality [en] BILBAO

Postal Code [en] 48001

Country Name [en] ES

ElectronicAddress

URI [en] https://trustcloud.tech/es

URI [en] mailto:contact@trustcloud.tech

TSP Information URI

URI [en] https://trustcloud.tech/es/

64.1 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals "Trustcloud Tech"

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

Service type description [en] A preservation service for qualified electronic signatures.

[es] Un servicio de la preservación de las firmas electrónicas reconocidas.

Valid from: *Tue Jul 16 13:37:00 CEST 2024*

Valid to: *Sun Jul 15 13:37:00 CEST 2029*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9A:48:28:0A:58:4C:30:8E:97:5A:68:58:99:A4:F3:20:FA:5B:48:3C:D1:3C:47:75:5C:9A:5E:15:7E:74:5D:00:11:3A:40:A0:8A:6F:9D:20:3F:C3:78:7E:FC:99:2E:0A:CF:F8:7B:C4:66:23:D5:63:F7:E3:9B:36:A6:3E:AA:AC:0C:8F:2F:A7:FE:0C:37:33:C7:E4:79:22:66:98:1C:69:B7:5A:AA:8C:06:C1:64:F7:51:7C:45:18:E3:AE:70:FA:10:E7:67:49:46:5D:88:D9:F6:09:89:B8:3D:80:DE:9E:A5:AA:41:14:4A:22:60:6F:D2:94:5E:6C:77:72:FF:0F:CF:B8:9D:73:22:34:F1:0C:BF:CF:61:4F:71:CE:C8:BE:09:1A:6D:95:B3:6E:48:35:BA:F4:9D:1D:82:DE:A8:93:58:5B:91:9C:CF:DA:27:45:A0:7E:B7:2F:41:5F:B8:84:14:03:70:3C:A4:3F:A2:B3:E0:9F:26:FE:53:BC:01:A3:79:38:93:68:E8:05:15:FD:7E:A3:41:43:24:83:86:C8:DD:2B:78:85:03:34:28:6E:32:98:20:5A:A9:8A:A2:0D:C8:62:1D:54:63:FC:23:16:AC:B8:52:69:F4:3A:A0:A6:48:EA:2A:ED:77:AE:03:B4:3D:00:5F:02:A1:35:02:D5:02:03:01:00:01*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_RetentionPeriod: 15
id_etsi_qcs_QcSSCD

Authority Info Access *http://www.uanataca.com/public/download/tsp_certificates/trustedRoot.p7c*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *3C:58:02:1B:82:4A:23:34:FD:92:74:E0:F6:B6:A9:D4:F0:16:5B:82*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 0.4.0.194112.1.3*
Policy OID: 1.3.6.1.4.1.47286.1.9.6
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Qualified certificate for e-seal in Remote QSCD]

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *adam.shaw@trustcloud.tech*

Key Usage: *digitalSignature - nonRepudiation - keyEncipherment*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CD:39:6F:37:DE:DC:1A:6B:8A:ED:8B:47:FF:5C:EC:7E:A3:0C:41:82:00:23:B4:C2:55:3B:B9:62:C5:75:E5:4C*

X509SubjectName

Subject 2.5.4.97: *VATES-B67693655*

Subject CN: *Firma certificado de evidencias Trustcloud como QTSP*

Subject SERIAL NUMBER: *B67693655*

Subject O: Trustcloud Tech SL

Subject C: ES

X509SKI

X509 SK I PFgCG4JKIzT9knTg9rap1PAWW4I=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2024-11-08T02:00:00Z

64.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

64.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

65 - TSP: BEYOND THE SCOPE S.L.

TSP Name

Name [en] *BEYOND THE SCOPE S.L.*

Name [es] *BEYOND THE SCOPE S.L.*

TSP Trade Name

Name [en] *Permisso*

Name [es] *Permisso*

Name [en] *VATES-B0494876*

PostalAddress

Street Address [en] *Ronda de Sant Pere, 52*

Locality [en] *Barcelona*

State Or Province [en] *Barcelona*

Postal Code [en] *08010*

Country Name [en] *ES*

ElectronicAddress

URI [en] *https://qtsp.permaniso.io/*

URI [en] *mailto:info@permaniso.io*

TSP Information URI

URI [en] *https://qtsp.permaniso.io/*

65.1 - Service (granted): Qualified certificates issued by Permisso CA Subordinada 01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

Service Name

Certificate fields details

Version: 3

Serial Number: 5148496260570565278

[illegible]

ESPAÑA (SPAIN) - Trusted List ID: TSL20260520 Page 1585

Valid from: *Mon Mar 06 14:55:18 CET 2023*

Valid to: *Sun Mar 09 14:55:18 CET 2036*

Public Key: *30:82:02:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CA:A6:C1:68:66:7F:34:B9:7D:2B:E7:8A:56:8D:C8:F2:1F:19:4C:00:3B:55:33:1B:93:06:1C:6C:80:8B:FF:99:80:5B:6E:13:90:6F:E3:11:A5:9D:61:C8:0F:35:68:4C:2B:D0:CA:E6:95:1B:BE:BF:1D:8D:B7:F9:5B:93:CC:55:C8:2F:2A:4F:28:B6:0D:D6:2E:EC:57:EE:38:FF:47:4E:46:A6:7F:FC:86:6F:9F:3C:2:2A:80:F1:F3:8A:AB:1A:DE:9D:E0:19:4B:3F:78:80:AC:58:8A:6D:53:7B:51:D0:34:AB:5E:E3:88:C8:0B:18:2A:C0:90:08:72:4D:F8:DE:BD:F4:05:8B:8B:F2:CC:3B:3C:66:13:E2:3F:F6:54:1B:7C:AA:30:02:08:83:46:69:61:1F:1C:A1:0B:DC:FE:C0:A2:24:C2:E1:8E:A2:23:68:D5:A7:8B:18:0F:FE:4A:6D:61:1F:B0:56:2D:C4:0E:BF:89:E7:18:EA:04:D2:1C:3F:3E:42:4D:F1:54:2E:74:60:66:2E:87:A9:1D:4A:FD:DE:B8:17:3F:EF:60:1C:2E:6B:57:4B:CS:4A:BD:42:AB:93:D7:BD:AC:E1:9C:79:D2:9F:8E:53:7B:EE:63:44:31:1A:01:05:CE:B5:BF:13:65:87:E1:0C:B1:8F:EA:7A:CA:E4:7F:3A:10:82:5E:C7:57:7C:DF:7C:AA:25:D7:41:1F:06:FB:CD:E8:36:8E:8B:70:86:D9:8A:D6:F6:98:2A:9A:05:70:08:75:84:FC:26:B4:CS:DE:16:B6:D3:00:BD:25:9C:94:66:88:94:28:4F:E2:E9:21:CC:6D:83:9D:77:F3:21:8B:AE:EA:00:A5:00:63:9B:8B:CE:A1:88:96:5D:CA:DD:9F:99:61:F2:AD:65:7D:96:BF:96:3A:3C:22:1E:EE:90:A2:09:40:1A:8F:7A:91:FD:0C:FC:C7:8C:ED:AA:15:0E:37:0F:56:FA:A9:81:34:33:F5:34:BD:9A:AC:A1:02:91:96:1D:6E:11:4D:E4:14:12:50:59:B3:36:AD:63:AE:81:36:87:35:56:35:19:8A:C2:4F:E8:2D:B2:FC:F1:2B:44:52:15:AC:AA:D5:07:F7:88:D3:44:93:94:75:C3:97:AB:E4:C0:B0:00:30:FD:15:09:65:E8:43:9B:E0:78:DD:A3:BC:07:74:17:1B:0D:0E:8F:87:28:57:B4:80:FC:57:81:A1:02:5E:05:29:6E:89:25:7D:90:04:42:57:FC:4B:8C:19:4E:AB:65:3A:CF:14:91:78:5E:F5:FF:B7:A1:04:D8:88:3F:85:8B:A3:98:39:84:3F:8F:E3:44:1E:D1:E3:A5:02:03:01:00:01*

Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/*

Subject Key Identifier *B3:B5:60:1A:02:45:2B:04:A6:46:EF:51:43:CD:61:B6:C6:DD:C7:A2*

Basic Constraints *IsCA: true - Path length: 0*

Authority Key Identifier *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS text: [Certificado de la Autoridad de Certificación Subordinada de BEYOND THE SCOPE S.L. - https://qtsp.permisso.io/]
CPS pointer: https://qtsp.permisso.io/cps/

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*

Subject Alternative Name *info@permisso.io*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4A:D8:10:EF:18:DB:53:E0:0F:84:D0:BC:61:28:35:03:44:E6:66:E7:D3:D3:7E:FE:1A:8C:21:16:44:60:BF:AC*

X509SubjectName

Subject C: *ES*

Subject L: *Barcelona*

Subject O: *BEYOND THE SCOPE S.L.*

Subject 2.5.4.97: *VATES-B04948766*

Subject OU: *TSP-Permisso*

Subject CN: *Permisso CA Subordinada 01*

X509SKI

X509 SK I s7VgGgJFKwSmRu9RQ81htsbdx6I=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] undefined.
[es] undefined.

Status Starting Time 2025-07-17T02:00:00Z

65.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

65.1.2 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.60078.1.2.3

Description

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.60078.1.1.3

Description

Policy Identifier:

Identifier [OIDA sURN] urn:oid:1.3.6.1.4.1.60078.1.3.3

Description

Description

65.1.3 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name	<i>[en]</i>	<i>Qualified certificates issued by Permisso CA Subordinada 01</i>
Name	<i>[es]</i>	<i>Certificados cualificados emitidos por Permisso CA Subordinada 01</i>

Service digital identities**X509SubjectName**

Subject C:	<i>ES</i>
Subject L:	<i>Barcelona</i>
Subject O:	<i>BEYOND THE SCOPE S.L.</i>
Subject 2.5.4.97:	<i>VATES-B04948766</i>
Subject OU:	<i>TSP-Permisso</i>
Subject CN:	<i>Permisso CA Subordinada 01</i>

X509SKI

X509 SK I	<i>s7VgGgJFKwSmRu9RQ81htsbdx6I=</i>

Service Status	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>

Status Starting Time	<i>2025-04-16T02:00:00Z</i>

65.1.3.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>

65.1.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier	<i>[OIDsURN]</i>	<i>urn:oid:1.3.6.1.4.1.60078.1.1.2</i>

Description

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.60078.1.1.3*

Description

Policy Identifier:

Identifier *[OIDsURN]* *urn:oid:1.3.6.1.4.1.60078.1.2.2*

Description

Description

66 - TSP: EDATALIA DATA SOLUTIONS, S.L.**TSP Name**

Name *[en]* *EDATALIA DATA SOLUTIONS, S.L.*

Name *[es]* *EDATALIA DATA SOLUTIONS, S.L.*

TSP Trade Name

Name *[en]* *VATES-B20935532*

Name *[en]* *Edatalia*

Name *[en]* *EDATALIA TSP*

PostalAddress

Street Address *[en]* *Paseo de los Arbustos, 18 - 1 IZ*

Locality *[en]* *Donostia*

State Or Province *[en]* *Guipúzcoa*

Postal Code *[en]* *20009*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Paseo de los Arbustos, 18 - 1 IZ*

Locality *[es]* *Donostia*

State Or Province *[es]* *Guipúzcoa*

Postal Code *[es]* *20009*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *https://edatalia.com/*

URI *[en]* *mailto:edatalia@edatalia.es*

TSP Information URI

URI *[en]* *https://edatalia.com/*

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified time stamps issued by EDATALIA QUALIFIED TSU01

Name [es] *Sellos de tiempo cualificados emitidos por EDATALIA QUALIFIED TSU01*

Certificate fields details

Version: 3

Serial Number: 6777637516184394150

[illegible]

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: UANATACA CA1 2021

Issuer OU: TSP-UANATACA

Issuer O: UANATACA S.A.

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B20935532*

Subject CN: *EDATALIA QUALIFIED TSU01*
Subject OU: *EDATALIA TSP*
Subject O: *EDATALIA DATA SOLUTIONS, S.L.*
Subject L: *SAN SEBASTIÁN*
Subject C: *ES*
Valid from: *Mon Sep 30 18:01:21 CEST 2024*
Valid to: *Sat Oct 02 18:01:21 CEST 2032*
Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:63:A3:64:DA:33:5E:E7:A3:60:03:10:EA:FB:87:43:97:88:E3:7F:DA:27:99:E5:31:C3:0F:13:22:76:14:DC:88:9D:2C:74:98:C9:27:3D:E8:EE:42:18:78:B2:AC:5C:7F:00:D5:D1:93:A4:09:17:7B:AA:E2:04:DE:4A:8D:87:B1:86:19:96:C5:02:01:08:69:93:9A:D2:2F:D1:47:DC:FE:B3:9E:7C:0F:8B:82:E5:C6:AF:E6:10:FC:9C:DB:8F:F6:7F:5A:99:14:A4:DD:CE:D6:59:B9:B5:D1:A7:F3:10:58:DA:1E:57:AF:B8:61:A7:80:EF:AF:D0:83:F5:48:CC:E0:C5:A9:DA:BD:91:60:24:BD:A8:46:FF:2F:6D:4E:2F:51:A9:73:66:A8:69:AB:DF:3F:92:25:F7:65:E9:A4:CC:08:F4:15:05:60:B3:DC:AB:29:AB:57:6A:1C:52:97:09:35:26:CC:9F:33:88:BA:3F:A7:27:26:8A:E1:09:6F:84:DD:71:94:11:72:CB:E2:37:50:C1:75:7D:40:E4:49:E7:B7:DE:A9:16:9A:44:F9:D3:F8:38:86:57:D4:2E:8E:D8:63:F5:C7:AD:9F:8B:66:6D:6B:A4:10:F0:CC:69:3D:38:B3:9C:7C:15:F2:0C:C5:0F:E7:03:ED:9E:41:79:A8:02:03:01:00:01*
Authority Info Access *http://ocsp1.uanataca.com/public/pki/ocsp/*
http://ocsp2.uanataca.com/public/pki/ocsp/
Subject Key Identifier *A8:9E:DB:57:9D:73:0F:8C:9A:75:38:24:B3:18:F8:1F:97:C6:C3:28*
Basic Constraints *IsCA: false*
Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*
Issuer Alternative Name *info@uanataca.com*
Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2
CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
Extended Key Usage *id_kp_timeStamping*
Subject Alternative Name *contacto@edatalia.com*
Key Usage: *digitalSignature*
Thumbprint algorithm: *SHA-256*
Thumbprint: *76:71:7F:DF:88:1C:4C:1F:AC:6F:D2:BD:84:FC:B7:5D:8F:9C:04:85:BD:EF:DB:52:B
E:87:B7:0B:54:35:CC:5D*

X509SubjectName

Subject 2.5.4.97:	VATES-B20935532
Subject CN:	EDATALIA QUALIFIED TSU01
Subject OU:	EDATALIA TSP
Subject O:	EDATALIA DATA SOLUTIONS, S.L.
Subject L:	SAN SEBASTIÁN
Subject C:	ES
X509SKI	
X509 SK I	qJ7bV51zD4yadTgksxj4H5fGwyg=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2025-09-03T02:00:00Z

67 - TSP: RUBRICAЕ BUSINESS SOLUTIONS, S.L.**TSP Name**

Name [en] RUBRICAЕ BUSINESS SOLUTIONS, S.L.

Name [es] RUBRICAЕ BUSINESS SOLUTIONS, S.L.

TSP Trade Name

Name [en] RUBRICAЕ

Name [es] RUBRICAЕ

Name [en] VATES-B88564398

PostalAddress

Street Address [en] C/ Bruselas, 36B

Locality [en] Las Rozas

State Or Province [en] Madrid

Postal Code [en] 28232

Country Name [en] ES

PostalAddress

Street Address [es] C/ Bruselas, 36B

Locality [es] Las Rozas

State Or Province [es] Madrid

Postal Code [es] 28232

Country Name [es] ES

ElectronicAddress

URI [en] mailto:soporte@rubricae.com

URI [en] https://rubricae.com/

TSP Information URI

URI [en] https://rubricae.com/

URI [es] <https://rubricae.com/>

67.1 - Service (granted): Qualified electronic time stamps issued by RUBRICA
QUALIFIED TSU01

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

Service Name

Name [en] *Qualified electronic time stamps issued by RUBRICA QUALIFIED TSU01*

Name [es] *Sellos cualificados de tiempo electrónicos emitidos por RUBRICA QUALIFIED TSU01*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 371376969020492470

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIEHjCCBWKgAwIBAgIIISdlyrW6SrywDQYKoZihvcNAQELBQAwYyxCZAJBgNVBAYTAkVTRiRw
EAYDVOQHDAICXXJZVwvbmExFjAUBGNVBAAQMDVVBTKFUDUNBIFMuO54xFIATBgNVBAsMDFRtUC1V
QUSVEFD0TEaMBGCA1UEAwRVUFI0OVR0Q0EgQDEwMDMeXGDAWBgNVBGEEMD1ZBVEVTLUE2Njcy
MTQ5OTAEfw0yNTA1MTIxMzQwMDNaFw0zMzA1MTIxMzQwMDNaMIGCMQswCQYDVOQGEWJFuzEcMBoG
A1UEBwwTTEFTTIFjPWkFTIERFIE1BRFJRDEpMCCGSA1UECqwgUUVCUKIDOUUgQIVTUSFU1MgU09M
VVRJOSTIEMutCkxTATBgNVBAsMD0VUQjQ0FFIRRTUdEhMBGCA1UEAwwyUUVCUKIDOUUgUUVVB
TEIGSUVEFRVTVAxMRgwFgYDVORhDA9WQVRfUy1CODg1NjQzOTgwggEiMA0GCSCqSib3DOEBAQUA
A4IBDWAwwgEKAoIBAQCWyoWISnSuPXBvCjDDAAApPDI3BMypgNUeA+MKeQsh5+684InjCULF0EEN
hGAnHmJUBBwqg2bbyhuXsm7Juew1UJZ75119MO4Cn5zH1dZCKM6eZORCly8ZRP+ZNSqZuv
EACmWicO24t+C8FIfHxo39+rlGqnY6l7EosmWCqB3e48OxiWYjWzH+5bWmjYl4gZy/0sCDYVtedx
s3NGjavgQLG+/jIHQDicuHUPAhwj1mLKgUY1QmUEPUuruxR8LimgXBuUcpgp5aZD7b0u
mm1QHYWYZLUBK05o2ez1nU7aGgijp34vcBSC+zoav8Xp7wst4qMBAAgpggLENiICwDCB
7QYKwYBBQUHAQEgeAwgd0wawYKwYBBQUHMAKGX2h0dHBzOibvd2VilnVhbmFOYWNhLmNvbS9j
L3Bra59vY3NwL2AdBgNVHQ4EFgQU4t6Hs1eE7DyfmjnP+g/NhBVmWcOYDVR0TBAlwADA/BGwV
H5MEGGAUgBSBzS2NLtatyQZSjyLpYyWvAdAcBgNVHRIEFjA1GrFRpbmZvHhbmFOYWNhLmNw
bTcBkwYDVROgBGLMIGIMHwGCSGAQO08gvE2AgUwbJA6BggRBgEFBOCCAJAuDCXZJ0aWZpY2Fk
bykZSBzZWxsbyBkZS80aWVtcG8gZWxtY3Ryw7NuaWNwLjAwBggrBgEFBQOCARykahR0cHM6Ly93
dScuWfuYXRhY2EuY29l3B1YmtpYy9y9wa2kvY3JsLzlwMjF0ZTfzdlWuY3JsMDYg
aHR0cDovL2NybDEudWfuYXRhY2EuY29l3B1YmtpYy9y9wa2kvY3JsLzlwMjF0ZTfzdlWuY3JsMDYg
OgA4hZodHRwOi8vY3JsM51YW5hdGFjY3Jl3B20vchVbGjL3Bra59jcmwMjF0ZTfzdlWuY3JsMDYg
cmwM2yDVR0PQVBAQOAgEAMyGA1UQEBWQMMAGACCcSAQUBwMMMBGCA1UeODYMBaBFHNV
cg9yGVAcnVicmJfYUuY29MA0GCSCqSib3DOEBCwUAA4ICAQAK6W07dehK9ASABCVyTpiYzS
m0H9vWfokCsRYtKpRvUg6Fhx4XN6/+nzDHSOJq7ZPdCKNmSwRRL9fS8liUlvfSp0a
KlUgK9MmI8wvSlRPa3ja7znRozs9pyrKl4l3eICUEznjw/0aVnPBAMRiCvHNOdW
OcvDk7lSVuoY+RGWNfTgtKmiA2z0Pk4qfBZOVP8lpf3Yg2kpT25NMI0hX3ES753oqijyGE
d7m7nC0emcKvYje5d+W806zoT+T54X0aQKrfOTBtqTLWys9zxGNaooq1Y5AFjBFRW8xmvE5
+Jm5PQ3KMcF7E5G5jY0GUYHhQmTq+L5YVOT1W2TEvubxuDagLeQopKE1Yfaim1Ug
VqShqRYUTs6yGbwWC0sieMVIZ2OIMSt9Usxm2/kv2AS0FTMGvH4eowj2K6GkklndNWtcZQh
nU4g4bx+X/e7hGqQI7Iyp5aWYDZfajNyWwVl3azl08N9B2yo700C0BwUgBF12aBtkIAPwQj+S
YF+HjUUD4mxat5FWFwE9p5uO8Rk0gop4Z2E6pLeedQVUegapFTWnetZV6v4LkMkC0C0gWx8
yv1DU5KTUuau6CnXa5Ya0mDlzcZapK0u0D2o2E6wX/ROYUdA==
-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA1 2021

Issuer OU: TSP-UANATACA

Issuer O: UANATACA S.A.

Issuer L: Barcelona

Issuer C: ES

Subject 2.5.4.97: *VATES-B88564398*

Subject CN: *RUBRICAЕ QUALIFIED TSU01*

Subject OU: *RUBRICAЕ TSP*

Subject O: *RUBRICAЕ BUSINESS SOLUTIONS S.L.*

Subject L: *LAS ROZAS DE MADRID*

Subject C: *ES*

Valid from: *Mon May 12 15:40:03 CEST 2025*

Valid to: *Thu May 12 15:40:03 CEST 2033*

Public Key:
 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:80:CA:85:88:48:DF:6E:3D:75:5B:08:9A:43:0C:00:29:3C:38:87:04:CC:AA:A4
 :D5:04:68:E3:0A:79:0B:21:1E:EE:BC:ED:99:E3:09:C5:05:00:41:0D:84:60:21:26:6A:C9:52:90:70:AA:AD:96:6F:28:6E:17:19:B3:EE:E7:60:D5:72:59:EF:98:85:F4:03:AD:01:C9:FF:E7:31:D
 :8:93:4D:8A:70:A3:7A:7B:63:91:08:8C:BC:65:1F:7E:64:DF:6A:FF:6B:AF:10:00:A6:5A:27:0E:DB:8B:7E:0B:C1:48:7C:7C:68:DF:AB:20:6A:A7:63:A9:7B:12:8B:26:58:2A:81:DD:EE:3C:3B
 :19:56:60:95:B3:1F:EE:5B:5A:68:D8:23:88:19:CB:FD:2C:08:36:15:B5:E7:71:B3:73:46:8E:36:AF:82:82:C6:FF:EA:C9:22:14:03:95:CB:A8:85:43:C0:87:02:75:98:89:06:51:8D:50:9B:FB:84
 :10:F5:22:8A:BB:81:47:C2:E3:98:62:57:07:F8:BE:FE:AA:79:69:90:D3:6F:FD:2E:9B:0D:50:88:75:4C:66:30:B5:BB:A2:B4:4A:8D:9E:CF:59:D4:ED:A4:9F:1A:38:F2:96:99:77:E2:F7:1C:07:9
 :0:BE:CE:8B:E8:6D:78:02:EF:08:07:02:03:01:00:01

Authority Info Access
https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *E2:DE:87:B3:57:84:EC:3C:9F:A6:62:27:8C:A3:FE:A3:F3:61:05:53*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS text: [Certificado de sello de tiempo electrónico.]
CPS pointer: https://www.uanataca.com/public/cps/
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *soporte@rubricae.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint:

62:6C:C5:7D:B4:63:56:30:03:A4:28:F6:A8:4E:38:18:77:63:84:82:DC:82:3F:B4:4F:53:F6:49:5D:4F:06:6D

X509SubjectName**Subject 2.5.4.97:**

VATES-B88564398

Subject CN:

RUBRICAЕ QUALIFIED TSU01

Subject OU:

RUBRICAЕ TSP

Subject O:

RUBRICAЕ BUSINESS SOLUTIONS S.L.

Subject L:

LAS ROZAS DE MADRID

Subject C:

ES

X509SKI**X509 SK I**

4t6Hs1eE7DyfpmlnjKP+o/NhBVM=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2025-11-19T00:00:00Z

68 - TSP: ZERTIBAN S.L.U.**TSP Name**

Name *[en]* *ZERTIBAN S.L.U.*

Name *[es]* *ZERTIBAN S.L.U.*

TSP Trade Name

Name *[en]* *ZERTIBAN*

Name *[es]* *ZERTIBAN*

Name *[en]* *VATES-B02703577*

PostalAddress

Street Address *[en]* *Plaza de España 12. Planta 1, oficinas A y B*

Locality *[en]* *Madrid*

State Or Province *[en]* *Madrid*

Postal Code *[en]* *28008*

Country Name *[en]* *ES*

PostalAddress

Street Address *[es]* *Plaza de España 12. Planta 1, oficinas A y B*

Locality *[es]* *Madrid*

State Or Province *[es]* *Madrid*

Postal Code *[es]* *28008*

Country Name *[es]* *ES*

ElectronicAddress

URI *[en]* *mailto:proveedores@zertiban.com*

URI *[en]* *https://zertiban.com*

TSP Information URI

URI *[en]* *https://zertiban.com*

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description	<i>[en]</i>	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	<i>[es]</i>	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>

Name	[en]	Qualified electronic time stamps issued by ZERTIBAN QUALIFIED TSU01

Name [es] *Sellos cualificados de tiempo electrónicos emitidos por ZERTIBAN*
QUALIFIED TSU01

Version: 3

Serial Number: 5051373642633312460

-----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *VATES-A66721499*

Issuer CN: UANATACA CA1 2021

Issuer OU: *TSP-UANATACA*

Issuer O: UANATACA S.A.

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B02703577*

Subject CN: *ZERTIBAN QUALIFIED TSU01*

Subject OU: *ZERTIBAN TSP*

Subject O: *ZERTIBAN S.L.U.*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Mon May 12 12:06:42 CEST 2025*

Valid to: *Thu May 12 12:06:42 CEST 2033*

Public Key:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CF:32:27:8E:A4:C6:E4:37:63:FF:BC:C6:9B:4B:F9:75:49:91:BF:B5:FB:55:4B:F
2:5B:5C:E7:6E:03:0A:50:8D:B2:8B:E6:DC:BE:49:6C:E3:52:85:0D:BA:47:8D:95:83:3E:BA:55:D0:8F:EE:54:47:1B:09:AE:29:23:E2:8F:F3:CD:52:C7:80:31:49:89:CA:57:27:CC:A4:8E:F9:CF:
B2:95:37:99:3D:15:CD:BA:6E:C4:85:7F:65:52:01:DC:3A:3D:19:E7:80:ED:9B:53:84:00:D6:BC:75:FF:FB:22:CB:37:EB:6C:23:C6:70:89:2A:DF:5D:A9:66:6B:EF:CF:64:75:CC:3A:EE:43:CE:B
3:74:A0:0A:CE:F8:2E:10:95:D3:4C:4B:FC:A3:97:90:3C:6D:C9:24:2C:F0:2B:61:2C:5A:38:1D:9C:51:C6:2A:E5:FC:AA:BB:6E:47:9A:DA:5E:FE:8B:F9:DF:3F:95:9F:76:D8:11:12:8A:4A:9A:04
:6A:3F:27:66:4F:FA:F3:F2:64:62:0A:7A:84:B3:02:03:5D:DB:EF:E3:CF:0E:0A:6E:22:A9:F9:9B:A5:75:C5:87:95:56:00:50:5F:47:70:C7:B1:C7:F1:39:F7:B6:08:3B:53:C0:73:13:EF:97:35:BB
:23:E1:FA:FC:6F:FF:D8:14:2F:2F:02:03:01:00:01

Authority Info Access
https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer
<http://ocsp1.uanataca.com/public/pki/ocsp/>
<http://ocsp2.uanataca.com/public/pki/ocsp/>

Subject Key Identifier *43:B5:9B:79:E4:7B:4A:57:F9:C2:E9:8C:55:23:23:2B:5F:DC:3F:11*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies
Policy OID: 1.3.6.1.4.1.47286.2.5
CPS pointer: <https://www.uanataca.com/public/cps/>
CPS text: [Certificado de sello de tiempo electrónico.]

Policy OID: 0.4.0.2042.1.2

CRL Distribution Points
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *proveedores@zertiban.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint:

*F1:CD:A3:A2:DA:D3:AE:4B:8E:94:65:6C:AC:51:20:78:75:0B:FA:D6:44:9F:21:23:D
1:6E:7B:A5:31:02:B5:5D*

X509SubjectName**Subject 2.5.4.97:**

VATES-B02703577

Subject CN:

ZERTIBAN QUALIFIED TSU01

Subject OU:

ZERTIBAN TSP

Subject O:

ZERTIBAN S.L.U.

Subject L:

MADRID

Subject C:

ES

X509SKI**X509 SK I**

Q7WbeeR7SIf5wumMVSMjK1/cPxE=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description *[en]*

undefined.

[es]

undefined.

Status Starting Time

2025-11-19T00:00:00Z

69 - TSP: FIRMAFY SOLUCIONES TECNOLOGICAS SL

TSP Name

Name [en] *FIRMAFY SOLUCIONES TECNOLOGICAS SL*

Name [es] *FIRMAFY SOLUCIONES TECNOLOGICAS SL*

TSP Trade Name

Name [en] *FIRMAFY*

Name [es] *FIRMAFY*

Name [en] *VATES-B19681642*

Name [en] *Firmafy Soluciones Tecnológicas SL*

PostalAddress

Street Address [en] *C/ Ciego de Arjona 2, Bajo*

Locality [en] *Granada*

State Or Province [en] *Granada*

Postal Code [en] *18012*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/ Ciego de Arjona 2, Bajo*

Locality [es] *Granada*

State Or Province [es] *Granada*

Postal Code [es] *18012*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:hola@firmafy.com*

URI [en] *https://firmafy.com/*

TSP Information URI

Page 1603

Issuer OU:	<i>TSP-FIRMAFY</i>
Issuer CN:	<i>Firmafy CA ROOT</i>
Subject C:	<i>ES</i>
Subject L:	<i>Granada</i>
Subject O:	<i>Firmafy Soluciones Tecnológicas SL</i>
Subject 2.5.4.97:	<i>VATES-B19681642</i>
Subject OU:	<i>TSP-FIRMAFY</i>
Subject CN:	<i>Firmafy CA Subordinada 01</i>
Valid from:	<i>Mon Mar 06 14:10:12 CET 2023</i>
Valid to:	<i>Fri Mar 05 14:10:12 CET 2038</i>
Public Key:	<pre> 30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CE:A1:DA:B8:D8:20:02:4A:D9:23:C5:3F:A0:CB:7C:AD:70:3E:83:42:D8:A2:E E:6E:B1:C4:CB:A7:8F:53:BC:19:64:AA:D9:87:EB:B4:8E:AC:DC:63:6C:46:FD:72:37:3C:15:08:C5:02:81:B4:2F:29:EF:3D:89:F3:AB:D6:83:92:22:65:25:61:82:49:45:32:48:AB:E5:76:17:C3 :71:A2:53:8E:34:CB:1C:08:D8:7C:EB:22:D3:8D:66:83:C4:87:CC:D3:94:00:89:58:86:E9:EB:8B:36:0D:58:6C:25:D8:43:53:27:A6:41:A3:EC:38:A1:11:4F:55:15:38:19:80:05:67:31:8A:B7: EC:6D:61:89:90:58:61:80:00:E7:24:14:F9:42:DD:23:58:FD:5D:EB:6B:FC:4A:91:90:F3:62:79:FE:D8:68:D4:C3:69:D5:85:AB:F1:0D:B0:31:F2:9C:FE:40:F7:97:83:7A:72:08:38:C5:41:97:C D:DA:5C:ED:9A:38:BD:14:1C:51:AC:FD:06:F4:1C:C8:D0:78:55:25:37:97:59:8D:C0:59:38:19:0E:D3:48:A1:51:62:96:A9:7F:CF:2E:41:29:20:48:77:07:98:48:40:E4:42:3E:28:CE:5D:1A:BA :42:61:57:C8:E0:F4:EF:92:C2:7B:45:E5:E2:6D:DC:5E:E8:25:7E:D2:78:18:94:EE:00:C7:88:41:17:FD:81:54:9D:B1:74:54:8D:B4:D7:33:1D:43:57:A2:8C:C0:D4:76:FA:DA:F0:46:50:E4:6A:F 2:BE:7E:E9:23:C8:BA:F7:E8:68:9E:F6:C0:4C:D7:32:06:7C:A5:A4:A2:A9:E6:F2:46:41:3A:27:2C:6D:E9:97:3E:55:1F:C5:89:5E:88:73:8D:AF:E3:46:A4:F0:F2:14:22:10:EE:ED:73:7A:16: EB:FD:12:8A:E7:84:83:64:2D:ED:87:0B:E4:5F:D4:44:7D:AB:3C:F1:6C:68:9B:7A:F2:BC:08:67:E7:8A:12:D7:3E:E1:70:20:44:94:7B:D3:66:44:4F:0E:DF:1A:E0:CE:0F:21:33:71:2E:27:56:6 4:25:C8:59:60:DD:80:D7:D0:8F:17:91:4E:80:24:59:D0:8C:F0:3D:14:7B:06:8B:5E:75:D7:43:FE:88:83:B4:1C:CD:14:89:B2:74:D9:28:F4:5D:E1:AB:D4:4E:0A:02:71:FB:97:BF:3B:03:89:83 :55:18:2A:CD:FE:BD:89:D7:88:4D:D9:C8:9D:2A:27:AA:37:41:B6:1E:A1:2A:83:65:BE:DB:E1:12:67:A3:89:CD:E9:20:4B:05:EF:9F:7C:E9:4B:10:C3:38:0A:A5:02:03:01:00:01 </pre>
Basic Constraints	<i>IsCA: true</i>
Authority Key Identifier	<i>FA:F4:02:89:47:6F:DE:FF:76:7D:5A:46:08:64:4C:B3:F6:1D:78:42</i>
Authority Info Access	http://ocsp1.modernpki.com/public/pki/ocsp/ http://ocsp2.modernpki.com/public/pki/ocsp/
Subject Alternative Name	<i>soporte@firmafy.com</i>
Certificate Policies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS text: [Certificado de la Autoridad de Certificación Subordinada de Firmafy - https://www.firmafy.com]</i> <i>CPS pointer: https://www.firmafy.com/public/cps</i>
CRL Distribution Points	http://crl1.modernpki.com/tsp/crl/arl_firmafy.crl http://crl2.modernpki.com/tsp/crl/arl_firmafy.crl
Subject Key Identifier	<i>94:25:61:CE:E5:85:00:82:39:90:58:6B:52:0D:63:47:7A:11:BC:A5</i>
Key Usage:	<i>keyCertSign - cRLSign</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>0E:04:3B:CC:C0:E9:DD:77:8A:1D:24:13:69:EC:5F:64:5B:D8:9A:53:6F:0E:B8:D9:A 2:4E:E3:C9:33:51:84:4E</i>

X509SubjectName

Subject C: *ES*

Subject L: *Granada*

Subject O: *Firmafy Soluciones Tecnológicas SL*

Subject 2.5.4.97: *VATES-B19681642*

Subject OU: *TSP-FIRMAFY*

Subject CN: *Firmafy CA Subordinada 01*

X509SKI

X509 SK I *ICVhzuWFAII5kFhrUg1jR3oRvKU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description [en] *undefined.*

[es] *undefined.*

Status Starting Time

2025-11-19T00:00:00Z

69.1.1 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

69.1.2 - Extension (critical): additionalServiceInformation**AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

69.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=atLeastOne**Policy Identifier:**

Identifier [OIDA sURN] *urn:oid:1.3.6.1.4.1.59806.1.1.3*

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.59806.1.2.3

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.59806.1.3.3

Description**Policy Identifier:**

Identifier [OIDsURN] urn:oid:1.3.6.1.4.1.59806.1.4.3

Description**Description**

69.2 - Service (granted): Qualified electronic time stamps issued by FIRMAFY QUALIFIED TSU01

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified electronic time stamps issued by FIRMAFY QUALIFIED TSU01

Name [es] Sellos electrónicos cualificados de tiempo emitidos por FIRMAFY QUALIFIED TSU01

Service digital identities**Certificate fields details**

Version: 3

Serial Number: 4040831636407677868

X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIHhGCCBWiGAWiBAgII0BPa9s09c6wwDOYJKoZihvcNAQELBQAwgaExijAgBqNVBAMMGUzDcm1h
ZnkqOQEqU3Vib3JkaWShZGEGMDExFDASBgNVBAsMc1RTUC1GSVINOuZzMRqWfgYDVORHDA9WQVRf
Uy1CMTk2ODEZNDkxLDA4BgNVBAsMOzZpcmlhZnkqU28sWmhpLz5icyBZWub2Ds2dp1ZfFfNM
MBAwDgYDVOQHDAHcmFyUWRhM0swCOYDVOQGEWJFuzAeFw0YjTA1MTIxMzA2NTIaIw0cMzA1MTIx
MzA2NTIaMIGqMSAwHgYDVOQDDBqGcSVINOuZzIffVQLXrkFRCBUu1UwMTEUMBGAIUECwWLFNQ
LUZJUK1BRkxkDAWBgNVBGEtODI2BVEVTLUxOTY4MTY0MEsGA1UEGWIxUjFwYXNjaW50YXNjaW50
QDFlTKYtFRFQ05PTMOTR0ID0VmaU0wMRAwDgYDVOQHDAHUKFOURBM0swCOYDVOQGEWJFuzCC
ASlWDOYJKoZihvcNAOEbBQADgEPADCCAQocggEBALhqvBz5y4iITC1cFsvn8sf4w4DS/Gizny
kqzKveKhlWIMhsa2lx8PLHNZjsEd7xPKF78UYkuef5u7vEH905T5MGtNj2mbEC3kyUjXIMMh
Wlebxp8brlpjZ/VE+DYS0AL9vz9pP+8QIAr6RXkpjhMIEYka7k+ssYx4mOKRzTm+HHQjbxRrWw
rCe+1/23Pfw6XULsi7B0rNirar05MIWWgp+HDjhioMGB3ixGULeZ3+2KsBso0Fed9a9retaa
HDlqY7Hb3oZPcbt7Qw1hIhOCCWdcFsa9j6uJf5a9j000LS9BE3H+MF7+9168eU2WHdZLA2Zgl
GEECAWEAAaOArkwgK1MAwGA1UdeWEbWOCMAAwHwYDVDR0BBgwFoAUCVnzWFAI5KfHrUq1j
R3oRvKlWgqOGCCsGAOUFBwEBBIIHMHMEFAGCCsGAOUFBzAChkRodHrW0i8vZmlybWFmeS5jb2V
chVibGJlZ2Vud25sd2FkL3RazF9jZX0aWZpY2FOZMvC+3Vib3JkaWShGULmMydDA3BggB8Gf
B0CwAYYraHR0cDovL29jc3A1Ln1VZGVyb2Bras5jb20vchVibGJlL3BraS9vY3NwLzA3BggB8Gf
B0CwAYYraHR0cDovL29jc3A1Ln1VZGVyb2Bras5jb20vchVibGJlL3BraS9vY3NwLzA3BggB8Gf
F2aYvRkzb3BvcnRlOGZpcmlhZnkqU28sWmhpLz5icyBZWub2Ds2dp1ZfFfNM
LgYkYwYBBQUHAgEWMh0dHbzOibvd3d3LmZpcmlhZnkqU28sWmhpLz5icyBZWub2Ds2dp1ZfFfNM
AgilWBSWAEMAZOBzYAHQAAOBMAgkAYwBhAGQAbwAgAGQAZQAgAHMAZOBzYAGwAbwAgAGQAZQAgAHQAA
aOBIAgACABwACAAZOBzYAHQAAOBMAgkAYwBhAGQAbwAgAGQAZQAgAHMAZOBzYAGwAbwAgAGQAZQAgAHQAA
GCCsGAOUFBwMIMIGIBGqNVHR8EqYAwfA9oDugOYY3aHR0cDovL2NybDeubW9kZXJucGtLmNvds9w
dWJsaWVmcGtL2NybDc9maXtYWZ5O0EKLmNvds9wDugOYY3aHR0cDovL2NybDlulbW9kZXJucGtL
LmNvds9wWJsaWVmcGtL2NybDc9maXtYWZ5O0EKLmNvds9wDadBgNVH4EFQlUjZjZ3RCRjZ3QE
eyY3DzZlqlAwDgYDVR0PAQH/BAQDAgeAMAGCCsqG5L3DOECWUAA4CAQALxNgFDBBxLn9M0M/h
1+MhgRppKxpUfElcmQEzvsEPi6Killy2KDFmth1KIKO4xrxDAQEqMU01WXI+JOnZcbXpva4m+
WTLSunDXh0anyUjXKMB8jppcmQ95Yb7I3A17f1Ubd++wTihYIvc++n+NelykNizj39ba4Xc
H1jkwPFCtWaWvXcKTPsPpG5Le6xpp4yUmZ1jB7Xy67j5JW1+B+3BjMx4CmxUj8Clt001Gtf
CBwcbQEFIPaobCZhxDRK7PAObfwkZeSZC12ZnkN0QrZSw4+EEFoljArBSTpP056LK+A+gcCgkn
jwshD8B8ECUWB0T3e5TPymwgyGzZeeP9g8mCpuyt+JfREubRMSfOIRuzMy5FS+caa0w
79NHZvtzlgsp2H7CuF1jQvmKmOK5t585mxuJHUOH6YF53OETuGBFZK1XOKP4H5AvGqdPKH04
+6aBjlaOB0WjOhM3yw+IADh7kyEFB+L4XQs8FikNMeUWM0BVMcaGLO5CcG7FfUKshSxwgidfh1w
vYLqE2L08g9a9g8YcKKNB9ePc1A5VLK5hTAgx07TA9tttRTrIojYf
cQayGFz+hdmp5KTXswfQarf9jWRZD7StQTrQ7vjZHQ7JA1ZCOAWMByK78A==

```

-----END CERTIFICATE-----

Signature algorithm:*SHA256withRSA***Issuer C:***ES***Issuer L:***Granada***Issuer O:***Firmafy Soluciones Tecnológicas SL***Issuer 2.5.4.97:***VATES-B19681642***Issuer OU:***TSP-FIRMAFY***Issuer CN:***Firmafy CA Subordinada 01***Subject C:***ES***Subject L:***GRANADA***Subject O:***FIRMAFY SOLUCIONES TECNOLÓGICAS SL.***Subject 2.5.4.97:***VATES-B19681642***Subject OU:***TSP-FIRMAFY***Subject CN:***FIRMAFY QUALIFIED TSU01***Valid from:***Mon May 12 15:06:52 CEST 2025***Valid to:***Thu May 12 15:06:52 CEST 2033***Public Key:**

```

30:82:01:22:30:00:06:09:24:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:04:02:82:01:01:00:B8:6A:BC:1C:D2:CB:82:22:7D:00:85:70:58:2F:9F:CB:18:7F:8C:38:0D:2F:C6
:8F:39:F2:92:AD:B1:55:E6:CA:85:69:4C:1E:C6:B6:97:1F:0F:2C:73:59:26:C9:04:77:BC:4F:28:5E:FA:51:88:E4:B9:E1:79:BB:BB:C4:1F:D7:F4:E5:3E:4C:1A:B3:68:27:69:9B:10:2E:64:C9:49
:57:32:53:0D:5A:27:9B:5E:9F:1B:AC:9A:49:97:F5:44:F8:36:12:00:02:FD:CA:3C:FD:A4:FF:BC:42:20:2B:E9:15:E4:83:18:E1:32:21:18:91:AE:E4:FA:CB:18:C7:89:BE:92:85:D3:9B:E1:C7:4
2:36:D7:AE:85:BD:AC:27:BE:D7:FC:F7:3C:97:F0:E9:78:8B:82:27:FC:42:83:63:AD:AA:CE:E4:C9:56:5A:04:7E:1C:3B:E1:6E:2A:0C:18:1D:E2:CD:71:AE:2F:79:0F:ED:8A:8D:14:AB:D0:5
7:9D:F5:AF:6B:7A:D6:9A:1C:32:2A:57:BB:41:DE:96:4F:71:82:2D:EC:EC:35:86:13:82:09:67:5C:0C:FA:A4:6B:A6:C9:15:26:85:F2:3D:34:D0:B4:8F:FC:11:37:21:FF:8C:17:BF:BD:27:AF:1E:
53:65:87:0F:32:C0:75:98:08:18:41:02:03:01:00:01

```

Basic Constraints*IsCA: false***Authority Key Identifier***94:25:61:CE:E5:85:00:82:39:90:58:6B:52:0D:63:47:7A:11:BC:A5*

Authority Info Access	http://firmafy.com/public/download/tsp_certificates/subordinate1.crt http://ocsp1.modernpki.com/public/pki/ocsp/ http://ocsp2.modernpki.com/public/pki/ocsp/
Subject Alternative Name	<i>soporte@firmafy.com</i>
Certificate Policies	<i>Policy OID: 1.3.6.1.4.1.59806.2.1</i> <i>CPS pointer: https://www.firmafy.com/public/cps</i> <i>CPS text: [Certificado de sello de tiempo electrónico.]</i> <i>Policy OID: 0.4.0.2042.1.2</i>
Extended Key Usage	<i>id_kp_timeStamping</i>
CRL Distribution Points	http://crl1.modernpki.com/public/pki/crl/firmafyCA1.crl http://crl2.modernpki.com/public/pki/crl/firmafyCA1.crl
Subject Key Identifier	<i>E8:9B:B6:8B:6D:D1:0A:28:9F:8F:74:04:7B:16:37:0E:86:49:AA:10</i>
Key Usage:	<i>digitalSignature</i>
Thumbprint algorithm:	<i>SHA-256</i>
Thumbprint:	<i>E6:17:5E:B6:39:7C:0A:28:8E:15:4A:BC:ED:64:DB:02:2E:8C:FE:53:C9:59:6F:F9:57:A9:0B:F8:1C:9A:A3:A7</i>

X509SubjectName

Subject C:	<i>ES</i>
Subject L:	<i>GRANADA</i>
Subject O:	<i>FIRMAFY SOLUCIONES TECNOLÓGICAS SL.</i>
Subject 2.5.4.97:	<i>VATES-B19681642</i>
Subject OU:	<i>TSP-FIRMAFY</i>
Subject CN:	<i>FIRMAFY QUALIFIED TSU01</i>

X509SKI

X509 SK I	<i>6Ju2i23RCiifj3QEexY3DoZJqhA=</i>

Service Status

Service status description	<i>[en] undefined.</i>
	<i>[es] undefined.</i>

Status Starting Time	<i>2025-11-19T00:00:00Z</i>

70 - TSP: BACKUP FILE, S.L.**TSP Name**

Name [en] *BACKUP FILE, S.L.*

Name [es] *BACKUP FILE, S.L.*

TSP Trade Name

Name [en] *GRUPO BACKUP*

Name [es] *GRUPO BACKUP*

Name [en] *VATES-B80067051*

PostalAddress

Street Address [en] *C/Julián Camarillo 26, Muelle C-D Planta 2 Nave 7*

Locality [en] *Madrid*

State Or Province [en] *Madrid*

Postal Code [en] *28037*

Country Name [en] *ES*

PostalAddress

Street Address [es] *C/Julián Camarillo 26, Muelle C-D Planta 2 Nave 7*

Locality [es] *Madrid*

State Or Province [es] *Madrid*

Postal Code [es] *28037*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:administracion@grupobackup.com*

URI [en] *https://www.grupobackup.com/*

TSP Information URI

URI [en] *https://www.grupobackup.com/*

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en]

A time-stamping generation service creating and signing qualified time-stamps tokens.

[es]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Name [en]

Qualified electronic time stamps issued by GRUPO BACKUP QUALIFIED
TSU01

Name *[es]*

Sellos cualificados de tiempo electrónicos emitidos por GRUPO BACKUP
QUALIFIED TSU01

Certificate fields details

Version: 3

Serial Number: 2333835448697961172

X509 Certificate -----BEGIN CERTIFICATE-----

[illegible]

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: VATES-A66721499

Issuer CN: UANATACA CA1 2021

Issuer OU: *TSP-UANATACA*

Issuer 0: UANATACA S.A.

Issuer L: *Barcelona*

Issuer C: *ES*

Subject 2.5.4.97: *VATES-B80067051*

Subject CN: *GRUPO BACKUP QUALIFIED TSU01*

Subject OU: *GRUPO BACKUP TSP*

Subject O: *BACKUP FILE, S.L.*

Subject L: *MADRID*

Subject C: *ES*

Valid from: *Mon May 12 13:01:11 CEST 2025*

Valid to: *Sat May 14 13:01:11 CEST 2033*

Public Key: *30:82:01:22:30:00:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B6:0F:52:FE:FF:AB:32:CC:D0:DA:1C:C8:FA:AD:57:FE:CE:41:87:ED:EC:98:3A:AD:27:30:EC:5B:8E:62:E7:47:A0:FD:95:79:48:25:F5:93:8F:84:19:30:1F:1D:22:EF:70:92:3B:24:F8:3F:10:89:52:08:40:E9:BB:BF:5F:A7:3F:85:0D:1B:1A:2A:64:D3:6C:17:81:14:86:85:2D:D3:4E:9E:CD:94:66:1C:EC:F5:99:42:35:EF:59:66:59:21:F9:7B:64:50:1B:EF:92:96:18:BB:C7:B0:EA:53:65:8E:0C:52:F9:5A:C7:AB:97:6D:50:0E:81:EA:A2:75:74:E1:DA:C4:EB:D1:76:E:C7:63:FC:D5:E9:84:05:FD:D8:56:7B:E7:44:F7:66:2A:F8:A0:44:10:4D:BB:C5:EE:49:24:66:F2:7C:28:51:DB:34:76:A9:14:EF:6D:BB:C1:8C:5F:40:6D:50:79:43:CC:A3:5F:EE:7E:5A:28:76:1F:AB:73:04:92:9F:CD:04:12:3C:D9:C7:BF:A3:CE:BE:99:91:95:D2:9E:AF:1D:09:15:51:47:1B:AA:29:6E:47:68:19:50:1F:88:7E:85:86:B3:30:3B:14:AE:C0:02:69:CF:99:51:8B:EE:38:0D:34:25:4B:24:8F:AD:DE:23:90:00:3B:02:03:01:00:01*

Authority Info Access *https://web.uanataca.com/common/project/pdf/autoridad-certificacion/07_subordinada-ca1-2021.cer*
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier *05:7F:DF:61:8F:67:BD:05:6F:4F:8A:3C:B4:46:22:91:53:0C:86:B3*

Basic Constraints *IsCA: false*

Authority Key Identifier *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

Issuer Alternative Name *info@uanataca.com*

Certificate Policies *Policy OID: 1.3.6.1.4.1.47286.2.5*
CPS pointer: https://www.uanataca.com/public/cps/
CPS text: [Certificado de sello de tiempo electrónico.]
Policy OID: 0.4.0.2042.1.2

CRL Distribution Points *http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*
http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

Extended Key Usage *id_kp_timeStamping*

Subject Alternative Name *sistemas@grupobackup.com*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint:

3C:6F:AB:3C:48:58:7A:D9:05:29:7F:31:92:F8:62:27:64:C6:9B:8E:49:B5:64:94:F8
:DD:B4:CD:69:15:22:08

X509SubjectName**Subject 2.5.4.97:**

VATES-B80067051

Subject CN:

GRUPO BACKUP QUALIFIED TSU01

Subject OU:

GRUPO BACKUP TSP

Subject O:

BACKUP FILE, S.L.

Subject L:

MADRID

Subject C:

ES

X509SKI**X509 SK I**

BX/fYY9nvQVvT4o8tEYikVMMhrM=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en]

undefined.

[es]

undefined.

Status Starting Time

2025-12-18T00:00:00Z

71 - TSP: VIAVANSI CORPORACIÓN, S.L.**TSP Name**

Name [en] *VIAVANSI CORPORACIÓN, S.L.*

Name [es] *VIAVANSI CORPORACIÓN, S.L.*

TSP Trade Name

Name [en] *VIAFIRMA*

Name [es] *VIAFIRMA*

Name [en] *VIAVANSI CORPORACION SOCIEDAD LIMITADA*

Name [en] *VATES-B56255151*

PostalAddress

Street Address [en] *GLORIETA FERNANDO QUIÑONES, S/N. EDIFICIO CENTRIS, BAJO, 3B*

Locality [en] *Tomares*

State Or Province [en] *Sevilla*

Postal Code [en] *41940*

Country Name [en] *ES*

PostalAddress

Street Address [es] *GLORIETA FERNANDO QUIÑONES, S/N. EDIFICIO CENTRIS, BAJO, 3B*

Locality [es] *Tomares*

State Or Province [es] *Sevilla*

Postal Code [es] *41940*

Country Name [es] *ES*

ElectronicAddress

URI [en] *mailto:psc@viavansi.com*

URI [en] *https://www.viavansi.com*

TSP Information URI

Subject CN: *VIAFIRMA TSA 007*
Subject OU: *VIAVANSI QTSP*
Subject O: *VIAVANSI CORPORACION SOCIEDAD LIMITADA*
Subject C: *ES*
Valid from: *Tue Nov 18 12:11:30 CET 2025*
Valid to: *Tue Nov 19 12:11:30 CET 2030*
Public Key: *30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:89:F0:7D:77:7E:72:A6:F5:D3:4A:E4:59:7E:38:55:BA:19:08:2E:8B:5E:8C:50:CA:34:66:6A:E3:5C:C4:66:64:5E:87:4B:D9:AA:71:53:5B:03:60:8E:5D:CD:58:5F:C2:8C:F9:9E:F6:F9:82:96:88:1B:FF:F9:34:61:66:8D:25:54:E0:5F:0C:D3:1E:4E:13:2B:61:6D:9A:3D:1E:28:D4:86:8A:B5:B1:7A:60:AA:AE:82:B4:85:DE:A2:4F:B2:C0:5F:2E:AB:95:D2:58:25:C0:29:0E:27:4D:D4:E7:A5:F4:7A:89:F8:A3:14:87:66:6F:34:18:BE:03:3B:7C:B9:88:84:4E:06:DC:2C:0E:0F:D4:5A:F3:27:8F:E2:3E:53:D0:21:DA:09:C5:61:A7:3A:F1:F2:40:56:23:A9:86:31:41:F5:80:C3:DD:D5:77:AC:34:98:F3:6E:D0:EB:BE:3D:2C:39:C6:1C:43:1C:E1:03:B5:C2:35:1A:CA:E7:13:6A:37:DA:3B:7C:6A:C2:28:76:86:D2:36:47:66:3F:7A:A5:0F:98:67:EF:A7:36:95:9A:E3:19:1E:13:86:75:A5:35:D1:D5:88:AD:DD:E3:5A:E5:95:E7:D5:F0:3A:0B:E5:E3:14:F3:63:10:FE:E5:02:73:F0:4A:9E:E9:C2:B1:85:01:42:8E:FC:9F:7C:17:3C:EF:FD:60:88:E5:F0:C9:E8:AC:FF:F3:25:FA:C3:17:89:03:CD:BA:69:9A:20:AC:2A:AA:16:F5:80:F1:C1:55:7F:1F:1D:58:69:C8:8C:9D:11:FF:1E:6F:63:3D:B1:64:48:B2:13:17:97:00:7F:94:60:BC:86:2C:F3:59:86:93:7B:D9:34:3C:AC:78:58:75:30:77:D8:ED:5A:C7:46:34:A2:D3:D5:0D:58:CA:9F:5D:3E:0A:C8:E2:DD:57:D7:C0:82:16:C7:0B:A5:69:52:EC:39:A2:84:F9:67:6A:3F:D3:B1:36:03:33:C8:81:A5:DA:4A:25:F2:06:DF:7C:1E:59:03:4D:8E:62:F1:F8:51:E7:01:83:B9:E3:5A:E3:C7:9D:F4:59:9A:31:35:68:87:69:98:7C:1F:4A:44:2F:36:DA:D6:8C:FA:A1:0B:27:E9:D1:33:57:A1:4C:DF:79:8D:4D:D5:F3:7A:B7:BF:E7:6B:2B:2F:0C:99:08:3D:A8:65:B5:73:56:EA:C7:33:19:C7:11:50:E5:2F:69:1F:0D:E5:DA:78:29:02:18:AE:23:93:D3:75:24:3B:8E:A2:B5:6D:41:7D:BF:92:A2:E9:4E:E7:9B:27:A7:CF:88:35:B4:55:67:B9:63:EE:8B:BC:80:2B:AB:B1:E4:09:02:03:01:00:01*
Authority Info Access *http://qtsp.viafirma.com/tsp/subca.crt*
http://qtsp.viafirma.com/ocsp
Subject Key Identifier *25:F8:8A:5D:3F:75:08:0F:E0:EC:BA:87:18:77:7E:52:7C:FF:DC:67*
Basic Constraints *IsCA: false*
Authority Key Identifier *4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26*
Certificate Policies *Policy OID: 1.3.6.1.4.1.34253.8.1*
CPS pointer: http://qtsp.viafirma.com/cps
CRL Distribution Points *http://qtsp.viafirma.com/tsp/tsa_subca.crl*
http://qtsp1.viafirma.com/tsp/tsa_subca.crl
Extended Key Usage *id_kp_timeStamping*
Key Usage: *digitalSignature - nonRepudiation*
Thumbprint algorithm: *SHA-256*
Thumbprint: *2C:73:6F:3A:FC:8C:D2:28:E7:8A:91:3B:DF:31:A9:CB:E7:C5:2C:F4:63:63:ED:50:B5:C1:99:B8:D5:C3:81:3F*

X509SubjectName

Subject 2.5.4.97: *VATES-B56255151*
Subject CN: *VIAFIRMA TSA 007*
Subject OU: *VIAVANSI QTSP*
Subject O: *VIAVANSI CORPORACION SOCIEDAD LIMITADA*

Subject C:	ES
X509SKI	
X509 SK I	JfiKXT91CA/g7LqHGHd+Unz/3Gc=
Service Status	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Service status description	[en] undefined.
	[es] undefined.
Status Starting Time	2026-05-20T03:00:00Z

TSL Scheme Operator certificate fields details

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIYEZCCA9CAwIwAgBlJAloYRYVltz
GAIfKZ0XhFNAQEMISMGWC6SFAIA
UkgT0YgUPT9XNlSMGQUZGQJISJE
AwwdL1JBtKtF3CBUIVtVCBT0QH0h
MTAE0DQZw3M3QsqwCOYDVOOGEgE
QUSJyGBK7KtF5YVSt6CtW939G
QOhTtUgT1BfUKFUT1IwggIIADAQo
EW8r7YbcY0OEENtCwG939G
XZ0BlySpXQZkXlUptF5MkaUEBXZ
UwD5wScF9schL9owI7M5spPqVOVU
nuY5Z3BPtR0T0Uy6SPKnm5cSkE
oZD0wLmZu9Y0lhXscQUS6U0+D
a5QZkVPiPCIO0s066gssQ6TcW12
26DlUclnad+Iw7mPHEHfVW7yqk
0mZl0VED0M3MhIEZVgIFmHwXs
N4f0cCS04rHdI6P3e82bSH5Ymk0
B2NMHARMAA4A4A31Ud0EwEwEwE
AR0lBAOWCAqBACRlNwMADmgCSQ
AQEMISMGWC6SFAIAwGCAQAGAg
93DRtAveZmbD0Zhx7tBPAm3be0
mZT0Zbz5013lDm5spghgKZryg
csE2Q949pCnB6U7p8Kx34JA
qW9h8MHd0E4T5FZM9ToqZ5DXtY
Ptbj8DL0REbK53Gp8bHwPBL9p
rb9QCGUg1pAqE977LLe39p9p9
jhpK6Z0X7CFFAUAd3UsBjPK6s0s
YjpydJ5Y0EWwrdlDmpPw21RAt0Ad
4YwUyV0CgRlR1GUTtEFAwGCAQ
-----END CERTIFICATE-----
```

Subject C: *ES*

Valid from: Tue Oct 31 11:38:46 CET 2023

Valid to: *Sun Oct 29 11:38:46 CET 2028*

[illegible]

Basic Constraints *IsCA: false*

Subject Key Identifier 2A:0E:A3:0B:61:C8:FD:B8:71:D4:CE:03:CB:1E:57:EB:54:BA:26:CA

Extended Key Usage	<i>id-tsl-kp-tslSigning</i>

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *18:0C:D5:36:DA:D2:B5:AC:93:32:36:D9:DC:D5:5D:17:AF:CD:99:49:FE:D0:81:89:
B8:AE:86:FE:7C:2B:C3:A7*