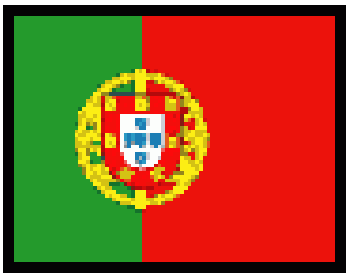

PORTUGAL (PORTUGAL) : Trusted List

Tsl Id: TrustServiceStatusList

Valid until nextUpdate value: 2027-01-01T12:00:07Z

TSL signed on: 2026-07-01T11:11:43Z

PDF generated on: Wed Jul 01 13:14:19 CEST 2026

TSL Scheme Information

TSL Id	*TrustServiceStatusList*
TSLTag	*http://uri.etsi.org/19612/TSLTag*
TSL Version Identifier	*6*
TSL Sequence Number	*114*
TSL Type	*http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric*

Scheme Operator Name

Name	*[en]*	*Gabinete Nacional de Segurança*
Name	*[pt]*	*Gabinete Nacional de Segurança*

PostalAddress

Street Address	*[en]*	*Rua da Junqueira, 69*
Locality	*[en]*	*Lisbon*
State Or Province	*[en]*	*Lisbon*
Postal Code	*[en]*	*1300-342 Lisboa*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Rua da Junqueira, 69*
Locality	*[pt]*	*Lisbon*
State Or Province	*[pt]*	*Lisbon*
Postal Code	*[pt]*	*1300-342 Lisboa*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:geral@gns.gov.pt*
URI	*[en]*	*https://www.gns.gov.pt*

Scheme Name

Name	*[en]*	*PT: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	*[pt]*	*PT: A Trusted List contem informações relacionadas com os Prestadores de Serviços de Confiança Qualificados, que são supervisionados por Portugal, juntamente com informações relacionadas com os serviços de confiança qualificados, de acordo com as disposições estabelecidas no Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de Julho de 2014 com a identificação electrónica e serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Directiva 1999/93/CE.*

Scheme Information URI

URI	*[en]*	*https://www.gns.gov.pt/pt/trusted-lists*
URI	*[pt]*	*https://www.gns.gov.pt/pt/trusted-lists*

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	*[pt]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/PT*

Scheme Territory

PT

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	*[pt]*	*O quadro jurídico aplicável à presente implementação desta TSL (Trusted-Service Status List) é o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de Julho de 2014, com os serviços de identificação e confiança eletrónicos para as transações eletrónicas no mercado interno e que revoga a 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-----

MIIH9DCCBdygAwIBAgIUYymXhglnqt2gl4PHVh4juzinht8wDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFOxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIHSVRBTFNJR04gUVVBTEIGSUVEIENBIEcxMB4XDTI0MDQyNjEyNDkyMloXDTI3MDQy
NjEyNDkyMlowggFKMQswCQYDVQQGEwJHUjE9MDsGA1UECwwO02VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2FoZSAtIE1lbWljcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWkSZ
QTFGTVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMS0wKwYJKoZIhvcNAQkBFh5hcG9zdG9sb3MuYXBs
YWRhc0lIYy5ldXJvcGEuZXUxEDAOBgNVBAQMB0FQTEFEQVMxEjAQBgNVBCoMCUFQT1NUT0xPUzEd
MBsGA1UECwwUUmVtb3RlUVNDRE1hbmFnZW1lbnQxGjAYBgNVBAMMEUFQT1NUT0xPUyBBUExBREFT
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsILa9o3bgz0lIdR1R01MhItrd6BLkxak
JxIqpnlc1fhT8R3uYGvSVwfsmjQei/YkbjMoNzakjo4voPhUJlBa9077jLGwZSghfkp0+vcg4yeC
LodAQatG7iEsh5Fr5uZgwPpLXExil0234QRcw7kJsI4k7wd7YvXAj1kv5zLTFo6sOr8ZF9km2rU1
7gbdZislH3/uR+JHkkhbIjm+MspETNN+Nva7duhkz14IIh/EIryTEPOLAdsgz+cRkBkyLQ1YYS6i
R3pifrsMvXzHYIwJY9AzPNd3cOBS2Ov05kB6tRyOka+6MREWY9aUZ2K/Q0anyrNCns5N/UXs589T
wrWp0QIDAQABo4ICuTCCArUwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRz5fFAHBQEfJoSf/ov
zVxnIxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRwczovL3FjYS1nMS5kaWdp
dGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRklFRENBRzEucDdlMC4GCCsGAQUFBzABhjodHRw
czovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMCkGA1UdEQQiMCCBHmFwb3N0b2xvcy5hcGxh
ZGFzQGVjLmV1cm9wYS5ldTBfBgNVHSAEWDBWMDcGCysGAQQBgcd8BAEBMCgwJgYIKwYBBQUHAgEW
Gmh0dHBzOi8vcGtpLmRpZZl0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEEMAkGBwQAi+xAAQIw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEsGA1UdHwREMEIwQKA+oDyGOmh0dHBzOi8v
cWNhLWcxLmRpZZl0YWxzaWduLnB0L0RJR0lUQUxTSUdoUVVBTEIGSUVEQ0FHMS5jcmwwHQYDVR0O
BBYEFHG/mw4edY/tZrrYu+8+Up7LgWyGMA4GA1UdDwEB/wQEAwIGQDCB0wYIKwYBBQUHAQMEgcYw
gcMwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATBqBgYEAI5GAQUwYDAu
FihodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfcHQucGRmEwJwdDAuFihodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfZW4ucGRmEwJlbjAVBggrBgEFBQcLAjAJBgcEAIvs
SQEBMBUGCCSGAQUFBwsCMAkGBwQAi+xjAQIwDQYJKoZIhvcNAQENBQADggIBALUt37pV7w5ZwRxB
B5PdTGTC+XcWytkuyuRJlVu+hVD5yVC2E+4+EPB2mRUzkjeE2M/3iMpzdwaNHe2YU9lCkoUFtD7V
LIEdiIfGO0MnXde2BAQN1VAt0s8xLwr3DNATsrtYPbtkQ73WCNqQwuNlg4LCFXHHpzvsKzYmYz+h
YgkA8daRZRJdnZx/eX05iYFtShbbz8VamNb+A1L/KmqSrt5iG8d9SLSSq95bNrntxSLaYDjfOITj
hW5KOwXBJPA+sQDYPhgHur1nLWUJg6QBBfo/YwMOTmylciurp8Qzktxfjl1wSZEpd/xZKoDWVDN
jJa8p0RFbQs/l7DpP/s57p8PKcntDOvQkYCajpRFLKl/69gKdVkB6nOKHFQCTmAeCDapWsI9+jPC
nriywN60ep+MMqedZ/lV8Lecbj/1E+kw6PhC6Rs4MlwmHHCe6BB/9oTK7SWW/CtIZh8ygtj0+5jI
DS/83b0F0JdnZUV2qhlZjIVORCcOljcWs7kYS8vWAqBbccAhYNpaaUh1rnKGqo2jpOo5HXhgSVHN
RrC+CylNNDUGAhpgPsAD93ui6jQCjdSzDkraWZAiGtmdpld0b7lR6HfR8s/QzeA4Rj7ChMMOFxD
ZPp2t6kEyPb1UOshC79fmoNRkBxmGKqMCPakQiiUoIg/BkLIUVYCIioQ8zsk

-----END CERTIFICATE-----
```


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: *Mon Apr 26 14:49:22 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:B0:82:DA:F6:8D:DB: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:60:6B: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:B0:65:28:21:7E:4A:74:FA:F7:20:E3:27:82:2E: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:B0:8E:24:EF:07:7B:62:F5:C0:8F:59:2F:E7:32:D3:16:8E:AC:3A:BF:19:17:D9:26:DA:B5:35:EE:06:DD:66:28:08:1F:7F:EE:47:E2:47:92:48:58:96:39:BE:32:CA:44:4C:D3:7E:36:F6:BB:76:E8:64:CF:5E:25:96:1F:C4:26:BC:93:10:F4:0B:01:DB:20:CF:E7:11:90:19:32:2D:0D:58:61:2E:A2:47:7A:62:7E:BB:0C:BD:7C:C7:62:5C:09:63:D0:33:3C:D7:77:73:40:52:D8:EB:F4:E6:40:7A:B5:1C:8E:91:AF:BA:31:11:16:63:D6:94:DB:62:BF:43:46:A7:CA:B3:42:9E:CE:4D:FD:45:EC:E7:CF:53:C2:B5:A9:D1:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

Authority Info Access

https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b

https://qca-g1.digitalsign.pt/ocsp

Subject Alternative Name *apostolos.apladas@ec.europa.eu*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25596.4.1.1

CPS pointer: https://pki.digitalsign.pt

Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4

Policy OID: 0.4.0.194112.1.2

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*

Subject Key Identifier *71:BF:9B:0E:1E:75:8F:ED:4F:3A:D8:BB:EF:3E:52:9E:CB:81:6C:86*

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B6:3D:41:67:44:E7:09:8B:F9:EC:2C:AA:59:6A:93:BC:24:68:E3:7F:82:84:BA:65:EC:C0:61:71:1B:CB:AA:18*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *212676479325594043390357602242635120 27*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG7zCCBNegAwIBAgIQEAAAAAAAnuXHXttK9Tyf2zANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQG
EwJCRTERMA8GA1UEBxMIQnJ1c3NlbHMxHDAaBgNVBAoTE0NlcnRpcG9zdCBOLlYuL1MuQS4xEzAR
BgNVBAMTCkNpdGl6ZW4gQDExDzANBgNVBAUTBjIwMTgwMzAeFw0xODA2MDEyMjA0MTIaFw0yODA1
MzAyMzU5NTIaMHAxCzAJBgNVBAYTAkJFMSMwIQYDVQQDExpQYXRyaWNrIEtyZW1lciAoU2lnbmF0
dXJlKTEPMA0GA1UEBBMGS3JlbWVyMRUwEwYDVQQgEwxOYXRyaWNrIEplYW4xFDASBgNVBAUTCzcy
MDIwMzI5OTcwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr7g7VnDYAas3R4LP0g7
uPH5inHzaVMOwFb/8YOW+9lVMHz/V5dJAzeTKvhLG554Pk6Kd2E+h18FiRonp70Gv2+ijtkPk7ZQ
kfez0ycuAbLXiNx2S7fc5GG9LGJafDJgBgTQuQm1aDVLDQ653mqR5tAO+gEf6vs4zRESL3MkYXAU
q+S/WocEaGplheNVAF3iPSkvEe3LvUjF/xXHWF4aMvgGK6kXGseaTcn9hgTbceuW2PAiEr+eDTNc
zkwGBDFXwzmnGFPMRez3ONk/jlKhha8TylDSfl/MX3ODt0dU3jvJEKPlfUJixBPehxMJMwWxTjFb
NuCK7tJ8qT2i154VQIDAQABo4ICjzCCAoswHwYDVR0jBBgwFoAU2TQhPjpCJW3hu7++R0z4Ag3j
L1QwcwYIKwYBBQUHAQEEZzBlMDkGCCsGAQUFBzAChi1odHRwOi8vY2VydHMuZWlkLmJlbGdpdW0u
YmUvY2I0aXplbjlwMTgwMy5jcnQwKAYIKwYBBQUHMAGGHGh0dHA6Ly9vY3NwLmVpZC5iZWxnaXVt
LmJlLzlwggEjBgNVHSAEggEaMIIBFjCCAQcGB2A4DAEBAgEwgfswLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBlcy0ub3j5LmVpZC5iZWxnaXVtLmJlMHHKBggrBgEFBQcCAjCBvQyBukdlYnJlaWsgb25k
ZXJ3b3JwZW4gYWFuIGFhbnNwcmFrZWxpamtoZWlkc2JlcGVya2luZ2VuLCB6aWUgQ1BTIC0gVXNh
Z2Ugc291bWlzIMOgIGRlcyBsaW1pdGF0aW9ucyBkZSByZXNwb25zYWJpbGl0w6kslHZvaXlgQ1BT
IC0gVmVyd2VuZHVuZyB1bnRlcmxpZWd0IEhhZnR1bmdzYmV2Y2hyw6Rua3VuZ2VuLCBnZW3DpHNz
IENQIzAjBgcEAlvsQAECMDkGA1UdHwQyMDAwLqAsoCqGKGh0dHA6Ly9jcmwuZWlkLmJlbGdpdW0u
YmUvZWlkYzlwMTgwMy5jcmwwDgYDVR0PAQH/BAQDAgZAMBMGA1UdJQQMMAoGCCsGAQUFBwMEMGwG
CCsGAQUFBwEDBGAwXjAIBgYEAI5GAQEwCAYGBACORgEEMDMGBgQAjkYBBTApMCcWIWh0dHBzOi8v
cmVwb3NpdG9yeS5laWQuYmVsZ2I1bS5iZRMCZW4wEwYGBACORgEGMAkGBwQAjkYBBgEwDQYJKoZI
hvcNAQELBQADggIBACBY+OLhM7BryzXWklDUh9UK1+cDVboPg+/lN1Et1AEoxV4y9zuXUWLco9t8
M5WfDcWFfDxyhatLedku2GurSJ1t8O/knDwLLyojE1r2Db9VrdG+jtST+j/TmJHAX3yNWjn/9dsj
iGQQuTjcce86rlzbGdUjjFTt5mGMm4zy4l/wKy6XiDKiZT8cFcOTevsl+l/vxiLiDnghOwTztVZh
mWExeHG9ypgMFYmIucHQ0SFZre8mv3c7Df+VhgV/sY9xLERK3Ffk4l6B5qRPylmXqGzNSWiDISd
YeUf4XoZLXJBEP7/36r4mInP2NWQ+c1ORjesuDAZBtD/yhMvR4DVG95EScjpTYvJwOmvB2IQrWnE
tygZIi60HXfozo8uOekBnqWyDc1kuizZsYRfVNlwhCu7RsOq4zNBgkaelI0fejuSNtBf2l9A+rc9L
Qeu6AcdPauWmbxtjV93H46pFptsR8zXo+JJn5m2P9QPZ3mvDkzldNTGLG+ukhN7IF2CCcagt/WoV
ZLq3qKC35WVcqeoSMEE/XeSrf3/mJ1OyFQm+tsfhTceOFDXuUgl3E86bR/f8Ur/bapwXpWpFxGl
pXLGaJXbzOGSTtyNEYrdENlh71I3OeYdw3xmzU2B3tbaWREOXtj2xjyW2tlv+vvHG6loR1QklkG
MFtzsT7W5U6ILetv

-----END CERTIFICATE-----
```


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:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AF:B8:3B:56:B8:83:63:86:AC:DD:1E:0B:3C:E8:3B:B8:F1:F9:8A:71:F3:69:53:
0E:C0:56:FF:F1:83:96:FB:D2:15:30:7C: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:B6:50:91:F7:B3:D3:27:2E:01:
B2:D7:98:DC:76:4B:B7: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:FB:38:CD:11:12:2F:73:24:61:70:14:AB:E4:BF:5A:87:0
4:68:6A: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:EB:96:D8:F0:22:12:BF:9E:0D:33:5C:CE:4C:06:04
:31:57:C3:39:A7:18:53:CC:45:EC:F7:38: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:C
2:2B: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/eidc201803.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:

643978552848424008220551052528366836395685220683

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIIBDCCBeygAwIBAgIUcMz/PU9hyZj1+vaAghkzK31AkUswDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTI1MTEyNDA5NTY0MVoXDTI5MTEy
Mz A5NTY0MVowggFWMQswCQYDVQQGEwJHUjE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXj0aWZpY2F0ZSAtIEJlbWjlcjEjMCEGA1UEYQwaTEVjWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMTEwLwYJKoZIhvcNAQkBFiJb2FubmEuS0FMT0dF
Uk9QT1VMT1VAZWMuZXVyb3BhLmV1MRcwFQYDVQQEDA5LQUxPR0VST1BPVUxPVTEPMA0GA1UEKgwG
SU9BTk5BMR0wGwYDVQQLDBRSZW1vdGVRU0NETWFuYWdlbWVudDEaMBwGA1UEAwwVSU9BTk5BIEtB
TE9HRVJPUE9VTE9VMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAswjmtemrpGlPsoCM
1tVfVICYiyK0elodby6nK00KfkS8K9gEou+OZJj5B85VmEC7u889RAG1DUr6k+75etz9E/qYdFhz
/3Gjw10XsEuRcwdzafvKM9DrXFFkGYRqKSkJ67/sKq1JKE7bCkbMZ/B8SDRUJ2veSoRS/oC5Ghuf
arAZOxXUwrzb723BTwQGkar/G0Y7co1eVOXX6hGy4mnPF36APvG941p/IuoMM5Ib610h/I1zB5DF
lgAVEI0HnICoLfQ6oqJcv01WfGKEIhppoepbhuhSE7EgQ0JLlufBzdunyY/Mmv24ItZjFV/OQf1R8
7StpL7AicC5BSCWfiXyD7wIDAQABo4ICvTCCArkwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRz
SfFAHBQEfJoSf/ovzVxnIxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFvQUxJRkIFRENBRzEucDdiMC4GCCsG
AQUFBzABhjodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMC0GA1UdEQQmMCSBIkIv
YW5uYS5LQUxPR0VST1BPVUxPVUBlYy5ldXJvcGEuZXUwXwYDVR0gBFgwVjA3BgsrBgEEAYHHfAQB
ATAoMCYGCCsGAQUFBwIBFhpodHRwczovL3BraS5kaWdpdGFsc2lnbi5wdDAQBg4rBgEEAYHHfAQC
AQEBBDAJBgcEAIvsQAECMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBLBgNVHR8ERDBC
MECqPoA8hjodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRkIF
RENBRzEuY3JsMB0GA1UdDgQWBBQOe+jKZg/EC79WvQ/Ven54zd1YxDAOBgNVHQ8BAf8EBAMCBkAw
gdMGCCsGAQUFBwEDBIHGMIHDMAgGBgQAjkYBATAIBgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYB
BgEwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX3B0LnBk
ZnMCMCQwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX2VuLnBkZnMCZ1WwFQYI
KwYBBQUHCwIwCQYHBACL7EkBATAVBggrBgEFBQcLAjAJBgcEAIvsSQECMA0GCSqGSIb3DQEBDQUA
A4ICAQBXav52/+LXYZAgA0MjuEl/+NacJC9E9VRIklvrLzAHcj2KQ2GLR1fL8C2UIJ6u2+LwG2m
lyyK2F16erDoOWKDV4OvxgGEfSwgin6GUhHmzuRDPBQhUW4C7btUFMoAr05UT+v03d9RrnlA5bpK
5lKaf2j3EGAfGR1DvvFJ+ZCFaVo+8rtcLpySS3f8ZPCgz3axaO3KeyK4LujbdZqGArKIF0vNKGR9
4rr7Pq7OIIHJBuOW9LGQG0r5e8kbKRL2BsPlHpgPvZc8M3EimqYnIg6hgPf0k+Mxhw5/lC4rikF
sMTNa43yBeGrk2pvM8cIZoenmQMgf/1L0+A9Pwol+7CUQfe4Bpj0fr1Acnx/4oPnAKmMDKvXnx91
fMW2b7Uen2y11TcijxYuXftq03bx8w/ms/giXYLGciDcwCF7XCXNnGuATW/GxPvOxOwu56ZDrm/o
G3zfa4l/tf/S5swoFrzmTDIIM05UzHDUuQAln103BGfEYKo7vw4bNfouHfS28gGWbotUSNzHfOEq
eC4LrdN7JmE8q0hZRXLFOIsPtGzSDfEkuoNI3znZPmk8oAy/xa1+3XnH1nJCVmTKDXQYaTPinAAE
nDbTqUjD97zmUFEd+ecOctica4DFhQoHtUDYUOzKEKfKHVEG0Apl3dpHzcLiuLXIQI0DBvfy3wsp
y6HL3A==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA512withRSA

Issuer CN:

DIGITALSIGN QUALIFIED CA G1

Issuer O:

DigitalSign Certificadora Digital

Issuer C:

PT

Subject CN:

IOANNA KALOGEROPOULOU

Subject OU:	*RemoteQSCDManagement*
Subject GIVEN NAME:	*IOANNA*
Subject SURNAME:	*KALOGEROPOULOU*
Subject E:	*Ioanna.KALOGEROPOULOU@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:	*Mon Nov 24 10:56:41 CET 2025*
Valid to:	*Fri Nov 23 10:56:41 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:B3:08:E6:B5:E9:AB:A4:69:4F:B2:80:8C:D6:D5:5F:54:80:98:8B:22:B4:78:8A:1D:6F:2E:A7:2B:4D:0A:7E:44:BC:2B:D8:04:A2:EF:8E:66:32:79:07:CE:55:98:40:BB:BB:CF:3D:44:01:B5:0D:4A:FA:93:EE:D2:7A:DC:FD:13:FA:98:74:58:73:FF:71:89:C3:5D:17:B0:4B: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:B9:1A: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:33:92:1B: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*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*Ioanna.KALOGEROPOULOU@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*0E:7B:E8:CA:66:0F:C4:0B:BF:56:BD:0F:D5:7A:7E:78:CD:DD:58:C4*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C0:64:1C:4F:7D:56:C4:31:B1:C9:24:74:2D:B7:FC:E9:C1:EE:F7:D7:FD:21:21:13:A2:76:84:86:B3:AB:CD:C5*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *287042771050117106830096624703098875244460545240*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIIjCCBn6gAwIBAgIUMkdxaYjTAuT2WRKfmeup7zDClNgwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gLVVBTEIGSUVEIENBIEcxMB4XDTI1MTxNzE0MzE1NFoXDTI5MTIx
NzE0MzE1NFowqgEMMQswCQYDVQQGEwJMVTFDMEEGA1UECww6O2VydGlmaWNhdGUgUHJlvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjExMC8GA1UECwwoRGlyZWN0b3Jh
dGUtR2VuZXJhbCBmb3IgRGlnaXRhbCBTZXJ2aWNlczEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
OTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1N/T04xJDAiBgkqhkiG9w0BCQEW
FUVVLVRSVVNUQGVjLmV1cm9wYSSIdTEcMBoGA1UEAwwTRVVST1BFQU4gQ09NTU1TUOlPTjCCAiIw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKJguyStfry/iDbqvGbthdtVqplyQ3p04V5hVtzW
WkERnp5zN4AU3E1jqK2UFvEtUyzgl6c30nEDlJS9LnbCqd7B+YVy+Ad/YXkSx1SNNcwrKMy9WiE
/xxGBw3CgM4Pl1Xe0wNtLEdv2Ds82ELVnE59vefFC1zNSgx7YLIl1Y433Lch7Koo7w0LGbJlYDaH
VRmbT4n+WzbXxQddDJHaST1piFcWXR07OlEehLUdoyGBlNX4sOe6APDoZL0pHQOmSbL9o0IhOT5z
avza7t10B9QU7+kHoPKUiVRYtPiYgMMkeIyLcO+C9aMhYknxvLaO4TjKAIXsWyC37u58lLsSun4B
dMA0e+YYAJa94fOyXNxAGrajV4pXFUlZOtAI7GcuLHz5Uy5kHvKNw6BeOX0dbrJz7HdKFKB6qz8x
cv8Fs3FiZrbYH/Ov5NmocW5wxD4lFgSm3ZtRdCv90eGYbFhGgb9fuj90kxvSk902db52Srm7OTr3
iuxEtiOhnubi+emaTeT74Q5Il2w6jIOhpQZejw7dIFDub3bdpsH0TTkFb481uMmKALBsE0h0Zto
YjCBTTWjgGCFBYDQNPCS1ITJEJjHFSXaY0Y6kfqkBDjvdWnlapvcmy7Hkk2Hx6AzTITyxZ20HtR
URiiKgGp8inZLB+Frj358FF7m0xBWKvemjDBAgMBAAGjggKZMIICTAMBgNVHRMBAf8EAjAAMB8G
A1UdIwQYMBaAFHNJ8UAcFAR8mhj/+i/NXGcjGOkUMIGGBggrB gEFBQcBAQR6MHgwRgYIKwYBBQUH
MAKGOmh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0LORjR0lUQUxTSUdOUVVBTEIGSUVEQ0FH
MS5wN2IwLgYIKwYBBQUHMAGGImh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L29jc3AwIAYD
VR0RBBkwF4EVRVUtVFJVU1RAZWMuZXVyb3BhLmV1MF8GA1UdIARYMFYwNwYLKwYBBAGBx3wEAQEw
KDAmBggrBgEFBQcCARYaaHR0cHM6Ly9wa2kuZGlnaXRhbHNpZZ4ucHQwEAYOKwYBBAGBx3wEAgEB
AQYwCQYHBACL7EABAzAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwgbwGCCsGAQUFBwED
BIGvMIGsMBUGCCsGAQUFBwsCMAkGBwQAi+xjAQIwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5G
AQYwCQYHBACORgEGAjBgBgYEAI5GAQUwYDAuFihodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5w
dC9QRFNfZW4ucGRmEwJlbjAuFihodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfcHQu
cGRmEwJwdDBLBgNVHR8ERDBCMECgPgA8hjpodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9E
SUdJVEFMUOlHTlFVQUxjRkIFRENBRzEuY3jsMB0GA1UdDgQWBBSHDNZIrZdGBhUl8nfHbH/C0pdK
BTAOBgNVHQ8BAf8EBAMCBkAwDQYJKoZIhvcNAQENBQADggIBAJQhD5ZXFK6w/6ODzWs82K5E3JMq
QBnHaMVXRi5mwsts3Y4h1pUOxTECqrRnn4IkwWLy5csHjjOO1RbXasI3s6LHV+WzVdebUVH92nsP
s9c7msxTwohXweCX429n8VBY0hJ1jpE41e/AaDHLOMBe3elrOF+3VUBnoFuTF+bDDROCw5B44ULY
Q+yHvJg0LVygnhQb08I+YtRpQNTA/O1Q9ALIuudEpL5vtAQVTBKPc0DyWGw1EiEFh++gogHAtCT7
6/8HOlLjwC7gTNe3W7WGhT1y3ZzKfp4T3q+dpqo7+yJSHMEAjWArmuMwTF0rHZDCKVfxhKPaJasl
cNww8Hwf6igaRYSbtajyWGD56ZLIlRttks0yU0ZWVcPONQUbFpWRF8DU4+yVSSI5var0p2MiHzLq
rrltSbZG+ykFr7Xz9rvpSKLzweRXELeuW/KcPL0gspUi/VWDZvqbun9sEoPhKG02ciNjpKuB5L4
A2uP3oH82GrTa+PSBnOmLLSDxKOHXFbFpTET7kirc3GLyxopppjw4feV/a9Rqm+gdjpbrJuHnuti9
xm2jAWThELxoNKmIuSSf1uPsh3GrxIeH8gbmvKsOWG4CCU+MW+bLuffFsxI2RHzytphb6LNVHtgaJ
7aUTuZHYBGI3SdZ+ogB/fjo9NM/unYnlfSRXesA8IJP+S5qt

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *EUROPEAN COMMISSION*

Subject E: *EU-TRUST@ec.europa.eu*

Subject O: *EUROPEAN COMMISSION*

Subject 2.5.4.97: *LEIXG-254900ZNYA1FLUQ9U393*

Subject OU: *Directorate-General for Digital Services*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *LU*

Valid from: *Wed Dec 17 15:31:54 CET 2025*

Valid to: *Mon Dec 17 15:31:54 CET 2029*

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:A2:60:BB:24:AD:7E:BC:BF:88:36:EA:BC:66:ED:85:DB:55:AA:92:32:43:7A:74:E1:5E:61:56:DC:D6:58:A1:11:9E:9E:73:37:80:14:DC:4D:65:8E:A2:B3:50:5B:C4:B5:4C:B3:AA:5E:9C:DF:49:ED:0C:82:52:F4:B9:DB:0A:A7:7B:07:E6:15:CB:E0:1D:FD:85:E4:4B: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:BD:E7:C5:0B:5C:CD:E6:0C:7B:60:B9:48:D5:8E:37:DC:B7:21:EC:AA:28:EF:0D:DB:19:B8:CB:60:36:87:55:19:9B:4F:89:FE:58:36:D7:C5:07:5D:0C:91:DA:49:3D:69:B8:57:16:5D:1D:3B:D0:91:1E:84:B5:1D:A3:21:81:94:D5:F8:B3:47:BA:00:F0:E8:64:BD:29:1D:03:A6:49:B2: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:BC:B6:8E: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:74:93:1B:D2:93:DD:36:75:BE:76:4A:B9:BB: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:B8:50:EE:6F:76:DD:A6:C1:F4:4D:39:05:6F:80:75:B8:C9:A2:28:02:FC:B0:4D: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:AA:6F:72:6C:BB: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*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*EU-TRUST@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*87:0C:D6:49:AD:97:46:06:15:25:F2:77:C7:6C:7F:C2:D2:97:4A:05*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*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*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*660862747298009142807362633871991440505734410485*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIoDCCBoigAwIBAgIUc8lcSUtvEKAMMvHm9QWU05kXsPUwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmlpYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gUVVBTEIgSUVEIENBIEcxMB4XDTIzMTExNzEwMTE0NloXDTI3MTEx
NzEwMTE0NlowggEVMQswCQYDVQQGEwJMVTFDMEEGA1UECww6Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjE5MDcGA1UECwwwRGlyZWN0b3Jh
dGUtR2VuZXJhbCBmb3IgRGlnaXRhbCBTZXJ2aWNlcyAoREIHSVQpM5MwIQYDVQRhDBpMRUlIYRyOy
NTQ5MDBaTlBMUZMVVE5VTM5MzEcMBoGA1UECgwTRVVST1BFQU4gQ09NTUlTU0lPTjElMCMGCSqG
Slb3DQEJARYWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTEcMBoGA1UEAwwTRVVST1BFQU4gQ09NTUlT
U0lPTjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKWYeBA9kYAREIGnHojRNpbby44G
+TSJcgHl9QtyXlYjB234hSAYyJvW+gKvoownskrogfUP6GOmOgEFZX335Y0sBwfppVemEoe9H9Aj
/cpT14Iqd805V4a88ASRfR0Va1xmOJrDsBZWgZHx0EEHBctIF5BjyTMAcQybha+4AOlotp3dfr/7Z
A3Cu4GYbN9BuQyyqfqrjMduDzzDjVwKC17aEsLev60C1FnIj/FVEda3JSGIlDSJyUceTaRcot1r
w6gjKrOVhwP/UHfevJ3jCsQsuAzkf7ivzHzYuPPPR9Ussecwr7O95Fr4wbPYlyX2AOTIieAC7GMV
XHN1/+4LH74ndvqlYEScXwmN9Skib3+G6TquOCQxvNXzHPZb95btCoSnVprCn14O3CXUTZMEKkhP
uKW8dl6pR2JSGbtT+xBKcc1wYl/UnzE3d+YK5SevUT2COwJM+AcjSoUaRTBINsD/ezDDvv7vtbF
1XccajjoCNkurzayTsMszGDvAF171LY69INY6yK0uzrS+3c/hEHctXa5KIC3PpWrBGQ5mw73KerR
vnAhzDZemVquPk1D59aJNfHoHXmy1bS52rHWYOwHH+2qbODdh8GkHwHXBzSpFit1Kg2brpavhztN
aGlj6GsLFAbr8okCUjlIOQLO8Tfy9Vnn5Rq0+7VTdd8dAxg9AgMBAAGjggKaMIICjAMBgNVHRMB
Af8EAjAAMBBGA1UdIwQYMBaAFHNJ8UAcFAR8nhJ+i/NXGcjGOKUMIGGcBggrBgEFBQcBAQR6MHgw
RgYIKwYBBQUHMAKGOmh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L0RjR0lUQUxTSUdOUVVB
TEIgSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGGImh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0
L29jc3AwIQYDVR0RBBowGIEWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTBfBgNVHSAEWDBWMDcGCysG
AQQBgcdBAEBMCgwIgYIKwYBBQUHAgEWGmh0dHBzOi8vcGtpLmRpZ2l0YWxzaWduLnB0MBAGDisG
AQQBgcdBBAIBAQEGMAkGBwQAi+xAAQMwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMIG8
BggrBgEFBQcBAwSBrzCBrDAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYBATAIBgYEAI5G
AQQwEwYGBACORgEGMAkGBwQAjkYBBgIwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGln
aXRhbHNpZ24ucHQvUERTX2VuLnBkZhMCZlW4wLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24u
cHQvUERTX380Ln8kZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRh
bHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZJRURDQUcxLmNybDAdBgNVHQ4EFgQUlO5hwcl9/63i
ssm59r+TIHeJSZwwDgYDVR0PAQH/BAQDAgZAMA0GCSqGSIb3DQEBDQUAA4ICAQCn8qjJhTe3SsD7
cB85BkDzt+CBnJJm7bOFc9t9IU6iKntVtjPU4T+cYiPk8Tn7+/w7dBphRzjZCL1sDfSJGQ5JPBw+
hBPuvzGqP4xVi5j4jhg/GpYSaa2+dkFXlKe65d+Ij/RnwB5nfqVfNZtasj7yX+ou9au5LSUPlKQ
xDrMie8KjsNtlkFjQDoIoGAx8b0u6WyhAuqwEacCznft20Dim3sC7XJw8GHumrnW52rUzI4sbXoT
BAt8F1zPCbEbjU0oc85bFNPlChh+9sHUorEmHIlcg30LBHihkDCx4mK8J60Jybk57D4U2RO29VsJ
fDmnvNxfJZxfLHEJ2tkh+AMgIJXPDlvXQ+rZ1NmLHrbXkcHOlqR3F8BakTi2Mi5AZZfkfjZjkigE
StN6Enaq6gwF7EssIqEKmhSQ8KlhxW5RqJKcnEUw+NhrvR4WuKlvYrmxlCLOj6q89Hh121aUGUh
L2L2WCVBjVXqux7s4mvECDzrucl5ilaVT32HO3g8qNLGD5lum53U5v/Nv68ltyHH96unztwBebmg
ox8giVRdzPhmPrpSfbmeNNDKj1p95CeOvd3P9jCUvChVvH2P2ZUjc24tWe+tzclsCji7GbKr6kjH
c1jFudjehfIAbm1lZAYdDNrhXamnsRVsz7iSH20eygCArlwSQ//WIQZPFrRffg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *EUROPEAN COMMISSION*

Subject E: *digit-dmo@ec.europa.eu*

Subject O: *EUROPEAN COMMISSION*

Subject 2.5.4.97: *LEIXG-254900ZNYA1FLUQ9U393*

Subject OU: *Directorate-General for Digital Services (DIGIT)*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *LU*

Valid from: *Fri Nov 17 11:11:46 CET 2023*

Valid to: *Wed Nov 17 11:11:46 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:A5:98:78:10:3D:91:80:11:12:51:A7:1E:82:51:36:96:DB:CB:8E:06:F9:34:89:
72:01:C8:F5:0B:72:5E:56:23:07:6D:F8:85:20:18:C8:9B:D6:FA:02:AF:A2:8C:27:B2:4A:E8:81:F5:0F:E8:63:A6:42:01:05:65:7D:F7:E5:8D:2C:07:07:E9:A5:57:A6:12:87:BD:1F:D0:23:FD:CA
:53:D7:82:2A:74:1D:39:57:86:BC:F0:04:91:7D:1D:15:6B:5C:66:40:9A:C3:B0:16:56:A9:91:F1:D0:41:07:05:CB:48:17:90:63:C9:33:00:71:0C:98:85:AF:B8:00:E2:28:B6:9D:DD:17:FE:D9:
03:70:AE:E0:66:1B:37:D0:6E:43:2C:AA:7E:AA:E3:31:DB:83:C7:30:E3:57:02:82:D7:B6:84:80:B7:AF:EB:40:85:16:72:09:FC:55:44:75:AD:E5:25:21:A2:94:3E:49:C9:47:1E:4D:A4:5C:A2:D
D:6B:C3:AB:23:2A:B3:95:87:03:FF:50:77:DE:BC:9D:C9:0A:C4:2C:B8:0C:E4:7F:B8:AF:CC:7C:D8:B8:F3:CF:47:D5:2C:B1:E7:30:AF:B3:BD:E4:5A:F8:C1:B3:D8:23:25:F6:00:E4:E5:89:E0:02
:EC:63:15:5C:73:75:FF:EE:0B:1F:BE:27:76:FA:09:60:44:9C:5F:09:8D:F5:29:22:6F:7F:86:E9:3A:AE:38:24:31:BC:D5:F3:1C:F6:5B:F7:96:ED:0A:84:A7:56:9A:C2:9F:5E:0E:DC:25:D4:4D:93
:04:2A:48:4F:B8:A5:BC:74:8E:A9:47:62:52:19:BB:53:FB:10:64:71:CD:70:61:59:54:9F:31:37:77:E6:0A:E5:24:9E:BD:44:F6:08:EC:09:33:E0:1C:8D:2A:14:69:14:C1:20:DB:03:FD:EC:C3:0
E:F8:FB:BE:D6:C5:D5:77:1C:68:98:E8:08:D9:2E:AF:36:82:4E:C3:2C:CC:60:EF:00:5D:78:D4:B6:3A:F6:53:58:EB:22:B4:BB:3A:D2:FB:77:3F:B4:41:DC:B5:76:B9:28:80:B7:3E:95:AB:D4:64
:39:9B:0E:F7:29:EA:D1:BE:70:21:CC:36:5E:99:5A:AE:3E:4D:43:E7:D6:B9:35:F1:E8:1D:79:B2:D5:B4:B9:DA:B1:D6:60:EC:07:1F:ED:AA:6C:E0:DD:87:C1:A4:1F:01:D7:07:34:A9:16:2B:75:
2A:0D:9B:AE:96:AF:87:3B:4D:68:69:63:E8:6B:0B:14:06:EB:F2:89:02:50:99:65:38:E2:D0:F1:37:F2:F5:59:E7:E5:1A:B4:FB:B5:53:75:DF:1D:03:18:3D:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

Authority Info Access *https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b*

https://qca-g1.digitalsign.pt/ocsp

Subject Alternative Name	*digit-dmo@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*94:EE:61:C1:C9:7D:FF:AD:E2:B2:C9:B9:F6:BF:93:20:77:89:49:9C*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*E0:A6:20:FB:B6:74:73:62:BB:93:3A:C4:41:69:D6:76:A5:53:44:47:16:CF:5F:31:60:5F:12:A2:2B:83:96:B1*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*416260670660158992857603279521251626757860879766*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----

MIIICDCCBfCgAwIBAgIUSOnGlxOHWc5N+Nk12eZPPCwr7ZYwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmlfYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIHSVRBTFNJR04gUVVBTEIGSUVEIENBIEcxMB4XDTI0MDUwNjEyNDUxNloXDTI3MDUw
NjEyNDUxNlowggFZMQswCQYDVQQGEwJFUzE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHlvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWlcjEjMCEGA1UEYQwaTEVlWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTUJUJNT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JlZlFNUQUZGMTIwMAYJKoZIhvcNAQkBFiN2aWNlbnRlLmFuZHll
dS1uYXZhcnJvQGVjLmV1cm9wYS5ldTEXMBUGA1UEBAwOQU5EUkVVIE5BVkFSUk8xEDAOBgNVBCoM
B1ZJQ0VOVEUxHTAbBgNVBAsMFFJlbW90ZVFTQ0RNYW5hZ2VtZW50MR8wHQYDVQQDDBZWSUNFTlRF
IEFORFJFVSBOQVZBUlJPMIIBIjANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAveJV7goW3mvq
Jq2kMT0cnrkfAnT/lyzbgaHVxd5JEMHy6Ryol1AF4JTIOWSjC+6fsNzApFR1Tv3w8/Wu5qjHTWfD
npqs20ijh979A5WwvfXuzcuUqeFFptdR/tjm/08TsTAD+CeA+rQo6K23B1xMYRwX/BNt/EL03Q/T
QOj5V4uV3Kyf0945yu5gOhmrMs/RZCZ8M+iahwTaVktf+ZvhocSsPt+a2OuPl8lpTU+xlWAXWuQ+
27Q7zzD0d6sqBdruDr1BclFtZXWNRikm9g6pCOAOKG/myszeUuy++TPtQnI3+OQlTuyDXsz9UNkb
oQCF2SNmfRoeBxcxO2t5/zUgPwIDAQABo4ICvjCCArowDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW
gBRz5fFAHBQEfjaSf/ovzVxnlxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRw
czovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTIFVQUxJRkIFRENBRzEucDdiMC4G
CCsGAQUFBzABhjodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMC4GA1UdEQOnMCWB
I3ZpY2VudGUuYW5kcmV1LW5hdmFycm9AZWMuZXVyb38hLmV1MF8GA1UdIARYMFYwNwYLKwYBBAGB
x3wEAQEwKDAmBggrBgEFBQcCARYaaHR0cHM6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwEAYOKwYBBAGB
x3wEAgEBAQQwCQYHBACL7EABAjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwSwYDVR0f
BEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFM
5UZjRURDQUcxLmNybDAdBgNVHQ4EFgQUjueweY4Fl0KGjetMh84vTsEnxOcwDgYDVR0PAQH/BAQD
AgZAMIHTBggrBgEFBQcBAw5BxjCBwzAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcE
AI5GAQYBMGoGBgQAjkYBBTBgMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19w
dC5wZGYTAnB0MC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19lbi5wZGYTAmVu
MBUGCCsGAQUFBwsCMAkGBw0Ai+xJAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjANBgkqhkiG9w0B
AQ0FAAOCAgEAHBjW4N8NKNCJlot414m/L76pB/15LKiGDi1/2V7MHe8u2GcplR1ljES rSEhhwUAW
1hwDIK9xJrj/hdDUMIQcKSc5jlCqTCb0Yk39yj/gfOYaN/3fqw8Pjh9k++3Ox7KnvY3R/foFvGjl
yiuqaai/jgBmc4qDBHSlDyo5gRw6v70osRPDR5sJs4Xh3FOjn9Y0JZPLF/skYtLrNVysL/4A4bbA
xB2Dcj5MpoIegh/fnJ5s2BOVq2Xq8ADpejoLFYbtlbP7NwsGgew2wKiDW963MlJL/Xa2AqcPVE/U
nXFkIBCwZH+covxSEQH2iVcF8cEDHBiYHGERaSmL/uHK/F8soDO9VQwtKNxsIlKAWsQHTYcKfEgV
uweyLj7TsCmh6T4plHqaNDqWvrgElo0ZwuBmfXVEd+JMSzSgIcj2bPR2KNoJ14MO4FFYdAAnVlfd
hipErsK6R23hlto7b3XKiMRUt9xrvPUjuEJdGI5hPm9CqGK1GxlRoKLewyX7A+OlcPMPu1KfuuUT
Un+3hLJlZO5H9k4uVMJ/FOhwzc2VhRpyvNjfmFZksFvseFGvMI5EWIqp3jCo0ltkOBG59uIBwg/9
9YOpT6LW9cviTzKIwDtHmQrIgYLa+lCYwWdGhIlaXynvLpWiVRZjvYrPIGpzQCRcw9Vzi8zT7nks
j7QF9v88kto=

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA512withRSA*
Issuer CN:	*DIGITALSIGN QUALIFIED CA G1*
Issuer O:	*DigitalSign Certificadora Digital*

Issuer C:	*PT*
Subject CN:	*VICENTE ANDREU NAVARRO*
Subject OU:	*RemoteQSCDManagement*
Subject GIVEN NAME:	*VICENTE*
Subject SURNAME:	*ANDREU NAVARRO*
Subject E:	*vicente.andreu-navarro@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:	*ES*
Valid from:	*Mon May 06 14:45:16 CEST 2024*
Valid to:	*Thu May 06 14:45:16 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:BD:E2:55:EE:0A:16:DE:6B:EA:26:AD:A4:31:3D:1C:9E:B9:05:02:74:FF:97:2C:DB:81:A1:D5:BD:DE:63:10:C1:F2:E9:1C:A8:23:50:1F:E0:94:E5:39:64:A3:0B:EE:9F:B0:DC:C0:A4:54:75:4E:FD:F0:F3:F5:AE:4A:08:C7:4D:67:C3:9E:9A:AC:DB:48:89:87:DE:FD:03:95:B0:BD:F5:EE:CD:CB:94:A9:E1:45:A6:D7:51:FE:D2:66:FF:4F:13:B1:30:03:F8:27:80:FA:B4:28:E8:AD:B7:07:5C:4C:61:1C:17:FC:13:6D:FC:42:F4:DD:0F:D3:39:08:F9:57:8B:95:DC:AC:9F:D3:DE:39:CA:EE:60:3A:19:AB:32:CF:D1:64:26:7C:33:E8:9A:87:04:DA:56:4B:5F:F9:9B:E1:A1:C4:AC:3E:DF:9A:D8:EB:8F:23:C2:29:4D:4F:B1:21:60:17:5A:E4:3E:DB:B4:3B:CF:30:F4:77:AB:2A:05:DA:EE:0E:BD:7A:72:51:6D:65:75:8D:46:29:26:F6:AE:A9:08:E0:0E:28:6F:E6:CA:CC:DE:52:EC:BE:F9:33:ED:42:72:37:F8:E4:25:4E:EC:83:5E:CC:FD:50:D2:9B:A1:00:85:D9:23:66:7D:1A:1E:07:17:31:D3:6B:52:FF:35:20:3F:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*vicente.andreu-navarro@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*8E:E7:B0:79:8E:0F:23:42:86:8D:EB:4C:87:CE:2F:4E:C1:27:C5:07*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*
id_etsi_qcs_QcSSCD

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DF:7E:29:36:0C:34:B2:B8:D6:D5:F4:03:25:C1:D4:D1:2C:99:22:CE:CD:33:B7:40:76:74:A7:4B:2B:3C:A1:E5*

TSL Type *http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists*

Scheme Territory *EU*

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 *2026-07-01T11:00:07Z*

Next Update

date Time *2027-01-01T12:00:07Z*

Distribution Points

URI *https://www.gns.gov.pt/media/TSLPT.xml*

1 - TSP: CEGER - Centro de Gestão da Rede Informática do Governo

.

TSP Name

Name	*[en]*	*CEGER - Centro de Gestão da Rede Informática do Governo*
Name	*[en]*	*ECCE*

TSP Trade Name

Name	*[en]*	*CEGER*
Name	*[pt]*	*Entidade Certificadora Comum do Estado (PKI nacional - SCEE)*
Name	*[en]*	*VATPT-600055639*
Name	*[en]*	*SCEE*
Name	*[en]*	*Centro de Gestão da Rede Informática do Governo*

PostalAddress

Street Address	*[en]*	*CAMPUS APP, Avenida João XXI nº 63*
Locality	*[en]*	*Lisbon*
State Or Province	*[en]*	*Lisbon*
Postal Code	*[en]*	*1000-300 Lisboa*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*CAMPUS APP, Avenida João XXI nº 63*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1000-300 Lisboa*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:certificacao@ecce.gov.pt*
URI	*[en]*	*https://www.ecce.gov.pt*

TSP Information URI

URI	*[en]*	*https://www.ecce.gov.pt*
URI	*[pt]*	*https://www.ecce.gov.pt*

1.1 - Service (withdrawn): ECCE (CA-Qualified Certificates)

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]*	*ECCE (CA-Qualified Certificates)*
Name	*[pt]*	*ECCE (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *153703741112188382806396968881839442505*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFDDCCAvSgAwIBAgIQc6JDhZgH+D9EqSk0elSKSTANBgkqhkiG9w0BAQUFADAzMQswCQYDVQQG
EwJQVDENMAsGA1UECgwEU0NFRTEVMBMGA1UEAwwMRUNSYWl6RXN0YWRvMB4XDTA2MDcwMzE0Mjcw
MFoXDTE4MDYyMzA4NDk0N1owPjELMAkGA1UEBhMCUFQxDTALBgNVBAoMBFNDRUUxETAPBgNVBAsM
CEVDRXN0YWRvMQ0wCwYDVQQDDARFQ0NFMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
zR3ZwOJ4zV8fbHZMPJUbQ0cBnpj3J6PUqHrGM6yCY/gbbeqF20zDYoy/UnK5BNbPleEAarWtSeqv
kQs/O372C6WarjloKuClpgTju+uWBgKL4p0YjyqJNDzal16k6nYhaRPIR4/3LKqtleOkTb8yxMjA
6TsrjZiRarI4JgTi1EAru76Bgnw+5LmYTN6qRzykma/KkX0sD78BEfl/gpotfuMbS29rjD3D7bn+
rvQOyXMxDXy6vBpxT/oO+bfV7VlTgd+aNqQu/xjQlHENn3/9TV5b8TZnNGzit6g3MvBkj9gH+VXD
U4kdCkj+lyLmKI7vTI77DWsbNyrPxmdpoti/fQIDAQABo4IBDzCCAQswDwYDVR0TAQH/BAUwAwEB
/zAdBgNVHQ4EFgQUWQtmzPp7FphoDvZcAPO5remmOnQwHwYDVR0jBBgwFoAUcX813vV3cW0dEpzh
kKS68KmDj4AwDgYDVR0PAQH/BAQDAgEGMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIB
FhpodHRwOi8vd3d3LmVjZWluZ292LnB0L2RwYzA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAGG
GGh0dHBzOi8vb2NzcC5lY2VILmdvdi5wdDA1BgNVHRBEJAsMCqgKKAmhiRodHRwOi8vY3Iscy5l
Y2VILmdvdi5wdC9jcmxzL0FSTC5jcmwwDQYJKoZIhvcNAQEFBQADggIBAFjkNeQX+prqbf6s9DKN
d2VHmt/au7tr1tG76cqxvll9R4mx8jXdiwRlkyPC5p9SMg45RHnrTiNRJeJ08NN3CUUPmayd5NEO
6UqHWJr/5pEzrKSgFZzGVl4cDbAkqBXUgSToZgi8AY9NXsFyoWO4IKz5iVV2DGeFdc95L2FPsIpo
Z5XaZrA0Gkl79fmMWAVbZ0TrDMrbEe4gP6EQ7AfCUjzDuFCstpU3rDICn2Il4mYmeNdlnRqPEuq0
0f3YGQ4BmV1vvlYLxCUAtyJeGRPfpVVsv1899xid7iXV9kr/YPvOP7VBXvq6keqYWADk3dGf4C/D
zFDi3npcpTDhs/RnND8ClnONSgRV13FKPtTums/dEPXDRoXoDKjq2macBP/59rnCdMoAF5jtwxbN
d1590ugnDCMyoncDsh4m/88EnvsSMkZACQ8K7POX/CdZmCQWw3fZ+/I9l0tP8glk8roPrinHoaUj
GzfgHRlVxxHf/WuXjP9qlkvQGx5PLfz9s99ci599PzjO7NbIJlNPPDxfamdffEb9GrqW/L5wQcKtS
q7iUapZ5Lsk8hNxjlFIMzt7jiYXMMsxfGbQrONqe879xlORf+RjqnXlaQ564VIlCMv4+xkQkrNss
pJZsqT9lkj3+BLKwL7X5TmFNbB7fTLditheWjfOtBLINieJuijta1enG

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ECRaizEstado*

Issuer O: *SCEE*

Issuer C: *PT*

Subject CN: *ECCE*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

Valid from: *Mon Jul 03 16:27:00 CEST 2006*

Valid to: *Sat Jun 23 10:49:47 CEST 2018*

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:1D:D9:C0:E2:78:CD:5F:1F:6C:76:4C:3E:35:1B:43:47:01:9E:98:F7:27:A3:D4:A8:7A:C6:33:AC:82:63:F8:1B:6D:EA:85:DB:4C:C3:62:8C:BF:52:72:B9:04:D6:CF:95:E1:00:6A:B5:AD:49:EA:AF:91:0B:3F:3B:7E:F6:0B:A5:9A:AE:39:68:2A:E0:A5:A6:04:E3:BB:EB:96:06:02:8B:E2:9D:18:27:2A:89:34:3C:DA:97:5E:A4:EA:76:21:69:13:C8:47:8F:F7:2C:AA:AD:21:E3:A4:4D:BF:32:C4:C8:C0:E9:3B:2B:89:98:91:6A:B9:78:26:04:E5:D4:40:2B:BB:BE:81:82:BC:3E:E4:B9:98:4C:DE:AA:47:3C:A4:99:AF:CA:91:7D:2C:0F:BF:01:11:F2:3F:82:9A:2D:7E:E3:1B:4B:6F:6B:24:3D:C3:ED:B9:FE:AE:F4:10:C9:73:31:0D:7C:BA:BC:1A:71:4F:FA:10:F9:B7:D5:ED:52:53:81:DF:9A:36:A4:2E:FF:12:50:20:71:0D:9F:7F:FD:4D:54:9B:F1:36:67:34:6C:E5:B7:A8:37:32:F0:64:8F:D8:07:F9:55:C3:53:89:1D:0A:48:FE:97:22:E6:2A:5E:EF:4C:8E:FB:0D:6B:1B:37:2A:CF:C6:67:69:A2:D8:BF:7D:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *59:0B:66:CC:FA:7B:16:98:68:0E:F6:5C:00:F3:B9:AD:E9:A6:3A:74*

Authority Key Identifier *71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.ecee.gov.pt/dpc

Authority Info Access *https://ocsp.ecee.gov.pt*

CRL Distribution Points *http://crls.ecee.gov.pt/crls/ARL.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *75:37:3A:D4:96:8B:3E:E9:64:96:5A:C8:85:CF:0A:4D:7A:5C:FF:7E:68:C2:D5:A5:D3:B9:F4:97:F8:50:72:96*

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

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

Status Starting Time *2018-06-23T23:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://www.ecce.gov.pt*

URI *[pt]* *https://www.ecce.gov.pt*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.1.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCE (CA-Qualified Certificates)*

Name *[pt]* *ECCE (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *ECCE*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *WQtmzPp7FphoDvZcAPO5remmOnQ=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.1.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *ECCE (CA-Qualified Certificates)*

Name *[pt]* *ECCE (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *ECCE*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *WQtmzPp7FphoDvZcAPO5remmOnQ=*

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

Status Starting Time *2007-07-04T00:00:00Z*

1.1.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.2 - Service (withdrawn): ECCE 001 (CA-Qualified certificates)

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]* *ECCE 001 (CA-Qualified certificates)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *122123656087890522745430251460747588937*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFQDCCAyigAwIBAgIQW+ApHj8MkelVitA9MDf1STANBgkqhkiG9w0BAQsFADAzMQswCQYDVQQG
EwJQVDENMAsGA1UECgwEU0NFRTEVMBMGA1UEAwwMRUNSYWI6RXN0YWRvMB4XDTE1MDYyNDE1NDM1
N1oXDTI3MDYyNDE1NDM1N1owQjELMAkGA1UEBhMCUFQxDTALBgNVBAoMBFNDRUUxETAPBgNVBAsM
CEVDRXN0YWRvMREwDwYDVQQDDAhFO0NFIDAwMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAMD1mmAQ6iiApgcE9KCvKGTn/3P3WNbrmGquwoUZqDPINSeopd1ifACyqPs0hXSCVbjlEVac
sJaQ4jUPAPxGs6/XO2SF49K1M+F02n5QVBDOm7RInu4c5uz6uUp/z0z/51OxBVjT0KCJ2aGnLB2v
o2atLcyP4pgqeb6lPT3HcTPNTnTnYytAPM2Kj82mJWfMNMop/3qwlaz2SYjvG5ZJNNewGLqOqC++
4LYkmNVYaU/r5hX/8p4dlQg+zEP1bQeol8rUQbbtmJ7ZRkD5H01pUngL+1rPE+0V+/qz787ib6jV
A513jes8bSxAR9QjMuhdab46q8FBdMqyMPTwqrMYjfcCAwEAAaOCAT8wggE7MA8GA1UdEwEB/wQF
MAMBAf8wHQYDVR0OBBYEFOMa2JoMNlrUDiOsDphvgVKeLI0FMB8GA1UdIwQYMBaAFHF/Nd71d3Ft
HRKc4ZCkuvCpg4+AMA4GA1UdDwEB/wQEAwIBBjA7BgNVHSAENDAyMDAGBFUdIAAwKDAmBggrBgEF
BQcCARYaaHR0cDovL3d3dy5lY2VlLmdvdi5wdC9kcGMwZAYIKwYBBQUHAQEEWDBWMCMGCCsGAQUF
BzABhhdodHRwOi8vb2Nzc5lY2VlLmdvdi5wdDAvBggrBgEFBQcwAoYjaHR0cDovL3RydXN0LmVj
ZWUuZ292LnB0L2VjcmFpei5jcnQwNQYDVR0fBC4wLDAqoCigIoYkaHR0cDovL2NybHMuZWNlZS5n
b3YucHQvY3Jscy9BUkwuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQDRjGHFQLgpVdEaDuyC7VwwzRBP
qMhhY5mHs84tZL6d1BAUKW6qzLrEB370xEnBgWdxE5dU9jKSZxFeZau9Mkt5Yau3fi2jrYwhacFa
+jzeBxthAfVGGD/x9zQU8wCfocrbC7Sfd6t9z7+0drAyAg0A/RwdBjMsrAhHpxxMf5m+5HxlaxY2
y5C85ZG0Ru/S4paBDHkIK1PNQdPyxrU8QgH/UD6slz48gqa5gFijyoaExquCmciX1T5CmxqDHc+c
4O6X3iQOB8ZAx2RYsENKJG3DM+thp1yo8mZxEsan1yJcQY4OpKHNvKAq0g9UNyu93ZL/Fn9okVQu
FNXp9L9APZsL8p70hAFt2aoThQATaQSRjtb99beGbm5DYvhWh7oli4QnvqmgA/YUrRBz3w0WGCqz
+lODVNXKCKJLPlWwImeil4YXNbK8Nr+XOvb/XT/yxV09IZBV+hXK/MwQ6dZLbEVwn84WPKiuM3ny
QzuEYJHD1iCLy8RM9GlM3INmTL/Wt6mfX66o4+OsR6ZG2PNZxPaPUetZAgXVCM1T1iL+H7z2aQ7
OIjZ1BMo2F27x/QpZSBMIYITZIqxRm0kTEyo90wi14VXIp6scGLcTj6fIE9SD4zOaXKkFg8gc5uz
fUtUg2u1fVvqdkywbF1PHgMud9e7scWuX/xLeKCvuTp+Arb78A==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ECRaizEstado*

Issuer O: *SCEE*

Issuer C: *PT*

Subject CN: *ECCE 001*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

Valid from: *Wed Jun 24 17:43:57 CEST 2015*

Valid to: *Thu Jun 24 17:43:57 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:C0:F5:9E:60:10:EA:28:80:A6:A7:04:F4:A0:AF:28:64:E7:FF:73:F7:58:D6:EB:98:68:2E:C2:85:19:80:33:E5:35:27:A8:A5:DD:62:7C:00:B2:80:FB:34:85:74:82:55:B8:C8:11:56:9C:B0:96:90:E2:35:0F:00:FC:46:B3:AF:D7:3B:64:85:E3:D2:B5:33:E1:74:DA:7E:50:54:10:CE:9B:B4:48:9E:EE:1C:E6:EC:FA:B9:4A:7F:CF:4C:FF:E7:53:B1:06:F2:53:D0:A0:A3:D9:A1:A7:2C:1D:AF:A3:66:AD:2D:CC:8F:E2:98:2A:79:BE:A5:3D:3D:C7:71:33:CD:4E:74:E7:63:2B:40:3C:CD:8A:8F:CD:A6:25:67:CC:34:CA:29:FF:7A:B0:95:AC:F6:49:88:EF:18:96:49:34:D7:B0:18:BA:BE:AB:2F:BE:E0:B6:24:98:D5:58:69:4F:EB:E6:15:FF:F2:9E:1D:95:08:3E:CC:43:F5:6D:07:A8:97:CA:D4:41:B6:ED:98:9E:D9:46:40:F9:1F:4D:69:52:78:0B:FB:5A:CF:13:ED:15:FB:FA:B3:EF:CE:E2:6F:A8:D5:03:9D:77:8D:EB:01:6D:2C:40:47:D4:23:32:E8:5D:69:BE:3A:AB:C1:41:74:CA:B2:30:F4:F0:AA:B3:18:8D:F7:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *E3:1A:D8:9A:0C:36:5A:D4:0E:23:AC:0E:98:6F:81:52:9E:2E:5D:05*

Authority Key Identifier *71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.ecee.gov.pt/dpc

Authority Info Access *http://ocsp.ecee.gov.pt*

http://trust.ecee.gov.pt/ecraiz.crt

CRL Distribution Points *http://crls.ecee.gov.pt/crls/ARL.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DA:AB:2E:45:04:FD:54:EF:7F:99:BB:49:E1:4C:3D:63:A6:DD:FF:8A:F5:60:4D:5B:A1:D0:1F:31:2B:52:04:E4*

Service Status

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

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

Status Starting Time

2026-06-22T15:30:00Z

Scheme Service Definition URI

URI *[en]* *https://www.ecce.gov.pt*

URI *[pt]* *https://www.ecce.gov.pt*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.2.3 - Extension (not critical): TakenOverBy

TakenOverBy

URI [en] *https://www.ecce.gov.pt/*

TSP Name

Name [en] *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name [en] *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.2.4 - History instance n.1 - Status: granted

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

Service Name

Name [en] *ECCE 001 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 001*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *4xrYmgw2WtQOI6wOmG+BUp4uXQU=*

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

Status Starting Time *2025-03-01T00:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.2.4.3 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.2.5 - History instance n.2 - Status: granted

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

Service Name

Name *[en]* *ECCE 001 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 001*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *4xrYmgw2WtQOI6wOmG+BUp4uXQU=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.2.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.2.6 - History instance n.3 - Status: accredited

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

Service Name

Name *[en]* *ECCE 001 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 001*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *4xrYmgw2WtQOI6wOmG+BUp4uXQU=*

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

Status Starting Time *2015-06-24T23:00:00Z*

1.2.6.6 - Extension (critical): Qualifiers [QCStatement, QCWithSSCD]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

1.3 - Service (granted): ECCE 002 (CA-Qualified certificates)

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]* *ECCE 002 (CA-Qualified certificates)*

Name *[pt]* *ECCE 002 (CA-Qualified certificates)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *248750055077206540935288537363947247 34*

X509 Certificate

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

MIIFsjCCA5qgAwIBAgIQErbAdcuQTs5fAzuj7AYVfjANBgkqhkiG9w0BAQsFADBiMQswCQYDVQQG
EwIQVDE4MDYGA1UECgwvU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGV0csOzbmlj Y5BkbyBF
c3RhZG8xGTAXBgNVBAMMEEVDUmFpekVzdGFkbyAwMDIwHhcNMjAwNzA2MTQ1NjM1WhcNMzIwNzA2
MTQ1NjM1WjB+MQswCQYDVQQGEwJQVDE6MDgGA1UECgwxQ2VudHJlvlGRIlEdlc3TDo28gZGEgUmVk
ZSBjbmZvcm3DoXRpY2EgZG8gR2922XJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwlRUNFc3Rh
ZG8xETAPBgNVBAMMCEVDQ0UgMDAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0meT
Z9cqzdX1WuM1aOEIeKybAu6uZ2OSfn0lbAaDLPhzq2eifbzVzFz9ATi/lWffmcXkFyhnMk4sEe
xA+15LH9R6gHBvlpG52RnYTKH7zjuNtrLhQY7NFFo4DOGdTvVNuPHus+ujLxNlUq1Eer7Kelhk65
Q57WrEWxo9T04hbB6i9bkee/Cj95lMe7OFkMk5cagB5lIHV1X0o0fQb13kiufki5ugoQgp37nKuB
Gs7EJYSefJUxace7yiGcJQjDTpGq9tlPpNWfK9u6hQPgGzKjBYbJ+I3/h+tBLUaD8z/qP9gjSos
s5p3lE+Y2PjBcn3qv68dwIlbpr9rorcrZQ(DAQABo4IBRjCCAUIwDwYDVR0TAQH/BAIwAwEB/zAd
BgNVHQ4EFgQUOCfk5/4aGOjrRCdpKtiB7PmlGRswHwYDVR0jBBgwFoAU/7+FOkGstaY+I1owpSVK
+pA2FeUwDgYDVR0PAQH/BAQDAgEGMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpo
dHRwOi8vd3d3LnNiZWUuZ292LnB0MDIGCCsGAQUFBzAChiZodHRwOi8vdHJ1c3QuZWNlZS5nb3Yu
cHQvZWNyYWl6MDAyLmNydDA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3Jscy5lY2VlLmdvdi5w
dC9jcmxzL0FSTC0wMDIuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQBps1tL7aY1Auv5tkEwpUP64GVA
3stpyZn/ojSXyDbji0a1u4ZKkIWRZXNdYN5RdeCSmn1wiR1fVqftMB6w4ro/H7jGsJnkOtgcva4c
qv2Q1EhDqSMrG36zm3Gf7ic1HDgHtBDsGHO7nRjJo7XJwnQ5jsVeojtpHb5ZdkDbj5ZQQdinv4j
XL/rQMDqEgDmXgTeQQ/y5B7UIK6PowiK4gNNxUXilk0/NYQyF2HJ5qKShy2MmXX63q+gIddXgve6
QFqtZr64dgyiZi6C4C10PYdpv4P0q+cgxJFLFJUxz8fNvusIenDLwxZLC6s5v0BgoC98xO/rP0mF
XhSodXXR4YvjrPktom5IMyMZQ6eRXF03hjOdwKQkmMpMPYdsMxNGcvSfHzlRB6nhPlFpNXvmfNmL
Tcygc5/4WkJyR8aLvMesqC0EDXyX+vpcv3UwTGtwzPj31690Q+GBSGNudYuUa/d/Lx52I6p3g0On
7ze9PpMbzyfEajuit9ThNL3VG4sQyeL+bPR0lcY9TdrS7ixPflkv1UcB2NBifD2zpVEMSl3fN2Qs
CF+AiMkWCuFLOIWCGvLF8achHOjqRyBZJYQlHW1dr/CLeX/HmqECCbtGoZl+RoI1xrvcBkvfRotq
RUE0l99AylSxm9Tb746SyRgoSb+XGwC/aB4Rqux3Yx3VK5GlxQ==

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

Signature algorithm: *SHA256withRSA*

Issuer CN: *ECRaizEstado 002*

Issuer O: *Sistema de Certificação Eletrónica do Estado*

Issuer C: *PT*

Subject CN: *ECCE 002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

Valid from: *Mon Jul 06 16:56:35 CEST 2020*

Valid to: *Tue Jul 06 16:56:35 CEST 2032*

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:D2:67:93:67:D7:2A:CD:D5:F5:5A:E3:35:6B:41:08:7A:4C:9B:02:EE:AE:CD:9
D:BE:49:F9:F4:21:B0:1A:0C:B3:E1:CE:0D:9E:B9:F6:F3:66:F6:45:CF:D0:13:BB:F9:56:7D:F9:9C:5E:41:72:86:73:24:E2:C1:1E:C4:0F:B5:E4:B1:FD:47:AB:07:06:F9:69:1B:9D:91:9D:84:CA:
1F:BC:E3:B8:DB:6B:2E:14:18:EC:D1:45:A3:80:CE:19:D4:EF:54:DB:BF:1E:EB:3E:BA:32:F1:34:85:2A:D4:47:AB:EC:A7:A5:86:4E:B9:43:9E:D6:AC:45:B1:A3:D4:F4:E2:16:C1:EA:2F:5B:91:E
7:BF:0A:3F:79:20:C7:BB:38:59:0C:93:97:1A:80:1E:65:20:75:75:5F:4A:34:7D:06:F5:DE:48:AE:7E:48:B9:BA:0A:10:AA:9D:FB:9C:AB:81:19:2E:C4:25:84:9E:7C:95:31:69:C7:BB:CA:21:9C:
25:08:C3:4E:91:AA:F6:D9:4F:A4:D5:9F:2B:DB:BA:85:03:E0:1B:32:A3:05:86:C9:DF:E9:77:26:1F:AD:04:B5:1A:0F:CC:FF:A8:FF:60:8D:2A:2C:B3:9A:77:20:4F:98:D8:F8:C1:72:7D:EA:BF:A
F:1D:C0:89:5B:A6:BF:6B:A2:B7:2B:65:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *39:C7:E4:E7:FE:1A:19:08:EB:44:27:69:2A:D8:81:EC:F9:A5:19:1B*

Authority Key Identifier *FF:BF:85:3A:41:AC:B5:A6:3E:23:5A:30:A5:25:4A:FA:90:36:15:E5*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/rep

Authority Info Access

http://ocsp.ecee.gov.pt

http://trust.ecee.gov.pt/ecraiz002.crt

CRL Distribution Points *http://crls.ecee.gov.pt/crls/ARL-002.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:25:A2:2B:AC:4D:9F:27:A7:25:55:AF:6A:FC:A4:53:C7:0F:10:F4:9C:C4:14:C8:CB:2E:79:EF:8C:E2:92:C6*

X509SubjectName

Subject CN: *ECCE 002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *Ocfk5/4aGQjrRCdpKtiB7PmlGRs=*

Service Status

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

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

Status Starting Time

2025-03-01T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://www.ecce.gov.pt*

URI *[pt]* *https://www.ecce.gov.pt*

1.3.1 - Extension (not critical): Qualifiers [QCForESig]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

1.3.2 - Extension (not critical): Qualifiers [QCForESeal]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.3*

1.3.3 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.4 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.5 - Extension (not critical): TakenOverBy

TakenOverBy

URI [en] *https://www.ecce.gov.pt/*

TSP Name

Name [en] *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name [en] *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.3.6 - History instance n.1 - Status: granted

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

Service Name

Name [en] *ECCE 002 (CA-Qualified certificates)*

Name [pt] *ECCE 002 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *Ocfk5/4aGQjrRCdpKtiB7PmlGRs=*

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

Status Starting Time *2020-08-23T23:00:00Z*

1.3.6.1 - Extension (not critical): Qualifiers [QCForESig]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

1.3.6.2 - Extension (not critical): Qualifiers [QCForESeal]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

1.3.6.3 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.6.4 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.7 - History instance n.2 - Status: granted

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

Service Name

Name [en] *ECCE 002 (CA-Qualified certificates)*

Name [pt] *ECCE 002 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *Ocfk5/4aGQjrRCdpKtiB7PmlGRs=*

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

Status Starting Time *2020-08-09T23:00:00Z*

1.3.7.5 - Extension (critical): Qualifiers [QCStatement, QCForESig, QCWithQSCD, QCForESeal]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

Description

1.3.7.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.7.7 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.3.8 - History instance n.3 - Status: granted

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

Service Name

Name [en] *ECCE 002 (CA-Qualified certificates)*

Name [pt] *ECCE 002 (CA-Qualified certificates)*

Service digital identities

X509SubjectName

Subject CN: *ECCE 002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *Ocfk5/4aGQjrRCdpKtiB7PmlGRs=*

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

Status Starting Time *2020-07-14T23:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

Description

1.3.8.9 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

1.4 - Service (withdrawn): ECCE - 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.*

Service Name

Name *[en]* *ECCE - TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *104095349347578371425405445008439040031*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFKzCCBBOgAwIBAgIQTlAI+EADSXlfYNa8CNrYHzANBgkqhkiG9w0BAQUFADB+MQswCQYDVQQG
EwJQVDE6MDgGA1UECgwxQ2VudHJyIGRlIEdlc3TDo28gZGEgUmVkZSBlbmZvcm3DoXRpY2EgZGBg
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3RhZG8xETAPBgNVBAMMCEVDQ0Ug
MDAyMB4XDTIwMDkxNTE0NTkwOFoXDTIzMDkxNTE0NTkwOFowga8xCzAJBgNVBAYTAlBUMTowOAYD
VQQKDDFDZW50cm8gZGUgR2VzdMOjby8kYSBSZWRlIEluZm9ybcOhdGljYSBkbyBHb3Zlcm5vMQ0w
CwYDVQQLDARTQ0VfMREwDwYDVQQLDAhFQ0VzdGFkbzEuMC0GA1UECwwmKWV5QaWRhZGUgQ2VydGlm
aWNhZG9yYSBDb211bSBkbyBFc3RhZG8xETAPBgNVBAMMCEVDQ0UtVFNBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkQvkjlF+4vuytT56ely1z3hD8qblZvQCtqkSzt3BYtvGtly7kMAI
R0oiBCAL3heGKTGx4nYj3yPfvcXTQIl12tTQfyamOGk0jBy0ocie2Fc0DFkUsTpRx44wTlEOqaEB
C25CFI+UUyGibNQ5npjtA8e0fD9YfFi5eL59CwZHjw0uQCrqePuTBuR75/Xfr7ZnYqU4bfnspy5r
NwWc26Pjn3wiGLYcLf4k5mUR6dIlUGrVA2gnZtwoGorBsjiLyntciwaGqeVfrWBJoGRu548Wqt7
Qc8BO8cWavTJlZj5PjRMZKlgisCM6HlNbYmcLPTUeKZsWnH0heSekh61Y/AMgQIDAQABo4IBcTCC
AW0wGAYlKwYBBQUHAQMEDDAKMAgGBgQAjkYBATAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAww
CgYlKwYBBQUHAwgwHQYDVR0OBBYEFPSozQO1u5CZjYj7y22WKoswjaMB8GA1UdIwQYMBaAFDnH
5Of+Ghki60Qna5rYgez5pRkbMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpodHRw
Oi8vd3d3LmVjY2UuZ292LnB0L2RwYzBmBggrBgEFBQcBAQRaMFgwIwYIKwYBBQUHMAGGF2h0dHA6
Ly9vY3NwLmVjY2UuZ292LnB0MDEGCCsGAQUFBzAChiVodHRwOi8vdHJ1c3QuZWNjZS5nb3YucHQv
ZWNjZS0wMDEuY3J0MAkGA1UdEwQCMAAwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2NybHMuZWNj
ZS5nb3YucHQvY3Jscy9jcmwtMDAyLmNybDANBgkqhkiG9w0BAQUFAAOCAQEARZ0kS/rnU4l48R/xxb
nbqxai2lC5gAsb0tC66hbvu4beBNdN1nPYTkGaVxcFmQt+WJHez88DUK0d6/nAcvzsGq+7EhsRMG
dAlBXgRUGn/s84gnHxQHSiTKtrxMmTibhUpR1RVeGCpFPFSQlfGljNr+uCwFHmLit67E0cuzBetU
qjghxkPbAWaxNnHqkZcm/Rf1T9BW/LpmKu21Hb5wMD2XDYnK+aYjTwcw8N0rvaiSBRRPYWwFstOl
19HqT5YABxgwwlZjBuZFTlPlbSUjrZOhICl2VM2YOAVSZuJaOoJ0YB8Q6UZNuGBA05XKEC1S5YU
Aok7hlmiW/BtRWm6kfjNBQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN:	*ECCE 002*
Issuer OU:	*ECEstado*
Issuer OU:	*SCEE*
Issuer O:	*Centro de Gestão da Rede Informática do Governo*
Issuer C:	*PT*
Subject CN:	*ECCE-TSA*
Subject OU:	*Entidade Certificadora Comum do Estado*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*
Valid from:	*Tue Sep 15 16:59:08 CEST 2020*
Valid to:	*Fri Sep 15 16:59:08 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:02:82:01:01:00:91:0B:E4:8C:81:7E:E2:FB:B2:B5:3E:7A:78:8C:B5:CF:78:43:F2:A6:C8:66:F4:02:B6:A9:12:CE:DD:C1:62:DB:C6:B6:5C:BB:90:C0:08:47:4A:22:04:20:0B:DE:17:86:29:31:B1:E2:76:09:DF:23:DF:BD:C5:D3:40:82:35:DA:D4:D0:7F:26:A6:38:69:34:27:CC:B4:A1:C8:9E:D8:57:34:0C:59:14:B1:3A:51:C7:8E:30:4C:81:0E:A9:A1:01:0B:64:82:14:8F:94:53:21:A2:6C:D4:39:9E:92:6D:03:C7:B4:7C:3F:58:7C:59:79:78:BE:7D:0B:06:47:8F:0D:2E:40:2A:EA:78:FB:93:06:E4:7B:E7:F5:DF:AF:B6:67:62:A5:38:6D:F9:EC:A7:2E:6B:37:05:9C:DB:A3:E3:9F:7C:22:88:62:D8:70:B7:F8:93:99:94:47:A7:65:95:41:BF:54:0D:A0:9D:9B:70:A0:6A:2B:06:C2:62:2F:29:ED:72:2C:1A:1A:A7:95:7F:F5:81:26:81:91:BB:9E:3C:5A:AB:7B:41:CF:01:3B:C7:16:6A:F4:E3:21:92:79:3C:94:4C:66:49:60:8A:C0:8C:E8:79:4D:6D:89:9C:2C:F4:D4:78:A6:6C:5A:71:F4:85:E4:9E:92:1E:B5:63:F0:0C:81:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*F4:A8:CD:04:35:BB:90:99:8D:82:58:8F:BC:B6:D9:62:A8:B3:08:DA*
Authority Key Identifier	*39:C7:E4:E7:FE:1A:19:08:EB:44:27:69:2A:D8:81:EC:F9:A5:19:1B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-001.crt*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/crl-002.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *34:8C:B9:B1:1A:89:79:94:62:28:97:08:A8:DC:35:0B:23:B1:BD:38:83:36:CE:63:5D:B2:0D:CC:63:81:13:6B*

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *9KjNBDW7kJmNgliPvLbZYqizCNo=*

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

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

Status Starting Time *2020-11-09T00:00:00Z*

1.4.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCE - TSA*

Service digital identities

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *9KjNBDW7kJmNgliPvLbZYqizCNo=*

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

Status Starting Time *2020-09-21T23:00:00Z*

1.5 - Service (withdrawn): ECCE-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.*

Service Name

Name *[en]* *ECCE-TSA*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *139594263648484130028220906267282365951*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFKzCCBBOgAwIBAgIQaQTgkvdp8lRfpB0xJjXd/zANBgkqhkiG9w0BAQUFADB+MQswCQYDVQQG
EwJQVDE6MDgGA1UECgwxQ2VudHJvIGRlIEdlc3TDo28gZGEgUmVkZSBjbmZvcm3DoXRpY2EgZGBg
R29ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3RhZGBxETAPBgNVBAMMCEVDQ0Ug
MDAyMB4XDTIwMTEwNTE1NDEzN1oXDTIzMTEwNTE1NDEzN1owga8xCzAJBgNVBAYTAlBUMTowOAYD
VQQKDDFDZW50cm8gZGUgR2VzdMOjbyBkYSBSZWRlIEluZm9ybcOhdGljYSBkbyBHb3Zlcm5vMQ0w
CwYDVQQLDARTQ0VfMREwDwYDVQQLDAhFQ0VzdGFkbzEvMC0GA1UECwwmRW50aWRhZGUgQ2VydGlm
aWNhZG9yYSBDb211b5BkbyBFc3RhZG8xETAPBgNVBAMMCEVDQ0UtVFNBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEApNi8BaPOXjvCtvUcnRtBhP3awpxvz8SqNIAy4HlAlAfeb5qZdiTr
CpiNKf7OKn4zFtxxp+X5jaM4bqnDXsZzbQxji85iPuTWG7v8OCsJ6Cd4BczeCkej5/Cqqxj7mygU
7iT8qjV/WhGG7g7a+D2WQVKu1tuZwYvDFRFCzP7EYHNghPjkcUEyT/vxTloNaRA9XnjLsVbvUiCx
0JDKQrupWgLB25xyzurEifRQNck8JOXQCdVqUssMe/BjydD8gGVnnXlnbCjhkCBpccRlxP78uzq5Fy
F2vZX8kbExrORRJKu1dYrhGns8p9K5WTtLnUEt6Fd+5XQaGVd2zOqNZEiBTJFwIDAQABo4IBcTCC
AW0wGAYIKwYBBQUHAwgwHQYDVR0OBBYEFOWXQ4M9gvHCUGgiSaVEevrNZjj2MBBGA1UdIwQYMBaAFDnH
5Df+GhkI60Qna5rYqez5pRkbMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpodHRw
Oi8vd3d3LmVjY2UuZ292LnB0L2RwYzBmBggrBgEFBQcBAQRaMFgwIwYIKwYBBQUHMAGGF2h0dHA6
Ly9vY3NwLmVjY2UuZ292LnB0MDEGCCsGAQUFBzAChiVodHRwOi8vdHJ1c3QuZWNjZS5nb3YucHQv
ZWNjZS0wMDluY3J0MAkGA1UdEwQCMAAwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2NybHMuZWNj
ZS5nb3YucHQvY3jscy9jcmwtMDAyLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAEvlyXGdu8Y3r8L6d
HU0Vu9p7Q8+Bce5QeVraUQ083Cxlq70hpiFr9GHBf1PlVZXbJDRBmzTvHgi0q63fcf8QeCU7OBJ0
nzGSJEPSacMGdpORtOQzDVc9oXSzvNS6CanUEKml5ral5TKiMFIHxxXu4CPUUNTf0CF3cwimniN
6Vr/w+fb9yLJohoVFv0clNg6fHdY3NsI5TW3GjYSZHCn6ofaqR2vb0VuMzfOtNHTbKg9VSzSnM5t
t2o9/caAqU4eDnoeyK53cOny08au3xFTnGQBtPYDS1AxCJr/0In+OkVt7c2LJbfY79CXLPAozB3T
Ld3KWxxCA8GibykKjkkufQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ECCE 002*

Issuer OU: *ECEstado*

Issuer OU: *SCEE*

Issuer O: *Centro de Gestão da Rede Informática do Governo*

Issuer C: *PT*

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*
Valid from:	*Thu Nov 05 16:41:37 CET 2020*
Valid to:	*Sun Nov 05 16:41:37 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:A4:D8:BC:05:A3:CE:5E:3B:C2:B6:F5:1C:9D:1B:41:84:FD:DA:C2:9C:6F:CF:C4:AA:36:50:32:E0:72:00:20:07:DE:6F:9A:99:76:24:EB:0A:98:8D:29:FE:CE:2A:7E:33:16:DC:71:A7:E5:F9:8D:A3:38:6E:A9:C3:5E:C6:73:6D:0C:63:8B:CE:62:3E:E4:D6:1B:BB:FC:38:2B:09:E8:27:78:05:CC:DE:0A:47:A3:E7:F0:AA:AB:18:FB:9B:28:14:EE:24:FC:AA:35:7F:5A:11:86:EE:0E:DA:F8:3D:96:41:52:AE:D6:DB:99:C1:8B:C3:15:11:42:CC:FE:C4:60:73:6A:84:F8:E4:71:41:32:4F:FB:F1:4C:8A:0D:69:10:3D:5E:78:CB:B1:56:EF:52:20:B1:D0:90:CA:42:BB:A9:5A:02:C1:DB:9C:72:CE:EA:C4:89:FB:50:35:C9:01:24:E5:D0:09:D5:6A:52:CB:0C:7B:F0:63:C8:3F:20:19:59:97:96:76:C2:8E:19:02:06:97:1C:44:8C:4F:EF:CB:B3:AB:91:72:17:6B:D9:5F:C9:1B:13:1A:CE:45:12:4A:BB:57:58:AE:11:A7:B3:CA:7D:2B:95:93:B4:B9:D4:12:DE:85:77:EB:17:41:A1:95:77:6C:CE:A8:D6:44:88:14:C9:17:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*E5:97:43:83:3D:82:F1:C2:50:68:22:49:A5:44:7A:FA:CD:66:32:76*
Authority Key Identifier	*39:C7:E4:E7:FE:1A:19:08:EB:44:27:69:2A:D8:81:EC:F9:A5:19:1B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-002.crt*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/crl-002.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*6A:05:F5:1A:ED:12:9D:5F:A4:2B:DA:D5:1D:7C:AC:73:36:D9:9D:66:7D:5F:59:45:DE:0C:93:37:DE:D5:94:2C*

X509SubjectName

Subject CN:	*ECCE-TSA*
Subject OU:	*Entidade Certificadora Comum do Estado*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *5ZdDgz2C8cJQaCJJpUR6+s1mMnY=*

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

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

Status Starting Time *2025-03-01T00:00:00Z*

1.5.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCE-TSA*

Service digital identities

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *5ZdDgz2C8cJQaCJJpUR6+s1mMnY=*

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

Status Starting Time *2020-11-09T00:00:00Z*

1.6 - Service (granted): ECCE- 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.*

Service Name

Name *[en]* *ECCE- TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *148941828192798839136791504379054664909*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFLDCCBBSgAwIBAgIQcA0nFp13JpNl/aUKcTgszTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQG
EwlQVDE6MDQrGA1UECqwxQ2VudHJlvIGRIlEdlc3TDo28gZGEgUmVkZSBlbmZvcm3DoXRpY2EqZGB8g
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3Rhi2G8xETAPBgNVBAMMCEVDQ0VR
MDAxMB4XDTI0MDMyMjE1MzQzNFoXDTI5MDMyMjE1MzQzNFowga8xCzAJBgNVBAYTAlBUMTowOAYD
VQQKDDFDZW50cm8gZGUgR2VzdMOjbyBkYSBSZWRlIEluZm9ybcOhdGljYSBkbyBHb3Zlcm5vMQ0w
CwYDVQQLDARTQ0VfMREwDwYDVQQLDAhFQ0VzdGFkbzEvMC0GA1UECwwmRW5aWRhZGUgQ2VydGlm
aWNhZG9yYSBDb211bSBkbyBFc3RhZG8xETAPBgNVBAMMCEVDQ0UtVFNBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAyQ6UB/BZ/p4HpGuXjBAES+W4CJ2P/WCBSaHffCrnD4lR5L3XPKdF
5M9KO3a86n+I2noHJQle5PH//cBnfGtzPRYHGFUSpi2ec49seEjkcxGkuc8D8l0KAiY6sUuVcWRd
EThM5eVkPcv3MZUe6sav7lGxukhyDdSUBBRFaMSbtjaAHLqxXwf9+cUiz2Sgpsd6QTKsDXGo8pE
VjctcLWfvB5oJq4ZXMCrZ6T4QIMkLBSnOAGRiAaR7xbZMoXXZqnIqOcptq8oNEoiq/ZNJVIXMr/N
g0GsKjMow+Ryk8i6XlK1uvbzW0IDzCFqZ3PC+Rdzud7c3wgMYbFA+ylBj7q7BQIDAQABo4IBcjCC
AW4wGAYIKwYBBQUHAQMEDDAKMAgGBgQAjkYBATAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwHQYDVR0OBBYEFChtM51T7ZsZY9ttsiKYfsL7t+uGMB8GA1UdIwQYMBaAFLee
QhEIEWFZu/+ajrFvJl1Hi1w5MDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpodHRw
Oi8vd3d3LmVjY2UuZ292LnB0L2RwYzBmBggrBgEFBQcBAQRaMFgwIwYIKwYBBQUHMAGGF2h0dHA6
Ly9vY3NwLmVjY2UuZ292LnB0MDEGCCsGAQUFBzAChiVodHRwOi8vdHJ1c3QuZWNjZS5nb3YucHQv
ZWNjZXEwMDEuY3J0MAkGA1UdEwQCMAAwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybHMuZWNj
ZS5nb3YucHQvY3Jscy9lY2NlcTAwM5SjcmwwDQYJKoZIhvcNAQELBQADggEBACwKgaVST1CYVra7
SzAIjxQlYAzAJQ3bl/l5HiwIdnoKTJbmMpZ+rImjrPr4hpfA85SFu1F32GX6QEK3f8JhjObRs3Rk
0njOL5Yf1OFTK6Q/Vu2BjWjqm/p98O/UwY3sGbK9jsO4CvtoCutmaOxPjGRRTut9eR6KFvcyMR7I
6waEP2auvNO4Xvz+/JcnybesGwQg97YO0e+YxUsWtb3aCHhvBSas+ZpHM2q8jD/6SA5nm5UN5hO2
2XUMopn+graNPWeYZDQTMsBztXu8hzK3Kvz+UYfDTC//UcrQ/wx5fr74j8tRjzup6ZJypxKCRb/g
Is0HIlOeAh5IgRak4raVJi0=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ECCEQ001*

Issuer OU: *ECEstado*

Issuer OU: *SCEE*

Issuer O: *Centro de Gestão da Rede Informática do Governo*

Issuer C: *PT*

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

Valid from: *Fri Mar 22 16:34:34 CET 2024*

Valid to:	*Thu Mar 22 16:34:34 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:C9:0E:94:07:F0:59:FE:9E:07:A4:6B:97:8C:10:04:4B:E5:B8:08:9D:8F:FD:60:81:49:A1:DF:7C:2A:E7:0F:82:11:E4:BD:D7:3C:A7:45:E4:CF:4A:3B:76:BC:EA:7F:A5:DA:7A:07:25:02:1E:E4:F1:FF:FD:C0:67:7C:6B:73:3D:16:07:18:55:12:A6:2D:9E:73:8F:6C:78:48:E4:73:11:A4:B9:CF:03:F0:8D:0A:02:26:3A:B1:48:95:71:64:5D:11:38:4C:49:E5:64:3D:CB:F7:31:95:1E:EA:C6:AF:EE:51:B1:BA:48:72:0D:D4:94:04:14:45:68:C4:98:B6:36:80:1E:22:EA:C5:7C:1F:F7:E7:14:8B:3D:92:82:9B:1D:E9:04:CA:B0:35:C6:A3:CA:44:56:37:2D:70:B5:9F:BF:C4:A8:26:0E:19:5C:C0:AB:67:A4:F8:42:53:24:2C:14:A7:38:01:91:88:06:91:EF:16:D9:32:85:D7:DA:A9:E5:A8:E7:29:B6:AF:28:34:4A:22:AB:F6:4D:25:58:97:32:BF:CD:83:41:AC:2A:33:28:C3:E4:72:93:C8:BA:5E:52:B5:BA:F6:F3:5B:42:03:CC:21:6A:67:73:C2:F9:17:73:B9:DE:DC:DF:08:0C:61:B1:40:FB:22:01:8F:BA:BB:05:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*28:6D:33:9D:53:ED:9B:19:63:DB:6D:B2:22:98:7E:C2:FB:B7:EB:86*
Authority Key Identifier	*B7:9E:42:71:25:11:61:59:BB:FF:9A:8E:B1:6F:26:5D:47:EB:5C:39*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecceq001.crt*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/ecceq001.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DE:7D:78:73:09:ED:C3:AB:9F:51:35:85:85:17:80:A7:2B:0F:88:05:2A:C2:55:05:DE:63:B0:C1:A9:AB:08:D7*

X509SubjectName

Subject CN:	*ECCE-TSA*
Subject OU:	*Entidade Certificadora Comum do Estado*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*

X509SKI

X509 SK I	*KG0znVPtmxlj222yIph+wvu364Y=*

Service Status

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

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

Status Starting Time *2025-03-01T00:00:00Z*

1.6.1 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.6.2 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCE- TSA*

Service digital identities

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *KG0znVPtmxlj222yIph+wvu364Y=*

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

Status Starting Time *2024-03-26T12:08:24Z*

1.7 - Service (granted): ECCEQ001

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]* *ECCEQ001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *71675592042153430773023579451995511061*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFzjCCA7agAwIBAgIQNew3hrrhZANlnS68puTZFTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQG
EwJQVDE6MDgGA1UECgwxQ2VudHJvIGRlIEdlc3TDo28gZGEgUmVkZSBjbmZvcm3DoXRpY2EgZG8g
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3RhZG8xETAPBgNVBAMMCEVDQ0Ug
MDAzMB4XDTI0MDEwOTExMzIxMloXDTMwMDEwOTExMzIxMlowfjELMAkGA1UEBhMCUFQxOjA4BgNV
BAoMMUNlbnRvbyBkZSBhNZXN0w6NvIGRhIFlZGUgSW5mb3ltw6F0aWNhIGRvIEdvdmVybmBxDTAL
BgNVBAsMBFNDRUUxETAPBgNVBAsMCEVDRXN0YWRvMREwDwYDVQQDDAhFQ0NFUTAwMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMynuMnvo7K+86Ew2Iw9hhSrvz0yzCYb7yolG1dgnnzG
ouI4+29yKCvBvsMBA/3gqUj+v2ZiYnRQHesdinCsMWVk5j/148BgBdB00Up4b+qEzssPyu1rBM6f
RkIxCf0lGKYVkogXU1By4xoRic5T2PjFy+13duPjG1GYYp2z6Z95pAhEIAwMF0kd3P+lWdQ1QT
zV5sgWmuG0z8Ij6gERCGHqfyeA5PuRTIyTCpQWqqVQ4Ya8oebfD1c2POAwLTrb0rjrTYRE8+geY5
Y2rsH2/LVziTOWzRTBYzIPB6UugoFSjksN7GxWOM71ehEgpZX5ZFboLg7cblOpuhRsfgI2cCAwEA
AaOCAUYwggFCMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFLeeQnElEWFZu/+ajrFvjl1H61w5
MB8GA1UdIwQYMBaAFCJN91GM3oWGHVAFFixlAEMC2ckLMA4GA1UdDwEB/wQEAwIBBjA7BgNVHSAE
NDAyMDAGBFUdIAAwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5zY2VlLmdvdi5wdC9yZXAwZgYI
KwYBBQUHAQEEWjBYMCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5lY2NlLmdvdi5wdDAxBggrBgEF
BQcwAoYlaHR0cDovL3RydXN0LmVjY2UuZ292LnB0L2VjY2UtMDAzLmNydDA6BgNVHR8EMzAxMC+g
LaArhilodHRwOi8vY3Jscy5lY2NlLmdvdi5wdC9jcmxzL0VDQ0UtMDAzLmNydDANBgkqhkiG9w0B
AQsFAAOCAgEAMBGQs6n+Go/FPpcK1brJ5Lh3+bPTcI7af0j7N5RT7Px60twKTkFNj9G3j9qZ/vdV
xYGAonIOzb3JQlOQIVCMxI7yLQi3RSrRnHKkiYEOZgx0E2Owjqw+s5Bi18Fv4j39uWZZxAFjDxBp
n34Ci0UTnv1FiZ3dblhRw1bToh51u2NvdaajtrXKAwh+LwLPbZq+im7FpMPXrgdSiAf7hkzlcSf0
g0AZl8Y1iggCCPKn/j3gRFKp5lN/OlVu4izuTSXA5TBitW1Y+PxKyesb0uWHDkCqWEF1ZSFRFOj8
d/BKWke4ig64kIhBbxUXwZDaLcPlZoPORrNk+J8OmP9gMMazzhCvQLezm5U0SxE38qGeciNTwza/
wvc/IBaf7KNDf3P2t7lbQQHlTxQldAD8MFNETd8UkRIAz5zto/s9yEEdnq4qT6rU3ybi1vKyRfsv
fcCCpa8ZwU3ZbNOPZOlu5dmLepakldOZ8eJqJok6Xny7ig1Y+Wmooi8TOJb1BfKtSUtZL3+ssh6T
oaE3bh5OMWzyPuOI+n+tTrjtr9vYuFuq9Ka18VUHGmZu7dBQG6DAlYuPjKouZ4yGZ65E3HCTG02k
vD51h6pfmDi2hbak5gaUtHwsQ3dkQUZcJUQ84VCNZUklk1xe/8+iHJzO2Hc1fjfEjJNlWEvVplnI
BNkNKtaV8OI=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ECCE 003*

Issuer OU: *ECEstado*

Issuer OU: *SCEE*

Issuer O: *Centro de Gestão da Rede Informática do Governo*

Issuer C: *PT*

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C:	*PT*
Valid from:	*Tue Jan 09 12:32:12 CET 2024*
Valid to:	*Wed Jan 09 12:32:12 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:CC:A7:B8:C9:EF:A3:B2:BE:F3:A1:30:D8:8C:3D:86:14:AB:BF:3D:32:CC:26:1B:EF:2A:25:1B:57:60:9E:7C:C6:A2:E2:38:FB:6F:72:28:2B:C1:BE:C3:01:03:FD:E0:A9:48:FE:BF:66:62:62:74:50:1D:EB:1D:8A:70:AC:31:65:64:E6:3F:F5:E3:C0:60:05:D0:74:D1:4A:78:6F:EA:84:CE:CB:0F:CA:ED:6B:04:CE:9F:46:42:31:09:FD:34:18:A7:D8:56:4A:2A:FF:15:35:6F:2E:31:A1:18:9C:E5:3C:CF:8D:FC:BE:D7:77:6E:3C:91:B5:19:86:29:DB:3E:99:F7:9A:40:84:42:00:C0:C1:74:91:DD:CF:F8:85:9D:43:54:13:CD:54:AC:81:69:AE:1B:4C:FC:20:9E:A0:11:10:86:1E:A7:F2:78:0E:4F:B9:14:E5:C9:30:A9:41:6A:AA:55:0E:18:6B:CA:1E:6D:F0:F5:73:63:CE:03:02:D3:AD:BD:2B:8E:B4:D8:44:4F:3E:81:E6:39:63:6A:EC:1F:6F:CB:57:38:93:39:6C:D1:4C:16:33:20:F0:7A:52:E8:28:15:28:E4:B0:DE:C6:C5:63:8C:EF:57:A1:12:0A:59:5F:96:45:6E:82:E0:ED:C6:C8:3A:9B:A1:46:C7:E0:97:67:02:03:01:00:01*
Basic Constraints	*IsCA: true*
Subject Key Identifier	*B7:9E:42:71:25:11:61:59:BB:FF:9A:8E:B1:6F:26:5D:47:EB:5C:39*
Authority Key Identifier	*22:4D:F7:51:8C:DE:85:86:1D:50:05:14:8C:48:94:00:8C:D9:C9:0B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.scee.gov.pt/rep*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-003.crt*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/ECCE-003.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2F:A6:69:12:6F:5D:D1:5F:7F:56:78:65:8C:AB:49:D3:A9:EF:FB:E5:83:79:92:24:BA:9E:DA:CD:18:C3:32:90*

X509SubjectName

Subject CN:	*ECCEQ001*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*

X509SKI

X509 SK I	*t55CcSURYVm7/5qOsW8mXUfrXDk=*

Service Status

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

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

Status Starting Time

2025-06-11T11:00:00Z

1.7.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.7.2 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.7.3 - Extension (not critical): Qualifiers [QCStatement, QCForESig, QCWithQSCD]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

Description

1.7.4 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCEQ001*

Service digital identities

X509SubjectName

Subject CN:	*ECCEQ001*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*

X509SKI

X509 SK I	*t55CcSURYVm7/5qOsW8mXUfrXDk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2025-03-01T00:00:00Z*

1.7.4.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.7.4.2 - Extension (not critical): TakenOverBy

TakenOverBy

URI	*[en]*	*https://www.ecce.gov.pt/*

TSP Name

Name	*[en]*	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name	*[en]*	*Gabinete Nacional de Segurança*
Scheme Territory	*PT*	

1.7.5 - History instance n.2 - Status: granted

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

Service Name

Name *[en]* *ECCEQ001*

Service digital identities

X509SubjectName

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *t55CcSURYVm7/5qOsW8mXUfrXDk=*

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

Status Starting Time *2024-03-26T13:38:18Z*

1.7.5.3 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.8 - Service (granted): ECCEQ001

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]* *ECCEQ001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *716755920421534307730235794519955110 61*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFzjCCA7agAwIBAgIQNew3hrrhZANlnS68puTZFTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQG
EwlQVDE6MDgGA1UECgwxQ2VudHJvIGRlIEdlc3TDo28gZGEgUmVkZSBjbmZvcm3DoXRpY2EqZG8g
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3RhZG8xETAPBgNVBAMMCEVDQ0Ug
MDAzMB4XDTI0MDEwOTExMzIxMloxDTMwMDEwOTExMzIxMlowfjELMAkGA1UEBhMCUFQxOjA4BgNV
BAoMMUNlbnRyb3kiZSBHZXN0w6NvIGRlbFlJZGUgSW5mb3Jtw6F0aWNhIGRvIEdudmVybm8xDTAL
BgNVBAsMBFNDRUUxETAPBgNVBAsMCEVDRXN0YWRvMREwDwYDVQQDDAhFQ0NFUTAwMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMynuMnvo7K+86Ew2Iw9hhSrvz0yzCYb7yolG1dgnnzG
oul4+29yKCvBvsMBA/3gqUj+v2ZiYnRQHesdinCsMWVk5j/148BgBdB00Up4b+qEzssPyu1rBM6f
RkIxCf0GKfYVkogXtJ1By4xoRic5T2PjFy+13duPfG1GYYp2z6Z95pAhEIAwMF0kd3P+lWdQ1QT
zVSsgWmuG0z8Jl6gERCGHqfyeA5PuRTlyTCpQWqqVQ4Ya8oebfD1c2PQAwLTrb0rjrTYRE8+geY5
Y2rsH2/LVziTOWzRTBYzIPB6UugoFSjksN7GxWOM71ehEgpZX5ZFboLg7cblOpuhRsfgI2cCAwEA
AaOCAUYwggFCMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFLeeQnElEWFZu/+ajrFvjI1H61w5
MB8GA1UdIwQYMBaAFCJN91GM3oWGHVAFFixlACM2ckLMA4GA1UdDwEB/wQEAwIBBjA7BgNVH5AE
NDAyMDAGBFUdIAAwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5zY2VlLmdvdi5wdC9yZXAwZgYI
KwYBBQUHAQEEWjBYMCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5lY2NlLmdvdi5wdDAxBggrBgEF
BQcwAoYlaHR0cDovL3RydXN0LmVjY2UuZ292LnB0L2VjY2UtMDAzLmNydDA6BgNVHR8EMzAxMC+g
LaArhilodHRwOi8vY3Jscy5lY2NlLmdvdi5wdC9jcmxzL0VDQ0UtMDAzLmNybDANBgkqhkiG9w0B
AQsFAAOCAgEAMBGQs6n+Go/FPpcK1brj5Lh3+bPTcI7af0j7N5fR7Px60twKTkFNj9G3J9gZ/vdV
xYGAonIOzb3JQlOQIVCMxI7yLQi3R5rRnHKkiYEOZgx0E2Owjqw+s5Bi18Fv4j39uWZZxAFjDxBp
n34Ci0UTnv1FiZ3dblhRw1bToh51u2NvdaajtrXKAwh+LwLPbZq+im7FpMPXrgdSiAf7hkzlcSf0
g0AZI8Y1iggCCPKn/j3gRFKp5lN/OlVu4izuTSXASTBitW1Y+PxKyesb0uWHDkCqWEF1ZSFRFOj8
d/BKWke4tg64kfhBbxUXwZDaLcPjZoPORrNk+jB0mP9gMMazzhCvQLezm5Uo5xE38qGeciNTwza/
wvc/IBaf7KNDf3P2t7lbQQHlTxQldAD8MFNETd8UkRIAz5zto/s9yEEdnq4qT6rU3ybi1vKyRfsv
fcCCpa8ZwU3ZbNOPZOlu5dmLepakldOZ8eJqJok6Xny7ig1Y+Wmooi8Tojb1BfKtSUtZL3+ssh6T
oaE3bh5OMWzyPuOI+n+tTrJtr9vYuFuq9Ka18VUHGmZu7dBQG6DAlYuPjKouZ4yGZ65E3HCTG02k
vD51h6pfmDj2hbak5gaUtHwsQ3dkQUZcJUQ84VCNZUklk1xe/8+iHJzO2Hc1fJfEjNiWEvVplnI
BNkNKtaV8OI=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *ECCE 003*

Issuer OU: *ECEstado*

Issuer OU: *SCEE*

Issuer O: *Centro de Gestão da Rede Informática do Governo*

Issuer C: *PT*

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

Valid from: *Tue Jan 09 12:32:12 CET 2024*

Valid to: *Wed Jan 09 12:32:12 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:CC:A7:B8:C9:EF:A3:B2:BE:F3:A1:30:D8:8C:3D:86:14:AB:BF:3D:32:CC:26:1B
:EF:2A:25:1B:57:60:9E:7C:C6:A2:E2:38:FB:6F:72:28:2B:C1:BE:C3:01:03:FD:E0:A9:48:FE:BF:66:62:62:74:50:1D:EB:1D:BA:70:AC:31:65:64:E6:3F:F5:E3:C0:60:05:D0:74:D1:4A:78:6F:E
A:84:CE:CB:0F:CA:ED:6B:04:CE:9F:46:42:31:09:FD:34:18:A7:D8:56:4A:2A:FF:15:35:6F:2E:31:A1:18:9C:E5:3C:CF:8D:FC:BE:D7:77:6E:3C:91:B5:19:86:29:DB:3E:99:F7:9A:40:84:42:00:
C0:C1:74:91:DD:CF:F8:85:9D:43:54:13:CD:54:AC:81:69:AE:1B:4C:FC:20:9E:A0:11:10:86:1E:A7:F2:78:0E:4F:B9:14:E5:C9:30:A9:41:6A:AA:55:0E:18:6B:CA:1E:6D:F0:F5:73:63:CE:03:0
2:D3:AD:BD:2B:8E:B4:D8:44:4F:3E:81:E6:39:63:6A:EC:1F:6F:CB:57:38:93:39:6C:D1:4C:16:33:20:F0:7A:52:E8:28:15:28:E4:B0:DE:C6:C5:63:8C:EF:57:A1:12:0A:59:5F:96:45:6E:82:E0:
ED:C6:C8:3A:9B:A1:46:C7:E0:97:67:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *B7:9E:42:71:25:11:61:59:BB:FF:9A:8E:B1:6F:26:5D:47:EB:5C:39*

Authority Key Identifier *22:4D:F7:51:8C:DE:85:86:1D:50:05:14:8C:48:94:00:8C:D9:C9:0B*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.scee.gov.pt/rep

Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-003.crt*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/ECCE-003.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2F:A6:69:12:6F:5D:D1:5F:7F:56:78:65:8C:AB:49:D3:A9:EF:FB:E5:83:79:92:24:BA:9E:DA:CD:18:C3:32:90*

X509SubjectName

Subject CN:	*ECCEQ001*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*

X509SKI

X509 SK I	*t55CcSURYVm7/5qOsW8mXUfrXDk=*

Service Status

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

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

Status Starting Time

2025-10-02T18:00:00Z

1.8.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.8.2 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.8.3 - Extension (not critical): Qualifiers [QCStatement, QCForESeal, QCWithQSCD]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

Description

1.8.4 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCEQ001*

Service digital identities

X509SubjectName

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *t55CcSURYVm7/5qOsW8mXUfrXDk=*

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

Status Starting Time *2025-06-11T11:00:00Z*

1.8.4.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.8.4.2 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.8.4.3 - Extension (not critical): Qualifiers [QCStatement, QCForESig, QCWithQSCD]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

Description

1.8.5 - History instance n.2 - Status: granted

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

Service Name

Name [en] *ECCEQ001*

Service digital identities

X509SubjectName

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *t55CcSURYVm7/5qOsW8mXUfrXDk=*

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

Status Starting Time *2025-03-01T00:00:00Z*

1.8.5.4 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.8.5.5 - Extension (not critical): TakenOverBy

TakenOverBy

URI [en] *https://www.ecce.gov.pt/*

TSP Name

Name [en] *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name [en] *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.8.6 - History instance n.3 - Status: granted

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

Service Name

Name *[en]* *ECCEQ001*

Service digital identities

X509SubjectName

Subject CN: *ECCEQ001*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *t55CcSURYVm7/5qOsW8mXUfrXDk=*

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

Status Starting Time *2024-03-26T13:41:00Z*

1.8.6.6 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

1.9 - Service (granted): ECCE -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.*

Service Name

Name *[en]* *ECCE -TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *164711685833335138755819888902278867550*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFK2CCBBOgAwIBAgIQe+pRGWQ0Ar5lOSEVXMnqXjANBgkqhkiG9w0BAQUFADB+MQswCQYDVQQG
EwJQVDE6MDgGA1UECgwxQ2VudHJvIGRlIEdlc3TDo28gZGEgUmVk2SBjbmZvcm3DoXRpY2EgZG8g
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwlRUNFc3RhZG8xETAPBgNVBAMMCEVDQ0Ug
MDAyMB4XDTIzMTAyNTE0MDcxN1oXDTI4MTAyNTE0MDcxN1owga8xCzAJBgNVBAYTAlBUMTowOAYD
VQQKDDFDZW50cm8gZGUgR2VzdMOjbyBkYSBSZWRlIEIuZm9ybC0hdGlJYSBkby8Hb3Zlcm5vMQ0w
CwYDVQQLDARTQ0VFMREwDwYDVQQLDAhFQ0VzdGFkbzEvMC0GA1UECwwmRW50aWRhZGUgQ2VydGlm
aWNhZG9yYSBDb211bSBkbyBFc3RhZG8xETAPBgNVBAMMCEVDQ0UtVFNBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAqvReFTaTRzQiKggW55odtqcOSmXf5tydCjGlocDV/nR7lvnw4Kva
oW/BuR8NTmwW17Z/ieEF0WdactSAWEp2IsWwYcwM34yyOKA53SXwwGLN6Dt1ProIjG1xjMQ/5xcu
rrU/9yFgF9+BEKtecWJoHMNY4NqWYr4k8h/6pDqOhkZw+DuF90TrhpjiNP2W5EHWIVZgmHTzsyAi
92AN9rn9Cpdymeirfwtin Pn0xhCrtXPC9VCbQ8T23+tuEyOUq1svUhtYQq92ff9q7yWz9THO0PcTQ
XtuepY8karhjkaNKABXPv5NAkdZoiq92NrY8uvK8rE/uuqZRcs4Co0yJqTzX/wIDAQABo4IBcTCC
AW0wGAYIKwYBBQUHAQMEDDAKMAgGBgQAjkYBATAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwHQYDVR0OBBYEFK5cVGnxFyj32WRcnw+jdUDpsNvFMB8GA1UdIwQYMBaAFDnH
5Of+GhkI60QnaSrYgez5pRkbMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYGCCsGAQUFBwIBFhpodHRw
Oi8vd3d3LmVjY2UuZ292LnB0L2RwYzBmBggrBgEFBQcBAQRaMFgwIwYIKwYBBQUHMAGGF2h0dHA6
Ly9vY3NwLmVjY2UuZ292LnB0MDEGCCsGAQUFBzAChiVodHRwOi8vdHJ1c3QuZWNjZS5nb3YucHQv
ZWNjZS0wMDluY3J0MAkGA1UdEwQCMAAwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2NybHMuZWNj
ZS5nb3YucHQvY3Jscy9jcmwtMDAyLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAA6TjiBLiiFKzesS
J6ch81c4C86r4VeRPRDVJEv0sadaCGyKFyqgx26cPhAhdwCuGcALKZ1WfpSut4I2NNloUQTeHsHG
51wYdhUXXkxywDDWJAT9Cniv1eLgMiUVrjx1NbUUq19OWACHrWHeEnJqyj2omQ7S9zWEu2+DEZjP
urD3AKAGAVdluyWlyZYOdYOd7w+vUk1oAWAGAoERG90Xqb150ii0q0zVsn7rPc/heIrO+gHOIIo
/bDlD+p1RZJaBycLlq2lzPztm315hvjZDHAGS3JKMFMM6hvduTk4qqGVnr0t4SgROXmeQqAWYPrj
tuIQDdtJwZtxB1eCVYOoVA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ECCE 002*

Issuer OU: *ECEstado*

Issuer OU: *SCEE*

Issuer O: *Centro de Gestão da Rede Informática do Governo*

Issuer C: *PT*

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

Valid from: *Wed Oct 25 16:07:17 CEST 2023*

Valid to: *Wed Oct 25 16:07:17 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:AA:F4:5E:15:36:93:47:34:22:2A:A8:16:E7:9A:1D:B6:A7:0E:4A:65:DF:E6:DC:
9D:0A:31:88:A1:C0:D5:FE:74:78:96:F9:F0:E0:AB:DA:A1:6F:C1:89:1F:0D:4E:6C:16:D7:B6:7F:89:E1:05:D1:67:5A:72:D4:80:58:4A:76:22:C5:B0:61:CC:0C:DF:8C:B2:38:A0:12:DD:25:F0:
C0:62:CD:E8:3B:75:3E:BA:08:24:6D:71:8C:C4:3F:E7:17:2E:AE:B5:3F:F7:21:60:17:DF:81:10:AB:5E:71:62:68:1C:C3:58:E0:D8:16:62:BE:24:F2:1F:FA:A4:38:10:B6:46:70:F8:3B:85:F7:44:
EB:86:98:E3:34:FD:96:B0:41:D6:95:56:60:98:74:F3:B3:20:22:F7:60:0D:F6:6F:42:A5:DC:A6:7A:2A:DF:C2:D8:A7:3E:7D:31:84:2A:ED:5C:F0:8D:54:26:D0:F1:3C:F7:FA:DB:B4:C8:E5:2A:D
6:CB:D4:86:D6:10:AB:DD:9F:7F:DA:BB:C9:6C:FD:60:73:B4:3D:C4:D0:5E:DB:9E:A5:8F:24:6A:B8:63:91:A3:4A:00:15:CF:BF:93:40:91:D6:68:8A:AF:76:36:B6:3C:BA:F2:BC:AC:4F:EE:BA:A
6:51:72:CE:02:A3:4C:89:A9:3C:D7:FF:02:03:01:00:01
```


QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier	*AE:5C:54:69:F1:17:22:77:D9:63:DC:9F:0F:A3:75:40:E9:B0:DB:C5*
Authority Key Identifier	*39:C7:E4:E7:FE:1A:19:08:EB:44:27:69:2A:D8:81:EC:F9:A5:19:1B*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-002.crt*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/crl-002.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*BD:FA:A0:D0:49:ED:E5:F6:AF:00:D6:2D:1E:ED:65:6B:1C:E3:BC:2A:28:7E:3B:B2:EC:69:EC:63:27:8C:74:BF*

X509SubjectName

Subject CN:	*ECCE-TSA*
Subject OU:	*Entidade Certificadora Comum do Estado*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*Centro de Gestão da Rede Informática do Governo*
Subject C:	*PT*

X509SKI

X509 SK I	*rlxUafEXInfZY9yfD6N1QOmw28U=*

Service Status

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

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

Status Starting Time

2025-03-01T00:00:00Z

1.9.1 - Extension (not critical): TakenOverBy

TakenOverBy

URI *[en]* *https://www.ecce.gov.pt/*

TSP Name

Name *[en]* *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Scheme Operator Name

Name *[en]* *Gabinete Nacional de Segurança*

Scheme Territory *PT*

1.9.2 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECCE -TSA*

Service digital identities

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *Centro de Gestão da Rede Informática do Governo*

Subject C: *PT*

X509SKI

X509 SK I *rlxUafEXInfZY9yfD6N1QOmw28U=*

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

Status Starting Time *2025-02-25T22:00:00Z*

2 - TSP: Instituto dos Registos e do Notariado I.P.

.

TSP Name

Name	*[en]*	*Instituto dos Registos e do Notariado I.P.*
Name	*[pt]*	*Instituto dos Registos e do Notariado I.P.*

TSP Trade Name

Name	*[en]*	*National eID (part of national PKI - SCEE)*
Name	*[pt]*	*Cartão de Cidadão (integrada na PKI nacional - SCEE)*
Name	*[en]*	*VATPT-508184258*
Name	*[en]*	*Cartão de Cidadão*

PostalAddress

Street Address	*[pt]*	*Av. D. João II, n.º 1.08.01E, Torre H, Piso 17*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1990-097 LISBOA*
Country Name	*[pt]*	*PT*

PostalAddress

Street Address	*[en]*	*Av. D. João II, n.º 1.08.01E, Torre H, Piso 17*
Locality	*[en]*	*Lisboa*
State Or Province	*[en]*	*Lisboa*
Postal Code	*[en]*	*1990-097 LISBOA*
Country Name	*[en]*	*PT*

ElectronicAddress

URI	*[en]*	*http://pki.cartaodecidadao.pt*
URI	*[en]*	*mailto:pkicc@igfej.mj.pt*

TSP Information URI

URI *[en]* *http://pki.cartaodecidadao.pt/*

2.1 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *415942932572011342 1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIOblC7yPj0Q0wDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMDcwMTI5MjEyOTM5WhcNMTMwMzMwMjEzOTM5WjCBjDFjMEcGA1UEAwxARUMgZGUgQXNz
aW5hdHVyYSBEaWdpdGFsIFF1YWxpZmlj YWRhIGRvIENhcnTDo28gZGUgQ2lkYWTDo28gMDAwMTEU
MBIGA1UECwwLc3VRUNFc3RhZG8xHDAaBgNVBAoME0NhcnTDo28gZGUgQ2lkYWTDo28xCzAJBgNV
BAYTAIBUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAutf+m5+bQVXs/ZVKO0xg52BP
RjcaC5Czw0NkB+ggP85/n8XA85OQ4L7rtZw5ytyBPK0uZZpU2CODXVqFPgiVkVZ4QKHkGMbHAFLi
B0n+nB1U+1hE1LHm15o2Uaa6yNlO1rjEvPogimjcsTNea7SXxE97YNC9NPlOyeQd4hTUx52PycX
vt0/wJde5rJw6EvsZwwT/6zPKw5quWxrhLNU4fwPT1sgFjd26QdWSznnSg1GZY7FEk65wt7U1tIP
YIGFBJy8abtKT2fFvg6r/T3k+9Z5NKLxfm5hTSjqYJCy3voMKofQ+TEWF8CKqTt1pQz2yYe3bV6C
dnsQ33qf52GN3wIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFPCGy6a49a8H8PICukfKkO6CeLgVMB8GA1UdIwQYMBaAFLjnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGwBAQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6AC8ALwBwAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABhAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBlAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMvY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
X2NybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8uchQvcHVibGllby9vY3NwMAOGCSqGSIb3DQEBBQUAA4ICAQAM
OzygC7s11ukHNQWiaGNjEBbgQ/LB+oVvXqe8pWJK2ikx6DaMwirDf2A4Tmai5LTcuiDA3hENegmU
Jg4gh2VExVpn8kq2A4SGXhyOy0UBoRYGfjVy17csqa24MzLztGDIFJxysNmuNoXLMJdwhFwbzaxO
rkktzIZdU7DHK3zIp7D8tXlR/SRzUlE4vDwZcVU4fiErLb7s00cuqDKWFFB7Fdj59cZn3xgVJAa
bdnXn1Ys5WLqmK5QO4GGEJT5UkVQlGuYJ9lVleu7SQFF+z7+06ZRBZOaobUt7EWIE/0k6+uOq14D
ETEWBCY3xbNCJBBw122YwhL4OozgbEd8AZpzMBTYc9SpaIFxMMk9Nm8vVbPM8IuRClEkQp7+2ARt
V6BRzgtdT9mCBExY/YOztKLsoitRB4DrYjhRRXrvKhilz+jUT/W7htr+SIG53tgoxVp9n9aQBxm
sOis4ZM8/d6PoBZxLLazgRl5c+zZOfShaXY2KWaHedoUUGlofRPvhOld0uPGsZ2+lEke69mB5bcl
sqFn9Up2XoGsBtKL6Apl0BAVmnYYWCpbueqCH9DU1LCsf3CrnwVc5KWPw+jsuFtbZkxqbCDtfjmZ
e+xh1ur19IzWXeVd1QuMqTWE9/pO/2olGVMPxiqIceWyVk+/SB2qhqiG2JdcloRLU38pNsMtHw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

Valid from: *Mon Jan 29 22:29:39 CET 2007*

Valid to: *Sat Mar 30 22:39:39 CET 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:BA:D1:7E:9B:9F:9B:41:55:EC:FD:95:4A:3B:4C:60:E7:60:4F:46:37:1A:0B:90:B3:C3:43:64:07:E8:2A:3F:CE:7F:9F:C5:C0:F3:93:90:E0:BE:EB:B5:9C:39:CA:DC:81:3C:AD:2E:D9:9A:54:D8:23:83:5D:3A:85:3E:08:95:91:56:78:40:A1:E4:18:C6:C7:00:52:E2:07:49:FE:9C:1D:54:FB:58:44:D4:B1:E6:D7:9A:36:51:A6:BA:C8:D9:4E:D6:B8:C4:BC:FA:20:8A:68:DC:B1:33:5E:6B:B4:97:C4:4F:7B:60:D0:BD:34:F2:0E:C9:E4:1D:E2:12:13:53:1E:76:3F:27:17:BE:DD:3F:C0:97:5E:E6:72:70:E8:4B:EC:67:0C:13:FF:AC:CF:2B:0E:6A:B9:6C:6B:84:B3:54:E1:FC:0F:4F:5B:20:16:37:76:E9:07:56:4B:39:E7:4A:0D:46:D9:8E:C5:12:4E:92:C2:DE:D4:D6:D9:4F:60:81:85:04:9C:BC:69:BB:4A:4F:67:C5:BE:0E:AB:FD:3D:E4:FB:D6:79:34:A2:F1:7E:6E:61:4D:28:EA:60:90:B2:DE:FA:0C:2A:87:D0:F9:31:16:17:C7:0A:A9:3B:75:A5:0C:F6:C9:87:B7:6D:5E:82:76:7B:10:DF:7A:9F:E7:61:8D:DF:02:03:01:00:01

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

Subject Key Identifier *F0:86:CB:A6:B8:F5:AF:07:F0:F9:42:BA:47:CA:90:EE:82:78:B8:15*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *72:C1:D1:D1:59:3A:48:82:E1:50:5B:59:7A:66:5B:11:BB:0B:BA:D3:1C:33:A7:3E:66:E2:9A:1C:32:E4:94:BB*

Service Status

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

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

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.1.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

Service digital identities

X509SubjectName

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

X509SKI

X509 SK I *8IbLprj1rwfw+UK6R8qQ7oJ4uBU=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.1.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

Service digital identities

X509SubjectName

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001*

X509SKI

X509 SK I *8IbLprj1rwfw+UK6R8qQ7oJ4uBU=*

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

Status Starting Time *2007-01-29T00:00:01Z*

2.1.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.2 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2366735987959252941*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIINhV129xx80wDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Rvw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMDgwMTE2MTY1NzI0WhcNMTQwMzE3MTcwNzI0WjCBjDFJMEcGA1UEAwxARUMgZGUgQXNz
aW5hdHVvYSBEaWdpdGFsIFF1YWxpZmljYWRhIGRvIEhhcnTDo28gZGUgQ2lkYWTDo28gMDAwMjEU
MBIGA1UECwwLc3viRUNFc3RhZG8xHDAaBgNVBAoME0NhcnTDo28gZGUgQ2lkYWTDo28xCzAJBgNV
BAYTAlBUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzwuM2/GoLWkjNDUoXFBdOKUl
jFmwdh/iN4Qfe7mB1ENYxp4utX+smSV+qfiCkJYnbElyqsf1EooQ6Kl5mt/68WATxOIvnm4EbmKW
tYIbyli5yWZcYVD8jjSplkAPYHca9mkVZYqdv3D2menm6B9TR3w4e3C7aOhUg4p69ptEuZJzmoSf
YtCs+Jp2w6BgUzV61SePmYrBB3OuiBsHZaxn/YX27zyg70I05uBKlsu7t2C1cLhBf3AZ7AYJ4h
gBEYsqOXjuA7Cp0aAGldvQhF09p1qAQvIvCn775nbIwGHOAKbkI7CPiqugot13yJ3ouF1HDxEYWv
g1KdP2wBwTqDlQIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBgEB/wIBADAQBgNVHO8BAf8EBAMC
AQYwHQYDVR0OBBYEFF2BRHXspLx65dCp/l5W5KDgOHjuMB8GA1UdIwQYMBaAFLjnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGwBAQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABhAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQBg
baweBtATaOtT43ZV8Vt0asTB6L6KMo3hYZxkXaKsZFiygm8AVbzD2jS1Vjlp3IGd5XEIXSzukNLX
iXHoN0KChLMB92QsWnXj5Mcm5fUS0CfWZx9iosk6X5puji2ED8VWGER4a7WB6HiPjGzpM5yA/+uU
TikuJk+Up1TaAwEdbj7SvMNZIla1Y/YKL5mwFHk4HkvsCQYHP+Cqdi+WeizkM2/0kuf2aMq6XLsG
xcE6AAwAw3gnZPXoR0/VwOZysmhX4P4uhJTXDzDSLguX84mRjUaDRJJmKofsPPFJQTJa41CQfIN/
pXoiOobp7I2Ib3tatobj8t6KFVuDeOVVZVYqypZ78goAIfjDuOGQ7Fr1L85f+hbddffs02R5PALP
hidz4j1tD4xOGtZC4D3PbxL14syUn19N6aXnPKrccVf5tJV5b8V3ThvnJm5tuPwfYrLIcJJXovf+
hK4cAucMEc3DNxI/8w/e8xSHDvURIp8/KNgZj5ztYPUQ/CdCt9RAov+ZEoK42bLKZkHk81R2d16j
VpYDPF0Nup1G8vQDaSaHWddLGKvAyh7s+5HcDrcxmA7wEMVCnsAGs1iSajmntFT7d8eo+wT1UKbl
k4vurhVsQqc3zYVvF/W5hTsyf2lX3F23s+d5+DCarFIru5o+O8r0mKv3dC287BG9VoN5VOmAIQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

Valid from: *Wed Jan 16 17:57:24 CET 2008*

Valid to: *Mon Mar 17 18:07:24 CET 2014*

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:CF:0B:8C:DB:F1:A8:2D:69:23:34:35:28:5C:50:5D:38:A5:25:8C:59:B0:76:1F:E2:37:84:1F:7B:B9:81:D4:43:58:C6:9E:2E:B5:7F:AC:99:25:7E:A9:F2:02:90:96:27:6C:42:32:AA:C7:F5:12:8A:10:E8:A9:79:9A:DF:FA:F1:60:13:C4:E2:2F:9E:6E:04:6E:62:96:B5:89:5B:C8:88:B9:C9:66:5C:61:50:FC:8C:94:A9:22:40:0F:60:77:1A:F6:69:15:65:8A:9D:BF:70:F6:99:E9:E6:E8:1F:53:47:7C:38:7B:70:B8:68:E8:54:83:8A:7A:F6:98:44:B9:92:73:9A:84:9F:62:D0:AC:F8:9A:76:C3:A0:60:53:35:7A:D5:27:8F:99:8A:FC:07:73:AE:88:1B:07:B5:96:B1:9F:F6:17:DB:BC:F2:AB:BD:25:D3:9B:81:2A:5B:2E:EE:DD:82:D5:C8:8B:84:17:F7:01:9E:C0:60:9E:21:80:11:18:B2:A3:97:8E:E0:3B:0A:9D:1A:00:69:5D:C5:08:45:D3:DA:75:A9:14:2F:96:F0:A7:EF:BE:67:6C:8C:0E:1C:E0:0A:6E:49:7B:08:F9:6A:BA:0A:2D:D7:7C:89:DE:8B:85:D4:70:F1:11:85:AF:83:52:9D:3F:3C:01:C1:3A:83:89:02:03:01:00:01

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

Subject Key Identifier *5D:81:44:75:EC:A4:BC:7A:E5:D0:A9:FC:8E:56:E4:A0:E0:38:78:EE*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *18:E3:2C:51:01:4A:2C:76:53:F3:B7:AC:2D:2B:01:40:42:D0:F4:10:5B:2F:72:C9:09:2D:A6:9D:63:C7:8A:BB*

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

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

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

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.2.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

Service digital identities

X509SubjectName

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

X509SKI

X509 SK I *XYFEdeykvHrl0Kn8jlbkoOA4eO4=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.2.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

Service digital identities

X509SubjectName

Subject C: *PT*

Subject O: *Cartão de Cidadão*

Subject OU: *subECEstado*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0002*

X509SKI

X509 SK I *XYFEdeykvHrl0Kn8jlbkoOA4eO4=*

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

Status Starting Time *2008-01-16T00:00:01Z*

2.2.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.3 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7176353201892883087*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIY5eHNxWP+o8wDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Rvw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMDkwMjE3MTYwMzQ3WhcNMTUwNDE5MTYxMzQ3WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZCI0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDAzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqwC9UGCbRC+OqZrj55OaD89
Bg5+8Ty9S2KujfGYJjx4qipl5KAfJR7R45jwEFjWp+tsAwkVyiO3eg2qofTvOhqvVOjXVXSTgyZ4
erg9KaYT0+duQ2zZwKJlP4rjA7fXWFJ/xh1ZBvzDWfufjBSuAJTBWVo2Bk8t+6q9tPzhaBx6DPZ0
laqmINbD/wjbuneflXO4sBL4EWJ1tpivoXSSI9X3SF4ai0f9A7oxbvW3NnO3N8MjEeisN95oOL9p
h1EP8fUvOje3/Rx3uv9UXFfnd38RppP+Dz5EMGNj/L4zzcDGD/GqU5RvQZDeQtrcj+zT3PZ7HNSU
bH5oB7piE6S+QQIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAqwBgEB/wIBADAQBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFDvUh+51F5WoZs4jjucejRnbSyN8MB8GA1UdIwQYMBaAFLjnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGw8AQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABlAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXj0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSib3DQEBBQUAA4ICAQBz
8zcUAHC6d6BByZVzq0xF1priEinsk/ei91FL7+nq50HjXkZ1N4EMBNy3JfNlkOtXtTTN5XGZJy6
9V4yZPzCpvCyhyTxhtoRL1CQET6eAjZpKlwcQTV9Vvl6o5UfdCT4oA7cQW7VHgihqnotdi9zxD87
HQApCNcm/TlbxObAVqIpWWGJhLrnSjff5X7tGr6jvEBeDBSi3tnnvlBU60jDj32pXCIwdP2+ppnN
R0OqZD0VkJVQ2YeKGAJTTzMM8m2bLqyNPrR12mh2RueeOnFc3bnTDmCAK2PdxKMnM+0f5qZiV3rH
oFAJ69pRiSAaIBCIqZAx9+Epw5CIiV8ygd1YtKJ9XL5/NJ4B8H4/l2vLGq8zasVWqc4CyPyjDh
DasaWd7xQ+cjaPba2eb6m8zF1XGLLZJDLDptRumti15H4FUNh7ovAmh8qX+jskD5P8XcAaIsb6eu
PXflBpLdp677afyHCpNOm3uvZQmG08JHd7bdcLhKUrDrfA3VSR8WYH25vw/mqc1VblIPmAFpgRJ9
KWpmHSe/g1tHfOSA2tXnoNV9sKjfwQLfeSWwxd1LRQeU/7bq2zm3BMFpB4G4KymgAv3nRCs/lHeO
nu16q0vIo59lsC5piZxqgRNlH73rjuaG1Riuw6os95jkmm4AE5vEoex5jR8sHTqadM1jtvBvMw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Tue Feb 17 17:03:47 CET 2009*

Valid to: *Sun Apr 19 18:13:47 CEST 2015*

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:AB:00:BD:50:60:9B:44:2F:8E:A9:9A:E3:89:2E:4E:68:3F:3D:06:0E:7E:F1:3C:BD:4B:62:AE:25:F1:98:26:3C:78:AA:2A:48:E4:A0:1F:25:1E:D1:E3:98:F0:10:58:D6:A7:EB:6C:03:09:15:CA:23:B7:7A:0D:AA:A1:F4:EF:3A:1A:AF:54:E8:D7:55:74:93:83:26:78:7A:B8:3D:29:A6:13:D3:E7:6E:43:6C:D9:C0:AF:E5:3F:BA:E3:03:87:D7:58:52:7F:C6:1D:59:06:FC:C3:59:FB:9F:8C:14:AE:00:94:C1:59:5A:36:06:4F:2D:FB:AA:BD:B4:FC:E1:68:1C:7A:0C:F6:74:95:AA:A6:20:D6:C3:FF:08:DB:BA:77:9F:21:73:B8:B0:12:F8:11:62:75:B6:98:AF:A1:74:92:97:D5:F7:48:5E:1A:8B:47:FD:03:BA:31:6E:F5:B7:36:73:B7:37:C3:23:11:E8:AC:37:DE:68:38:BF:69:87:51:0F:F1:F5:2F:D2:37:B7:FD:1C:77:BA:FF:54:5C:57:E7:77:7F:11:A6:93:FE:0F:3E:44:30:63:63:FC:BE:33:CD:C0:C6:0F:F1:AA:53:94:6F:41:90:DE:42:DA:DC:8F:EC:D3:DC:F6:7B:1C:D4:94:6C:7E:68:07:BA:62:13:A4:BE:41:02:03:01:00:01

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

Subject Key Identifier *3B:D4:87:EE:75:17:95:A8:66:CE:23:8E:E7:1E:25:19:DB:4B:23:7C*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FD:07:2E:F9:E1:BB:0F:27:59:A1:17:66:A2:4E:9B:2E:F3:10:C2:59:5E:F7:23:D4:37:36:CE:EC:09:DF:E7:40*

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

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

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

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.3.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *O9SH7nUXlahmziOO5x4lGdtLI3w=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.3.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.3.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0003*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *O9SH7nUXlahmziOO5x4lGdtLI3w=*

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

Status Starting Time *2009-02-17T00:00:01Z*

2.3.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.4 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2016756349056267015*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIG/z1NtgDMwcwDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Rvyx7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMTAwMzE2MTQzMTE0WhcNMTYwNTE1MTQ0MTE0WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA0MlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsLNztHzntD46Vb5OT1H4Ug8E
nhlanMClDrCjfoXd893S7ygfxO8Ghrsnc4DhYTJxaD/4SX2sp8R5MjyIFvaBbYgybYVmm3LJvf1v
3mYryzQFJopVqnKQ3YfuGjzmHkrpR7E6axmoxDNpj4nPmSifUX6DQYQigyiGMf6kXlu6TbqBUrxG
mEWBvJUTAvLuK+dehN8WWNxN1CfpcnVP+FfWWwycFSqoN9bvN2tAPwuHbbIcD9icVNWcYj4q+WT9
C0wO3qLPi5nkihXlmXQOsdWfCTlL9Tvk7seZIG5IFWdfPwjQj/j02HXJfxbZsbkpXmmMFXPdFfIbZ
aIwr4EkylK1p1QIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBqEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFOqnvXlvBw9jk0MN/B04bdJnpWm0MB8GA1UdIwQYMBaAFLJnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGwBAQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABhAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQBA
J4O+vO5NDaqVa+7ZEV8POVghWg8BY5V759LRmvcZ1ikRahbz6B5yZOozF2pl4Csn5gUrhkyD3qvN
izwMZGjFFPGNbphdnDRh6fzYLX37eF00jI3ikc/V6yQqs/IHj5ytmZ9egE5EjjcmKHK3Y9TpIjyC
rFCCReBW0E0tHM4YC6s7RSz4x6y60jC4B8I+9KlvuZhesOUiY+nTlwt5UorPtDQUBAmHeymEpMv5
EtpxoD9qUf5zj17wDMdlgeM0CbTZyFrbBhEGEYztZI2cbqOhK25A/NSysrn4MB0iC746YWkWQY4i
9/J8e9sUTI3yHKbGx4+aICMNY7awpLpWQrynwMipp8kZsng9fDRK8GZZikcjYo1JFtG3tuMlkvI
dsHm2aY5HVoadP2n/fo10YAeoSxyl7l4zMdEU/DA3PujtVt+2H39KTIVAHd4SMEHs1JZGXpCmLc0
PdYt8Munp6BW3T/8yndV3VI67RPylbL6Solrh0VB03LwFAvGDUWkkKhpS2rpAIGWOK14zjCDBkRP
Hb9EtW9Bl7dw/SwvGgT1kUS/ynTd+zcE9YL2WReIaElw8JovexKTQ2ksFXnunUJjXoHDkm4WpY5d
ao1Cbpr5bnswn05KOj7tZO1HSorXeXAxopvRJpdLjh9aq0C2pYIZKtKhu5hvy95T+Usalj+Dfg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Tue Mar 16 15:31:14 CET 2010*

Valid to: *Sun May 15 16:41:14 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:B0:B3:73:B4:7C:E7:B4:3E:2C:55:BE:50:4F:51:F8:52:0F:04:9E:19:5A:9C:C0:A5:0E:B0:A3:7E:85:DD:F3:DD:D2:EF:28:1F:C4:EF:06:86:BB:27:73:80:E1:61:32:71:68:3F:F8:49:7D:AC:A7:C4:79:32:3C:88:16:F6:81:6D:88:32:6D:85:66:9B:72:C9:BD:FD:6F:DE:66:2B:CB:34:05:26:8A:55:AA:72:90:DD:87:EE:1A:3C:E6:1E:4A:E9:47:B1:3A:6B:19:A8:C4:33:69:8F:89:CF:99:28:9F:51:7E:83:41:84:22:AB:28:86:31:FE:A4:5E:5B:BA:4D:BA:81:52:BC:46:98:45:81:BC:95:13:02:F2:EE:2B:E7:5E:84:DF:16:58:DC:4D:D4:27:E9:72:75:4F:F8:57:D6:5B:0C:9C:15:2A:A8:37:D6:EF:37:6B:40:3F:0B:87:6D:B9:5C:0F:D8:9C:54:D5:9C:62:3E:2A:F9:64:FD:0B:4C:0E:DE:A2:CF:89:29:E4:8A:15:E5:99:74:0E:B1:D5:9F:09:39:4B:F5:3C:64:EE:C7:99:20:6E:65:15:67:5F:3F:08:D0:FE:3D:36:1D:72:5F:C5:B6:6C:6E:4A:57:9A:63:05:5C:F7:45:7E:50:59:6A:5C:2B:E0:49:32:96:4D:69:D5:02:03:01:00:01

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

Subject Key Identifier *EA:A7:BD:72:2F:07:0F:63:93:43:0D:FC:1D:38:6D:D2:67:A5:69:B4*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D0:E6:46:69:1C:73:4A:08:80:E6:45:2F:B2:6E:63:25:F0:8E:72:A9:03:7E:24:B8:CA:C4:B7:91:F9:40:8B:21*

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

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

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

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.4.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *6qe9ci8HD2OTQw38HTht0melabQ=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.4.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0004*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *6qe9ci8HD2OTQw38HTht0melabQ=*

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

Status Starting Time *2010-03-16T00:00:01Z*

2.4.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.5 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *341054323862704202*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIBLurGb7ykEowDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Rvw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMTEwNDA1MTQ1NTQ3WhcNMTcwNjA0MTUwNTQ3WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2l0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA1MlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApkLEHf+gusYcAgeUpylr50vQ
tA0A2UK8W11F2K/GBJBzOyQ5RmwaHwJzhYZZEpiD++9jhr4DAWZ8oCTXCw9s7G8SZcPjqBuRjdXM
+yg22xaXORZy748/rOf6mtR/qrJe3T2UNFOTzGwFpDQrxrLgz/trsgTQkBvFL/vbqUNKSeeybP3G
cQ9zTqNt0kTRFVXwmxqeSCCFr/dGlbyymYrbaFlDT/pbROdgUZ8kNCOcPABCG/e/oYcncxXe71Kl
Ao3ErHgw3xYWkRmY9D44BDUcWtUdQat7weyOZxp+peuxtsKX7/gVI4yURNGG5xCyJj2bZvGvXrq
y3NPCCnAxt7OYQIDAQABo4IChDCCAoAwEqYDVR0TAQH/BAqwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFMZzcxkzLhLOm8auJcgahVHElZFpMBBGA1UdIwQYMBaAFLJnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGw8AQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABlAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQBg
VRbACZ3hM65P+0vn+V0ZCuLQlaYCMQctWT3wV5T48naCwrC2UVx6wGoH9Hph1akt8Q r1a63nv/ND
tFz7SiAKsSnAsX5j3NBfPudFBOI1lzUeHUlDV7UYb5zpi2mpbTukSNt+cGjmMruAbQTdxNwPFKYy
agVcSR/7hq1UctQSCwrBT5XE2FCo8jDToaF9TjjElm82VNWOkFtfurpfVlA77el/10MuO/bdH2J2
6q7P4ghoJTORprEcJsV3h3iIMJ1Y5r7YLt2ynrfNu5xO9KlhVOeCCb+q4ToP4xalHz4zkgXsPMb4
7C7FEGR2uNRyTWVN/o/mAKp8VxxO0/FYCknVNFtqqXwC2N1s8s4oz0Ka8ZlgvXciK/Up7/HyENd
rvX5kCKUsuxAlx9/rZfN8BOnX93kTBzOI0egxYauvCOkLqAkPpVQvjN+1NlUTwrABdMqKZcaNP1
vkefTaLXrmY+U9Xvm+xSLN1BIMWV5IsAfUdRDVEB6v0gjR+YnRSJ/jxkhvk0CUHrVhJ96P+I53Ct
ZsI3NAFAfVamk8Zknc49fJgwNsWEeStIEVeFoVxpZ8agB7/GkeTKktOe+TT2IbX5Yu+asID79rpd
PW5vuZVsNSZRcknjmsibZ0w0VJazLmGOjBrk4rfq9OsCBhSqbWgQc3Tu4dcwJ6jwJ2EBUZDYdg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Tue Apr 05 16:55:47 CEST 2011*

Valid to: *Sun Jun 04 17:05:47 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:A6:42:C4:1D:FF:A0:BA:C6:1C:02:07:94:A7:29:6B:E7:4B:D0:B4:0D:00:D9:42:BC:5B:5D:45:D8:AF:C6:04:90:73:43:24:39:46:6C:1A:1F:02:73:85:86:59:12:98:83:FB:EF:63:86:BE:03:01:66:7C:A0:24:D7:0B:0F:6C:EC:6F:12:65:C3:E3:A8:1B:91:8D:D5:CC:FB:28:36:DB:16:97:39:16:72:EF:8F:3F:AC:E7:FA:9A:D4:7F:AA:B2:5E:DD:3D:94:34:53:93:CC:6C:05:A4:34:2B:C6:B2:E0:CF:FB:6B:B2:04:D0:90:1B:C5:2F:FB:DB:A9:43:4A:49:E7:B2:6C:FD:C6:71:0F:73:4E:A3:6D:D2:44:D1:15:55:F0:9B:1A:9E:48:20:85:AF:F7:46:95:BC:B2:99:8A:DB:68:52:03:4F:FA:5B:44:E7:60:51:9F:24:34:23:9C:3C:00:42:1B:F7:BF:A1:87:27:73:15:DE:EF:52:88:02:8D:D9:12:B1:E0:C3:7C:58:5A:44:66:63:D0:F8:E0:10:D4:71:6B:54:75:06:AD:EF:07:B2:39:9C:69:FA:97:AE:C6:DB:0A:5F:BF:E0:54:8E:32:51:13:46:1B:9C:42:C8:98:F6:6D:9B:C6:BD:7A:EA:CB:73:4F:08:29:C0:C6:DE:D0:61:02:03:01:00:01

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

Subject Key Identifier *C6:73:73:19:33:2E:12:CE:9B:C6:AE:25:C8:1A:85:51:C4:21:91:69*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0B:CE:12:D1:E7:CF:19:A9:8E:46:92:13:92:51:DA:AF:CA:1F:4E:B2:2B:0D:38:6C:D6:B3:C5:BF:01:C4:2F:4E*

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

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

Status Starting Time *2017-06-04T15:05:47Z*

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.5.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *xnNzGTMuEs6bxq4lyBqFUcQhkWk=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.5.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0005*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *xnNzGTMuEs6bxq4lyBqFUcQhkWk=*

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

Status Starting Time *2011-04-04T23:00:01Z*

2.5.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.6 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2862931070566785772*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIJ7sso+WP4uwwDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Rvw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMTIwMjI4MTI1NzIxWhcNMTgwNDI5MTMwNzIxWjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA2MlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsGWakT9Sz4+M57zINELrsDcC
fK3OsFLtgc9gDnncmRoZjbwxl1VC8eB2bfIzBhSbNkdfr/xAB4YQ8q7EP19v421NjZh7YawTTWKX
E/Mmr46s+R+XFsXSK69Nkc31mng7sjvK16XeBA0A52cfgjx17UGlSOIO7CVHV2S02d9NXzw/nOuS
blms+SeV1OU/7D0C/8OmtaqSj/CYsicF96N9ZjZjOIlvk6kgrq2UPCJ9tyDAWnek42XNemtPne50
l4/GGdff0xArc34SNextBddqsYlUdxTZsAGNpXEzw1bgX/+ZEPooBRjPAkICOAtnHCjcaxRDNd/E
2eA+y6zuLaWh+wIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFJeVhEW2tmO5tPY9ne37tyGehOVrMB8GA1UdIwQYMBaAFLJnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGw8AQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABlAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBlAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMvY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XzNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJl0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQA4
O3DhVXadRlnLtw++Sr3grnB7NE4QIkJvCqYvn0mwTBlqDHNnSWHm5sgZHHBMq/UlwGRNeTdlMrPLO
+3kqvGRxMUPKOZYCEdsPeoBP8/JRG4lOoD7XNPm4GjMvDU/QOUCencIkvIyoPTmxt83JAnhQkVXH
wQMbBzgyALkwt06+4l8Z1x9rWLJ+Q9hoTH7B47L8UVvtbB3vaFt5E3Cjc/y5Xq+qYjfqDwDC7Ys3
m34k5sCrN2LGXMgPDsqZ1xjllwe1ysEwwitUxEMAQcwjGum1icvv8axFb52hKWt/3RrQgy3Vx2Li
o4cUdZcDk1ICR6qgwBC5UN8GazkCSnRHXLKN6RWGUO7rtUD+2VCjPauSN+YLaMCZaXz8lBEgLQQ6
RtXA+39WrPQDkbRkllpcd6WqOzIQBVah54kY+Z/cgetHnmufBCvWRxgCrLi8mnRANlLgjRS3RQIc
z1cEHJ1jnoua25ydREs6NIHCcGiw/RjbWeCcxCoGtTeuRNU6+u7F/G0ofhIlHzlygO8On5f9AjHS
uq1RNc8F448ygujtFN02/UKy98Kv0RKOH7W8Q5FPTyfcyh+dQRtT1nm8+EE8fnQxwHLA+9Lvwu+S
uxi1Jdu7GMuyjRGBy+k1bTnICkrAXr+NovtHbx6b0RdQDLlyR3uu5N1amhP5eOhG68Qc/sBxEw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Tue Feb 28 13:57:21 CET 2012*

Valid to: *Sun Apr 29 15:07:21 CEST 2018*

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:B0:65:9A:91:3F:52:CF:8F:8C:4B:BC:E5:34:42:EB:B0:37:02:7C:AD:CE:B0:52:ED:81:CF:60:0E:79:DC:99:1A:19:8D:BC:31:97:55:42:F1:E0:76:6D:F9:73:06:14:9B:36:47:5F:AF:FC:40:07:86:10:F2:AE:C4:3F:5F:6F:E3:6D:4D:8D:98:7B:61:AC:13:7D:62:97:13:F3:26:AF:8E:AC:F9:1F:97:16:C5:D2:2B:AF:4D:91:CD:F5:9A:78:3B:B2:3B:CA:D7:A5:DE:04:0D:00:E7:67:1F:B2:3C:75:ED:41:B8:49:09:50:EC:25:47:57:64:B4:D9:DF:4D:5F:3C:3F:9C:EB:92:6E:59:AC:F9:27:95:D4:E5:3F:EC:3D:02:FF:C3:A6:B5:AA:92:8F:F0:98:B2:27:05:F7:A3:7D:66:36:63:42:52:2F:93:A9:20:AE:AD:94:3C:22:7D:B7:20:C0:5A:77:A4:E3:65:CD:7A:6B:4F:9D:E4:B4:23:8F:C6:19:D7:DF:3B:10:2B:73:7E:12:35:EC:6D:05:D7:6A:B1:89:54:77:14:D9:B0:01:8D:A5:71:33:C3:56:E0:5F:FF:99:10:FA:28:05:12:4F:02:49:42:D0:0B:67:1C:28:DC:6B:14:43:35:DF:C4:D9:E0:3E:CB:AC:EE:2D:A5:A1:FB:02:03:01:00:01

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

Subject Key Identifier *97:95:84:45:B6:B6:63:B9:B4:F6:3D:9D:ED:FB:B7:21:9E:84:E5:6B*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *23:61:0C:57:DB:32:79:98:18:E2:17:83:7C:A2:AB:0D:0B:E6:AF:43:50:55:C8:88:EC:AD:65:39:13:0B:4F:CC*

Service Status

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

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

Status Starting Time

2018-04-29T13:07:21Z

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.6.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *l5WERba2Y7m09j2d7fu3IZ6E5Ws=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.6.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.6.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0006*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *l5WERba2Y7m09j2d7fu3lZ6E5Ws=*

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

Status Starting Time *2012-02-28T00:00:01Z*

2.6.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.7 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6176269300471585484*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIVbaENjvCWswwDQYJKoZIhvcNAQEFBQAwgYQxIDAeBgNVBAMMF0NhcnTD
o28gZGUgQ2lkYWTDo28gMDAxMREwDwYDVQQLDAhFQ0VzdGFkbzFAMD4GA1UECgw3U0NFRSAtIFNp
c3RlbWEgZGUgQ2VydGlmaWNhw6rDo28gRWxlY3Rvw7NuaWNhIGRvIEVzdGFkbzELMAkGA1UEBhMC
UFQwHhcNMTMwNTAzMTEyNDM2WhcNMTkwNzAzMTEzNDM2WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2l0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA3MiIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvxNbxLdZDhZFCfQ0b5BIWY7Vg
x2KOBd+0ZDPXp4tkcRDI2slyngO0SoiAKCc16QuNpD5Jp1SpoyDbrKS1LOmMYg4Qtw/a1rbtp9BP
BD1fAPwNBgFYxYg/SkrQ4Twd7ZXxLUKOsTk0po/tJnhN9GoOTA1NixRS8BxGNZdCSu+Vh7gVgSOm
kmjZS9kS0m7OEQaSHwwoh7Etn5acP9DODMue5zdr4OgPQNFbEja7WKbNSvD3T8aYRMQna4BzS7t5
d1P7Fdx1NAY3G5sm7k+H+mdpusXTwmFzLCLsi+SSIWaA9B9Iprgf1JpRZsfrGAVXtjrvLfYwl5aOZ
AOnpkQQGblfJxwIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFLYtaRv5eHMCYRPXMcwGPHgGb2NJMB8GA1UdIwQYMBaAFLJnMLLPRWrjkbVv
O2P7jain4W2eMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGwBAQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABhAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMV9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQDm
KizfRKzLxxUB2bZarwBHWwY8R2PhccfCIhatSsRsaRPiMCeq8KpCUB02jstAdazMg1CoOwqTeKAW
UuRPDvX7JI2I4yngktzJVz2ZNUCivceBWzE9zxdLpoVKPgBjNI2LAIAXxeiMU8x6IBbmPWuNhRTn
36yfxRYLcRKOvQ6Kk6eMZcbwIqiOY208zebt2jrh9J2iIJQglwjSCmCItNxjccjuNVOItcSIX6ik
KjW9EDelmtbr5KSXqu1jnL6pjwLa+0dbOeuqEeOalt/3+fF9ktuK+6yTcurJWBKM2MmhaL7ZFhhb
KFPKH+9tBF67yw3s8GQm24KvoNlj6VA5KqF9wVEuB6arwej52auZ/chaG+sfT4W8CDhKh7KBePHS
Cs0ujXYaRq6fceYbjlIC9mNY1bcMJj0LQlMKyzI53dSL6+uTrmLfyYJTVsLqyoPNxrsMRchOJuy2
T/U6PCFf0eCx6x9aIDtuPYmT5zJTA1HLTpT/MPFlWZNqnSJMcGSVaPhSkS6F0ZoZ3N1MsoY52E4F
ckCDI8yzc7d2q0jqJ5GC5zH0qw2jIyatr3UGJJrjf8ebV8/T72GNJQu5RIYgo3bzajHYdzIXx02B
ub9H3+UQ/hvP9S/T2RTSnIHeiLqQ2vNVGZD3ucQ86cQ753ZnyCesCrVriPNfK0Xu0ZcR1i/2Eg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer C: *PT*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer OU: *ECEstado*

Issuer CN: *Cartão de Cidadão 001*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Fri May 03 13:24:36 CEST 2013*

Valid to: *Wed Jul 03 13:34:36 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:BF:13:5B:C4:B7:59:0E:16:45:09:F4:34:6F:90:56:63:B5:60:C7:62:8E:05:DF:B4:64:33:D7:A7:8B:64:71:10:E5:DA:C9:72:9E:A3:B4:4A:88:80:28:27:35:E9:0B:8D:A4:3E:49:A7:54:A9:A3:20:D8:AC:A4:B5:2C:E9:8C:62:0E:10:B7:0F:DA:D6:B6:ED:A7:D0:4F:04:3D:5F:00:FC:0D:06:01:58:C5:8A:BF:4A:4A:D0:E1:3C:1D:ED:95:F1:2D:42:8E:B1:39:34:A6:8F:ED:26:78:4D:F4:6A:0E:4C:0D:4D:BB:14:52:F0:1C:46:35:97:42:4A:EF:95:87:B8:15:81:23:A6:92:68:D9:4B:D9:12:D2:6E:CE:11:06:92:1F:0C:28:87:B1:2D:9F:96:9C:3F:D0:CE:0C:CB:9E:E7:37:6B:E0:E8:0F:40:D1:5B:12:36:BB:58:A6:CD:4A:F0:F7:4F:C6:98:44:C4:27:6B:80:73:4B:BB:79:77:53:FB:15:DC:75:34:06:37:1B:9B:26:EE:4F:87:FA:67:69:BE:C5:D3:C2:61:73:2C:22:EC:8B:E4:92:95:66:80:F4:1F:65:A6:B8:05:52:94:59:B1:FA:C6:01:55:ED:8E:BB:CB:7D:8C:25:E5:A3:99:00:E9:E9:91:04:06:6C:87:C9:C7:02:03:01:00:01

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

Subject Key Identifier *B6:2D:69:1B:F9:78:73:02:61:13:D7:31:CC:06:3C:78:06:6F:63:49*

Authority Key Identifier *B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *70:A7:6C:5A:F4:3E:16:3C:DE:9D:2E:90:44:72:4E:34:BE:CC:B8:7D:4A:0F:69:E4:64:2C:C3:F9:1B:EA:D2:DE*

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

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

Status Starting Time *2019-08-05T23:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.7.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *ti1pG/l4cwJhE9cxzAY8eAZvY0k=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.7.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.7.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0007*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *ti1pG/l4cwJhE9cxzAY8eAZvY0k=*

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

Status Starting Time *2013-05-02T23:00:01Z*

2.7.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.8 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6337522604016849785*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIV/NnOxBu03kwDQYJKoZIhvcNAQEFBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXj0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDIwHhcNMTMwNTIwMTcyODAyWhcNMTkwNzIwMTczODAyWjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZCI0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA4MlIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzI6+uYvjepLzSlWsKTqUb47o
DA4luUYEffoduxTOot3G9luptpCYX73s+R8+B7whwxvnwFaUvKkHFcvsxQkLyeWyq3Ye+fjM8E+G
nbbolnNx4gmc/DlvtvT6jbQHM1s3iCkUrYXe2xA/tZFyF7BIWL7Wfa1/kZeTVLazHbSMMHIFujOJ
/xFqCnA5Gq2tyW/HZ6w7FkYymzvOfjEiAAuDn/6Dn55aqv15HHNgONxzy7rgdNl9C707FnnllekU
ivOU06+uKoVhPhDoT3vKfj5ficrjMRD0hZ+fxsnOy1O64ZrYFYnZDXZkjTLuLc2iPUufE2dgJya
Z2V+A386KjhWVwIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFD+HQHdG+Ub3o170bxwb4A0gK3rjMB8GA1UdIwQYMBaAFPLPvRIwrDC8wMky
L8PTcgDIakQVMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGw8AQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABlAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBlAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMl9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQBy
HxfZ5Xuo4613n2guUUrXrchgr4ARES0Add1Kbn3bTpQF1nxQVaT2R/j+ttA3dmqQTk2zzM7CrG36
6vB3L+P8mqyngBbQjlwFerL3QiiPjBkSgRttNTfPQdo9B1kKpovjHNaJw+asS/tP1kxUaHPNmmqB
XIw3kpG+ffp+APgRusUPHGNg9gFyq9Ca5tcgQxHF+Y7WGAbtr5Ij6kJ1F+Zobs6+HeJzB/cU0bV9
+c2T+Xpb+U7paz8J+fj4XAWTKV2tFigkYatMyhG+kBtdHeOOKdHHoEF7y8ik8+tgKd+48YabyJKn
1Ub5hiDAETi/xrn0zL9PyLwoZP5eMGefPPTGdfBXdG3iC1b+IrgXTewvUH1Lru+ZZiY2a4gTdyWQjT
eg1pOwQ1Eqpcp7rKwSMIY6Vid0Pay60GjJ6HqpPq6rNxBmMNijjNeLB4fgYUyHMDKcC0XfRDI3pD
aRV3XiUcHj/YPnAMygvJzvuhKFsvGVGn0vtlVlsgxuAmZVDyfxWnJSPA5eXA4u687VQnETIJPv5c
BoSgNXy8ZVjXRX0bkSrNByUnAH6MCkEbyjPgHcxd0RC3ta6rPFrcaKFEezolUFWjbv0ca4apMvWi
IwoOj88UwZDYygIXvRcsGNBdfr9lILbUykacALla1a/R8ZmL6zoPlwDOo4DmeLkaFZ4j7i+cyA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Cartão de Cidadão 002*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Mon May 20 19:28:02 CEST 2013*

Valid to: *Sat Jul 20 19:38:02 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:CC:8E:BE:B9:8B:E3:7A:92:DD:48:85:AC:29:38:14:6F:8E:E8:0C:0E:08:B9:46:04:7D:FA:1D:B8:14:CE:A2:DD:C6:F6:5B:A9:B6:90:98:5F:BD:EC:F9:1F:3E:07:BC:21:C3:1B:E7:C0:56:94:BC:A9:07:15:CB:EC:C5:09:0B:C9:E5:82:AB:76:1E:F9:F2:4C:F0:4F:86:9D:B6:E8:96:73:71:E2:09:9C:FC:39:6F:B6:F4:FA:25:B4:07:33:58:37:88:29:14:AD:85:DE:D8:10:3F:B5:91:72:17:B0:48:58:BE:D6:7D:AD:7F:91:97:93:54:B6:B3:1D:B4:8C:30:72:05:BA:33:89:FF:11:6A:0A:70:12:1A:AD:AD:C9:6F:C7:67:AC:3B:16:46:32:9B:3B:CE:7C:91:22:00:0B:83:9F:FE:83:9F:9E:5A:AA:FD:79:1C:73:60:38:DC:73:CB:BA:E0:74:D9:7D:0B:BD:3B:16:79:E5:95:E9:14:8A:F3:94:D3:AF:AE:2A:85:61:3E:10:E8:4F:7B:CA:7E:3E:7C:72:2A:C9:35:10:C6:85:9F:9F:C6:C9:CE:CB:53:BA:E1:9A:D8:15:89:D9:0D:76:64:25:32:EE:2D:CD:A2:3D:4B:89:7C:4D:9D:80:9C:9A:67:65:7E:03:7F:3A:28:98:56:57:02:03:01:00:01

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

Subject Key Identifier *3F:87:40:77:46:F9:46:F7:A3:5E:F4:6F:1C:1B:E0:0D:20:2B:7A:E3*

Authority Key Identifier *F2:CF:BD:12:30:AC:30:BC:C0:C9:32:2F:C3:D3:72:00:C8:6A:44:15*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl002_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *03:EC:63:D9:36:C9:9D:34:70:A3:50:5E:87:E1:BB:05:16:59:6E:2E:1B:92:7B:8D:AE:4B:60:0A:75:A2:D4:9D*

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

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

Status Starting Time *2019-08-05T23:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.8.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *P4dAd0b5RvejXvRvHBvgDSAreuM=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.8.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.8.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0008*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *P4dAd0b5RvejXvRvHBvgDSAreuM=*

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

Status Starting Time *2013-05-19T23:00:01Z*

2.8.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.9 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6608938539843144063*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHGjCCBQKgAwIBAgIIW7eqlhm9SX8wDQYJKoZIhvcNAQEFBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVOQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0Vzdc6FkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDIwHhcNMTQwNzEwMTEzMTIwWhcNMjAwOTA4MTE0MTIwWjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDA5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt3Qp7hrLoDBUH5qNv79/don
ENxd2NO1Wj2E7AYU+jiW5bQU/vEI6FprktUcEY+W735AK8Un6Nv5aZr9afEJBZQ858Fp7foCkr3D
1uN46VS1e7oW6J100tEf3F/YrQ2iY7u/yL/vrSagLT6O4GnrR1IDjOueBXi1PYvZZzegVgAZnhEK
t517pgm2ldGbJlwB1oBymPm1uFZLeeIv1+5IQ7ECeocMBtXvD2vGz2kIDr77jAyFD2GwaD6seFm
+Ulj/jsa6S8Lil0KKlVQbhjF8DmXYrn85pfhYfsXOeLuWnDVkGfDD8sCDIMtz5z3gCw/q/+MCglor
rupF3wmpis/oewIDAQABo4IChDCCAoAwEgYDVR0TAQH/BAgwBqEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFOIGI8cPtIMna0JNeiwiUnxBhMpDFMB8GA1UdIwQYMBaAFPLPvRIwrDC8wMky
L8PTcgDIakQVMIIBcQYDVR0gBIIBaDCCAWQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8v
d3d3LnNjZWUuZ292LnB0L3BjZXJ0MIHFBgtghGw8AQECBAABAjCBtTCBsgYIKwYBBQUHAgIwgaUe
gaIAaAB0AHQAcAA6ACBALw6wAGsAaQAuAGMAYQByAHQAYQBvAGQAZQBjAGkAZABhAGQAYQBvAC4A
cAB0AC8AcAB1AGlAbABpAGMAbwAvAHAAbwBsAGkAdABpAGMAYQBzAC8AcABjAC8AYwBjAF8AcwB1
AGlALQBJAGMAXwBjAGkAZABhAGQAYQBvAF8AYQBzAHMAcQBfAHAAYwAuAGgAdABtAGwwZgYKYIRs
AQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJs
aWNvL3BvbGl0aWNhcy9kcGMuY2NfZWNfY2lkYWRhb19kcGMuaHRtbDBXBgNVHR8EUDBOMEygSqBI
hkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFv
XZNybDAwMl9jcmwuY3JsMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Au
cm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMA0GCSqGSIb3DQEBBQUAA4ICAQCs
bE0+eyWPGhuae8GgfFHx7WocKfgqymTRPXxPYVWLSl2lwbsGQV3GC58Dbs1WxT94xusWKirjlDxC
QV8tKUlW704eQr85L2D5wz9etC50qBg2p1y4YlNDAvTlL9CVm4hGXTn29byQWClstF8zY5GRQBuH
xo7/wVWEYfzcYgKwSqAqRNzsSD8yRPbz95fiatTiIEN4U2h1qHI/vOSMDwkB/gs3TO5X/2Omn5Qy
GLGUPQzuB5bbh9ck2WoloMnUdzpdug9Fr5OiPE/0wnag278v6zrC0bqPAnsuYuRatn19Vgb8SSj9
iVaFDaFsX5P6rsmd+3hsXZVbkSytme+/AVec+49+v0a0N3tLqn1WL6vx6G5xmT4aevEl4TYZctn
zH+PybRBNWUjk3ho1lXuANnsxeEzpzyqjD1wxWyiq7SwKQPlkdepj1qixVqmYlgWaKW7MrEBFWxe
QSi0Yj7rHlnkcW5m5ePQUMKbjWxrcjGlpeKZePjYuITioiuVfWBd7rrQkS1A95zl+jgyZGt8dB4t
9fvXndgPGMKZVYbOYrjMhmIjSEWCkOwMumwfjiwuPoxjlohfin3kdX3wr+LP7WWuCMykuabC4DOC
haDwd3anZq3FwZTEsXAHTy7jWEK6VdDz1dn/1EhDPjHijDsf+z5Ptdquae2Zz5QB3CPvUERgoA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Cartão de Cidadão 002*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu Jul 10 13:31:20 CEST 2014*

Valid to: *Tue Sep 08 13:41:20 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:B4:8D:CE:A5:88:6B:2E:80:C1:50:7E:6A:36:FE:FD:FD:DA:27:10:DC:5D:D8:D3:B5:5A:3D:84:EC:06:14:FA:38:96:E5:B4:14:FE:F1:08:E8:5A:6B:92:D5:1C:11:8F:96:EF:7E:40:2B:C5:27:E8:DB:F9:69:9A:FD:69:F1:09:05:94:3C:E7:C1:69:ED:FA:02:92:BD:C3:D6:E3:78:E9:54:B5:7B:BA:16:E8:9D:74:D2:D1:1F:DC:5F:D8:AD:0D:A2:63:BB:BF:C8:BF:EF:AD:26:A0:2D:3E:BE:E0:69:EB:47:52:03:8C:EB:9E:05:78:B5:3D:BB:D9:67:37:A0:56:A0:19:9E:11:0A:B7:9D:7B:A6:09:B6:21:D1:9B:24:9C:01:D6:80:72:98:F9:B5:B8:56:4B:79:E2:2F:D7:EE:65:43:B1:02:7A:87:0C:06:D5:EF:0F:6B:C6:CF:69:22:0C:5A:FB:EE:30:32:14:3D:86:C1:A0:FA:B1:E1:66:F9:42:7F:26:C6:BA:4B:C2:E2:97:42:8A:FD:54:1B:86:31:7C:0E:65:D8:AE:7F:39:A5:F8:58:7E:C5:CE:78:BB:96:9C:35:64:19:F0:C3:F2:C0:83:94:CB:73:E7:3D:E0:0B:0F:E8:FF:E3:02:82:5A:2B:AE:EA:45:DF:09:A9:8A:CF:E8:7B:02:03:01:00:01

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

Subject Key Identifier *E2:06:23:C7:0F:B4:83:27:6B:42:4D:7B:08:94:9F:10:61:32:90:C5*

Authority Key Identifier *F2:CF:BD:12:30:AC:30:BC:C0:C9:32:2F:C3:D3:72:00:C8:6A:44:15*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl002_crl.crl*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AA:7C:17:8E:B2:5B:AC:02:3E:FC:90:01:2E:54:1E:6D:20:6F:64:B6:7B:3B:9C:55:19:65:5A:E8:A1:48:9E:A7*

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

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

Status Starting Time *2020-11-09T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.9.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *4gYjxw+0gydrQk17CJSfEGEykMU=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.9.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.9.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0009*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *4gYjxw+0gydrQk17CJSfEGEykMU=*

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

Status Starting Time *2014-07-09T23:00:01Z*

2.9.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.10 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6772195039640580314*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGwjCCBKgAwIBAgIIXfurggdwcNowDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVOQKDDdTQ0VFIC0gUZlzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXND1YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjby8kZSBDaWRhZMOjbyAw
MDMwHhcNMTUwNjA0MTE0NjIwWhcNMjEwODA2MTE0NjIwWjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDEwMlIBIjAN8gkqhkiG9w0BAQEFAACCAQ8AMIIBCgKCAQEAxwcC9PLufWkIRCfYcA3AW
9M4sN3Gbnv4QGDuKX0pPLcnzz3QVlBQ7tEdAODEDQWIXA6Ywwi+l54fgBFaYXjAD3gRy5dB9TIrn
poG004ZSobjgr7cD834XC3SMyhm75GeOvKAuWMV6ux5kDgIWJeCdPcuPLkW+M145rQYjPJ1ytRt3
92puAbWEJw5fWY9pBQDu1Xec5PbgDjLLj60F1b1p3JkBm7XH7K2SRWx5rU64xHwBRJV7fVBrh5f7
2Cap33HSVBVbuuPt5FNi4ScpPIY2Mu7nX+HcjSlh2jJ2KWHjph5MvCXAeA9a/gmOOym+6eYZqh/tn
OSzEJWyIMHRoQwIDAQABo4ICLDCCAigwTAYIKwYBBQUHAQEEQDA+MDwGCCsGAQUFBzABhjBodHRw
Oi8vb2NzcC5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL29jc3AwHQYDVR0OBBYEFPvO
UAxm1zkHM8u5IEwSxRH9l5xbMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUPN/Ks1o8
OR6M5ul5gnAKiaz9LvYwggEZBgNVHSAEggEQMIIBDDBmBggphGwBAQECBAAHMFgwVgYIKwYBBQUH
AgEWSmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2RwYy9j
Y19IY19jaWRhZGFvX2RwYy5odG1sMG4GC2CEbAEBAQIEAAECMF8wXQYIKwYBBQUHAgEWUWh0dHA6
Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL3BjL2NjX3N1Yi1jY19j
aWRhZGFvX2Fzc3FfcGMuaHRtbDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cuc2Nl
Z5nb3YucHQvcGNlcnQwNVwYDVR0fBFAwTjBMoEqgSIZGaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFk
YW8ucHQvcHVibGljby9scmMvY2NfZWNfY2lkYWRhb19jcmwwMDNfY3JsLmNybDAOBgNVHQ8BAf8E
BAMCAQYwDQYJKoZIhvcNAQELBQADggIBAI+QHiI4Ixb6i9ZjkWYX736u2PmyrIlsYeoARIExoEzo
eqAiC2Ie+s6sTqUr+kZedAnRBHm+pkxFa5Beuvj+A7aXuAz4hySzIP5nlRpIFnvSSjrIA9lWxAf9
njO3lxTR4UR1E+Fnmmz51599MlbOwKvqDQakOQ7TiHzkmLvLKovYZwPFCJYy+1BbpXN6rhWnNEfPh
8IdLwIJzqmo/0XE5YGNzbhfS2/tD4DHruRAOmGsrC0dasnv6o1iQG0RFCIhSTfI5NP/FEJ4m8Grv
hCe204dKcoRTOaYMG/L3H3hOPzkNsErAH95XrJrw0IPRCkMLPI27r55EtntV0Z7ENhAPXYvUy5M7
ZjSHHxYgdMhBLGM99p6V49zQWWxSbZIi6jNAYxgKcQqTvAs9Yeg1Kq4Np0hYm0NYKUQEepLUb8XU
wtCTEnKL5l6BidkYvEj7KuZjYxdX947lPOlVfh6w7TJhUl8njw1k62iEaGpvznqjRk3dfK1Ikw0F
9EHJ2d/G4tQhv8KwF2cLzXaLyX/z5N8HDAjXyJXTG/VFKEQoYRo+Ei+ijmWqjls3CrmKvfIwQizq
NwQ7m2cSO1SQAIC1KMI+Z5WmF06QN0C9KmEw82o2sNTJqfu3ypbat0LRy537RTr3k1gDLBTjIrTo
l5Pb+16OlUJ1DswEZxkiwuapj0+9Xu2f

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 003*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu Jun 04 13:46:20 CEST 2015*

Valid to: *Tue Aug 03 13:46:20 CEST 2021*

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:C7:07:02:58:F2:C8:B9:F5:A4:96:54:42:21:F6:1C:03:70:16:F4:CE:2C:37:71:9B:9E:FE:10:18:3B:8A:5F:4A:4F:2D:C9:F3:CF:74:15:20:14:3B:B4:47:40:38:31:03:41:69:57:03:A6:30:C2:2F:A5:E7:87:E0:04:56:98:5E:30:03:DE:04:72:E5:D0:7D:4E:5A:E7:A6:81:B4:D3:86:52:A1:B8:E0:AF:B7:03:F3:7E:17:08:74:8C:CA:19:B8:E4:67:8E:BC:A0:2E:58:C5:7A:B8:1E:64:0E:02:16:25:E0:9D:3D:CB:BF:2E:45:BE:33:5E:39:AD:06:23:3C:9D:72:B5:18:77:F7:6A:6E:01:B5:84:27:0E:5F:59:8F:69:F1:00:EE:D5:77:9C:E4:F6:E0:0C:92:CB:27:AD:05:D5:BD:69:DC:99:01:9B:B5:C7:EC:AC:E2:49:15:B1:E6:B5:3A:E3:11:F0:05:12:55:ED:F5:41:9B:97:FB:D8:26:A9:DF:71:D2:54:15:5B:BA:E3:C8:E4:53:62:E1:27:29:3C:86:36:32:EE:E7:5F:E1:DC:8D:22:21:DA:32:76:29:61:E9:85:23:2F:09:70:1E:03:D6:BF:82:63:8E:CA:6F:BA:79:86:6A:87:FB:67:39:2C:C4:25:6C:A2:30:74:68:43:02:03:01:00:01

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *FB:CE:50:0C:66:D7:39:07:33:CB:B9:94:4C:12:C5:11:FD:97:9C:5B*

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

Authority Key Identifier *3C:DF:CA:B3:5A:3C:39:1E:8C:E6:E2:39:82:70:0A:89:AC:FD:2E:F6*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl003_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EC:33:D1:70:93:C0:F4:5B:B8:A2:7E:B9:E3:05:69:65:83:80:1F:61:44:B8:E9:D4:9E:73:A8:E3:0A:2A:2E:20*

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

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

Status Starting Time *2021-12-06T13:28:03Z*

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.10.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.10.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010*

Service Digital Identity

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.10.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.10.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0010*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *+85QDGbXOQczy7mUTBLFEf2XnFs=*

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

Status Starting Time *2015-06-03T23:00:01Z*

2.10.4.3 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.11 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0011

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0011*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3355974077051950438*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGwjCCBKggAwIBAgIILpLQpHIZ1WYwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDMwHhcNMTYwNzE1MjAxODIyWhcNMjIwOTE0MjAxODIyWjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmFDdXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArRBctjVZeSKQkByDvTBvxTU4
AF8MUuDgfIl8Z9/DyobpQ8lbwNe4uZQlmSSoumRC8iC5YOqzKgfgiyPEZ1sIlmBMcqPKy9RZa9lq
cG0DiQUFuMdbwFA9wLVYmbpfF0hh5aXRtfK6BmjiCLy0RYtBFG3codkSok7jdIpiceZA6K++tunk
erNo8vynyRGhajrYEd8mrddwB/O95rPtDcIWKejyPtHEuqqLzw6+jNh5FztuhxhF+B+VjZGXTui4a
IQsDAIGoMqPo+gzTKI0FoYXGLtpizX5C6sqF3dyQYpd/eXitatTPCLc4ZAQwAXg4KL7uyEemj340
IvyhD+4vMF9UxwIDAQABo4ICLDCCAigwTAYIKwYBBQUHAQEEQDA+MDwGCCsGAQUFBzABhjBodHRw
Oi8vb2NzcC5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL29jc3AwHOYDVR0OBBYEFJ1a
Xm7C/6OUleVon45YOYAUKLNUvMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUPN/Ks1o8
OR6M5ul5gnAKiaz9LvYwggEZBgNVHSAEggEQMIIBDDBmBgpghGwBAQECBAAHMFgwVgYIKwYBBQUH
AgEWSmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2RwYy9j
Y19lY19jaWRhZGFvX2RwYy5odG1sMG4GC2CEbAEBAQIEAAECMF8wXQYIKwYBBQUHAgEWUWh0dHA6
Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL3BjL2NjX3N1YiUY19j
aWRhZGFvX2Fzc3FfcGMuaHRtbDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cuc2Nl
ZS5nb3YucHQvcGNlcnQwVwYDVR0fBFAwTjBMoEggSIZGaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFk
YW8ucHQvcHVibGljby9scmMvY2NfZWNfY2lkYWRhb19jcmwwMDNfY3JsLmNybDAOBgNVHQ8BAf8E
BAMCAQYwDQYJKoZIhvcNAQELBQADggIBADK7SkveHEgf4sHNAjCpcqOZ2nKsX/PEbpDj1KYRdFMc
73H/iTwoBQHSfHLxOqZN7FyQuh8L/UaXtjIN6y5V7LTFk/1mTkhp1wtszsxbNhaTs/D7Tb1EaKqT
G0Ze779MEeUCuIVxeYLqTSEew33YA9X1RTC7dESr5D2xiqXfkJhZb/+Czj+ZvFFY+wkHJ5Vm0opK
V9ZTdRohy7vEaUdVTjn2FN/ftaasQNFVUGRj4LULwuYlTTwhF6dChXAwMZt0iTnnyykyC7wsJJS1
TmWDaT4rHiYU+RUU3VuANpObGFfl/CxH8Gpi1GwNJsyfgoD1EoUHXnrEEwK5rTAdBjnnb3p15F
AKu43Ry1gozp16WMAQgnF6TOBRjOsMOiGF6BEWt/sn220S5DFwL24XfIlxd8A0P5t1setpdGl6zo4
w8VAiZraqIYaX8phhBxxOl+TNmphUjjXy9Ndhan1FzpmWsUJx4/cHsEsXPgHFYrgJp3YlWY4DOWW
nBXBWi5FtHdjG5LXPaKdJw4YPyao35V8muWrkrs52PcLRxO/Gbk5s4UHXYSCQld+RbN0sOySdPw/
tN/ZinK9wW5ML5cGQ4caqNg8Ex6TkkLFned2NdkxjOY2aRjizcjEwqvl/U9ODN45H6+6tqfBq4ys
he0I+896aAnwEDIV7Y5FIxc5rfoxh4f/

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 003*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0011*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Fri Jul 15 22:18:22 CEST 2016*

Valid to: *Wed Sep 14 22:18:22 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:AD:10:5C:B6:35:59:79:22:90:90:1C:83:BD:30:6F:C5:35:38:00:5F:0C:52:E0:
E0:7E:59:7C:67:DF:C3:CA:86:E9:43:C9:5B:C0:D7:B8:B9:94:08:99:24:A8:BA:64:42:F2:20:B9:60:EA:B3:2A:07:E0:8B:23:C4:67:5B:08:22:60:4C:72:A3:CA:CB:D4:59:6B:D9:6A:70:6D:03:8
9:05:05:B8:C7:5B:C0:50:3D:C0:B5:58:99:BA:5F:17:48:61:E5:A5:D1:B5:F2:BA:06:62:62:08:BC:B4:45:8B:41:14:6D:DC:A1:D9:12:A2:4E:E3:74:8A:62:71:E6:40:E8:AF:BE:B6:E9:E4:7A:B3
:6B:F2:FC:A7:C9:11:A1:6A:3A:D8:11:DF:26:AD:D7:70:07:F3:BD:4A:B3:ED:0D:C5:8A:78:9C:8F:B4:71:2E:AA:A2:F3:C3:AF:A3:36:14:85:CE:DB:A1:C6:11:7E:07:E5:63:64:65:D3:BA:2E:1A:
95:08:03:00:81:A8:32:A3:E8:FA:0C:D3:2A:5D:05:A1:85:C6:2E:DA:62:CD:7E:42:EA:CA:85:DD:DC:90:62:97:7F:79:78:AD:6A:D4:CF:08:B7:38:64:04:30:01:78:38:28:BE:EE:C8:47:A6:8F:
7E:34:96:FC:A1:0F:EE:2F:30:5F:54:C7:02:03:01:00:01
```

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *9D:5A:5E:6E:C2:FF:A3:94:79:5A:27:E3:96:0E:60:05:0A:2C:D5:2F*

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

Authority Key Identifier *3C:DF:CA:B3:5A:3C:39:1E:8C:E6:E2:39:82:70:0A:89:AC:FD:2E:F6*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl003_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2C:9C:84:AF:13:6B:AA:10:B6:F6:E8:5C:EC:A0:83:3E:2A:EB:D6:65:27:C9:11:2D:BD:F0:C2:AB:8E:A8:2E:A6*

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0011*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *nVpebsL/o5R5Wifjlg5gBQos1S8=*

Service Status

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

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

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *https://pki.cartaodecidadao.pt/*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

2.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.12 - Service (withdrawn): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1153025449084049349*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGwjCCBKgAwIBAgIIEABeiXWj18UwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVOQKDDdTQ0VFIC0gUZlzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDMwHhcNMTcwNjI4MTQ0NjE0WhcNMjMwODI4MTQ0NjE0WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmFOdXJhlERpZZl0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDEyMIIBIjANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxwneT7ZHI+Lc/g/YugFRUALg
4xOQ00mB+SWqA7HA5XMe+kpmcohw1U05Y+kFVd1UjlhHrjRo8RNm1YIB9pw08VElZaM25xdleQs
vayVhc5SfLJz3icDyO0gviS2UFBtONYj/zMDFRrd/65n9KvhKXbjNUE7k1StSlEstXP5YS60fkuR
CcoigEhyl/by3j97YBECvGdUFeNUy8lem1jnawg6yY/sL95SU/yR002ocrj6P3c9BG4yAElgoDbc
jnL88WB90C7VobQVo7UPaJlb9oF/hqfm0dX0EO8AJAQICTHAZ7VNg9dHbcXlXxcyJMQW3K23OVty
8AnoMD9wLltOhwIDAQABo4ICLDCCAigwTAYIKwYBBQUHAQEEQDA+MDwGCCsGAQUFBzABhjB0dHRw
Oi8vb2NzcC5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL29jc3AwHQYDVR0OBBYEFPrE
x92mhVNZ7SKg4/7NqAconnGaMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUPN/Ks1o8
OR6M5ul5gnAKiaz9LvYwggEZBgNVHSAEggEQMIIBDDBm8gpghGwBAQECBAAHMFgwVgYIKwYBBQUH
AgEWSmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2RwYy9j
Y19IY19jaWRhZGFvX2RwYy5odGl5sMG4GC2CEbAEBAQIEAAECMFBwXQYIKwYBBQUHAgEWUWh0dHA6
Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL3BjL2NjX3N1Yi1IY19j
aWRhZGFvX2Fzc3FfcGMuaHRtbDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cuc2NI
ZS5nb3YucHQvcGNlcnQwVwYDVR0fBFAwTjBMoEggSIZGaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFk
YW8ucHQvcHVibGljby9scmMvY2NfZWNfY2lkYWRhb19jcmwwMDNfY3JsLmNybDAOBgNVHQ8BAf8E
BAMCAQYwDQYJKoZIhvcNAQELBQADggIBAIGSo2J4Zw/bG5dXpHaF6zEsZE5ku+2oguHW6l/I3Etr
P0zmr4AfcNZQ18fYng2Vj5qV1vefOqVoD5K5lsnz8VxoIRaulhrjdDz0MxdwiuNiit Q8mwx7D8ZP
nLNq53gim6XJxIvIB0/HwHJF77Wvy0zTA55xwUpylS+qQUP2vbnUkv6qRniMb5zzB1V/INIFwx87
Rw7YgQWicxi08lamq/GvBhRenoG8blYsv3iq24KQWPtXqRe+6sK+m6Ntj/NXzMHAng0R4h9pOeGn
yyXOcvUvmVXsT6z2Mi5IZ2Hoe9dMeErXC4fmAljCf6VNoX9W1b5iERB95l/z9nDUHg0yLmuGUV5E
/6/QrresHCktkBmJzGtBcK0uSPqKsXp20GrxHeN0j1ICgmtIWkge4AJfOLpzJwKQJr/1zúsrslSh
DPX1oiK/h7BFh//+ZGf8TKoIbbBXaWZdcwlszCVJo6rG7150CÛevWd+Gm2/WzqQD5EVi01Q8Pzfg
4SbP3jrrotXUPcz1axU8nmuhM5TNT4e+neu3IlgXRlKvv5SOAcKA/8ohvePBMg2VzUQoAghTvGWw
lpgjYslZd52SY53p8HCuYuly9pPU3RFu2UF/TPQ7TxsdhD6CCEIgkuCgACVokEgtUMV9m/CftlN9
i2Z9balUumnMYg6IzIYm+sHmAN/w2c3I
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 003*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012*
Subject OU:	*subECEstado*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*
Valid from:	*Wed Jun 28 16:46:14 CEST 2017*
Valid to:	*Mon Aug 28 16:46:14 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:C7:09:DE:4F:B6:47:97:E2:DC:FE:0F:D8:BA:01:51:50:02:E0:E3:13:90:D3:49:81:F9:25:A0:03:B1:C0:E5:73:1E:FA:4A:66:72:88:70:D5:4D:12:63:E9:05:55:DD:54:8C:98:62:1E:B8:CF:A3:C4:4D:9B:56:08:07:DA:70:D3:C5:44:95:96:8C:DB:9C:5D:95:E4:2C:BD:AC:95:85:CE:52:7C:B2:73:DE:27:03:C8:ED:20:BE:24:B6:50:50:6D:38:D6:23:FF:33:03:15:1A:DD:FF:AE:67:F4:AB:E1:29:76:E3:35:41:3B:93:54:AD:48:81:2C:B5:73:F9:61:2E:B4:7E:4B:91:09:CA:22:80:48:72:27:F6:F2:DC:9F:7B:60:11:02:8C:67:54:15:E3:54:CB:C9:5E:9B:58:E7:6B:08:3A:C9:8F:EC:2F:DE:52:53:FC:91:D3:4D:A8:72:B2:7A:3F:77:3D:04:6E:32:00:42:20:A0:36:DC:8E:72:FC:F1:60:7D:D0:2E:D5:A1:B4:15:A3:B5:0F:6A:32:1B:F6:81:7F:86:A7:E6:D1:D5:F4:10:EF:00:24:04:25:09:31:C0:67:B5:4D:83:D7:47:6D:C5:E5:5F:17:32:24:C4:16:DC:AD:B7:39:5B:72:F0:09:EB:30:3F:70:2C:8B:74:87:02:03:01:00:01*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Subject Key Identifier	*FA:C4:C7:DD:A6:85:53:59:ED:22:A0:E3:FE:CD:A8:07:28:9E:71:9A*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*3C:DF:CA:B3:5A:3C:39:1E:8C:E6:E2:39:82:70:0A:89:AC:FD:2E:F6*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html* *Policy OID: 2.5.29.32.0* *CPS pointer: http://www.scee.gov.pt/pcert*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl003_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DB:B6:0D:2A:5A:01:D0:C7:47:5B:8F:73:43:F2:3F:DD:39:33:53:88:65:4B:05:09:8C:2D:61:8E:48:3F:6B:60*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012*
Subject OU:	*subECEstado*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I *+sTH3aaFU1ntIqDj/s2oByiecZo=*

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

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

Status Starting Time *2023-12-05T12:00:54Z*

2.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.12.2 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert, 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.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Description

2.12.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0012*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *+sTH3aaFU1ntIqDj/s2oByiecZo=*

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

Status Starting Time *2017-12-27T01:00:00Z*

2.12.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.12.3.2 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert, 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.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Description

2.13 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0013

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0013*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2856484774989273598*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGwjCCBKqgAwIBAgIIJ6RFxL+MGf4wDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXNOYWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDQwHhcNMTcwODE3MTM0NzQ5WhcNMjkwODE3MTM0NzQ5WjCBjDELMAkGA1UEBhMCUFQxHDAaBgNV
BAoME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmFtdXJhIlERpZJlOYWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDEzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0XnQ72OIYA57hdxoZqfFhDXE
wmejYUw1nGPwP+mbOsSSVTCVPJ6YT/rZRUBGR39HvFSyyBJCagRqcUui22RLGmgIegGmG75nSveU
cfvd/IoY+01tVrMXM3iRjiVWRqmiKq9IoqksKX7jt3NI6EsGjDyGVGtWO47WHQrQCnIUgt+a0n+3
Y5MVN0tjkEw1uDGuc4mh+LLjEzjgZDecRUuqoTXwQK5pj3/A0i20tqJgLhOjNi2W+JEznlnfUKo9
iqU/s6vDVrPTMqwI1NWp7LT3W9MxU539IbyHZWnQ580f+Ff19DKdkCq261a4KnEiNcuCSwfYIHWIU
xEwG+pjKPrM8vQIDAQABo4ICLDCCAigwTAYIKwYBBQUHAQEEQDA+MDwGCCsGAQUFBzABhjBodHRw
Oi8vb2Nzcc5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL29jc3AwHQYDVR0OBBYEFKlm
Jxb5FiEDauANuYuKS19/cYkiMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUGXYMrv4B
YWIEtkHz6Q4c8L7nTowggEZBgNVHSAEggEQMIIBDDBmBgphKwBAQECBAAHMFgwVgYIKwYBBQUH
AgEWSmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2RwYy9j
Y19IY19jaWRhZGFvX2RwYy5odG1sMG4GC2CEbAEBAQIEAAECMF8wXQYIKwYBBQUHAgEWUWh0dHA6
Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL3BjL2NjX3N1YiJlY19j
aWRhZGFvX2Fzc3FfcGHAaHRtbDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cuc2Nl
ZS5nb3YucHQvcGNlcnQwVwYDVR0fBFAwTjBMoEqgSIZGaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFk
YW8ucHQvcHVibGljby9scmMvY2NfZWNfY2lkYWRhb19jcmwwMDRfY3JsLmNybDAOBgNVHQ8BAf8E
BAMCAQYwDQYJKoZIhvcNAQELBQADggIBAHdHGzy8lIBkEdZYzQtzoHEOOGGvmDjcpzetz4/nZLo
DDjZPAgHYkjyZx8AL229etMvgm7WYvpJbcT5cdntaOBDMhpyFAQZr08INJBetKTUn7+7Wbouq2cc
ggRkSbHlClmgJxF6kWX47YD3cWxDpy8zBJRCnHsw/OnLEuHb99YDZ3QCBHCclNEwbL9q5vLM/T04
uhEWMHsbxtYstl/ZNJYw2dR9ezG6/AU4O7oxfcC7RlnYM82uJD/4GSP6Ns84KdH0Z4sDnjfRSQ2M
a/+a8HBCPHkHTQ2ffpSqc3k2rzZfnYYj9kbGwNJUW8X1HtGQYFaGswnzlCLtU7O6kPtFhyX9ZuG
SD5OWShOTYcpyuLFp3gjJ7fY+rF3VcbtXj7je435bE7XNikK2gRYF43ewu7gAvo22jzHn/RJHP
f+IBT1luXx7dn2YHvWYeH3W2PEkovHXTQ0vgAq4RkX3DU+PoAwa6kDJYRmj0WfbD0IWp/vQI4B7
wtpLNhdg9FA/HfBaISWdDyRKETQp/F7Lj541/cc8WHdPsMxTvQvDXe7qGY3FbdyMGRBuo9ONp+Oo
1T3dlYCEbVcKXwI4yfV+0ynmcy76WWwbaCusFVBcXGYzLUpJtMkd84rq7nl++MHVBJHvD+OHi8Ji
uwIJGdp/3ZUshLC9rcPFYHf2G4o8ifM/

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 004*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0013*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu Aug 17 15:47:49 CEST 2017*

Valid to: *Fri Aug 17 15:47:49 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:D1:79:D0:EF:63:88:60:04:BB:85:DC:68:66:A2:45:84:35:C4:C2:67:89:61:4C:
35:9C:63:F0:3F:E9:9B:3A:C4:92:55:30:95:3C:9E:98:4F:FA:D9:45:40:46:47:7F:47:BC:54:B2:C8:12:42:6A:04:6A:71:4B:A2:DB:64:4B:1A:68:25:7A:01:A6:1B:BE:67:4A:F7:94:71:FB:DD:FC
:8A:18:FB:4D:6D:56:B3:17:33:78:91:8E:25:56:46:A9:A2:2A:AF:48:A2:A9:2C:29:7E:E3:B7:73:48:E8:4B:06:8C:3C:86:54:6B:56:3B:8E:D6:1D:0A:D0:0A:78:94:82:DF:9A:D2:7F:B7:63:93:1
5:37:4B:63:90:4C:35:B8:31:AE:73:89:A1:F8:B2:E3:13:32:60:64:37:9C:45:4B:AA:A1:35:F0:40:AE:69:8F:7F:C0:D2:2D:B4:B6:A2:60:2E:14:23:36:2D:96:F8:91:33:9E:59:DF:50:AA:3D:8A:
A5:3F:B3:AB:C3:54:F4:CC:AB:02:35:35:6A:78:2D:3D:D6:F4:CC:54:E7:7F:62:6F:21:D9:5A:74:39:F3:47:FE:15:FD:7D:0C:A7:64:0A:AD:BA:D5:AE:0A:9C:48:8D:72:E0:B9:C1:F6:08:1D:62:
14:C4:4C:06:FA:98:CA:3E:B3:3C:BD:02:03:01:00:01
```


Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *A9:66:27:16:F9:16:21:03:6A:E0:0D:B9:8B:8A:4B:5F:7F:71:89:22*

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

Authority Key Identifier *19:76:0C:AE:FE:01:61:69:44:B6:41:EB:CF:A4:38:73:C2:FB:9D:3A*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl004_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D6:5D:ED:68:A1:89:63:4D:67:F5:71:27:9B:D9:94:BC:C0:C0:2E:2A:57:A2:FD:71:80:67:3E:35:8D:00:37:C8*

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0013*

Subject OU: *subECEstado*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *qWYnFvkWIQNq4A25i4pLX39xiSI=*

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

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

Status Starting Time *2017-12-27T01:00:00Z*

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

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Description

2.13.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

2.14 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0014

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] *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0014*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2397598264976225653*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG9zCCBN+gAwIBAgIIIUX660lANXUwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVOQKDDdTQ0VFIC0gUZlzdGVtYSBkZSBDZXj0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFktbzEgMB4GA1UEAwwXQ2FydMCjbyBkZSBDaWRhZMOjbyAw
MDQwHhcNMTgwMzAxMTQwMjIzWhcNMzAwMzAxMTQwMjIzWjCBwTELMAkGA1UEBhMCUFQxMzAxBgNV
BAoMKkluc3RpdHV0byBkb3MgUmVnaXN0b3MgZSBkbyBOb3RhcmlhZG8gSS5QLjEcMBoGA1UECwwT
Q2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8xSTBHBgNVBAMMQEVDIGRl
IEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkby BOYXj0w6NvHGRlIENpZGFkw6NvIDAw
MTQwgqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCqXSLo9jrVNBglFomch0Ood2KuwUu3
b/T4xflMt9P2JXnKG9ffQM3JhqoMuhn9pDm+t0Jl8w5plNk8RDBpkCAoRrbTMVEXSzS4dFozU6HL9
q1pbvxwArnhJa48WTL4r3a/dzF3H7g5cC/vrW8ueefhXycLlUeZ/8c7KCjrWJiKYktIlyqpQlA68
8GSoNr2LVckxsKu7v4yc5yCV6Y5ir7V2jBsAN8yuT+nVTyghAOfo8GzfWdChmHBRVEsIC3EpEwc1
0amu6YqE+o14vY1B/6CSUhPtJyEOQDCsPsVn963ImTE3Dr6KH5shWxukVLMgRa5ItV4I3OJ8JzMO
lmSCNoS5AgMBAAGjggIsMIICKDBMBggrBgEFBQcBAQRAMD4wPAYIKwYBBQUHMAGGMGh0dHA6Ly9v
Y3NwLnJvb3QuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDAdBgNVHQ4EFgQU5wv+goU0
F/jzjx/3UN7VWC7qH7owEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBQZdgyu/gFhaUS2
QevPpDhzwvuq0jCCARkGA1UdIASCARAwggEMMGYGCmCEbAEBAQIEAAcwWDBWBggrBgEFBQcCARZK
aHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvZHBjL2NjX2Vj
X2NpZGFkYW9fZHBjLmh0bWwwbgYLYIRsAQEBAgQAAQIwXzBdBggrBgEFBQcCARZRaHR0cDovL3Br
aS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2Nfc3ViLWVjX2NpZGFk
YW9fYXNzcV9wYy5odG1sMDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cDovL3d3dy5zY2VlLmdv
di5wdC9wY2VydDBXBgNVHR8EUDBOMEygSqBIhkZodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5w
dC9wdWJsaWNvL2xyYy9jY19lY19jaWRhZGFvX2NybDAwNF9jcmwuY3JsMA4GA1UdDwEB/wQEAwIB
BjANBgkqhkiG9w0BAQsFAAOCAgEAvby1N64NvjTDacRpcJaxFFU3UWg0rm3OfkInFeCWiiiFLiS2
OmnlzUl96bcL1VEKtGhgZqLObIrFyAjhgj3cG3XnbHZvG257lwvL7LmenHAv4Ie55hORKB6MsST3
dsZd103ECfbG9wvL6wGXf0LrOr9ehuSN6PFHnkpXmGLaIDLC44Y+8gNb5jcAoiBe2XvyjYTVE5Wm
UTGfzP4czm+ail0cWAhSZb+YXN/2r9kZWhxBQpFwoD62h5sen5ZYjQX5F7qBB0w0M4HCs1jH+pEF
nzLyOIHI/M+ZOYQw+NMMXsWM29gWlkR03YKlLA+s85xl2Gramh+EfuRsXFRdwdnXi9nAaj1hoIMn
o0HjHUwCl/hYN+ztJL1WOJKXNmv2OeOd4tbtLAFP6cqNfzjUBknWxjlOXYgfM1bfeaDxQ2L+J01c
Qtx66aGWeiB61BpcgqQoQPv2lFBt5djlAULXmjgr9oUlOYKcH4V8rUkx8kBEX8/Dq4vMTwSi0wN+
nves4vNkHhWFg6hYlKUt7SMYn/o+pf4AV19K5BUUGgeUxnw9Q/H+6NOskdnC5c+9w8Pd320aDyLZ
vUuthwYj+E5dBZWrzdOBqY+BYMZTV7XI7jXO4msrbGT9bhtraUVtY0wSDKxj5AGCrwu23BctFj6O
kEgZZfmsmbevtLqXzccFUsReOzk=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 004*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0014*

Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*
Valid from:	*Thu Mar 01 15:02:23 CET 2018*
Valid to:	*Fri Mar 01 15:02:23 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:AA:5D:22:E8:F4:9A:D5:37:CA:A5:16:89:9C:87:44:28:77:62:AE:C1:4B:B7:6F:F4:F8:C5:F9:4C:B7:D3:F6:25:79:CA:1B:D7:DF:40:CD:C9:86:AA:0C:BA:19:FD:A4:39:BE:B7:42:7C:C3:9A:48:36:4F:11:0C:1A:64:08:0A:11:AD:B4:CC:54:45:D2:CD:2E:1D:16:8C:D4:E8:72:FD:AB:5A:5B:BF:1C:00:AE:78:49:6B:8F:16:4C:BE:2B:DD:AF:DD:CC:5D:C7:EE:AE:5C:0B:FB:EB:5B:CB:9E:79:F8:57:C9:C2:C8:51:E6:7F:F1:CE:CA:08:9A:D6:26:22:98:2A:D9:48:CA:AA:50:94:0E:BC:F0:64:A8:36:BD:8B:55:C9:31:B0:AB:BB:BF:8C:9C:E7:20:95:E9:8E:62:AF:B5:76:8C:1B:00:37:CC:AE:4F:E9:D5:4F:28:21:01:07:E8:F0:6C:DF:59:D0:A1:98:70:51:54:4B:25:0B:71:29:13:07:35:D1:A9:AE:E9:8A:84:FA:8D:78:BD:8D:41:FF:A0:AC:52:13:ED:27:21:0E:40:37:2C:3E:C5:67:F7:AD:C8:99:31:37:0E:BE:8A:1F:9B:21:5B:1B:A4:54:B3:20:45:AE:65:B5:5E:08:DC:E2:7C:27:33:0E:96:64:82:36:84:B9:02:03:01:00:01*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Subject Key Identifier	*4B:0B:FE:82:85:34:17:F2:73:8F:1F:F7:50:DE:D5:58:2E:EA:1F:BA*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*19:76:0C:AE:FE:01:61:69:44:B6:41:EB:CF:A4:38:73:C2:FB:9D:3A*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html* *Policy OID: 2.5.29.32.0* *CPS pointer: http://www.scee.gov.pt/pcert*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl004_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1E:AF:84:01:88:B1:4F:9D:D1:2C:07:AC:A3:43:E1:96:C3:8D:8F:52:56:B1:E3:6F:FF:51:9A:44:2B:DA:53:EE*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0014*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

X509SKI

X509 SK I *Swv+goU0F/Jzjx/3UN7VWC7qH7o=*

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

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

Status Starting Time *2018-06-10T23:00:00Z*

2.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Description

2.15 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0015

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8405128266739339248*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIH9zCCBd+gAwIBAgIIdKUDoFaXz/AwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXNOYWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDQwHhcNMTgwNjI3MTI1MzMwWhcNMzAwNjI3MTI1MzMwWjCBwTELMAkGA1UEBhMCUFQxMzAxBgNV
BAoMKkluc3RpdHVv0byBkb3MgUmVnaXN0b3MgZSBkbyBDb3RhcmlhZG8gSS5QLjEcMBoGA1UECwwT
Q2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8STBHBgNVBAMMQEVDIGRl
IEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENpZGFkw6NvIDaw
MTUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC55oMBzWnnpeZ9CiW90wV/6uNWhNws
UwCI30CpykMQ7rt0W9O5bsNIXkppt PqW6VnSvvzWjINSvlOYKAc3puVquAp77CA2+0k4fs0nayZ
go734EOj0nYwc5Kr3Du1yLH3CQZTwMB/ubHE3ccSQHwMGh3/mIQGzHQI4q8vEATZel9IAk8RYQS
X7H44i+5ahhiNHLi8ys+3/sMmrOEBLo/Nt1OdWdLDd4qODXJlW0QHzwunhjTXifS6ckvf2lDIlgE
GuleLmg7j2ixiEuFbePPPv4ZkNLXzJ4ny2UCBjr4OvbhcNfrKLK00107lhmhcgB8K0iPF+WOJvJ1
OLkMldZfroLHrfM8MU/6fdGAwIzvfRMjK6+lEZDZXxNiD/SccQPCXu1mJtgeuCLmu+cDnFzPswGg
Fstu6QLWOKrqumido2bGei7lOK1AM5QORhY5FKRbtTPHAFsMTnGHjNUIq0Nmo28CjXOtz6uqDL4F
I/Gtgb4/c+kGuPrraLtAkCnh9LbZLhQf63fN1WUwcGpl0K6gvIYtFg2dDw72YpbDP5MaRLSu20VP
jDTyEzP/9b9wApbLhrVYtWRvzaDFMfTixLEOFF5q1nmT1mQkpdUwlK0X3AvETKzypGPePhrTV9AK
lpF2mvP9pLTwk9dRPzfiXRFNSGhPll1GDJSgKlMpynLhAQIDAQABo4ICLDCCAigwTAYIKwYBBQUH
AQEEQDA+MDwGCCsGAQUFBzABhjBodHRwOi8vb2NzcC5ybZ90LmNhcnRhb2RlYZlkYWRhby5wdC9w
dWJsaWNvL29jc3AwHQYDVR0OBBYEFKbQ79SADAWrpj55NvSjGMfLxweGMBIGA1UdEwEB/wQIMAYB
Af8CAQAwHwYDVR0jBBgwFoAUGXYMrv4BYWIEtkHrz6Q4c8L7nTowggEZBgNVHSAEggEQMIIBDDBm
BgpghGwBAQECBAAHMFgwVgYIKwYBBQUHAgEWSmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vcG9saXRpY2FzL2RwYy9jY19JYWRhZGFvX2RwYy5odG1sMG4GC2CEbAEBAQIE
AAECMF8wXQYIKwYBBQUHAgEWUWh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28v
cG9saXRpY2FzL3Bjl2NjX3N1Yi1lY19jaWRhZGFvX2Fzc3FtcGMuaHRtbDAyBgRVHSAAMCowKAYI
KwYBBQUHAgEWHGh0dHA6Ly93d3cuc2NlZS5nb3YucHOvcGNlcnQwVwYDVR0fBFAwTjBMoEqgSlZG
aHR0cDovL3Bra5SjYXJ0YW9kZWNlpZGFkYW8ucHOvcHVibGljby9scmMuY2NlZWNfY2lkYWRhb19j
cmwwMDRfY3JsLnNvbDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAIRW2USZkcNC
wlcADbAw/vQfvGHGp+vECDlqFuYaJ7a3ZkCWRM6/s1gulz7H6xgnthOvqvFLwca9Hil9V+so+05T
c/26lhY1KT3q0R1ExX4yymZQm2H+W+hTCBs3P4OQmxMloHjCT84Q6x2VlUNtgrTlTkAMjhnMAJi
F4DEqFPUWXv8uwArWu1EaJlblh5EaFPn3GGFF7Omwxc15ZTuPakaZRL9X3hIDlG3XfRZppzyRqtvQ
o+znNFpbNuVuhSy7dy9QgqibNcyntrePvM/0BJWpOgZXo8Z4HnzGLpQ1n5SHcnfqKXxB6C4zwES9
MxbBRW1wGE0w99XpEpiZs+gwcc/Kclx7Fsmvx6NOAQjBhej9aUGJNziXkGFyN6rW+St8sOc2eAFU
BBLvS73hWQpC6uLTwjY2p1ZhbPy1mroEd9IbinQSUf7j39IUQWJwOwI3GjezS0qDE62cX5WpdJAC
u8yavjFy+ki30brdCOPrvE+z7YjW0WEEd0Xu0jZ/nPpLD0ATvNg/i531hQW5uajdLw9+YaUHB335
qjVCJc1Jyl5CnCugIgcu+qNCHyKaXI62jfd5oURYwoEMtHw+/LCLgFx15TakvjUtXv3QGk6IW3MC
uCfDm+vy0IlNoScXWjSLWEvX4CV5Cx9UyBoTAgS0UmAw5ZiNq0K/9U0gSPcrKq74

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 004*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0015*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

Valid from: *Wed Jun 27 14:53:30 CEST 2018*

Valid to: *Thu Jun 27 14:53:30 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:B9:4A:83:01:CD:69:E7:A5:E6:7D:0A:25:BD:D3:05:7F:EA:E3:56:84:DC:2C:53
:00:88:0F:40:A9:CA:43:10:EE:BB:74:5B:D3:B9:6C:8B:0D:21:79:29:A6:D3:EA:5B:A5:67:4A:FB:F3:5A:32:0D:4A:F2:0E:60:A0:1C:DE:9B:95:AA:E0:29:EF:B0:80:DB:ED:24:01:FB:34:9D:AC:
99:82:8E:F7:E0:43:A2:D2:76:30:73:92:AB:DC:3B:B5:CB:B1:F7:09:06:53:C0:C0:7F:B9:B1:C4:DD:C7:12:40:7C:0C:1A:1D:E2:FE:62:10:1B:31:D0:23:8A:BC:BC:40:18:65:E9:7D:22:40:3C:4
5:8D:12:5F:B1:F8:E2:2F:B9:6A:18:62:34:72:E2:F3:2B:3E:DF:FB:0C:9A:B3:84:04:BA:3F:36:DD:4E:75:67:4B:0D:DE:20:38:35:C9:21:6D:10:1F:3C:2E:9E:18:D3:5E:27:D2:E9:C9:2F:7F:69:
43:8A:58:04:1A:E2:1E:2E:68:3B:8F:68:B1:88:4B:85:6D:E3:CF:3E:FE:19:90:D2:D7:CC:9E:27:CB:65:02:06:3A:F8:3A:F6:E1:70:D7:EB:28:B9:34:D3:5D:3B:96:19:A1:72:00:7C:2B:48:8F:17
:E5:8E:26:F2:75:38:B9:0C:95:D6:5F:AE:82:C7:AD:F3:01:31:4F:FA:7D:D1:80:C2:5C:EF:7D:13:23:2B:AF:88:11:90:D9:5F:13:62:0F:F4:9C:71:03:C2:5E:ED:66:26:D8:1E:B8:22:E6:BB:E7:0
3:9C:5C:CF:B3:01:A0:16:CB:6E:E9:02:D6:38:AA:EA:BA:68:9D:A3:66:C6:7A:2E:E5:38:AD:40:33:94:0E:46:16:39:14:A4:5B:B5:33:C7:00:5B:0C:4E:71:B7:8C:D5:1F:AB:43:66:A1:9F:02:8D
:73:AD:CF:AB:AA:0C:BE:05:97:F1:AD:A9:BE:3F:73:E9:06:B8:FA:EB:68:BB:40:90:29:E1:F4:B6:D9:2E:14:1F:EB:77:CD:D5:65:30:70:6A:48:D0:AE:A0:BE:56:2D:16:0D:9D:0F:0E:F3:62:96:
C3:3F:93:1A:44:B4:AE:DB:45:4F:8C:34:F2:13:33:FF:F5:BF:70:02:96:CB:86:B5:58:B5:64:6F:CD:A0:C5:31:F4:E5:C4:B1:0E:14:5E:6A:D6:79:93:D6:64:24:A5:D5:30:94:AD:17:DC:0B:C4:4
C:AC:F2:A4:63:DE:3E:1A:D3:57:D0:0A:96:91:76:9A:F3:FD:A4:B4:F0:93:D7:51:3F:37:E2:5D:11:4D:48:68:4F:96:5D:46:0C:94:AA:2A:53:29:CA:72:E1:01:02:03:01:00:01
```


Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *A6:D0:EF:D4:80:0C:05:AB:A6:3E:52:36:F4:89:18:C7:CB:C7:07:86*

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

Authority Key Identifier *19:76:0C:AE:FE:01:61:69:44:B6:41:EB:CF:A4:38:73:C2:FB:9D:3A*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

Policy OID: 2.16.620.1.1.1.2.4.0.1.2

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl004_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *38:B3:49:37:90:24:E0:7B:43:BB:6C:20:36:DD:F3:13:5E:BE:94:51:36:C2:08:37:27:5B:C4:D0:25:A5:47:04*

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0015*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

X509SKI

X509 SK I *ptDv1IAMBaumPlI29IkYx8vHB4Y=*

Service Status

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

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

Status Starting Time

2019-01-23T00:00:00Z

2.15.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.15.2 - Extension (not critical): Qualifiers [QCForESig]

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

2.16 - Service (withdrawn): Serviço de Validação Cronológica do Cartão de Cidadão 000002

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6256225402553284294*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIl5TCCBs2gAwIBAgIIVtKT21H2tsYwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmFOaXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE1MB4XDTE5MDExMDE0NDEzMloXDTI1MDcxMjE0NDEzMlowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDIwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC9/AZ+gwLLk1H2zj+3
F1yYs3zh0uArn/Uux/uPO6ela3+f/cTIVxNNd7rpXkfCrT+s/LKf3O1EfM2WQyDt7+KcXDkFvOak
aO21/bc9hjoNeO4HXEPOc82pQKmIjEUq4ZT+V7Nz4utX+mEVYFy/BRYxv1OgLWjaF25JfXjVgpUb
nLJeA04Hjpq9oxtUzUUjUA3Irlo9oVnI2OwuiLmuxpF2Xqxl9RCbQe3facG8R3150p/hY4EIja5D
GDW6aBwUqgD7VqTeiiGuT8KUqpHfh+sEOusFEd5spoUibr6p4cw1GW4eUfv/mpxPjQ9RGybY+G/w
3Q8cKamPriDlQLFKDFaFH5R0OS+aqfjHr33y2m6Ic7W6ovrQy22HbcOHuSpGdZqKPUiGTZYZZRfj
o6uV5I7Nwzpe1+opTACLGn2a3ETcLzDb/6CK3hCUqapL7+xDVhMvdN/VSXjN9KlYDK79gmIaIQtS
GQvAeZlNuuWqmbD81fZ2eHhwXhoTI2M0jtxf9rsCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUptDv1IAMBaumPIl29lkYx8vHB4YwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTVfZGVsdGFfcDAwMDEuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3BraS5jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdg1L
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Yi1Iy19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DIGnOnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1lLXN0YW1wIHRva2VuIGlzIGlzc3VlZCBhcyBhIHF1YWxpZmllZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWoZYaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9fYXNzaW5hdHVyYV9jcmwwMDE1X3AwMDAxLmNybDAdBgNVHQ4E
FgQUf9XMPXA8vqdevVPl/qbDzU+QZqQwDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQAnUYPtpmjNeezb+ODtODLgrKqzXOn7cXBpHuLQNC1VVJsq8zCqygmG6TE+B6CBGxuR2t87jru6
aMltYMHKURCnX/C2KgGuy1IgktYYbzay++6xo8F3KsVVdrDjz0oIaU9BTkVwr/ZjpZusdPL191XJ
vzZd1Ea7jGj98Q8K+E3wi45Ov5Qu+m0fdBryklW53OOfm4KpEkEOnWhgehzlI0QU4tbkcVmVeATd
NUUTZthIgIvaTRYqkHdAboBlYNySADfv1TdLIOibvZegnhK7iIOgGDdVQlN53LbJDAdCh56m8uWi
04LispBSym3Y/cpHcRowsi6x3DzSWEKFre6wMsRzh7QOBnrcFH4MX6jDIcRJagNpzieUYo/YrsJN
w/Cua+j1YpLKptkyy7oEceL6/h7xGYS5gLi94PuXEEvOmXpHud6CjbRQFASV+dq6A2JMHfM8I22X
nGXsPHPX3Zk08r0X4FpbHrRbnXb/GJd+R7Dkq/LpQMQryV9hHE3xo0OE1iuv/hcFQpu0A1U0hnC
W5gAG0zY9cXGL1UYmT+j0xCW0kc+XujSKvNHabXttAKC53jsbrk4cDOqTvv7yCvKnTfUDHYOhOo
l4lISRSPu9yZ3L+lR62nb8O2XPlQisaEG9AwM9FdGktLwMHgx/f78BcRZkoP1fCJX6/0961j9i8+
Jg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0015*

Issuer OU: *subECEstado*

Issuer OU:	*Cartão de Cidadão*
Issuer O:	*Instituto dos Registos e do Notariado I.P.*
Issuer C:	*PT*
Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000002*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*
Valid from:	*Thu Jan 10 15:41:32 CET 2019*
Valid to:	*Sat Jul 12 16:41:32 CEST 2025*
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:BD:FC:06:7E:83:02:CB:93:51:F6:CE:3F:B7:17:5C:98:B3:7C:E1:D2:E0:2B:9F:F5:2E:C7:FB:8F:3B:A7:88:6B:7F:9F:FD:C4:C8:57:13:4D:77:BA:E9:5E:47:C2:AD:3F:AC:FC:B2:9F:DC:ED:44:7C:CD:96:43:20:ED:EF:E2:9C:5C:39:05:BC:E6:A4:68:ED:B5:FD:B7:3D:86:3A:0D:78:EE:07:5C:43:CE:73:CD:A9:38:A9:88:8C:45:2A:E1:94:FE:57:B3:73:E2:EB:57:FA:61:15:60:5C:BF:05:16:31:BF:53:A0:2D:68:DA:17:6E:49:7D:78:D5:AA:95:1B:9C:B2:5E:03:4E:07:8E:9A:BD:A3:1B:54:CD:45:23:50:0D:C8:AE:5A:3D:A1:59:C8:D8:EC:2E:94:B9:AE:C6:91:76:5E:AC:48:F5:10:9B:41:ED:DF:69:C1:BC:47:7D:52:D2:9F:C7:63:81:08:8D:AE:43:1B:45:BA:68:1C:14:AA:00:FB:56:A4:DE:8A:21:AE:4F:C2:94:AA:91:DF:87:EB:04:3A:EB:05:11:D4:AC:A5:D5:22:6D:FE:A9:E1:CC:35:19:6E:1E:51:FB:FF:9A:9C:4F:8D:0F:51:18:26:D8:F8:6F:F0:DD:0F:1C:29:A9:8F:AE:20:E5:40:B1:4A:0C:56:9F:1F:94:74:39:2F:9A:A8:58:C7:AF:7D:F2:DA:6E:A5:73:B5:BA:A2:FA:D0:CB:6D:87:6D:C3:87:B9:2A:46:75:98:0A:3D:48:C6:4D:96:19:65:17:C9:A3:AB:95:E4:8E:CD:C3:3A:5E:D7:EA:29:4C:00:8B:1A:7D:9A:DC:44:DC:2F:30:DB:FF:A0:8A:DE:10:94:A9:AA:4B:EF:EC:43:56:13:2F:74:DF:D5:49:78:CD:F4:A2:18:0C:AE:FD:82:62:1A:95:0B:52:19:0B:C0:79:99:4D:BA:E5:AA:99:B0:FC:D5:F6:76:78:78:70:5E:1A:13:23:63:34:26:DC:5F:F6:BB:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*A6:D0:EF:D4:80:0C:05:AB:A6:3E:52:36:F4:89:18:C7:CB:C7:07:86*
Authority Info Access	*http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0015_p0001.crl*
Subject Key Identifier	*7F:D5:CC:3D:70:3C:BE:A7:5E:BD:53:C8:FE:A6:C3:CD:4F:90:66:A4*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*89:DF:7D:7F:BA:2B:84:05:63:E6:E5:61:D2:B0:74:75:72:A8:A8:6A:E2:92:BC:53:9D:65:4F:65:00:85:5B:0D*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000002*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*f9XMPXA8vqdevVPl/qbDzU+QZqQ=*

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

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

Status Starting Time *2025-10-27T13:00:00Z*

2.16.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000002*

Service digital identities

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000002*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*f9XMPXA8vqdevVPl/qbDzU+QZqQ=*

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

Status Starting Time *2019-01-23T00:00:00Z*

2.17 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0016

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7754940379922124339*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHxzCCBa+gAwIBAgIIa58VMCeXTjMwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXNOYWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDUwHhcNMTkwNTE0MTMxOTI2WhcNMzEwNTE0MTMxOTI2WjCBwTELMAkGA1UEBhMCUFOxMzAxBgNV
BAoMKkluc3RpdHV0byBkb3MgUmVnaXN0b3MgZSBkbyBOb3RhcmlhZG8gSSSQLjEcMBoGA1UECwwT
Q2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8xSTBHBgNVBAMMQEVDIGRl
IEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENpZGFkw6NvIDAw
MTYwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCvuXL3VYHyeWHw/UhjZXC9VEAooDcr
QAZin24heEUWY0KIL7A0sj3/WIDKUVAcBKzTyqIDwPlkyL4g04miLZbzBHtjfiO+BsNkQPX4KPF
10eQkt8W3alazDZ2FdC3Qq T0TArEbLVmT5a/wJrEKtOOXg0AFMQok9GiN1rEIQBn5bQoUfpJDkMS
72XMwzovTz1/Pggj9SDQRWOdgIceDr4oE8/LPccpB0hbtNkgwtwqnIcH7ccVTDK47eNUpPedUS/I
qjjk6QMNCi5Q92JZvpXPPXlmZaKPMPVM+CrGbRSFWwNWqpOzHNje60RPtb8qcXCKFDBlom7o0kTq
q4rpBG1vmIxdTH9TWvjNVanpYtevaNlkKutIpTjWp0qxDyhVrWm5o5VZKky94GmUdlynDxqh2mJ
m9OI9qza+fSYYou1M+UfKqvekerTqesnXJaMQcvQd1fdqzslxhnsKnEEH1u+MdM1K6o0X4CoYrYj
mgHX3c1bnSABbN79ZD/s7ZRYXdBhKSSXSLcZ+rDeUC+QKqIrH2Njj7EZN/ozjfXjHQ1EDpFYtq+m
ccqu6kUAiYvPHgRoHNE6c8BIQTYPyGnpD7pNqRDvKQ0xphMDAGO2RMkh2EcSeo39daLDP7gNw6Rv
VBl3keBLA6jZkC9FNZE58ZZ/1IbTWubxLEvtS53J7DBQ8wIDAQABo4IB/DCCAfgwTAYIKwYBBQUH
AQEEQDA+MDwGCCsGAQUFBzABhjBodHRwOi8vb2NzcC5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9w
dWJsaWNvL29jc3AwHQYDVR0OBBYEFK8buyfUPto0BWSddgC28rqPDFiIMBIGA1UdEwEB/wQIMAYB
Af8CAQAwHwYDVR0jBBgwFoAU9suDso8DYFqMZFx9kdFOtTlm4SkwgeoGA1UdIASB4jCB3zBUBgpg
hGwBAQECBAAHMEYwRAYIKwYBBQUHAgEWOGh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1
YmxpY28vcG9saXRpY2FzL2Nwcy5odGJsMFQGC2CEbAEBAQIEAAECMEUwQwYIKwYBBQUHAgEWN2h0
dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NwLmh0bWwwMQYE
VR0gADApMCcGCCsGAQUFBwIBFhtodHRwczovL3d3dy5zY2VlLmdvdi5wdC9yZXAwVwYDVR0fBFAw
TjBMoEqgSIZGaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9scmMvY2NfZWNf
Y2lkYWRhb19jcmwwMDVPY3JsLmNvbDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIB
AHUfnXEV2Yj0mZdH4G3q8T2WTy9+uR3hxif7B4DQvmqo3hS8T1c+AtrnAQj3fbZKzip3TbTLTM1x
Jr0Wobq2OpgmzPd92xIig0htLz+hUNmqB9EyjCymSVkD2pBFxUi2ANWSSBfIkKGv1QeUQSvYNaQ4
1ymr6lptnZ79fE9BuhyeeRHNGPdTdI/2RRDY1P7cXVlNe3X5OdL7+f/c++wQONtT/i7OZWQy07o
P240+7cO7mzOHYpjAGhCGakIpDlcQNFnhpw7HHnNUgkY93WXC7UbVK7szaaErnzK6Cp6Xcueve5EE
+ovhj0gH2lzHFFQwqPZefKl2DlKfGnTrBadRBP0ty5B6TaWaXqo298rTUuDQS4VQn6lxlgLNhCH0
0w6DmxLdyLQ+/4Il6IraRaKzlSDGiz/SYrlzxHkMbbogNvA/m9tDgPw28ZaODc0eOom84wqsgEox
A2esukoRmsdtxoG0LqR83MTsWYSvujNoLI3UO7DphQNwgu0b0o6/KefrjrV4FCV0XxP665+gNV3t
8NNgEQWMH+j/GDL/mbjXBA4zSA5kobrlAmPOQWp72htZ9iLn0X/sLtIljaxgYQj/4UDR4StMaGut
NHhgJ3DkAJ3tlR7Ujwv4ujr//iLRzfBc4HqfiSFPeR8CpyyrE41g5WolbqK0FqDyMqTqMWVINcYR

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 005*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0016*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C:	*PT*
Valid from:	*Tue May 14 15:19:26 CEST 2019*
Valid to:	*Wed May 14 15:19:26 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:AF:B9:72:F7:55:81:F2:79:61:F0:FD:48:49:65:70:BD:54:40:28:A0:37:2B:40:06:62:9F:3E:21:78:45:16:63:42:A5:2F:B0:34:B2:3D:FF:58:80:CA:51:50:1C:04:AC:D3:CA:A8:83:C0:F2:24:C8:BE:20:D3:89:A2:2D:96:FF:CC:11:ED:25:F8:90:F8:1B:0D:29:03:D7:E0:A3:C5:D7:47:90:92:DF:16:DD:A9:5A:CC:36:76:15:D0:B7:42:A4:F4:4C:0A:C4:6C:B5:66:4F:96:BF:C0:9A:C4:2A:D3:8E:5E:0D:00:14:C4:28:93:D1:A2:37:5A:C4:21:00:67:E5:B4:28:51:FA:49:0E:43:12:EF:65:CC:C3:3A:2F:4F:3D:7F:3E:A8:09:F5:20:D0:45:63:9D:80:87:1E:0E:BE:28:13:CF:CB:3D:C7:29:07:48:5B:B4:D9:20:C2:DC:2A:9E:57:07:ED:C7:15:4C:32:B8:ED:E3:54:A4:F7:9D:51:2F:E5:AA:38:E4:E9:03:0D:0A:2E:50:F7:62:59:BE:95:CF:3D:79:66:65:A2:8F:30:F5:4C:F8:2A:C6:6D:14:85:5B:03:56:AA:93:B3:1C:D8:DE:EB:44:4F:B5:BF:2A:71:70:BA:14:30:65:A2:6E:E8:D2:44:EA:AB:8A:E9:04:6D:6F:9A:5C:5D:4C:7F:53:5A:F8:CD:55:A9:E9:62:D7:AF:68:D9:64:84:AB:AD:22:94:E3:5A:9D:2A:C4:3C:A1:56:B5:A6:4A:8E:55:64:A9:32:F7:81:A6:51:D9:72:9C:3C:6A:87:69:89:9B:D3:A2:F6:0C:DA:F9:F4:98:62:8B:B5:33:E5:1F:2A:AB:DE:91:EA:D3:A9:EB:27:5C:96:8C:41:CB:D0:77:57:DD:AB:3B:25:C6:19:EC:2A:71:04:1F:5B:BE:31:D3:35:2B:AA:34:5F:80:A8:62:B6:23:9A:01:D7:DD:CD:5B:9D:20:01:6C:DE:FD:64:3F:EC:ED:94:58:5D:D0:67:29:24:97:48:B7:19:FA:B0:DE:50:2F:90:2A:A2:2B:1F:63:49:8F:B1:19:37:FA:33:8D:F5:C9:1D:0D:44:0E:91:58:B6:AF:A6:71:CA:AE:EA:45:00:89:BB:CF:1E:04:68:1C:D1:3A:73:C0:65:41:36:0F:C8:69:E9:0F:BA:4D:A9:1D:EF:29:0D:31:A6:13:03:00:63:B6:44:C9:21:D8:47:12:7A:8D:FD:75:A2:C3:3F:B8:0D:C3:A4:6F:54:19:77:91:E0:4B:03:A2:59:90:2F:45:35:91:39:F1:96:7F:D4:86:D3:5A:E6:F1:2C:4B:ED:4B:9D:C9:EC:30:50:F3:02:03:01:00:01*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Subject Key Identifier	*AF:1B:BB:27:D4:3E:DA:34:05:64:9D:76:00:B6:F2:BA:8F:0C:58:A5*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*F6:CB:83:B2:8F:03:60:5A:8C:64:5C:7D:91:D1:4E:B5:39:66:E1:29*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl005_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0C:B2:DF:D0:EF:42:43:D9:A7:DB:E3:27:35:F5:53:38:33:0C:6E:06:61:AD:CF:70:49:DD:3E:0C:12:49:81:73*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0016*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*

X509SKI

X509 SK I	*rxu7J9Q+2jQFZJ12ALbyuo8MWKU=*

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

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

Status Starting Time *2019-08-05T23:00:00Z*

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

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

2.17.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.18 - Service (withdrawn): Serviço de Validação Cronológica do Cartão de Cidadão 000004

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000004*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3831263620395555372*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIl5TCCBs2gAwIBAgIIN5th9r6N2iwwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dGBpZGFlZ2lzdG9zIGUgZG8gTm9QYjpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE2MB4XDTE5MDUyOTE0MTA1NloXDTI1MTEyODE0MTA1NlowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0dW8NvlGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUsw5QYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDQwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDV8ivcgsolqvNsFgW2
ajFrbIskM21Jhv0qD2BIfO0CrKnP35RL2IQzfbx1vr2Sw4g8Jl611byFAEOdI94knWgXmE1YS7+k
j33HasdvQ69McmqgAQlchew64+I2WG5KljztDRMu7YgMfIHCmzDcnamuUlCpe3yXZe8n8bFKsTX
EOeUyg7MIX/VC7eb0lnfROXEijmwdIDIS4E71z1/YFQm9zbX4L0kYfm7Bk7IVSz2Lqxbu+NUrxje
OF+Tq084tsgU/vcxADFoieLNe0yiGthcR+Ig9bPdTsGE2o5d1xTj0ognxEzcSzv7ODuHC2kcUt7a
s0KHCDPuNcjZxgsUqgAaiQqnoHxf18MCDvfufp5ZXuE5Xcy7DTyNfgjxfhMha3d6xY+4JfZH6JMJ
Yo59seK56b43tjMe8gruPiXj3L nnnsd7yMtce7BSVeSYozix4UVG3c9G1jsnXc9U7UXUV+LIJq
h7+TlehelI4WHg25gaN57OeRhwxV+p2vozNfBUcMCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUrxu7J9Q+2jQFZJ12ALbyuo8MWKUwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2Mu Y2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY2Bvb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTZfZGVsdGFfcDAwMDEuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdgYL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZaaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Y1I1Y19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DlGnQnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZS8pc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1lLXN0YWtlwIHRva2VuIGlfGlzc3VlZCBhcyBhIHF1YWxpZmlfZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHR0ZSBSRUdVTEFUSU9OIChfVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWoZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9fYXNzaW5hdHVyYV9jcmwwMDE2X3AwMDAxLmNybDAdBgNVHQ4E
FgOUQeYWhrQe30D2MxraYkNy3gG+IA8wDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQAWpUh1UTre/s1DvNMYpG4xaeNXN1LzTz7EKHIDN8fYSdt3u5UFYlRubwhfknw3QEQ8SeFxxuLE
ejBi5U0PIDmMYjFAK3M2+R7iMeOuC7oPKLgI+HuOFNjH2FXClxdOqeHg9JML8vhmrQsgxiC8CMW0
e4zmlh2wSw+vjXPgAMal2umzeXfP60L2oeoOXP6QXiF5mzlCLgkwjU6Cw+t0xAxC8e/MRZ5fNjvG
AwT6D5mzERKiirfq3sCTbOSntE4Fd+rfjMs+TBjpPuoHcxHyasUE+QGKBLxfnURJc+hgwHAz7qzp
69NUVrUB0VUcLh21/3qUoRKZkaG5nLRMWDnz4Ch5W7LB47qUH3E1JLccbb3AoRhKlOGcIHkwrBr
qb0BdX48/eX9W/FqezKdpzeQ4NkgvdUS/VxP1CVwlXmlrw74p4bWsq2VN1SWiXCWcBlQQBdEh8xn
5ehx5hdwCKbfxYMeR+71/j2El7jhXooTIWyF2pCd8pfh4mkBZP6E6j5/cwWPNEm2MvzDSqi7P3vl
ep8Dg+e56oo/qU9CpveVXOj7X5gSU9wLj+NP/ODOzcKt1JEinxzrEM2tsR0WxMhrDdXeKKv5RwU7
uJNu8hoT9OzKwt9nWMDfJAoFY4Dt6vy4U6qm3UDdqCDVTnPq65MHjjH4OoA0j8XHPCrOyQt1FX5
4Q==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0016*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000004*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Wed May 29 16:10:56 CEST 2019*

Valid to: *Fri Nov 28 15:10:56 CET 2025*

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:D5:F2:2B:DC:82:CA:25:AA:F3:6C:16:05:B6:6A:31:6B:6E:5B:24:33:6D:49:86
:FD:2A:0F:60:48:7C:ED:02:AC:A9:CF:DD:24:4B:D8:84:33:7D:BC:75:8E:BD:92:C3:88:3C:24:8E:B5:D5:BC:85:00:4D:1D:BB:DE:24:9D:68:17:98:4D:58:4B:BF:A4:8F:7D:C7:6A:C7:6F:43:A
F:4C:72:6A:A0:01:09:5C:85:EC:3A:E3:E2:36:FD:61:B9:28:88:F3:B4:34:4C:BB:B6:20:31:F8:87:0A:6C:C3:72:76:A6:B9:42:42:A5:ED:F2:5D:97:BC:9F:C6:C5:2A:C4:D7:10:E7:94:CA:0E:CC:
95:7F:D5:0B:B7:9B:D2:59:DF:44:E5:C4:8A:39:B0:74:80:C8:4B:81:3B:D7:3D:7F:60:54:26:F7:36:D7:E0:BD:24:61:F9:BB:06:4E:C8:55:2C:F6:2E:AC:5B:BB:E3:54:AF:18:DE:38:5F:93:AB:4
F:38:B6:C8:14:FE:F7:31:00:31:68:89:E2:CD:7B:4C:A2:1A:D8:5C:47:E2:20:F5:B3:DD:4E:C1:84:DA:8E:5D:D7:14:E3:D2:88:27:C4:4C:DC:4B:3B:FB:3B:3B:87:0B:69:1C:52:DE:DA:B3:42:8
7:0B:33:EE:35:C8:D9:C6:0B:14:AA:00:1A:89:0A:A7:A0:7C:5F:D7:C3:02:0E:F7:EE:7E:9E:59:5E:E1:39:5D:CC:B8:0D:3C:8D:7E:08:F1:7E:13:21:6B:77:7A:C5:8F:B8:25:F6:47:E8:93:09:62:
8E:7D:B1:E2:92:E9:BE:37:B6:33:1E:F2:0A:EE:3E:25:E3:DC:B9:E7:9E:C7:7B:C8:CB:5C:7B:B0:52:55:E4:98:A3:38:B1:E1:45:46:DD:CF:46:D6:3B:27:5D:CF:54:ED:45:D4:57:FF:8B:94:82:6
8:87:BF:93:21:E8:5E:23:85:87:83:6E:60:68:D4:BB:D1:E4:61:C3:15:7E:A7:6B:E8:CC:D7:C1:51:C3:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *AF:1B:BB:27:D4:3E:DA:34:05:64:9D:76:00:B6:F2:BA:8F:0C:58:A5*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0016_p0001.crl*
Subject Key Identifier	*41:E6:16:86:B4:1E:DF:40:F6:33:1A:DA:62:43:72:DE:A1:BE:94:0F*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*8E:5C:1A:20:79:EA:F7:86:38:6D:87:5D:F8:E6:0A:7E:CD:6E:93:D2:A5:C4:C8:C7:54:F0:98:CB:D4:F5:C7:69*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000004*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*QeYWhrQe30D2MxraYkNy3qG+lA8=*

Service Status

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

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

Status Starting Time

2026-01-27T12:00:00Z

2.18.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000004*

Service digital identities

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000004*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*QeYWhrQe30D2MxraYkNy3qG+lA8=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2019-08-05T23:00:00Z*

2.19 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*2479456644485653305*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHxzCCBa+gAwIBAgIIImjMrnKMozkwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gQUZzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjIyBFbGVjdHLDs25pY2EgZG8g
RXNOYWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDYwHhcNMjAwMjA2MTYxNjE1WhcNMzIwMjA2MTYxNjE1WjCBwTELMAkGA1UEBhMCUFQxMzAxBgNV
BAoMKkluc3RpdHV0byBkb3MgUmVnaXN0b3MgZSBkbyBOb3Rhcmlhn ZG8gSS5QLjEcMBoGA1UECwwT
Q2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViUlNFc3RhZGBXSTBHBgNVBAMMQEVDIGRl
IEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENpZGFkw6NvIDAw
MTcwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNmZDbqDacIW/vG2aC7UCcuLZl4lcJ
RVggiwjIiiipjSOIZZ8eVpd60gBQkMwHeOLDP/iHF1XJxS07wPh0qGedusSewDVBGlaSYKYJKTne
y3qeKivZcmYB03lHqVnk25z+Bhb80i5cb1TXbUTMcyynfX3VjOomUYmUdlLX/JyO3XQHcASoejrz
nq+tY87xO3jwKcyn6rofwTOfAcBsLfsy2vnQbNJkhsU+DNXsKZAuGpFRqJ8/nbLaQxovPl6fX979
FcRdo8Bfmq3fmdsaShQv6yW75y/teKOQls3EQdWlVOrVu03STvzZhIHw3Rg+KfqhpkgSTyG7nxFX
eKnkInuf/jx9BlGRzTMFvPcxaXfxOqer1E76ufPV+NSQNZmvOtUik/2Z2KNRpSeFH1iRd5cZVsx
CsGWaNT5ilfm3Uuu9IeAj8ZtLwJtKKc77HVObAdRUb+OpYK7Dq/zpSHGmQiUGA19RIEPidB3LMP
upvO1mtCPQHuiWez8KyW1pM48MhZCbX1DF2//9oO2ifZ5XS5dctb2uR8rMoSaMCpg3fjjRRaTJLO
dilDknsMaI0KxKVNjX+FfGgjCXsDt9u5gdo8uFi0O/UV1LUXWzM4xR58Z4piRdP9ZzKfRiCxyvpl
SevAnHKv1IbZe1zlj+pMGKySTrC6zJ70eyBmeqyq3k6Y7QIDAQABo4IB/DCCAfgwTAYIKwYBBQUH
AQEEQDA+MDwGCCsGAQUFB2ABhjBodHRwOi8vb2Nzc5yb290LmNhcnRhb2RlY2lkYWRhby5wdC9w
dWJsaWNuL29jc3AwHQYDVR0OBBYEFNMDskPSj9V98K5oWecjwdHbWtOMBIGA1UdEwEB/wQIMAYB
Af8CAQAwHwYDVR0jBBgwFoAUNltjEKmUu52gay1z5LNLe3MhsDwwgeoGA1UdIASB4jCB3zBUBgpg
hGwBAQECBAAHMEYwRAYIKwYBBQUHAgEWOGh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1
YmxpY28vcG9saXRpY2FzL2Nwcy5odG1sMFQGC2CEbAEBAQIEAAECMEUwQwYIKwYBBQUHAgEWN2h0
dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NwLmh0bWwwMQYE
VR0gADApMCcGCCsGAQUFBwIBFhtodHRwczovL3d3dy5zY2VlLmdvdi5wdC9yZXAwVwYDVR0fBFAw
TjBMoEggSIZGaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9scmMvY2NfZWNf
Y2lkYWRhb19jcmwwMDZfY3JsLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIB
ADw8YixSniepS85dODmgz7lIOBHk7eb0MkfZ5B1AACL7CSBwyvRvLQ6psfKXyPpJDZh2EOxcLp5
vO9vY5ZsbB4U5PRyF10apSoUM8WFiWeo37IKCY7m8s4Oppk0ynfsTdF+sN4ZjfGZAr7N66uWelJ
c5FBx6yagTyHJKg2NKzFEHYaEymDQUuNLHrH2jjx9UzMLcu/C88SNxpjVTk3bqPhRusIApA6Ng6T
UjaWF2/EOm9BvOor3k2M+0tzb5n07NXXhwYpcdSw10EJGEi5XfP+uITdoRK2FOMRK4ZbN5WsZeu8
dIpOTj6u3jN9UXZwUBajnzKZv/kF5B3fuf1QPSwBOwNlC6LzrRHKwcnC+C+FLFW/pr3tLhwrvef3
FoYUx26tnfowp8DW59kcSZ5EtSEfZEJmIE7S7wXcPQ1mCnnFnV2vk/8+OIxBp1KWU1Bd7BX8SCkW
1U0ysTa3KgQl8kbD36x56jxlFcTNksSyMU9XWwMSH+mPNFYJW35o+BPxg52PndP10ex8udy0lDDl
wHKHb/bXlOFj7+uAAoKrmQCtYPBH+xr1bRzf65VbJm0S+Pz8mBC3NQ8l5vUG2c3DdkTRpPfzvdFr
U+V0n5geKbLZfUkSMkAuF2Vn9rTNpmMh6G4TfpOhhj/ujcEKjLYOWzJoH+B+7so0yoCVJ4O50/mx

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 006*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

Valid from: *Thu Feb 06 17:16:15 CET 2020*

Valid to: *Fri Feb 06 17:16:15 CET 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:CD:99:90:DB:A8:36:9C:21:6F:EF:1B:66:82:ED:40:9C:B8:B6:65:E2:57:09:45:
58:20:8B:08:C8:8A:28:A9:8D:23:88:65:9F:1E:56:97:7A:D2:A0:50:90:CC:07:78:E2:C3:3F:F8:87:17:55:C9:C5:2D:3B:C0:F8:74:A8:67:9D:BA:C4:9E:C0:35:41:1A:56:92:60:A6:09:29:39:D
E:CB:7A:9E:2A:2B:D9:72:66:01:D3:72:07:A9:59:E4:DB:9C:FE:06:16:FC:D2:2E:5C:6F:54:D7:6D:44:CC:73:2C:A7:7D:7D:D5:24:EA:26:51:89:94:74:82:D7:FC:9C:8E:DD:74:07:70:04:A8:7
A:3A:F3:9E:AF:AD:63:CE:F1:43:78:F0:29:CC:A7:EA:BA:1F:C1:34:1F:01:C0:6C:2D:FB:32:DA:F9:D0:6C:D2:64:86:C5:3E:0C:D5:EC:29:90:2E:1A:91:51:80:9F:3F:9D:B2:DA:43:1A:2F:3E:5E:
9F:5F:DE:FD:15:C4:5D:A3:C0:5F:9E:AD:DF:99:DB:1A:4A:14:2F:EB:25:BB:E7:2F:ED:78:A3:90:96:CD:C4:41:D5:A5:54:EA:D5:BB:4D:D2:4E:FC:D9:84:81:F0:E5:18:3E:29:FA:A1:A6:48:12:
4F:21:BB:9F:11:57:78:A9:E4:22:78:9F:FE:3C:7D:06:51:91:AF:34:CC:16:F3:DC:C5:A5:DF:C4:EA:9E:AF:51:3B:EA:E7:CF:57:E3:52:40:D6:66:54:EB:54:8A:4F:F6:67:62:8D:46:94:9E:14:7D
:62:45:DE:5C:65:5B:31:0A:C1:96:68:D4:F9:8A:57:E6:DD:4B:AE:F6:27:80:27:C6:6D:2F:02:6D:28:A7:3B:EC:75:4E:6C:07:51:51:BF:B4:3A:96:0A:EC:3A:BF:CE:94:87:1A:64:22:50:60:35:F
5:19:44:3E:27:41:DC:B3:0F:BA:9B:CE:D6:6B:42:3D:01:EE:89:67:B3:F0:AC:96:D6:93:38:F0:C8:59:09:B5:F5:D0:5D:BF:FF:DA:0E:DA:27:F6:E5:7E:79:75:CB:5B:DA:E4:7C:AC:CA:12:68:C0
:A9:83:77:E3:8D:14:5A:4E:32:CE:76:29:43:92:7B:0C:68:8D:DA:C4:A5:4D:8D:7F:85:7C:68:09:09:7B:03:B7:DB:92:81:DA:3C:B8:58:B4:3B:F5:15:D4:85:17:5B:33:38:C5:1E:7C:67:8A:62:
45:D3:FD:67:32:9F:46:20:B1:CA:FA:65:49:EB:C0:9C:72:AF:D4:86:D9:7B:5C:E5:27:EA:4C:18:AC:92:4E:B0:BA:CC:9E:F4:7B:20:66:7A:AC:AA:DE:4E:98:ED:02:03:01:00:01
```


Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*

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

Authority Key Identifier *36:5B:49:10:A9:94:B9:2D:A0:6B:2D:73:E4:B3:4B:7B:73:21:B0:3C*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl006_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*80:A0:D9:B3:05:17:6C:42:92:B5:84:2D:43:9B:B5:D5:F8:7C:B6:97:0B:48:B0:98:F2:F4:95:46:F8:97:F7:B7*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*

X509SKI

X509 SK I	*0wOyQ99KP1X3wrmhZ5yPB0dta04=*

Service Status

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

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

Status Starting Time

2020-03-19T00:00:00Z

2.19.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

2.20 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000006

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000006*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6738902634389219097*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJ5TCCBs2gAwIBAgIIXYVkPeK2pxkwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCplbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE3MB4XDTIwMDQwMzE1MzkzMloXDTI2MTAwNDE1MzkzMlowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDYwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC6VJzJVQper+Juk9AP
YQEMdvpT40bnFU+Bqpk2X9Me/M5aEjRc/GRaQ1VrPNKc30V4g23FK9P58pH8xwGbNLGhxmVXO4yn
MeZKh1A0TeRynNE1LoudYYB2pvKOnt83iG66srcK8BqTZAbBwYIT2HlFOqrp9TcFYpL1QF4MVnMy
NR/NbCb1W7HcrlkruENoMRZQQlcqDOfQGrUQG7jt7FNYR0j7Tk8eNVlquRxccxO7caBAlqcX3xox
ZGE4jUWtbdXOWlmDfKndVR8KhgYnaGj+s8GC+hJUg1FiVHhhEm+TpAIrjjmrhWP8AhF+NcxOht5s
I/Ct0pHP/+W5LDgMVPOetRMto2nMZsULc9RZB6LE7xP5+VCQJH7vo8yJ594gtnZwFKANsveiXAr7
VPlyx/Q40Jq4bXbXpy06leR8idK2q9S1eo5Gx/00mLyHMwP5mua8jmJCYh/Co2BreYTQtxk+WIll
/MO8elTINDyJtgMBLrGdFP4Jajru/G2M5FVQH10CAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU0wOyO99KP1X3wrmhZ5yPB0dta04wSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhjodHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMCSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTdfZGVsdGFfcDAwMDEuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAOcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdgYL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Yi1lY19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIG2BgcEAIGXXgEB
DIGnQnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1lLXN0YW1wIHRva2VuIGlzIGlzc3VlZCBhcyBhIHF1YW xpZmllZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWoZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2Np2GFkYW9fYXNzaW5hdHVyYV9jcmwwMDE3X3AwMDAxLmNybDAdBgNVHQ4E
FgQUipUp0o43tAZfDc18lvreNKdqMtQwDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQC76UE1wlqZRlNPD1aZ7oUjcl6cGWN3mxQ/dlG1n4kHI7YhODAv3zkpfF21fsBjwYh9e4Bj91mA
mMAr8HbQNstwsB5HmVlhvDVjRRlXolqS3buaMStCJSTVXWMdgzkK4BfTwI1cc6mv1s6fZOBSDQ/X
6WF3CZCCGej3ufsZLnj9Dy2q+U7vTsdJTbQ5ixS2LD8Qa2Jz1DKqsMa3YPtheimTGN6YHILyWta
XjLfKYMqP5rs+hGSN7CJnhMM3I4oU5VV4tdU/roTlsyYQiU6zBb57k6fDp95sMt857Uvps8oue
rFi+yypWJArL16pWcz93THzN+ZlZqbdvw+LrdlnBd5wk/hv2ca7HCym9a+VWOpVQWnk6pQlTxkla
XOaMfTkhDEvkix1nU+N3ANjcj82kdzLbsFtaCUo8qT6qXP2zzd1JjtpqdDEv/R1HzfWyhDUyp6nL
AMgbV8R35IMwZ+1UrKjikRm4zilXP8bifk8CEELNW1QDLbyH5GvzgcQ6bt/k8EC0TRd5HYxdxq5z
WGnoq1cHD2RmVo2BKAtzk1DbA5kGH/ZNkQvPbL2xVYtrArcfZa452ve41A+zq7CKKfKfH96MtNw
wyqsif7ohc02A2XHUzP1ij46To6zU5upR90W+Hx5EgM+kZJOQXjOPpE0HBeKrd4z0xcRAZ0EOWzy
Hg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*
Issuer OU:	*subECEstado*
Issuer OU:	*Cartão de Cidadão*
Issuer O:	*Instituto dos Registos e do Notariado I.P.*
Issuer C:	*PT*
Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000006*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*
Valid from:	*Fri Apr 03 17:39:32 CEST 2020*
Valid to:	*Sun Oct 04 17:39:32 CEST 2026*
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:BA:54:9C:C9:55:0A:5E:AF:E2:6E:93:D0:0F:61:01:0C:76:FA:53:E3:46:E7:15:4F:81:A2:99:36:5F:D3:1E:FC:D4:9A:12:34:5C:FC:64:5A:3B:55:6B:3C:D2:9C:DF:45:78:83:6D:C5:2B:D3:D2:F2:91:FC:C7:01:9B:34:B1:A1:C6:65:57:3B:8C:A7:31:E6:4A:87:50:34:4D:E4:72:9C:D1:35:2E:BB:9D:61:80:76:A6:F2:8E:9E:DF:37:88:6E:BA:B2:B7:0A:F0:1A:93:64:06:C1:C1:82:13:D8:79:45:3A:AA:E9:F5:37:05:62:92:F5:40:5E:0C:56:73:32:35:1F:CD:6C:26:F5:5B:B1:DC:AC:89:2B:B8:43:68:31:16:50:40:87:2A:0C:E7:D0:1A:B5:10:1B:B8:ED:EC:53:58:47:48:FB:4E:4F:1E:35:59:6A:B9:1C:5C:73:13:BB:71:A0:40:22:A7:17:DF:1A:31:64:61:38:8D:45:AD:6D:D5:CE:5A:59:83:7C:A9:DD:55:1F:0A:86:06:27:68:62:7E:B3:C1:82:FA:18:D4:AB:51:62:54:7B:61:12:6F:93:A4:02:2B:8A:39:AB:85:63:FC:02:11:7E:35:CC:4E:86:DE:6C:23:F0:AD:D2:91:CF:FF:E5:B9:2C:3A:8C:54:F3:9E:B5:13:2D:A3:69:8C:66:C5:0B:73:D4:59:F3:A2:C4:EF:13:F9:F9:50:90:24:7E:EF:A3:CC:A3:E7:DE:20:B6:76:70:14:A0:0D:B2:F7:A2:5C:0A:FB:54:F9:72:C7:F4:38:D0:9A:B8:6D:76:D7:A7:2D:3A:95:E4:7C:89:D2:B6:AB:D4:B5:7A:8E:46:C7:FD:34:98:BC:B7:33:03:F9:9A:E6:BC:8E:62:42:62:1F:C2:A3:60:6B:79:84:D0:B7:19:3E:5A:59:65:FC:C3:BC:78:84:E5:34:3C:89:B6:03:01:2E:B1:9D:14:FE:09:6A:3A:EE:FC:6D:8C:E4:55:50:1F:5D:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*
Authority Info Access	*http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0017_p0001.crl*
Subject Key Identifier	*8A:95:29:D2:8E:37:B4:06:5F:0D:CD:7C:96:FA:DE:34:A7:6A:32:D4*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *FD:3E:3D:9B:8E:5F:3A:46:20:3B:91:EB:AA:29:49:AF:2F:9E:01:32:63:3E:04:28:78:4E:E8:04:E5:D1:D3:08*

X509SubjectName

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000006*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *ipUp0o43tAZfDc18lvreNKdqMtQ=*

Service Status

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

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

Status Starting Time

2020-05-19T23:00:00Z

2.21 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000007

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000007*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6566819489833138301*

X509 Certificate

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

MIIl5TCCBs2gAwIBAgIIWyIHijOduH0wDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dGBpZG9zIFIlZ2lzdG9zICUgZG8gTm9OYXjpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE3MB4XDTIwMDQwMzE1NDAxM1oxDTI2MTAwNDE1NDAxM1owgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0W6NvIGRlIEApZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUsw5QYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDcwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC7+MRyNSLL8YEChsgP
DYtA4cYPvPMJGHdLONcKSiLe4oNMj0sACa25Bltxu1NvK81iCYzmu9b5df7UYu+hPX5qZEe1F2Az
4JZkWU8plGMt/4IAICsaDRrxBjBchKAE/4aKb00xwPmleK2Y1zEgJgwxHb/l6PlQvX9ZrGsE9uIC
GZaeB033cwn7Ow/9TFBWPXG8HuYzRGKy3bdxjL3Ec57XM7nqmVLV50pNJGvcz2F83S5tZS6Tx9QY
LqZG/bVLgWQxq2ZSduXBa/KpeiFYvzA300Sc7JUupwOeOewAEH89USHXtUAWafzwYamEBgpn5n+q
TFz3KhEL7x7IBQNOjlsWI6Nd0hwkLP1gw5SbRaeKJSsgU3uqQVrfRziGm36vww3otMpfarkspeyn
9sIR4bb66tpnUEly6CZVe53JI/c8HXNKWJlU0TaMB53BBIowMbzFRmsmU2P/uKiChfFnAYDSUXXqG8
BjXXUMI9TCxIPqwWA4hLofwj9LdTvhJAWJQeSpMCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU0wOyQ99KP1X3wrmhZ5yPB0dta04wSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2Nzc5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTdFZGVsdGFfcDAwMDEuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdgYL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Y1i1Y19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DlGnQnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZS8pc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1lLXN0YW1wIHVsZVUlGlzIGlzc3VlZCBhcyBhIHF1YWxpZmlfZCBlbGlvjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHR0ZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWoZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9YXNzaW5hdHVyYV9jcmwwMDE3X3AwMDAxLmNybDAdBgNVHQ4E
FgOUFUgYd4FhI53OnyUkiHOP5fj6Il9swDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQCNneVpk4b3hEMzTtsGRwkdyFJFBumOxBsvl2yEWMWApBmpOtvH7ZYtjrBJquehfFwfBiuPfgj
TAC/bBryAj+m3lzJPUMGZ/DNl+LXore/FfulAlzvzAfFYYRSt060uffRWeHLqj0A8sKyZ/eAgd7O
B1JNoabwU1PK+ZGp/j0EL8TnN7ViKEo+/6QAQPmVcll1UXzuVjwttNA+X/DY5I0KUCukaYKxx97u
6pDikZCV1wAMU3i6X7bMQ1rM6gF18p0t4UU6V2Fbnnj/YjikNiaJ6AaPbjxlZFdPbt0A9J8BePR3
89Lqkku6ahfOtG3alBe0lkaK8O2j+a1k0/V4kVFiUPbM/moK4d5KZfAm554WacomTlvw5Bxpwv8V
uZpm72xzo7E9rnNSHmAqXSB0wE14Oo37k6XqYlk/vr8HSLq7/4xIYyDz/AZ3SQM4t5V2vkX8A+Q8
uc14iA7OvxVzBtwN+CuoTcBtLf45Jv22K8Jc+ChwNLf7OCJWTzg41FP8ZC2A1yCClsTrYnCAkHEn
RtOLUEBOhJt6LJY2qTlXpExitflmO5fOfIQi9TPcWg1+1IO8pP98HVomzOCtB+hSi6VOwLt+hZxm
wY3SdC6vpAfM9K06T2ieHtV4ZjVqQHUhRWGqkz1LzLRUFFdufRLa11mhWbLz68s4HkiGu3XmsK+9
cg==

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

Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000007*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Fri Apr 03 17:40:13 CEST 2020*

Valid to: *Sun Oct 04 17:40:13 CEST 2026*

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:BB:F8:C4:72:35:22:CB:F1:81:02:86:C8:0F:0D:8B:40:E1:C6:0F:BC:F3:09:18:77:4B:3B:D7:0A:E6:22:DE:E2:83:4C:8F:4B:00:09:AD:B9:06:5B:71:BB:53:6F:2B:CD:62:09:8C:E6:BB:D6:F9:74:5E:D4:62:EF:A1:3D:7E:6A:64:47:B5:17:60:33:E3:F6:64:59:4F:29:94:63:2D:FF:89:40:94:2B:1A:0D:1A:F1:B6:30:5C:84:A0:04:27:86:8A:6F:4D:31:C0:F9:A5:78:AD:98:D7:31:20:26:0C:31:1D:BF:FF:E8:F2:10:BD:7F:59:AC:6B:04:F6:E9:42:19:96:9E:07:4D:F7:73:09:FB:3B:0F:FD:4C:50:56:3D:71:BC:1E:E6:33:44:62:B2:DD:B7:71:8C:BD:C4:73:9E:D7:33:B9:EA:99:52:D5:E7:4A:4D:24:6B:DC:CF:61:7C:DD:24:AD:65:2E:93:C7:D4:18:2E:A6:46:FD:B5:4B:81:64:31:AB:66:52:76:E5:C1:6B:F2:A9:7A:21:58:BF:30:37:D3:44:9C:EC:95:2E:A7:03:9E:39:EC:00:10:7F:3D:51:21:D7:B5:40:16:69:FC:F0:61:A9:84:06:0A:67:E6:7F:AA:4C:5C:F7:2A:11:08:EF:1E:C8:05:03:50:8C:8B:16:23:A3:5D:D2:1C:24:2C:FD:60:C3:94:9B:45:A7:BA:21:2B:20:53:7B:AA:41:5A:DF:47:38:86:9B:7E:AF:C3:0D:E8:B4:CA:5F:6A:B9:2C:A5:EC:A7:F6:C2:11:E1:BE:BA:B6:99:D4:12:5C:BA:09:95:5E:E7:72:48:FD:CF:07:5C:D2:96:25:4D:25:ED:A3:3C:4B:7F:01:A3:03:1B:CC:54:66:B2:65:36:3F:FB:8A:88:28:5F:16:7E:18:0D:25:17:5E:A1:BC:06:35:D7:50:C2:3D:4C:2C:65:3E:AC:16:03:88:4B:A1:FC:23:F4:B7:53:BE:12:40:58:94:1E:4A:93:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0017_p0001.crl*
Subject Key Identifier	*15:48:18:77:81:61:21:2D:D0:9F:25:24:88:73:8F:E5:F8:FA:23:DB*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F5:B9:F3:00:A0:72:6C:3E:CC:4E:64:13:72:B8:F7:66:D6:7C:18:FA:42:87:27:19:7D:DF:3D:F8:B5:C4:6E:69*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000007*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*FUgYd4FhIS3QnyUkiHOP5fj6I9s=*

Service Status

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

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

Status Starting Time

2020-05-19T23:00:00Z

2.22 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000008

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000008*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1392795787398220743*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIJ5TCCBs2gAwIBAgIIE1Q0Y6iIC8cwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJl2ZlzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE3MB4XDTIxMDIxMjE1MjYwOFoXDTI3MDgxNTE1MjYwOFowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0ws6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXj2acOnbyBkZSBWYWxpZGHDp8Ojby8Dcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDgwggGiMA0GCSqGSib3DQEBAQUAA4IBjwAwggGKAoIBgQCq2HOAnSCb4G79tg8i
IA6N1F7XZA1k9415B4+AoSbQ31+F+cX0NSjRoOfXwfW/8Xwg/SkVOgWmsK7s7mRqgdgu+8UKw0h/
mnlH55GDCO05z5WA0wvNYRvXXVpYmE0GhbwJne36Bj+jPhzxWEvNYAFlXrOGG0jBQ6YEAkO8g+E
V4NLiX7Ylm7xgkmp7HAjrC1MRp9wgNect7pe+5cu7E7DeC4+WgbTCSjPodUa0x3h/x04U/0Owtd
hdQ6xi7sFCg703Phms+WQxwNh+tlWPvVqkUldPU2vNIp091U/TMWRPsnAfoNpNRC4PNpfUSydUJS
Qtl/k2XyT6yBZR1FNaMy3TycKKnXkyMw3quJRPk9ZypPl0z7b3iXxuaF4CjEGIB/LIv/KEhH1wl
1v5YtfH5blqzOZbZFt30nGD6rbMr81wZwdyXG/QPY4rrwxZD8yb4OZfNyIozjIBJVanAazo/Z2Ku
BE7pr1Kn0AZfK4Rvs2rNaQoe9e67Ht/y3MQyi5UCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU0wOyO99KP1X3wrmhZ5yPB0dta04wSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2Nzc5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2Nzc0BvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTdfZGVsdGFfcDAwMDkuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAOcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdgYL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Yi1IY19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DIGnQnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyBQaW1ILXN0YW1wIHRva2VuIGlzIGlzc3VlZCBhcyBhIHF1YWxpZmlfZCBlbGVjdHJvbmij
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWGZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2Np2GFkYW9fYXNzaW5hdHVyYV9jcmwwMDE3X3AwMDA5LmNybDAdBgNVHQ4E
FgQUnwA5YCBe0UntjmfYYabG1rdEppEwDgYDVR0PAQH/BAQDAgbAMA0GCSqGSib3DQEBCwUAAA4IC
AQA/0EI4YXGezWtH7mc6wY07dt9U80yq0oO6QxdF9clu7n34BwDgMAanrln1UYYEVWM9R3UZr1mD
bA/SLbXwYhqO+3vml/OgCwImA0QiTk8cML2CgnjH4ANAAr/u/vga1V3234ajLrZtu9PYpXfmxT2L
TpQaRxdMHpY3Punpd623uQA9lvqs1VpHRYJr66DQ+96anL9ruCsp1dT7sM+pQPiDFY0goqtw4LIh
PFBFJlwIlW8v9sLOUjxDy5ODpwRNNLDcQmq1ply3cA+Gpo6GjJo5khYrx6XGo7lWwMbDDJbRuqP
jx5rexLTEajUwleWQAjI7AfQ0m47y5O7xz08LV0UGrrPyykPaf71592HD2V29WpdmGlJXqLGQ2yj
+nKnBIPd+GO9bRh15nl+Xqh+AgjYcLhGgBhJiqfjZnZBv5Fq3lHMm3uZRvR41tJcRz8S8gWT4Iaw
CFrauJnOiCKmoZujFFc52NaXaYmf0YC1t9V2BLzXCTpws+H07wIM8N0BPisb2QmfywB9OHv/1TTP
Kd5V5gx2mMwS83+t9d3/MqQ6MzVrVOU5u5Iq2Sf3nNOETu4e09ICWb1YwgoC6joix0DX8zX9G7GM
wxZTa4Tx8OMUf3rIy7I+ZFXIckrtLkXzn3xVTCJfJM3ijBZavAj7sIU4g6JvuFp1HMJQ1JTW6L+
Vw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000008*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Fri Feb 12 16:26:08 CET 2021*

Valid to: *Sun Aug 15 17:26:08 CEST 2027*

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:AA:D8:73:80:9D:20:9B:E0:6E:FD:B6:0F:22:20:0E:8D:D4:5E:D7:64:0D:64:F7:8D:79:07:8F:80:A1:26:D0:DF:5F:85:F9:C5:F4:35:28:D1:A0:E7:D7:C1:F5:A2:F1:7C:2A:FD:29:15:3A:05:A6:B0:AE:EC:EE:64:6A:81:D8:2E:FB:C5:0A:C3:48:7F:9A:79:47:E5:21:83:08:ED:39:CF:95:80:D3:0B:CD:61:1B:D7:5D:5A:58:98:4D:06:85:BC:09:9D:ED:FA:F2:3F:A3:3E:1C:F1:58:4B:CD:60:01:48:5E:B3:86:1B:42:41:43:A5:58:10:09:0E:F2:0F:84:57:83:4B:95:7E:D8:A6:59:B8:C6:09:26:A7:B1:C0:8E:B0:B5:31:1A:7D:C2:03:5E:72:DE:E9:7B:EE:5C:BB:B1:3B:0D:E0:B8:F9:68:1B:4C:24:A3:3E:87:54:6B:4C:77:87:FC:74:E1:4F:F4:3B:0B:5D:85:D4:3A:C6:2E:EC:14:28:3B:D3:73:E1:9A:CF:96:43:1C:0D:87:EB:48:58:FB:D5:AA:45:25:74:F5:36:BC:D2:29:D3:DD:54:FD:33:16:44:FB:27:01:FA:0D:A4:D4:42:E0:F3:69:7D:44:B2:75:42:52:42:D9:7F:93:65:E2:C9:3E:B2:05:94:75:14:D6:8C:CB:74:F2:70:A2:A7:5E:4C:8C:C3:78:2E:25:13:E4:F5:9C:A9:3E:5D:33:ED:BD:E2:5F:1B:9A:17:80:89:10:62:3C:FC:B9:6F:FC:A1:21:1F:5C:25:D6:FE:58:B5:F1:F9:6E:5A:B3:39:96:D9:16:DD:F4:9C:60:FA:AD:B3:2B:F3:5C:19:C1:DC:97:1B:F4:0F:63:8A:EB:C3:16:43:F3:26:F8:39:97:CD:C8:8A:33:8C:80:49:55:A9:C0:6B:3A:3F:67:62:AE:04:4E:E9:AF:52:A7:D0:06:5F:2B:84:6F:B3:6A:CD:69:0A:1E:F5:EE:BB:1E:DF:F2:DC:C4:32:8B:95:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.1.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html

Policy OID: 2.16.620.1.1.1.2.4.1.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0017_p0009.crl*

Subject Key Identifier *9F:00:12:60:20:5E:D1:49:ED:26:67:D8:55:A6:C6:D6:B7:44:A6:91*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A3:36:33:21:B9:38:30:1F:38:A2:5E:91:36:1D:DA:F4:E1:E6:C3:1F:B9:59:9F:96:76:25:7B:18:5C:61:B3:2F*

X509SubjectName

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000008*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *nwASYCBe0UntJmfYVabG1rdEppE=*

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

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

Status Starting Time *2021-02-24T00:00:00Z*

2.23 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000009

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *9147212756524563382*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIl5TCCBs2gAwIBAgIIfvFtib2Re7YwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE3MB4XDTIxMDIxMjE1MTAxNFoXDTI3MDgxNTE1MTAxNFowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMDkwggGiMA0GCSqGSib3DQEBAQUAA4Ii8jwAwggGKAoIBgQC+NEwhybkE7oXwy+rr
AzJeafiLluwI4ruWaT+NfBq70DqbZj5LdBEC2dAK6tZTwUE9Zzlyxh vXA4SgPvZDh90f2BF/Kf
CdzN0rDvS1PsV2FL9d5cx733UXF7NWcdBRi/YxtSdA01n6sFubEsCnOye+0gEsx4K67+JlaqZurN
ZlzD0JJk0mZedE8+HV99OehcrTL5gtgdJz6QrIFnJlxgVjTs/3LAeLoKsX2cg9ir/r56Nj P4npS/
y0g5MhfmpbT4LIQVV+62C9pERqWO2yTnU0IVvHWXEsGSG+UO8+I3goTtpPlV8O/opVdagt9LhTha
Bp0Lr5a7X++x5EciVJwn67+C8JfKJBV75/00n38k33K0GkWfb9Guq03/76E2PUkoPqQFZBZN/iY
6QPIECsufRpi1HjtAbPCjrqaa4wNk4ezt+pW6GRobN8ZhhbyIzcF4vzUYo5zdL5EIAIEMEqSF/Zw
9DMR7Vvv8CVW7GQAGumgWyJ8RsxEfZKx2hlZY2UCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU0wOyQ99KP1X3wrmhZ5yPB0dta04w5wYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTdfZGVsdGFfcDAwMDkuY3jsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdg YL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Yi1IY19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DIGnOnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1lLXN0YW1wIHRva2VuIGlzIGlzc3VlZCBhcyBhIHF1YWxpZmllZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygW6ZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9fYXNzaW5hdHVyYV9jcmwwMDE3X3AwMDA5LmNybDAdBgNVHQ4E
FgQURtLclWU/+k8x0tVAT4ZVtGqhxzmMwDqYDVR0PAQH/BAQDAgbAMA0GCSqGSib3DQEBCwUAA4IC
AQBVQhC7cEXaDYIuUUmNmNS+cfIKwVmRG9uvNYERhZnLIZCvyO1Cdt+W/SFwIMvWnqyn6td6W82C
pZ17e9eudn+BFmDLom1wF3bJyen8eH86JQiTbmkT0+pLj23gAuIlUpSLo5mOgX3mbXuUz1c78Qg6
tvjIHYKhM6Zh0mwx4bwmzZp4j96U8Ar+bGDuALELrK9fUiQov1h6tmGwLfmuzZgKzMlpXbYp65p
/C3N/AXEMmImdL5kctdTBHEwf+PMKkN/AZ3/nvnPgP6grpYQdtEVUkJ2Xz7WIN92jpuO+ely4c+
BUUOfOtxQkO5YYLgrn9H6TxFBN/IhYyxeYubEu4wANTtQHe7s39Xo0KB4FnvW34UevZr8y6icabj
IPT1WROI2oZ3drj+5f11aLI/DZMbJYxNx7AYc3DfWIMTAVjTRlpyovjRcnIlgyZLqUz4Pk350aR/
N9DqZ7b7j7BBddpmHm1WO7iSO0uHJmxmMUjLgW5yZjp8bwzIn2j8V+pz3RHTtLE4DIMWcjzsZvV7
HNm1e5UB67B527tA/yrnOy0Lx4c8/YbKLD9WgMhuIBLY+sp Yhvckdjuw/aNuEBXIDytG4SZI0o
xURjvuwcjyRsLfwjKx+dq0YBdTNj3MjfqvSPJHqdnSceK4CDiIWv0hD0+ii6FJyfAEqPXMS65IAU
Qg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000009*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C:	*PT*
Valid from:	*Fri Feb 12 16:10:14 CET 2021*
Valid to:	*Sun Aug 15 17:10:14 CEST 2027*
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:BE:34:4C:21:C8:19:04:EE:85:F0:CB:EA:EB:03:32:5E:69:F8:8B:22:EC:25:E2:BB:96:69:3F:8D:7C:1A:BB:D0:3A:9B:66:3E:4B:74:11:02:D9:D0:0A:EA:D6:53:C1:41:3D:67:32:32:5D:C8:6F:55:70:38:4A:03:EF:64:38:7D:D1:FD:81:17:F2:9F:09:DC:CD:D2:B0:EF:4B:53:EC:57:61:4B:F5:DE:5C:C7:BD:F7:51:71:7B:35:67:1D:05:18:BF:63:1B:52:74:0D:35:9F:AB:05:B9:B1:2C:0A:73:B2:7B:ED:20:12:CC:78:2B:AE:FE:24:86:AA:66:EA:CD:66:5C:C3:D0:92:64:D2:66:5E:74:4F:3E:1D:5F:7D:39:E8:5C:AD:32:F9:82:D8:1D:27:3E:90:AC:81:67:26:5C:60:56:34:EC:FF:72:C0:78:BA:0A:B1:7D:9C:83:D8:AB:FE:BE:7A:36:33:F8:9E:94:BF:CB:48:39:32:17:E6:A5:B4:F8:2C:84:15:57:EE:B6:08:DA:44:46:A5:8E:DB:24:E7:53:49:55:BC:75:97:12:C1:92:1B:E5:0E:F3:EB:77:82:84:ED:A4:F9:55:F0:EF:E8:A5:57:5A:82:DF:4B:85:38:5A:06:9D:0B:AD:26:BB:5F:EF:B1:E4:47:22:54:9C:27:EB:BF:82:FF:C2:5F:28:90:55:EF:9F:F4:A2:7D:FC:93:7D:CA:D0:69:16:7D:BF:46:BA:AD:37:FF:BE:84:CC:F5:24:A0:FA:8E:15:90:59:37:FF:D8:E9:03:E5:10:2B:2E:7D:1A:62:D4:78:ED:01:B3:C2:8E:BA:9A:6B:8C:0D:93:87:B3:B7:EA:56:E8:64:68:6C:DF:19:86:16:F2:23:37:05:E2:FC:D4:62:8E:73:74:BE:44:94:09:44:30:4A:92:17:F6:70:F4:33:11:ED:5B:EF:F0:25:56:EC:64:00:1A:E9:AA:5B:22:7C:46:CC:44:7D:92:B1:DA:19:59:61:95:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*
Authority Info Access	*http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0017_p0009.crl*
Subject Key Identifier	*46:D2:DC:21:65:3E:93:CC:74:B5:50:13:E1:95:6D:1A:A8:71:CE:63*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*FA:10:A6:24:EE:CF:43:C5:C9:8D:20:37:9D:D6:A2:81:ED:AE:3B:68:F4:93:0B:D6:C1:36:74:0A:7D:4E:04:42*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000009*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*RtLcIWU+k8x0tVAT4ZVtGqhxzmM=*

Service Status

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

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

Status Starting Time

2021-02-24T00:00:00Z

2.24 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000010

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000010*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7165217532999730742*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIl5TCCBs2gAwIBAgIIY2/3YiDZhjYwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVOQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsMEDNhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE3MB4XDTIxMDUyNzA5NDUxMloXDTI3MTEyNzA5NDUxMlowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhbw6fDo28gQ3Jvbm9sw7NnaWNhMUsw5QYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTAwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDFMpySfJnpHlwWVi4S
di30+5qtM0h7gCnTGD2u74iFC5f2Ms5AaoBEn7/nrDNBuGt1XRcmE+vDa2o4PIGI0QyDBswFaV27
RRKAR4PWZs/5z6KTmQx1QWER89a2kjh0KWyhLV30JR4pHR9WivrFASjAtEZ+L1x2eY33tHL8x8rn
otoGMtd6phb7sx7cBrdDO40OFARPsGsoIFwnaaqnHAELHag+kohC3go5anuGezEQ2MvGfSKTrlDM
Mx6kne325yafdybfTtJlyvWl3+T2D/thsAWUxwlgUZ5e5D8CwXYS68MWMGfPT5lITloXeIlmw7LoO
Tggei+crMDtedkWeYT6GE25HB8x9HfIXC0+SaQ1I1APtmqIeZszh9odXJ9LV8VrbufvPt4n4ER4E
rBaUoFAEGXWx1Hw66SMVqnZy3hsVsi7xD4uMgyoELzZU+tIj8KqIf3xffHQALDeCQpC5IAbH4TgMK
z5QIzaB49KMa+dIrvvFQMq/DNluFW/iDWPrdIc8CAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU0wOyQ99KP1X3wrmhZ5yPB0dta04wSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2Nzc5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMTdfZGVsdGFfcDAwMTMuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdgYL
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Y1I1Y19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DIGnQnkgaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyBDaW1ILXN0YW1wIHRva2VuIGlzIGlzc3VlZCBhcyBhIHF1YWxpZmllZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3lkaW5nIHRvIHRoZSB5RUdVTEFUSU9OIChfVSkgTm8gOTEwLzIwMTQw
aQYDVR0fBGIwYDBeoFygWoZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9fYXNzaW5hdHVyYV9jcmwwMDE3X3AwMDEzLmNybDAdBgNVHQ4E
FgQUp3W1AXXToZoy5GOOqbogGAD04z0wDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQByee5LpGY+reXV714Nm3gI6UuQSavUxM20+qjWsEFm5mB0KQ0MhLyo+IA5HRLh5HNku/PrsQfH
aHqLIT8sJLn1ioPTzw+T+GUTaFE3s2lIZxBYQSR9I3K3IXReqBCrYyQCYIQPRYdfyvzVBIWaycBz
iCozqje+b0J+IyZM1mlVx8N5wZGE6Qn4cBp70F2YBBKWSrGWxxwe+KV53EnKv2Whbb88wUqWGurej
0/7LCwvLFk00ruluBdF5cU1IHuIwwVmRiRyyIKj4Gr9pdTXVXGNjrSefvttY6COREPGEi0JeLhDJ
I6Trp4cHtKmvZZzfIKleuf0AYbzLUTrHRDDPqZ1IP/VCPQg26yLpMHpGoYn8wdrIcrSrDJvBdsW2
ldOA37C9GndCYWj3z61oMVRQv2H7NfgcIZCCi0arj4himnFMehHCrbR8945pGbvorCpGzbLY3rWu
FtiRv5VPBuqNCMI6VfH6Lj8++PyX+qvPfsrcylfmIFAGz59I6NIza1Smg6SPksb6XNG3ZmejlyBz
EdWIc+jmUJlr6LzvX8daWTlgXdab+CUmpheS+S1RbSrm7xM7nvB8rPOa5sgSRGF6c0zUlZVujpt0F
jW2zYgzx5hwhQa1MgyZda72ltok04mC4PXJQuVmMvLkUngUMyZrXzbX62ztvMr2d22fPMar/R2nC
Lw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0017*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000010*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu May 27 11:45:12 CEST 2021*

Valid to: *Sat Nov 27 10:45:12 CET 2027*

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:C5:32:9C:92:7C:99:E9:1C:8C:16:56:2E:12:76:2D:F4:FB:9A:AD:33:48:7B:A8:
29:D3:18:3D:AE:EF:88:85:0B:97:F6:32:CE:40:6A:80:44:9F:BF:E7:AC:33:41:B8:6B:75:5D:17:26:13:EB:C3:6B:6A:38:3C:81:A5:D1:0C:83:06:CC:05:69:5D:BB:45:12:80:47:83:D6:66:CF:F
9:CF:A2:93:99:0C:75:41:61:11:F3:D6:B6:92:38:74:29:6C:A1:2D:5D:F4:25:1E:29:1D:1F:56:8A:FA:C5:01:28:C0:B4:46:7E:2F:5C:76:79:8D:F7:B4:72:FC:C7:CA:E7:A2:DA:06:32:D7:7A:A6:
16:FB:B3:1E:DC:06:B7:43:3B:8D:0E:14:04:4F:B0:6B:28:20:5C:27:69:AA:A7:1C:01:0B:1D:A8:3E:92:88:42:DE:0A:39:6A:7B:86:7B:31:10:D8:CB:C6:7D:22:93:AE:50:CC:33:1E:A4:9D:ED:
F6:E7:26:9F:77:26:DF:4E:D2:09:CA:F5:A5:DF:E4:F6:0F:FB:61:B0:05:94:C7:09:60:51:9E:5E:E4:3F:02:C1:76:12:E8:13:16:30:67:CF:4F:99:53:96:85:DE:94:89:B0:EC:BA:0E:4E:A8:1E:8B:
E7:28:30:3B:5E:76:45:9E:61:3E:86:13:6E:47:07:CC:7D:1D:F9:57:0B:4F:92:69:0D:65:D4:03:ED:9A:A2:5E:66:CC:E1:F6:B7:57:27:D2:D5:F1:5A:DB:B9:FB:CF:B7:89:FB:11:1E:04:AC:16:9
4:A0:50:04:19:75:B1:D4:7C:3A:E9:23:15:AA:76:72:DE:1B:15:B2:2E:F1:0F:8B:8C:83:2A:04:2F:36:54:FA:D2:23:F0:AA:88:7F:7C:5F:1D:00:0B:0D:E0:90:80:2E:65:01:B1:F8:4E:03:0A:CF:
94:09:CD:A0:78:F4:A3:1A:F9:D2:2B:BE:F1:50:32:AF:C3:36:5B:85:5B:F8:83:58:FA:DD:21:CF:02:03:01:00:01*

Basic Constraints *IsCA: false*

Authority Key Identifier *D3:03:B2:43:DF:4A:3F:55:F7:C2:B9:A1:67:9C:8F:07:47:6D:6B:4E*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.1.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html

Policy OID: 2.16.620.1.1.1.2.4.1.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0017_p0013.crl*

Subject Key Identifier *A7:75:B5:01:75:D3:A1:9A:32:E4:63:8E:A9:BA:2A:18:00:F4:E3:3D*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DC:BA:48:89:ED:0C:20:92:EE:34:D1:9A:C0:2C:51:8D:F7:90:E8:46:D7:F0:D8:F5:BA:6F:68:A9:A9:4E:BE:EE*

X509SubjectName

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000010*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *p3W1AXXToZoy5GOOqboqGAD04z0=*

Service Status

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

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

Status Starting Time

2021-06-22T23:00:00Z

2.25 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *584350194013467672271747319798205481 28*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHzzCCBbegAwIBAgIQK/Ys5NMqE1CtZaeGhSbAIDANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UE
BhMCUFQxQDA+BgNVBAoMN1NDRUUgLSBTaXN0ZW1hIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOz
bmljYS8kbyBFc3RhZGBxETAPBgNVBAsMCEVDRXN0YWRvMSAwHgYDVQQDDBdDYXl0w6NvIGRlIENp
ZGFkw6NvIDAwNjAeFw0yMTExMTgxMTU3MTBaFw0zMzExMTgxMTU3MTBaMIHBMQswCQYDVQQGEwJQ
VDEzMDEGA1UECgwqSW5zdGl0dXRvIGRvcyBSZWdpc3RvcyBlIGRvIE5vdGFyaWFkbyBjLlAuMRww
GgYDVQQLDBNDYXJ0w6NvIGRlIENpZGFkw6NvMRQwEgYDVQQLDAtzdWlFQ0VzdGFkbzFjMEcGA1UE
AwxARUMgZGUgQXNzaW5hdHVyYSBEaWdpdGFsIFF1YWxpZmlj YWRhIGRvIENhcnTDo28gZGUgQ2lk
YWTDo28gMDAxODCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALIUmWBvlVkpGhcA4jFw
rTZ2cQTH9Q70x8RUYruy5KotxVf4xW5vHmsWvDXJEuuopSywWQ+MW3uXzNjMY0seimuTKk8NZVK2
qVCnKL1Izf5JxzyVXjddDMtqEPAa/iaagVzORuu75dCMfLDy3I7waYwNUI7BJHG5YLoU81zkgS2
OzaS9egq2DTWRioVIxnJ1uXRtI/cxD3w8noTbe6zU5G1E8F3dJf37fz2r05iEhMibG3n5KPjMS
/zWQTh2P5nTsMCmncab9UVwm6YMytOQjo763vw5J1RHvqW47pBRGNrPzlIRQp2u+vApiLTrYS2Q2
4ggvQ9NU+knGlWTMY42Q6cfkb/E6xn4fFlwa+ZOI/zpmlkJ/l7XUdTpSzbEIZ/OiV0PFi+gWG1Ic
5qZT9s0/T0xCgWX98GS5JDWIL0EwRmAQ9r2NQ5luk0nvWqJaF+g7Dv2ET7dAY3x92xm6X4N3IfzI
RI39/BI1aXKUKmMfBOjp28zjUAYb0XdMigabzYCmtUj9hDsleZZ420N0HbHeU6j6ef50i5mj6vsZ
51GRhobI5gPYLBsuQlKwNTy/XiTyAhM9HUcWO1xKroOZge2fu8LsCmcO02sTiohr91BI5Vg8o5ZG
4zMjvA2HtNpbLS5HN8US4UK9zKXhK/T8p+iwgmM/WhGGDdpxobP4/NHdAgMBAAGjggH8MIIB+DAS
BgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFDZb5RCplLktoGstc+Sz53tzlbA8MEwGCCsG
AQUFBwEBBEAwPjA8BggrBgEFBQcwAYYwaHR0cDovL29jc3Aucm9vdC5jYXJ0YW9kZWNpZGFkYW8u
cHQvcHVibGljby9yY3NwMIHqBgNVHSAEgeIwgd8wMQYEVR0gADApMCcGCCsGAQUFBwIBFhtodHRw
czovL3d3dy5zY2VlLmdvdi5wdC9yZXAwVAYKYIRsAQEBAgQABzBGMEQGCCsGAQUFBwIBFjhodHRw
Oi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL3BvbGl0aWNhcy9jcHMuaHRtbDUBgtg
hGwBAQECBAABAjBFMEMGCCsGAQUFBwIBFjdodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9w
dWJsaWNvL3BvbGl0aWNhcy9jcC5oqG1sMFcGA1UdHwRQME4wTKBKoEiGRmh0dHA6Ly9wa2kuY2Fy
dGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vbHjjL2NjX2VjX2NpZGFkYW9fY3JsMDA2X2NybC5jcmww
HQYDVR0OBBYEFBMEvMtr/1IYQFVeHzwyYR5EKr0VMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0B
AQsFAAOCAgEAi0WSS5pTpoE8kLpeoz/2GO0ZOQOR42H9xDoNxZO/m2+AoB6QoY3jgLKZYGF5N5TE3
8DtfRi+84+RfE6eNaqxJo1HuDqCIr8MO3gzCyXmXvutU2VTlVK0mUFwYyKJ6gRWmR2TdjEMayHRN0
oq14F0kzFgnGgvK9mtfXRtlsupMD654jNQ/tK7Gfhl+a7F39UnPcoWKjBoPA5vCTnXOp7bLm8dgr
xdyr3XrB2Ylzmvzvdjkf6tCXxX1H8jNDd3eXRVhIQpifwraaEyfjrDDHwF/efa/RPocpdHgFjiuiw
sw46ehD8s3TXSiqXlI3lrmSeYdCBSgmG5+mp1DnglNVLfKg2EOKgfLd5axWgENd+kloIYdOCa8ID
eiFwnDjpM2sC3wWwNdS2bTuR20jzb4PrPeqKRgA67T8UgzcKVZxZKLQAxFibFsD0THdlWVFPQzu
bHU5utvHcrA57+Wbzss8h5TUAU12myGfQImogyYEus/sdzOHGdmzgL1ALfE7aYkK9a3ghgfpWuxS
wag+27orW+NN6Mp+llxsfj7rweLuB+ECsMLCAPoxu95PkfR9Dbf/S9PRvQycauIGqEuaB514fEHn
5OVvyICzwIZogPcF1oK1fnjPhiDMNmKg4vXZNcZDc66Hvf+wbBjCmCNOMVoFPZjmD+LpV51Dsvhj
lg+1Okd/ubc=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 006*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C:	*PT*
Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*
Valid from:	*Thu Nov 18 12:57:10 CET 2021*
Valid to:	*Fri Nov 18 12:57:10 CET 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:B2:14:99:60:6F:21:59:29:1A:17:00:E2:31:70:AD:36:76:71:04:C7:F5:0E:F4:C7:C4:54:62:BB:B2:E4:AA:2D:C5:57:F8:C5:6E:6F:1E:6B:16:BC:35:C9:12:EB:A8:A5:2C:B0:59:0F:8C:5B:7B:97:CC:D8:CC:63:4B:1E:8A:68:93:2A:4F:0D:65:52:B6:A9:50:A7:28:BD:48:8B:37:F9:27:1C:F2:55:78:DD:74:33:2D:A8:43:C0:6B:F9:5A:6A:05:73:39:18:AE:EF:97:42:31:F2:C3:CB:72:3B:C1:A6:30:35:42:3B:04:91:C6:E5:82:EB:53:CD:73:92:04:B6:3B:36:92:F5:E8:2A:D8:37:D3:59:18:A8:56:5C:67:27:5B:95:5D:19:5F:FD:CC:43:DF:00:67:A1:36:DE:EB:35:12:1B:51:3C:17:77:49:7F:7E:DF:CF:6A:F4:E6:21:21:32:26:C6:DE:7E:4A:3E:33:12:FF:35:90:4E:1D:8F:4A:74:EC:30:29:A7:71:A6:FD:51:5C:26:E9:83:32:B4:E4:23:A3:BE:B7:BF:0E:49:D5:11:EF:A9:6E:3B:A4:14:46:36:B3:F3:94:84:50:A7:6B:BE:BC:0A:62:2D:3A:D8:4B:64:36:E2:A8:2F:43:D3:54:FA:49:C6:21:64:CC:63:8D:90:E9:C7:E4:6F:F1:3A:C6:7E:1F:14:8C:1A:F9:93:A5:FF:3A:66:96:42:7F:23:B5:D4:75:3A:52:CD:B1:08:67:F3:A2:57:43:C5:8B:E8:16:1B:52:1C:E6:A6:53:F6:CD:3F:4F:4C:42:81:65:FD:F0:64:92:24:35:88:2F:41:30:46:60:10:F6:BD:BD:43:92:2E:2B:49:EF:5A:A2:5A:17:E8:3B:0E:FD:B4:4F:B7:40:63:7C:7D:DB:19:BA:5F:83:77:95:FC:C8:44:8D:FD:FC:12:35:69:72:94:2A:63:1F:05:08:E9:DB:CC:E3:50:06:1B:D1:77:4C:8A:A6:9B:CD:80:A6:B5:48:FD:84:3B:08:79:96:78:DB:43:74:1D:B1:DE:53:A8:FA:79:F4:B4:8B:99:89:EA:FB:19:E7:51:91:86:86:C8:4A:03:D8:2C:1B:2E:42:52:B0:35:3C:BF:5E:24:F2:02:13:3D:1D:47:16:3B:5C:4A:AE:83:B6:81:ED:9F:BB:C2:EC:0A:67:0E:D3:6B:13:8E:88:6B:F7:50:62:E5:58:3C:A3:96:46:E3:33:23:BC:0D:87:B4:DA:5B:2D:2E:47:37:C5:12:E1:42:BD:CC:A5:E1:2B:F4:FC:A7:E8:B0:82:63:3F:5A:11:86:0D:DA:71:A1:B3:F8:FC:D1:DD:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*36:5B:49:10:A9:94:B9:2D:A0:6B:2D:73:E4:B3:4B:7B:73:21:B0:3C*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cp.html*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl006_crl.crl*
Subject Key Identifier	*13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*94:7E:C4:0B:C4:1A:BC:B8:76:5B:29:BC:61:2E:AF:D2:19:F5:DE:5F:EF:2A:56:9B:CF:73:BA:DB:26:61:E0:94*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*
Subject OU:	*subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

X509SKI

X509 SK I *EwS8y2v/UhhAVV4fPDJhHkQqvRU=*

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

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

Status Starting Time *2021-12-06T13:29:03Z*

2.25.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.25.2 - Extension (not critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

2.26 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000011

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000011*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *9119714372100171949*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIII5TCCBs2gAwIBAgIIfo+75zIOKK0wDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIlERpZZI0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE4MBdXDTIxMTExODE1MTI0DFoXDTI4MDUyMDE1MTI0DFowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUsw5QYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2Eg ZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTEwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDaOeORq5kXbKJO8Q3F
gWiVCSQ01Il85bouhXxyTcvlay5nyhjW89itij9Lf6Tnm1c1jsDYfVhnEWZb3paywaku3L b9rFcN
Lfb6vq7hNksKsrdWHAYloFJw2lnOWakNxS1jm/+7EO6GFmq0/fjOVgvF3o+F1yNWb26aG/4pmdDC
r6XHL14N+dpxyv5bR3R1yLoapvm5AgKPy/Ne0ihNwn/0LVhNAhsIYx5xWTUvqG4Zr+YSLmWqHhwI
yRJzfedGf2Bq6OvgZfhZqWSsOkNOROC7bb1CwggA/woA958qJhikVyhqblUgGfHF2g8B9mVYLWkW
R1LTpyc6OC0U4OYAqfC424 7cFO6m6xm0cp/eV2WWFteaZAfn8pAvePIOQ94cVIuU5bMKmc/C7UyY
b//rPEy4FOBeQv/ogPfKBSfESaPWF7IKw/6Vp2N2Xwl/sKXi/4MKi4nCxqhSlakvbn2yHddpole+
CGh4OyUC8tlF862SetPrEMViS5O49vvDuZ0wYkMCAwEAAaOCA1gwggNUMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUEwS8y2v/UhhAVV4fPDjhHkQqvRUwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMThfZGVsdGFfcDAwMDEuY3JsMIHpBgNV
HSAEgeEwgd4wZAYLYIRsAQEBAgQAAQcwVTBTBggrBgEFBQcCARZHaHR0cDovL3Bra55jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYXMvcGMvY2NfdGltZXN0YW1wX3BjLmh0bWwwdg1L
YIRsAQEBAgQBAAcwZzBlBggrBgEFBQcCARZZaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQv
cHVibGljby9wb2xpdGljYXMvZHBjL2NjX3N1Yi1Y19jaWRhZGFvX2Fzc2luYXR1cmFfZHBjLmh0
bWwwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwgcYGCCsGAQUFBwEDBIG5MIG2MIGzBgcEAIGXXgEB
DIGnQnkqaW5jbHVzaW9uG9mIHRoaXMgc3RhbGVtZWS0IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQg
dGhpcyB0aW1ILXN0YW1wIHRva2VuIGZlGlzc3VlZCBhcyBhIHF1YWxpZmllZCBlbGVjdHJvbmlj
IHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdVTEFUSU9OIChFVSkgTm8gOTEwLzIwMTQw
aQYDR0fBGlwYDBeoFygWoZYaHR0cDovL3Bra55jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9s
cmMvY2Nfc3ViLWVjX2NpZGFkYW9fYXNzaW5hdHVyYV9jcmwwMDF4X3AwMDAxLmNybDAdBgNVHO4E
FgQUbr744orY2ubRkxIBAJNwrAxdvCQwDgYDVR0PAQH/BAQDAgbAMA0GCSqGSIb3DQEBCwUAA4IC
AQCFovy2D/+FcYqScu/2zCbmHJ/vpC/J2TiNJuF01xluPKJjy28qFozvu8r/TBuWMT90Mwte+RX4
JO3mwEnFcoqJH9p32/OykuJsh+tbTFAjdGcPBptMrIjTfw6UdtXbrEbp0Gu0gZ1HEw9/jXbcGzVB
rW1I3jIYbMCtxU9RVyYq/Skltp0CE4Cd6v1FYYtgbN/p6TWzszxtc0/iX47ebk84YRUUv7LQcJ2p
0WBpF2ofOsYjFXCwlbvAIooFrU9Kcn1KXtzUWB3QaFXcYsW91j+ARrBvYOwyvxUEKICB/N22sX
9+O/S+V9yNlAcjT1xXsJWnjh5N/2JhXsvqm2cQrj1uKtgvrnPT3/zXjAcOuTpaIwwH+xLJ6Wphof
cVZWXX+T3P4nP59yY+dszFZ5LUe/VaR8gxxMs87I75fhjJcHVRftAXH+rr55FRebpx1YraqraDTj
zxfa6QFcZkh42I2rlRJRUrSgQ3NxUbE3rGR3UVilDayTF3Q/MACQbTmzJhIrFb5yv8dgVkir9t57
CaxwoQu48dck3BqLckxqg5mmE5jutc2KkOMkzTXLOfRE85Red5pwKXKVZnZtA3qylo590E6947M
E/PftfdQUTxpUArC0PAsI8KhhwFJosa03M3sd1JcECL7H49B/sxgOeo2h9gillclz83XwlMgvBLw
0Q==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000011*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu Nov 18 16:12:48 CET 2021*

Valid to: *Sat May 20 17:12:48 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:DA:39:E3:91:AB:99:17:6C:A2:4E:F1:0D:C5:81:68:95:09:24:34:D4:99:7C:49:
BA:2E:85:7C:72:4D:CB:E5:6B:2E:67:CA:18:D6:07:D8:AD:8A:3F:4B:7F:A4:E7:9B:57:35:26:C0:D8:7D:58:67:11:66:5B:DE:96:B2:C1:A9:2E:DC:B6:FD:AC:57:0D:2D:F6:FA:BE:AE:E1:36:4B:
0A:B2:B7:56:1C:06:25:A0:52:70:D8:89:CE:59:A9:0D:C5:2D:63:9B:FF:BB:10:EE:86:16:6A:B4:FD:F8:CE:56:0B:C5:DE:8F:85:D7:23:56:6F:6E:9A:1B:FE:29:99:D0:C2:AF:A5:C7:2F:5E:0D:F
9:DA:71:CA:FE:5B:47:74:75:C8:BA:1A:A6:F9:B9:02:02:8F:CB:F3:5E:D2:28:4D:C2:7F:F4:2D:58:4D:02:1B:08:63:1E:71:59:35:2F:A8:6E:19:AF:E6:12:2E:65:AA:1E:1C:08:C9:12:73:7D:E7:
46:7F:60:6A:E9:0B:E0:65:F8:59:A9:64:AC:3A:43:4E:44:E0:BB:6D:BD:42:C2:08:00:FF:0A:00:F7:9F:2A:26:18:A4:57:28:6A:6C:85:20:19:F1:C5:DA:0F:01:F6:65:58:2D:69:16:47:52:D3:A7:
27:3A:40:2D:14:E0:E6:00:A9:F0:B8:DB:8E:DC:14:EE:A6:EB:19:B4:72:9F:DE:57:65:96:16:D7:9A:64:07:E7:F2:90:2F:78:FD:4E:43:DE:1C:56:2B:94:E5:B3:0A:99:CF:C2:ED:4C:98:6F:FF:EB
:3C:4C:B8:14:E0:5E:42:FF:E8:80:F7:CA:05:27:C4:49:A3:D6:17:82:0A:C3:FE:95:A7:63:76:5F:09:7F:B0:A5:E2:FF:83:0A:8B:89:C2:C6:A8:52:95:A9:2F:6E:7D:B2:1D:D7:69:A0:87:BE:08:6
8:78:3B:25:02:F2:D9:45:F3:AD:92:7A:D3:EB:10:C5:62:4B:93:B8:F6:FB:C3:B9:9D:30:62:43:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0018_p0001.crl*
Subject Key Identifier	*6E:BE:F8:E2:8A:D8:DA:E6:D1:91:79:41:00:93:70:AC:0C:5D:BC:24*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*31:78:D1:92:2C:40:C7:F9:9B:B2:69:54:23:D8:60:82:0E:B0:8D:7E:E2:35:91:F9:AF:8B:C9:1E:C2:E1:A8:A1*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000011*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*br744orY2ubRkXIBAJNwrAxdvCQ=*

Service Status

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

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

Status Starting Time

2021-12-06T13:30:28Z

2.27 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000012

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000012*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *646037643281482037*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIItjCCBp6gAwIBAgIICPcv0E9SwTUwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE4MB4XDTIyMTAyNjE0MjczMFoXDTI5MDQyNzE0MjczMFowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIlEiNpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXj2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTIwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDiee81rA2AWAMqVw13
O5apU5Cmbv/PWnbecptDQemZ+iPI/D98GPtzbzC+nvZDkVyhsXG3y8WGkW0mZS9S14We9Dk9wc01R
Ujwn734PvRPyDRAD6lqFj9oNz6HHT3iRzoB1ACgmyC+YmqUiH1n0iTjwq0sWfllp7yLmj2c8Ruml
hSciX+G+Rnib3jXQwSG3UYUBjXBZNJHjhkIshwd+tmif8a+cw2dfDcE78yi3quWNz+IA/ga0V8wN
RalusigcwjMR6QRswy0XCp1wWlRTdnU4NySvV1X2JZfYGK//N2+qPR5VAgoARwogmduAkztQTzM/
KZ8JajZO53C1ruKimdgj3yyyhHhLhUbsMUAOUsND5PjyLBzm9dB27rx6PeYzu+tw3rIeQpfXWDIA
U2JvZF8kd88yL0du6vM4IPrkMq2MhtoqYg4VZlHY6Vc4fznD/8+C/JQ3zxy46WpqsG2ixi7yEAGt
9bMDO473JPfii1ycgNr4U+05ps88sUu4axFUkhECAwEAAaOCAykwggMlMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUEwS8y2v/UhhAVV4fPDJhHkQqvRUwSwYKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2Nzc0BvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMThfZGVsdGFfcDAwMTAuY3JsMIG6BgNV
HSAEgbIwga8wVQYLYIRsAQEBAgQAAQcwRjBEBggrBgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFv
ZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NwLmhObWwwVg1LYIRsAQEBAgQBAAcwRzBF
BggrBgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRp
Y2FzL2Nwcy5odG1sMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMIHGBggrBgEFBQcBAwSBuTCBtjCB
swYHBACBl14BAQyBp0j5IGluY2x1c2lvbiBvZiB0aGlzIHN0YXRlbWVudCB0aGUgaXNzdWVvIGNs
YWltcy B0aGF0IHRoaXMgdGlzZS1zdGFtcCB0b2tlbiBpcyBpc3N1ZWQgYXMgYSBxdWFsaWZpZWQg
ZWxlY3Rybz5pYyB0aW1lLXN0YW1wIGFjY29yZGluZyB0byB0aGUgUkVHVUx8VEIPTAoRVUpE5v
IDkxMC8yMDE0MGkGA1UdHwRiMGAwXqBcoFqGWGh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJjL2NjX3N1Yi1IY19jaWRhZGFvX2Fzc2luYXR1cmFfY3JsMDAxOF9wMDAxMC5j
cmwwHQYDVR0OBBYEFKo5HwFUO6jQXMxFAO5omZg1IVD4MA4GA1UdDwEB/wQEAwIGwDANBgkqhkiG
9w0BAQsFAAOCAgEACKQGcxTMLtrkSwaBfa5Ot08XTc7HdQHKZWrR5BPfgyqF/pbusjYOnX6D5XYo
v5ACD5FkjLlICQkICdgmk3I5I1ysW+5DY774olip75H7LygInERQgCDRnHlcAeQeTEynRTBduQpx
1Sa3spJSKRyX+NQWFcQ9ZR5GgHRWe8apo3g8E36WsYoJwlc+j1TbQS/YeYl/7o7T1KTrJsRX7X7V
YvOh16D1QStetQUoOWrecHpsZuWbbgSmi3DE9jNuXbg0W9zVa8RGXVSheKp/NCbo2l1cjqoz0o00
6YqGovx3yifmwpHuvJn1XK8lz+wU9QAAXk+3+vgNblDUZYKbKKcvObFX7OiftpxHElbjkam0bSvYf
UNNQjbKFkgP6GDgc18BJgxECGMqS3zsPVShbjbb/4dsa3ThAMwSNVfUcZOdRUgkokF1oh5cCDGwp
7SF7wi96tst/TReluUOj+56/lUTuy5h/vDw39rMVuzjS++0MkHAyMkZ8iBd2+PZ2+H+g//HN9wZH
8zoPjrv9FkcFlhEHrttF8TctFNbtcIzXCoyyWCMn1AZQ2tIl5BldCJfjCDWByEEjkvZsACAj6vpX
2ITHW16jANizCiQV9kWACeTyYhInbuvYUsfe7vBAr2OfVRBJIg T5jVwymokCb3d19PV30uTdSRLE
43D+hBrR65mG2mM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000012*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Wed Oct 26 16:27:30 CEST 2022*

Valid to: *Fri Apr 27 16:27:30 CEST 2029*

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:E2:79:EF:35:AC:0D:80:58:03:2A:57:0D:77:3B:96:A9:53:90:A6:6E:FF:CF:5A:76:DE:72:9B:43:41:E9:99:FA:23:D5:0F:DF:06:3E:DC:DB:CC:2F:AB:BD:90:E4:57:28:6C:5C:6D:F2:F1:61:8A:5B:49:99:E7:D4:B5:E1:67:BD:0E:43:F0:73:4D:51:52:3C:27:EF:7E:0F:BD:13:F2:0D:10:03:E8:8A:B5:8F:DA:0D:CF:A1:C7:4F:78:91:CE:80:75:00:28:26:C8:2F:98:9A:A5:22:1F:59:F4:89:38:F0:AB:4B:16:7E:59:69:EF:22:E6:8F:67:3C:46:E9:A5:B5:27:22:5F:E1:BE:46:78:9B:DE:35:D0:C1:21:B7:51:B5:01:BD:70:59:34:91:E3:B6:42:2C:B7:07:7E:B6:68:9F:F1:AF:9C:C3:67:5F:0D:C1:38:F3:28:B7:AA:E5:BD:CF:E9:40:FE:06:B4:57:CC:0D:45:A9:6E:B2:28:1C:C2:33:11:E9:04:6C:C3:2D:17:0A:9D:70:58:84:53:76:75:38:37:24:AF:57:55:F6:25:97:D8:18:AF:FF:37:6F:AA:3D:1E:55:02:0A:00:47:0A:20:99:DB:80:93:3B:50:4F:33:3F:28:6F:09:68:96:4E:E7:70:B5:AE:E2:A2:99:DA:A3:DF:2C:B2:84:78:4B:85:46:EC:31:40:0E:52:C3:43:E4:F8:F2:2C:1C:E6:F5:D0:73:EE:BC:7A:3D:E6:33:BB:EB:70:DE:B2:1E:42:97:D7:58:32:00:53:62:6F:64:5F:24:77:CF:32:2F:47:6E:EA:F3:38:20:FA:E4:32:AD:8C:86:DA:2A:62:0E:15:64:81:D8:E9:57:38:7F:39:C3:FF:CF:82:FC:94:37:CF:1C:B8:E9:6A:6A:B0:6D:A2:C6:2E:F2:10:01:AD:F5:B3:03:3B:8E:F7:24:F7:C8:8B:5C:9C:80:DA:F8:53:ED:39:A6:CF:3C:B1:4B:B8:6B:11:54:92:11:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Key Identifier *13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.1.7

CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html

Policy OID: 2.16.620.1.1.1.2.4.1.0.7

CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0018_p0010.crl*

Subject Key Identifier *AA:12:1F:01:54:3B:A2:50:5C:CC:45:00:EE:68:99:98:35:89:50:F8*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B2:21:B4:7E:3C:59:01:F6:A4:97:EC:1B:2C:87:66:E8:70:70:7C:E5:FE:22:37:32:AE:D4:8C:64:CD:DE:68:93*

X509SubjectName

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000012*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *qhIfAVQ7olBczEUA7miZmDWJUPg=*

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

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

Status Starting Time *2022-12-19T14:22:21Z*

2.28 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000013

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000013*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *8909210294585921858*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIItjCCBp6gAwIBAgIIe6Pfj1YMEUIwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2l0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE4MB4XDTIzMDkyMDE1MDAzNVoXDTMwMDMyMjE1MDAzNVowgcYxC2AJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTMwggGiMA0GCSqGSib3DQEBAQUAA4IBjwAwggGKAoIBgQDG1G/rIZQ8hBr6aD8y
j8gVK4eQV+BWNkXe+Vq8OJ7Wd4a50m57CTX4AxkDxr4+HdWlb0Ap6PZLL/QiX5dKF8W2Wc7yp1N
lvmdWHoXLfIMZmFtaHUajyR/skuLrhIIl9KuaqkC65CtomjChhn0ODoQLDCHecahbVfodSvXk7rN
n94kKxzN6Pm0NHJvDI1p4+FkMQhRXj4zi4LfZoi9iIM79z7Orzpq9sa31K2L/ohWmU5/XTLNZnLO
AGCyovqFVt5a1wlRYKvxHo+MNSBGLQGo1ZzgCvswtXQuVYk8d6qyKwcFEK5aGY2rtDN6ImgHSaym
Z0w1l/S3TDP7HJjC2ZdLD+pAwkQns9YUDYVKf7LRSCLR0w6ltBuT5AGmsFJJQCJ6o8fWenzEKf9
sq/cOKAc51pcSjowxm1+1yAswP/VmMs5HlCIT3pOwmQd/x+46/OGGQt1Kyo00/UVk00ltEr6nSGW
lfukWOAgFeUVuIPkOs8oPWzp02f78W3jI1V6/kCAwEAAaOCAykwggMlMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUEw58y2v/UhhAVV4fPDJhHkQqvRUwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMThfZGVsdGFfcDAwMTYuY3JsMIG6BgNV
HSAEgbIwga8wVQYLYlRsAQEBAgQAAQcwRjBEBggrBgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFv
ZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NwLmh0bWwwVgYLYlRsAQEBAgQBAAcwRzBF
BggrBgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRp
Y2FzL2Nwcy5odG1sMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMIHGBggrBgEFBQcBAwSBuTCBtjCB
swYHBACBl14BAQyBp0j5IGluY2x1c2lvbiBvZiB0aGlzIHN0YXRlbWVudCB0aGUgaXNzdWVyIGNs
YWltcy B0aGF0IHRoaXMgdGlzZS1zdGFtcCB0b2tlbiBpcyBpc3N1ZWQgYXMgYSBxdWFsaWZpZWQg
ZWxlY3Ryb25pYyB0aW1lLXN0YW1wIGFjY29yZGluZyB0byB0aGUgUkVHVUxBVElPTiAoRVUpIE5v
IDkxMC8yMDE0MGkGA1UdHwRiMGAwXqBcoFqGWGh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJjL2NjX3N1Yi1IY19jaWRhZGFvX2Fzc2luYXR1cmFfY3JsMDAxOF9wMDAxNi5j
cmwwHQYDVR0OBBYEFCDGksiFyciv3TB+2g7/EafUdBLeMA4GA1UdDwEB/wQEAwIGwDANBgkqhkiG
9w0BAQsFAAOCAgEAJIs8IlAnoLGsDUVB8jGqrAvhfrR4GjpIKzOvLpAWl5jEfzbd2Pdq3tDC2+oa
ax+W82EOAquKafv/g4UzUXti6kbu5Vk0zEseaFFhGGIg51faPhAd7tDwsdKxmDQfP1JDKss0ZLHd
wQVCANHNxDESHSijO25gWZskpNajCETjnE21OgKHEBPnG3u7ZKEAXz08zsyin/9na6Jn29ksqWpW
mAL50+dZHypyM2BFvOEN7s2/y+icODCtvUIMM6rzM8gCFThVFbKUA6q+evYG3gLXMOjA+86m1usH
ndM4QBQIdv3yPPSK9rgrQA+BawIlbUmPbhdP+ozRgKpZCsvE6pcID71CmWARQdsb6V2By+yWPwKz
FWV1bXkvJBOiiVvfTxMTOAf1QS8kz7HKa8sH932YnYinWJK0JrxmPo4Q7h86ibdQ9mC4/bliMs+F
5HRHOiVrAoYjNTX+UG595K76p+cx615e6W/iCtftARZ8+lS+yGd3xHdGVWpD7tj+Bex6GI61byr5
qBBTW9x0P0yhjIDW8eDwiM3xvzVcwZEPN45vgm/kZX7KPL3eFgdvQAvn+gkINU0oqm5+LpQuHS2d
AP3OdE6T1mfkEBn8RXRtqdui6SfdyQiN8clzSOddQO0YntjQQIKXXmDmynpdZX7ZLRhI5NogPhUr
qw8TXw9ydNMizq4=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000013*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C:	*PT*
Valid from:	*Wed Sep 20 17:00:35 CEST 2023*
Valid to:	*Fri Mar 22 16:00:35 CET 2030*
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:C6:D4:6F:EB:21:94:3C:84:1A:FA:68:3F:32:8F:C8:15:2B:87:90:57:E0:56:36:45:DE:F9:58:3C:38:9E:D6:77:86:B9:D2:64:BB:09:F4:D7:E0:0C:64:0F:1A:F8:F8:77:56:95:BD:00:A7:A3:D9:2C:BF:D0:89:7E:5D:28:5F:16:D9:67:13:CA:9D:4D:22:F9:9D:58:7A:17:2D:F9:4C:66:61:6D:68:75:1A:8F:24:7F:B2:4B:8B:AE:12:25:23:D2:AE:6A:A9:02:EB:90:AD:A2:62:42:86:19:F4:38:3A:10:2C:30:87:79:C6:A1:6D:57:E8:75:2B:D7:93:BA:CD:9F:DE:24:2B:1C:CD:E8:F9:B4:34:72:6F:0C:8D:69:E3:E1:64:31:08:51:5E:3E:33:8B:82:DF:66:88:BD:88:83:3B:F7:3E:CE:AF:3A:6A:F6:C6:B7:D4:AD:8B:FE:B8:56:99:4E:7F:5D:32:CD:66:72:CE:00:60:B2:A2:FA:85:56:DE:5A:D7:09:51:60:AB:F1:1E:8F:8C:35:20:46:2D:01:A8:D7:6C:E0:0A:FB:30:B5:74:2E:55:89:01:77:AA:B2:2B:07:05:10:AE:5A:19:8D:AB:B4:33:7A:96:68:07:49:AC:A6:67:4C:35:8A:5E:77:4C:33:FB:1C:97:36:65:D2:C3:FA:90:30:91:09:EC:F5:85:03:61:52:9F:EC:B4:52:08:B4:74:C3:A2:2D:06:E4:F9:00:69:AC:14:92:09:40:22:7A:A3:C7:D6:7A:7C:C4:91:F2:3D:B2:AF:DC:38:A0:1C:E7:5A:5C:4A:3A:30:C6:6D:7E:D7:20:2C:C0:FF:D5:98:CB:39:1E:50:A2:4F:7A:4E:C2:64:1D:FF:1F:B8:EB:F3:86:19:0B:75:2B:2A:34:D3:F5:15:93:4D:25:B4:4A:FA:9D:21:96:95:FB:A4:58:E0:20:15:E5:15:B8:83:E4:3A:CF:28:3D:6C:E9:D3:67:FB:F1:6D:E3:23:55:7A:FC:99:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*
Authority Info Access	*http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0018_p0016.crl*
Subject Key Identifier	*2D:06:92:C8:85:C9:C8:AF:DD:30:7E:DA:0E:FF:11:A7:D4:E0:12:DE*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D9:47:D1:1B:34:83:5D:72:F6:D0:9A:BE:21:1E:98:83:1C:8F:49:C9:CC:BB:F2:1E:F5:A9:D0:18:8B:3E:E2:85*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000013*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*LQaSyIXJyK/dMH7aDv8Rp9TgEt4=*

Service Status

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

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

Status Starting Time

2024-01-09T17:03:12Z

2.29 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0019

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0019*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *494777123083895326214520357384828820271489626155*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFjDCCBIWgAwIBAgIUVqqS0sDlTrNkjgRu3GyNnEvoMCswCgYIKoZIzj0EAwIwgYQxCzAJBgNV
BAYTAlBUMUAwPgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLD
s25pY2EgZG8gRXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBD
aWRhZMOjbyAwMDgwHhcNMjQwMjE0MTEwMjM4WhcNMzYwMjE1MDAwMDAwWjCBwTELMAkGA1UEBhMC
UFQxMzAxBgNVBAoMKkluc3RpdHV0byBkb3MgUmVnaXN0b3MgZSBkbyBOb3RhcmlhZG8gSS5QLjEc
MBoGA1UECwwTQ2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8xSTBHBgNV
BAMMQEVDIGRlIEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENp
ZGFkw6NvIDAwMTkwdjA0BgcghkjOPQIBBgUrgQOAIgNiAAQA0h6BcyZ40GOD+U+nkMHf5QVQsmydt
bWSetqwWROgLqsrixzKl5sDuS7vlK6MD50t4b4OKRYQwm1Lytmx2TTPKh8Bd5yQdl4N7DTWN7yCL
b+tAT/5FjIAvUyxtNhhap22jggJ3MIICczASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaA
FKsAgCv7M0T5Pfhe+d7/sXNnmWL+MIGsBggrBgEFBQcBAQSBnzCBnDBfBggrBgEFBQcwAoZTaHR0
cDovL3BraTluY2FydGFvZGVjaWRhZGFvLnB0L2VudGlkYWRlLWNlcnRpZmljYWNhby1jYy9jZXJ0
aWZpY2Fkb3MvQ0NfUm9vdDAwOC5jcnQwOQYIKwYBBQUHMAGGLWh0dHA6Ly9vY3NwLnJvb3QucGtp
Mi5jYXJ0YW9kZWNpZGFkYW8ucHQvb2NzcDCB9AYDVR0gBIHsMIHpMDIGBFUdIAAwKjAoBggrBgEF
BQcCARYcaHR0cHM6Ly93d3cuc2NlZS5nb3YucHQvcmVwLzBYBgpghGwBAQECBAAHMEowSAYIKwYB
BQUHAgEWPGh0dHA6Ly9wa2kyLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL3ByYXRpY2F2LWNl
cnRpZmljYWNhbzBZBgfghGwBAQECBAABAjBKMEgGCCsGAQUFBwIBFjxodHRwOi8vcGtpMi5jYXJ0
YW9kZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYS1jZXJ0aWZpY2Fkb3MwZwYDVR0fBGAwXjBc
oFqgWlZWaHR0cDovL3BraTluY2FydGFvZGVjaWRhZGFvLnB0L2VudGlkYWRlLWNlcnRpZmljYWNh
by1jYy9saXN0YS1yZXZvZ2FjYW8vQ0NfUm9vdDAwOC5jcmwwHQYDVR0OBBYEFBw273lpGPq/o4oa
XRcMuBCA1DrwMA4GA1UdDwEB/wQEAwIBBjAKBggqhkjOPQODAgOBjAAwgYgCQgGcYUvVLnvvaDGF
rSaf3y0j28fjA6PH/q5/M4oEibTGJ6/oLjH3RUJHJP1cCDDwpy3FD3XtTKrnr0tWoo9Hn/3yQJC
AJxn0fFkrhctov1Q83mvWUiTCotzaMi7okk33bwLhv00DL+alRodMxKZStw2sbkSFwZsjCf8M6Sl
7UbiKdSYu7EN

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer CN: *Cartão de Cidadão 008*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0019*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C:	*PT*
Valid from:	*Wed Feb 14 12:02:38 CET 2024*
Valid to:	*Fri Feb 15 01:00:00 CET 2036*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:00:D2:1E:81:73:26:78:D0:64:03:F9:4F:A6:90:C1:F9:41:54:2C:9B:27:6D:6D:64:9E:B6:AC:16:44:E8:0B:AA:CA:E2:C7:32:88:E6:C0:EE:4B:BB:E5:2B:A3:03:E7:4B:78:6F:83:8A:45:84:30:9B:52:F2:B6:6C:76:4D:33:CA:87:C0:5D:E7:24:1D:23:83:7B:0D:35:8D:EF:20:8B:6F:EB:40:4F:FE:45:8C:80:2F:53:2C:6D:36:18:5A:A7:6D*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*AB:00:80:2B:FB:33:44:F9:3D:F8:5E:F9:DE:FF:B1:73:67:99:62:FE*
Authority Info Access	*http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/certificados/CC_Root008.crt* *http://ocsp.root.pki2.cartaodecidadao.pt/ocsp*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep/* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki2.cartaodecidadao.pt/publico/politica-certificados*
CRL Distribution Points	*http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/lista-revogacao/CC_Root008.crl*
Subject Key Identifier	*1C:36:EF:79:69:18:FA:BF:A3:8A:1A:5D:17:0C:B8:10:80:D4:3A:F0*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*73:A0:D6:BF:AA:D0:17:08:40:90:EE:16:44:32:66:05:04:31:B2:74:83:0C:46:15:81:9A:34:2C:59:D2:8C:D7*

X509SubjectName

Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0019*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*

X509SKI

X509 SK I	*HDbveWkY+r+jihpdFwy4EIDUOvA=*

Service Status

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

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

Status Starting Time

2024-03-08T13:38:05Z

2.29.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.30 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000014

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000014*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6853240843527102386*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIItjCCBp6gAwIBAgIIXxuaPLahn7IwDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnN0aXR1dG8gZG9zIFJlZ2lzdG9zIGUgZG8gTm90YXJpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE4MB4XDTI0MTAxNTE0MTI0N1oXDTMxMDQxNzE0MTI0N1owgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCB1ZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhw6fDo28gQ3Jvbm9sw7NnaWNhMUswSQYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8Ojby8Dcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTQwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC4WlADFouSGtBtiVj/
f3HVYU8z87U0aHcrDuw7jWQh/hW5ca/nCazdxgYqOpcTeIiTvXksxMDImt2YibZOC813ZG4XzrVC
AWII7qGruQNf7k1Tuv/wP7fVtpd4nwRam6ODGXlRhUHW+Di27k7LbH5QX4JJcbddBaaI9SXy/jwE
kKvrPaDEO2wb/UkGFeahRa74Xl3qX2MoIKSqluruqOFXcN9RjCStt XOFY9wxoLt5hp5m8tTZABfq
drDPZ8RZr8NLJnxid7BfT9zUl6iO5xinaS4UrU9rgRk5E4asBuIHUrfNNLjHZApFTy5vL7ltkIXL
seDUVzkQH8Lt5jL8T77b9dMjCeELBwfF2RLgMyWa+dYZ+INROOEiGky2dXbOD7+pLUka5x6MT331r
gZu2VLSeifwbee/LJD1vCb3urtdjW2DhAlrrK46AbqxV1QFaCnqBz5t+5cVumacH1x6C5SnGpF1i
vqXnGwaLk8Cdujztkxgs515uh0H8M9hhUG1M4KkCAwEAAaOCAykwggMIMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUEw58y2v/UhhAVV4fPDJhHkQqvRUwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMThfZGVsdGFfcDAwMjAuY3JsMIG6BgNV
HSAEgbIwga8wVQYLYlRsAQEBAgQAAQcwRjBEBggrBgEFBQcCARY4aHR0cHM6Ly9wa2ku Y2FydGFv
ZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NlwLmh0bWwwVgYLYlRsAQEBAgQBAAcwRzBF
BggrBgEFBQcCARY5aHR0cHM6Ly9wa2ku Y2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRp
Y2FzL2Nwcy5odG1sMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMIHGBggrBgEFBQcBAwSBuTCBtjCB
swYHBACBl14BAQyBp0j5IGluY2x1c2lvbiBvZiB0aGlzIHN0YXRlbWVudCB0aGUgaXNzdWVyIGNs
YWltcy B0aGF0IHRoaXMgdGltZS1zdGFtcCB0b2tlbiBpcyBpc3N1ZWQgYXMgYSBxdWFsaWZpZWQg
ZWxlY3Ryb25pYy B0aW1lLXN0YW1wIGFjY29yZGluZyB0byB0aGUgUkVHVUxBVElPTiAoRVUpIE5v
IDkxMC8yMDE0MGkGA1UdHwRiMGAwXqBcoFqGWGh0dHA6Ly9wa2ku Y2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJjL2NjX3N1YiI1Y19jaWRhZGFvX2Fzc2luYXR1cmFfY3JsMDAxOF9wMDAyMC5j
cmwwHQYDVR0OBBYEFBZmf3xMkAVUGoQ1mVlnI9pd1MA4GA1UdDwEB/wQEAwIGwDANBgkghkiG
9w0BAQsFAAOCAgEAYkfXbcgEx7uszBCr+UFhJlXrhlhLgOIVb2B4LpMnRmPDqz5j5QQAx+3QEkQG
fUwm7tTlr8nl2b4IxhmVt7weOjVJDJLOzhaGv8+PPmkfB7ZqLh98X5ZW4orgt1WDh9zTpwjNZeVK
090TNvAZuZYC8f9hxYIGle6iIQ5Fw+8H9jErsQdUFlqCPEWRK23QcagvdvScbvAbZhp/w+yih+Sf
Yw56m2iBFqF+EbyYe6b5IAM5rZmKuiwjX5+3ym2Vds2pfz0Rb1/el0+mDj74yxT38eg/UNPz1MhT
JUEPdjqq2fimxGxf/EWtWy7ucQVmRMho8B3Z6rDOerjWf63Q5oFuCNp/cMslPWjuN+VLhwjZlpG
3hvsRsVEvBB/PiIulUzxPbzKEudtiwsHlm4ULMVmVfQjlw7L6S65lOh1ZkkULx2z3iODAv6tfd0F
6/RajbD0QlakmjDr4xnnKZEjcpXAz2S2zbQu0dscLEN5Su8FmStxQQ1RI56RZjjAQu67eswko504
xtVJeAVGh3vhHeR/Z5rkhgLa0MOHy4AgTjPVQIq68YmA34v60DhTyLNcAUswFQcqhV+V5CLiEfzc
33BX+qRN+H3qAGcIDgzji8L0KkpVSD/nZal2bSZe/RuiuVR1UmeGiGK7KrKd8s/8A5zmtwXLFdns
M54CAdh6u0by5Fk=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Issuer OU: *subECEstado*

Issuer OU:	*Cartão de Cidadão*
Issuer O:	*Instituto dos Registos e do Notariado I.P.*
Issuer C:	*PT*
Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000014*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*
Valid from:	*Tue Oct 15 16:12:47 CEST 2024*
Valid to:	*Thu Apr 17 16:12:47 CEST 2031*
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:B8:58:80:03:16:8B:92:1A:D0:6D:89:52:7F:7F:71:D5:61:4F:33:F3:B5:34:68:77:2B:0E:EC:3B:25:64:21:FE:15:B9:71:AF:E7:09:AC:DD:C6:06:2A:42:97:13:78:88:93:BD:79:2C:C0:C0:C8:9A:DD:98:89:B6:4E:0B:CD:77:64:6E:17:CE:B5:42:01:62:25:EE:A1:AB:B9:03:5F:EE:4D:53:BA:FF:F0:3F:B7:D5:B6:97:78:9F:04:5A:9B:A3:83:19:72:11:85:41:D6:F8:38:B6:EE:4E:CB:6C:7E:50:5F:82:49:71:B7:5D:05:A6:88:F5:25:F2:FE:3C:04:90:AB:EB:3D:A0:C4:3B:6C:1B:FD:49:06:15:E6:A1:45:AE:F8:5C:8D:EA:5F:63:28:20:A4:AA:96:EA:EE:A8:E1:57:70:DF:51:24:24:AD:B5:73:85:63:DC:31:A0:BB:79:86:9E:66:F2:D4:D9:00:17:EA:76:B0:CF:67:C4:59:AC:13:4B:26:7C:62:77:B0:5F:4F:DC:D4:97:AF:CE:E7:18:A7:69:2E:14:AD:4F:6B:81:14:52:13:86:AC:F2:E9:47:52:B7:CC:34:B2:47:64:0A:45:4F:24:AF:2F:B2:2D:90:85:CB:81:E0:D4:57:39:10:1F:C2:ED:E4:92:FC:4F:B6:FD:74:C8:C2:78:42:C1:C1:F1:76:44:BA:8C:C9:66:BE:75:86:7E:20:D4:4E:38:48:86:93:2D:9D:5D:B3:83:EF:EA:4B:52:46:B9:C7:A3:13:DF:7D:6B:81:9B:B6:54:B4:9E:89:FC:1B:79:EF:CB:24:3D:6F:09:BD:EE:AE:D7:63:5B:60:E1:00:8A:EB:2B:8E:80:6E:AC:55:D5:01:5A:0A:7A:81:CF:9B:7E:49:C5:6E:99:A7:07:D7:1E:82:E5:29:C6:A4:5D:62:BE:A5:E7:1B:06:8B:93:C0:9D:BA:3C:ED:93:18:2C:E7:5E:6E:87:41:FC:33:D8:61:50:6D:4C:E0:A9:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*
Authority Info Access	*http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0018_p0020.crl*
Subject Key Identifier	*16:66:7F:7C:4F:8A:40:15:B9:51:A8:43:58:A6:54:89:FD:A6:97:75*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D6:35:FD:21:3F:8B:16:CF:C0:7E:83:D4:73:8F:12:3D:0B:15:0A:CF:72:FF:F4:39:8D:BF:22:D6:FB:3D:26:75*

X509SubjectName

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000014*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

X509SKI

X509 SK I *FmZ/fE+KQBW5UahDWKZUif2ml3U=*

Service Status

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

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

Status Starting Time

2024-10-23T15:20:00Z

2.31 - Service (granted): EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020

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]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *268305699434924918275381070614893547343320993 08*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFIzCCBIWgAwIBAgIUBLMf1n6q1Wqs6FNul2uSl0a5OuwwCgYIKoZIzj0EAwIwgYQxCzAJBgNV
BAYTAlBUMUAwPgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXI0aWZpY2HDp8OjbyBrbGVjdHLD
s25pY2EgZG8gRXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBD
aWRhZMOjbyAwMDgwHhcNMjUxMTEyMTcxOTIwWhcNMzcxMTA5MDAwMDAwWjCBwTELMAkGA1UEBhMC
UFQxMzAxBgNVBAoMKkluc3RpdHV0byBkb3MgUmVnaXN0b3MgZSBkbyBOb3RhcmlhZG8gSS5QLjEc
MBoGA1UECwwTQ2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8xSTBHBgNV
BAMMQEVDIGRlIEFzc2luYXR1cmEgRGlnaXRhbCBRdWFsaWZpY2FkYSBkbyBDYX0wI6NvIGRlIENp
ZGFkw6NvIDAwMjAwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAASUOjSTuSBfXXVrfqY048Y7YMf0zVdM
x8jBjC7RPl4aD2NFvoGTbiG2vxosdTTqsMb8692/cfb+zMBdVKyHiPMTYH61Q3Ygh8yzOpOVziz3
UyVqN6ccWrXxxDjB3YRJ8t6jggJ3MIICczASBgNVHRMBAf8ECDAGAQH/AgEAMBBGA1UdIwQYMBaA
FKsAgCv7M0T5PfHe+d7/sXNnmWL+MIGsBggrBgEFBQcBAQSBnzCBnDBfBggrBgEFBQcwAoZTaHR0
cDovL3BraTluY2FydGFvZGVjaWRhZGFvLnB0L2VudGlkYWRlLWNlcnRpZmlj YWNhby1jYy9jZXJ0
aWZpY2Fkb3MvQ0NfUm9vdDAwOC5jcnQwOQYIKwYBBQUHMAGGLWh0dHA6Ly9vY3NwLnJvb3QucGtp
Mi5jYXJ0YW9kZWNpZGFkYW8ucHQvb2NzcDCB9AYDVR0gBIHsMIHpMDIGBFUdIAAwKjAoBggrBgEF
BQcCARYcaHR0chM6Ly93d3cuc2NlZS5nb3YucHQvcmVwLzBYBggphGwBAQECBAAHMEow5AYIKwYB
BQUHAgEWPGh0dHA6Ly9wa2kyLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL3ByYXRpY2FzLWNl
cnRpZmlj YWNhbzBZBgtghGwBAQECBAABAjBKMEgGCCsGAQUFBwIBFjxodHRwOi8vcGtpMi5jYXJ0
YW9kZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGljYS1jZXJ0aWZpY2Fkb3MwZwYDVR0fBGAwXjBc
oFqgWIZWahRDcDovL2BzaTluY2FydGFvZGVjaWRhZGFvLnB0L2VudGlkYWRlLWNlcnRpZmlj YWNh
by1jYy9saXN0YS1yZXZvZ2FjYW8vQ0NfUm9vdDAwOC5jcmwwHQYDVR0OBBYEFPkW5mG2VvCf2brG
BHm5u4qxI/GzMA4GA1UdDwEB/wQEAwIBBjAKBggghkjOPQQDAgOBiwAwgYcCQSjlit8p+WVdQpaj
HzSCDPObR8M44RmyFHiw7GavS1ER11T8ilaavxRuGkBFm+uIhccUMRL0Mj5aNuqzUzVuH2ldAkIB
5FSy5PF1pa9jOk04RKej+j8P80tHzTrTAmIdB42IKTec0e55jfR3/XzLNzNb/3bhtgNlnNBOY+pT
/yr3422wefU=
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer CN: *Cartão de Cidadão 008*

Issuer OU:	*ECEstado*
Issuer O:	*SCEE - Sistema de Certificação Electrónica do Estado*
Issuer C:	*PT*
Subject CN:	*EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Instituto dos Registos e do Notariado I.P.*
Subject C:	*PT*
Valid from:	*Wed Nov 12 18:19:20 CET 2025*
Valid to:	*Mon Nov 09 01:00:00 CET 2037*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:94:3A:34:93:B9:20:5F:5D:75:6B:7E:A6:34:E3:C6:3B:60:C7:F4:CD:57:4C:C7:C8:C1:24:2E:D1:3E:5E:1A:0F:63:45:BE:81:93:6E:21:B6:BF:1A:2C:75:34:EA:B0:C6:FC:EB:DD:BF:71:F6:FE:CC:C0:5D:54:AC:87:88:F3:13:60:7E:B5:43:76:20:87:CC:B3:3A:93:95:CE:2C:F7:53:25:6A:37:A7:1C:5A:B5:F1:C4:38:C1:DD:84:49:F2:DE*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*AB:00:80:2B:FB:33:44:F9:3D:F8:5E:F9:DE:FF:B1:73:67:99:62:FE*
Authority Info Access	*http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/certificados/CC_Root008.crt* *http://ocsp.root.pki2.cartaodecidadao.pt/ocsp*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep/* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao* *Policy OID: 2.16.620.1.1.1.2.4.0.1.2* *CPS pointer: http://pki2.cartaodecidadao.pt/publico/politica-certificados*
CRL Distribution Points	*http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/lista-revogacao/CC_Root008.crl*
Subject Key Identifier	*F9:16:E6:61:B6:56:F0:9F:D9:BA:C6:04:79:B9:BB:8A:B1:23:F1:B3*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*78:28:A5:B9:06:75:9A:62:7D:31:CB:62:8B:EF:84:77:DD:3C:7F:14:4E:09:5C:26:3B:22:BA:12:83:26:81:33*

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

X509SKI

X509 SK I *+RbmYbZW8J/ZusYEebm7irEj8bM=*

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

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

Status Starting Time *2025-11-28T12:00:00Z*

2.31.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.31.2 - Extension (not critical): Qualifiers [QCSSCDStatusAsInCert, QCForESig, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *2.16.620.1.1.1.2.10*

Description

Description

2.31.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020*

Service digital identities

X509SubjectName

Subject CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0020*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Instituto dos Registos e do Notariado I.P.*

Subject C: *PT*

X509SKI

X509 SK I *+RbmYbZW8J/ZusYEebm7irEj8bM=*

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

Status Starting Time *2025-11-28T12:00:00Z*

2.31.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

2.32 - Service (granted): Serviço de Validação Cronológica do Cartão de Cidadão 000015

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.*

Service Name

Name *[en]* *Serviço de Validação Cronológica do Cartão de Cidadão 000015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7930265231939395261*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIltjCCBp6gAwIBAgIIbg32Nkxg3r0wDQYJKoZIhvcNAQELBQAwgcExCzAJBgNVBAYTAlBUMTMw
MQYDVQQKDCpJbnNQaXR1dGBgZGQazIiIZ2lzdG9zIGUgZGBgTrn9OYXjpYWRvIEkuUC4xHDAaBgNV
BAsME0NhcnTDo28gZGUgQ2lkYWTDo28xFDASBgNVBAsMC3N1YkVDRXN0YWRvMUkwRwYDVQQDDEBF
QyBkZSBBc3NpbmF0dXJhIERpZ2I0YWwgUXVhbGlmaWNhZGEgZG8gQ2FydMOjbyBkZSBDaWRhZMOj
byAwMDE4MB4XDTI2MDQzMDE0NDEyNloXDTMyMTAzMDE0NDEyNlowgcYxCzAJBgNVBAYTAlBUMRww
GgYDVQQKDBNDYXJ0w6NvIGRlIENpZGFkw6NvMSkwJwYDVQQLDCBTZXJ2acOnb3MgZG8gQ2FydMOj
byBkZSBDaWRhZMOjbzEhMB8GA1UECwwYVmFsaWRhbw6fDo28gQ3Jvbm9sw7NnaWNhMUsw5QYDVQQD
DEJTZXJ2acOnbyBkZSBWYWxpZGHDp8OjbyBDcm9ub2zDs2dpY2EgZG8gQ2FydMOjbyBkZSBDaWRh
ZMOjbyAwMDAwMTUwggGiMA0GCSqGSib3DQEBAQUAA4IBjwAwggGKAoIBgQDCYAqqyQz2pUTfXZmq
o3uABDbd0iw4XFaGV/BJStRZBbUsF3l4LOvhO)+vM+LbpbipCIFSlex67Ik6HUERIQF5aApVZWCt
JeJs0IMm8jTBm+65Rm6fhLZqqgn4f9BfKvBWCjp6cyF6z8fCuDdf4RL3E0T3I2T0Jy91mHMZAkDm
DmCEnFEqVX4v46mpuK0HIrs+btYBqorbxBTM44ZmfV7wNdn4qivtyn/OYdw4/e9HsOcOGXPkONhA
MStQM4yk6riWj1YxpDHEL3bauHYlPKtRsHRBvaHdlJnHixAxAJUuKnz3FM16xkL4yB4SLo5/MmVQ
S3dm9LGKLsMQCy6vK80ldqm0+n9dwRfj69A4OJxB+Kex3YiFlmaYdt8bpJKGbC1El1zJzlpHc45
O4tC4trM5Or05TSDDJyUze46vEnUXEbQHMj/zLRPSWP8/77IEZZJ5/2c0J4V22Zg7BKvQMSPOPc
+99gp140PBCtznFQoRS7bPh44XAMMNeumISrhqsCAwEAAaOCAykwggMIMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUEwS8y2v/UhhAVV4fPDJhHkQgvRUwSwYIKwYBBQUHAQEEPzA9MDsGCCsGAQUF
BzABhi9odHRwOi8vb2NzcC5hc2MuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY2Bvb2NzcDBvBgNV
HS4EaDBmMGSgYqBghl5odHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL2xyYy9j
Y19zdWltZWNfY2lkYWRhb19hc3NpbmF0dXJhX2NybDAwMThfZGVsdGFfcDAwMjAuY3JsMIG6BgNV
HSAEgbIwga8wVQYLYlRsAQEBAgQAAQcwRjBEBggrBgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFv
ZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2FzL2NwLmh0bWwwVgYLYlRsAQEBAgQBAAcwRzBF
BggrBgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRp
Y2FzL2Nwcy5odG1sMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMIHGBggrBgEFBQcBAw5BuTCBtjCB
swYHBACBl14BAQyBp0j5lGluY2x1c2lvbiBvZiB0aGlzIHN0YXRlbWVudCB0aGUgaXNzdWVyIGNs
YWltcy B0aGF0IHRoaXMgdGltZS1zdGFtcCB0b2tlbiBpcyBpc3N1ZWQgYXMgYSBxdWFsaWZpZWQg
ZWxlY3Ryb25pYy B0aW1lLXN0YW1wIGFjY29yZGluZy B0byB0aGUgIkVHVUxBVEIPTAoRVUpIE5v
IDkxMC8yMDE0MGkGA1UdHwRiMGAwXqBcoFqGWGh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHljL2NjX3N1Yi1IY19jaWRhZGFvX2Fzc2luYXR1cmFtY3JsMDAxOF9wMDAyMC5j
cmwwHQYDVR0OBBYEFKgHkwPClmqov29m4MLSEbebjEDHMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG
9w0BAQsFAAOCAgEAmLxMgyav9D+2UmUX9K9Ta8CacSD/ZRE8ENH4zm+qPwF2P2NWXg9mOYJaS0+C
B36dowWfChoRmBD4iAEBcYSj5MV/jc+oi1KuZvLLTiRu+FB3gOEtla7+F5fu2ObaV3Kq/ngmNa/M
HPjnU/kvU/nj32E4xp4q35tpS4VmdDHmPQlbJLo9EL9N/0j+6AzdUGZrqklDYKo08R0654sG1/aM
4V24RKsSWZHa5yLeWtF2CLZD0VaY8WhLrLx/QPCGJ9of03HtcZohpV3Fv+o4BERA666OefbwR79X
MNUjQAKORThj6ik+Tk1FTomLz597HcHlnAlYLYwntA1x3mMjV+bKsiG5c+vlAx+hwz/ROfa7gY3y
k0qNlCtet3lc1WEc3v9+Om+R9wubVUt9LUE+o8dttDS64TCFZ6HybcW2OU5jnWAeUiyB24WAg
rGz5v1ixTeaVS2cUzbV4qG9RiKRPL6fMSFvfmDbQUX2ulhIn88enpvKXfZTqan46iToKAZV6KUrt
wXVcfWfGGOQcGiuWSOtzvsByp MlhDQojAvPx/m5sciT75AKV4I9ThRooQXkj+ouhXzqpfGNp62Cp
bsbgKgWB8y26WI3lixBwq78Pl5/odw6N0sQrjevdRbOstZHMvi/33tG/pptM7cU3FBnJhEqnDkyT
7QfArP87LFR96Q8=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *EC de Assinatura Digital Qualificada do Cartão de Cidadão 0018*

Issuer OU: *subECEstado*

Issuer OU: *Cartão de Cidadão*

Issuer O: *Instituto dos Registos e do Notariado I.P.*

Issuer C: *PT*

Subject CN: *Serviço de Validação Cronológica do Cartão de Cidadão 000015*

Subject OU: *Validação Cronológica*

Subject OU: *Serviços do Cartão de Cidadão*

Subject O: *Cartão de Cidadão*

Subject C: *PT*

Valid from: *Thu Apr 30 16:41:26 CEST 2026*

Valid to: *Sat Oct 30 16:41:26 CEST 2032*

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:C2:60:0A:AA:C9:0C:F6:A5:44:DF:5D:99:AA:A3:7B:80:04:36:DD:D2:2C:38:5
C:56:86:57:F0:49:4A:D4:59:05:B5:2C:17:72:38:2C:E8:E1:3A:3F:AF:33:E2:DB:A5:B8:A9:08:81:52:95:EC:7A:EF:59:3A:1D:41:11:95:01:79:68:0A:55:65:60:AD:25:E2:6C:D2:23:26:F2:34:
FC:98:EE:B9:46:6E:9F:84:BD:AA:AA:09:F8:7F:D0:5F:2A:FF:16:70:9A:7A:73:21:7A:CF:C7:C2:BB:37:45:E1:12:F7:12:84:F7:23:64:F4:27:2F:75:98:73:19:02:40:E6:0E:60:84:9C:51:2A:55:
7E:2F:E3:A9:A9:B8:AD:07:22:BB:3E:6E:D6:01:AA:8A:DB:C4:14:CC:E3:86:66:7D:5E:F0:35:D9:F8:AA:2B:ED:CA:7F:CE:61:DC:38:FD:EF:47:B0:E7:0E:19:73:E4:38:D8:40:31:2B:50:33:8C:
A4:EA:B8:96:8F:56:31:A4:31:C4:2F:76:DA:B8:76:25:3C:AB:51:B0:74:41:BD:A1:DD:94:99:C7:8B:10:31:00:95:2E:2A:7C:F7:14:CD:7A:C6:42:F8:C8:1E:12:2E:8E:7F:32:65:50:4B:77:66:F
4:81:8A:2E:C3:10:0B:2E:AF:2B:CD:08:76:A9:B4:FA:7F:5D:C1:17:E3:EB:DD:C0:E0:E2:71:07:E2:9E:C7:76:22:16:59:9A:61:DB:7C:6E:92:4A:19:B0:B5:12:5D:73:27:32:69:1D:CE:39:3B:8B
:42:E2:DA:CC:48:EA:F4:E5:3B:03:0F:25:33:7B:8E:AF:12:75:17:11:B4:07:32:3C:FF:CC:B4:4F:49:63:FC:FF:BE:E5:13:F6:59:8D:2F:F6:73:42:78:57:6D:99:83:B0:4A:BD:03:12:3C:E3:DC:FB
:DF:60:A7:5E:34:3C:10:AD:CE:71:50:A1:14:BB:6C:F8:78:E1:70:0C:30:D7:AE:9A:54:AB:86:AB:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *13:04:BC:CB:6B:FF:52:18:40:55:5E:1F:3C:32:61:1E:44:2A:BD:15*

Authority Info Access *http://ocsp.asc.cartaodecidadao.pt/publico/ocsp*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.16.620.1.1.1.2.4.1.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl0018_p0020.crl*
Subject Key Identifier	*A8:07:93:03:C2:96:6A:A8:BF:6F:66:E0:C2:D2:11:B7:9B:8C:40:C7*
Key Usage:	*digitalSignature*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1D:51:EE:D5:89:B9:29:33:93:70:4D:5E:0D:D1:73:2F:D1:27:EA:97:DD:1B:0A:97:ED:6A:EF:25:13:6B:AC:17*

X509SubjectName

Subject CN:	*Serviço de Validação Cronológica do Cartão de Cidadão 000015*
Subject OU:	*Validação Cronológica*
Subject OU:	*Serviços do Cartão de Cidadão*
Subject O:	*Cartão de Cidadão*
Subject C:	*PT*

X509SKI

X509 SK I	*qAeTA8KWaqi/b2bgwtIRt5uMQMc=*

Service Status

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

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

Status Starting Time

2026-05-06T17:30:00Z

3 - TSP: Justica

.

TSP Name

Name	*[en]*	*Justica*
Name	*[pt]*	*Justica*

TSP Trade Name

Name	*[en]*	*ECM Justiça - Ministry of Justice Certification Service Provider (national PKI - SCEE)*
Name	*[pt]*	*ECM Justiça - Entidade Certificadora do Ministério da Justiça (PKI nacional - SCEE)*
Name	*[en]*	*VATPT-510361242*
Name	*[en]*	*SCEE*

PostalAddress

Street Address	*[en]*	*Av. D. João II, n.º 1.08.01E, Torre H, Piso 17*
Locality	*[en]*	*Lisboa*
State Or Province	*[en]*	*Lisboa*
Postal Code	*[en]*	*1990-097 LISBOA*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Av. D. João II, n.º 1.08.01E, Torre H, Piso 17*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1990-097 LISBOA*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:pki@igfej.mj.pt*
URI	*[en]*	*http://icp.igfej.mj.pt*

TSP Information URI

URI *[en]* *http://icp.igfej.mj.pt*

3.1 - Service (withdrawn): ECM Justica (CA-Qualified Certificates)

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]* *ECM Justica (CA-Qualified Certificates)*

Name *[pt]* *ECM Justica (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4858866416297404952*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGxTCCBK2gAwIBAgIIQ24pQyJ7ahgwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xMjAwBgNVBAMMKU1VTFRJQ0VSVCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE4MDcxMDEwMzAzOVoXDTE5MDEwNzEwMzAzOVowQTELMAkGA1UEBhMCUFQxDTALBgNV
BAoMBFNDRUUxETAPBgNVBAsMCEVDRXN0YWRvMRAwDgYDVQQDDAdKdXN0aWNhMIICIjANBgkghkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEAr5bP3YChchO77DDEuF72kLUGUU4QUiQnjnjaFadAWtGVDEuZ
OE5rrO19wgz497fc4DgQX8a9tPR6aJlm8mgfoZcq4jEhHNofQPrLI3p8wk+3lSizzHZpDop02nC9
xFqAEx4bP4bs2D2rwEtgx9im7vMM0E9uxFNRL3Lbry/QUoKOndZvwIUzy2E43pL1/6DUj9OxQH5o
KU7nd/Q6v+2idF+fy+ubhS3GePPv8TKLmrhKUi6XdrefvY5Y9NRLueONREgVIHo1GaWlCngqsXtB
Y1+2ycApT2jtV87JqmWbEZf1zlanxGecANdwyqmCScRdLmzUES14ERfQkaW4M2/sbxroj6gcAwB
y/FQuPLh5jYxA/81sOOtmN/ldQe7ZxlNq4OXBg32kyXTxix9Vtxyt2ivp9gDtVNizw3LipbifVyR
0qk+REpMzw8D4x2mr56vBw/wgPuty9gHPg3S2KyBGL957Ka+uZ8+jV+S3lkOuWjHZWal6CcDQnRP
pNs2fVC/s6HFnzjX2/dJx05vfPRxOuGmwP+mtEUKaAh5bCNW1oOu50rc5d+yRtSjeuBLQjCz50Ks
h9gBlSZZnp6kmTouL6Oa/OGEsbnxogOTUUUjGVHueOWzoooOQ9hSnnJQQIl5DxwsALhC70tiQYKIB
GZi9wzuPb9po+Esg0B+ovkQdoDUCAwEAAaOCAXowggF2MDoGCCsGAQUFBwEBBC4wLDAqBggrBgEF
BQcwAYYeaHR0cDovL29ic3AubXVsdGljZXJ0LmNvbS9vY3NwMB0GA1UdDgQWBBS9qDlNK0PVu6Vz
/VjtX6kK3eawCzAS8gNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNU5HJxbbwSqopVM7yDd
KXSkxUVxMIGQBgNVHSAEgYgwgYUwPAYNKwYBBAGBw24BAQEABzArMCkGCCsGAQUFBwIBFh1odHRw
Oi8vcGtpcm9vdC5tdWx0aWNlcnQuY29tLzA9Bg4rBgEEAYHDbgEBAQABAjArMCkGCCsGAQUFBwIB
Fh1odHRwOi8vcGtpcm9vdC5tdWx0aWNlcnQuY29tLzAGBgRVHSAAMEEGA1UdHwQ6MDgwNqA0oDKG
MGh0dHA6Ly9wa2lyb290Lm11bHRpY2VydC5jb20vY3JsL3Jvb3RfbWNfY3JsLmNybDAOBgNVHQ8B
Af8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAA5BEZIhVfrayCj849aoWuAKGfmf8RBRRYtKT0Eq
EyDAgHSXpwZojtV+sWLYAvJawj4qsoozQMCFf8TbrxoBRr6VnS8dxbLRc+YuekDNgoZtnnRBXewF
fgdcSptLy2pkWqld/Vt9UGxGa83TiWjMvyRjmUbUfPxQqgViC3v3Sp43xfX2cLL7MgDsePquExjt
kn6zyI/lIBuVW44F1kTdwEZOmWznwzLe0zGNbdll+sngOTGbOabJLyshr/p+MJrOn2Y9hc4WeRel
of5bbYpDwvGRTSTXpN56Da/fo4uH089OV9OtwETpUUnthvHlB1D3e5OEf5KFyUpOf9XejizWlR3c
1nDxMWzPo3Zf9w2v1B5b7KNj6cFb9gojOZhoypPUdN6pSFvfM3FUow89ppPQgSv1iT4smAZsiCw
RM4sGqcw7jlp5r28XwfrAQy1b2P36b6yk0N68GF4pDQRXVJebtghRWAil2qJbWxN1PvGP+uMZUvA
WbW3wJfl0NkGNFCYXCixfENaTtacqt2YmfEJkMtxdawVcDIWFDWxifNxgRmr6+8WTMAxnmzzuxeE
Q4hCms0Il8z4J/G5v48fOlzg0Pdp62Rqbeu09Ux3Q95C8RCXd9L/1zC8kVH+4EKXGNTW20EC/izV
3tZNJKPRlSzA3ZwuY3xbZfVYt7uUdXXLAzmZ

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

Valid from: *Tue Jul 10 12:30:39 CEST 2018*

Valid to: *Mon Jan 07 11:30:39 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:AF:96:CF:DD:80:A1:72:13:BB:EC:30:C4:B8:5E:F6:90:B5:06:51:4E:10:52:24:27:8E:78:DA:15:A7:40:5A:D1:95:0C:4B:99:38:4E:6B:AC:ED:7D:C2:0C:F8:F7:BB:5C:E0:38:10:5F:C6:BD:B4:F4:7A:68:92:66:F2:68:1F:A1:97:2A:E2:31:21:1C:DA:1F:40:FA:CB:97:7A:7C:C2:4F:B7:21:28:B3:CC:76:69:0E:8A:74:DA:70:BD:C4:5A:80:13:1E:1B:3F:86:EC:D8:3C:EB:C0:4B:60:C7:D8:A6:EE:F3:0C:A0:4F:6E:C4:53:51:2F:72:DB:AF:2F:D0:52:82:8E:9D:D6:6F:C0:85:33:CB:61:38:DE:92:F5:FF:A0:D4:8F:D3:B1:40:7E:6B:29:4E:E7:77:F4:3A:BF:ED:A2:74:5F:9F:CB:EB:9B:85:2D:C6:78:F1:6F:F1:32:8B:9A:B8:4A:52:2E:97:76:B7:9F:BF:2E:58:F4:D3:CB:B9:E3:8D:44:48:15:94:7A:35:19:A5:88:0A:78:2A:B1:78:41:60:8F:B6:C9:C0:29:4F:68:ED:57:CE:C9:AA:65:9B:11:97:F5:CC:86:A7:C4:67:9C:00:D7:70:CA:A9:82:49:C4:5D:2E:29:B3:50:44:B5:E0:44:5F:42:46:96:E0:CD:BF:B1:BC:6B:A2:3E:A0:70:0C:01:CB:F1:50:B8:F2:E1:E4:96:31:03:FF:35:B0:E3:AD:98:DF:E5:75:07:BB:67:12:0D:AB:83:97:06:0D:F6:93:25:D3:C6:2C:7D:56:DC:72:B7:6B:AF:A7:D8:03:B5:53:62:CF:0D:CB:8A:96:E2:7D:5C:91:D2:A9:3E:44:4A:4C:CF:0F:03:E3:1D:A6:AF:9E:AF:07:0F:F0:80:FB:AD:CB:D8:07:3E:0D:D2:D8:AC:81:18:BF:79:EC:A6:BE:B9:9F:3E:25:5F:92:DC:89:0E:B9:68:C7:65:66:88:E8:27:03:42:74:4F:A4:DB:19:7D:50:BF:B3:A1:C5:9F:38:D7:DB:F7:49:C7:4E:6F:7C:F4:71:3A:E1:A6:C0:FF:A6:B4:45:0A:68:08:79:6C:23:56:D6:83:AE:E7:4A:DC:E5:DF:B2:46:D4:A3:7A:E0:4B:42:30:B3:E7:42:AC:87:D8:01:95:26:59:9E:9E:A4:99:3A:2E:B4:BE:8E:6B:F3:86:12:C6:E7:C6:88:0E:4D:45:23:19:51:EE:78:E5:B3:A2:8A:10:F6:14:A7:9C:94:10:8A:5E:43:C7:0B:00:2E:10:BB:A2:D8:90:62:49:41:19:98:BD:C3:3B:8F:6F:DA:68:F8:4B:20:D0:1F:A8:BE:44:1D:A0:35:02:03:01:00:01

Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *BD:A8:32:0D:2B:43:D5:BB:A5:73:FD:58:ED:5F:A9:0A:DD:E6:B0:0B*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: http://pkiroot.multicert.com/

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2

CPS pointer: http://pkiroot.multicert.com/

Policy OID: 2.5.29.32.0

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B8:2E:02:6F:2D:33:18:8E:3D:CA:77:AE:95:80:B3:7C:F1:59:2B:F8:8F:8A:1C:FF:05:5F:B3:3A:86:FA:EB:64*

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *vagyDStD1bulc/1Y7V+pCt3msAs=*

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

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

Status Starting Time *2019-06-23T23:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

3.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

3.1.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECM Justica (CA-Qualified Certificates)*

Name *[pt]* *ECM Justica (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *vagyDStD1bulc/1Y7V+pCt3msAs=*

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

Status Starting Time *2018-07-10T23:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

3.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

3.1.4 - History instance n.2 - Status: granted

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

Service Name

Name *[en]* *ECM Justica (CA-Qualified Certificates)*

Name *[pt]* *ECM Justica (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *vagyDStD1bulc/1Y7V+pCt3msAs=*

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

Status Starting Time *2018-02-09T00:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

3.1.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

3.1.5 - History instance n.3 - Status: withdrawn

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

Service Name

Name *[en]* *ECM Justica (CA-Qualified Certificates)*

Name *[pt]* *ECM Justica (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *vagyDStD1bulc/1Y7V+pCt3msAs=*

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

Status Starting Time *2018-02-09T00:00:00Z*

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

3.1.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

3.1.6 - History instance n.4 - Status: granted

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

Service Name

Name *[en]* *ECM Justica (CA-Qualified Certificates)*

Name *[pt]* *ECM Justica (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *vagyDStD1bulc/1Y7V+pCt3msAs=*

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

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

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

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.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

3.1.6.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

4 - TSP: ECAR

.

TSP Name

Name	*[en]*	*ECAR*
Name	*[pt]*	*ECAR*

TSP Trade Name

Name	*[en]*	*ECAR - Assembly of the Republic Certification Service Provider (national PKI - SCEE)*
Name	*[pt]*	*ECAR - Entidade certificadora da Assembleia da Republica (PKI nacional - SCEE)*
Name	*[en]*	*VATPT-600054128*
Name	*[en]*	*SCEE*

PostalAddress

Street Address	*[en]*	*Palácio de S. Bento*
Locality	*[en]*	*Lisboa*
State Or Province	*[en]*	*Lisboa*
Postal Code	*[en]*	*1249-068 Lisboa*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Palácio de S. Bento*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1249-068 Lisboa*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:ecar.correio@ar.parlamento.pt*
URI	*[en]*	*http://www.ecar.parlamento.pt/*

TSP Information URI

URI *[en]* *http://www.ecar.parlamento.pt/*

4.1 - Service (withdrawn): ECAR (CA-Qualified Certificates)

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]* *ECAR (CA-Qualified Certificates)*

Name *[pt]* *ECAR (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *153011951768217544694210381804578517321*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGDDCCA/SgAwIBAgIQcx0HrIEQg8JHWTP7DzOxSTANBgkqhkiG9w0BAQUFADAzMQswCQYDVQQG
EwJQVDENMAsGA1UECgwEU0NFRTEVMBMGA1UEAwwMRUNSYWl6RXN0YWRvMB4XDTA3MTIwNzExNTly
N1oXDTE5MTIwNzExNTlyN1owPjELMAkGA1UEBhMCUFQxDTALBgNVBAoTBFNDRUUxETAPBgNVBAsT
CEVDRXN0YWRvMQ0wCwYDVQQDEwRFQ0FSMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
5yQtzGup+79ilU7TPh3IAP65FPzjIDBcUrqadqQLxaf4B5GpV2TI0K+E7E1E2I1fvci9DC/lsaaZ
CxJu097FQkBjWoTnY/Gxf/4QyMTLiGf7oELWrbQA2jVkRd74IDbnPyX2+kh78c7hAuhLbbC5tLP2
S0DoKYXsevGPmXb+jLPmZCbIbEurU0j9zqPSretvDeRo/tZISGO0gTyA0wPuHP1jrIffmsNFoLEu
jBd5g3i7oYbS3wxkC2UaCVqwn7ejxuiy5Plr25j3rRANxPpcidLCaRIgc5eTiPF1DBo8QZq1Nczj
EuU6It9KsmwEEDVedyOfcNZLKT0gmuNYm95vZdEd3AGNr4CFKZ4DnZ2Obx2cIe7Zb28nK7oOHzsM
JcNjtym56tcZVCzxq/48Bsre04fYuZrDmWUfzW0zVdzKIKfsZlmWWZgfADnDuVUrzQMXxVYYLeUh
aXPo9GsjOmf2KQWV0pHtw1uBKB9MmMfqkCHiAjg90HDK0YqEx6BAdvfRRf13VRNODz1FsKksp3zD
o53LHnnqDLrkKp8Mb7q75yfcbJBES1RJ80qw7LGknoe15DTHYTco8rpYru9Y9wkwjrvuIXrMQfIc
aKeO52C2o6GEresivWdpyJchdrg8tZyZThZBOZde3B2UT6GMQbpsoGi3Iu4Ls2GT4IEyYD7f1W8C
AwEAAaOCAQ8wggELMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFG7nJTv4CDK2dnC0LK2RZKIJ
Lgf+MB8GA1UdIwQYMBaAFHF/Nd71d3FtHRKc4ZCkuvCpg4+AMA4GA1UdDwEB/wQEAwIBBjA7BgNV
HSAENDAyMDAGBFUdIAAwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5lY2VlLmdvdi5wdC9kcGMw
NAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwczovL29jc3AuZWNlZS5nb3YucHQwNQYD
VR0fBC4wLDAqoCigJoYkaHR0cDovL2NybHMuZWNlZS5nb3YucHQvY3jscy9BUkwuY3JsMA0GCSqG
SIb3DQEBBQUAA4ICAQArApE4PrW821MVsgta+J3FzpeHYXBpve0uasGXg0YpzOwnQX+I8tTQJDge
xopRqjznFCU9PelZuZpvEJGOmJrBLgp3tEgcg6YCM2kiEmEW5+4GrSfpyvYGZlsFSzQ0nKWe00iT
CWWHYc1dIpe87gHXSfqzcULU2xfLt0Rhjdo6kavC2V/UPAO9HinPEUUi1NBzrT3aIVOjYVhNReoR
80NbaKhcXRcGDDKU02kueh50WrNRrIUlm7Q8NWyl416C68DzlW5LovBMreQQZyknMkPUVjrgY4AK
8RX+8O+Bv0z1mMx3Ipd1j5kj412ioPqOw+4D4Z6Dr76Vqq/O8EBlSFuSRA8Y+jgsHHnq9zBzoAqr
b5ocGwP1A7DCofIXA915YOkh0wRAOi1Ka9iuwb//ijp785LB7HjwMGLOZa8ox4URdlnJK4vNvgdG
8n4/qCY1J9DmdcYKH3O6stvvt4IU6m+N3qeVM26t0yg+o5Pja9fDkp6Jl//cBH/D+RozDcruIQtj
4wZLRK2lWe5B+qSwYFD+x+bgte8r0u7Uy3W8JuGsh5L6+07lIMap61ZdaNW8KVsqAoAgiLGdR58tE
O33AhL2EPHbRja7dhZ0l5BuEetgDpnphk5DbGiLV7Frmg6cq9mUR++BzfVUfw9/T+fVAoHbW7q8O
2eo0CxHvPKha7AbzdA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ECRaizEstado*

Issuer O: *SCEE*

Issuer C: *PT*

Subject CN: *ECAR*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

Valid from: *Fri Dec 07 12:52:27 CET 2007*

Valid to: *Sat Dec 07 12:52:27 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:E7:24:08:CC:6B:A9:FB:BF:62:53:B4:CF:87:79:40:3F:AE:45:3F:38:C8:0C:17:22:52:BA:9A:76:A4:0B:C5:A7:F8:07:91:A0:57:64:C8:38:AF:84:EC:4D:44:D8:9D:5F:BD:C8:BD:0C:2F:C8:B1:A6:B6:0B:12:6E:D3:DE:C5:42:40:63:5A:84:E7:63:F1:B1:7F:FE:10:C8:C4:CB:88:67:FB:A0:42:D6:AD:B4:00:DA:35:64:45:DE:F8:94:36:E7:3F:25:F6:FA:48:7B:F1:CE:E1:02:E8:4B:6D:B0:B9:B4:B3:F6:4B:40:E8:29:85:EC:7A:F1:8F:99:76:FE:8C:B3:E6:64:26:C8:6C:4B:AB:53:48:FD:CE:A3:D2:AD:EB:6F:0D:E4:68:FE:D6:48:48:63:B4:A9:3C:80:D3:03:EE:1C:FD:63:AC:87:DF:9A:C3:45:A0:B1:2E:8C:17:79:AB:78:BB:A1:86:D2:DF:0C:64:0B:65:1A:09:5A:B0:9F:B7:A3:C6:E8:B2:E4:F2:2B:D8:98:F7:AD:10:0D:C4:FA:5C:89:D2:C2:69:12:20:71:27:93:88:F1:75:0C:1A:3C:41:9A:B5:35:CC:E3:12:E5:3A:96:DF:4A:B2:6C:04:10:35:5E:77:23:9F:70:D6:4B:29:3D:20:9A:E3:58:9B:DE:6F:65:D1:1D:DC:01:BD:AF:80:85:29:9E:03:9D:9D:8E:B7:1D:9C:21:EE:D9:6F:6F:27:2B:BA:0E:1F:3B:0C:25:C3:63:B7:29:B9:EA:D7:19:54:2C:F1:83:FE:3C:06:CA:DE:D3:87:D8:BB:6A:C3:99:65:1F:CD:6D:33:55:DC:CA:20:A7:EC:64:99:96:59:98:1F:00:39:C3:B9:55:2B:CD:03:17:C5:56:18:2D:E5:21:69:73:E8:F4:6B:23:3A:67:F6:29:05:95:D2:91:ED:C3:5B:81:28:1F:4C:98:C7:EA:90:21:E2:02:38:3D:D0:70:CA:D1:8A:84:C7:A0:40:76:F7:D1:45:FD:77:55:13:4E:0F:3D:45:B0:A9:2C:A7:7C:C3:A3:9D:CB:1E:79:EA:0C:BA:E4:2A:9F:0C:6F:BA:BB:E7:27:DC:6C:90:44:4B:54:49:F3:4A:B0:EC:B1:A4:9E:87:B5:E4:34:C7:61:37:28:F2:BA:58:AE:EF:58:F7:09:30:8E:BB:EE:95:7A:CC:41:F9:5C:68:A7:8E:E7:60:B6:A3:A1:84:AD:EB:22:BD:67:69:C8:97:21:76:B8:3C:B5:9C:99:4E:16:41:39:97:5E:DC:1D:94:4F:A1:8C:41:BA:6C:A0:68:B7:22:EE:0B:B3:61:93:E0:81:32:60:3E:DF:D5:6F:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *6E:E7:25:3B:F8:08:32:B6:76:70:B4:2C:AD:91:64:A2:09:2E:07:FE*

Authority Key Identifier *71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.ecee.gov.pt/dpc

Authority Info Access *https://ocsp.ecee.gov.pt*

CRL Distribution Points *http://crls.ecee.gov.pt/crls/ARL.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E3:C1:8F:CB:5D:6A:F9:F2:2E:04:38:D9:24:10:33:6D:C8:4E:85:03:02:9D:BD:61:E8:34:C5:6A:EA:97:A6:26*

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

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

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

Scheme Service Definition URI

URI *[en]* *http://www.ecar.parlamento.pt/*

URI *[pt]* *http://www.ecar.parlamento.pt/*

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

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

4.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

4.1.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *ECAR (CA-Qualified Certificates)*

Name *[pt]* *ECAR (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *ECAR*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

X509SKI

X509 SK I *buclO/gIMrZ2cLQsrZFkogkuB/4=*

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

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.620.1.1.1.2.10*

4.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

4.1.4 - History instance n.2 - Status: accredited

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

Service Name

Name [en] ECAR (CA-Qualified Certificates)

Name [pt] ECAR (EC-Certificados Qualificados)

Service digital identities

X509SubjectName

Subject CN: ECAR

Subject OU: ECEstado

Subject O: SCEE

Subject C: PT

X509SKI

X509 SK I buclO/gIMrZ2cLQsrZFkogkuB/4=

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

Status Starting Time 2007-12-08T00:00:00Z

4.1.4.3 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier 2.16.620.1.1.1.2.10

5 - TSP: MULTICERT - Serviços de Certificação Electrónica S.A.

.

TSP Name

Name	*[en]*	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Name	*[pt]*	*MULTICERT - Serviços de Certificação Electrónica S.A.*

TSP Trade Name

Name	*[en]*	*MULTICERT S.A.*
Name	*[pt]*	*MULTICERT S.A.*
Name	*[en]*	*VATPT-505767457*

PostalAddress

Street Address	*[en]*	*Alfrapark, Edifício E Estrada de Alfragide, nº 67*
Locality	*[en]*	*Amadora*
Postal Code	*[en]*	*2610-008*
Country Name	*[en]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:info@multicert.com*
URI	*[en]*	*https://pki.multicert.com/index.html*

TSP Information URI

URI	*[en]*	*https://pki.multicert.com/index.html*

5.1 - Service (withdrawn): Multicert 001 (CA-Qualified Certificates)

.

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]*	*Multicert 001 (CA-Qualified Certificates)*
Name	*[pt]*	*Multicert 001 (EC-Certificados Qualificados)*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *120033008*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFkjCCBHqgAwIBAgIEByeO8DANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJjRTESMBAGA1UE
ChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYDVQQDExlCYWx0aW1vcmUgQ3li
ZX(UcnVzdCBSb290MB4XDTEzMDczMTE5MjMwNloXDTIwMDUyOTE5MjE0OFowgbcxC2AIBgNVBAYT
AlBUMUIwQAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6rDo28gRWxl
Y3Ryw7NuaWNhIFMuQ54xLzAtBgNVBAsMJkVudGlkYWRlIGRlIENlcnRpZmljYcOnw6NvIENyZWRl
bmNpYWRhMTMwMQYDVQQDDCpNVUxUSUNFUlQgLSBFbnRpZGFkZSBkZSBDZXJ0aWZpY2HDp8OjbyAw
MDEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCVBakRYT1dfNnFVQZ4O3k9Vc90fm0Y
Pf09sf8tpiXmrFGAzD3iFXUxiZbfULI0+xjAw8ia7qd8J7V/B1y0F/cK1rscyD/xxN3Sqy/9p5f1
HKy4/vq6J5gaI+LbarQOJE16/1PtjX9FaCfGccZa7dc8Run0FmEwmqp5b8nZNdyfLgyB2SOWCquC
UJpgP18JgU1LvwTcYsdkaBajMPlslG0Fzf3wRTSX17ACbj5Hc5QuReFAfuEDlqO2oBJlIlc2vqA
3jw7PdzVdh8n8WlXfrLb9oCsfhBFfj49Ct68pafeugrnejoCOBE5+pYhI+Gzyfupg6OYEG92QLra
uSe7AW23GLtkxoBNmIrzAIDXZnNxRB5CgmnWBfwNBCdfX85xqr8tarvf9JZEKVpMV/eQ+2muZKIC
cJFdUnRNnW/0SESBqO3jsCwvqxtPVqK/89NAjkb7ttBzUzHbQ2e/vzHUqgzfsN3iz0YF1WfhEerv
PaXBqsGDYRitVcg/nAaQrWHS4616NXhWQg1HEiFoshMzuIuInYNqu8eHscG52TndIFPc5GtgCxCn
3HjxORa3aXRSCsb4IljcQRbiOraqUUzyWLnk61EIsdYixmP/KzeFtzAoXtg6SjYFS3k8iFwaF/K
qIxU02DJuR7IGW4knWngdvnbT5KU7SV2xzxgDxX7vwfupQIDAQABo4IBADCB/TA5BgNVHRMBAf8E
CDAGAQH/AgEBMFMGA1UdIARMMEowSAYJKwYBBAGxPgEAMDswOQYIKwYBBQUHAgEWLWh0dHA6Ly9j
eWJlcnRydXN0Lm9tbmlyb290LmNvbS9yZXBvc2lOb3J5LmNmbTAOBgNVHQ8BAf8EBAMCAQYwHwYD
VR0jBBgwFoAU5ZJZMjfHWMys+ghUNoZ7OrUETfAwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2Nk
cDEucHVibGlqLXRydXN0LmNvbS9DUkwvT21uaXJvb3OyMDI1LmNybDAdBgNVHQ4EFgQUfzNyf0za
NMgOp3XLLoOYGwa4ppAwDQYJKoZIhvcNAQEFBQADggEBAAatUQlI2YtFFRbXSYx7rG+99GkMAuo
s8utQkDkTQAIPRs+Bn5ez2Nug0FzrMbaXsK1jXyTvJLb9QgIlvpfMLiDuNSkqENQ599rZng7IzQg
bU89u44zkUL/2B+BMKno0NuKEdG29xv5oB2Oxrz8ux9j9WKal24+yrqkO1edDu1IK0X9lu8QuV7G
wj4KYWu/19uLfsO+BqmHu0Y1G1HMaA6AZZLBHZX8yJ2GOPGZPlQEkLpR2c+A4yr8nrVe1MPt2l4
WxmncEf5A2969wbJLXHCsqeYuRG1A1VNDFpd/xiIJV60Ga/oA3TUrVbAvwD6CwUR6BIlvIteMVq5r
2xxdHGw=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Baltimore CyberTrust Root*

Issuer OU: *CyberTrust*

Issuer O: *Baltimore*

Issuer C: *IE*

Subject CN: *MULTICERT - Entidade de Certificação 001*

Subject OU: *Entidade de Certificação Credenciada*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Wed Jul 31 21:23:06 CEST 2013*

Valid to: *Fri May 29 21:21:48 CEST 2020*

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:02:82:02:01:00:95:F1:A9:11:61:3D:5D:7C:D9:C5:55:06:78:3B:79:3D:55:CF:74:7E:6D:18:3D
:F3:BD:81:FF:2D:A6:25:E6:AC:51:80:CC:3D:E2:15:75:31:89:96:DF:50:B9:74:FB:18:C0:C3:C8:9A:EE:A7:7C:27:B5:7F:07:5C:B4:17:F7:0A:D6:BB:1C:C8:3F:F1:C4:DD:D2:AB:2F:FD:A7:97:
F5:1C:AC:B8:FE:FA:BA:27:98:1A:23:E2:DB:6A:B4:0E:24:4D:7A:FF:53:ED:8D:7F:45:68:27:C6:71:C6:5A:ED:D7:3C:46:E9:F4:16:61:30:9A:AA:79:6F:C9:D9:35:DC:9F:2E:0C:81:D9:23:96:0
A:AB:82:50:9A:60:3F:5F:09:81:4D:4B:BF:04:DC:62:C7:64:6A:E0:5A:8C:C3:C8:B2:51:B4:17:37:F7:C1:14:D2:5F:5E:C0:09:B8:F9:1D:CE:50:B9:17:85:01:FB:84:0E:5A:8E:DA:80:49:96:22:
1C:DA:FA:80:DC:9C:3B:3D:DC:D5:76:1F:27:F1:62:17:7E:B2:DB:F6:80:AC:7E:10:45:14:9E:3D:0A:DE:BC:A5:A7:DE:BA:0A:E7:7A:3A:1C:38:11:39:FA:96:21:23:E1:B3:CA:1B:A9:1B:A3:98:
10:6F:76:40:BA:DA:B9:27:BB:01:6D:B7:18:BB:64:C6:80:4D:98:8A:F3:00:80:D7:66:73:71:44:1E:42:82:69:D6:05:FC:0D:04:27:5F:5F:C4:B1:AA:B0:6D:6A:BB:C5:F4:96:44:29:5A:4C:57:F
7:90:FB:69:AE:64:A2:02:70:91:5D:52:74:4D:9D:6F:F4:48:44:81:A8:ED:E3:B0:2C:2F:AB:18:4F:56:A2:BF:F3:D3:40:8E:46:FB:B6:D0:73:53:31:DB:43:67:BF:BF:31:D4:AA:0C:DF:B0:DD:E2
:CF:46:05:D5:67:E1:11:EA:EF:3D:A5:C1:AA:C1:83:61:18:AD:55:C8:3F:9C:06:90:AD:61:D2:E3:AD:7A:35:78:56:42:0D:47:12:21:68:B2:13:33:BA:5B:88:9D:83:6A:BB:C7:87:B1:C1:B9:D9:
39:DD:94:53:DC:E4:6B:60:0B:10:A7:DC:78:F1:D1:16:B7:69:74:52:0A:C6:F8:94:88:DC:41:16:E2:94:EA:DA:A9:45:33:C9:62:E7:93:AD:44:22:C7:58:8B:19:8F:FC:AC:DE:16:DC:C0:A1:7B:
60:E9:28:D8:15:2D:E4:F2:21:70:68:5F:CA:82:5C:54:D3:60:C9:B9:1E:E5:19:6E:24:9D:69:E0:E2:F9:DB:4F:92:94:ED:25:76:C7:3C:60:0F:15:FB:BF:07:EE:A5:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 1*

Certificate Policies *Policy OID: 1.3.6.1.4.1.6334.1.0*

CPS pointer: http://cybertrust.omniroot.com/repository.cfm

Authority Key Identifier *E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0*

CRL Distribution Points

http://cdp1.public-trust.com/CRL/Omniroot2025.crl

Subject Key Identifier

7F:33:72:7F:4C:DA:34:C8:0E:A7:75:CB:2E:83:98:1B:06:B8:A6:90

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

CB:E0:12:82:26:7B:9E:E5:E0:0D:33:70:A3:3A:E8:67:56:49:CD:DE:1D:70:B4:9F:10:B8:31:FA:D6:E0:21:90

Certificate fields details

Version:

3

Serial Number:

919343176892588118 9

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHADCCBOigAwIBAgIf5WhfCWeQ2UwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xMjAwBgNVBAMMKU1VTFRlQ0VSVCBSb29lENlcnRpZmlj YXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE2MTEyOTE3NTEwOFoXDTIwMTEyODE3NTEwOFowgbcxC2AJBgNVBAYTAlBUMUIwQAYD
VQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNh
IFMuQS4xLzAtBgNVBAsMJkVudGlkYWRlIGRlIENlcnRpZmlj YcOnw6NvIENyZWRlbmNpYWRfMTMw
MQYDVQQDDCpNVUxUSUNFUlQgLSBFbnRpZGFkZSBkZSBDZX0aWZpY2HDp8Ojby4wMDEwggIlMA0G
CSgGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCV8akRYT1dfNnFVQZ4O3k9Vc90fm0YPfO9sf8tpiXm
rFGAzD3iFXUxiZbfULl0+xjAw8ia7qd8j7V/B1y0F/cK1rscyD/xxN3Sqy/9p5f1HKy4/vq6j5ga
I+LbarOOjE16/1PfjX9FaCfGccZa7dc8Run0FmEwmqp5b8nZNdyfLgyB2SOWCquCUJpgP18JgU1L
vwTcYsdkauBajMFlsIc0Fzf3wRT5XJ7ACbj5Hc5QuReFAfuEDIqQ2o8JlIc2vqA3Jw7RdzVdhBn
8WIXfrLb9oCsfhBFFJ49Ct68pafeugrmejocOBE5+pYhl+GzyhupG6OYEG92QLrauSe7AW23GLtk
xoBNmlrzAIDXZnNxRB5CgmnWBfwNBCdfX8SxqrBtarvF9JZEKVpMV/eQ+2muZKICcJFdUnRNnW/0
SE5BqO3jsCwvqxtPvqK/89NAjkb7ttBzUzHbQ2e/vzHUggzfsN3iz0YF1WfhEervPaXBqsGDYRit
Vcg/nAaOrWH54616NXhWQg1HEiFoshMzuIuInYNguBeHscG52TndIFPc5GtgCxCn3HjxORa3aXRS
Csb4IIjcQRbilOraqUUzyWLnk61EIsdYixmP/KzeFtzAoXtg6SjYFS3k8iFwaF/KgIxU02DJuR7l
GW4knWng4vnbT5KU7SV2xzxgDxX7vwfupQIDAQABo4IBPjCCATowOgYIKwYBBQUHAQEELjAsMCoG
CCsGAQUFBzABhh5odHRwOi8vb2NzcC5tdWx0aWNlcnQuY29tL29jc3AwHQYDVR0OBBYEFHBzcn9M
2jTIDqd1yy6Dm8sGuKaQMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAU1TkcnFtvBKqi
lUzvlN0pdKTFRXEwVQYDVR0gBE4wTDBKBg0rBgEEAYHDbgEBAQAHMDkwNwYIKwYBBQUHAgEWK2h0
dHA6Ly9wa2lyb290Lm11bHRpY2VydC5jbZ0vcG9sL2luZGV4Lmh0bWwwQQYDVR0fBDowODA2oDSg
MoYwaHR0cDovL3BraXJvb3QubXVsdGljZXJ0LmNvbS9jcmwvcm9vdF9tY19jcmwuY3JsMA4GA1Ud
DwEB/wQEAwIBBjANBgkghkiG9w0BAQsFAAOCAgEAIyiu4XwaaopV7JWHytYA+uZghYMGU9ZN0if1
A6XAu6XZ25gzpYvGWBiPzE7Ym T4hiRjSgA0EfoOJK7nyMialitO9FbN5HeYGaXi5uzd6tHjCgYm
PXJ/wssz9+IfTszE6ib4BSlnGL0BTj3m6eQSuNpxGlyXjAPdg/LITjg8QFbCmAauXct6NmBrJAmZ
yEaPiIWCRg0ZJDNe2PjdlxorpGy9Eo4EV0ujo5a9yFgyJSj/EmMSiRZp+tf66Pc9B5ntWi7vD4cu
LGP5t7lSdXcmdLMtq8kWxwFLkoca0xphDAREnr2VznwNCPykeTMA2ifktgnOzFZV3H7v2bpKuc+
EIW9GrWbjn83AIWFMW8iWPQ/RR9yi4OzRmqlbLxM1cPT6eTZ5vVWdd r34cKbJURq4WncVBRyFcunA
NtQ6aHc8hxWSm2iBWov4FCb56j+x5x1c4Zskl4HKqyjEu1S+K1RVFT+9MLA4Vu4IDjSUH8UWHXc
Dji6P3zYFzLnxpFd3/lg8QNOixmd4B4KmaPhZWBvcg7/QsEsklkmWDBsgtkWiofXo/OghQFHm7QH
4RjVyYrOCE0CzgAK791V7InUbc4v1mvbTsadenCYaR43L3YbdwDNoONOSUavOqOPrN45MQZMwliz
Rcwj23cMNKo53/axtMg0XPkxOiXqmGztR+O4DG4=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

MULTICERT Root Certification Authority 01

Issuer O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Issuer C:

PT

Subject CN:

MULTICERT - Entidade de Certificação 001

Subject OU:

Entidade de Certificação Credenciada

Subject O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Subject C:

PT

Valid from:

Tue Nov 29 18:51:08 CET 2016

Valid to:

Sat Nov 28 18:51:08 CET 2020

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:02:82:02:01:00:95:F1:A9:11:61:3D:5D:7C:D9:C5:55:06:78:3B:79:3D:55:CF:74:7E:6D:18:3D
:F3:8D:81:FF:2D:A6:25:E6:AC:51:80:CC:3D:E2:15:75:31:89:96:DF:50:B9:74:FB:18:C0:C3:C8:9A:EE:A7:7C:27:B5:7F:07:5C:84:17:F7:0A:D6:BB:1C:C8:3F:F1:C4:DD:D2:AB:2F:FD:A7:97:
F5:1C:AC:B8:FE:FA:BA:27:98:1A:23:E2:DB:6A:B4:0E:24:4D:7A:FF:53:ED:8D:7F:45:68:27:C6:71:C6:5A:ED:D7:3C:46:E9:F4:16:61:30:9A:AA:79:6F:C9:D9:35:DC:9F:2E:0C:81:D9:23:96:0
A:AB:82:50:9A:60:3F:5F:09:81:4D:4B:BF:04:DC:62:C7:64:6A:E0:5A:8C:C3:C8:B2:51:B4:17:37:F7:C1:14:D2:5F:5E:C0:09:B8:F9:1D:CE:50:B9:17:85:01:FB:84:0E:5A:8E:DA:80:49:96:22:
1C:DA:FA:80:DC:9C:3B:3D:DC:D5:76:1F:27:F1:62:17:7E:B2:DB:F6:80:AC:7E:10:45:14:9E:3D:0A:DE:BC:A5:A7:DE:BA:0A:E7:7A:3A:1C:38:11:39:FA:96:21:23:E1:B3:CA:1B:A9:1B:A3:98:
10:6F:76:40:BA:DA:B9:27:BB:01:6D:B7:18:BB:64:C6:80:4D:98:BA:F3:00:80:D7:66:73:71:44:1E:42:82:69:D6:05:FC:0D:04:27:5F:5F:C4:B1:AA:B0:6D:6A:BB:C5:F4:96:44:29:5A:4C:57:F
7:90:FB:69:AE:64:A2:02:70:91:5D:52:74:4D:9D:6F:F4:48:44:81:A8:ED:E3:B0:2C:2F:AB:1B:4F:56:A2:BF:F3:D3:40:8E:46:FB:B6:D0:73:53:31:DB:43:67:BF:BF:31:D4:AA:0C:DF:B0:DD:E2
:CF:46:05:D5:67:E1:11:EA:EF:3D:A5:C1:AA:C1:83:61:18:AD:55:C8:3F:9C:06:90:AD:61:D2:E3:AD:7A:35:78:56:42:0D:47:12:21:68:B2:13:33:BA:5B:88:9D:83:6A:BB:C7:87:B1:C1:B9:D9:
39:DD:94:53:DC:E4:6B:60:0B:10:A7:DC:78:F1:D1:16:B7:69:74:52:0A:C6:F8:94:88:DC:41:16:E2:94:EA:DA:A9:45:33:C9:62:E7:93:AD:44:22:C7:58:8B:19:8F:FC:AC:DE:16:DC:C0:A1:7B:
60:E9:28:D8:15:2D:E4:F2:21:70:68:5F:CA:82:5C:54:D3:60:C9:B9:1E:E5:19:6E:24:9D:69:E0:E2:F9:DB:4F:92:94:ED:25:76:C7:3C:60:0F:15:FB:BF:07:EE:A5:02:03:01:00:01
```

Authority Info Access	*http://ocsp.multicert.com/ocsp*
Subject Key Identifier	*7F:33:72:7F:4C:DA:34:C8:0E:A7:75:CB:2E:83:98:1B:06:B8:A6:90*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7* *CPS pointer: http://pkiroot.multicert.com/pol/index.html*
CRL Distribution Points	*http://pkiroot.multicert.com/crl/root_mc_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*4A:13:D7:ED:E3:19:1D:32:FD:A0:FF:BB:6C:06:7F:11:90:50:E1:54:2F:D0:71:5F:10:E7:9E:26:91:42:1A:EF*

Service Status

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

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

Status Starting Time

2020-11-09T00:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://pki.multicert.com*
URI	*[pt]*	*https://pki.multicert.com*

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

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

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

5.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.1.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Multicert 001 (CA-Qualified Certificates)*

Name *[pt]* *Multicert 001 (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT - Entidade de Certificação 001*

Subject OU: *Entidade de Certificação Credenciada*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *fzNyf0zaNMgOp3XLLoOYGwa4ppA=*

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

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

5.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.1.4 - History instance n.2 - Status: accredited

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

Service Name

Name *[en]* *Multicert 001 BTM(CA-Qualified Certificates)*

Name *[pt]* *Multicert 001 BTM(EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT - Entidade de Certificação 001*

Subject OU: *Entidade de Certificação Credenciada*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *fzNyf0zaNMgOp3XLLoOYGwa4ppA=*

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

Status Starting Time *2014-03-01T00:00:01Z*

5.1.4.3 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

5.2 - Service (withdrawn): Multicert 002 (CA-Qualified Certificates)

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]* *Multicert 002 (CA-Qualified Certificates)*

Name *[pt]* *Multicert 002 (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *120041007*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFzjCCBLagAwIBAgIEByeuLzANBgkghkiG9w0BAQsFADBaMQswCQYDVQQGEwJlRTESMBAGA1UE
ChMJQmFsdGltb3JlIMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYDVQQDExlCYWx0aW1vcmUgQ3li
ZXJUcnVzdCBSb290MB4XDTE0MDUxNDE5NTQ1MloXDTI1MDUxMjIzNTkwMFowga4xCzAJBgNVBAYT
AlBUMUIwQAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxl
Y3Ryw7NuaWNhIFMuQS4xKzApBgNVBAsMIkFjY3JlZGl0ZWQgQ2VydGlmaWNhdGlvbiBBdXRob3Ij
dHkxLjAsBgNVBAMMJU1VTFRJQ0VSVCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAwMDIwggIiMA0G
CSqG5Ib3DQEBAQUAA4ICDwAwggIKAoICAQC7Q5cdo8k6aBayWG9KSO20RGzASJLUPNqdH8+tpCsw
IRWArZHqohavns5OhEBARn4MUZ5+jYmBYC8mq+xE0PATIKPCrsISRlNj5i8WL+u5/C6RpFnyDejyD
ntA7UO4iFucK20xFrckFotQHU6XfmYOYtfvE3ls1GPMrEz+/Gc6aABdajD81Vgrkq2p1C0R4mbe5
EG/Zl3L5nnG6tnwna6CLZjruPW4GtAC340GQCpp+ByPO27ImgbnK7s3Um9Qi2dosfyIdkvtFXgS5
Fx9TcYYyJoYVEd5hs43Z4OrCirFad4hUiidEqETMV7oB35C8q7HgTeqJ6ovOevo73pAFdfB415vl
NS95L5iW5JYE+Z5km3WrBGGX1YA8MQ7zGCv2IMVEgbBeY1tdS8LqLKk6hbVgh8tcNXqZu99JNGNE
9ifdpdnn0v5kzNk+2cv+gxhOr3VxiOCejBQC074vYwDP+PXtfr8UtrsryFZO6FzajvBEEF5YsL
rWXI5/uHFjrv9hLz6+gLx7XXjFVxEqm95S17DnQUOOFCHo72gijLCLjYQM57WSXwjP1Nw/lgbyo0
nReSviFA/bzXExOe7ek/Ya+/P126LtFhs5i8ZhJwrd3xstdRYmEM8jfWuhfNxur5a2sxATUErbHb
idL/YbhTKjr1WKysxDdiMc3K3vCFWapNtwIDAQABo4IBRTCCAUEwEgYDVR0TAQH/BAgwBgEB/wIB
ATBTBgNVHSAETDBKMEgGCCsGAQQBsT4BADA7MDkGCCsGAQUFBwIBFi1odHRwOi8vY3liZXJ0cnVz
dC5vbW5pcm9vdC5jb20vcmVwb3NpdG9yeS5jZm0wQgYIKwYBBQUHAQEENjA0MDIGCCsGAQUFBzAB
hiZodHRwOi8vb2Nzcc5vbW5pcm9vdC5jb20vYmFsdGltb3Jlcm9vdDAOBgNVHQ8BAf8EBAMCAQYw
HwYDVR0jBBgwFoAU5Z1ZMIJHWMys+ghUNoZ7OrUETfAwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDov
L2NkcDEucHVibGljLXRydXN0LmNvb59DUkwvT21uaXJvb3QyMDI1LmNybDAdBgNVHQ4EFgQULPTO
Al54AFqcQ9bjIzejaNn5E8wDQYJKoZIhvcNAQELBQADggEBAETpDTyT+0laN+E5QDleYNCjioxv
OLqx5Wms0T3zlV0Cho0ZtIlrD+aSZVHKrCi7sXmgLMLmgxIpyziPbUzqVI98z3lGmNtxZ5rYrFdk
dnkvhod/+gJ7Yrz0AkonWeTJszLEmRDiPIECq9EmE7Mida3Hc2ObGFxekTBkM8pPPuAHb8RC57fw
gaKJTk0Xuww4AHjfUEaHQ29yNn29v6a12qOuQgyQWfvrh+eZacH2cQea8nJ3mlaK5039VfvgUel4
xgbzDaK4k6FArzj04N/RsFvLr296why9u1pAVyZ6+DMtTK/0W4anAcApiMUbDoDQrSAcNWKONStj
QnCe0YXf9/o=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Baltimore CyberTrust Root*

Issuer OU: *CyberTrust*

Issuer O: *Baltimore*

Issuer C: *IE*

Subject CN: *MULTICERT Certification Authority 002*

Subject OU: *Accredited Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Wed May 14 21:54:52 CEST 2014*

Valid to: *Tue May 13 01:59:00 CEST 2025*

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:BB:43:97:1D:A3:C9:3A:68:16:B2:58:6F:4A:48:ED:B4:44:6C:C0:48:92:D4:3C
:DA:9D:1F:CF:AD:A4:2B:30:21:15:80:AD:91:EA:A2:16:AF:9E:CE:50:84:40:40:46:7E:0C:53:6E:7E:25:89:81:60:2F:26:AB:EC:44:D0:F0:13:20:A3:C2:AE:C2:12:44:D2:79:8B:C5:8B:FA:EE:7
F:0B:A4:69:16:7C:83:78:9C:83:9E:D0:3B:50:EE:22:16:E7:0A:CF:4C:45:AD:C9:05:A2:D4:07:53:A5:DF:99:83:98:B5:FB:C4:DC:8B:35:18:F3:2B:13:3F:BF:19:CE:9A:00:17:5A:8C:3F:35:56:
0A:E4:AB:6A:75:0B:44:78:99:B7:B9:10:6F:D9:97:72:F9:9E:71:BA:B6:7C:27:6B:A0:8B:66:3A:EE:3D:6E:06:B4:00:B7:E3:41:90:0A:9A:7E:07:23:CE:DB:B9:66:81:B9:CA:EE:CD:D4:9B:D4:2
2:D9:DA:2C:7F:22:1D:92:FB:45:5E:04:B9:17:1F:53:71:86:32:26:86:15:11:DE:61:B3:8D:D9:E0:EA:C2:8A:B1:5A:77:88:54:22:27:44:A8:44:CC:57:BA:01:DF:90:BC:AB:B1:E0:4D:EA:89:EA
:8B:CE:7A:FA:3B:DE:90:05:75:F0:78:D7:9B:E5:35:2F:79:2F:98:96:E4:96:04:F9:9E:64:9B:75:AB:04:61:97:D5:80:3C:31:0E:F3:18:2B:F6:20:C5:44:A9:B0:5E:63:5B:5D:4B:C2:EA:2C:A9:3
A:B5:B5:60:87:CB:5C:35:7A:99:BB:DF:49:34:63:44:F6:27:DD:A5:D9:E7:D2:FE:65:93:33:64:FB:67:2F:FA:0C:61:3A:BD:D5:C6:23:82:78:90:50:08:4E:F8:BD:8C:03:3F:E3:D7:B5:FA:FC:52:
DA:EC:AF:21:5F:64:EE:B5:CD:A2:6F:04:41:05:49:8B:08:AD:65:C8:E7:FB:87:14:9A:EF:F6:12:F3:EB:E8:0B:C7:B5:D7:8C:55:71:12:A9:BD:E5:2D:78:0E:74:14:38:E1:42:1E:8E:F6:82:22:4B
:08:B8:D8:40:CE:7B:59:25:F0:8C:FD:4D:C3:F9:60:6F:2A:34:9D:17:92:BE:21:40:FD:BC:D7:13:13:9E:ED:E9:3F:61:AF:BF:3F:5D:BA:2E:D1:61:B3:98:BC:66:12:70:AD:DD:F1:B2:D7:51:62:
61:0C:F2:37:D6:BA:17:CD:C6:EA:F9:6B:6B:31:01:35:04:AD:B1:DB:89:D2:FF:61:B8:53:28:9A:F5:58:AC:AC:C4:37:62:31:CD:CA:DE:F0:85:59:AA:4D:B7:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 1*

Certificate Policies

Policy OID: 1.3.6.1.4.1.6334.1.0

CPS pointer: http://cybertrust.omniroot.com/repository.cfm

Authority Info Access

http://ocsp.omniroot.com/baltimoreroot

Authority Key Identifier

E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

CRL Distribution Points

http://cdp1.public-trust.com/CRL/Omniroot2025.crl

Subject Key Identifier

2C:F4:CE:00:8E:78:00:5A:AA:71:0F:5B:8E:5C:DE:8D:A3:67:E4:4F

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

1F:06:4C:55:C8:14:C8:B6:EA:77:7A:84:22:16:CA:C8:FE:35:AC:70:A8:7D:8C:DF:5 5:BC:2D:80:28:E8:D0:09

Certificate fields details

Version:

3

Serial Number:

3555021600213451201

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIG9zCCBN+gAwIBAgIIMVX5T2GQQcEwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xMjAwBgNVBAMMKU1VTFRJQ0V5VCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE0MDUyMTE0MzMwNloXDTI1MDkxOTE0MzMwNlowga4xCzAJBgNVBAYTAlBUMUIwQAYD
VQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNh
lFMuQS4xKzApBgNVBAsMIkFjY3JlZGl0ZWQgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxLjAsBgNV
BAMMJU1VTFRJQ0VSVCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAwMDIwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC7Q5cdo8k6aBayWG9KSO20RGzA5JLUPNqdH8+tpCswIRWArZHqohav
ns5QhEBARn4MUD5+jYmBYC8mq++xEOPATIKPCrsISRNJ5i8WL+u5/C6RpFnyDejyDntA7UO4iFucK
z0xFrckFotQHU6XfmYOYtfvE3Is1GPMrEz+/Gc6aABdajD81Vgrkq2p1C0R4mbe5EG/Zl3L5nnG6
tnwna6CLZjruPW4GtAC340GQCpp+ByPO27lmgbnK7s3Um9Qi2dosfyIdkvtFXgS5Fx9TcYYyJoYV
Ed5hs43Z4OrCirFad4hUIidEqETMV7oB35C8g7HgTeqJ6ovOevo73pAFdfB415viNS95L5iW5jYE
+Z5km3WrBGGX1YA8MQ7zGCv2IMVEqbBe1Itd58LqLKk6hbVghBtchNXqZu9I9JNGNE9ifdpdnn0v5I
kzNk+2cv+gxhOr3VxIOCejBQC074vYwDP+PXtfr8UtrsryfTZO6FzajvBEEFSYsLrWXI5/uHFjrv
9hLz6+gLx7XXjFVxEqm95S17DnQUOOFCHo72gijLCLjYQM57WSXwjP1Nw/lgbyo0nReSvIFA/bzX
ExOe7ek/Ya+/P126LtFhs5i82hJwrd3xstdRYmEM8jfWuhfNxur5a2sxATUErbHbidL/YbhTKJr1
WKysxDdiMc3K3vCFWapNtwIDAQABo4IBPjCCATowQgYIKwYBBQUHAQEEIjAsMCoGCCsGAQUFBzAB
hh5odHRwOi8vb2NzcC5tdWx0aWNlcnQuY29tL29jc3AwHQYDVR0OBBYEFCz0zgCOeABaqnEPW45c
3o2jZ+RPMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAU1TkcnFtvBKqiUzvlN0pdKTF
RXEwVQYDVR0gBE4wTDBKBg0rBgEEAYHDbgEBAQAHMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly9wa2ly
b290Lm11bHRpY2VydC5jb20vcG9sL2luZGV4Lmh0bWwwQQYDVR0fBDowODA2oDSgMoYwaHR0cDov
L3BraXlvb3QubXVsdGljZXJ0LmNvb59jcmwvcm9vdF9tY19jcmwuY3jsMA4GA1UdDwEB/wQEAwIB
BjANBgkqhkiG9w0BAQsFAAOCAgEAA/B1g7OfjhlTwetJU48eTd2WzlaWmK26K7ajQnz84QTSB9CK
UQKjldmOzP4P3gHJGl0ikNXb0d6U3ntGfvvIdCM+hdoT9n0TjPm6CkwxcXHtxnc8Wp1BHdA5MnTb
99gtvFGe6UojO+jYBg6cEAmbRdJkzC3DSL0I13vDinIEVvR7VPDUzsxSWfbW7azlSO77eIK89NAi
7GDqDbtrmVyUXqU3QMP0I+28RVHu/Ebki+ijbW//fR8MkG0HMDJdXzHGyA2A89m9ptAASa3jr7WPx
IZKBB2f4ZNKfgIXJOZs15qzuQvXoiGo8IWKU/jk2GuWxf38b9soENLkA0yrt3++t+2S5SKdDR5jBb
3d6BngaYyfo1LIEx13qPL+lkXTlUbhUu2FWG2Mi1fYNph7FCzF8NfguGpEAp0RYjnKA6YLhleIT6
cUWamgsUuZX/1OWDxDsh6esUTPTCIUFmFBEeiBP8EoF8afqny6QUShrdIp5vbs1pVoEdLSQFQ1Pv
0L1ENwiLX1rjcBn1ZlvyXx5G0rYTC5tOfqPcWruU3Yeaigh Y48eN0Ut9d36RdjmOmIL51Ax+/mX
52MFGxlP7D5Gf3dWV8MsKFlRdiQWi3Bl+2hL0A8cVFC4IKJZa9MP96phevft1xVoHRU8HlxG+P04
Jug7VAREVi+sD60etzDHGJk8Inc=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

MULTICERT Root Certification Authority 01

Issuer O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Issuer C:

PT

Subject CN:

MULTICERT Certification Authority 002

Subject OU:

Accredited Certification Authority

Subject O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Subject C:

PT

Valid from: *Wed May 21 16:33:06 CEST 2014*

Valid to: *Fri Sep 19 16:33:06 CEST 2025*

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:BB:43:97:1D:A3:C9:3A:68:16:B2:58:6F:4A:48:ED:B4:44:6C:C0:48:92:D4:3C:DA:9D:1F:CF:AD:A4:2B:30:21:15:80:AD:91:EA:A2:16:AF:9E:CE:50:84:40:40:46:7E:0C:53:6E:7E:25:89:B1:60:2F:26:AB:EC:44:D0:F0:13:20:A3:C2:AE:C2:12:44:D2:79:8B:C5:88:FA:EE:7F:0B:A4:69:16:7C:83:78:9C:83:9E:D0:3B:50:EE:22:16:E7:0A:CF:4C:45:AD:C9:05:A2:D4:07:53:A5:DF:99:83:98:B5:FB:C4:DC:8B:35:18:F3:2B:13:3F:BF:19:CE:9A:00:17:5A:8C:3F:35:56:0A:E4:AB:6A:75:0B:44:78:99:B7:B9:10:6F:D9:97:72:F9:9E:71:BA:B6:7C:27:6B:A0:8B:66:3A:EE:3D:6E:06:B4:00:B7:E3:41:90:0A:9A:7E:07:23:CE:DB:B9:66:81:B9:CA:EE:CD:D4:9B:D4:22:D9:DA:2C:7F:22:1D:92:FB:45:5E:04:B9:17:1F:53:71:86:32:26:86:15:11:DE:61:B3:8D:D9:E0:EA:C2:8A:B1:5A:77:88:54:22:27:44:A8:44:CC:57:BA:01:DF:90:BC:AB:B1:E0:4D:EA:89:EA:8B:CE:7A:FA:3B:DE:90:05:75:F0:78:D7:9B:E5:35:2F:79:2F:98:96:E4:96:04:F9:9E:64:9B:75:AB:04:61:97:D5:80:3C:31:0E:F3:18:2B:F6:20:C5:44:A9:B0:5E:63:58:5D:4B:C2:EA:2C:A9:3A:85:B5:60:87:CB:5C:35:7A:99:BB:DF:49:34:63:44:F6:27:DD:A5:D9:E7:D2:FE:65:93:33:64:FB:67:2F:FA:0C:61:3A:BD:D5:C6:23:82:78:90:50:0B:4E:F8:BD:8C:03:3F:E3:D7:B5:FA:FC:52:DA:EC:AF:21:5F:64:EE:85:CD:A2:6F:04:41:05:49:8B:0B:AD:65:C8:E7:FB:87:14:9A:EF:F6:12:F3:EB:E8:0B:C7:B5:D7:8C:55:71:12:A9:BD:E5:2D:7B:0E:74:14:38:E1:42:1E:8E:F6:82:22:4B:08:B8:D8:40:CE:7B:59:25:F0:8C:FD:4D:C3:F9:60:6F:2A:34:9D:17:92:BE:21:40:FD:BC:D7:13:13:9E:ED:E9:3F:61:AF:BF:3F:5D:BA:2E:D1:61:83:98:BC:66:12:70:AD:DD:F1:B2:D7:51:62:61:0C:F2:37:D6:BA:17:CD:C6:EA:F9:6B:6B:31:01:35:04:AD:B1:DB:89:D2:FF:61:B8:53:28:9A:F5:58:AC:AC:C4:37:62:31:CD:CA:DE:F0:85:59:AA:4D:B7:02:03:01:00:01

Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *2C:F4:CE:00:8E:78:00:5A:AA:71:0F:5B:8E:5C:DE:8D:A3:67:E4:4F*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies *Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7*

CPS pointer: http://pkiroot.multicert.com/pol/index.html

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *91:4A:87:BD:B2:B3:5F:73:AE:F7:C2:13:30:9A:23:09:21:CD:18:2C:56:68:A6:B5:C4:BE:9B:FF:6A:1C:03:B3*

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

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

Status Starting Time *2022-06-14T10:01:29Z*

Scheme Service Definition URI

URI *[en]* *https://pki.multicert.com*

URI *[pt]* *https://pki.multicert.com*

5.2.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert, QCStatement, QCForESig, QCQSCDManagedOnBehalf, QCForESeal]

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

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

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 *[en]* *Multicert 002 (CA-Qualified Certificates)*

Name *[pt]* *Multicert 002 (EC-Certificados Qualificados)*

Service Digital Identity

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

Status Starting Time *2019-08-05T23:00:00Z*

5.2.3.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert, QCStatement, QCForESig, QCQSCDManagedOnBehalf, QCForESeal]

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

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

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: granted

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

Service Name

Name *[en]* *Multicert 002 (CA-Qualified Certificates)*

Name *[pt]* *Multicert 002 (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Certification Authority 002*

Subject OU: *Accredited Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *LPTOAI54AFqqcQ9bjlzejaNn5E8=*

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

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

5.2.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.2.5 - History instance n.3 - Status: accredited

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

Service Name

Name *[en]* *Multicert 002 BTM(CA-Qualified Certificates)*

Name *[pt]* *Multicert 002 BTM(EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Certification Authority 002*

Subject OU: *Accredited Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *LPTOAI54AFqqcQ9bjlzejaNn5E8=*

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

Status Starting Time *2014-05-14T00:00:01Z*

5.2.5.5 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *1.3.6.1.4.1.25070.1.1.1.1.0.1.2*

5.3 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *196908454547477761*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHbzCCBVegAwIBAgIIG1OX9ep22QEwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xKjAoBgNVBAsMIU1VTFRjQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNDA3MzAxMzMyMTJaFw0yMTAxMjkxMzMyMTJaMGS3M0swCQYDVQQGEwJQVDFCMEAGA1UE
CgwSTVVMVEIDRVJUICOgU2VydmnDp29zIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOzbmljYSBT
LkEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDMxNDAy
BgNVBAMMK01VTFRjQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3JpdHkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEcaBo1aYkW9p/C6cFmmVdIFAp8c32zowlWGHTa0Tk
Y/KleOqnaLKS9mh+3ZVqzfy0qlxb4Tzcq5uDqWgsVXRAtHZ6d88PZ9LQdJmE2NfBviMZmt8C9
PeUFwyjZEjqZI7CBCeeU+rOxePbvGZHHG8RwP8I4mwhvCNQuGc+A5NWOjf8+Nt/+JoxvzhYzxMsl
7B/6S7748hvrEJEDSv8YW35WETSEWhwPc4nTabfeErdq9OJGRrxc+Y7NSSRMosZtjUyzpQanYFUO
l/lUHj+C+9vBEq4NJl18vhoQ+5k4YDqsbwytw/1929wx9r+q0VCrSagPoOYzlzcjLUd9tY/JAgMB
AAGjggI0MIICcDAbBggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY2NwLm11bHRp
Y2VydC5jb20vb2NzcDAdBgNVHQ4EFgQUu0zWZ3OkWGstj4CjjViDjX9S+CMwDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqlwAFTrjCPR+Mc0XCBiTI5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdHM0cGtpLm1bHRpY2VydC5jb20vY3JsL2NybF9tdHNjYTAwMV9kZWx0YS5jcmwwggEuBgNV
HSAEggEIMIIBTCB0gYPKwYBBAGBw24BAQEcAAEBMIG+MIG7BggrBgEFBQcCAjCBrgyBq0NlcnRp
ZmljYWRvIGVtaXRpZG8gZGUgYWNvcmRvIGNvbSBhIFBvbMOtdGljYSBkZSBDZXJ0aWZpY2Fkb3Mg
ZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFjYy9yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUg
UG9saWN5IGluIGh0dHA6Ly90czRwa2kubXVsdGljZXj0LmNvbS9wb2wvaW5kZXguaHRtbDBKBg4r
BgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIBFjpodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb20v
cG9sL2luZGV4Lmh0bWwwQOYDVR0fBDowODA2oDSgMoYwaHR0cDovL3RzNHBra5StdWx0aWNlcnQu
Y29tL2NybC9jcmxfbXRzY2EwMDEuY3JsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggr
BgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEAiTiPdzRyXTR/mxA2FIlhwmdihP+EahUSdvcHpI6A
FlyMyDkv7Ikyco72YW4W7XxONy99avcBLE5mqY4E8yc8cv5zHgpUi/TKd1TIj6LDlh51Ew+DaPTU
c1cbdO27YXfIQAoUe9xkZzhQVs9sLCfWAXnbFCLq/oNSW/qqWlIlDnsZlqUZzl6TdcAdypy0c12T
2ubmC134qWl6CSeDJ1JI0UXErdcYUNpt/KSvamLRvdX3bdsJRk5/A6cN0l9YOycJGYHvfV6O2Afg
93PO/dA6zEUEpJ1NQPr2tjzIwkupBRINNERbcD5TtyZDvHuPeGPPiZNNyPn9ufpKi/u0v8KBhHsm
cwNhr8fhibMbNr9j+PjMCEpn2/i3ouocdzbG67w2oFXyzEnZMjkOM6xFjk4NgsO3szwowdEsdP9j
5AuaVqgsFF5y99Aq2gxHTkU7cXyocebmWhXAxIDEQOvqFqIMo+LruPdJ3uaxcqK5kkxVqZpty/HW
uDUPee1PR6z3NxFXGKVmf0WRh2cycjLFr884BHd0ztHkd2RyEAltzrKLcdShYaqt4giXRDcixShc
Y3bQNgCGONzmxTBOSk6XYgKC5ti3pETzG573lDbt1ub1cmAAWpxywv+2DjHaeYd3kWg44Vi6PBdS
X7Fi36Ettb6fzU7LIU0MBnSUpgGLDNwgDKU=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000003*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Wed Jul 30 15:32:12 CEST 2014*

Valid to: *Fri Jan 29 14:32:12 CET 2021*

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:C4:71:A0:68:D5:A6:24:5B:DA:7F:0B:A7:05:9A:65:5D:94:50:29:F1:CD:F6:CE
:8C:25:58:61:D3:6B:44:E4:63:F2:88:78:EA:A7:68:B2:92:F6:6F:E1:FB:76:55:AB:3C:DF:CB:4A:A5:C5:BE:3B:CD:CA:82:E6:E0:EA:5A:0B:15:5D:10:2D:1D:9E:9D:F3:C3:D9:F4:B4:1D:26:61:
36:35:F0:6F:88:C6:66:B7:C0:BD:3D:E5:05:C3:28:D9:12:3A:99:97:B0:81:09:E7:94:FA:B3:B1:78:FE:AF:19:91:C7:1B:C4:70:3F:C2:38:9B:08:6F:08:D4:2E:19:CF:80:E4:D5:8E:8D:FF:3E:36
:DF:FE:26:8C:6F:CE:16:33:C4:CB:25:EC:1F:FA:4B:BE:F8:F2:1B:EB:10:91:03:4A:FF:18:58:7E:56:11:34:84:5A:1C:0F:73:89:D3:69:B7:DE:12:B7:6A:F4:E2:46:46:BC:5C:F9:8E:CD:49:24:4C
:A2:C6:6D:8D:4C:B3:A5:06:A7:60:55:0E:97:F9:54:1E:3F:82:FB:DB:C1:12:AE:0D:26:5D:7C:BE:1A:10:FB:99:38:60:3A:AC:6F:0C:AD:C3:FD:7D:DB:DC:31:F6:BF:AA:D1:50:AB:49:AA:8F:A0
:E6:33:23:37:23:2D:47:7D:B5:8F:C9:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *BB:4C:D6:67:73:A4:58:6B:2D:27:80:A3:8D:58:83:8D:7F:52:F8:23*

Basic Constraints *IsCA: false*

Authority Key Identifier *9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*

Certificate Policies *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1*

CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]

Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7

CPS pointer: http://ts4pki.multicert.com/pol/index.html

CRL Distribution Points *http://ts4pki.multicert.com/crl/crl_mtsca001.crl*

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *34:26:EC:3C:07:80:65:D7:5A:72:93:80:21:94:0C:1E:3F:54:AD:F6:A4:C4:1D:87:1C:18:93:D0:28:A9:35:40*

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

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

Status Starting Time *2021-02-24T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://ts4pki.multicert.com/pol/index.html*

URI *[pt]* *http://ts4pki.multicert.com/pol/index.html*

5.3.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000003*

Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*u0zWZ3OkWGstJ4CjjViDjX9S+CM=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

5.3.2 - History instance n.2 - Status: withdrawn

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

Service Name

Name	*[en]*	*MULTICERT Qualified Time Stamping Authority*
Name	*[pt]*	*Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000003*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*u0zWZ3OkWGstJ4CjjViDjX9S+CM=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Status Starting Time	*2016-06-30T22:00:00Z*

5.3.3 - History instance n.3 - Status: undersupervision

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000003*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *u0zWZ3OkWGstJ4CjjViDjX9S+CM=*

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

Status Starting Time *2014-09-24T00:00:01Z*

5.4 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3351623168285604190*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHbzCCBVegAwIBAgIILoNbg46h+V4wDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDNVLUSUNFUlQgLSBTZXQ2acOnb3MgZGUgQ2VydGlmaWNlIw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xKjAoBgNVBAsMIU1VTFRlQ0VSVCBUCnVzdCBTZXQ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNDEwMzAxMDUzMjdaFw0yMTA1MDExMDUzMjdaMIG5MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TUVMVEIDRVJUICOgU2VydmnIDp29zIGRlIENlcnRpZmlj Yzcnw6NvIEVsZWN0csOzbmlj YSBT
LkEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDQxNDAy
BgNVBAMMK01VTFRlQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3JpdHkwggEiMA0G
CSqG5Ib3DQEBAQUAA4IBDwAwggEKAoIBAQDVd/Ghr/WdGcjXOa+CHsjiu/cRSgjXpHLlmnNnqEnA
Jne6+DFkVlETkDdbLvm395rbBEvYUm4T51qGBgICOofwLLKo0tHdNk6ILUViOAP4g09pOQ6hgKGj
fd8JLBolW8REnEyr/kld3QOvUB7EiZLSntcOha73gTQz2iCPmjXnt9RbKPsAaxZieRN5e9jNLhm
4wQF26LKyuhA5oYptr35hxKTwU/+c6qrsnPq5C6pxMkZe06OlTEM6hMRGua16A26oMz7StDTcDiZ
NY1qGTadybW0HX2Acw4A9vqx+4tQmE+5KWZYwZnYLb+PLIIa9KAJW/7BPDggXaqymy2rTeijAgMB
AAGjggJ0MIICcDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRp
Y2VydC5jb2Vvb2Nzc0Ad8gNVHQ4EFgQUIlRCPzt50T6nmFmLL9kGHOMFg30wDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqlwAFTrjCPR+Mc0XCBiTI5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdHM0cGtpLm11bHRpY2VydC5jb2vY3lsL2NybF9tdHNjYTAwMV9kZWx0YS5jcmwwggEuBgNV
HSAEggElMIIBITCB0gYPKwYBBAGBw24BAQECAAEBMIG+MIG7Bggrbg EFBQcCAjCBrgyBq0NlcnRp
ZmljYWRvIGVtaXRpZGBqZGUgYWNvcmRvIGNvbSBhIFBvbMOtdGlj YSBkZSBDZX0aWZpY2Ficb3Mg
ZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFjY29yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUg
UG9saWN5IGluIGh0dHA6Ly90czRwa2kubXVsdGljZXj0LmNvb59wb2wvaW5kZXguaHRtbDBKBg4r
BgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIBFipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb2Ov
c G9sL2luZGl4Lmh0bWwwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3RzNHBra55tdWxQaWNlcnQu
Y29tL2NybC9jcmxfbXRzY2EwMDEuY3lsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggr
BgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEAyvatiFrPeNztreMWDn6/K0gos5zpUjLmP02uGjF8
972R3aSz5jY9vyQsjh/YS2WCi1u+0jnbY6g1PiR88+Mc+4HNWvXFVYSVSBkdlnuuzsfk3SvmlLJo
Y9MiwLVpAhpdfe7dUsjuDvdK2fFEvqwjXGp+Hqz/Jc2Uzq+OB2mWkOkE11mtHTAuNRxgoUiIzfCw
b+n0rhyGdPCW3xeHZDmvYx9vs5sd4aTcCJnjCbN3UlsjyiaMi7wzQe84ugvIAv4VTAYW/grBiRUjK
KaX9HOrzZvcjNDSMTyxeLe/QhUAF9yYOt2rBKhjqNVb0mp/FKI9aaoEDDB4jVfXNHjVjRGDZG2/M
7D9uVEylNegGRbsU9fpJx5uQbdFiImu1pmE8RHrdptU4NpqRikuqrDQjkCGksoVO5BWkcdOONWFy
7ArugelOsdgrctYp3FumUfw/EHHamw30sl+W5G7FW6KKRTWyO/wtyVunvmUKhBPOz02UUKU+im43
DyA6bTho5TME2wxZxZm8oAyOgZqHTZ1B1QyL4WlUQZqOxcu9Wv6E+a0VlYO0oDUZR0QGlFdq1As
JoFKsfnpYVSj0FCqtsRqAPw87RqvvuGMLIAUdA3lzGqU8O6Iwg0Bw9xWf11mhfHYbCbAc7i/FfWF
HB7so4KzMFi2bWX3do1iF0Lq12XEl8tAfMg=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000004*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Thu Oct 30 11:53:27 CET 2014*

Valid to: *Sat May 01 12:53:27 CEST 2021*

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:D5:77:F1:A1:AF:F5:9D:19:C8:D7:39:AF:82:1E:C8:E2:BB:F7:11:4A:08:D7:A4:
72:E5:9A:73:67:A8:49:C0:26:77:BA:F8:31:64:54:81:13:90:37:5B:2E:F9:B7:F7:9A:DB:04:4B:D8:52:6E:13:E7:5A:86:06:09:42:3A:87:F0:2C:B2:A8:D2:D1:DD:36:4E:A5:2D:45:62:38:03:F
8:83:4F:69:39:0E:A1:80:A1:A3:7D:DF:09:2C:1A:25:5B:C4:44:9C:81:32:AF:F9:25:77:74:0E:BD:40:7B:12:36:4B:4A:7B:5C:3A:16:BB:DE:04:D0:CF:68:82:3E:68:D7:9A:DF:51:6C:A3:EC:01
:AC:59:89:E4:4D:E5:EF:63:34:B8:66:E3:04:05:DB:A2:CA:CA:E8:40:E6:86:29:B6:BD:F9:87:12:93:C1:4F:FE:73:AA:AB:B2:73:EA:E4:2E:A9:C4:C9:19:7B:4E:8E:95:31:0C:EA:13:11:1A:E6:B
5:E8:0D:BA:A0:CC:FB:49:F0:D3:70:38:99:35:8D:6A:19:36:9D:C9:B5:B4:1D:7D:80:73:0E:00:F6:FA:B1:FB:8B:50:98:4F:B9:29:66:58:C1:99:D8:2D:BF:8F:2C:82:1A:F4:A0:09:5B:FE:C1:3C:
38:20:5D:AA:B2:9B:2D:AB:4D:E8:89:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *96:54:42:3F:3B:79:D1:3E:A7:98:59:8B:2F:D9:06:1C:E3:05:83:7D*

Basic Constraints *IsCA: false*

Authority Key Identifier *9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1* *CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]* *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7* *CPS pointer: http://ts4pki.multicert.com/pol/index.html*
CRL Distribution Points	*http://ts4pki.multicert.com/crl/crl_mtsca001.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*8E:59:6F:FD:2B:D1:B3:56:46:37:B4:58:CC:FF:80:22:28:CC:03:57:B8:84:6C:03:BD:B4:4B:74:53:1C:9D:44*

Service Status

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

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

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://ts4pki.multicert.com/pol/index.html*
URI	*[pt]*	*http://ts4pki.multicert.com/pol/index.html*

5.4.1 - History instance n.1 - Status: withdrawn

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name	*[en]*	*MULTICERT Qualified Time Stamping Authority*
Name	*[pt]*	*Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000004*
Subject OU:	*Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *llRCPzt50T6nmFmLL9kGHOMFg30=*

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

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

5.4.2 - History instance n.2 - Status: undersupervision

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000004*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *llRCPzt50T6nmFmLL9kGHOMFg30=*

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

Status Starting Time *2014-12-11T02:00:00Z*

5.5 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1003203698841180884*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHbzCCBVegAwIBAgIIDewYcurJWtQwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xKjAoBgNVBAsMIU1VTFRJQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNTAyMDMxMzA1NDFaFw0yMTAyMDMxMzA1NDFaMIG5MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TVVMVEIDRVJUIC0gU2VydmnDp29zIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOzbmljYSBT
LkEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDUxNDAy
BgNVBAMMK01VTFRJQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3JpdHkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC67TrgZ6OQ9C1OF08HfnFNb82j8ZDuMc9YPmM/8Vnj
fz3Gf1aYvM7MPkNp7014KvOenfEhdyzsfPfehCFe3bIceLTbwpz3KzKhI9f2Zlen0C8/CIRAy3M
iNzvyRpm0cn8jsgy9VRmJQB8gETJaTVmMYefby9jyCLqHeZvZMAem2tcSAjLc9FWfOWG30p5xPqv
P6JnkYJD4Oaq67Yhmxhco FB/bMLi0ED03AGcZG4PNGr0VopluaCxUghkSLm4SvRoO+kOHyfE5WXq
0+2vE0TjlGpebx+R/9r9jyf8gNAGXWUz+bHPpv28qh1THCtiyz7pmKYEuuvmiNahHB9YuK5AgM8
AAGjggI0MIICcDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHA6Ly9yY3NwLm11bHRp
Y2VydC5jb2vvb2NzcDAdBgNVHQ4EFgQUbX5BzvMo8XQXXHAj7qV2hv4fdPowDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqlwAFTrjCPR+Mc0XCBiTI5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdFlM0cGtpLm11bHRpY2VydC5jb2ovY3JsL2NybF9tdHNjYTAwMV9kZWxOYS5jcmiwggEuBgNV
HSAEggEIMIIBTCB0gYRKwYBBAG8w24BAQECAAEBMIG+MIG7Bggr8gEFBQcCAjCBrgyBq0NlcnRp
ZmljYWRvIGVtaXRpZG8gZGUgYWNvcmhvIGNvbSBhIFBvbMQtdGlj YSBkZSBDZXI0aWZpY2Fkb3Mg
ZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFjY29yZGFuY2Ugd2I0aCB0aGUgQ2VydGlmaWNhdGUg
UG9saWN5IGluIGh0dHA6Ly90czRwa2kubXVsdGljZXj0LmNvbS9wb2wvaW5kZXguaHRtbDBKBg4r
BgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIBFipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb2ov
cC9tL2luZGV4Lmh0bWwwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3RzNHBra55tdWx0aWNlcnQu
Y29tL2NybC9jcmxfbXRzY2EwMDEuY3JsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggr
BgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEApGoBBdtb9lBHA/OiqxUUPM+84s/8HRkOb5KgzG3p
JFpaxjxj4hHnT1IhjEenP5qGMyHR9ZecX1pb5c5BxlftSg3bvYjnAGRDDIN17QChpm+PzqHOI4y
3bnWPDjFsO0T2HGrkoszAdg0OlR5hh95IB0gGDs/xvT8nALefykFH5yxWFKGsW15VAXPNGkqIu0
mkrJH1lGByQC8c/DALUbAzLibtdyDTNWuPOR4IeMzyBFRGOO9SGpXWj8PYHDNBeG5vbRh1/mmnJC
WD+04Y1+HLP8l/mpnVkX8dcTj3QdyYHxQdvQ6YjOy+OQdDMDmD5a7RdBkgXNDKSyeXyRlhX14zJ1
h4dwK/5VIAT1uhjpgi/PfmjklZYNn4p3f8bAW6XbaKNgiaJs/t0/u86Nc5FVbf63QXUr5WejCwma
Hb1ThSsvGYF2vDgNup15ALv85tNAxO33BAaUlByJmA2OsupyVYwYS9EneeaIO7+SYD7iDgMiAA3TB
BOz12OzLwECzoLHi97p2cW1ihK0Hf4yiwKCOMYDUiWj21syyjLtI7jlnzins j8lAGLasz3lhm/ru
Hi14U6xmCCBhadV/yaFXhTmGtdatVPGisctUOEb4V7JKzbY715BS4WX1vgUnqZO1X2OatqYzc2Xm
vTPtM0T/dg2v8qEqt8pXJ3Wm0nYNhCGGEVE=
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000005*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Tue Feb 03 14:05:41 CET 2015*

Valid to: *Wed Feb 03 14:05:41 CET 2021*

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:ED:3A:E0:67:A3:90:F4:2D:4E:17:4F:07:7E:71:4D:6F:CD:A3:F1:90:EE:31:CF:58:3E:63:3F:F1:59:C9:7F:3D:C6:7F:56:98:BC:CE:CC:3E:43:69:EF:4D:78:2A:F4:1E:9C:50:61:77:2C:EC:7C:F7:DE:84:21:1E:DD:B9:63:71:E2:D3:6F:0A:73:DC:AC:CA:84:8F:5F:D9:99:5E:9F:40:BC:FC:29:51:03:2D:CC:88:DC:EF:C9:1A:66:D1:C9:FC:8E:C8:32:F5:54:66:25:00:7C:80:44:C9:69:35:66:31:87:9F:6F:2F:63:C8:22:EA:1D:E6:6F:64:C0:1E:9B:6B:5C:48:08:CB:73:D1:56:7C:E5:86:DF:4A:79:C4:FA:AF:3F:A2:67:91:82:43:E0:E6:AA:EB:B6:21:9B:18:5C:A0:50:7F:6C:C2:E2:D0:40:F4:DC:01:9C:64:6E:0F:34:6A:F4:56:BA:48:B9:A0:B1:52:08:64:48:B9:88:4A:F4:68:3B:E9:0E:1F:27:C4:E5:65:EA:D3:ED:AF:13:44:E3:94:6A:5E:6F:1F:91:FF:DA:FD:8F:27:E3:F2:03:40:19:75:94:CF:E6:C7:3E:9B:F6:F2:A8:75:4C:70:AD:8B:2C:FB:A6:62:98:12:EB:AF:98:83:5A:84:70:7D:62:E2:B9:02:03:01:00:01

Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *6D:7E:41:CE:F3:28:F1:74:17:5C:70:23:EE:A5:76:86:FE:1F:74:FA*

Basic Constraints *IsCA: false*

Authority Key Identifier *9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1

CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]

Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7

CPS pointer: http://ts4pki.multicert.com/pol/index.html

CRL Distribution Points *http://ts4pki.multicert.com/crl/crl_mtsca001.crl*

Extended Key Usage *id_kp_timeStamping*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9D:11:BF:0D:9F:27:E3:D5:BF:36:2A:0F:61:07:10:29:FF:BA:34:2C:5C:29:31:1D:35:2A:96:0B:96:51:DE:16*

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

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

Status Starting Time *2021-02-24T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://ts4pki.multicert.com/pol/index.html*

URI *[pt]* *http://ts4pki.multicert.com/pol/index.html*

5.5.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000005*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*bX5BzvMo8XQXXHAj7qV2hv4fdPo=*

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

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

5.5.2 - History instance n.2 - Status: withdrawn

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

Service Name

Name	*[en]*	*MULTICERT Qualified Time Stamping Authority*
Name	*[pt]*	*Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000005*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*bX5BzvMo8XQXXHAj7qV2hv4fdPo=*

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

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

5.5.3 - History instance n.3 - Status: undersupervision

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000005*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *bX5BzvMo8XQXXHAj7qV2hv4fdPo=*

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

Status Starting Time *2015-02-09T00:00:00Z*

5.6 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *1203717942046108825*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHbzCCBVegAwIBAgIIELR3FzlsLjkwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLS8TZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xKjAoBgNVBAsMIU1VTFRlQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNjAyMTYxOTIwNDdaFw0yMjAyMTYxOTIwNDdaMIG5MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TVVMVEIDRVJUIC0gU2VydmnDp29zIGRlIENlcnRpZmlj YcOnw6NvIEVsZWN0csOzbmlJYSBT
LlEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDYxNDAy
BgNVBAMMK01VTFRlQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3JpdHkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9CzR41+0zAQnANZ2M1HxZECVFagTlPp+909KL1Xkt
0sfZuUYu/TYRa1Fm1232ySJPC6M9BLgm75sDIy3zN0btQF8s6h2iZ12Ic7ps2GnvhrtN1u8nqfPs
2qIOJlNK547Zu//m9y46SOJpOjrC8yNn/udp4pYpdCJLx08BVFiC24n+KctdfaFL67bKWVCSLZAho
XCkCqpuWbROyD+y5NtlSmc8CrGxdgv/J3dht2O4SRaQ2r/OzuGepGlXpquFfUGI664OUmZVddUJG
8DlBh4zZoWuwffwQECcFigHYO/7/2ixRdO0olsOAos1SzoEUSLyDe6kzbQgCFHNieF43m9B9AgMB
AAGjggJ0MIICcDA6BggrBgEFBQcBAQQuMCwwKg YIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRp
Y2VydC5jb2Ovb2NzcDAaBgNVHO4EFgQU/85e75G2nILyCUadgJdA5+DICEcwDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqIwAFTrjCPR+Mc0XCBiTl5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdHM0cGtpLm11bHRpY2VydC5jb20vY3JsL2NybF9tdHNjYTAwMV9kZWx0YS5jcmwwggEuBgNV
HSAEggEIMIIBITCB0gYPKwYBBAGBw24BAQECAAEBMIG+MIG7BggrBgEFBQcCAjCBrgyBq0NlcnRp
ZmlY WRvIGVtaXRpZG8gZGUgYWNvcmRvIGNvbSBhIFBvbMOtdGlj YSBkZSBDZXJ0aWZpY2Fkb3Mg
ZW0vQ2VydGlmaWNhdGUgaXNzdWVkdGluIGFjY29yZGFu Y2Ugd2I0aCB0aGUgQ2VydGlmaWNhdGUg
UG9saWN5IGluIGh0dHA6Ly90czRwa2kubXVsdGljZXJ0LmNvb59wb2wvaW5kZXguaHRtbDBKBg4r
BgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIBFipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb20v
cG9sL2luZGV4Lmh0bWwwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3RzNHBraS5tdWx0aWNlcnQu
Y29tL2NybC9jcmxfbXRzY2EwMDEu Y3lsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggr
BgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEAFuOLgTGr8U1mZTej4IQU7h6Ngj/SMZAm06BYLHhp
LvPUiOKDUSwcjMqsK95Q5a7XF8wLokUUWKSqpz/eOlGz3Z7AW1CskWJfpPiLWa3woCkOVqaR7oeP
VneQKIj4PlqQPwlk7lvcNi8OTcy+pNGQNDos29t6Zr1pP2kKK4OBp7kOHiSeD2u226reyxq+asjw
8hBVifjczeRyziw2dR1B8UEDu0Mnhmvpg65Xa4L/iCtKOdpEeyls+KzKejP5KpDl6/EfzZwBiGq
I6Eeox1wZGndy3LxtBohimzl12G9lKndgjii0LCUoBNXoGgHw8SWcM8aB3nnJKftOEu0ULWXfCyJ
wfObAaoS60A5RHyLBgep35a4195Hhe22M+eAgyqKeeUfQvWmowBX4QGYmfKcR1ePeUOnfVBftobS
hQU6plmQSEm688UIIkqvWq9zAjOwrSHIpKax/5pQ7k2G/fgyL3svKDCmjkPS20uGOQoH9bHmrvGa
k3qDKAmHUK4OOf0WUxOZrCsMuFJNCZ3pKEUz5kfUXF+8NPeEU9gtrj0UQj/A8rz0BGCW0zhub0tz
osVohVkm738J4faUyAS9tArcLmXUw/h8AtDaK+UBnQLKpSHoWttb2oo5qRhxkSSRpbptECJmlHDk
GVEYnPcEzOFoWXB4vmaeS+qk5VUPo3U/xEA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000006*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Tue Feb 16 20:20:47 CET 2016*

Valid to: *Wed Feb 16 20:20:47 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:BD:0B:34:78:D7:ED:33:01:09:C0:35:9D:8C:D4:7C:59:10:25:45:6A:04:E5:3E
:9F:BD:D3:D2:8B:D5:79:2D:D2:C7:D9:B9:46:2E:FD:36:11:6B:51:66:D7:6D:F6:C9:22:4F:08:A3:3D:04:B8:26:EF:98:03:23:2D:F3:37:46:ED:40:5F:2C:EA:1D:A2:67:5D:88:73:BA:6C:D8:69
:EF:86:BB:4D:D6:EF:27:A9:F3:EC:DA:02:0E:24:93:4A:4B:8E:D9:BB:FF:E6:F7:2E:3A:48:E2:69:3A:3A:C2:F3:23:67:FE:E7:69:E2:96:29:74:22:4B:C7:4F:01:54:59:36:E2:7F:8A:72:D7:5F:68
:52:FA:ED:B2:96:54:24:BB:64:08:68:5C:29:02:AA:9B:96:6D:13:B2:0F:EC:B9:36:D9:52:99:CF:02:AC:6C:5D:82:FF:C9:DD:D8:6D:D8:EE:12:45:A4:36:AF:F3:B3:BB:67:A9:18:85:E9:AA:E1:
5F:50:62:3A:EB:83:94:99:95:5D:75:42:46:F0:39:7C:87:8C:D9:A1:6B:B0:7D:FC:10:10:27:05:8A:01:D8:3B:FE:FF:DA:2C:51:74:ED:28:22:C3:80:A2:CD:52:CE:81:14:48:BC:83:7B:A9:33:6
D:08:02:14:73:62:78:5E:37:9B:D0:7D:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *FF:CE:5E:EF:91:B6:9C:82:F2:09:46:9D:80:97:40:E7:E0:E5:08:47*

Basic Constraints	*IsCA: false*
Authority Key Identifier	*9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1* *CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]* *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7* *CPS pointer: http://ts4pki.multicert.com/pol/index.html*
CRL Distribution Points	*http://ts4pki.multicert.com/crl/crl_mtsca001.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C5:F2:89:2C:4B:20:40:1A:E1:8D:4A:24:B4:C6:55:0F:CC:86:03:42:01:76:C8:7E:4B:C1:FE:DC:E4:61:99:64*

Service Status

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

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

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI	*[en]*	*http://ts4pki.multicert.com/pol/index.html*
URI	*[pt]*	*http://ts4pki.multicert.com/pol/index.html*

5.6.1 - History instance n.1 - Status: withdrawn

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name	*[en]*	*MULTICERT Qualified Time Stamping Authority*
Name	*[pt]*	*Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000006*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I */85e75G2nILyCUadgJdA5+DlCEc=*

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

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

5.6.2 - History instance n.2 - Status: undersupervision

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

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000006*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I */85e75G2nILyCUadgJdA5+DlCEc=*

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

Status Starting Time *2016-02-29T00:00:00Z*

5.7 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Name *[pt]* *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *570604023422947529*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHbzCCBVegAwIBAgIIB+sxVgulkMkwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUx0SUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xKjAoBgNVBAsMIU1VTFRlQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNzAyMjQxOTU5MTNaFw0yMzA4MjcxOTU5MTNaMIG5MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TVVMVEIDRVJUIC0gU2VydmnDp29zIGRlIENlcnRpZmlj YcOnw6NvIEVsZWN0csOzbmlj YSBT
LkEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDcxNDAy
BgNVBAMMK01VTFRlQ0VSVCBRdWFsaWZpZWQgVGlltZSBTdGFtcGluZyBBdXRob3Ijpdlkwggg EIMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBQ0Tg3E6sRjaVWLsgfkpH0W4+65VrmiXXtQqz/Tcr
sj5NZv9xCpwO4KkxfwIaN1labdVU/8TavfPlHfiQNhR149jajp6oxWCrM1fZfhK19jkwAt94It0J
qUlWgXmQnib/Pfi8ndoSI/dSGYjVSwPmzTZDoMGTNHzik705bHDDASrkpNZ05o9JlRrWFwl/Ojio
/n9NujMDALLC2+3AFvcIWe5z1jpqRiN4zGYXI+YPOyoPausNXVhHqlUl0tj6seE8uV3KfHNfyOwktB
sGMAvAoH+GAEaScHlcnCmBMDAaopVNqO4VgpEeDfF6R8GYckrLRTjzfg2yRDxIWR6KtAsbDLAgMB
AAGjggJ0MIICCDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRp
Y2VydC5jb20vb2NzcDAdBgNVHQ4EFgQUAb+xnBZXLZHbl8C0LBtTmyVBOyIwDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqIwAFTrjCPR+Mc0XCBiTI5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Ol8vdHM0cGtpLm11bHRpY2VydC5jb2OvY3JsL2NybF9tdHNjYTAwMV9kZWx0YS5jcmwwggEuBgNV
HSAEggEMIIBITCB0gYPKwYBBAGBw24BAQECAAEBMIG+MIG7BggrBgEFBQcCAjCBrgyBq0NlcnRp
ZmljYWRvIGVtaXRpZG8gZGUgYWNvcmRvIGNvbSBhIFBvbMOtdGljYSBkZSBDZXJl0aWZpY2Fkb3Mg
ZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFjY29yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUg
UG9saWNSIGluIGh0dHA6Ly90czRwa2kubXVsdGljZX0LmNvb59wb2wvaW5kZXguaHRtbDBKBg4r
BgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIBFipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb20v
cG9sL2luZGV4Lmh0bWwwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3RzNHBraS5tdWx0aWNlcnQu
Y29tL2NybC9jcmxfbXRzY2EwMDEuY3JsMA4GA1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggr
BgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEARmBOkVusPssEMPLg3uhhWR4SaHluOyeLjnh++K+r
z5HEn41YW1dlxx4l58/x2xlrp6MBVYDedDRCFPDk9wpZchnHqtEtHXkjyT+LFPC4wDE8gyEtgI74
5nL2BqiGcVzn3uvFINYN9yLEj0iffPA5rpxArVl9ntQOU6pLLiEpuErtdwYao+TXpG3ARAo0x0So
v2l/FcsMz128/38lrfjlahSPOYs6eP+P1YcwxjadEM51fEyRw8wud0mvjrW13CFi+buIHcZU2Low
b1MfHoguaeZTtdicz6jI19UlutzkLKTxWnKLZfphio1U3rVlLMVBtzFIIl+qD87zTQV6zyhgTOxrA9
mjT4OSr4njLFxcwB82MRsu53SD3yChLHX38LeNCkZPUxQVqmYwTO6OPtEqe+w8RfPHnga3SCMwl2
flqwK8ORDqzxzljHU87yRU7Khx6vJSiowoDMhsoqgHlkuHHZS8EnXb0T4HQzTR0KGGo7aZHzwHsQ
a1/rzyNs3p5ejY6mdz1hcpj+sLXPRC+CFAh5NYuGoRacvKQRvBKi8eiE/uMHPZ4yy9t/pULv7xd
nby868R6pcldhin+GQv7jfkSKSjddcIw1PYP7wWg4vi3FFWGOij4sjcTYeBjYupZsrVmeWoQSkK3d
/zUJzosWiE/C7Se3uHfeyFZOB84ywNKqktE=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000007*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from:	*Fri Feb 24 20:59:13 CET 2017*
Valid to:	*Sun Aug 27 21:59:13 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:C1:43:44:E0:DC:4E:AC:46:36:95:58:BB:20:7E:4A:47:D1:6E:3E:EB:95:6B:9A:25:D7:B5:0A:B3:FD:37:2B:B2:3E:4D:66:FF:71:0A:9C:0E:E0:A9:31:7F:02:1A:37:52:1A:6D:D5:54:FF:C4:DA:BD:F3:E5:1D:F8:90:36:14:75:E3:D8:DA:26:9E:AB:C5:60:AB:33:57:D9:7E:12:B5:F6:39:30:02:DF:78:22:DD:09:A9:49:56:81:79:90:9E:26:FF:3D:F8:BC:9D:DA:12:23:F7:52:19:88:D5:4B:03:E6:CD:36:43:A0:C1:93:34:7C:E2:93:BD:39:6C:70:C3:01:2A:E4:A4:D6:74:E6:8F:49:95:1A:D6:17:09:7F:38:98:A8:FE:7F:4D:BA:33:03:00:B0:B6:FB:70:05:BD:C5:9E:E7:3D:63:A6:A4:62:37:8C:C6:61:72:3E:60:F4:32:A0:F6:AE:B0:D5:D5:84:7A:89:2E:5D:2D:8F:AB:1E:13:CB:95:DC:A7:C7:35:FC:8E:C2:4B:41:B0:63:00:BC:0A:07:F8:60:04:69:27:07:21:C9:C2:98:13:03:01:AA:29:54:D8:10:E1:5A:A9:11:E0:ED:17:A4:7C:19:87:24:AC:B4:53:27:37:E0:DB:24:43:C4:85:91:E8:AB:40:B1:B0:CB:02:03:01:00:01*
Authority Info Access	*http://ocsp.multicert.com/ocsp*
Subject Key Identifier	*01:BF:B1:9C:16:57:2D:91:DB:97:C0:B4:2C:1B:53:9B:25:41:3B:22*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1* *CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]* *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7* *CPS pointer: http://ts4pki.multicert.com/pol/index.html*
CRL Distribution Points	*http://ts4pki.multicert.com/crl/crl_mtsca001.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F1:F9:E7:67:D9:0D:BA:CA:B9:9C:5D:EC:4C:4A:1E:D8:E7:47:CD:BD:1E:A7:82:BE:53:97:F0:54:39:3E:CB:6B*

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000007*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*Ab+xnBZXLZHbl8C0LBtTmyVBOyI=*

Service Status

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

Service status description [en] *undefined.*

Status Starting Time *2025-02-28T00:00:00Z*

Scheme Service Definition URI

URI [en] *http://ts4pki.multicert.com/pol/index.html*

URI [pt] *http://ts4pki.multicert.com/pol/index.html*

5.7.1 - History instance n.1 - Status: granted

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

Service Name

Name [en] *MULTICERT Qualified Time Stamping Authority*

Name [pt] *Multicert (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000007*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *Ab+xnBZXLZHbl8C0LBtTmyVBOyI=*

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

Status Starting Time *2017-03-26T23:00:00Z*

5.8 - Service (granted): MULTICERT Trust Services Certification Authority 002

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]* *MULTICERT Trust Services Certification Authority 002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *7394183213738552410*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHLTCCBRWgAwIBAgIIZp1qdPMK7FowDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xMjAwBgNVBAMMKU1VTFRlQ0VSVCBSb290IENlcnRpZmlj YXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE3MTIxMjE1NTgxNFoXDTMwMDYxMjE1NTgxNFowgbIxC2AJBgNVBAYTAlBUMUIwQAYD
VQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNh
IFMuQS4xIDAeBgNVBAsMF0NlcnRpZmlj YXRpb24gQXV0aG9yaXR5MT0wOwYDVQQDDDRNVUxUSUNF
UlQgVHJ1c3QgU2VydmlzZXMgQ2VydGlmaWNhdGlvbiBBdXRob3IpdHkgMDAyMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEAsLPfMR5+Ej4INIDZblcPzIfa5ppk1eCfgLMgDU3Ot7uqTQUz
/4tlBE8+BSyvjBQCImsGRU9RaYiwmtVWTmh5mZCl2ckdZ/c+ZguuQxGfZUuj8Rm/8CaRyLACOmFU
tjxFSEDnmFgGOfTZb09hJiFe7TPwLEEPKIKwCSDGSL3eSvGI+voUMM2g4VRj460nHS7xKYLaUIyB
QySp3yDP3dFmLOU9EVDuMOegRSlsb92C26RH2oV9jit8YEEajy1lVSBSOVid57RMaMLGAfRrH30r
pef+mXNAvWUY5+bWksD+4CLgehHmkq/t+TKnMsCDk4DRW22r6AiUP2bVlaCMGRXRbNYGFb/lEPZo
u+MEAhvCQrpPSZXJriYE8/zv1Ig+dhMUr3YUq8ABW7r+f69k2DqX2syT+ANiyBFZGjjq2KKf+CFF
+tnqX8Yfh9YeYkXg3Oug7krs/jJ6ZVQBcgaZzOtCT++Dmc6e6dCB/owtdVBmyMK6YakR08wv7In3
duJUqnpkkt095Oi7V3WXP7RcRZC7ufHRSxq8abbXd6Igb0ewJfooxbf2wkMJ5IM+1zLpnxFm+I5
pFg5CGJ62Pl15mYXB+6ygg9mX8ET7I9yWDQbLu9bCVbHU7mhh4dqIGRLK5mH6Fvk4Ern6AjFMyoi
ErC37/t3V5Hjz+2zRgVgvn5ViIMCAwEAAaOCAXAwggFsMDoGCCsGAQUFBwEBBC4wLDAqBggrBgEF
BQcwAYYeaHR0cDovL29jc3AubXVsdGljZXJ0LmNvbS9vY3NwMB0GA1UdDgQWBBQ7xcITe+P1IfRQ
4IFv8xYugS76BjAS8gNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNU5HJxbbwSqopVM7yDd
KXSkxUVxMIGGBgNVHSAEfzB9MDwGDSsGAQQBgcNuAQEBAAcwKzApBggrBgEFBQcCARYdaHR0cDov
L3BraXJvb3QubXVsdGljZXJ0LmNvbS8wPQYOKwYBBAGBw24BAQEAAQIwKzApBggrBgEFBQcCARYd
aHR0cDovL3BraXJvb3QubXVsdGljZXJ0LmNvbS8wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3Br
aXJvb3QubXVsdGljZXJ0LmNvbS9jcmwvcm9vdF9tY19jcmwuY3JsMA4GA1UdDwEB/wQEAwIBBjAN
BgkqhkiG9w0BAQsFAAOCAgEAK6NEOdYyqAtXnkTW6buYwSw93Tv28Lsfs29+ggQeWYiWSMEjdnJ
R6kFW8zq6Bmrh56JLyaPjFYfuACvgYuwlFbnwnWIXCzv00AejQsBZrIZw2hy7e5qKfIVgLgURZIr
zdJ8nmfhWU2e+AzU78s70Kk0sYA1mDhS6pqSmUTg/mDQtatUufXHnTCDmDARgaWIVfcm2mahwetM
fDrg43bJUPpELwQtTE/n4dojH/phthn3PKTSj6+yL5XF1zMHEVCJwh2PtrzSRR2/wKe/1pXbNfaI
Dc5NxDjkdlkgJTeIJDQBp4XNGwPz7CNj/xedxO NKcLc9MOeqesc2ESg/HIHmjQnFFfy3gMgf07c
Kwx2dyhH2AKbjBElGZwi/tbFUdHH2Mg4nqII7ynPg3BAazFYHxdjc9MjRno4jZJnMHHtj6HzFUuA
1g1ji1skNeozdu8ezDhRZgM7ta2qKcMmLBwUruoiuX2VTrwOqZrpeuNaIVx7V5N6y5PfONnKvwoH
GU3RyVCSVvpKhVqklZQGXLnkHtneGR+HrlWMm+z1O1EhrRHidp9Ij/uozGxGTl8AsRqvy9fKsaDy
yZ8YqrpIwbND7yRg/egKFHozGwmBz45C50pmsLMkbknAdFtUr7xL2LwFmXlNzagO8D4IvBR5uCB
yYdaU9VdLffodVOK86R9xWA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Trust Services Certification Authority 002*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Tue Dec 12 16:58:14 CET 2017*

Valid to: *Wed Jun 12 17:58:14 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:B0:B3:DF:31:1E:7E:12:3E:08:34:80:D9:6C:87:0F:CC:87:DA:4A:9A:64:D5:E0
:9F:80:B3:20:0D:4D:CE:B7:BB:AA:4D:05:33:FF:8B:65:04:4F:3E:05:2C:AF:8C:14:02:22:6B:06:45:4F:51:69:88:B0:9A:D5:56:4E:68:79:99:90:A5:D9:C9:1D:67:F7:3E:66:0B:AE:43:11:9F:6
5:4B:A3:F1:19:BF:F0:26:91:C8:B0:02:3A:61:54:B6:3C:45:48:40:E7:98:5A:86:39:F4:D9:6F:4F:61:26:21:5E:ED:33:F0:2C:41:0F:2A:52:B0:09:20:C6:48:BD:DE:4A:F1:A5:FA:FA:2E:30:CD:A
A:E1:54:63:E3:AD:27:1D:2E:F1:29:82:DA:52:5C:81:43:24:A9:DF:20:CF:DD:D1:66:2C:E5:3D:11:50:EE:30:37:A0:45:22:2C:6F:DD:82:DB:A4:47:DA:85:7D:8E:2B:7C:60:41:1A:8F:2D:65:5
5:20:52:0D:52:1D:E7:B4:4C:68:C2:C6:01:F3:EB:1F:7D:2B:A5:E7:FE:99:73:40:BD:65:18:E7:E6:D6:B0:3F:B8:08:B8:1E:84:79:A4:AB:F8:FE:4C:A9:CC:80:20:E4:E0:34:56:DB:6A:FA:02:25:
0F:D9:B5:62:25:A0:8C:19:15:D1:6C:D6:06:15:BF:E5:10:F6:68:BB:E3:04:02:1B:C2:42:BA:4F:49:95:C9:AE:26:04:F3:FC:EF:D4:88:3E:76:13:14:AF:76:14:AB:C0:01:58:BA:FE:7F:AF:64:D8
:3A:97:DA:CC:93:F8:03:62:C8:11:59:18:98:EA:D8:A2:9F:F8:21:45:FA:D9:EA:5F:C6:1F:87:D6:1E:62:45:E0:DC:EB:A0:EE:4A:EC:FC:92:7A:65:54:01:72:06:99:CC:EB:42:4F:EF:83:99:CE:9
E:E9:D0:81:FE:8C:2D:75:50:66:C8:C2:BA:61:A9:11:D3:CC:2F:EC:89:F7:76:E8:F4:52:A9:E9:92:4B:74:F7:93:A2:ED:5D:D6:5C:FE:D1:71:16:42:EE:E7:C7:45:2C:6A:F1:A6:DB:5D:DE:A5:81
:BD:1E:C0:97:E8:A3:16:DF:DB:09:0C:27:99:4C:FB:5C:CB:A6:7C:45:9B:E9:79:A4:58:39:08:68:FA:CC:F2:35:4A:66:17:07:EE:B2:82:0F:66:5F:C1:13:EE:5F:72:58:34:1B:2E:EF:5B:09:56:C
7:53:B9:A1:87:87:6A:20:64:4B:5D:29:87:E8:5B:E4:E0:4A:E7:EB:08:C5:33:2A:22:12:B0:B7:EF:FB:77:57:91:C9:CF:ED:B3:46:05:60:BE:74:95:8A:23:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *3B:C5:C9:53:7B:E3:F5:21:F4:50:E0:81:6F:07:16:2E:81:2E:FA:F2*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: http://pkiroot.multicert.com/

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2

CPS pointer: http://pkiroot.multicert.com/

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *82:CF:DA:E3:A7:0B:6E:37:5A:96:ED:3C:FC:91:2E:81:A0:20:10:4A:8B:A8:86:27:2B:59:63:AD:EC:A2:44:11*

X509SubjectName

Subject CN: *MULTICERT Trust Services Certification Authority 002*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *O8XJU3vj9SH0UOCBbwcWLoEu+vI=*

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

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

Status Starting Time *2020-11-09T00:00:00Z*

5.8.1 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCForESig, QCForESeal, QCStatement, QCQSCDManagedOnBehalf]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

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]* *MULTICERT Trust Services Certification Authority 002*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Trust Services Certification Authority 002*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *O8XJU3vj9SH0UOCBbwcWLoEu+vI=*

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

Status Starting Time *2018-01-03T01:00:00Z*

5.8.4.1 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCForESig, QCForESeal, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

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*

5.9 - Service (granted): MULTICERT SSL Certification Authority 001

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]* *MULTICERT SSL Certification Authority 001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *2927614233995221994*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHIjCCBQggAwIBAgIIKKD5onipm+owDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDINVUxUSUNFUlOqLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhIFMuQS4xMjAwBgNVBAMMKU1VTFRJQ0VSVCBSb290IENlcnRpZmlj YXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE3MTIxMjE2MDAwOFoXDTMwMDYxMjE2MDAwOFowgacxCzAJBgNVBAYTAlBUMUIwQAYD
VQQKDDINVUxUSUNFUlOqLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNh
IFMuQS4xIDAeBgNVBAsMF0NlcnRpZmlj YXRpb24gQXV0aG9yaXR5MTIwMAYDVQQDDCINVUxUSUNF
UlOgU1NMIENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IDAwMTCCAiIwDQYJKoZIhvcNAQEBBQADggiP
ADCCAgoCggIBAOTX1Zh09z52UHsBb4itNN1nHE4jmbvw4QxQP6jzPBE2HYL0N3RDqIUc7jEiOgTM
N90w2Z+Zp40BUrpW50+sIRcZl14McSrzIUjLAqHu6n6ZyDfRzAjtIhkoKXprimqVXI0zQkFRBGrO
9SfPOqncIByt Mv6CyRV19vwIjyS21+tvzhId401j5ab/weycKRi0VZki4V1vPOIkW2ygqXSAzBXw
LObvhTdyETHZCFEpge7vczc2HCTLQ90ijcTEy0DYmQUSj05KuYsHp7g0tc9UH0X+/LEQqqSv9k4
B8RYTgzP5QU7aG/85Lu8jbb2Rce+Rf2uuKds2XVmqhKb/k4OQ057unOy9EKVRsqA012ofyEUIjSi
xdSaF/Bz8qtCxX6Qeyvjjk5a2k93xdr/DoDJdRv60YWwbkNVCk9gj6CttbF8m2YHuVaOxCjo79/p
zTnsgBZf2/C0thKdctuzvkXy75Fa1Oa20BXDDVSHQGq4iuexcyEr98nraAGm1sFkzcaRprtwNCjy
rYNdlehLehamzZOU9+y+0v4qZGfBLpRz8Ac0Bjf7NdfUIUiZ8Ghwj3Ml9mhdG+ND0P+LhtAil9m3
MnAkNoAHS1VAQGgshp4TAew3vvuSKvZ9Eb7ct9vz5c5YPZ6Y70bE14wlqpu4ZlDbb+KaMZa2CNHA
MuCFmuCjW9CbAgMBAAGjggFwMIIBbDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHA6
Ly9vY3NwLm11bHRpY2VydC5jb20vb2NzcDAdBgNVHQ4EFgQUsAI5UgpPc5rI2YFFNl0RnV8jOZcw
EgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBTVORycW28EqgKVTO8g3Sl0pMVFcTCBhgYD
VR0gBH8wfTA8Bg0rBgEEAYHDbgEBAQAHMCswKQYIKwYBBQUHAgEWHWh0dHA6Ly9wa2lyb290Lm11
bHRpY2VydC5jb20vMD0GDiSGAQOBgcNuAQEBAAECMCswKQYIKwYBBQUHAgEWHWh0dHA6Ly9wa2ly
b290Lm11bHRpY2VydC5jb20vMEEGA1UdHwO6MDgwNqA0oDKGMGh0dHA6Ly9wa2lyb290Lm11bHRp
Y2VydC5jb20vY3JsL3lvb3RfbWNfY3lsLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQEL
BQADggIBAlavxMfz3Sp5Xy2GnCLLVSQlyczO Y3c23Drnubdh5EGZhAQpD4DL7/tSFYGuvLuwMwBG
B6AKQGw7CGtBTZBb+u1nJ8HnBRcSZhsRqfxfLR3IERUVN1jq9lQLoFkGvLowv80EduJh7OvSxzfk
lNtK36fYf8EruqmqKbtkUbRrq8scAbyeu7Yh9GbIFR01H3tcCchW92vL/CRiMdzAbek15BPnk+X
gT5QuGRrZfycNlIRkHlnUVbAPrshg9u6iZ7pXexq2qDvlRLu7ep5mJwbSRXU0lnl77IGZ7iASH0E
k3tkZc2qcY+KVb1sQP87cic4nU3KAhKtCpA2Gxb5CjucyiyxGP3KQU40Zc5X7NYulMUCYIWH3z+7
vHu/DDHybib6rRfWumgkV/jv3DVGZRhT+8dBZq3JaM94G3OBr0hW/62HeE0gQJ98JFWW8udUqbz
StNZbOxNF5Fga3dSyDVvNeo9IbV6ta41VgB1cAr7Dd15mDzbyNKAkXO+aSE6s7tyxZZFKFiMazP
ugtwh6j/NiAeL9A5KDsrf8qA8Ln5G679A05Rn1FDs/w9BI953h54AVkToCSBIEDywDD13KYDFAvZ
ji297HaUFIM/BCr6XpMmDKq4sxcKvgiXVSzy/o/+cyPY52aVbll8xJd+4Tnrdlblue+5kHrOwQ+V
0ULarahD

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT SSL Certification Authority 001*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Tue Dec 12 17:00:08 CET 2017*

Valid to: *Wed Jun 12 18:00:08 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:E4:D7:D5:98:74:F7:3E:76:50:7B:01:6F:88:AD:34:DD:67:1C:4E:23:99:BB:F0:
E1:0C:50:3F:A2:73:3C:11:36:1D:82:F4:37:74:43:A8:85:1C:EE:31:22:3A:04:CC:37:DD:30:D9:9F:B6:A7:8D:01:52:BA:56:4B:4F:AC:21:17:19:97:5E:0C:71:2A:F3:21:48:CB:02:A1:EE:EA:7
E:99:C8:37:D1:CC:02:6D:96:19:28:29:7A:68:8A:6A:95:5C:8D:33:42:41:51:04:6A:CE:F5:27:CF:3A:A9:DC:88:1C:AD:32:FE:82:C9:15:75:F6:FC:08:8F:24:B6:D7:EB:6F:CE:12:1D:E3:4D:49
:E5:A6:FF:C1:EC:9C:29:18:B4:57:69:22:E1:5D:6F:3C:E2:24:5B:6C:A0:A9:74:80:CF:C5:F0:2C:E6:EF:85:37:72:11:31:D9:08:51:29:81:EE:EF:73:37:36:1C:24:CB:43:DD:22:25:C4:C4:CB:4
0:D8:99:05:39:8F:4E:4A:B9:8B:07:A7:B8:34:B5:CF:54:1F:45:FE:23:F2:C4:42:AA:92:BF:D9:38:07:C4:58:4E:0C:CF:E5:05:3B:68:6F:FC:E4:BB:BC:25:B6:F6:45:C7:BE:45:FD:AE:B8:A7:6C:
D9:75:66:AA:12:98:FE:4E:0E:43:4E:7B:BA:73:B2:F4:42:95:46:CA:80:D3:5D:A8:7F:21:14:20:94:A2:C5:D4:9A:17:F0:73:F2:AB:42:C5:7E:90:7B:2B:E3:8E:4E:5A:DA:4F:77:C5:DA:FF:0E:8
0:C9:75:1B:FA:D1:85:B0:6E:43:55:0A:4F:60:8F:A0:AD:B5:B1:7C:9B:66:07:B9:56:8E:C4:28:E8:EF:DF:E9:CD:39:EC:80:16:5F:DB:F0:B4:B6:12:9D:72:DB:B3:BE:45:F2:EF:91:5A:D4:E6:B6:
D0:15:C3:0D:54:87:40:68:38:8A:E7:B1:73:21:2B:F7:C9:EB:68:01:A6:D6:C1:64:CD:C6:91:A6:BB:70:34:28:F2:AD:83:5D:95:E8:4B:7A:16:A6:CD:93:94:F7:EC:BE:D2:FE:2A:64:67:C1:2E:9
4:73:F0:07:34:04:97:FB:35:D7:D4:21:48:99:F0:68:70:27:73:25:F6:68:5D:1B:E3:43:D0:FF:8B:B6:D0:22:23:D9:B7:32:70:24:36:80:07:4B:55:40:40:68:2C:86:9E:13:01:EC:37:BE:FB:92:2
A:F6:7D:11:BE:DC:B7:DB:F3:E5:CE:58:3D:9E:98:EF:46:C4:D7:8C:25:AA:9B:B8:66:50:DB:6F:E2:9A:31:96:B6:08:D1:C0:32:E0:85:9A:E0:A3:5B:D0:9B:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *B0:02:39:52:0A:4F:73:9A:C8:D9:81:45:36:5D:11:9D:5F:23:39:97*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: http://pkiroot.multicert.com/

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2

CPS pointer: http://pkiroot.multicert.com/

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FF:45:3A:54:13:EA:55:8F:E7:06:2A:B6:FE:83:10:73:E7:F3:0F:E6:BA:75:B8:2E:AD:52:09:DB:07:75:CA:D0*

X509SubjectName

Subject CN: *MULTICERT SSL Certification Authority 001*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *sAI5UgpPc5rI2YFFNl0RnV8jOZc=*

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

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

Status Starting Time *2018-01-03T01:00:00Z*

5.9.1 - Extension (critical): Qualifiers [QCStatement, QCForWSA]

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.*

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.4*

Description

5.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.10 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5563023195650613480*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIIODCCBiCgAwIBAgIITTPUH04DYOgwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xKjAoBgNVBAsMIU1VTFRjQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xNzEyMjkxNDUyNDVaFw0yNDA2MzAxNDUyNDVaMIG5MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TVVMVEIDRVJUIC0gU2VydmnDp29zIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOzbmljYSBT
LkEuMR8wHQYDVQQLDBZUaW1lIFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDgxNDAy
BgNVBAMMK01VTFRjQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3JpdHkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfU9zCCJ7+jFQG6oEYy/QFqbUNCHdU9wP6R5WQ5o2i
6n19hMxjoOEvuMgksQ4EMtbqsa1FdXgotkCGQkZiIUwemK/BQwLaET8ipXOh7lMqDHaIKCizX0q9
+6fj32UsVaaHxaIvZgTLgbOhOuCSjggDz9LxOZD2zqvIKpXHrX619mSVk8w/XFFpRZuFiakmHRCu
yi9MsusNAmOuX7jICfMg2HeSVgBCezBb2l+vKTv29zw4hbuOp9v6BGqzHUWDmYqQ2Y3pqITMNV/
xNlfxNmjM47itkGgbogwE+HBMQ843Z7JnbBx5mjY1WVgYvOWA/SdMB+x/UiZL5BpxbojfjFRAgMB
AAGjggM9MIIDOTA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0dHABLy9vT3NwLm11bHRp
Y2VydC5jb20vb2NzcDAdBgNVHQ4EFgQUJDFJMSYbj3JUgWVE/9gOyzLCMjkwDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqlwAFTrjCPR+Mc0XCBiTl5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdHM0cGtpLm11bHRpY2VydC5jb20vY3JsL2NybF9tdHNj YTAwMV9kZWx0YS5jcrnwwgcYGCCsG
AQUFBwEDBIGS MIG2MIGzBgcEAIGXXqEBDIGnQnkqaW5jbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50
lHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQgdGhpcyB0aW1lLXN0YW1wIHRva2VuIGlzIGlzc3VlZCBh
cyBhIHF1YWxpZmllZCBlbGVjdHJvbmljIHRpbWUtc3RhbXAgYWNjb3JkaW5nIHRvIHRoZSBSRUdV
TEFUSU9OIChFVSkgTm8gOTEwLzIwMTQwggEuBgNVHSAEggEIMIIBITCB0gYPKwYBBAGBw24BAQEC
AAEBMIG+MIG7BggrBgEFBQcCAjCBrgyBg0NlcnRpZmlpYWRvIGVtaXRpZGBgZGUgYWNvcmRvIGNv
bSBhIFBvbMOtdGlj YSBkZSBDZXJ0aWZpY2Fkb3MgZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFj
Y29yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUgU9saWN5IGluIGh0dHA6Ly90czRwa2kubXVs
dGljZXj0LmNvbS9wb2wvaW5kZXguaHRtbDBKBg4rBgEEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIB
FipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb20vcG9sL2luZGV4LmhlbWwwQQYDVR0fBDowODA2
oDSgMoYwaHR0cDovL3RzNHBra55tdWx0aWNlcnQuY29tL2NybC9jcmxfbXRzY2EwMDEuY3JsMA4G
A1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEA
fWaXCMU52CcXeIv/KfmHNqK2ZHtHDisOrVpQ6nvKfhWOHREIiDQCHybYS1UU0sIwLYkrmKPpqkI9r
S/TDzEDRHDntmdrsyjm8jgxy+1Kknk2v/h7bLGpED95tDUvL4Wj6QdBGZvQs9aIP2jTjZh9kWKr
oIGDYYu+hcHM0der0sAWmnf5KWe5C9FPPHggAx2RCxqtOAqgPGmpkbj/HJxscWbMhmpZf70m0DW
zAp38nkhd/LxWBt6MbViLo2dvKQcyaZ3PeZGOXGHzqNoqA2Xh9IPD7nk6v3NIGjr6DU28TYkozPJ
IGkTLV/dqC+h7VhH6WiPmEfYXYoj4sC3eFRloUztOjdrRzaONPi62d2VE4wWtqsIxp423Ou1nDgO
+FOcrnJGqzw6Rdt5DhpO06I6OLunjmZj//+0YjXFUocE6+Ap1wdGOzofcxXDMwVbkm0pMoTL/NKE
td1ZOL4EJOM8xWN2gdFb1j1eDp8nTV81VVKP55m+ZGfvajadx2GcVzWECIcWuZL9DXgCoQh9wrMF
rK9tgKYrNcy/baNNehpI8jy+hwvCv/cmvxTYf5QhgqwyW0Ukh1yFZZJXYCuCZmXoLs/+dTltRuon
sIJ6SxeXMpxNY7zMtjsV3FBn3VwCE7+aWFylabybENux5/GEq3W7eWt4gyh88De23wNdUsuo7nY=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000008*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from:	*Fri Dec 29 15:52:45 CET 2017*
Valid to:	*Sun Jun 30 16:52:45 CEST 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:02:82:01:01:00:9F:53:DC:C2:08:9E:FE:24:54:06:EA:81:18:BF:F4:05:A9:B5:0D:08:77:54:F7:03:FA:47:95:90:E6:8D:A2:EA:7D:7D:84:CC:63:A0:E1:2F:B8:CB:24:B1:0E:04:32:D6:EA:B1:AD:45:75:78:28:B6:40:86:42:46:62:95:4C:1E:9A:4F:C1:43:02:DA:11:3F:22:A5:73:A1:EC:83:2A:D0:76:A2:28:28:B3:5F:4A:BD:FB:A7:C9:DF:65:2C:55:A6:87:C5:A9:6F:66:04:CB:81:B3:A1:3A:E0:92:26:08:03:CF:D2:F1:39:90:F6:CE:AB:C8:2A:95:C7:AD:7E:B5:F6:64:95:93:CC:3F:5C:51:69:45:9B:85:89:A9:26:1D:10:AE:CA:2F:4C:B2:EB:0D:02:63:AE:5F:B8:C8:09:F3:20:D8:77:92:56:00:42:7B:30:5B:D8:8F:AF:29:3B:F6:F7:3C:38:85:BB:8E:A7:DB:FA:04:6A:B3:1D:45:83:99:8F:EA:43:66:37:A6:A2:13:30:D5:7F:C4:D9:5F:C4:D9:A3:33:8E:E2:B6:41:AA:6E:88:30:13:E1:C1:31:0F:38:DD:9E:C9:9D:B0:71:E6:68:D8:D5:65:60:62:FD:16:03:F4:9D:30:1F:B1:FD:48:99:2F:90:69:C5:BA:09:B4:91:51:02:03:01:00:01*
Authority Info Access	*http://ocsp.multicert.com/ocsp*
Subject Key Identifier	*24:31:49:31:26:1B:27:72:54:81:65:44:FF:D8:0E:CB:32:C2:32:39*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1* *CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]* *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7* *CPS pointer: http://ts4pki.multicert.com/pol/index.html*
CRL Distribution Points	*http://ts4pki.multicert.com/crl/crl_mtsca001.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*72:7C:3B:7D:A0:0A:F9:4D:1C:2D:FE:A4:EF:C4:52:42:C7:2B:7D:22:E5:26:5B:7E:C0:73:0D:ED:02:4A:FA:D2*

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000008*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*JDFJMSYbJ3JUgWVE/9gOyzLCMjk=*

Service Status

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

Service status description [en] *undefined.*

Status Starting Time *2025-02-28T00:00:00Z*

5.10.1 - History instance n.1 - Status: granted

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

Service Name

Name [en] *MULTICERT Qualified Time Stamping Authority*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000008*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *JDFJMSYbJ3JUgWVE/9gOyzLCMjk=*

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

Status Starting Time *2018-01-03T01:00:00Z*

5.11 - Service (withdrawn): MULTICERT Qualified Time Stamping 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.*

Service Name

Name [en] *MULTICERT Qualified Time Stamping Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1541972321544869692*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIIODCCBiCgAwIBAgIIFWYvqB8qlzwwDQYJKoZIhvcNAQELBQAwgbwxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDINVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xKjAoBgNVBAsMIU1VTFRlQ0VSVCBUcnVzdCBTZXJ2aWNlcyBQcm92aWRlcjE9MDsG
A1UEAww0TVVMVEIDRVJUIFRydXN0IFNlcnZpY2VzIENlcnRpZmlj YXRpb24gQXV0aG9yaXR5IDAw
MTAeFw0xOTAyMDQxMDQxMDhaFw0yNTA4MDMxMDQwNTJaMIGS MQswCQYDVQQGEwJQVDFCMEAGA1UE
Cgw5TVVMVEIDRVJUIC0gU2VydmnDp29zIGRlIENlcnRpZmlj Yc Onw6NvIEVsZWN0csOzbmlj YSBT
LkEuMR8wHQYDVQQLDBZUaW1IFN0YW1waW5nIFNlcnZpY2VzMQ8wDQYDVQQFEwYwMDAwMDkxNDAy
BgNVBAMMK01VTFRlQ0VSVCBRdWFsaWZpZWQgVGltZSBTdGFtcGluZyBBdXRob3lpdHkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBlOFWOAEj0ongU/phLpDm5CSLWrWPWtXmKZB5GS7+
+3K7KuLyzqIzE+LrUBDERhU49p4saW29+yEcXu8ZV6xuR5+EMZqENX6Eajh1/FkBH17XY7ZIGCH2
85MIQTsxscNTn6EEUhlX1S+L1GGWhNgsKYdXAKFxvnAq5iyegy2t4shXlBBmx1NaVdkmdqp9p3cE
4UOfi9yJfumgGEECj8W2RE7y1ajTEPhIxztmuSQnRbm2WG92aEJAfCLh3EHA4fQ8eAa0AS/50Gm/
nr1FZi2GmQzxjZwVtQ84cwDkjz4X1M/cG3SQ7vtZ887VvkG302/vJLD4JNNTgX6xUgLqXGHAgMB
AAGjggM9MIIDOTA6BggrBgEFBQcBAQQuMCwwKg YIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRp
Y2VydC5jb2vb2NzcDAdBgNVHQ4EFgQUezo0Uaa7nTgV0meYZYUbLXv7KEkwDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSdqlwAFTrjCPR+Mc0XCBiTl5NSpTBHBgNVHS4EQDA+MDygOqA4hjZodHRw
Oi8vdHM0cGtpLm11bHRpY2VydC5jb2Ovy3JsL2NybF9tdHNjYTAwMV9kZWx0YS5jcmwwgcYGCCsG
AQUFBwEDBIGS MIGzBgcEAIGXKgEBOlGnQnkqaWSjbHVzaW9uIG9mIHRoaXMgc3RhdGVtZW50
IHRoZSBpc3N1ZXIgY2xhaW1zIHRoYXQgdGhpcyB0aW1lLXN0YW1wIHRva2VuIGlzIGlzc3VlZCBh
cyBhIHF1YWxpZmllZCBlbGVjdHJvbmljIHRpbWUtc3RhbXAgYWNjb3lkaW5nIHRvIHRoZSBSRUdV
TEFUSU9OIChFVSkg Tm8gOTEwLzIwMTQwggEuBgNVHSAEggEl MIIlBITCB0gYPKwYBBAGBw24BAQEC
AAEBMIG+MkG7BggrBgEFBQcCAjCBrgyBq0NlcnRpZmlj YWRlIGVtaXRpZGBgZGUgYWNvcmRvIGNv
bSBhIFBvbMOtdGljYSBkZSBDZXJ0aWZpY2Fkb3MgZW0vQ2VydGlmaWNhdGUgaXNzdWVkIGluIGFj
Y29yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUgUG9saWN5IGluIGh0dHA6Ly90czRwa2kubXVs
dGljZXj0LmNvb S9wb2wvaW5kZXguaHRtbDBKBg4rBgEAYHDbgEBAQIABzA4MDYGCCsGAQUFBwIB
FipodHRwOi8vdHM0cGtpLm11bHRpY2VydC5jb2vcG9sL2luZGV4LmhtbWwwQOYDVR0fB0owODA2
oDSgMoYwaHR0cDovL3RzNHBra S5tdWx0aWNlcnQuY29tL2NybC9jcmxfbXRzY2EwMDEuY3JsMA4G
A1UdDwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEA
mMEFTiX4gHgDfwVAkTwvp1EWzjlq2mo0a9jkxcK9pVjVtCRBP+wPTNpOrMumCsDWejiTIGWwFt0Y
KA4wGweZxUDfDU53xx0kv5iZdKUJp5Fiu/WfE3uc+8qy4q1vUT/NdsGytQA5vIBU524mxMlVC2j
/1rGDlypbvy09jh1w3nZsYs5LlebKa5ei9jd4oq6jc64548gfd9pIHDXqmc1iKRJ/KCtLCBKDmZi
MUMTfgJMiHmXDhrglYqznNigRHgz5vVPqfW7go09+RsnrCIN6yTFfk7hqhwdVix8p/qcnk0F+WZG
WK1xFCL6cF9QDshzYHLG8sDJkV0OzGocNCjecU50C4+rEMkus/uVtOYKbyBrNtt4XiMnKrgzG30P
bEc64DXg3nCnSBuMd6WE5jHkCZ0+BH/llxsjrv+bg39KP5gAKJaPrYHEG+DZSOWrIiysYMqLIfS/
L1Ncdzz2x4LbUV02fGCr8Uh83prhjveVasUAqDABHrKg75lIMenEkuDKHvm2in4hu+D/OBW7E5wJz
Fj8RkA4Q07phOQEhQjhm+j6OsQfMcyA8fVN3teFapLdHbkDj/88ecv0jiLpKviP1PHL72wJK09AF
lsFqNrgt/nGcZOgXsGXB40jbB6E2601ChDzT/x4472FMvgmUi6mYzi9nnWhX4ck2zPITQiIRyZE=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Trust Services Certification Authority 001*

Issuer OU: *MULTICERT Trust Services Provider*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000009*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Feb 04 11:41:08 CET 2019*

Valid to: *Sun Aug 03 12:40:52 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:C1:0C:55:8E:00:48:F4:A2:78:14:FE:98:4B:A4:39:92:09:22:D6:AD:63:D6:B4:
85:E6:29:90:79:19:2E:FE:FB:72:BB:2A:E2:F2:CE:09:73:13:E2:EB:50:10:C4:46:15:38:F6:9E:2C:69:6D:BD:FB:21:1C:5E:EF:19:57:AC:6E:3F:9F:84:31:9A:84:35:7E:84:6A:38:75:FC:59:01:
1F:5E:D7:63:B6:65:18:21:F6:F3:93:25:41:3B:31:B1:C3:53:9F:A1:04:52:19:57:D5:2F:8B:D4:61:96:84:D8:2C:29:87:57:00:A1:71:BE:70:2A:E6:2C:9E:83:2D:AD:E2:C8:57:94:10:66:C7:53
:5A:55:D9:26:76:AA:7D:A7:77:04:E1:43:9F:8B:DC:89:7E:E9:A0:18:41:02:27:C5:B6:44:4E:F2:D5:A2:53:10:F8:48:C7:3B:66:B9:24:27:45:B9:B6:58:6F:76:68:42:40:7C:22:E1:DC:41:C0:E
1:F4:3C:78:06:B4:01:2F:F9:D0:69:BF:9E:BD:45:66:2D:86:99:0C:F1:8D:9C:15:B5:0F:38:73:FC:03:92:3C:F8:5F:53:3F:70:6D:D2:43:BB:ED:67:CF:3B:56:F9:06:DF:4D:BF:BC:92:C3:E0:93:
4D:4E:05:FA:C5:48:0B:A9:71:87:02:03:01:00:01
```


Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *7B:3A:34:51:A6:BB:9D:38:15:D2:67:98:65:85:1B:2D:7B:FB:28:49*

Basic Constraints *IsCA: false*

Authority Key Identifier *9D:AA:5C:00:15:3A:E3:08:F4:7E:31:CD:17:08:18:93:23:93:52:A5*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.1.1* *CPS text: [Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://ts4pki.multicert.com/pol/index.html]* *Policy OID: 1.3.6.1.4.1.25070.1.1.1.2.0.7* *CPS pointer: http://ts4pki.multicert.com/pol/index.html*
CRL Distribution Points	*http://ts4pki.multicert.com/crl/crl_mtsca001.crl*
Extended Key Usage	*id_kp_timeStamping*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*51:F0:0A:65:93:00:3D:54:6C:BE:4E:66:AA:57:3C:08:63:97:61:C2:19:21:2E:F2:96:9C:AD:CE:9B:D9:50:8A*

X509SubjectName

Subject CN:	*MULTICERT Qualified Time Stamping Authority*
Subject SERIAL NUMBER:	*000009*
Subject OU:	*Time Stamping Services*
Subject O:	*MULTICERT - Serviços de Certificação Electrónica S.A.*
Subject C:	*PT*

X509SKI

X509 SK I	*ezo0Uaa7nTgV0meYZYUbLXv7KEk=*

Service Status

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

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

Status Starting Time

2025-10-27T13:00:00Z

5.11.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *MULTICERT Qualified Time Stamping Authority*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Qualified Time Stamping Authority*

Subject SERIAL NUMBER: *000009*

Subject OU: *Time Stamping Services*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *ezo0Uaa7nTgV0meYZYUbLXv7KEk=*

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

Status Starting Time *2019-06-23T23:00:00Z*

5.12 - Service (granted): MULTICERT Trust Services Certification Authority 005

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]* *MULTICERT Trust Services Certification Authority 005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *220666502927607348758755205193897537 58*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHSzCCBTOgAwIBAgIQEJnh25ovRat6dw5QmVaxnjANBgkghkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBF
bGVjdHLDs25pY2EgUy5BLjEyMDAGA1UEAwwpTVVMVElDRVJUIFjyb3QgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkqMDEwrHcNMTkxMjA5MTgzNDM3WhcNMzIwNjA4MTgzNDM3WjCBsjELMAkGA1UEBhMC
UFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVj
dHLDs25pY2EgUy5BLjEgMB4GA1UECwwXQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxPTA7BgNVBAMM
NE1VTFRJQ0VSVCBUIcnVzdCBTZXJ2aWNlcyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAwMDUwggIi
MA0GC5qG5Ib3DQEBAQUAA4ICDwAwggIKAoICAQDhbCC7vCHTPmF3t3Z36QMZK4wbfqkFV32GY6wq
USOaOq72f2J0KjbpzN2Q9UoD/DaPgwtZQ5kVK++qu7A2+DJ0QVYNc4bL3FNYAdoADDQyM385eIIO
VRLBgecQ8vpw05bs2lxcIN8owI68Ai0r+V+orm7YKQ2jvgU/GXgN09D/WbB5UzM0VJ1fQ4PHoko+
1JCPZyAZjoRr6Isid9mVYb0bGxuT8aOB23b+UUbGnDcpy2X+ko9Fc1ZfLFgf43B+AfrjRIp9KIOj
WIOFIUmPNqWa82cvHy8f9r3QbvcKLmfUqHoZQDhNc6G+IRAblzSZBn+hIbXKZT7CiOGr7vBFTH+
JW4irs/Fk9IE9C0b3G76X52JhtE+IMYEjEQgTTaLIpY6tpttraVh730aDtvF94BaY9Ozhh5LjE2N
jxqYPBlFgb7fuwFNTD0H3A6OQ9evWK3tz7YxOb0xwhe4Ua7XJ9YVv/kszO80ozY2pua2cU+Olo4B
NrqCha8k2SRMs759mMLVTUNrsRAZrEgWHEMYERqLZOuuCvAG2f5xZTgVS09kOW9LQ4/S84Ces+p5
yLaCy9Z3V1j/iBiLO+Q1DAHWdprB6xN5sz7G3CJVanpSm7z+PS/XMi6sKQENBCdNQazIRYJRs7ZZ7
xrrP3lqrn4KE/yZ5gVA3RLq6iOvmMRfjb+rzOQIDAQABo4IBhjCCAYIwdQYIKwYBBQUHAQEEaTBn
MDkGCCsGAQUFBzAChi1odHRwOi8vcGtpcm9vdC5tdWx0aWNlcnQuY29tL2NlcnQvcm9vdDAwMS5j
ZXIwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRpYZVydC5jb20vb2NzcDAdBgNVHQ4EFgQU
B6ZVpnqlwavf5UEjz+mgKkO2uggwEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBTVORyc
W28EqgKVTO8g3Sl0pMVFc1BDBgNVHSAEPDA6MDgGDSsGAQQBgcNuAQEBAAcwJzAlBggrBgEFBQcC
ARYZaHR0cHM6Ly9wa2kubXVsdGljZXJ0LmNvbTBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vcGtp
cm9vdC5tdWx0aWNlcnQuY29tL2NybC9yb290X21jX2NybC5jcmwwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdJQOWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkghkiG9w0BAQsFAAOCAgEAmKGifK0lUcq7
ciq7IuW3uJSDH2zV52RxL+bl9VtMvd3iqpCm0WtWJf6t2z6zknBjWUjYymvURXHDJlW+WeuVHl
m2/wbHSL9QxJr4tV8PLWo/WEehomxXS+dwDDUhtla9cGH65ZtozJ2/iLuMPvYCVTXlj/uJ/rQOi
yW2ILAfOUBr7zogrcEa5xNl0o6+2qKdQJ5Nkgdn+6m/GACSIlyxMav/5rFCnoLUVrrg2svWK7eFB
9RWIbeKZRVzTbMBislbhIG7Ativ9f/pwS8GWCjaw/evjAycDlUcuZVKBHNqUVZi/NtwChxjLs62
b/63seMlI9Xd+mobLyq8cfh/7yOOWiBlV75smGih/orro8/Knh1m58bBPAhBL1C/nTn4eLxsYDOX
kEH4RNUhHokU8gOQ8lISgwNVWN2Z93x9OqN4YNAfwtDP9jU7Nnhv054xjO+K9/DXriiko3nqsUW
dkE9ZyrG9RgRk2MCR+gPZ0qrQY3FVlooocbz+AmEOq/KzVNxzfZz40/yxcdgPvWjakKK1WeLZ1Q95
+/TkfGfbJ6R5qiS7Xw2vzhNT0o8Mt4uCH0fR9KxqYTtVFIOxY5jgRPXSYhBrmbeXLx57AMAxQ/P4
dFY5hUJCDdecAZahjZwcFp1VxGnZGc1P0SYfoW6mCH2hx38A4IpDzvF1UOENHMg=

-----END CERTIFICATE-----
```

Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Trust Services Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Dec 09 19:34:37 CET 2019*

Valid to: *Tue Jun 08 20:34:37 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:E1:6C:20:BB:BC:21:D3:3E:61:77:B7:76:77:E9:03:19:2B:8C:1B:7E:A9:05:57:
7D:AA:63:AC:2A:51:23:9A:3A:AE:F6:7F:62:74:2A:36:E9:CC:DD:90:F5:4A:03:FC:36:8F:83:0B:59:43:99:15:2B:EF:AA:BB:B0:36:F8:32:74:41:56:0D:73:86:CB:DC:53:58:01:DA:00:0C:34:3
2:33:7F:39:78:89:4E:55:12:FC:81:E7:10:F2:FA:70:D3:96:EC:D8:8C:5C:20:DF:28:C0:8E:BC:00:8D:2B:F9:5F:A8:AE:6E:D8:29:0D:A3:BE:05:3F:19:78:0D:D3:D0:FF:59:B0:52:53:33:34:54:
9D:5F:43:83:C7:A2:4A:3E:D4:90:8F:DB:20:19:8E:84:6B:E8:8B:22:77:D9:95:61:BD:1B:1B:1B:93:F1:A3:81:DB:76:FE:51:46:C6:9C:37:29:CB:65:FE:92:8F:45:73:56:5F:2C:58:1F:E3:70:7E
:01:FA:C9:44:8A:7D:28:83:A3:58:83:85:95:49:BF:36:A5:AB:F3:67:2F:1F:2F:1F:F6:BD:D0:6E:F7:24:2E:67:D4:A8:7A:3F:65:00:E1:35:CE:86:F8:84:40:6E:5C:D2:64:19:FE:84:86:D7:29:94:
FB:0A:23:86:AF:BC:81:15:31:FE:25:6E:22:AE:CF:C5:93:D2:04:F4:2D:1B:DC:6E:FA:5F:9D:89:86:D1:3E:20:C6:04:8C:44:20:4D:36:8B:96:96:3A:B6:9B:6D:AD:A5:61:EF:7D:1A:0E:DB:C5:F
7:80:5A:63:D3:B3:86:1E:4B:8C:4D:8D:8F:1A:98:3C:19:45:81:BE:DF:BB:01:4D:4C:3D:07:DC:0E:8E:43:D7:AF:58:AD:ED:CF:B6:31:39:BD:31:C2:17:B8:51:AE:D7:27:D6:15:BF:F9:2C:CC:E
F:34:A3:36:36:A6:E6:B6:71:4F:8E:22:8E:01:36:BA:82:85:AF:24:D9:24:4C:B3:B4:BD:98:C2:D5:4D:43:6B:B1:10:19:AC:48:16:1C:43:18:11:1A:8B:64:EB:AE:0A:F0:06:D9:FE:71:65:38:15:
4B:4F:64:39:6F:4B:43:8F:D2:F3:80:9E:B3:EA:79:C8:B6:82:CB:D6:77:57:58:FF:B8:18:8B:43:E4:35:0C:01:D6:76:9A:C1:EB:13:52:E7:3E:C6:DC:22:55:6A:7A:52:9B:BC:FE:3D:2F:D7:32:2E
:AC:29:01:0D:F0:27:4D:D9:EC:C8:45:8F:D1:B3:B6:7B:C6:BA:CF:DE:5A:AB:9F:82:84:FF:26:79:81:50:37:44:BA:BA:88:EB:E6:31:17:E3:6F:EA:F3:39:02:03:01:00:01*

Authority Info Access

http://pkiroot.multicert.com/cert/root001.cer

http://ocsp.multicert.com/ocsp

Subject Key Identifier *07:A6:6F:A6:7A:A5:C1:AB:DF:E5:41:23:CF:E9:A0:2A:43:B6:BA:A8*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: https://pki.multicert.com

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Extended Key Usage *id_kp_clientAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *48:A1:53:E2:1E:1B:8C:64:DC:BD:CB:A0:34:DA:B2:EF:85:27:A7:79:A1:BA:2A:A2:38:AC:C4:8A:2C:6F:CA:CF*

X509SubjectName

Subject CN: *MULTICERT Trust Services Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *B6Zvpnqlwavf5UEjz+mgKkO2uqg=*

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

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

Status Starting Time *2020-03-29T23:00:00Z*

5.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.12.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.12.3 - Extension (critical): Qualifiers [QCStatement, QCForESig, QCForESeal, QCSSCDStatusAsInCert, QCQSCDManagedOnBehalf]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

5.13 - Service (granted): MULTICERT QWAC Certification Authority 005

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]* *MULTICERT QWAC Certification Authority 005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *115075157036243863931272732520205380553*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHQTCCBSmgAwIBAgIQVpKr5MTcDVUO1MUTKpXryTANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8Qjby8F
bGVidHLDs25pY2EgUy5BLjEyMDAGA1UEAwwpTVVMVEIDRVJUIFJvb3Qg02VydGlmaWNhdGlvbiBB
dXRob3JpdHkgMDEwHhcNMTkxMjA5MTgzNTQ4WhcNMzIwNjA4MTgzNTQ4WjCBqDELMAkGA1UEBhMC
UFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVj
dHLDs25pY2EgUy5BLjEgMB4GA1UECwwXQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxMzAxBgNVBAMM
Kk1VTFRJQ0VSVCBRV0FDIENlcnRpZmlJYXRpbZ4gQXV0aG9yaXR5IDAwNTCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBALncsmOzznWMuQh0Tgnb8ycEh9LepEOEc0FQudFhCifsrvSmnJDP
+nkiR67Cm9WTcfYXZLlazRjBw/QG4O45wF6g0PhC3oQuJbx325nL6YPPFPbMS2Ee51U4TWwI8QUr
+OAxdHKY1mnRByfLk9uS2YsmFZyY00Dqw80GZagQ85/3ye3r5WjbZ14OzOibOn0xURGdn3TkRPTa
cLHFwL+KnsFLn1/GVi5Q5xnwCurD6ZOqw7NhWUvbIWqgtXTSrQ8ueSIs0E7CAc0FBA6zA8y7u5nC
Slal+n4f8+hZpPyMxYHlk61hP731hLy1xYN/rhf27mCIKE6gldu/TWCloffBzyvzkG4nHftXSZ4Q
PjrAMw+G1TAlD1AJnv6YKEK50PjNVO2+pqXz/u2CXc9lZRqG6QOkK/y1Z3z+jlZF72vSG9jx6Yiv
jrs5NvgDxYLEG/pAi9XS67ZiCukTcw4TtE5Vswx64+onSMiePmQuHX70IaoTgg7lzvgJOmfCpDo0
VrvYObyA8zW+7aWNltVIFOe2wMRpYjIGDahfeMRKBPrU7yySbP27a2tAPwPXvt8eeZ1hCoWo0v3g
VltGjymHtwidt4xXKqJ1iVLsXsupgYgctU95ePdw8rhukNV5iFeBh/HrwQAQFUO810sNKAff3y/m
ZwWftbjfrmcb5aD+0mBhSbZTAgMBAAGjggGGMIIBgjB1BggrBgEFBQcBAQRpMGcwOQYIKwYBBQUH
MAKGLWh0dHA6Ly9wa2lyb290Lm11bHRpY2VydC5jb20vY2VydC9yb290MDAxLmNlcjAqBggrBgEF
BQcwAYYeaHR0cDovL29jc3AubXVsdGlJZX0LmNvb59vY3NwMB0GA1UdDgQWBBRWR7CZkf9uiuE1g
zXUjBeW11+ZyqzASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNU5HJxbbwSqopVM7yDd
KXSkxUVxMEMGA1UdIAQ8MDowOAYNKwYBBAGBw24BAQEABzAnMCUGCCsGAQUFBwIBFhlodHRwczov
L3BraS5tdWx0aWNlcnQuY29tMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly9wa2lyb290Lm11bHRp
Y2VydC5jb20vY3JsL3lvb3RfbWNfY3JsLmNybDAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0lBBYwFAYI
KwYBBQUHAwEGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQBOaWtAHyShjeTpBOw7M8//2G/m
YYYcMcZ2wYQGKte3BA60dC8dxeYquNslwpmuNnegKi3grn7Bjb8w93hrbejyKcqFrFMC8n/NyePc
OxLIT5YSlWsaqrV3MH3XCtUBRcv3gl/sglfG++NVVHcm5UjRadgrdxN9KhlSPrjGWh2rfQwHaboV
eEadmSq7g7tfd+LfoWQQqM6paYG6KjgzBfnyv0I9acXTkddXJkG3RgrUaqZ/h02DuIL93k9/q5q7
UFbUGmKfybEfN1Ve5wtfNwCnptD7g2wpWyIPfG0Frjesdd8TiZin1IBiXFYEEDGF9U36I5Nrh Y8U
1Kt88dN+89cmrIc2fLI7rx9c7h7HHafRWiXpfjPYPeH6nRT8LQBPGM4a7KgVmIYbGW8xG7m4qPF6
5oMIvfBU/qxi6HYm9tAfWNuwyXP5hvlZq703lSydoAPznrBAj6qt5nzHUAxMUXI57BMNBQ+gKUjX
EjWiVRUOa4OTDUQq2NI1NXcorh2WwPEuY6r0/v5El6ULxquabfj1mdKSL2E8Wm96MdhQlQOgOVvB
l2eeyzqvMKHkJlzLzabBG3H8s6pZqnhovbd2lQOjmdr9MeHkZVd5ka5Mqp559MiPGBaY8YL6LGO5
vZMEqlL6tCQPRVBbxwwFmr4LX9cvTw6nT4/atywr2/5etElY2w==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT QWAC Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Dec 09 19:35:48 CET 2019*

Valid to: *Tue Jun 08 20:35:48 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:B9:DC:B2:63:B3:CE:75:8C:B9:08:74:4E:09:DB:F3:27:04:87:D2:DE:A4:43:84:73:41:50:B9:D1:61:0A:27:EC:AE:F4:A6:9C:90:CF:FA:79:22:47:AE:C2:9B:D5:93:71:F6:17:64:B2:1A:CD:12:41:C3:F4:06:E0:EE:39:C0:5E:AA:D0:F8:42:DE:84:2E:25:BC:77:DB:99:CB:E9:83:CF:14:F6:CC:4B:61:1E:E7:55:38:4D:6C:08:F1:05:2B:F8:E0:31:74:72:98:D6:69:D1:07:27:C8:93:DB:92:D9:8B:26:15:9C:98:D3:40:EA:C0:1D:06:65:A8:10:F3:9F:F7:C9:ED:E8:E5:62:5B:67:5E:0E:CC:E8:9B:3A:7D:31:51:11:9D:9F:74:E4:44:F4:DA:70:B1:C5:C0:BF:BA:9E:C1:4B:9F:5F:C6:56:24:90:E7:1A:F0:0A:EA:F4:E9:93:AA:C3:B3:61:59:4B:DB:21:6A:A0:B5:74:D2:AD:0F:2E:79:29:6C:D0:4E:C2:01:CD:05:04:0E:B3:03:CC:BB:BB:99:C2:4A:56:88:FA:7E:1F:F3:E8:59:A4:FC:8C:C5:81:C8:93:AD:61:3F:BD:F5:84:BC:B5:C5:83:7F:AE:17:F6:EE:60:88:28:4E:A0:95:DB:BF:4D:60:A5:A1:F7:C1:CF:2B:F3:90:6E:27:1D:FB:57:49:9E:10:3C:9A:C0:33:0F:86:D5:30:25:0F:50:09:9E:FE:98:28:42:B9:D0:F2:4D:54:ED:BE:A6:A5:F3:FE:ED:82:5D:CF:48:65:1A:86:E9:03:A4:2B:FC:B5:67:7C:FE:8C:86:45:EF:6B:D2:1B:D8:F1:E9:88:AF:8E:BB:39:36:F8:03:C5:82:C4:1B:FA:40:8B:D5:D2:EB:B6:62:0A:E9:13:73:0E:13:B4:4E:55:B3:0C:7A:E3:EA:27:48:C8:9E:3E:64:2E:1D:7E:F4:95:AA:13:AA:0E:C8:CE:F8:09:3A:67:C2:A4:3A:34:56:BB:D8:39:BC:80:F3:35:BE:ED:A5:8D:96:D5:65:14:E7:B6:C0:C4:69:60:99:46:0D:A8:5F:78:C4:4A:04:FA:D4:EF:2C:92:6C:FD:BB:6B:6B:40:3F:03:D7:BE:DF:1E:79:9D:61:0A:85:A8:D2:FD:E0:54:8B:46:8F:29:87:B7:08:9D:B7:8C:57:2A:A2:75:89:52:EC:5E:CB:A9:81:88:1C:B5:4F:79:78:F7:70:F2:B8:6E:90:D5:79:88:57:81:87:F1:EB:C1:00:10:15:43:BC:D7:4B:0D:28:07:DF:DF:2F:E6:67:05:9F:B5:B8:DF:AE:67:1B:E5:A0:FE:D2:60:61:49:B6:53:02:03:01:00:01

Authority Info Access

http://pkiroot.multicert.com/cert/root001.cer

http://ocsp.multicert.com/ocsp

Subject Key Identifier

56:47:B0:99:91:FF:6E:B8:4D:60:CD:75:23:F1:E5:B5:D7:E6:72:AB

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier

D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: https://pki.multicert.com

CRL Distribution Points

http://pkiroot.multicert.com/crl/root_mc_crl.crl

Extended Key Usage

id_kp_serverAuth

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

35:A1:FA:A8:C8:11:25:66:6D:26:F0:A6:E8:64:DD:EA:A7:04:31:CC:15:70:DC:88:3C:F1:47:CD:19:6E:4A:B6

X509SubjectName

Subject CN:

MULTICERT QWAC Certification Authority 005

Subject OU:

Certification Authority

Subject O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Subject C:

PT

X509SKI

X509 SK I

VkewmZH/brhNYM11I/Hltdfmcqs=

Service Status

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

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

Status Starting Time

2024-10-23T16:00:00Z

5.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.13.2 - History instance n.1 - Status: granted

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

Service Name

Name [en] *MULTICERT QWAC Certification Authority 005*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT QWAC Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *VkewmZH/brhNYM11l/Hltdfmcqs=*

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

Status Starting Time *2020-03-29T23:00:00Z*

5.13.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.13.2.2 - Extension (critical): Qualifiers [QCForWSA, QCStatement, QCSSCDStatusAsInCert]

Qualifier type description [en] *undefined.*

Criteria list assert=all

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.4*

Description

5.14 - Service (granted): MULTICERT Timestamping Certification Authority 005

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.*

Service Name

Name *[en]* *MULTICERT Timestamping Certification Authority 005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *87404832348392367630550043988318301056*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHPzCCBSegAwIBAgIQQcGO8qw14xeat/UR1gUrgDANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBF
bGVjdHLDs25pY2EgUy5BLjEyMDAGA1UEAwwpTVVMVElDRVJUIFJvb3QgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkgMDEwrfhcNMTkxMjA5MTgzNDA5WhcNMzIwNjA4MTgzNDA5WjCBsDELMAkGA1UEBhMC
UFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVj
dHLDs25pY2EgUy5BLjEgMB4GA1UECwwXO2VydGlmaWNhdGlvbiBBdXRob3JpdHkxOzA5BgNVBAMM
Mk1VTFRJQ0VSVCBUaW1lc3RhbXBpbmcgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMDA1MIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAgyZ+0dyq7Tftq2E5gsggwcr5YmuKH5GhUrYsIZ1C
0wG6Bfc63FFwzl6+VTrr+Y3v/U9MYvWpZgrmE8KE5w7oEVmsVlMXUGkqxIgdLpG32ryiDbYSpL84
m8SAj3oJWp34uHdkDVeK/HLT9StuwhJAgWwL2n463v1m1QrHJftX+8fWYFbzEpYpxpD712vXB6FC
6HARHbSrM8jdpVNJ34f5HV53GwIUA/5A5Ghds4i4aVvJXWOqTtoiQ+630g4/k8CRnfpc47hzETRh
K+LNOCKeHdBvB59Rclu9ZOGXYIZEdINlaLpfj4G0HS7wqlUvVzXMI+8iBZldx+dOtzfsS6Pj3L6i
5lkmJHVSREne6qX9XbY1tgNE+M5un55ibpzG5jULqS1QZR2FuXqKNm0t89p8SKcn5dnjR5oEQ+Kj
b4ZekQI+V3CetClm/8TDGrZXl3L1Lv5vPzZUOz94j7kW/BslVXgTSYLjlQo3Lm2ez+tZmrXoT0da
mf+VfDosxqSjdtyp+L/fkkshNZtL5BaMj5yA3jq6t24hU4Qv5TzEleT5WBFTh4JEyD4WIJNCfOek
1x3O3drVtQWUOj6jDekK7TLEQAoGs7jPu7sbjDudZbAXC4oaNCCB2nqTVKXmLU8Pm2Sk7c72bu/wx
o685TfhL2Noq3vGPMR/WBZDxlmASOnW6T2MCAwEAAaOCAXwwggF4MHUGCCsGAQUFBwEBBGkwZzA5
BggrBgEFBQcwAoYtaHR0cDovL3BraXJvb3QubXVsdGljZXJ0LmNvbS9jZXJ0L3Jvb3QwMDEuY2Vy
MCoGCCsGAQUFBzABhh5odHRwOi8vb2NzcC5tdWx0aWNlcnQuY29tL29jc3AwHQYDVR0OBBYEFNyQ
DNmNSiqUe1K7OLQ/E3reqC6WMBIGA1UdEwEB/wQIMAYBAfBCAQAwHwYDVR0jBBgwFoAU1TkcnFtv
BKqIUzvlN0qdKTFRXEwQwYDVR0gBDwwOjA4Bg0rBgEEAYHDbqEBAOAHMCcwJQYIKwYBBQUHAgEW
GWh0dHBzOi8vcGtpLm11bHRpY2VydC5jb20wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3BraXJv
b3QubXVsdGljZXJ0LmNvbS9jcmwvcm9vdF9tY19jcmwuY3JsMA4GA1UdDwEB/wQEAwIBBjATBgNV
H5UEDDAKBggrBgEFBQcDCDANBgkqhkiG9w0BAQsFAAOCAgEAIgRGfFCP7OhFH8HT/WySrtlNNvmN
0H8z1pMoUR1TxgebZc5wwQF5+fCgGh4qW4dB7ctxCHafG0vgY4ZawW2EvWu6hmORimoYGuQ5Q1op
8L6SUzU9vnvT0aPWtEUbakWPj58kqKU8LCcFNelB0/SsgvfcUlNgfo/wc7zJBxjA9vMnTnbAxIFy
fFxO41k2YmibW3tlwyIlhmaKVuM2u1IuOdq99YatEYKiAX+OXNlE1MyGARzlUnw0INXO04GS3WnC
hBwGr/AlZjcfT3lNaDxyos2aiWjKxDNNMM7e4pokeoy7P8szccvGv1pHUqj3glcpx6TaCWZxqjlk
o5AMlmKZySj5FjMQYNOjrHB5psQujSYOQTO5ARrENGEG6ME65ZjxtQLg1hVKSoWWZUjNz6AoHAVQP
lMeRAAf3dgCN0G6noi2aBra+dFZ/6UxXR1EXw9jizgQimYCNygkAUQgj1sTnn/KXlniBpr8X7j25
oiNXvbv2hLoir2YSEqwI4N86NqIiA1F4Q2n3jGGCBBCtzg1tVAKPBMei8KCtrU68PjmmnahUzA68
KkD9rxUp0XAjx+LgMNLxsA9juyv1QxfHkWsx1IrVWlCBZRHGkfyZ6a8ykpSpQk1Yq96DfuLsaBwI
F00JdQxEAweokZby1W/36wZiVinYJxDEWARcDhwEg7YVxuM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Timestamping Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Dec 09 19:34:09 CET 2019*

Valid to: *Tue Jun 08 20:34:09 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:AB:26:7E:D1:DC:AA:4D:F9:6D:AB:61:39:82:C8:20:C1:CA:D2:62:6B:8A:1D:21:A1:52:B6:2C:21:9D:42:D3:01:BA:05:F7:3A:DC:51:70:CE:5E:BE:55:3A:E8:F9:8D:EF:FD:4F:4C:62:F5:A9:66:0A:E6:13:C2:84:E7:0E:E8:11:59:AC:54:83:17:50:69:2A:C4:88:1D:2E:91:B7:DA:BC:A2:0D:B6:12:A4:BF:38:9B:C4:80:8F:7A:09:5A:9D:F8:B8:77:64:0D:57:BA:FC:72:D3:F5:2B:6E:C2:12:40:81:6C:0B:DA:7E:3A:DE:FD:66:D5:0A:C7:25:FB:57:FB:C7:D6:60:56:F3:12:96:29:C6:90:FB:D7:6B:D7:07:A1:42:E8:70:11:1D:B4:AB:33:C8:DD:A5:53:49:DF:87:F9:1D:5E:77:1B:02:14:03:FE:40:48:68:5D:B3:88:B8:69:5B:C9:5D:64:2A:4E:DA:22:43:EE:B7:D2:0E:3F:93:C0:91:9D:FA:5C:E3:B8:73:11:34:61:2B:E2:CD:38:22:9E:1D:D0:6F:07:9F:51:72:5B:BD:67:41:97:62:56:44:76:53:65:68:BA:5F:8F:81:B4:1D:2E:F0:A2:55:2F:57:35:CC:97:EF:22:07:69:5D:C7:E7:4E:B7:39:6C:4B:A3:E3:DC:BE:A2:E6:59:26:24:75:52:44:49:DE:EA:A5:FD:5D:B6:35:B6:03:44:F8:CE:6E:9F:94:A2:6E:9C:C6:E6:35:0B:A9:2D:50:65:1D:85:B9:7A:8A:36:6D:2D:F3:DA:7C:48:A7:27:E5:D9:E3:47:9A:04:43:E2:89:6F:B6:5E:91:02:3E:57:70:9E:B4:22:26:FF:C4:C3:1A:B6:57:23:72:F5:2E:FE:6F:3F:36:54:3B:3F:78:8F:B9:16:FC:1B:25:55:78:13:49:82:E3:21:0A:37:2E:6D:9E:CF:EB:59:9A:B5:E8:4F:47:5A:99:FF:95:7C:3A:2C:C6:A4:89:76:DC:A9:F8:BF:DF:92:4B:21:35:9B:4B:E4:16:8C:27:9C:80:DE:3A:BA:B7:6E:21:53:84:2F:E5:3C:C4:21:E4:D2:58:11:53:87:82:44:C8:3E:16:20:93:42:7C:E7:A4:D7:1D:CE:DD:DA:D5:7D:05:94:3A:3E:A3:0D:E2:BB:4C:B1:0E:02:81:AC:EE:33:EE:EE:C6:E3:0E:E7:76:6C:05:C2:E2:86:8D:08:2F:36:9E:A4:D5:29:79:8B:53:C3:E6:67:99:3B:73:BD:9B:BB:FC:31:A3:AF:39:4D:F8:4B:D8:DA:2A:DE:F1:8F:31:1F:D6:05:90:F1:96:60:12:3A:75:BA:4F:63:02:03:01:00:01

Authority Info Access

http://pkiroot.multicert.com/cert/root001.cer

http://ocsp.multicert.com/ocsp

Subject Key Identifier *DC:90:0C:D9:8D:4A:2A:94:7B:52:BB:40:B4:3F:13:7A:DE:A8:2E:96*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: https://pki.multicert.com

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Extended Key Usage *id_kp_timeStamping*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E8:62:7A:C2:36:18:3A:42:0E:15:13:83:9A:CE:EE:F8:33:D2:7A:45:51:27:17:A9:BA:FD:E8:50:6B:B5:C1:CF*

X509SubjectName

Subject CN: *MULTICERT Timestamping Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *3JAM2Y1KKpR7UrtAtD8Tet6oLpY=*

Service Status

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

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

Status Starting Time

2020-03-29T23:00:00Z

5.15 - Service (recognisedatnationallevel): MULTICERT Advanced Certification Authority 005

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

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

Service Name

Name *[en]* *MULTICERT Advanced Certification Authority 005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *119320829196114557397712571397601614592*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHRTCCBS2gAwIBAgIQWcRbFU1JOnTHZpj9sVnbADANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBF
bGVjdHLDs25pY2EgUy5BLjEyMDAGA1UEAwwpTVVMVEIDRVlUIFJvb3Qgb2VydGlmaWNhdGlvbiBB
dXRob3JpdHkgMDEwHhcNMTkxMjA5MTgzNTI0WhcNMzIwNjA4MTgzNTI0WjCBrDELMAkGA1UEBhMC
UFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVj
dHLDs25pY2EgUy5BLjEgMB4GA1UECwwXQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxNzA1BgNVBAMM
LkC1VTFRJQ0VSVCBBZHZhbnNlZCBDZXJ0aWZpY2F0aW9uIEF1dGhvcmI0eSAwMDUwggIMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDJdwhqCFVHwsN1E04CQR0+6AkJtCYlEwCimhQm1dhRjESl
fB1Fn6g96AU+lZskd2tegq0558uZLBE5n4NGAlscOPDGI2k99I90Od+jPR/AQ28pqambjmYeXH+0
BKWisp8iKJwGjLlz6lV+HbO9VOqZfoqpy+diZN7u/E91evsUzN5+SLhA8WiaZCE+lJF5byAlhs8w
Kix6dzxRyWMGTlbuxP29Je/80LCTaKredgeAtM7Lpn5McivEcZ/nNqf37vZCZyTN8uiLdyKNU3K5
Tzfn+Jxmxraua+TKUZjmH7UtPNn5CPb20toeckPlSPhaEpRYpL49K9v1rSSQch27ICqiwNdli650
WVYPgMqgH+2kclgBs/XQiwJsk+HZyQUKh8BmJ6CoorP+OgDgMVOzJCa72jtFCHdwGcUAu4eqBMXp
HpHBPnU3gxEgytUx4thQzqnc00Q9FkiHgaBZlI6iXwib69Zn213sYs5DfN5zVAzXeYIfu1OeDSVw
WVRDneq8WPUbnYfecW/6DOMPMeBCAH2Ye8c2/cIgDkNXOZYpQgatyh++pWs05kLUyzTO1tOt7jXL
eBoIuIwyJDTLE8t3BfLjHRXfbN81h9XjCyCmFrsvTy7QTEg9nCktwpdgR4s0Qhm4sCSwo2qUXMOx
oWL0GxfWZQS1WesYK5Bj0uRpSm1u5wIDAQABo4IBhjCCAYIwdQYIKwYBBQUHAQEEaTBnMDkGCCsG
AQUFBzAChi1odHRwOi8vcGtpcm9vdC5tdWx0aWNlcnQuY29tL2NlcnQvcm9vdDAwM55jZXIwKgYI
KwYBBQUHMAGGHmh0dHA6Ly9vY3NwLm11bHRpY2VydC5jb20vb2NzcDAdBgNVHQ4EFgQUVbqXmCUR
hMmuMtD7nFY6iC4z+swEqYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBTVORycW28EqgKV
TO8g3Sl0pMVFcTBDBgNVHSAEPDA6MDgGDSsGAQQBgcNuAQEBAAcwJzAlBggrBgEFBQcCARYZaHR0
cHM6Ly9wa2kubXVsdGljZXJ0LmNvbTBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vcGtpcm9vdC5t
dWx0aWNlcnQuY29tL2NybC9yb290X21jX2NybC5jcmwwDgYDVR0PAQH/BAQDAgEGMB0GA1UdJQQW
MBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQsFAAOCAgEANnqbDxXmvXPVZDufqsJ
MHaNF8/yhJVUXS4khgb8X4qWk1uEoB56zmWuUQxizyREDGbW77Wy7O1hKxBVzRfpVzLBehEzFUR2
Yj9Cfc029rq4TDXU4y1aziTOS0eiYECTihViYefMB+oPKA8kacn0/pBgC40THDxP8YneJwjajdPu
zPmPYVWtZ0X7Q7eTTIpmRyO+U7SU0oALVmdhQ8BMrtM+oxg2ZsswmYBE01828ykNbtjdkXIHiQQd
NupKsox3unDuK7XH5PdhZAocTTunIj7NVxxI/bX8L55pNWBnq10RZvcS0ISoSejxWUpCI55plE2
IjONfAujS/VdSjBNJFeyXRozVFI0EYOBdJTqfvwqlsvR6jDiTw4U3pz2RSHE/rp9Arentagst3lA
R6FU62PMhu4oaeLI1g1SDt7ouhP4Q0rcqpvwTzlQGYQSIA28vwo3YGGzMjvhlqtfnKgIdZMQvAIx
hfmP9KZYjmSjwNN1W8542xC72Fro7BK1AGr+CeueHIDNM/qX9lA9L+JiOfZQ2tDrebbfeLtHrjlV
G9YfOY7wQZY+ZCroGMtAcHPToonsaz59I8nkCghUW3IDpSpymZXEaaiDYRHRvvG7SoqyWP2edGl
454RIWnfbz7/wAHnU0gIAs7hDbzZjw+TbTUPMRZZ2CCVS38Pul6217Y=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Advanced Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Dec 09 19:35:24 CET 2019*

Valid to: *Tue Jun 08 20:35:24 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:C9:77:08:6A:08:55:47:C2:C3:75:13:4E:02:41:1D:3E:E8:09:09:B4:26:25:13:00:A2:9A:14:26:D5:D8:51:8C:44:88:7C:1D:45:9F:A8:3D:E8:05:3E:95:9B:24:77:6B:5E:82:AD:12:E7:CB:99:2C:11:39:9F:83:46:02:5B:1C:38:F0:C6:97:69:3D:F6:5F:74:39:DF:89:3D:1F:C0:43:6F:29:A9:A9:9B:8E:66:1E:5C:7F:B4:04:A5:A2:B2:9F:22:28:9C:06:8C:B9:73:EA:5B:FE:1D:B3:BD:54:EA:99:7E:8A:A9:CB:E7:62:64:DE:EE:FC:4F:75:7A:FB:14:CC:D4:BE:48:B8:40:F1:68:9A:64:21:3E:94:91:79:6F:20:25:86:CF:30:2A:2C:7A:77:3C:51:C9:63:06:4C:86:EE:C4:FD:BD:25:EF:FC:D0:B0:93:68:AA:DE:76:07:80:B4:CE:CB:A6:7E:4C:72:2B:C4:71:9F:E7:36:A7:F7:EE:F6:42:67:24:CD:F2:E8:8B:77:22:8D:53:72:B9:4F:37:E7:F8:9C:66:C6:B6:AE:6B:E4:CA:51:98:E6:1F:B5:2D:3C:D9:F9:70:F6:F6:D2:DA:1E:72:43:C8:4B:F8:5A:12:94:58:A4:BE:3D:2B:DB:F5:AD:24:90:72:1D:BB:88:2A:A2:C0:D7:65:8B:AE:74:59:56:0F:80:CA:AA:1F:ED:A4:72:58:01:B3:F5:D0:8B:02:6C:93:E1:D9:C9:05:0A:87:C0:66:27:A0:A8:A2:B3:FE:3A:00:E0:31:53:B3:24:26:BB:DA:3B:45:08:77:70:19:C5:00:B8:87:AA:04:C5:E9:1E:91:C1:3E:75:37:83:11:20:CA:D5:31:E2:D8:50:CE:A9:DC:D3:44:3D:16:48:87:81:A0:59:96:5E:A2:5F:08:9B:EB:D6:67:DB:5D:EC:62:CE:43:7C:DE:73:54:0C:D7:79:89:5F:B8:53:9E:0D:25:70:59:54:43:9D:EA:BC:58:F5:1B:9D:B7:DE:71:6F:FA:0C:E3:0F:31:E0:42:00:7D:98:78:C7:36:FD:C2:20:0E:43:57:39:96:29:42:A6:AD:CA:1F:BE:A5:6B:34:4A:42:D4:CB:34:D0:D6:D3:AD:EE:35:CB:78:1A:25:B8:8C:32:24:34:CB:13:CB:77:05:FD:63:1D:15:DF:6C:DF:35:B7:DC:49:0B:20:A6:16:BB:2F:4F:2E:D0:4C:4A:BD:9C:29:2D:C2:97:60:47:8B:34:42:19:B8:B0:24:B0:A3:6A:94:5C:C3:B1:A1:62:F4:1B:17:D6:65:04:B5:59:EB:18:2B:90:63:D2:E4:69:4A:6D:6E:E7:02:03:01:00:01

Authority Info Access

http://pkiroot.multicert.com/cert/root001.cer

http://ocsp.multicert.com/ocsp

Subject Key Identifier

55:BA:97:98:25:11:84:C9:A2:32:D0:FB:9C:56:3A:88:2A:F8:CF:EB

Basic Constraints

IsCA: true - Path length: 0

Authority Key Identifier

D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: https://pki.multicert.com

CRL Distribution Points

http://pkiroot.multicert.com/crl/root_mc_crl.crl

Extended Key Usage

id_kp_clientAuth

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

24:ED:D4:E5:03:A8:D3:FD:B5:FF:B4:AF:66:C8:87:35:99:01:CB:E6:87:A5:A0:76:0D:10:A0:8E:ED:99:A7:C3

X509SubjectName

Subject CN:

MULTICERT Advanced Certification Authority 005

Subject OU:

Certification Authority

Subject O:

MULTICERT - Serviços de Certificação Electrónica S.A.

Subject C:

PT

X509SKI

X509 SK I

VbqXmCURhMmiMtD7nFY6iCr4z+s=

Service Status

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

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

Status Starting Time

2020-03-29T23:00:00Z

5.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.15.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.16 - Service (recognisedatnationallevel): MULTICERT SSL Certification Authority 005

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

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

Service Name

Name *[en]* *MULTICERT SSL Certification Authority 005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *644350331733086556621586211437006193 01*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHQDCCBSigAwIBAgIQMHm8aY18HMhRjPMtMBxAJTANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBF
bGVjdHLDs25pY2EgUy5BLjEyMDAGA1UEAwwpTVVMVEIDRVJUIFJvb3QgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkgMDEwHhcNMTkxMjA5MTgzNTAwWhcNMzIwNjA4MTgzNTAwWjCBpzELMAkGA1UEBhMC
UFQxQjBABgNVBAoMOU1VTFRJQ0VSVCAtIFNlcnZpw6dvcyBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVj
dHLDs25pY2EgUy5BLjEgMB4GA1UECwwXQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxMjAwBgNVBAMM
KU1VTFRJQ0VSVCBTU0wgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMDA1MIICjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAv/kI5Ci7PPqpPzhQTmLB0zyqRthCsp+PyuIGlMB6OICfBWC1h8OS
/3Dt4zQtfiqto7E2qZbvqh4I+MP5wr6dlpUAsrsI0Ox8OPkKpZ6UXxCOiGdy2/Q3xkKd29ad9B0G
3sDYf+Wr0imUT0pgcUjUgWq76uXEbft4xFeKTKGPsf6bmCGXcFP5R62kgkV/tDJYeHTy0mJQjUc/
TqlEhGUKnam/w4iSxxZXiy9jBUZAkOeZLaW2GKux2ezMRW/SIwSVWWI5UffjfZhZD86KWvg64d1R
KlUYje6EehIxFdhCIFFBOjaHMrbKjwO4+Ilv7oH3uGAeUmAKgfrVeNGcrzS0B0ayRQ4tYAUm9psmd
4A9QCECenIz2RT8ySBCjnnIRGDtNCAtV3oTr2mAoEewdOi4tXgAXTvG/Y8EhWi8BpiDaol0z2gA1
tlpYt/d1ABpKjagIKgMZOSyw1gyUolwkArhs62M9QdpTgYH1hDS64+VNzlIF3nJD61Io0yugtg1I
VXlnUqNGryds6WEYNIF5JyafyHvXHX19cVZGoXw7nRFnbBLURHuBjA5HCGSBuBYm8POgvzDXqFvG
ydDfqt8VvO7eYHqjozH26h9hk3FcqHLVYKdjl9t8ZvgPR7sSHYCRAIApGIDcheMLZTInsf3zVSv
/OB1QGjOAjKcrGN+AhV0IzsCAwEAAaOCAYYwggGCMHUGCCsGAQUFBwEBBGkwZzA5BggrBgEFBQcw
AoYtaHR0cDovL3BraXJvb3QubXVsdGljZXJ0LmNvbS9jZXJ0L3jvb3QwMDEuY2VyMCoGCCsGAQUF
BzABhh5odHRwOi8vb2NzcC5tdWx0aWNlcnQuY29tL29jc3AwHQYDVR0OBBYEFCWgATKqynejer7n
ijpEixm1TUgtMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAU1TkcnFtvBKgilUzvfN0p
dKTFRXEwQwYDVR0gBDwwOjA4Bg0rBgEEAYHDbgEBAQAHMCcwJQYIKwYBBQUHAgEWGWh0dHBzOi8v
cGtpLm11bHRpY2VydC5jb20wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3BraXJvb3QubXVsdGlj
ZXJ0LmNvbS9jcmwvcm9vdF9tY19jcmwuY3JsMA4GA1UdDwEB/wQEAwIBBjAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAGaKemvkxPn+FWuOJFRoA1WHr5eY
ruXe7ALRM9khmHqSCbs+Cycnqoosy QQpxSoRzAmWjSs4jlxOBkYRwSBcp+ohpc7mBf91BRWfTYgd
rApurgmbzq95no907ywp6unYSegbDbsYEDrwaEGxw6H9i0ewhs+FAPiDrVnkcg9rXPdSdzkNoaBv
dIFIC91ezYZ7iLiloJh7KCNb0pch0ZCUAofwMOfzkvQP6h9Sdg8488PicWV5YkZAf+xdqjPDEi
t5s+gwRsosua7jaBweiWoz2m59JrsnzTWLzcIYS2M8N/TqlW98j0z5P5D0XYaG3nLwoIV4wV1H1Z
uX0bE76beeZCNKIvaCFbu+so1rAc8p9gGvwKs67AhYwTXIMuue4O9Rrv+Cd9N//WdCKIwL6MkoM1
R4YbQLk0y4C1cEqeKDCfU3XyvCHtQ7vTmPlo1HOcqrtTdAShNje0aJVwo+iPL1tw3RGBvdEpwCfv
R631od0znVs1ncNKxlGOnYgBVdvNrFLVZlLSAkLp9F51vGxdGvds5uMYCB/jkTy4fY9zXchvZwEl
cw0PRWCloelcU8vmbatJoY9Ygen9WYEJpPgXYwuFR6TSBpftHLWh04ZmeOYkwATPDwOFSJkwYPmv
fF0b6ZgfZp13dYr5aJj1qgjNmLEs7oJJpeK1Sr60lQaEoio

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT SSL Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Mon Dec 09 19:35:00 CET 2019*

Valid to: *Tue Jun 08 20:35:00 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:BF:F9:25:E4:28:BB:3C:FA:A9:3F:38:50:4E:62:C1:D3:3C:AA:46:D8:42:B2:9F:
8F:CA:E2:46:24:C0:7A:3A:50:9F:F1:60:B5:87:C3:92:FF:70:ED:E3:34:2D:7E:5A:AD:A3:B1:36:A9:96:EF:AA:1E:25:F8:C3:D2:C2:BE:9D:22:95:00:82:BB:08:D0:EC:7C:38:F9:0A:A5:9E:94:5
F:10:8E:88:67:72:DB:F4:37:C6:42:9D:DB:D6:9D:F4:1D:06:DE:C0:D8:7F:E5:AB:D2:29:94:4F:4A:6A:71:48:D4:81:6A:BB:EA:E5:C4:6D:FB:78:C4:57:8A:4C:A1:8F:B1:FE:9B:98:21:97:70:53
:F9:47:AD:A4:AA:45:7F:B4:32:58:78:74:F2:D2:62:50:8D:47:3F:4E:A9:44:84:65:0A:9D:A9:BF:C3:88:92:C7:16:57:8B:2F:63:05:46:40:90:E7:99:2D:A5:B6:18:AB:B1:D9:EC:CC:45:6F:D2:9
7:04:95:59:69:79:51:F9:63:7D:98:59:0F:CE:8A:5A:F8:3A:E1:DD:51:2A:55:18:25:EE:84:7A:12:31:15:D8:42:88:51:41:3A:36:87:32:B6:CA:8F:03:B8:F8:8B:FB:A0:7D:EE:18:07:94:98:02:A
0:7E:B5:5E:34:67:2B:CD:2D:01:D1:AC:91:43:8B:58:01:49:95:A6:C9:9D:E0:0F:50:08:40:9E:9E:5C:F6:45:3F:32:48:10:A3:9E:72:11:18:3B:4D:08:08:55:DE:84:EB:DA:60:28:11:EC:1D:3A
:2E:2D:5E:00:17:4E:F1:BF:63:C1:21:5A:2F:01:A6:20:DA:A2:5D:33:DA:00:35:B6:5A:58:B7:F7:75:00:1A:4A:8D:AA:89:2A:A3:19:39:2C:B0:D6:0C:94:A0:8C:24:02:B8:6C:EB:63:3D:41:DA:
53:A9:81:F5:84:34:BA:E3:E5:4D:CE:59:45:DE:72:43:EB:59:68:D3:2B:A0:B6:0D:48:55:79:67:52:A3:46:AF:27:6C:E9:61:18:34:81:79:27:26:9F:C8:7B:D7:1D:7D:7D:71:56:46:A1:7C:3B:9
D:11:67:6C:12:D4:44:78:81:8C:0E:47:08:64:81:B8:16:26:F0:F3:A0:BF:30:D7:A8:5B:C6:C9:D0:DF:AA:DF:15:BD:0E:FF:79:81:EA:8E:8C:C7:DB:A8:7D:86:4D:C5:72:01:CB:55:82:9D:8C:8
F:6D:F1:9B:E0:3D:1E:EC:48:76:02:44:02:00:A4:62:03:72:17:8C:2D:94:C8:9E:C7:F7:CD:54:AF:FC:E0:75:40:68:CE:02:32:9C:AC:63:7E:02:15:74:23:3B:02:03:01:00:01*

Authority Info Access

http://pkiroot.multicert.com/cert/root001.cer

http://ocsp.multicert.com/ocsp

Subject Key Identifier *25:A0:01:32:AA:CA:77:A3:7A:BE:E7:8A:3A:44:8B:19:B5:4D:48:2D*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: https://pki.multicert.com

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Extended Key Usage *id_kp_serverAuth*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:E1:F1:B8:DB:DD:05:D8:AD:04:F2:CA:8A:73:42:F4:61:D9:9D:79:E7:B4:66:D4:92:84:B1:90:9C:28:E2:D8*

X509SubjectName

Subject CN: *MULTICERT SSL Certification Authority 005*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *JaABMqrKd6N6vueKOkSLGbVNSC0=*

Service Status

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

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

Status Starting Time

2020-03-29T23:00:00Z

5.16.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.17 - Service (deprecatedatnationallevel): MULTICERT Advanced Certification Authority 001

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

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

Service Name

Name *[en]* *MULTICERT Advanced Certification Authority 001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4197759556185954571*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHjzCCBQ+gAwIBAgIIOkFwE173GQswDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlBUMUIw
QAYDVQQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNlhw6fDo28gRWxlY3Ryw7Nu
aWNhlFMuQS4xMjAwBgNVBAMMKU1VTFRJQ0VSVCBSb290IENlcnRpZmlj YXRpb24gQXV0aG9yaXR5
IDAxMB4XDTE3MTIxMjE1NTQ1NVoXDTMwMDYxMjE1NTQ1NVowgawxCzAJBgNVBAYTAlBUMUIwQAYD
VOQKDDlNVUxUSUNFUlQgLSBTZXJ2acOnb3MgZGUgQ2VydGlmaWNhw6fDo28gRWxlY3Ryw7NuaWNh
lFMuQS4xIDAeBgNVBAsMF0NlcnRpZmlj YXRpb24gQXV0aG9yaXR5MTcwNQYDVQQDDC5MVUxUSUNF
UlOgQWR2YW5jZWQgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMDAxMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAztHJZ6rpvfZRljD01TtenETToUp1/mWsB4cfUU5iZf5RfJhiTiivhKvf
13R2cPz7ArGj0UVK7OGsUNR+iyVw+BePEJMgMqUL238KrDMb5MhBjF8Gwiq6qUeKSCJlcylySzxk
+xYChamtqZrRdoRxr8r3EGOMQdpG8NCTLYL+OCVVI4GkplMXZT/YZTEAUiyXiRH9gYvD9brnGmF
eKM9EpcDHQq3NsN7eXCJCwXKdKVuHzxoocqB0CyUe7v5jGzEEDF/Rc82DCvJzcDzkYnfaSQh/Bzf
iaSEWz3e+CLFj2zt1rH3tJs6L7rLUuTDoegHgCatg2KlDhRrfOwjXoUGe8VUxmZ8KHrIO038ESru
o4W2ePloRPSgqUb05Jj/dVqdzmo4EvlawP2nxmWHnXrSNcephghkifsPEO5YAcmlm6AIX/QZeBlr
k2WuUmkZG+q2vpR0fa0p7r4g9b7MFrfUqejzLrz5wQyd3e5whtsvE9Q3h24sTVlyC4mIWNK6Mz+sk1
ckFZLtPMNOpG0iKFZ9fq6OI90MiYpQNERZ25uosYv/9GlghnGg8gaGbKOs+Ct4YqCLZm+jAinxMy
73Rf8wyrNTRo8Ijaj43B+gWJh7T2qq/FXDIylZUd33ZsjEZsLnkCvmbR7NRH5gl4x4tjT45VDe+vB
Qw+KWG6h/aOFu6K4p78CAwEAAaOCAXAwggFsMDoGCCsGAQUFBwEBBC4wLDAqBggrBgEFBQcwAYYe
aHR0cDovL29jc3AubXVsdGljZXJ0LmNvbS9vY3NwMB0GA1UdDgQWBBRbK+nW0ZOdgQk+cTZfpp33
Ph2n3DASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNU5HJxbbwSqopVM7yDdKX5KxUVx
MIGGBgNVHSAEfzB9MDwGDSsGAQQBgcNuAQEBAAcwKzApBggrBgEFBQcCARYdaHR0cDovL3BraXJv
b3QubXVsdGljZXJ0LmNvbS8wPQYOKwYBBAGBw24BAQEAAQIwKzApBggrBgEFBQcCARYdaHR0cDov
L3BraXJvb3QubXVsdGljZXJ0LmNvbS8wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL3BraXJvb3Qu
bXVsdGljZXJ0LmNvbS9jcmwvcm9vdF9tY19jcmwuY3JsMA4GA1UdDwEB/wQEAwIB8jANBgkqhkiG
9w0BAQsFAAOCAgEAcnXQ5fC5pz6hSmwa3aqkXOLUWJgA3fCsOBD0pWE4SeQCucw1m3iPb4EVlgq9
8wBM/M3icEb3g556fNnY+DWa4MRAXPjowpZzuhOMxcuyecfqPQuHwTD5xsSNzgblEODCYX6F8Gzk
1lD9L/Nm8mYUYgU/UaWvErZGm5TUZ5DfD2M7irV2DrZanV4RS1IlwuM1MumqJmJYT0SNQGhYzOfb
0wsCOKirvqvpLpx3K+UWxAz0Vl/78JjTfN1wjayhh7ji32MOhbDIxGik+jnvmrFjkq77e+FhySP
x0If/ULnzzn/6z0RT2x491HjldOMurgdBdVm79oBhhsxfjXy8pIhOcfVxjtvuBmyMwJ77BFpCBS6
ifQJddyy1o9QlpBbOppWUX9fhUethU44EYdCvjN3r2lYGLZ/ihtJvr7cHYjWka4tdj8gJqC436GN
zTbGFoNHP6xCyGZYBJuS6P2GcVf8iWagOEyhPZZFPe+jKQQw+LyYRr+YOfnKuRWlUCdOkEbVFFj
zKB0bhCDOGOb4In497IHIr02oCvC5swfQ+fRQG4RnTk5RAoFzsowyZApOVExUBTqMPHRHX1+U4
hUYn9+v5c8dOVF50DK3NkeEPZN//Ele4T9G/zz6O37KfbIGg8BIOWAi99xLa/1AKJ7TGhdNjTDOd
HXKPk0hIUIZd5CU=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *MULTICERT Root Certification Authority 01*

Issuer O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Issuer C: *PT*

Subject CN: *MULTICERT Advanced Certification Authority 001*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

Valid from: *Tue Dec 12 16:54:55 CET 2017*

Valid to: *Wed Jun 12 17:54:55 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:CE:D1:C9:67:AA:E9:BD:F6:51:22:30:F4:D5:3B:5E:9C:44:D3:A1:4A:75:FE:65:AC:07:87:1F:51:4E:48:65:FE:51:7C:98:62:4E:58:AF:84:AB:DF:D7:74:76:70:FC:FB:02:B1:A3:D1:45:4A:EC:E1:AC:50:D4:7E:8B:25:70:F8:17:8F:10:93:20:32:A5:0B:DB:7F:0A:AC:33:1B:E4:C8:41:8C:5F:06:C2:2A:BA:A9:47:8A:48:22:65:73:29:72:4B:3C:64:FB:16:02:85:A9:AD:A9:9A:D1:76:84:71:AF:CA:F7:10:6D:0C:D1:DA:46:F0:D0:93:2D:82:FE:38:25:55:97:81:A4:A6:53:17:65:3F:D8:65:31:00:52:2B:C9:5E:24:47:F6:06:2F:0F:D6:EB:9C:69:B5:78:A3:3D:12:97:03:1D:0A:87:36:C3:7B:79:70:B9:0B:05:CA:74:A5:6E:1F:3C:68:A1:CA:81:D0:2C:94:7B:BB:F9:8C:6C:C4:10:31:7F:45:CF:36:0C:2B:C9:CD:C0:F3:91:89:DF:69:24:21:FC:1C:DF:89:A4:84:5B:3D:DE:F8:22:C5:8F:6C:ED:D6:B1:F7:B4:9B:3A:2F:BA:CB:52:E4:C3:A1:E8:07:80:26:AD:83:62:A5:0E:14:6B:7C:EC:23:5E:85:06:7B:C5:54:C6:66:7C:28:7A:C8:3B:4D:FC:11:2A:EE:A3:85:B6:78:F2:28:44:F4:A0:A9:46:F4:E4:92:7F:75:5A:9D:CE:6A:38:12:F9:5A:C0:FD:A7:C6:65:87:9D:7A:D2:35:C7:A9:86:A8:64:89:FB:0F:10:EE:58:01:C9:A5:9B:A0:08:5F:F4:19:78:19:6B:93:65:AE:52:69:19:1B:EA:B6:BE:94:74:7D:AD:29:EE:BE:20:F5:BE:CC:16:B7:D4:A9:E8:F3:2E:BC:D2:C0:EC:9D:DD:EE:70:1E:CB:C4:F5:0D:C7:DB:8B:13:56:5C:82:E2:65:8D:2B:A3:33:FA:C9:35:72:41:59:2E:D3:CC:34:EA:46:D2:22:85:67:D7:EA:E8:E2:3D:D0:C8:98:A4:E3:44:45:9D:B9:BA:8B:18:BF:FF:46:96:08:67:1A:0F:20:68:66:CA:3A:CF:82:B7:86:2A:08:B6:66:FA:30:22:9F:13:32:EF:74:5F:F3:0C:AB:35:34:68:F0:96:A3:E3:70:7E:81:62:61:ED:3D:AA:AB:F1:57:0C:9C:A5:65:47:77:DD:9B:23:11:9B:0B:9E:40:AF:99:B4:7B:35:11:F9:AA:5E:31:E2:D8:D3:E3:95:43:7B:EB:C1:43:0F:8A:58:6E:A1:FD:A3:85:BB:A2:B8:A7:BF:02:03:01:00:01

Authority Info Access *http://ocsp.multicert.com/ocsp*

Subject Key Identifier *5B:2B:E9:D6:D1:94:1D:81:09:3E:71:36:5F:A6:9D:F7:3E:1D:A7:DC*

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

Authority Key Identifier *D5:39:1C:9C:5B:6F:04:AA:A2:95:4C:EF:20:DD:29:74:A4:C5:45:71*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.7

CPS pointer: http://pkiroot.multicert.com/

Policy OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2

CPS pointer: http://pkiroot.multicert.com/

CRL Distribution Points *http://pkiroot.multicert.com/crl/root_mc_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EF:72:A0:54:69:1F:85:5D:52:A3:19:88:43:9B:75:BD:E4:9F:03:89:9A:DF:0E:BC:14:2C:B9:6E:34:83:D6:F7*

X509SubjectName

Subject CN: *MULTICERT Advanced Certification Authority 001*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *Wyvp1tGUHYEJPnE2X6ad9z4dp9w=*

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

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

Status Starting Time *2026-02-25T12:30:00Z*

5.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.17.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.17.3 - History instance n.1 - Status: recognisedatnationallevel

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

Service Name

Name *[en]* *MULTICERT Advanced Certification Authority 001*

Service digital identities

X509SubjectName

Subject CN: *MULTICERT Advanced Certification Authority 001*

Subject OU: *Certification Authority*

Subject O: *MULTICERT - Serviços de Certificação Electrónica S.A.*

Subject C: *PT*

X509SKI

X509 SK I *Wyvp1tGUHYEJPnE2X6ad9z4dp9w=*

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

Status Starting Time *2020-05-19T23:00:00Z*

5.17.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

5.17.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

6 - TSP: British Telecommunications plc

.

TSP Name

Name	*[en]*	*British Telecommunications plc*
Name	*[pt]*	*British Telecommunications plc*

TSP Trade Name

Name	*[en]*	*British Telecommunications plc*
Name	*[en]*	*British Telecommunications plc*
Name	*[en]*	*VATPT-507015851*

PostalAddress

Street Address	*[en]*	*BT Trust Service, P.O. Box 641,*
Locality	*[en]*	*Cardiff*
State Or Province	*[en]*	*Cardiff*
Postal Code	*[en]*	*CF1 1YL*
Country Name	*[en]*	*UK*

PostalAddress

Street Address	*[pt]*	*BT Trust Service, P.O. Box 641,*
Locality	*[pt]*	*Cardiff*
State Or Province	*[pt]*	*Cardiff*
Postal Code	*[pt]*	*CF1 1YL*
Country Name	*[pt]*	*UK*

ElectronicAddress

URI	*[en]*	*mailto:support@trustwise.com*
URI	*[en]*	*http://www.globalservices.bt.com/*

TSP Information URI

URI	*[en]*	*http://www.globalservices.bt.com*

6.1 - Service (withdrawn): BT/DigitalSign (CA-Qualified Certificates)

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]* *BT/DigitalSign (CA-Qualified Certificates)*

Name *[pt]* *BT/DigitalSign (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *129306905431624887482487812001666232948*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFkDCCBHigAwIBAgIQYUeap4Wb5VWhWJkplyTydDANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQG
EwJHOjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMR8wHQYDVQQLExZW
ZXJpU2InbiBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExJCVCBDbGFzcyAylENBlC0gRzIwHhcNMDgw
ODE0MDAwMDAwWhcNMTUwODEzMjM1OTU5WjCCATIxCzAJBgNVBAYTAkdCMScwJQYDVQQKEx5Ccml0
aXNoIFRlbGVjb21tdW5pY2F0aW9uczBwbGMxPjA8BgNVBAs7NlUx5QSAtIERpZ2l0YWxTaWduIENl
cnRpZmljYWRvcmEgRGlnaXRhbCAoUFQ1MDcwMTU4NTEpMR8wHQYDVQQLExZWZXJpU2InbiBUcnVz
dCBOZXR3b3JrMTwwOgYDVQQLEzNUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudHJ1c3R3aXNl
LmNvbS9ycGEgKGMpMDgxNTAzBgNVBAs7LENsYXNzIDIgTWFuYWdlZCBQ50kgSW5kaXZpZHVhbCBT
dWJjY3JpYmVlIENBMSQwIgYDVQQDExtCVC9EaWdpdGFsU2InbiBRdWFsaWZpZWQgQOEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+iZFQlNPEI3EQnTaBQDNLbBZlHTM30wExetq/Zt/h
YBHL0PVbThxzgVaLj/YJvCOVV+UfnpmRlnZGyO9pyCbo0uqxOwVWX9L+B3/4SwrKOleLFYClNPrd
Ryd3aBG4MVCüaTzcuto1xgJpTczHLv4pi7OeNw9zlRiXDMbz+o9LchNaIF3fFFrTp7mTaAg5it8Q
Mcj+hVeMDsUQF+FajfI0vFAdltDEtbC1h/ixptE4xYplMAR0St6D3zNrxbNybL4+nzjfbMgMdmjh
1CqOGiLBqe6hokqBf4IP9aLBmnNfwTmfY1tiKEDZuXZfpS2TvA5OzZAIhOTcs9oRuYXxLGExAgMB
AAGjggFcMIIBWDASBgNVHRMBAf8ECDAGAQH/AgEAMHIGA1UdIARrMGkwZwYLYIZlAYb4RQEHFwIw
WDApBggrBgEFBQcCARYdaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9jcHMwKwYIKwYBBQUHAgIw
HxodaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9ycGEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDov
L29uc2l0ZWNvbC50cnVzdHdpc2UuY29tLDJUQ2xhc3MyQDEtRzluY3JsMA4GA1UdDwEB/wQEAwIB
BjARBglghkgBhvhCAQEEBAMCAQYwKAYDVR0RBCEwH6QdMBsxGTAXBgNVBAMTEGJ0MjA0OGMyUHVi
MS0yMDIwHQYDVR0OBBYEFKGDcho9np8i5t6Cx5DJUQH/gylrMBBGA1UdIwQYMBaAFGg7BXz93s3m
2wjKO9lOJD07V7P0MA0GCSqGSIb3DQEBBQUAA4IBAQAmK5Ztsjx5bduPflMp1thpGHj7PGbXW3To
Yk8n2C9QLX9kZ4fZ1sUXmpX/+uF31/ibs6KlmdwofMccjNw9W28vszeC+Elm/rYATneAIQWa3Cg
5yL9lyKD65gmuuapc3bqTb7BOGJldbiFsgX6MXvC8zvmQyb+1AYOrqmCwVHaTQmCJ+XpxlPbybJl
naWWxQkxCARtD4QjjhBg5C/bYaC9pqrPYaKs2UlYNWeL1ee7hXeWnEqNYG4k2WsEq7NYcArELdnw
hLC8h0K0mXgqaCbQ6OaRbLrc1Xe+B72M/FXPkSqEtLPsTzzYy8a84IQj9VhDb/qnydMMBJYX6eSj
el2v
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *BT Class 2 CA - G2*

Issuer OU: *VeriSign Trust Network*

Issuer O: *British Telecommunications plc*

Issuer C: *GB*

Subject CN: *BT/DigitalSign Qualified CA*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Terms of use at https://www.trustwise.com/rpa (c)08*

Subject OU: *VeriSign Trust Network*

Subject OU: *LRA - DigitalSign Certificadora Digital (PT507015851)*

Subject O:	*British Telecommunications plc*
Subject C:	*GB*
Valid from:	*Thu Aug 14 02:00:00 CEST 2008*
Valid to:	*Fri Aug 14 01:59:59 CEST 2015*
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:BE:89:91:50:94:D3:C4:23:71:10:9D:36:81:40:33:4B:6C:16:65:1D:33:37:D3:01:31:7A:DA:BF:66:DF:E1:60:11:CB:D0:F5:58:4E:1C:73:81:56:8B:8F:F6:09:BC:23:95:57:E5:21:36:99:91:96:76:46:C8:EF:69:C8:26:E8:D2:EA:B1:3B:05:56:5F:D2:FE:07:7F:F8:4B:0A:CA:38:87:8B:15:80:88:34:FA:DD:47:27:77:68:11:B8:31:50:AE:69:3C:DC:BA:DA:35:C6:A2:69:4D:CC:C7:2E:FE:29:8B:B3:9E:37:0F:73:21:18:97:0C:C6:F3:FA:8F:4B:72:13:5A:94:5D:DF:14:5A:D3:A7:B9:93:68:08:39:8A:DF:10:31:C8:FE:B5:57:8C:0E:C5:10:17:E1:5A:25:F2:34:BC:50:1D:96:D0:C4:B5:B0:B5:87:F8:81:A6:D1:38:C5:8A:65:30:04:74:4A:DE:83:DF:33:6B:C5:B3:72:6C:BE:3E:9F:32:5F:6C:C8:0C:76:68:E1:D4:2A:8E:1A:22:C1:81:EE:A1:A2:4A:81:7F:82:0F:F5:A2:C1:9A:B3:5F:C1:39:9F:63:5B:62:28:40:D9:B9:76:5F:A5:2D:93:BC:04:8E:CD:90:08:84:E4:DC:B3:DA:11:B9:85:F1:2C:61:31:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.trustwise.com/cps* *CPS text: [https://www.trustwise.com/rpa]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/BTClass2CA-G2.crl*
Subject Alternative Name	*CN=bt2048c2Pub1-202*
Subject Key Identifier	*A1:83:72:1A:3D:9E:9F:22:E6:DE:82:C7:90:C9:51:01:FF:83:29:6B*
Authority Key Identifier	*6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C3:B8:33:EF:F2:FD:D5:6F:6F:B2:6B:68:61:53:4D:D7:81:45:D6:01:90:31:41:93:4B:04:2B:B3:BC:BE:51:0B*

X509SubjectName

Subject CN:	*BT/DigitalSign Qualified CA*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Terms of use at https://www.trustwise.com/rpa (c)08*
Subject OU:	*VeriSign Trust Network*
Subject OU:	*LRA - DigitalSign Certificadora Digital (PT507015851)*
Subject O:	*British Telecommunications plc*
Subject C:	*GB*

Service Status

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

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

Status Starting Time *2016-06-30T23:59:59Z*

6.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

6.1.2 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *BT/DigitalSign (CA-Qualified Certificates)*

Name *[pt]* *BT/DigitalSign (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *BT/DigitalSign Qualified CA*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Terms of use at https://www.trustwise.com/rpa (c)08*

Subject OU: *VeriSign Trust Network*

Subject OU: *LRA - DigitalSign Certificadora Digital (PT507015851)*

Subject O: *British Telecommunications plc*

Subject C: *GB*

X509SKI

X509 SK I *oYNyGj2enyLm3oLHkMlRAf+DKWs=*

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

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

6.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

6.1.3 - History instance n.2 - Status: accredited

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

Service Name

Name [en] BT/DigitalSign (CA-Qualified Certificates)

Name [pt] BT/DigitalSign (EC-Certificados Qualificados)

Service digital identities

X509SubjectName

Subject CN: BT/DigitalSign Qualified CA

Subject OU: Class 2 Managed PKI Individual Subscriber CA

Subject OU: Terms of use at https://www.trustwise.com/rpa (c)08

Subject OU: VeriSign Trust Network

Subject OU: LRA - DigitalSign Certificadora Digital (PT507015851)

Subject O: British Telecommunications plc

Subject C: GB

X509SKI

X509 SK I oYNyGj2enyLm3oLHkMlRAf+DKWs=

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

Status Starting Time 2009-04-22T23:00:01Z

6.2 - Service (deprecatedatnationallevel): DigitalSign (LRA in Portugal)

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

Service type description [en] *A registration service that verifies the identity and, if applicable, any specific attributes of a subject for which a certificate is applied for, and whose results are passed to the relevant certificate generation service.*

Service Name

Name *[en]* *DigitalSign (LRA in Portugal)*

Name *[pt]* *DigitalSign (Entidade de Registo em Portugal)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *129306905431624887482487812001666232948*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFkDCCBHigAwIBAgIQYUeap4Wb5VWhWJkplyTydDANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQG
EwJHQjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMR8wHQYDVQQLExZW
ZXJpU2InbiBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExJCVCBDbGFzcyAyIENBIC0gRzIwHhcNMDgw
ODE0MDAwMDAwWhcNMTUwODEzMjM1OTU5WjCCATIxCzAJBgNVBAYTAkdCMScwJQYDVQQKEx5Ccml0
aXNoIFRlbGVjb21tdW5pY2FQaW9ucyBwbGMxPjA8BgNVBAsTNUx5QSAtIERpZ2l0YWxTaWduIENl
cnRpZmljYWRvcmEgRGlnaXRhbCAoUFQ1MDcwMTU4NTEpMR8wHQYDVQQLExZWZXJpU2InbiBUcnVz
dCBOZXR3b3JrMTwwOgYDVQQLEzNUZXItcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudHJ1c3R3aXNl
LmNvbS9ycGEgKGMpMDgxNTAzBgNVBAsTLENsYXNzIDIgTWFuYWdlZCBQ5DkgSW5kaXZpZHVhbCBT
dWJzY3Ip YmVyIENBMSQwIgYDVQQDExtCVC9EaWdpdGFsU2InbiBRdWFsaWZpZWQgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+iZFQlNPEI3EQnTaBQDNLbBZlHTM30wExetq/Zt/h
YBHL0PVbThxzgVaLj/YjvCOVV+UfiNpmRlnZGyO9pyCbo0uqxOwVWX9L+B3/4SwrKOleLFYClNPrd
Ryd3aBG4MVCua7zcuto1xqJpTczHLv4pi7OeNw9zIRiXDMbz+o9LchNalF3fFFrTp7mTaAg5it8Q
Mcj+hVeMDsUQF+FajfI0vFAdltDEtbC1h/ixptE4xYpIMAR0St6D3zNrxbNybL4+nzjfbMgMdmjb
1CqOGiLBge6hokqBf4IP9aLBmrNfwTmfY1tiKED2uXZfpS2TvASOzZAIhOTcs9oRuYXxLGExAgMB
AAGjggFcMIIBWDASBgNVHRMBAf8ECDAGAQH/AgEAMHIGA1UdIARrMGkwZwYLYIZIAYb4RQEHFwIw
WDApBggrBgEFBQcCARYdaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9jcHMwKwYIKwYBBQUHAgIw
HxodaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9ycGEwOQYDVR0fBDowODA2oDSgMoYwaHR0cDov
L29uc2l0ZWNybC50cnVzdHdpc2UuY29tL0JUQ2xhc3MyQ0EtRzIuY3JsMA4GA1UdDwEB/wQEAwIB
BjARBglghkgBhvhCAQEEBAMCAQYwKAYDVR0RBCEwH6QdMBsxGTAXBgNVBAMTEGJ0MjA0OGMyUHVi
MS0yMDIwHQYDVR0OBBYEFKGDcho9np8i5t6Cx5DJUQH/gyIrMB8GA1UdIwQYMBaAFGq7BXz93s3m
2wjKO9lQDD7U7P0MA0GCSqGSIb3DQEBBQUAA4IBAQAmK5Ztsjx5bduPflMp1thpGHj7fGbXW3To
Yk8n2C9QLX9kZ4lfZ1sUXmpX/+uF31/ibs6KlmdwofMcqJNw9W28vszeC+Elm/rYATneAIQWa3Cq
5yL9lyKD65gmuuapc3bqTb7BOGJldbiFsgX6MXvC8zvmQyb+1AYOrqmCwVHaTQmCJ+XpxlPbybJl
naWWxQkxCArtD4QjjhBgSC/bYaC9pqrPYaKs2UlYNWeL1ee7hXeWnEqNYG4k2WsEq7NYcArELdnw
hLC8h0K0mXgqaCbQ6OaRbLrc1Xe+B72M/FXPkSqEtLPsTzzYy8a84lOj9VhDb/qnydMMBJYX6eSj
el2v

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *BT Class 2 CA - G2*

Issuer OU: *VeriSign Trust Network*

Issuer O: *British Telecommunications plc*

Issuer C: *GB*

Subject CN: *BT/DigitalSign Qualified CA*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Terms of use at https://www.trustwise.com/rpa (c)08*

Subject OU: *VeriSign Trust Network*

Subject OU: *LRA - DigitalSign Certificadora Digital (PT507015851)*

Subject O: *British Telecommunications plc*

Subject C: *GB*

Valid from: *Thu Aug 14 02:00:00 CEST 2008*

Valid to: *Fri Aug 14 01:59:59 CEST 2015*

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:BE:89:91:50:94:D3:C4:23:71:10:9D:36:81:40:33:4B:6C:16:65:1D:33:37:D3:01:31:7A:DA:BF:66:DF:E1:60:11:CB:D0:F5:5B:4E:1C:73:81:56:8B:8F:F6:09:BC:23:95:57:E5:21:36:99:91:96:76:46:C8:EF:69:C8:26:E8:D2:EA:B1:3B:05:56:5F:D2:FE:07:7F:F8:4B:0A:CA:38:87:8B:15:80:88:34:FA:DD:47:27:77:68:11:B8:31:50:AE:69:3C:DC:BA:DA:35:C6:A2:69:4D:CC:C7:2E:FE:29:8B:B3:9E:37:0F:73:21:18:97:0C:C6:F3:FA:8F:4B:72:13:5A:94:5D:DF:14:5A:D3:A7:B9:93:68:08:39:8A:DF:10:31:C8:FE:B5:57:8C:0E:C5:10:17:E1:5A:25:F2:34:BC:50:1D:96:D0:C4:B5:B0:B5:87:F8:B1:A6:D1:38:C5:8A:65:30:04:74:4A:DE:B3:DF:33:6B:C5:B3:72:6C:BE:3E:9F:32:5F:6C:C8:0C:76:68:E1:D4:2A:8E:1A:22:C1:81:EE:A1:A2:4A:81:7F:82:0F:F5:A2:C1:9A:B3:5F:C1:39:9F:63:5B:62:28:40:D9:B9:76:5F:A5:2D:93:BC:04:8E:CD:90:08:84:E4:DC:B3:DA:11:B9:85:F1:2C:61:31:02:03:01:00:01

Basic Constraints

IsCA: true - Path length: 0

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.trustwise.com/cps

CPS text: [https://www.trustwise.com/rpa]

CRL Distribution Points

http://onsitecrl.trustwise.com/BTClass2CA-G2.crl

Subject Alternative Name

CN=bt2048c2Pub1-202

Subject Key Identifier

A1:83:72:1A:3D:9E:9F:22:E6:DE:82:C7:90:C9:51:01:FF:83:29:6B

Authority Key Identifier

6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

C3:B8:33:EF:F2:FD:D5:6F:6F:B2:6B:68:61:53:4D:D7:81:45:D6:01:90:31:41:93:4B:04:2B:B3:BC:BE:51:0B

X509SubjectName

Subject CN:

BT/DigitalSign Qualified CA

Subject OU:

Class 2 Managed PKI Individual Subscriber CA

Subject OU:

Terms of use at https://www.trustwise.com/rpa (c)08

Subject OU:

VeriSign Trust Network

Subject OU:

LRA - DigitalSign Certificadora Digital (PT507015851)

Subject O:

British Telecommunications plc

Subject C:

GB

Service Status

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

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

Status Starting Time

2016-06-30T23:59:59Z

Scheme Service Definition URI

URI *[en]* *http://www.digitalsign.pt*

6.2.1 - History instance n.1 - Status: recognisedatnationallevel

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

Service Name

Name	*[en]*	*DigitalSign (LRA in Portugal)*
Name	*[pt]*	*DigitalSign (Entidade de Registo em Portugal)*

Service digital identities

X509SubjectName

Subject CN:	*BT/DigitalSign Qualified CA*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Terms of use at https://www.trustwise.com/rpa (c)08*
Subject OU:	*VeriSign Trust Network*
Subject OU:	*LRA - DigitalSign Certificadora Digital (PT507015851)*
Subject O:	*British Telecommunications plc*
Subject C:	*GB*

X509SKI

X509 SK I	*oYNyGj2enyLm3oLHkMlRAf+DKWs=*

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

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

6.2.2 - History instance n.2 - Status: undersupervision

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

Service Name

Name	*[en]*	*DigitalSign (LRA in Portugal)*
Name	*[pt]*	*DigitalSign (Entidade de Registo em Portugal)*

Service digital identities

X509SubjectName

Subject CN:	*BT/DigitalSign Qualified CA*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Terms of use at https://www.trustwise.com/rpa (c)08*
Subject OU:	*VeriSign Trust Network*
Subject OU:	*LRA - DigitalSign Certificadora Digital (PT507015851)*
Subject O:	*British Telecommunications plc*
Subject C:	*GB*

X509SKI

X509 SK I	*oYNyGj2enyLm3oLHkMlRAf+DKWs=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2009-04-22T23:00:01Z*

7 - TSP: DigitalSign - Certificadora Digital

.

TSP Name

Name	*[en]*	*DigitalSign - Certificadora Digital*
Name	*[pt]*	*DigitalSign - Certificadora Digital*

TSP Trade Name

Name	*[en]*	*DigitalSign - Certificadora Digital, S.A.*
Name	*[pt]*	*DigitalSign - Certificadora Digital, S.A.*
Name	*[en]*	*VATPT-507015851*
Name	*[en]*	*British Telecommunications plc*
Name	*[en]*	*DigitalSign Certificadora Digital*
Name	*[en]*	*DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*

PostalAddress

Street Address	*[en]*	*Largo Pe. Bernardino Ribeiro Fernandes, 26*
Locality	*[en]*	*Nespereira - Guimarães*
State Or Province	*[en]*	*Guimarães*
Postal Code	*[en]*	*4835-489 Nespereira - Guimarães*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Largo Pe. Bernardino Ribeiro Fernandes, 26*
Locality	*[pt]*	*Nespereira - Guimarães*
State Or Province	*[pt]*	*Guimarães*
Postal Code	*[pt]*	*4835-489 Nespereira - Guimarães*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:geral@digitalsign.pt*

URI *[en]* *http://www.digitalsign.pt/ECDIGITALSIGN/cps/*

TSP Information URI

URI *[en]* *http://www.digitalsign.pt/ECDIGITALSIGN/cps/index_en.jsp*

URI *[pt]* *http://www.digitalsign.pt/ECDIGITALSIGN/cps/index.jsp*

7.1 - Service (withdrawn): DigitalSign Qualified 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.*

Service Name

Name *[en]* *DigitalSign Qualified CA*

Name *[pt]* *Digitalsign (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *502642120162434749938532431808470763 5*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFUTCCBDmgAwIBAgIQA8gNst29Izdf7G1q4Y41MzANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQG
EwJHOjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMR8wHQYDVQQLExZW
ZXJpU2InbiBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExjCVCBDbGFzcyAyIENBICDgRzlwHhcNMDqw
NjEzMDAwMDAwWhcNMTgwNjExMjM1OTU5WjCB9DELMAkGA1UEBhMCUFQxLDAgBgNVBAoTI0RpZ2l0
YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYDVQQLExZWZXJpU2InbiBUcnVzdCBO
ZXR3b3JrMTwwOgYDVQQLEzNUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNv
bS9ycGEgKGMpMDIgxNTAzBgNVBAsTLENsYXNzIDIgTWFuYWdlZCBQ50kgSWSkaXZpZHVhbcBTdWJz
Y3JpYmVyIENBMSEwHwYDVQQDExhEaWdpdGFsU2InbiBRdWFsaWZpZWQgQ0EwggEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCnpbFC+LeXCigYZLRotgC295f7W60aeRSiVTNE5CgeP7qk2R/z
+GjRMLXn9hcy8/92fjqTn9CMenyzsr/wE1Ki0vcE73SSLOvMKsyVn5yFt2UJ5RpmUloC743HsPlv
8Xdy1k7iuj+4W3+hIXsyA9o7OSbJmWMI8x2avSg28ocpCsOmtTTakvSqJC3Q33hOomF/MSXEzAEo
SNuNQwJWux1Z2YTlunJb4B7g6zKGvPWGB5tof6/MIo53IRRgofaG9S8o3xZgZgMaaBQ4aOjRMvE0
kORa+L4j6gxqE/Tizzr/n//V/6UedE9kYyijQejb1XsDg4bmApvIAnZ3INeP4hHZAgMBAAGjggFc
MIIBWDAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8C
AQAwKAYDVR0RBCEwH6QdMBsxGTAXBgNVBAMTEGJ0MjA0OGMyUHVlM50yMDEwHQYDVR0OBBYEFLsf
RB3sIveq9SvyjyOQWfiymSCqMHIGA1UdIARrMGkwZwYLYIZIAYb4RQEHFwIwWDApBggrBgEFBQcC
ARYdaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9jcHMwKwYIKwYBBQUHAgIwHxodaHR0cHM6Ly93
d3cudHJ1c3R3aXNlLmNvbS9ycGEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL29uc2l0ZWNybC50
cnVzdHdpc2Uuy29tL0JlUQ2xhc3MyQ0EtRzluY3JsMB8GA1UdIwQYMBaAFGq7BXz93s3m2wjKO9lO
JD07V7P0MA0GCSqGSIb3DQEBBQUAA4IBAQB2uiu2wtZWS+HL10IE0FtBRSmLRKbKIagFNWEOIfX7
QoqK6nJnYAUheCzwMg77USCc0ivzwRyNvbY6U9V5eRdw6Ppcfcj77sIO1d0boOczioOg8ywmnRPF
d7CZcQp7WQIh/W57H1k8qcUwKrCcjOCW+JDz5d4tjHe3aFLsjNwjGHyUq25Fes1WFDfMc3EHq3M2
YXHSOUgjIGVnW3TeURVCURos6hxqUF24957YDYfwZQyY9EqFWLPlsytaCwcG7w0HbqJUL12IiIAHv
HtGoXNtvYNptuGbwfRhs8wgswoe3hthBXGFSnwkMCdEaj/ZZIGgIcGH2ex0gtPdu5Ruhr5Jw

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *BT Class 2 CA - G2*

Issuer OU: *VeriSign Trust Network*

Issuer O: *British Telecommunications plc*

Issuer C: *GB*

Subject CN: *DigitalSign Qualified CA*

Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Terms of use at https://www.trustwise.com/rpa (c)08*
Subject OU:	*VeriSign Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*
Valid from:	*Fri Jun 13 02:00:00 CEST 2008*
Valid to:	*Tue Jun 12 01:59:59 CEST 2018*
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:A5:B1:42:F8:B7:97:0A:28:18:64:B4:68:B6:00:B6:F7:97:FB:5B:AD:1A:79:14:A2:55:33:44:E4:28:1E:3F:BA:A4:D9:1F:F3:F8:68:D1:30:B5:E7:F6:17:32:F3:FF:76:7E:3A:93:9F:D0:8C:7A:7C:B3:B2:BF:F0:13:52:A2:D2:F7:04:EF:74:92:2C:EB:CC:2A:CC:95:9F:9C:85:B7:65:09:E5:1A:66:52:5A:02:EF:8D:C7:B0:F2:2F:F1:77:72:D6:4E:E2:BA:3F:B8:5B:7F:A1:21:7B:32:03:DA:3B:41:26:C9:99:63:08:F3:1D:9A:BD:28:36:F2:87:29:0A:C3:A6:B5:34:DA:92:F4:AA:24:2D:D0:DF:78:50:A2:61:7F:31:25:C4:CC:01:28:48:DB:8D:43:02:56:BB:1D:59:CD:84:C8:BA:78:DB:E0:1E:E0:EB:32:86:BC:F5:86:07:98:68:7F:AF:CC:22:8E:77:21:14:60:A1:F6:86:F5:2F:28:DF:16:60:66:03:1A:68:14:38:68:E8:D1:32:F1:34:90:E4:5A:F8:BE:23:EA:AC:6A:13:F4:E2:CF:3A:FF:9F:FF:D5:FF:A5:1E:74:4F:64:63:28:89:39:E2:5B:D5:7B:03:83:86:E6:02:9B:C8:02:76:77:20:D7:8F:E2:11:D9:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Alternative Name	*CN=bt2048c2Pub1-201*
Subject Key Identifier	*BB:1F:44:1D:EC:22:F7:A0:F5:2B:F2:8F:23:90:59:F8:B2:99:20:AA*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.trustwise.com/cps* *CPS text: [https://www.trustwise.com/rpa]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/BTClass2CA-G2.crl*
Authority Key Identifier	*6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*84:FA:E8:C3:AE:EB:CA:60:60:50:BC:11:48:7F:EC:E7:46:4C:12:10:A4:E6:EA:F2:61:CE:CB:01:36:81:BC:AB*

Service Status

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

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

Status Starting Time

2018-06-11T23:59:59Z

Scheme Service Definition URI

URI	*[en]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*
URI	*[pt]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*

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

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.44.2*

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]* *DigitalSign Qualified CA*

Name *[pt]* *Digitalsign (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign Qualified CA*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Terms of use at https://www.trustwise.com/rpa (c)08*

Subject OU: *VeriSign Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *ux9EHewi96D1K/KPI5BZ+LKZIKo=*

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 [QCQSCDStatusAsInCert, QCStatement, QCForESig]

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.44.2*

7.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.1.4 - History instance n.2 - Status: undersupervision

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

Service Name

Name *[en]* *DigitalSign Qualified CA*

Name *[pt]* *Digitalsign (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign Qualified CA*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Terms of use at https://www.trustwise.com/rpa (c)08*

Subject OU: *VeriSign Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *ux9EHewi96D1K/KPI5BZ+LKZIKo=*

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

Status Starting Time *2011-12-19T00:00:01Z*

7.1.4.3 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.44.2*

7.2 - Service (withdrawn): DigitalSign TSA (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.*

Service Name

Name *[en]* *DigitalSign TSA (Qualified TSA)*

Name *[pt]* *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *83530414347578653836659220680697836552*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFGTCCBAGgAwIBAgIQPtdfZGlWUoqJ3zrqYEX0CDANBgkqhkiG9w0BAQUFADCB9DELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2I0YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLEx2WZXJpU2lnbiBUcnVzdCBOZXR3b3jrMTww0gYDVQQLEzNUZXJtcyBvZiB1c2UgYXQgaHR0
cHM6Ly93d3cudHJ1c3RaXNlLmNvbS9ycGEgKGMpMDgxNTAzBgNVBAsTLENsYXNzIDIgTWFuYWdl
ZCBQS0kgSW5kaXZpZHVhbCBTdWJzY3JpYmVyIENBMSEwHwYDVQQDExhEaWdpdGFsU2lnbiBRdWFs
aWZpZWQgQ0EwHhcNMTIwNjI3MDAwMDAwWhcNMTgwNjExMjM1OTU5WjBVMQswCQYDVQQGEwJQVDEs
MCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJQaWZpY2Fkb3JhIERpZ2I0YWwxGDAWBgNVBAMTD0Rp
Z2I0YWxTaWduIFRTQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN+4C31C5k3s/BfC
rCpVxgTmmzBsdJktBT7f0N6UXqN/+ct3/048bbqpfvW455J8D5qRN6hkz32Ec4jC3WVpCjnxP+E
Xl/dj6bBq5nEXRg+Bn+tvz/2377T1WzYLI+tiP4397RhXiRCtcNlwOnnObRSPk3OkMe584N1q3d8
+BzjcOdvaZ6ls+2yhGk3KO2Z2Pg+gjDJH98AmP9PE/TRIXHWljXT4gz7TKkEYWOYtawO4LNngcls
PReFgICs+AgSULbj1OuN1m5TCJ2YDZ0b4trMpl2XY26vrlsnYQKgBcJm2LqCHZNVxl/4tt620Ioh
SkkOzkavr16WqW37G+8kp80CAwEAAaOCAUMwggEMAwGA1UdEwEB/wQCMAAwVAYDVR0gBE0wSzBJ
BgtghkgBhvhFAQcXAjA6MDgGCCsGAQUFBwIBFixodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9F
Q0RJR0lUQUxTSUdOL2NwczBxBgNVHR8EajBoMGagZKBihmBodHRwOi8vb25zaXRlY3JsLnRydXN0
d2lzZS5jb20vRGlnaXRhbFNpZ25DZXJQaWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmlIZENlcnRpZmlj
YXRlL0xhdGVzdENSTC5jcmwwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBTk7wHOjFbq1kDl4BTW
EgM16Jyo0TAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAWgBS7H0Qd7CL3oPUr8o8j
kFn4spkggjANBgkqhkiG9w0BAQUFAAOCAQEALIKgofl89pm+B70cTwBX5Z6U1+6wgus8hef9xmwp
uRQKQ2d9tNwMfjMZXt+jYynO/am/YDN3qvrOHLmVqGZdrsuydsTKVEb+6ssInjuEoDA9oUfcOrN
k7QOojgeZrVDO7Duatw6rjDPSG767twLWVItaL+mXgVFQiIfejIDtRBOZFBr5ijz2+XrqjjPNTy
4Og9TT4SzUOkFrpjt36BD03pzAUVP3NccNlVqpQwebkuleovJ/Cso6BtyZn/paMVLiecg1ip23HE
UDQqNJarXzAtPwmWVUp7pL8+CGkWLSgyl/fHGJbEF0Ki1OQg3fzvkmTi3KdJhBDLf+YkbWg9cQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *DigitalSign Qualified CA*

Issuer OU:	*Class 2 Managed PKI Individual Subscriber CA*
Issuer OU:	*Terms of use at https://www.trustwise.com/rpa (c)08*
Issuer OU:	*VeriSign Trust Network*
Issuer O:	*DigitalSign - Certificadora Digital*
Issuer C:	*PT*
Subject CN:	*DigitalSign TSA*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*
Valid from:	*Wed Jun 27 02:00:00 CEST 2012*
Valid to:	*Tue Jun 12 01:59:59 CEST 2018*
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:DF:B8:0B:7D:42:E6:4D:EC:FC:17:C2:AC:2A:55:C6:04:E6:AE:7C:C1:B1:D2:64:7C:14:FB:7F:43:7A:51:7A:8D:FF:E7:2D:DF:FD:38:F1:B6:EA:A5:FB:D6:E3:9E:49:F0:34:AA:44:DE:A1:93:3D:F6:11:CE:23:0B:75:95:A4:28:E7:C4:FF:84:5C:8F:DD:8F:A6:C1:AB:99:C4:5D:18:3E:06:7F:AD:BF:3F:F6:DF:BE:D3:D5:6C:D8:2C:8F:AD:88:FE:37:F7:B4:61:5E:24:42:B5:C3:48:C0:E9:E7:39:B4:52:3E:4D:CE:90:C7:B9:F3:83:75:AB:77:7C:F8:1C:E3:70:E7:6F:69:9E:88:B3:ED:B2:84:69:37:28:ED:99:D8:FA:BE:82:30:C9:1F:DF:00:98:FF:4F:13:F4:D1:21:71:D6:96:35:D3:E2:0C:FB:4C:A9:04:61:63:98:B5:AC:0E:E0:B3:67:81:C2:2C:3D:17:85:80:80:AC:F8:0A:92:50:B6:E3:D4:EB:8D:D6:6E:53:08:9D:98:0D:9D:1B:E2:DA:CC:A6:5D:97:63:6E:AF:AE:5B:27:61:02:AA:05:C2:66:D8:BA:82:1D:93:55:C6:5F:F8:B6:DE:B6:38:8A:21:4A:49:0E:CE:46:AF:AF:5E:96:A9:6D:FB:1B:EF:24:A7:CD:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificate/LatestCRL.crl*
Subject Key Identifier	*E4:EF:01:CE:8C:56:E0:D6:40:E5:E0:14:D6:12:03:35:E8:9C:A8:D1*
Extended Key Usage	*id_kp_timeStamping*
Authority Key Identifier	*BB:1F:44:1D:EC:22:F7:A0:F5:2B:F2:8F:23:90:59:F8:B2:99:20:AA*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*56:84:FB:DE:60:03:55:56:FE:34:67:8E:A5:2E:5F:5E:42:CD:3C:AC:F1:61:9A:BF:B0:A8:AE:C7:E3:7D:B5:1E*

Service Status

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

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

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI [en] *https://www.digitalsign.pt/ECDIGITALSIGN/cps*

URI [pt] *https://www.digitalsign.pt/ECDIGITALSIGN/cps*

7.2.1 - History instance n.1 - Status: undersupervision

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

Service Name

Name [en] *DigitalSign TSA (Qualified TSA)*

Name [pt] *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *5O8BzoxW4NZA5eAU1hIDNeicqNE=*

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

Status Starting Time *2013-06-21T00:00:01Z*

7.3 - Service (withdrawn): DigitalSign TSA - G2 (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.*

Service Name

Name [en] *DigitalSign TSA - G2 (Qualified TSA)*

Name [pt] *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *119699217490681307043009295385993682 88*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIF+TCCBOGgAwIBAgIQCQFStOb9/Bp5UMn1VuM2YDANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2I0YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGF2cyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBICQgRzIwHhcNMTMxMDMxMDAwMDAwWhcNMTkxMDMwMjM1OTU5WjB7MQswCQYDVQQGEwJQVDEs
MCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZpY2Fkb3JhIERpZ2I0YWwxHzAdBgNVBAsTFlN5
bWFudGVjIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMTFERpZ2I0YWxTaWduIFRTQSAtIEcyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvH+Na4N+aBBjzTt46fnW63iN4kEwj01JydNjBW7V
k9nNboiD85Dxk8OV19VwWd2ryrMM3TG3MwM1cDBRPlWsOAsm16BMNYvtDastB014y1u6jUJeNTk8
cwmuHmBNY+Q4kt+NNzlrtgwetLbe36B1FWDYfTGwe4vqy5l7n47UnwpQHeYgBbIMLKZ4HF4A3Mrq
aazjggwFCXAYNpguNNtZWEUARoWWhLdpUel5oPwO7zlb9PoD2MlO3YTPyUpT0uAEVd6uGFjQhCa8
rAMyLqKcp0XsUWOnebFse43h6V17qF14ZuQwm0l58Zj8RLtzxI7JMNHHrG4VCwY5SenkziXk2QID
AQABo4ICNjCCAjIwDgYDVR0PAQH/BAQDAgbAMCIGCCsGAQUFBwEDBBYwFDAIBgYEAI5GAQEwCAYG
BACORgEEMB0GA1UdDgQWBBQnhvIl8YQ6aGsfMhnmt9GRsJ69KTAMBgNVHRMBAf8EAjAAMIIBHwYD
VR0gBIIBFjCCARIwggEOBgtghkgBhvhFAQcXAjCB/jA4BggrBgEFBQcCARYsaHR0cHM6Ly93d3cu
ZGlnaXRhbHNpZ24ucHQvRUNESUdJVEFMU0lHTi9jcHMwOgYIKwYBBQUHAgIwLhosaHR0cHM6Ly93
d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdJVEFMU0lHTi9ycGEwgYUGCCsGAQUFBwICMHkad0luIGV2
ZW50IG9mIGEgY29uZmxpY3QgYmV0d2VlbiB0aGUgdGVybXMgb2YgQlQgQ1BTIGFuZCB0aGUgdGVy
bXMgb2YgRGlnaXRhbFNpZ24gQ1BTLCB0aGUgdGVybXMgb2YgQlQgQ1BTIHNoYWxsIGNvbnRyb2wu
MHMGA1UdHwRsMGowaKBmoGSGYmh0dHA6Ly9vbnNpdGVjcmwudHJ1c3R3aXNlLmNvbS9EaWdpdGFs
U2lnbkNlcnRpZmlj YWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHMi9MYXRlc3RDUkwu
Y3jsMBYGA1UdIQEB/wQMMAoGCCsGAQUFBwMIMB8GA1UdIwQYMBaAFCjt5T2CrVmXEUFsILOwSrjZ
iRR5MA0GCSqGSIb3DQEBCwUAA4IBAQCHg+x+oHvI96icfdV4sLY6Fd+aaxVRU7smb6nExRCPTnt+
qwtMc9gHSet+ioEdwtF6SasJLgTHn5MExBqVAfuKAGVhBYdZr59a6sjb23DIxqpovP35Xt4TRSzF
va+dBrSq/9MxOlBcdvaGYes8Xb+IIlZWpzm8ZgK/XsmFPWoasIM5CQ/CunbZolGp6y5mtCGzTmen
bfuOD8kF3z33mEon55khnkg4qTdPFkKC1E9+f7OS6UiTyo6VsN5yjyXaLH96KOsh4BKFrWO4SaUI
C9hCHufrTICeJpC1VsE8K2OdaeEUAENKsLyCzjx/IAouHeXKZ9M0SNq1VbXgX7c2tPHN

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G2*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G2*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Thu Oct 31 01:00:00 CET 2013*

Valid to: *Thu Oct 31 00:59:59 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:BC:7F:8D:6B:83:7E:68:10:63:CD:3B:78:E9:F9:D6:EB:78:8D:E2:41:30:8F:4D:
49:C9:D3:49:05:6E:D5:2B:D9:CD:6E:88:C3:F3:90:F1:90:13:95:D7:D5:70:59:DD:AB:CA:B3:0C:DD:31:B7:33:03:35:70:30:51:3C:85:AC:D0:0B:26:D7:A0:4C:35:8B:ED:0D:AB:2D:F3:4D:7
8:C8:8B:BA:8D:42:5E:35:39:3C:73:09:AE:1E:60:4D:63:E4:38:92:DF:BD:37:39:6B:B6:0C:1E:B4:B6:DE:DF:A0:75:15:60:D8:7D:31:B0:7B:8B:E0:CB:99:7B:9F:8E:D4:9F:0A:50:1D:E6:20:0
5:B8:8C:2C:A6:78:1C:5E:00:DC:CA:EA:69:AC:E3:82:0C:05:09:70:18:36:98:2E:34:DB:59:58:45:00:46:85:96:84:B7:69:51:E9:79:A0:FC:0E:EF:39:5B:F4:FA:03:D8:C9:4E:DD:84:CF:C9:4A:
53:D2:E0:04:55:DE:AE:18:58:D0:84:26:BC:AC:03:32:2E:A2:9C:A7:45:EC:51:63:A7:79:B1:6C:7B:8D:E1:E9:5D:7B:A8:5D:78:66:E4:30:9B:42:39:F3:68:FC:44:BB:73:C6:5E:C9:30:D1:C7:A
C:6E:15:0B:06:39:49:E9:E4:CE:25:E4:CD:02:03:01:00:01
```


QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

Subject Key Identifier *27:86:F9:48:F1:84:3C:68:6B:1F:32:19:A6:B7:D1:91:B0:9E:BD:29*

Basic Constraints *IsCA: false*

Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]* *CPS text: [In event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl*
Extended Key Usage	*id_kp_timeStamping*
Authority Key Identifier	*28:ED:49:3D:82:AD:59:97:11:41:6C:94:B3:B0:4A:B2:59:89:14:79*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*08:9F:1A:E9:8E:B6:F3:20:A9:E1:DC:89:7D:D2:F8:87:FE:2E:97:EF:91:12:43:5D:B8:06:7A:57:62:ED:6A:38*

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

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

Status Starting Time *2020-01-28T11:26:25Z*

Scheme Service Definition URI

URI	*[en]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*
URI	*[pt]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*

7.3.1 - History instance n.1 - Status: granted

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

Service Name

Name	*[en]*	*DigitalSign TSA - G2 (Qualified TSA)*
Name	*[pt]*	*Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign TSA - G2*
Subject OU:	*Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *J4b5SPGEPGhrHzIZprfRkbCevSk=*

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

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

7.3.2 - History instance n.2 - Status: withdrawn

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

Service Name

Name *[en]* *DigitalSign TSA - G2 (Qualified TSA)*

Name *[pt]* *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G2*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *J4b5SPGEPGhrHzIZprfRkbCevSk=*

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

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

7.3.3 - History instance n.3 - Status: undersupervision

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

Service Name

Name	*[en]*	*DigitalSign TSA - G2 (Qualified TSA)*
Name	*[pt]*	*Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign TSA - G2*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*J4b5SPGEPGhrHzlZprfRkbCevSk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2014-02-06T00:00:01Z*

7.4 - Service (withdrawn): DigitalSign TSA - G2 (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.*

Service Name

Name	*[en]*	*DigitalSign TSA - G2 (Qualified TSA)*
Name	*[pt]*	*Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*154868363469230800929269397163666099011*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGZzCCBU+gAwIBAgIQdIKP1IfLRJ5uHelZl7TLQzANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAgBgNVBAoTI0RpZ2lOYWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzIwHhcNMTQxMDE1MDAwMDAwWhcNMjAxMDE0MjM1OTU5WjB7MQswCQYDVQQGEwJQVDEs
MCoGA1UECChMjRGlnaXRhbFNpZ24gLSBDZXj0aWZpY2Fkb3JhIERpZ2l0YWwxHzAdBgNVBAsTFlN5
bWFudGVlIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMTFERpZ2l0YWxTaWdulFRTQSAtIEcyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4z5iBVwsYki9BhFOYXfZyO0BwSqwCnsYh0xbv7O8
qmev8Cj+u8J+3wsBffFoM7zNb3uS9G3V97AVkqVlQHyexsctbIdSuPVvkxgG250UQ8F2SQI07bcK
8qhlI7VAPRmyelcUxlrvE9RaDCCXeWftxxbhJcig1Bode382N6ZSVRe2EPNDF/n5Z7AWXthai5Lj
EHDGXQOn5v3gsOYKj9CH7Ib5WUCh1VReZBWH5wPDx9vhrEtwMl91xNIv50E/Pf6FYhBENQasYkRbd
mPndH2icbUmDnbJbFZn2ByZ 67myZ6gNeg85TowjZ8q6IGyjOOuz+DmMU5qWleKq3RqKno6HniQlD
AQABo4ICpDCCAqAwggEkBgNVHSAEggEbMIIBFzCCARMGC2CGSAGG+EUBBxcCMIIBAjA4BggrBgEF
BQcCARYsaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9jcHMwOgYIKwYB
BQUHAgIwLhosaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9ycGEwgYkG
CCsGAQUFBwICMH0ae0ulHRoZSBldmVudCBvZiBhIGNvbmZsaWN0IGJldHdlZW4gdGhlIHRlcm1z
IG9mIEJlIENQUyBhbmQgdGhlIHRlcm1zIG9mIERpZ2l0YWxTaWdulENQUywgdGhlIHRlcm1zIG9m
IEJlIENQUyBzaGFsbCBjb250cm9sLjBzBgNVHR8EbDBqMGigZq8khmJodHRwOi8vb25zaXRlY3Js
LnRyZXN0ZXIzZS5jb20vRGlnaXRhbFNpZ25DZXj0aWZpY2Fkb3JhIGlnaXRhbFF1YWxpZmllZENl
cnRpZmlj YXRlRzlvTGF0ZXN0Q1JMLmNybDAOBgNVHQ8BAf8EBAMCBsAwIqYIKwYBBQUHAQMEFjAU
MAgGBgQAjkYBATAIBgYEAI5GAQQwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
CDBnBgNVHREEYDBepFwwWjELMAkGA1UEBhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWduIC0gQ2Vy
dGlmaWNhZG9yYSBEaWdpdGFsMR0wGwYDVQQDExREaWdpdGFsU2lnbiBUU0EgLSBHMjAdBgNVHQ4E
FgQUQo1YZfuDY574VXe2u55yIY9zF34wHwYDVR0jBBgwFoAUKO1JPYKtWZcRQWyUs7BKSlmJFHkw
DQYJKoZIhvcNAQELBQADggEBAAZGbd0lHFuminDirOOpsNHbv89DjjWRgHBfrwkN+xsu37JEeoD2
nBD5u6Or99P09iwaOM/ioWZD4cAgqm8T/qpyfTLEf5+X4q7jZUisZdvg6NKwAZimsdOP49lStRvF
Fk3qeRFPKiW5fDZKCBpkbA1PSM75gf5MC/uriUDRz5g/Y+Eo3p3uW+phHcI08OUo59g3pRiNk2wQO
Tun0JLM61zWbiO6fksAy6Ue7HTqA2dviXELUWhRaTD7IaAd6td2QV8i6KrhbBSvvydvp3Dk5upYy
DsgT7+5mAZtmoBA0TBgCXSQGqnnRhCte4n3E5lqMDCy4A6kx+uBFCW9T2SEuj2Y=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G2*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G2*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Wed Oct 15 02:00:00 CEST 2014*

Valid to: *Thu Oct 15 01:59:59 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:E3:3E:62:05:5C:2C:62:48:BD:06:11:4E:61:77:D9:C8:ED:01:C1:2A:B0:0A:78
:18:87:4C:58:BF:B3:BC:AA:67:AF:F0:28:FE:BB:C2:7E:DF:0B:01:7D:F1:68:33:BC:CD:6F:7B:92:F4:6D:D5:F7:B0:15:92:A5:65:40:7C:9E:C6:C7:2D:6E:57:52:B8:F5:6F:93:18:06:DB:9D:14:
AB:C1:76:49:09:74:ED:B7:0A:F2:A8:65:23:B5:40:3D:19:B2:7A:57:14:C6:5A:EF:13:D4:5A:0C:20:97:79:67:ED:C7:16:E1:25:C8:A0:D4:1A:1D:7B:7F:36:37:A6:52:55:17:B6:10:F3:43:17:F
9:F9:67:B0:16:5E:D8:5A:8B:92:E3:10:70:C6:5D:04:27:E6:FE:60:B1:06:0A:8F:D0:87:ED:BE:56:50:28:6E:55:17:99:05:61:F9:C0:F0:F1:F6:F8:6B:12:DC:0C:97:DD:71:34:8B:D2:D0:4F:CF:
7F:A1:58:84:11:0D:41:AB:18:91:16:DD:98:F9:DD:1F:68:9C:6D:49:83:9D:B2:5B:15:99:F6:07:26:7A:EE:6C:99:EA:03:5E:83:CE:53:A3:08:D9:F2:AE:88:1B:28:CE:3A:EC:FE:0E:63:14:E6:A
5:88:78:AA:B7:46:A2:A7:A3:A1:E7:89:02:03:01:00:01
```


Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]

CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]

CRL Distribution Points

http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

id_etsi_qcs_QcSSCD

Basic Constraints	*IsCA: false*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*CN=DigitalSign TSA - G2, O=DigitalSign - Certificadora Digital, C=PT*
Subject Key Identifier	*42:8D:58:65:FB:83:63:9E:F8:55:77:B6:BB:94:B2:21:8F:73:17:7E*
Authority Key Identifier	*28:ED:49:3D:82:AD:59:97:11:41:6C:94:B3:B0:4A:B2:59:89:14:79*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*51:B6:56:75:D6:DA:57:69:BA:9F:2F:73:F5:8B:BA:4C:53:C9:4E:E7:7A:1A:62:5D:8E:04:E0:FB:CA:D5:B0:87*

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

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

Status Starting Time *2020-11-09T00:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*
URI	*[pt]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*

7.4.1 - History instance n.1 - Status: granted

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

Service Name

Name	*[en]*	*DigitalSign TSA - G2 (Qualified TSA)*
Name	*[pt]*	*Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign TSA - G2*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I *Qo1YZfuDY574VXe2u5SyIY9zF34=*

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

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

7.4.2 - History instance n.2 - Status: withdrawn

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

Service Name

Name *[en]* *DigitalSign TSA - G2 (Qualified TSA)*

Name *[pt]* *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G2*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *Qo1YZfuDY574VXe2u5SyIY9zF34=*

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

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

7.4.3 - History instance n.3 - Status: undersupervision

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

Service Name

Name *[en]* *DigitalSign TSA - G2 (Qualified TSA)*

Name *[pt]* *Digitalsign (Serviço de Validação Cronológica Qualificado - TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G2*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *Qo1YZfuDY574VXe2u5SyIY9zF34=*

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

Status Starting Time *2014-10-15T23:00:01Z*

7.5 - Service (withdrawn): DigitalSign 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.*

Service Name

Name *[en]* *DigitalSign Qualified CA - G2*

Name *[pt]* *Digitalsign Qualified CA - G2 (EC-Certificados Qualificados)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *80811149735177971733479972391529313340*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFBTCCA+2gAwIBAgIQPMupS7Zy9G+u4ehyNk10PDANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQG
EwJHQjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExJCVCBDbGFzcyAyIENBIC0gRzIwHhcNMTMx
MDI0MDAwMDAwWhcNMjExMDIzMjM1OTU5WjCBuzELMAkGA1UEBhMCUFQxLDAqBgNVBAo7I0RpZ2I0
YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYDVQQLExZTeW1hbnRlYyBUcnVzdCBO
ZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtlIlEluZGl2aWR1YWwgU3Vic2NyaWJl
ciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVkIENBIC0gRzIwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDCZCMEqk4VSbD2kcyjmgdOlcE1Qg74YTbl+oYKHKfftgRZAKU
u2Qrh61WUwyiF13csVaZ8JhcW8Bwz45B7ZO4qMBlUe6kArk8+YDHDbEQVVH8Bc WCbUTTdu7u+f+
qirH2ZjjpQpLOCUsY8xIQy6bAyIMrqG2WyE1mQPrVU1s3BrhtnH3dU3F7NQpNcduFaoXuse2pK8O
nAWzlOo1DlrU+6yowFnY0U+Ys6sY07LWm/dqRVMK3NRp1Rb8s2glOP1q5zmr8PUxY6C73VHF5NGx
fWc/I5lJZ1liuq603l8dal7t0w0legmSd3nJ7bXwj8YNj9noMy/jGn5dupyWF4jFAgMBAAGjggFJ
MIIBRTASBgNVHRMBAf8EBDADAQH/AgEAMHIGA1UdIAR rMGkw2wYLYIZAAYB4RQEHFwIwWDApBggr
BgEFBQcCARYdaHR0cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9jcHMwKwYlKwYBBQUHAgIwHxodaHR0
cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9ycGEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL29uc2l0
ZWNy bC50cnVzdHdpc2UuY29tL0JUQ2xhc3MyQ0EtRzIuY3JsMA4GA1UdDwEB/wQEAwIBBjAoBgNV
HREEITAfpB0wGzEZMBcGA1UEAxMQYnQyMDQ4YzJQdWxLTlxMTAdBgNVHQ4EFgOUKO1JPYktWZcR
QWytS7BKslmjFHkwHwYDVR0jBBgwFoAUJarsFfP3ezebbCMo72U4kPTEXs/QwDOYjKoZIhvcNAQEL
BQADggEBAI4wMH8qi4XNotpe/LoBSGfxNJCJEwmLkPna8CN0ONYBKOQvKyL2jmqyfpSDNCT9/6hU
2qZTiKBtuXyqtrDzNkLCiej/98m+7tmxmu8j3qAOjOx1jfTnVYnTFV4b0v/sPeNgdlxPBj7BAWN0
ifUT+IPGVhBvixOKzCsKRcUkm4IYzfjmg4z6VmGj4C3rk+83etRJ/gAAQxd9JpKWZT1LqSh0kgU4
vvKmV2YERkYB8teLNveNaItRrz86DkIdJ5jhR8KhTbp8E/MID178gwERGBCZOOstH/D7jxR5
SViEjr7vEYTRjiBW9/SxcqY6xZ187QE0nL5ltrzpoZpuEew=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN:	*BT Class 2 CA - G2*
Issuer OU:	*VeriSign Trust Network*
Issuer O:	*British Telecommunications plc*
Issuer C:	*GB*
Subject CN:	*DigitalSign Qualified CA - G2*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*
Valid from:	*Thu Oct 24 02:00:00 CEST 2013*
Valid to:	*Sun Oct 24 01:59:59 CEST 2021*
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:C2:64:23:04:AA:40:15:49:B0:F6:91:CC:A3:9A:07:4E:95:C1:35:42:0E:F8:61:3B:5B:23:EA:18:28:72:9F:7E:D8:11:64:02:94:BB:64:2B:87:AD:56:53:0C:A3:16:5D:DC:B1:56:99:44:98:5C:5B:C0:70:CF:8E:7C:ED:93:B8:A8:CF:08:51:EE:A4:02:B9:3C:F9:80:C7:0D:B1:10:55:51:FC:05:C5:82:6D:42:13:4D:D8:BB:BB:E7:FE:AA:2A:C7:D9:98:E3:A5:0A:4B:38:25:2C:63:CC:48:43:2E:9B:03:22:0C:AE:A1:B6:5B:21:35:99:03:EB:55:4D:6C:DC:1A:E1:B6:71:F7:75:4D:C5:EC:D4:29:35:C7:6E:15:AA:17:BA:C7:B6:A4:AF:0E:9C:05:B3:94:EA:35:0E:5A:D4:FB:AC:A8:C0:59:D8:D1:4F:98:B3:AB:18:D3:B2:D6:9B:F7:6A:45:53:0A:DC:D4:69:D5:16:FC:B3:68:25:38:FD:6A:E7:39:AB:F0:F5:31:63:A0:BB:DD:51:C5:E4:D1:B1:7D:67:3F:23:99:49:67:52:22:BA:AE:B4:DC:8F:1D:68:8E:ED:D3:0D:08:7A:09:92:77:79:C9:ED:B5:F0:8F:C6:0D:8F:D9:E8:33:2F:E3:1A:7E:5D:BA:9C:96:17:88:C5:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.trustwise.com/cps* *CPS text: [https://www.trustwise.com/rpa]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/BTClass2CA-G2.crl*
Subject Alternative Name	*CN=bt2048c2Pub1-211*
Subject Key Identifier	*28:ED:49:3D:82:AD:59:97:11:41:6C:94:B3:B0:4A:B2:59:89:14:79*
Authority Key Identifier	*6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*87:A7:41:83:C8:30:A8:74:FC:36:1D:74:53:1F:C8:63:BB:0A:F2:63:63:AD:4B:5A:77:27:E5:BF:94:B3:53:9F*

Service Status

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

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

Status Starting Time

2022-12-27T09:05:11Z

Scheme Service Definition URI

URI	*[en]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*
URI	*[pt]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*

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

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

Criteria list assert=all

Policy Identifier:

Identifier	*2.16.840.1.113733.1.7.23.2*

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]*	*DigitalSign Qualified CA - G2*
Name	*[pt]*	*Digitalsign Qualified CA - G2 (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign Qualified CA - G2*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I *KO1JPYKtWZcRQWyUs7BKslmJFHk=*

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 [QCQSCDStatusAsInCert, QCStatement, QCForESig]

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.23.2*

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]* *DigitalSign Qualified CA - G2*

Name *[pt]* *Digitalsign Qualified CA - G2 (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign Qualified CA - G2*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *KO1JPYKtWZcRQWyUs7BKslmJFHk=*

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

Status Starting Time *2014-10-15T23:00:01Z*

7.5.4.3 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.23.2*

7.5.4.4 - Extension (not critical): expiredCertsRevocationInfo

dateTime *2016-06-30T21:00:39Z*

7.6 - Service (withdrawn): DigitalSign TSA - G3 (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.*

Service Name

Name *[en]* *DigitalSign TSA - G3 (Qualified TSA)*

Name *[pt]* *DigitalSign TSA - G3 (Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *473929943987668569725598821282493072 88*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGjjCCBXKgAwIBAgIQI6ePB2aWLaSjQcoZLxPAmDANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWdulCDgQ2VydGlmaWNhZG9uYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzIwHhcNMTUxMDA4MDAwMDAwWhcNMjExMDA3MjM1OTU5WjB7MQswCQYDVQQGEwJQVDEs
MCoGA1UECChMjRGlnaXRhbFNpZ24gLSBDZXj0aWZpY2Fkb3jhIERpZ2l0YWxtaAdBgNVBAsTFIN5
bWFudGVlIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMTFERpZ2l0YWxtaWdulFRTQSAtIEczMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAngxVJB/rXs2a+OkQu/glRsh2trW3zgOGjS4MLASs
n+hzQEiAj4L8J1GPF5LpF8uYEc6G8+8jvfvzPaqEKnTMxh3OiYa8GuwVk35AwExW+SqlpkrfMjSH
ZSO3Dn7/1hYf+1XE7wFEXvt9ERifDpe6bWFgtoHw5cEFy6z7U7ekx6d2bhmLN+3I1sV997upcbE9
ZPILpXDoeZnFb0sG7jGv54i7df5a7VF4BgFeLdoyc4fA+z+KfKSnbO7VLbJ4x0GWhTda+5L8j3E5
tAwsXtkvQiRuO6UF8RQt/pPdIf996ZWlzXQAtx8CX3LUW8ODHCboyfWjEEFnrjWmdr1+9c3yCwID
AQABo4ICxzCCAsMwDAYDVR0TAQH/BAIwADCCASQGA1UdIASCARswggEXMIIBEwYLYIZIAYb4RQEH
FwIwggECMDgGCCsGAQUFBwIBFixodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lUQUxT
SUdOL2NwczA6BggrBgEFBQcCAjAuFixodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lU
QUxTSUdOL3JwYTCBiQYIKwYBBQUHAgIwfRp7SW4gdGhlIGV2ZW50IG9mIGEgY29uZmxpY3QgYmV0
d2VlbiB0aGUgdGVybXMgb2YgQlQgQ1BTIGFuZCB0aGUgdGVybXMgb2YgRGlnaXRhbFNpZ24gQ1BT
LCB0aGUgdGVybXMgb2YgQlQgQ1BTIHNoYWxsIGNvbnRyb2wuMHMGA1UdHwRsMGowaKBmoGSGYmh0
dHA6L9vbnNpdGVjcmwudHJlc3R3aXNlLmNvb59EaWdpdGFsU2lnbkNlcnRpZmjYWRvcmFEaWdp
dGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHMi9MYXRlc3RDUkwuY3JsMBYGA1UdJQEB/wQMMAoGCCsG
AQUFBwMIMA4GA1UdDwEB/wQEAwIGwDAiBggrBgEFBQcBAwQWMBQwCAYGBACORgEBMAgGBgQAjkYB
BDCBiQYDVR0RBIGBMH+kfTB7MQswCQYDVQQGEwJQVDEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBD
ZXj0aWZpY2Fkb3jhIERpZ2l0YWxtaAdBgNVBAsTFIN5bWFudGVlIFRydXN0IE5ldHdvcmsxHTAb
BgNVBAMTFERpZ2l0YWxtaWdulFRTQSAtIEcyMB0GA1UdDgQWBBRa1VLt4lxmkXVrjszMOVmJGq9l
NjAfBgNVHSMEGDAWgBQo7Uk9gq1ZlxFBbJ5zsEqyWYkUeTANBgkqhkiG9w0BAQsFAAOCAQEAP7o/
iiw4cvqJzPsjiCQRQ+57xZK/GPCnWQBxz7NoGeObUG+3Oj78ucQGNYwML34sAc4XJSEnsMieEzwg
FjzyiOyRSI8oxc/cMFknZFqmaReB5YEWTrch52qtsyt/l05BYVnBiwre0CMn/EOp+QTF+kSvzg9j
ph1mj9yC3fy+N+ZLEN8zoDxSt5qt2X6gEqOtiVsuKbEeZhbZ+PqzC8i8/ZlJQREJSTK04VNuwCQ6
gcKeWNvEfjKhBUyuR68hSh5jko2nM/xu4myqciYWgX7pb06Gg0i9/Ecj0flzkAOlFMMJxKJd/wcT
2PlgyrcRUXEZRu/Al3EfIYvos7bNw1X4Iw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G2*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G3*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Thu Oct 08 02:00:00 CEST 2015*

Valid to: *Fri Oct 08 01:59:59 CEST 2021*

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:02:82:01:01:00:9E:0C:55:24:1F:EB:5E:CD:9A:F8:E9:10:BB:F8:25:46:C8:76:B6:B5:B7:CE:03:
86:8D:2E:0C:2C:04:AC:9F:E8:73:40:48:80:27:82:FC:27:51:8F:17:92:E9:17:CB:98:11:CE:86:F3:EF:23:BD:FB:F3:3D:AA:84:2A:74:CC:C6:1D:CE:89:86:BC:1A:EC:15:93:7E:40:C0:4C:56:F9
:2A:A5:A6:4A:DF:32:34:87:65:23:B7:0E:7E:FF:D6:16:1F:FB:55:C4:EF:01:44:5E:FB:7D:11:18:9F:0E:97:BA:6D:61:60:B6:81:F0:E5:C1:05:CB:AC:FB:53:B7:A4:C7:A7:76:6E:19:8B:37:ED:C
8:D6:C5:7D:F7:BB:A9:71:81:3D:64:F9:4B:A5:70:E8:79:99:C5:6F:4B:06:EE:31:AF:E7:88:BB:75:FE:5A:ED:51:78:06:01:5E:2D:DA:32:73:87:C0:FB:3F:8A:7C:A4:A7:6C:EE:D5:2D:B2:78:C7
:41:96:B5:37:5A:FB:92:FC:27:71:39:B4:0C:2C:5E:D9:2F:42:24:6E:3B:A5:05:F1:14:2D:FE:93:DD:21:FF:7D:E9:95:A5:CD:74:00:B7:10:42:5F:72:D4:5B:C3:83:1C:26:E8:C9:F5:A3:10:41:6
7:AE:35:A6:76:BD:7E:F5:CD:F2:0B:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]

CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]

CRL Distribution Points *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl*

Extended Key Usage *id_kp_timeStamping*

QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Subject Alternative Name	*CN=DigitalSign TSA - G2, OU=Symantec Trust Network, O=DigitalSign - Certificadora Digital, C=PT*
Subject Key Identifier	*5A:D5:52:ED:E2:5C:66:91:75:6B:26:CC:CC:39:59:89:1A:AF:65:36*
Authority Key Identifier	*28:ED:49:3D:82:AD:59:97:11:41:6C:94:B3:B0:4A:B2:59:89:14:79*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B3:C0:F2:80:55:68:42:7D:39:F4:87:47:BF:97:23:20:D7:99:A9:C8:53:FE:49:BE:27:04:81:D2:64:F7:18:1F*

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

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

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

Scheme Service Definition URI

URI	*[en]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*
URI	*[pt]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*

7.6.1 - History instance n.1 - Status: withdrawn

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

Service Name

Name	*[en]*	*DigitalSign TSA - G3 (Qualified TSA)*
Name	*[pt]*	*DigitalSign TSA - G3 (Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign TSA - G3*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*WtVS7eJcZpF1aybMzDlZiRqvZTY=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Status Starting Time	*2016-06-30T22:00:00Z*

7.6.2 - History instance n.2 - Status: undersupervision

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

Service Name

Name	*[en]*	*DigitalSign TSA - G3 (Qualified TSA)*
Name	*[pt]*	*DigitalSign TSA - G3 (Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign TSA - G3*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*WtVS7eJcZpF1aybMzDlZiRqvZTY=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2015-10-07T23:00:01Z*

7.7 - Service (withdrawn): DigitalSign Qualified CA - G3

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]*	*DigitalSign Qualified CA - G3*

Name *[pt]* *DigitalSign Qualified CA - G3*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *383825803800262048687823507104734022 68*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFBTCCA+2gAwIBAgIQHOA3Uacj5dzwpxE0LBgnnDANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQG
EwJHQjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMR8wHQYDVQQLExZT
eW1hbnRlYyBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExJCVCBDbGFzcyAyIENBIC0gRzMwHhcNMTYw
OTI3MDAwMDAwWhcNMjQwOTI2MjM1OTU5WjCBuzELMAkGA1UEBhMCUFQxLDAqBgNVBAoTI0RpZ2Il0
YWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYDVQQLExZTeW1hbnRlYyBUcnVzdCBO
ZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtlIEluZGl2aWR1YWwgU3Vic2NyaWJl
ciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVkIENBIC0gRzMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDI0rXwVGqY12Dj9DW7K/EjbLIT15tU05iltp9KlKOzluS2NCiw
yIUAEpaBXF5r8+JPMLUFYpmmUa6QOFM5cfDWzQcRjt+nM0CmafA5vRbQc5ZjIDbExhCIUYvTI1Op
Wcwc/TfiodsPZPuGihdSk2OqJXYBk4vd4jRuDEUKjpAXZXCFRiFh5nZ/xZXDa82D06/CsIWyWABA
PJxMKBQdGOOhEyLDeoZTMTS7PVjgH8enAcBSLkf4lHVcujm6NlO3dBYOMe8T0pQTMHrhmhSkjBm
1wydtJltRtfHudkJZrrsAxTCyqrkwLa2Bc8plNypY65L4igEhGNdlnI2SNs9sF3fAgMBAAGjggFJ
MIIBRTA5BgNVHRMBAf8ECDAGAQH/AgEAMHIGA1UdIARrMGkwZwYLYIZlAYb4RQEHFwIwWDApBggr
BgEFBQcCARYdaHR0chM6Ly93d3cudHJ1c3R3aXNlLmNvbS9jcHMwKwYIKwYBBQUHAgIwHxodaHR0
cHM6Ly93d3cudHJ1c3R3aXNlLmNvbS9ycGEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL29uc2l0
ZWNybC50cnVzdHdpc2UuY29tL0JUQ2xhc3MyQ0EtRzMuY3JsMA4GA1UdDwEB/wQEAwIBBjAoBgNV
HREEITAfpB0wGzEZMBcGA1UEAxMQYnQyMDQ4YzQdWlxL7lyODAdBgNVHQ4EFgQU+16OQpwjqH30
G4xcfDsYg9nZ90AwHwYDVR0jBBgwFoAU6HtzrH/o3WQEh7tbZb6PkP1kGVcwDOYJKoZIhvcNAQEL
BQADggEBAHyODmKOt62w1sKq+5+uj7C3AWGnYVHHkc2M6trWw1wp3OKQiBhCBebbp3VduSFtcP0p
sj2bclXM+PvnmMTr51gjm6eHLWSiQRKfraLQmxp/7eqn+NsoTnTkSDOL/4CxfKnN2CtxQgZJc6QR
wDxPx7Gjv/OT/iwQIbf4KEaAuAASIJ7Pq+1oamth20SiQS5RfRXD/EXI2oQAOSGyfQv6qUdQuBi2
0XjtHgODnhUeB8k4180RlHp3nb5EKqmbyDLen+pMlAONryUiwKhvTM/Yjwx6w+xcEED+GwvTAjRc
291548elQwKAWwVb7EOjkHl+BuT47WEm4jacvA6qGQSz+IU=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *BT Class 2 CA - G3*

Issuer OU: *Symantec Trust Network*

Issuer O: *British Telecommunications plc*

Issuer C: *GB*

Subject CN: *DigitalSign Qualified CA - G3*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Tue Sep 27 02:00:00 CEST 2016*

Valid to: *Fri Sep 27 01:59:59 CEST 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:C8:D2:B5:F0:54:6A:98:D7:60:E3:F4:35:BB:2B:F1:23:6C:B9:53:D7:9B:54:D3
:98:88:B6:9F:4A:96:43:B3:22:E4:B6:34:2B:B0:CA:55:00:12:96:81:5C:5E:6B:F3:E2:4F:30:B5:05:62:99:A6:51:AE:90:38:53:39:71:F0:D6:CD:07:11:BE:DF:A7:33:40:A6:69:F0:39:BD:16:D
0:73:96:63:BB:36:C4:C6:10:A5:51:BB:D3:97:53:A9:59:CC:1C:FD:37:E2:A1:DB:0F:64:FB:86:8A:17:52:93:63:AA:25:76:01:93:BB:DD:E2:34:6E:0C:45:0A:22:90:17:65:70:B5:46:21:61:E6:
76:7F:C5:95:C3:6B:CD:B3:D3:AF:C2:B0:95:B2:58:00:40:3C:9C:4C:28:14:1D:18:E3:A1:13:22:C3:7A:B6:53:31:34:BB:3D:58:A3:80:7F:1E:9C:07:01:48:B9:1F:E2:51:D5:72:E8:E6:E8:D9:4
E:DD:D0:58:38:C7:BC:4F:4A:50:4C:C1:EB:B6:68:52:92:30:66:D7:0C:9D:B4:92:2D:46:D7:C7:B9:D9:09:66:BA:EC:03:14:C2:CA:AA:E4:C0:B6:B6:05:CF:29:94:DC:A9:63:AE:4B:E2:28:04:8
4:63:5D:22:79:76:48:DB:3D:B0:5D:DF: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.trustwise.com/cps* *CPS text: [https://www.trustwise.com/rpa]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/BTClass2CA-G3.crl*
Subject Alternative Name	*CN=bt2048c2Pub1-228*
Subject Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Authority Key Identifier	*E8:7C:F3:AC:7F:E8:DD:64:04:87:BB:5B:65:BE:8F:90:FD:64:19:5B*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*27:58:8A:16:FC:F2:F5:22:02:6A:22:06:3E:D3:83:45:40:32:56:01:4B:25:08:A5:97:42:C2:18:9C:D0:FC:B9*

Service Status

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

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

Status Starting Time

2023-01-20T11:18:27Z

Scheme Service Definition URI

URI	*[en]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*
URI	*[pt]*	*http://www.digitalsign.pt/ECDIGITALSIGN/cps/*

7.7.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert, QCStatement, QCQSCDManagedOnBehalf, QCForESig, QCForESeal]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

7.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.7.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.7.4 - History instance n.1 - Status: granted

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

Service Name

Name [en] *DigitalSign Qualified CA - G3*

Name [pt] *DigitalSign Qualified CA - G3*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign Qualified CA - G3*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *+16OQpwjqH30G4xcfDsYq9nZ90A=*

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

Status Starting Time *2016-09-27T00:00:00Z*

7.7.4.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert, QCStatement, QCQSCDManagedOnBehalf, QCForESig, QCForESeal]

Qualifier type description [en] *undefined.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.2*

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.3*

Description

7.7.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.7.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.7.5 - History instance n.2 - Status: granted

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

Service Name

Name [en] *DigitalSign Qualified CA - G3*

Name [pt] *DigitalSign Qualified CA - G3*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign Qualified CA - G3*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *+16OQpwjqH30G4xcfDsYq9nZ90A=*

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

Status Starting Time *2016-09-26T23:00:00Z*

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

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

Criteria list assert=all

Policy Identifier:

Identifier *2.16.840.1.113733.1.7.23.2*

Description

7.7.5.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.8 - Service (withdrawn): DigitalSign TSA - G4 (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.*

Service Name

Name *[en]* *DigitalSign TSA - G4 (Qualified TSA)*

Name *[pt]* *DigitalSign TSA - G4 (Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *617924404578879585558137220213694871 09*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIHGzCCBgOgAwIBAgIQLnzKiD8uQF93G75B/TAfBTANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWdulCQgQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbhRIYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMTYxMDA0MDAwMDAwWhcNMjIxMDAzMjM1OTU5WjCBlTELMAkGA1UEBhMCUFQx
LDAqBgNVBAoTI0RpZ2lOYWxTaWdulCQgQ2VydGlmaWNhZG9yYSBEaWdpdGFsMRgwFgYDVQRhEw9W
QVRQVC01MDcwMTU4NTExHzAdBgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMT
FERpZ2lOYWxTaWdulFRTQSAtIEc0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzMcu
eaEDoHFH8IffM1rfEpcOr+ASdUfllqRTlsWCB+2eAWXGQy9XSH3XblnCX99dmkcIPpdz+n4z++rR
8YVLLxO1CvyQ65Ipy3KJSYqlGq2yuVCgGhqBv9A25rGfeDg+c/BMo/+k0NLkmM60BP1L2aVIYbRL
STrY1Iukwr7Ih2k5iN38IVwNzrkQxeC3p4UI/955cCYf5/ZbTVUI+aFnUfx8oKIEEQWbhkkd92xd+
9EtINQ7R8Qj+gaCRGfozCliosdlWcam5HhhAsm93VfSv6QWHdEW02ELteM1uh80mi/4fenyKow3P
SdU7Q4Sz4lyZaefqNdk/XpyAO0XhQIBLfQIDAQABo4IDPTCCAzkwDAYDVR0TAQH/BAIwADCCASQG
A1UdIASCARswggEXMIIBEwYLYIZIAYb4RQEHFwIwggECMDgGCCsGAQUFBwIBFixodHRwczovL3d3
dy5kaWdpdGFsc2lnbi5wdC9PQ0RjR0lUQUxTSUdOL2NwczA6BggrBgEFBQcCAjAuDCxodHRwczov
L3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lUQUxTSUdOL3JwYTCBiQYIKwYBBQUHAgIwfQx7SW4g
dGhlIGV2ZW50IG9mIGEgY29uZmxpY3QgYmV0d2VlbiB0aGUgdGVybXMgb2YgQlQgQ1BTIGFuZCB0
aGUgdGVybXMgb2YgRGlnaXRhbFNpZ24gQ1BTLCB0aGUgdGVybXMgb2YgQlQgQ1BTIHNoYWxsIGNv
bnRybzwuMHMGA1UdHwRsMGowaKBmoG5GYmh0dHA6Ly9vbnMpdGVjcmwudHJ1c3R3aXNlLmNwb59E
aWdpdGFsU2lnbkNlcnRpZmljYWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHMy9MYXRl
c3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIGwDCBugYIKwYBBQUHAQMEga0wgaowFQYIKwYBBQUHCwIw
CQYHBAL7EkBAjAIBgYEAI5GAQEwCAYGBACORgEEMH0GBgQAjkYBBTBzMDYWMGh0dHBzOi8vd3d3
LmRpZ2lOYWxzaWduLnB0L0VDREIHSVRBTFNJRdvY3BzL2RkcBMCUFQwORYzaHR0cHM6Ly93d3cu
ZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9jcHMvZGRwX2VuEwJFTjBnBgNVHREEYDBepFww
WjELMAkGA1UEBhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdp
dGFsMR0wGwYDVQQDExREaWdpdGFsU2lnbiBUU0EgLSBHNDAdBgNVHQ4EFgQULCfLggIOjjep1ij2
zP4t1BXfGpUwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwHwYDVR0jBBgwFoAU+16OOQpwjqH30G4xc
fDsYq9nZ90AwDQYJKoZIhvcNAQELBQADggEBAMagrhKfzmv1PJH7WUmc/MRnGa3/7hlpQkkTtOWi
EhSIs0vp8lgqwAyKOsCzd3uzbslbSRIjlIC1lU+RGKGD0quN5fzI0fr/ppm74+hzdrY0bY0h2ieo
BXgdSOTO+XR2JuPxRSjgMWNjv36a6OiFGE0jXqm5kmhJd/yjCfRAgHYVqf/SP54d90ExW0YOXvIY
1ayy232Sksf4F5RYrFAQ8gFDvlaaIVupqR3ltuxUyip3qs3+JxP0BuetckJfxvNvPbALMDQWqYpB2
Iyr/IdXGDagOYEXGRK+7LF2iovoNYQuGo9bAksaLfVoRWkTjcBVuHJXLFvxL4ztNQXMzjdeULws=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G4*

Subject OU: *Symantec Trust Network*

Subject 2.5.4.97: *VATPT-507015851*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Tue Oct 04 02:00:00 CEST 2016*

Valid to: *Tue Oct 04 01:59:59 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:CC:C7:2E:79:A1:03:A0:71:47:F2:57:DF:33:5A:DF:12:97:0E:AF:E0:12:75:47:
E5:96:A4:53:22:C5:82:07:ED:9E:01:65:C6:43:2F:57:48:7D:D7:6E:59:C2:5F:DF:5D:9A:47:08:3E:97:73:FA:7E:33:FB:EA:D1:F1:85:4B:2F:14:35:0A:FC:90:EB:99:69:CB:72:89:49:8A:A5:1A
:AD:B2:B9:50:A0:1A:1A:81:BF:D0:36:E6:B1:9F:78:38:3E:73:F0:4C:A3:FF:A4:D0:D2:E4:98:CE:B4:04:FD:4B:D9:A5:48:61:B4:4B:49:3A:DB:D4:8B:A4:C2:BE:E3:87:69:39:88:DD:FC:57:03:
73:FE:44:31:78:2D:E9:E1:45:3F:F7:9E:5C:09:87:FF:B3:F6:5B:ED:55:3E:68:59:D4:7F:1F:28:28:81:04:41:6B:61:92:47:7D:DB:17:7E:F4:4B:62:35:0E:D1:F1:02:7E:81:A0:91:19:FA:33:08:
88:A8:B1:D9:56:71:A9:B9:1E:18:40:B2:6F:77:55:F4:AF:E9:05:87:74:45:B4:D8:42:ED:78:CD:6E:87:CD:26:8B:FE:1F:7A:7C:8A:A3:0D:CF:49:D5:3B:43:84:B3:E0:8C:99:69:E7:EA:35:D9:3
F:5E:9C:80:3B:45:E1:42:50:4B:7D:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]

CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]

CRL Distribution Points *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*

QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Subject Alternative Name	*CN=DigitalSign TSA - G4, O=DigitalSign - Certificadora Digital, C=PT*
Subject Key Identifier	*2C:27:CB:AA:09:4E:8E:37:A9:D6:28:F6:CC:FE:2D:D4:15:DF:1A:95*
Extended Key Usage	*id_kp_timeStamping*
Authority Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A8:38:B8:AE:B8:46:14:C2:BD:22:C5:E1:CD:B6:F8:10:01:0D:58:26:BB:C4:5F:6A:E3:63:8C:DF:9F:96:08:61*

X509SubjectName

Subject CN:	*DigitalSign TSA - G4*
Subject OU:	*Symantec Trust Network*
Subject 2.5.4.97:	*VATPT-507015851*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*LCfLqglOjjep1ij2zP4t1BXfGpU=*

Service Status

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

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

Status Starting Time

2016-10-06T23:00:00Z

Scheme Service Definition URI

URI	*[en]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*
URI	*[pt]*	*https://www.digitalsign.pt/ECDIGITALSIGN/cps*

7.9 - Service (withdrawn): DigitalSign TSA - G6 (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.*

Service Name

Name *[en]* *DigitalSign TSA - G6 (Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *168374388766573446129279371925334875759*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH3zCCBsegAwIBAgIQfgu6S9Cf2FSEjibbO8vFebzANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbnRlYyBUcnVzdCBQZXR3b3JrMTUwMwYDVQQLExxDbGFzcyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWljciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBIC0gRzMwHhcNMTgwMTA0MDAwMDAwWhcNMjQwMTAzMjM1OTU5WjCBITELMAkGA1UEBhMCUFQx
GDAWBgNVBGETD1ZBVFBULTUwNzAxNTg1MTEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZp
Y2Fkb3JlhIERpZ2l0YWwxHzAdBgNVBAsTFlN5bWFuZGVlIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMT
FERpZ2l0YWxTaWdulFRTQSAtIEc2MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAEtEnZ
Gn/llM7BcuW6ES8NDZAykrbc8xN3zE4rX3twGurJ62aDh5nT85aro/SUTvggdJMKa0uRCtxMQQB3
UkbMKMWwZtPukKZXHEiL98QdsOh/ZmdqUuK3J+iXKd/Xf+Dl4n2//4DHQ6X+5UmqQgF/CIG17lUG
vNoOroHNVf+o+W1tykEnfDMab58H8YnWiv8LEzcu0DGUFub3edHkNTqZYQpqYp9RT1R+5WVnkBEX
zfZX7/5HGcz/WZVaXx+Ay8N1bqLrzC2gEdLO+2lhO+62uha/4HoxYXOH3MnMM3WTYgnosp6Y9K5Z
7I3WySMCigN+Drm+UeRnw5bhqrzuG2oHeQIDAQABo4IEATCCA/0wdwYIKwYBBQUHAQEEazBpMGcG
CCsGAQUFBzAChltodHRwOi8vb25zaXRlY3JsLnRydXN0d2lzZS5jb20vRGlnaXRhbFNpZ25DZXJ0
aWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmllZENlcnRpZmlj YXRlRzMvY2EuY3J0MAwGA1UdEwEB/wQC
MAAwgqEKBgNVHSAEgqEbMIIBFzCCARMGCZCGSAGG+EUBBxcCMIIBAjA4BggrBgEFBQcCARYsaHR0
cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdjVEFMU0lHTi9jcHMwOgYIKwYBBQUHAgIwLgws
aHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdjVEFMU0lHTi9ycGEwgYkGCCsGAQUFBwIC
MH0Me0luIHRoZSBldmVudCBvZiBhIGNvbmZsaWN0IGJldHdlZW4gdGhlIHRlcm1zIG9mIEIUENQ
UyBhbmQgdGhlIHRlcm1zIG9mIERpZ2l0YWxTaWdulENQUywgdGhlIHRlcm1zIG9mIEJUENQUyBz
aGFsbCBjb250cm9sLjBzBgNVHR8EbDBqMGigZqBkhmJodHRwOi8vb25zaXRlY3JsLnRydXN0d2lz
ZS5jb20vRGlnaXRhbFNpZ25DZXJ0aWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmllZENlcnRpZmlj YXRl
RzMvTGF0ZXN0Q1JMLmNybDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAOBgNVHQ8BAf8EBAMCBsAw
gcUGCCsGAQUFBwEDBIG4MIG1MAkGBwQAgZdeAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjAIBgYE
AI5GAQEwCAYGBACORgEEMHGBgQAjkYBBTBzMDYWMGh0dHBzOi8vd3d3LmRpZ2l0YWxzaWduLnB0
L0VDRElhSVRBTFNjR04vY3BzL2RkcBMCUFQwORYzaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQv
RUNESUdjVEFMU0lHTi9jcHMvZGRwX2VuEwjFTjCBpgYDVR0RBIGeMIGbpIGYMIGVMRgwFgYDVQQF
Ew9WQVRQVC01MDcwMTU4NTExCzAJBgNVBAYTAlBUMSwwKgYDVQQKEyNEaWdpdGFsU2lnbiAtIENl
cnRpZmljYWRvcmEgRGlnaXRhbDEfMB0GA1UECxMWU3ltYW5DZWMgVHJ1c3QgTmV0d29yazEdMBsG
A1UEAxMURGlnaXRhbFNpZ24gVFNBIC0gRzYwHQYDVR0OBBYEFLq+3YyjBNkBpVFJadMJEjwbev2E
MB8GA1UdIwQYMBaAFPtejkKc16h998uMXHw7GKvZ2fdAMA0GCSqGSib3DQEBCwUAA4IBAQB/6kBn
c1Nif3hY+3tNl41Im5qTFE3XRQAR2CsV/022ZabyxqLTC846lRKmyFHhfMGnQ/8fLGdtWeoUVXUJ
cPlBq81KttArcWmoJCb01otrz+8lALy+q0ET+ddiNz5wcQYZLQPfjmOS1Gv3pfb4uQRvhizgR/wB
/Gigwx1eEJEI1naU5cm/s1Cwu0BN8uMXCdkUPN1Sq2sQUuBWp6XSlHFGAbE+KeQS+wgw/Cs3AOXp
WcpWEUPsur2ujXCB5HxSPeHzmo1FuWRk5G8ToGuEaFVUFF0XmpHFms1Qkp7Gth8aZk594qzleTQS
XjUhxNcVKePqvZvgUNWRo9B1b6Ng44S2
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G6*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

Valid from: *Thu Jan 04 01:00:00 CET 2018*

Valid to:	*Thu Jan 04 00:59:59 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:B4:49:D9:1A:7F:E5:94:CE:C1:72:E5:BA:11:2F:0D:0D:90:32:92:B6:DC:F3:13:77:CC:4E:2B:5F:7B:70:1A:EA:C9:EB:66:83:87:99:D3:F3:96:AB:A3:F4:94:4E:FA:A0:74:93:0A:6B:4B:91:0A:DC:4C:41:00:77:52:46:CC:28:C5:B0:66:D3:EE:90:A6:57:1C:42:0B:F7:C4:1D:B1:08:7F:66:67:6A:52:E2:B7:27:E8:97:29:DF:D7:7F:E0:E5:E2:7D:BF:FF:80:C7:43:A5:FE:E5:49:AA:42:01:7F:0A:51:B5:EC:95:06:BC:DA:0E:AE:81:CD:55:FF:A8:F9:6D:6D:CA:41:27:7C:33:1A:6F:9F:07:F1:89:D6:8A:FF:0B:B7:37:2E:D0:31:94:16:E6:F7:79:D1:E4:35:3A:99:61:0A:6A:62:9F:51:4F:54:7E:E5:65:67:90:11:17:CD:F6:57:EF:FE:47:19:CC:FF:59:95:5A:5F:1F:80:CB:C3:75:6E:A2:EB:CC:2D:A0:11:D2:CE:FB:69:61:3B:EE:B6:BA:16:BF:E0:7A:31:61:73:87:DC:C9:CC:33:75:93:62:09:E8:B2:9E:98:F4:AE:59:EC:8D:D6:C9:23:02:8A:A3:7E:0E:B9:BE:51:E4:67:C3:96:E1:AA:BC:EE:1B:6A:07:79:02:03:01:00:01*
Authority Info Access	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt*
Basic Constraints	*IsCA: false*
Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]* *CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*
Extended Key Usage	*id_kp_timeStamping*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Subject Alternative Name	*CN=DigitalSign TSA - G6, OU=Symantec Trust Network, O=DigitalSign - Certificadora Digital, C=PT, SERIALNUMBER=VATPT-507015851*
Subject Key Identifier	*BA:BE:DD:8C:A3:04:D9:01:A5:51:49:69:D3:09:12:3C:1B:7A:FD:84*
Authority Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1E:10:41:9F:D5:0D:BA:17:35:8D:5B:7F:0E:0D:8E:8A:04:A8:27:2B:89:C4:BF:52:62:E7:5E:A4:52:54:42:44*

X509SubjectName

Subject CN:	*DigitalSign TSA - G6*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject 2.5.4.97:	*VATPT-507015851*
Subject C:	*PT*

X509SKI

X509 SK I *ur7djKME2QGlUUlp0wkSPBt6/YQ=*

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

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

Status Starting Time *2025-02-28T00:00:00Z*

7.9.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *DigitalSign TSA - G6 (Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G6*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *ur7djKME2QGlUUlp0wkSPBt6/YQ=*

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

Status Starting Time *2018-01-05T01:00:00Z*

7.10 - Service (withdrawn): DigitalSign TSA - G7 (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.*

Service Name

Name *[en]* *DigitalSign TSA - G7 (Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *6931649214377758071826935958465765 5653*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIH3zCCBsegAwIBAgIQNCXe69QdEddD1jJnllXHZTANBgkqhkiG9w0BAQsFADCBuzELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2l0YWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMR8wHQYD
VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMTUwMwYDVQQLEyxDbGFzcyAyIE1hbmFnZWQgUEtj
IEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTEmMCQGA1UEAxMdRGlnaXRhbFNpZ24gUXVhbGlmaWVk
IENBICQgRzMwHhcNMTgxMjEyMDAwMDAwWhcNMjQwOTI2MjM1OTU5WjCBlTELMAkGA1UEBhMCUFQx
GDAWBgNVBGETD1ZBVFBULTUwNzAxNTg1MTEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZp
Y2Fkb3JlbIERpZ2l0YWwxHzAdBgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxHTAbBgNVBAMT
FERpZ2l0YWxTaWdulFRTQSAtIEc3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2SQM
gHgIHY9KFH5pPcqdHCbdgQEgcDpuOKDOZ+FySETH1AWMkdFjOhhDr9BngCDefao4X7ujbXEV5JMI
Fn7mD3rfgDqsZX51I595kvTIOfZZe5mAoVZaFycp0/mIE86OxVHYhpIUIDzkM7u3ogbWpnL3GE4x
z3oEgpVWAYKhPMjuwRI7X9wI++aVvOLSABclZ3eEWtpbsfZZabUQjtXdRj9samt7iI/ydiA3RxvW
R0hSa/ggdEOlg+uDtPTJCEFYSs3YNzfqCMQam2pR0FuM5zeo51U+lWzQvnyptk6Ns|26vZdu+T3Z
lzWG6XEKArxePi/jY63soW16c3B5wcvxrwIDAQABo4IEATCCA/0wdwYIKwYBBQUHAQEEazBpMGcG
CCsGAQUFBzAChitodHRwOi8vb25zaXRlY3j6LnRydXN0d2lzZS5jb20vRGlnaXRhbFNpZ25DZXJ0
aWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmllZENlcnRpZmljYXRlRzMvY2EuY3J0MAwGA1UdEwEB/wQC
MAAwggEkBgNVHSAEggEbMIIBFzCCARMGC2CGSAGG+EUBBxcCMIIBAjA4BggrBgEFBQcCARYsaHR0
cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTI9jcHMwOgYIKwYBBQUHAgIwLgws
aHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTI9ycGEwgYkGCCsGAQUFBwIC
MH0Me0luIHRoZSBldmVudCBvZiBhIGNvbmZsaWN0IGJldHdlZW4gdGhlIHRlcm1zIG9mIEJUIENQ
UyBhbmQgdGhlIHRlcm1zIG9mIERpZ2l0YWxTaWduIENQUywgdGhlIHRlcm1zIG9mIEJUIENQUyBz
aGFsbCBj6250cm9sIjBzBgNVHR8EbDBqMGigZqBkhmJodHRwOi8vb25zaXRlY3JsLnRydXN0d2lz
Z5sjb20vRGlnaXRhbFNpZ25DZXJ0aWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmllZENlcnRpZmljYXRl
RzMvTGFOZXN0Q1JMLmNybDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAOBgNVHQ8BAf8EBAMCBsAw
gcUGCCsGAQUFBwEDBIG4MIG1MAkGBwQAgZdeAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjAIBgYE
AI5GAQEwCAYGBACORgEEMHOGBgQAjkYBBTBzMDYWMGh0dHBzOi8vd3d3LmRpZ2l0YWxzaWduLnB0
L0VDREIhSVRBTFNJR04vY3BzL2RkcBMCUFQwORYzaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQv
RUNESUdlVEFMU0lHTI9jcHMvZGRwX2VuEwIFTjCBpgYDVR0RBIGeMIGbpIGYMIGVMRgwFgYDVQQF
Ew9WQVRQVC01MDcwMTU4NTExCzAJBgNVBAYTAlBUMSwwKgYDVQQKEyNEaWdpdGFsU2lnbiAtIENl
cnRpZmljYWRvcmEgRGlnaXRhbDEfMB0GA1UECxMWU3ltYW50ZWMgVHJ1c3QgTmV0d29yazEdMBsG
A1UExMURGlnaXRhbFNpZ24gVFNBICQgRzcwHQYDVR0OBBYEFOlv64OjAYwq/Ofg2/3B420+0gDA
MB8GA1UdIwQYMBaAFPtejkKcI6h99BuMXHw7GKvZ2fdAMAOGCSqGSIb3DQEBCwUAA4IBAQAG9Zy2
+2zki5HXG1GTHkhqP68g+BlhCQSlPu7gqRplFl2M3ihlTx+Qazp5j4bnWgtvRkxJGWFI9tcnS1FO
VzbbsVz775IxV2ui7nj007J7GHaqv7rRkNjwo+/aVrhir31+1fhQd3XO75nc8HlSGXtZcEmaj3RS
zm2tiniv13P15/j55ku+Nj6vL2LTzzQK2D7KKnqeEt3Xm/BJeNGT0iAPlt+o5nwwJ/mxv6qsz/7R
oBgpuBB5wPGU8jd9AhC1PzOA4kaVxCbCfLCA+Y5ul/FxHvbyPvFQDG/cZnSpCYiY2T9a5ZPMbIsP
JWOHL8OkYzjmBnBZaOVmuqpRH+6POl3B

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G3*

Issuer OU: *Class 2 Managed PKI Individual Subscriber CA*

Issuer OU: *Symantec Trust Network*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G7*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

Valid from: *Wed Dec 12 01:00:00 CET 2018*

Valid to: *Fri Sep 27 01:59:59 CEST 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:D9:24:0C:80:78:08:1D:8F:4A:14:7E:69:3D:CA:9D:1C:26:DD:81:01:20:70:3A
:6E:38:A0:CE:67:E1:32:48:44:C7:D4:05:8C:91:D1:63:3A:18:43:AF:D0:67:80:20:DE:7D:AA:38:5F:BB:89:6D:71:15:E4:93:08:16:7E:E6:0F:7A:DF:80:3A:AC:65:7E:75:95:2F:79:92:F4:E5:0
D:F6:59:7B:99:80:A1:5D:9A:17:27:29:D3:F9:A5:13:CE:8E:C5:51:D8:86:92:14:94:3C:CA:33:BB:B7:A2:A6:D6:A6:72:F7:18:4E:31:CF:7A:04:82:95:56:01:82:A1:3C:C8:EE:C1:19:7B:5F:DC
:08:FB:E6:95:BC:E2:D2:00:17:08:67:77:84:5A:DA:5B:B1:F6:59:69:B5:10:26:D5:DD:46:3F:6C:6A:6B:7B:8A:5F:F2:76:20:37:47:1B:D6:47:48:52:6B:F8:20:74:4D:08:83:EB:83:B4:F4:C9:0
8:41:58:4A:CD:DB:37:37:EA:08:C4:1A:9B:6A:51:D0:5B:8C:E7:37:A8:E7:55:3E:95:6C:D0:BE:7C:A9:B6:4E:8D:B0:9D:BA:BD:97:6E:F9:3D:D9:23:35:86:E9:71:0A:02:BC:5E:3E:2F:E3:63:A
D:EC:A1:6D:7A:73:70:79:C1:CB:F1:AF:02:03:01:00:01
```


Authority Info Access *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/ca.crt*

Basic Constraints *IsCA: false*

Certificate Policies	*Policy OID: 2.16.840.1.113733.1.7.23.2* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]* *CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl*
Extended Key Usage	*id_kp_timeStamping*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Subject Alternative Name	*CN=DigitalSign TSA - G7, OU=Symantec Trust Network, O=DigitalSign - Certificadora Digital, C=PT, SERIALNUMBER=VATPT-507015851*
Subject Key Identifier	*E2:2F:EB:83:A3:01:8C:2A:FC:E7:E0:DB:FD:C1:E3:6D:3E:D2:00:C0*
Authority Key Identifier	*FB:5E:8E:42:9C:23:A8:7D:F4:1B:8C:5C:7C:3B:18:AB:D9:D9:F7:40*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D7:DB:EB:5A:50:56:A4:9C:A0:13:BB:BE:DB:04:E5:F0:1C:36:5A:4B:CD:88:4B:D4:34:E2:64:52:97:83:B9:2A*

X509SubjectName

Subject CN:	*DigitalSign TSA - G7*
Subject OU:	*Symantec Trust Network*
Subject O:	*DigitalSign - Certificadora Digital*
Subject 2.5.4.97:	*VATPT-507015851*
Subject C:	*PT*

X509SKI

X509 SK I	*4i/rg6MBjCr85+Db/cHjbT7SAMA=*

Service Status

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

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

Status Starting Time

2025-02-28T00:00:00Z

7.10.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *DigitalSign TSA - G7 (Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G7*

Subject OU: *Symantec Trust Network*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *4i/rg6MBjCr85+Db/cHjbT7SAMA=*

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

Status Starting Time *2018-12-19T01:00:00Z*

7.11 - Service (deprecatedatnationallevel): DigitalSign CA - G4 (non-qualified CA)

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

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

Service Name

Name *[en]* *DigitalSign CA - G4 (non-qualified CA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *121499145618793256630945179199413653034*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFDzCCA/egAwIBAgIQW2fiX/FW6is2mRtR9zuOKjANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQG
EwJHQjEnMCUGA1UEChMeQnJpdGlzaCBUZWxlY29tbXVuaWNhdGlvbnMgcGxjMRBwHQYDVQQLExZT
eW1hbnRlYyBUcnVzdCBOZXR3b3JrMRswGQYDVQQDExlCVCBDbGFzcyAyIENlbIC0gRzMwHhcNMTgx
MDA5MDAwMDAwWhcNMjQxMDA4MjM1OTU5WjCBpjELMAkGA1UEBhMCUFQxLDAqBgNVBAoTI0RpZ2I0
YWxTaWduIC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMRQwEgYDVQQLEwtQVDUwNzAxNTg1MTE1MDMG
A1UECxMsQ2xhc3MgMiBNYW5hZ2VkIFBLSSBJbmRpdmlkdWFsIFN1YnNjcmliZXIgQ0ExHDAaBgNV
BAMTE0RpZ2I0YWxTaWduIENlCC0gRzQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9
yf78EkRp8nOD2rCRVuFFZZIO6Z4jI2W3VT7ETUb2mAPZA6o8d0iPDQkUeyTVSlNkIoXx490nGtlv
wr9FMVA39y4N4w1Q4Fy2Z/XiV/CZIjC1qLsFczHMnSSBxNiqf/n6GGrZuuwp5yp6S/oS89+WKypG
Js/DuZz7vewz+msL2oG8PV/NXluWgGLObl/iX1xnzhKKWMFcTmbFALRrP+AgovnK1iDiCnf9Q4H4
Gv8iRn0E9gQQWa3ulb0F1dAC60tI0x3T1B+uaGn6hwkin05ehirS0GmY5MEB/599pdPwrNQa6IxM
+ivq3Iwh5WdNM8nFvseeeDRK/13urw5AbEV9AgMBAAGjggFoMIIBZDASBgNVHRMBAf8ECDAGAQH/
AgEAMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly9vbnNpdGVjcmwudHJ1c3R3aXNlLmNvbS9CVENs
YXNzMkNBLUczLmNybDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQD
AgEGMCgGA1UdEQQhMB+kHTAbMRkwFwYDVQQDExBCVFB1YlJlTMjA0OHZGNjAxMB0GA1UdDgQWBBRt
WnzWmXxxWDvORVm/DciXYSTtaTByBgNVHSAEazBpMGcGC2CGSAGG+EUBBxcCMFgwKQYIKwYBBQUH
AgEWHWh0dHBzOi8vd3d3LnRydXN0d2lzZS5jb20vcnBhMB8GA1UdIwQYMBaAFOh886x/6N1kBle7W2W+j5D9ZBlbMA0G
d3d3LnRydXN0d2lzZS5jb20vcnBhMB8GA1UdIwQYMBaAFOh886x/6N1kBle7W2W+j5D9ZBlbMA0G
CSqGSIb3DQEBCwUAA4IBAQCDRMryW4jfXQVdjziazjnCuTxdMhkDJgos1J0GKrgkLROFWEvrRri
v7Od9YPbHk8o+ZQB4I9E6SYeAnyjqOnoAY4izSl6QIVccHoBMAwMM4A8dmT+s3N2Kc7bZWjZ8Xr
FTKTl81IlLXUjPA/D6UCSAligVuEnbTUVupvY1B7Ya+XzhBIUfZdtCG4Syga3igBU8QyWUv2DccU
oD+eONOlSoBk+pGjhR4+dgu3SWlLgIOTOuPgn+mYzNGxn5pGWR+TsYQ2BkMIT1xKgDRaDQfNk9Pj
VVg0OHanVAIGj/UvGMCi+yqgh2tjVSei4Fb9+ZyffVTIMAfdzf0s/QPbZEXt

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *BT Class 2 CA - G3*

Issuer OU: *Symantec Trust Network*

Issuer O: *British Telecommunications plc*

Issuer C: *GB*

Subject CN: *DigitalSign CA - G4*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *PT507015851*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

Valid from: *Tue Oct 09 02:00:00 CEST 2018*

Valid to: *Wed Oct 09 01:59:59 CEST 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:BD:C9:FE:FC:12:44:69:F2:73:83:DA:B0:91:56:E1:45:65:92:0E:E9:9E:23:23:
65:B7:55:3E:C4:AD:46:F6:98:03:D9:03:AA:3C:77:48:8F:0D:09:14:7B:24:D5:4A:53:64:96:85:F1:E3:DD:27:1A:D2:2F:C2:BF:45:31:50:37:F7:2E:0D:E3:0D:50:E0:5C:B6:67:F5:E2:57:F0:B3
:96:30:B5:A8:BB:05:73:31:CC:9D:24:81:C4:D8:AA:7F:F9:FA:18:6A:D9:8A:EC:29:E7:2A:7A:4B:FA:12:F3:DF:96:2B:2A:46:26:CF:C3:B9:9C:FB:BD:EC:33:FA:6B:0B:DA:81:BC:3D:5F:CD:5E:
5B:96:A8:62:CE:6F:49:62:5F:5C:67:CE:12:8A:58:C1:5C:4E:66:C5:00:B4:6B:3F:E0:2A:A2:F9:CA:D6:20:E2:0A:77:FD:43:81:F8:1A:FF:22:46:7D:04:F6:04:10:59:AD:EE:21:BD:05:D5:D0:02
:EB:4B:65:D3:1D:D3:D4:1F:AE:68:69:FA:87:09:22:9F:4E:5E:86:2A:D2:D0:69:98:E4:C1:01:FF:9F:7D:A5:D3:F0:AC:D4:1A:E8:9C:4C:FA:2B:EA:DC:8C:21:E5:67:4D:33:C9:C5:BE:C7:9E:78:
34:4A:FF:5D:EE:AF:0E:40:6C:45:7D:02:03:01:00:01
```


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

CRL Distribution Points *http://onsitecrl.trustwise.com/BTClass2CA-G3.crl*

Extended Key Usage *id_kp_clientAuth*

Subject Alternative Name *CN=BTPubRS2048vF601*

Subject Key Identifier *6D:5A:7C:D6:99:7C:71:58:3B:CE:45:59:BF:0D:C8:97:61:24:ED:69*

Certificate Policies

Policy OID: 2.16.840.1.113733.1.7.23.2

CPS pointer: https://www.trustwise.com/cps

CPS text: [https://www.trustwise.com/rpa]

Authority Key Identifier	*E8:7C:F3:AC:7F:E8:DD:64:04:87:BB:5B:65:BE:8F:90:FD:64:19:5B*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1B:5C:35:CC:AD:3D:08:1E:9A:90:2E:E2:78:49:0A:64:36:D2:3F:6F:CD:11:49:E0:87:B5:11:AB:96:90:16:AA*

X509SubjectName

Subject CN:	*DigitalSign CA - G4*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*PT507015851*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*bVp81pl8cVg7zkVZvw3Il2Ek7Wk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel*
Service status description *[en]*	*undefined.*
Status Starting Time	*2023-01-20T11:23:15Z*

7.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.3 - History instance n.1 - Status: recognisedatnationallevel

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

Service Name

Name [en] *DigitalSign CA - G4 (non-qualified CA)*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign CA - G4*

Subject OU: *Class 2 Managed PKI Individual Subscriber CA*

Subject OU: *PT507015851*

Subject O: *DigitalSign - Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *bVp81pl8cVg7zkVZvw3Il2Ek7Wk=*

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

Status Starting Time *2020-01-28T11:21:14Z*

7.11.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.4 - History instance n.2 - Status: recognisedatnationallevel

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

Service Name

Name [en] *DigitalSign CA - G4 (non-qualified CA)*

Service digital identities

X509SubjectName

Subject CN:	*DigitalSign CA - G4*
Subject OU:	*Class 2 Managed PKI Individual Subscriber CA*
Subject OU:	*PT507015851*
Subject O:	*DigitalSign - Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*bVp81pl8cVg7zkVZvw3Il2Ek7Wk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*
Status Starting Time	*2019-06-23T23:00:00Z*

7.11.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.4.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.11.4.5 - Extension (critical): Qualifiers [QCForESig, QCForESeal]

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

Criteria list assert=atLeastOne

Policy Identifier:

Identifier	*[OIDAsURI]*	*1.3.6.1.4.1.25596.1.2.1*

Policy Identifier:

Identifier	*[OIDAsURI]*	*1.3.6.1.4.1.25596.1.2.2*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.3*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.4*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.101*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.102*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.103*

Policy Identifier:

Identifier *[OIDAsURI]* *1.3.6.1.4.1.25596.1.2.104*

Description

7.12 - Service (withdrawn): DigitalSign TSA - G8

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.*

Service Name

Name *[en]* *DigitalSign TSA - G8*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *119284983958929513777771899111888586496*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIILTCCBpWgAwIBAgIQWb1zxs1FZTjEQSM2bLMHADANBgkqhkiG9w0BAQsFADCBpDELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2lOYWxTaWdulC0gQ2VydGlmaWNhZG9yYSBEaWdpdGFsMT8wPQYD
VQQLEzZDbGFzcyAyIERpZ2lDZXJlIFBLSSBQbGF0Zm9ybSBjbmRpdmlkdWFsIFN1YnNjcmlzZXIg
QDExjjAkBgNVBAMTHURpZ2lOYWxTaWduIFF1YWxpZmllZCBDQSAtIEc0MB4XDTE5MDgyMDAwMDAw
MFoXDTI1MDgxOTIzNTk1OVowdDELMAkGA1UEBhMCUFQxGDAWBgNVBGETD1ZBVFBULTUwNzAxNTg1
MTEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZpY2Fkb3JhIERpZ2lOYWwxHTAbBgNVBAMT
FERpZ2lOYWxTaWduIFRTQSAtIEc4MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9g7U
BI7Qq7176yhL9PTz+zeOAtUGfgytUQpXhm4MK16au9Xvdf2kdgrpJywudDZHFo2Jfa0bXHHdTkJE
7tj4hX+oeDGBNZ7smSm1RRTjTzE45xlKh1Gtl7wddhGnkuQTMnGPfOe+QHsZgUmLkXYe3/Njpl/2h
NwRR8m0nzz3rWFSzxOQw0Pt3sbA7WwFUsGFUAb2KVQ8+o2w/GMGjRp1alx2cnZfGtWElgnTTmCXd
QcX+fnLdzcKQbJHKPfSe6dkhyl02BG26U+LhnKJ7oG5CXsf4xH06XpOfdBOTnxTc4NkwGBsYfCo1
uPeaPuuMLNhA0wbcbq6WXwENqpwdgRjAYQIDAQABo4IECDCCBAQwgYEGA1UdEQR6MHikdjB0MRgw
FgYDVQQFEw9WQVRQVC01MDcwMTU4NTExCzAJBgNVBAYTAlBUMSwwKgYDVQQKEyNEaWdpdGFsU2ln
biAtIENlcnRpZmlj YWRvcmEgRGlnaXRhbDEdMBsGA1UEAxMURGlnaXRhbFNpZ24gVFNBIC0gRzgw
DAYDVR0TAQH/BAIwADCCASIGA1UdIASCARkwggEVMIIBEQYJKwYBBAG+WAADMIIBAjA4BggrBgEF
BQcCARYsaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9jcHMwOgYIKwYB
BQUHAgIwLgwsaHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9ycGEwgYkG
CCsGAQUFBwICMH0Me0luIHRoZSBldmVudCBvZiBhIGNvbmZsaWN0IGJldHdlZW4gdGhlIHRlcm1z
IGUtMTEuIENQUy8hbmQgdHlldHRlcm1zIGlnIERpZ2lOYWxTaWduIENQUywgdGhlIHRlcm1zIG9m
IEJUIENQUyBzaGFsbCBjb250cm9sLjBzBgNVHR8EbDBgMGigZqBkhmJodHRwOi8vb25zaXRlY3Js
LnRydXN0d2lzZS5jb20vRGlnaXRhbFNpZ25DZXJ0aWZpY2Fkb3JhRGlnaXRhbFF1YWxpZmllZENl
cnRpZmlj YXRlRzQvTGF0ZXN0Q1JMLmNybDCBxQYIKwYBBQUHAQMEgbgwgbUwCQYHBACBl14BATAV
BgqrBgEFBQcLAjAJBgcEAIvsSQECMAgCBgQAjkYBATAIBgYEAI5GAQQwFQYGBACORgEFMHMwNhYw
aHR0cHM6Ly93d3cuZGlnaXRhbHNpZ24ucHQvRUNESUdlVEFMU0lHTi9jcHMvZGRwEwJQVDA5FjNo
dHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RJR0lUQUxTSUdOL2Nwcy9kZHBfZW4TAkVOMIGk
BggrBgEFBQcBAQSBlzCBlDApBggrBgEFBQcwAYYdaHR0cDovL3N0ZC1vY3NwLnRydXN0d2lzZS5j
b20wZwYIKwYBBQUHMAKGW2R0dHA6Ly9vbnNpdGVjcmwudHJ1c3R3aXNlLmNvb59EaWdpdGFsU2ln
bkNlcnRpZmlj YWRvcmFEaWdpdGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHNC9jYS5jcnQwFgYDVR0l
AQH/BAwwCgYIKwYBBQUHAwgwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBTnggg9MJFogHxTT5zW
CPNkgCANwDAfBgNVHSMEGDAWgBTW3w96HB1fLFlv2LG+2OI5Hw T5fjANBgkqhkiG9w0BAQsFAAOC
AYEAbBcn80XCspyHYi0yg72xxcWlcXRhIAZs/2gxJ8UuZTBtNumAYKC9CiPsSMhrVMKqlkmebZ5
IjbQTF07g8xwfaisNlKe6FQ95Xt+5TUVa1yQZdcjYDqRN6Romsr5hy8FsX5opvXtQCsNr2Jlsl
/D8CngosMpNqW8pAL8VAJY6nn9T2H7A/SwEhptBn/SxdPyCD3+I6A8F2GUY91xfm4H9E5Pl5i3HA
QYugHjiqOQxOFj1Z7Q/Wmq0W9L+cWafA9rdUptm4C8rH1N1IL6y+jhaDrKbvMZLXbiIn7a20H/sf
EdSXtwlX1IKaG/1wgX0E9Pb65AmtNg7aPuN1ZsfkFVz23g+B7HknSv9YDAOdT7pFRjD1x5yEZ1Fv
IlwwMmkLPXGk4f4b9orXz9Ulwa3mHfy2CWHFFRQjGjWQBB1ZUG2uKu2cFG/kgNGeGqplX4ZhDo22z9
Ov31/77Bt0X87AWTAdE84Zj9UkgrX4Z6P67kdEhCdN2IlV6xfcCI650i6jmk

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *DigitalSign Qualified CA - G4*

Issuer OU: *Class 2 DigiCert PKI Platform Individual Subscriber CA*

Issuer O: *DigitalSign - Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign TSA - G8*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

Valid from: *Tue Aug 20 02:00:00 CEST 2019*

Valid to: *Wed Aug 20 01:59:59 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:F6:0E:D4:04:8E:D0:AB:BD:7B:EB:28:4B:F4:F4:F3:FB:37:8E:02:D5:06:7E:0C:
AD:51:0A:57:86:6E:0C:2B:5E:9A:BB:D5:EF:75:FD:A4:76:0A:E9:27:2C:2E:74:36:47:16:8D:89:7D:AD:1B:5C:71:DD:4E:42:44:EE:D8:F8:85:7F:A8:78:31:81:35:9E:EC:99:29:B5:45:14:E3:B
5:9E:39:C6:52:A1:D4:6B:4B:EF:07:5D:84:69:E4:B9:04:CC:9C:63:DF:41:EF:90:1E:C6:60:52:62:E4:5D:87:B7:FC:D8:E9:97:FD:A1:37:04:51:F2:6D:27:CF:3D:EB:58:54:B3:C4:E4:30:D0:FB:
77:B1:B0:38:5B:01:54:B0:61:54:01:8D:8A:55:0F:3E:A3:6C:3F:18:C1:89:46:9D:5A:97:16:5C:9D:97:C6:B5:61:25:82:74:D3:98:25:DD:41:C5:FE:7E:12:DD:CD:C9:10:6C:98:47:28:F7:D2:
7B:A7:64:87:2D:36:04:6D:BA:53:E2:E1:9E:42:7B:A0:6E:42:5E:C7:F8:C4:7D:3A:5E:93:9F:74:13:93:9F:14:DC:E0:D9:30:18:1B:18:7C:2A:35:B8:F7:9A:3E:EB:8C:2C:D8:40:D3:06:DC:6E:A
E:96:5F:01:0D:AA:9C:1D:81:18:C0:61:02:03:01:00:01
```


Subject Alternative Name *CN=DigitalSign TSA - G8, O=DigitalSign - Certificadora Digital, C=PT, SERIALNUMBER=VATPT-507015851*

Basic Constraints *IsCA: false*

Certificate Policies

Policy OID: 1.3.6.1.4.1.8024.0.3

CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps

CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]

CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]

CRL Distribution Points *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/LatestCRL.crl*

QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Authority Info Access	*http://std-ocsp.trustwise.com* *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/ca.crt*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*E7:82:08:3D:30:91:68:80:7C:53:4F:9C:D6:08:F3:64:80:20:0D:C0*
Authority Key Identifier	*D6:DF:0F:7A:1C:1D:5F:2C:52:2F:D8:B1:BE:D8:E9:79:1F:04:F9:7E*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D5:79:5A:61:7E:39:53:D7:A4:C1:6E:5E:D6:84:23:97:26:80:89:88:A3:F7:7E:E7:B7:AD:72:64:DD:69:AE:53*

X509SubjectName

Subject CN:	*DigitalSign TSA - G8*
Subject O:	*DigitalSign - Certificadora Digital*
Subject 2.5.4.97:	*VATPT-507015851*
Subject C:	*PT*

X509SKI

X509 SK I	*54IIPTCRaIB8U0+c1gjzZIAgDcA=*

Service Status

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

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

Status Starting Time

2025-10-27T13:00:00Z

7.12.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *DigitalSign TSA - G8*

Service digital identities

X509SubjectName

Subject CN: *DigitalSign TSA - G8*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *54IIPTCRaIB8U0+c1gjzZIAgDcA=*

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

Status Starting Time *2019-09-23T23:00:00Z*

7.13 - Service (granted): DigitalSign TSA - G9

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.*

Service Name

Name *[en]* *DigitalSign TSA - G9*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *138713287312026906525292751598002004571*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIILTCCBpWgAwIBAgIQaFs1FlKGicsIJd4wAgpiWzANBgkqhkiG9w0BAQsFADCBpDELMAkGA1UE
BhMCUFQxLDAqBgNVBAoTI0RpZ2l0YWxTaWduICg0Q2VydGlmaWNhZG9yYSBEaWdpdGFsMT8wPQYD
VQQLEzZDbGFzcyAyIERpZ2lDZX0lFBLSSBQbGF0Zm9rbSBjbmRpdmlkdWFsIFN1YnNjcmlIZXIg
QOExIjAkBgNVBAMTHURpZ2l0YWxTaWduIFF1YWxpZmlIZCBDQSAtIEc0MB4XDTIwMDczMDAwMDAw
MFoXDTI2MDcyOTIzNTk1OVowdDELMAkGA1UEBhMCUFQxGDAWBgNVBGETD1ZBVFBULTUwNzAxNTg1
MTEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZpY2Fkb3JhIERpZ2l0YWwxHTAbBgNVBAMT
FERpZ2l0YWxTaWduIFRTQSAtIEc5MIIBjANBgkqhkiG9w0BAOEFAAOCAQ8AMIIBCgKCAQEA3Pcc
fhL/47usAAo7du8ZbHRmUJNWV3w8CZmtnjHSTi4DMVy5db40nzoccFQt4CT3/a+x2tUsnTAwUm
BAEK28jNalTccjt1BJ/cGWIDhBU0KhtCKDzucZILIs2Q5I2eIUtUDw3Pbq5kv18JIh9LbMUUyCEN
rCQICXYKt2R/62SetOmLdeLUI1VnX1CsIqB5aAcsIkbpoU12CMtac4s627FjPTch+y6ggXHfcLVh
qHNPMn0ks32h6M9rrHb/T8eERKVeb+nKKZmGicSTd9yoqQBeZS0k6DyI/VKwERFDW4jKT7kUGc57
dYpbcdP7ByqUlkqulpTfQuZ5dD2zTh34kOIDAQABo4IECDCCBAQwFgYDVR0lAQH/BAwwCgYIKwYB
BQUHAwgwDgYDVR0PAQH/BAQDAgbAMIGBBgNVHREEejB4pHYwdDEYMBYGA1UEBRMPVkFUUFQtNTA3
MDE1ODUxMQswCQYDVQQGEwJQVDEsMCoGA1UEChMjRGlnaXRhbFNpZ24gLSBDZXJ0aWZpY2Fkb3Jh
IERpZ2l0YWwxHTAbBgNVBAMTFERpZ2l0YWxTaWduIFRTQSAtIEc5MB0GA1UdDgQWBBTxI9A9IkTZ
mv5Oce+RobFSbybDaTAMBgNVHRMBAf8EAjAAMIIBgYDVR0gBIIBGTCCARUwggERBgkrBgEEAb5Y
AAMwggECMDgGCCsGAQUFBwIBFixodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lUQUxT
SUdOL2NwczABBggrBgEFBQcCAjAuDCxodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lU
QUxTSUdOL3JwYTCBiQYIKwYBBQUHAgIwfQx7SW4gdGhlIGV2ZW50IG9mIGEgY29uZmxpY3QgYmV0
d2VlbI0aGUgdGVybXMgb2YgQlQgQ1BTIGFuZCB0aGUgdGVybXMgb2YgRGlnaXRhbFNpZ24gQ1BT
LCB0aGUgdGVybXMgb2YgQlQgQ1BTIHNoYWxsIGNvbnRyb2wuMHMGA1UdHwRsMGowaKBmoGSGYmh0
dHA6Ly9vbnNpdGVjcmwudHJ1c3R3aXNlLmNvbS9EaWdpdGFsU2lnbkNlcnRpZmljYWRvcmFEaWdp
dGFsUXVhbGlmaWVkQ2VydGlmaWNhdGVHNC9MYXRlc3RDUkwuY3JsMIHFBggrBgEFBQcBAwSBuDCB
tTAJBgcEAIGXXgEBMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwCAYGBACORGEBMAgGBgQAjkYBBDB9
BgYEAI5GAQUwczA2FjBodHRwczovL3d3dy5kaWdpdGFsc2lnbi5wdC9FQ0RjR0lUQUxTSUdOL2Nw
cy9kZHATAIBUMDkWM2h0dHBzOi8vd3d3LmRpZ2l0YWxzaWduLnB0L0VDRElHSVRBTFNJR04vY3Bz
L2RkcF9lbhMCRU4wgaQGCCsGAQUFBwEBBIGXMIGUMCkGCCsGAQUFBzABhh1odHRwOi8vc3RkLW9j
c3AudHJ1c3R3aXNlLmNvbTBnBggrBgEFBQcwAoZbaHR0cDovL29uc2l0ZWNybC5ocnVzdHdpc2Uu
Y29tL0RpZ2l0YWxTaWduQ2VydGlmaWNhZG9yYURpZ2l0YWxRdWFsaWZpZWRDZXl0aWZpY2F0ZUc0
L2NhLmNydDAfBgNVHSMEGDAWgBTW3w96HB1fLFlv2LG+2OI5HwT5fjANBgkqhkiG9w0BAQsFAAOC
AYEA3AoUOTDq+iyv552euoCBj9UnNdP8oLmpQCbhisds/TsDk8W08zMDe2eQOaDiSqN1rf0PmZy
X8I9FS9QW2Hc6M9aIqN+NioEnZAAd+jA9IujwnFkST2Fj9jKdX35642ewEinxS7WLUNOFMVcjpIK
9WLY8bqOvNfrm80KJcB90krJg15OAcKB6aHOwfni5edupU6UBcVyC3Z4zHiZBJENf6bDSALAqdDl
yv5H+JHpWx0bPOrYFLbKYmVmnGPRw813gPZydMTZXLYb096C68CxpaYIA1Ix73XmQDdFO68NBcsN
pkj38ddhJdFp+fmnloSFsi8NGP7DCFXNCMY65+rm8zFajeVZJ+NlHfjI6x+BV0B1pRt/dUgmrd2L
iyPw5jP5P94rBSABZmrhYVJu3/kvnxdobo9V9NDQayNA39nL5ytYk9/3DlqUuw2wNGkKTjNkaVg4
uR3LuCY5LKrHRKzyMN7HMqIxeORZ7iakRZYmEjRO9Q+806F7WXw5kUxsQnDh
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN:	*DigitalSign Qualified CA - G4*
Issuer OU:	*Class 2 DigiCert PKI Platform Individual Subscriber CA*
Issuer O:	*DigitalSign - Certificadora Digital*
Issuer C:	*PT*
Subject CN:	*DigitalSign TSA - G9*
Subject O:	*DigitalSign - Certificadora Digital*
Subject 2.5.4.97:	*VATPT-507015851*
Subject C:	*PT*
Valid from:	*Thu Jul 30 02:00:00 CEST 2020*
Valid to:	*Thu Jul 30 01:59:59 CEST 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:DC:F7:1C:7E:12:E5:E3:BB:AC:00:0A:3B:76:EF:19:6C:74:66:2C:93:49:59:5A:F7:C3:C0:99:9A:D9:C9:1D:24:E2:E0:33:15:C9:27:5B:E3:49:F3:A1:C7:05:3A:DE:2D:4F:7F:DA:FB:1D:AD:52:C9:D3:03:05:26:04:01:0A:DB:C8:CD:6A:54:DC:72:3B:75:04:9F:DC:19:69:43:84:15:34:2A:1B:42:28:3C:EE:71:92:0B:96:CD:90:E4:8D:9E:21:4B:54:0F:0D:CF:6E:AE:64:BF:5F:09:22:1F:4B:6C:C5:14:C8:21:0D:AC:24:08:09:76:0A:B7:64:7F:EB:64:9E:B4:E9:8B:75:E2:D4:23:55:67:5F:50:AC:22:A0:79:68:07:2C:96:46:E9:A1:4D:76:08:CB:5A:73:8B:3A:DB:B1:49:3D:37:21:FB:2E:A0:81:71:DF:70:B5:61:A8:73:4F:32:7D:24:B3:7D:A1:E8:CF:6B:AC:76:FF:4F:C7:84:44:A5:5E:6F:E9:CA:29:99:86:89:C4:93:77:DC:A8:A9:00:5E:65:2D:24:E8:3C:89:FD:52:B0:11:11:43:5B:88:CA:4F:B9:14:19:CE:7B:75:8A:5B:71:D3:FB:07:2A:94:96:4A:AE:96:94:DF:42:E6:79:74:3D:B3:4E:1D:F8:91:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Alternative Name	*CN=DigitalSign TSA - G9, O=DigitalSign - Certificadora Digital, C=PT, SERIALNUMBER=VATPT-507015851*
Subject Key Identifier	*F1:23:D0:3D:22:44:D9:9B:2E:4E:71:EF:91:A1:B1:52:6F:26:C3:69*
Basic Constraints	*IsCA: false*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.8024.0.3* *CPS pointer: https://www.digitalsign.pt/ECDIGITALSIGN/cps* *CPS text: [https://www.digitalsign.pt/ECDIGITALSIGN/rpa]* *CPS text: [In the event of a conflict between the terms of BT CPS and the terms of DigitalSign CPS, the terms of BT CPS shall control.]*
CRL Distribution Points	*http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/LatestCRL.crl*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Authority Info Access	*http://std-ocsp.trustwise.com* *http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/ca.crt*
Authority Key Identifier	*D6:DF:0F:7A:1C:1D:5F:2C:52:2F:D8:B1:BE:D8:E9:79:1F:04:F9:7E*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4F:5D:C0:29:20:00:C3:67:27:E0:2C:FD:EA:54:12:41:FD:F3:7B:32:86:EF:A5:D9:9B:13:5B:5F:6A:11:58:60*

X509SubjectName

Subject CN: *DigitalSign TSA - G9*

Subject O: *DigitalSign - Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *8SPQPSJE2ZsuTnHvkaGxUm8mw2k=*

Service Status

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

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

Status Starting Time

2020-08-04T23:00:00Z

7.14 - Service (granted): DIGITALSIGN 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.*

Service Name

Name *[en]* *DIGITALSIGN QUALIFIED CA G1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *330444127560240380976396101945240260095972967226*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGxjCCBK6gAwIBAgIUOeGgjQYOPiLKP2cmoUmE5xNvgzowDQYJKoZIhvcNAQENBQAwYjELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIUIRgZZlOYWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDErNMCUG
A1UEAwweRElHSVRBTFNjR04gR0xPQkFMIFJPT1QgUlNBIENBMB4XDTIxMDEyMjEwMTE1MFoXDTMz
MDExOTEwMTE1MFowXzELMAkGA1UEBhMCUFQxKjAoBgNVBAoMIURpZZlOYWxTaWdulENlcnRpZmlj
YWRvcmEgRGlnaXRhbDEkMCIGA1UEAwwbRElHSVRBTFNjR04gUVVBTElGSUVEIENBIEcxMIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAzsLUgL6D++qIEVSlk2jZBuI6KtVAKJomNMhCnWW
eOobV679YoBE0FOFEBMKRQ+Cn5MaLV1SxZJhbiGIWF8os9Gx25zDHanvz9bhhYGnnBskyvn4OFEF
wsCYQ3Q9J7+qb6r4/beToE7GMQoSh0JolTMLsxn2bwSFHg80jNkOJnNOwEQtdgT/HYu/QHnLQGx5
/iyaM7ux55mtOdysm3bEwZfhGdjoXpT078iMGSOPv2C2pMfSUtLUzL2BHZDYUw3NC3Sgzehqkoez
9EFMEFDvoot+uXlG1Jn6EObiLsM53X1on3n7MEYtyzrRnlcxcFA32R83Q++fWkuqUVthE3XKpnc8
POaDmbGHA8xfCM20jKO59BNRwIjdp0M359EyNSBEBUGki7NKqJkETgMgS/f7dzemLOYRh8OtHg9P
INAQ+2gbVyPIG/dxwF/EvK7ipSWkP/l1YcFdGxCtySTmBkDOtmenGJUDxQ7lGGFqRFVZKq4yix0l
p//VGuXUqbSRmxUIVFtX5PLJWQfczklcVdKY7YYu/7RzHcDSHTWIMwOr8slNOzNdei66vFjmgkry
K0lNjGy2jrd48QT279iiQls3uYAtvCKxi+B6gv+uhi2RZsTxpjDUevd3qpnRYZyUzajuUkeM8ituR
Bm+UQl+foKAKdqvyE2ZDJcjVvKftoh0NoBUCAwEAAaOCAXUwggFxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwHwYDVR0jBBgwFoAUtTa8Plwaqyz2WRktgxTakyUV1oYwWQYIKwYBBQUHAQEETTBLMEkGCCsG
AQUFBzAChj1odHRwOi8vcm9vdC1yc2EuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNjR05HTE9CQUx5
T09UUlNBQ0EucDdiMEEGA1UdIAQ6MDgwNgYLKwYBBAGBx3wEAQEwJzAlBggrBgEFBQcCARYZaHR0
cDovL3Bra55kaWdpdGFsc2lnbi5wdDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwTgYD
VR0fBEcwRTBDoEGgP4Y9aHR0cDovL3Jvb3QtcnNhLmRpZ2lOYWxzaWduLnB0L0RjR0lUQUxTSUdO
R0xPQkFMUk9PVFJTQUNBLmNybDAdBgNVHQ4EFgQUc0nxQBwUBHyaEn/6L81cZyMY6RQwDgYDVR0P
AQH/BAQDAgEGMA0GCSqGSIb3DQEBDQUAA4ICAQAF1it2joqAVDLZNqvYXO/u7e3GroVGfz+u6ymM
ONcvjpu9dYvWrNARPEwXxBWc/EBa9VcB3ejEupOiBjVrggfOlqM2nEvwOD4nMn+cpSvLBsdxcD2o
SI+cUHRazC5Buy9K7gxuKxYtuKzPhntDr+ge8QS+Nf75csqgqjmRvsQKWZRwF2+R5APzebGYbf1/
Pw80iKfqLAm1mi0SU1JmWqn+2xKfz/vE7bicU3yOOFfrtWi1N1KbeKZjEg8BiH5peKJGSd/v3qgz
fQNwls/Uj1etxzcgpZZnrfpvM5equuVPiTKga+t1moSjTVb0bOTDqzUkVs0wY0LDNV1LpKHq/l93
CN22ZLNVcEEKcPRgOo8sx+FmDMpJUk3ayKJJPBQ1MgY9+BTA38kRAYh1clCU5Na8tm0gdcvkAQ
fuR57naJRcgGwn6Dk6AbogsjUOlJlyCjDkC81B2YcEdJh201vTMrmmtOu+RXzzJm4UZBI1j92Mv
yChBq/oses76UCN4terl4vLjd1+krxdT55u3v9vee0OwmvTmLE4DLgUzxX+/Zqnzz+ik044yz4ip
0X/ZlH/9CvRvBQ4et7nrOKliiFkrYL35eu+nyEAQYGqtHfhk4629v7qEdrFXkrqO/buWsht98rRW
pXyYbumAYv2oEpPvc47R87eM5z+D8KFikaR/dg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT RSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN QUALIFIED CA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

Valid from: *Fri Jan 22 11:11:50 CET 2021*

Valid to: *Wed Jan 19 11:11:50 CET 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:CE:C2:D4:80:BE:83:FB:EA:A5:11:54:88:29:DD:A3:64:1B:94:E8:AB:55:00:A2
:68:98:D3:21:0A:75:96:78:EA:1B:57:AE:FD:62:80:44:D0:53:85:10:13:0A:45:0F:82:9F:93:1A:2D:59:79:C7:62:61:6E:21:88:58:5F:28:83:D1:B1:DB:9C:C3:1D:A9:EF:CF:D6:E1:85:51:A7:9
C:1B:24:CA:F9:F8:38:51:05:C2:C0:98:43:74:3D:27:BF:AA:6F:AA:F8:FD:B7:93:A0:4E:C6:31:0A:12:87:42:68:95:33:0B:B3:19:F6:6F:04:85:1E:0F:34:8C:D9:0E:26:73:4E:C0:44:2D:76:04:F
F:1D:8B:BF:40:79:CB:40:6C:79:FE:2C:9A:33:BB:81:E7:99:AD:39:DC:AC:9B:76:C4:C1:97:E1:19:D8:E8:5E:94:F4:EF:C8:8C:19:23:8F:BF:60:B6:A4:C7:D2:51:F2:D4:CC:BD:81:1D:90:D8:5
3:0D:CD:0B:74:A0:CD:E8:6A:92:82:F3:F4:41:4C:10:50:EF:A2:8B:7E:B9:79:46:D6:59:FA:10:E6:C8:2E:C3:39:DD:7D:68:9F:79:FB:30:46:2D:CB:3A:D1:9E:57:31:70:50:37:D9:1F:37:43:EF:
9F:5A:4B:AA:51:5B:61:13:75:CA:A6:77:3C:3C:E6:83:99:B1:87:03:CC:5F:08:CD:B4:8C:A3:B9:F4:13:51:C0:88:DD:A7:43:37:4B:D1:32:35:20:44:05:41:A4:8B:B3:4A:A0:99:04:4E:A3:20:4
B:F7:FB:77:37:A6:2C:E6:11:87:C3:AD:1E:0F:4F:94:D0:10:FB:68:18:57:23:C8:1B:F7:71:C0:5F:C4:BC:AE:E2:A5:25:A4:3F:F2:35:61:C1:5D:1B:10:AD:C9:24:E6:06:40:CE:B6:67:A7:18:95:
03:C5:0E:E5:18:61:6A:44:55:59:2A:AE:32:88:1D:08:A7:FF:D5:1A:E5:D4:A9:B4:91:98:15:08:54:5B:57:E4:F2:C9:59:07:DC:CE:49:5C:55:D2:98:ED:86:2E:FF:B4:73:1D:C0:D2:1D:35:88:3
3:03:AB:F2:C9:4D:3B:33:5D:7A:2E:BA:BC:58:E6:82:4A:F2:2B:49:4D:8C:6C:B6:8E:B7:78:F1:04:F6:EF:D8:A2:40:8B:37:B9:80:2D:BC:22:B1:8B:E0:7A:82:FF:AE:86:2D:91:66:C4:F1:A6:30:
D4:7A:F7:77:AA:99:D1:61:9C:94:CD:A8:EE:52:47:8C:F3:CB:91:06:6F:94:42:5F:9F:A0:A0:0A:76:AB:F2:13:66:43:25:C8:D5:BC:A7:ED:A2:1D:0D:A1:B5:02:03:01:00:01
```


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

Authority Key Identifier *B5:36:BC:3C:8C:1A:AB:2C:F6:59:19:2D:83:14:DA:93:25:15:D6:86*

Authority Info Access *http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.p7b*

Certificate Policies

Policy OID: 1.3.6.1.4.1.25596.4.1.1

CPS pointer: http://pki.digitalsign.pt

Extended Key Usage *id_kp_clientAuth*

CRL Distribution Points *http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.crl*

Subject Key Identifier *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *27:BB:49:D2:06:B6:DE:C1:61:EB:B8:EA:73:95:30:E9:0A:C6:84:98:D2:EE:A0:5A:7E:D9:60:3D:1D:CE:0F:D5*

X509SubjectName

Subject CN: *DIGITALSIGN QUALIFIED CA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *c0nxQBwUBHyaEn/6L81cZyMY6RQ=*

Service Status

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

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

Status Starting Time

2021-03-25T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://pki.digitalsign.pt/*

7.14.1 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement, QCForESig, QCForESeal, QCQSCDManagedOnBehalf]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

7.14.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.14.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.15 - Service (granted): DIGITALSIGN QUALIFIED CA V1

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]* *DIGITALSIGN QUALIFIED CA V1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *605964386803062595644947631554319857491063941952*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDgTCCAwegAwIBAgIUaiRiA7dayDHVuPOjlkXMgnNlK0AwCgYIKoZIzj0EAwMwZDELMAkGA1UE
BhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEpMCcGA1UE
AwwgREIHSVRBTFNJR04gR0xPQkFMIFJPT1QgRUNEU0EgQ0EwHhcNMjEwMTIyMTAxMDQ5WhcNMzMw
MTE5MTAxNDQ5WjBfMQswCQYDVQQGEwJQVDEqMCgGA1UECgwhRGlnaXRhbFNpZ24gQ2VydGlmaWNh
ZG9yYSBEaWdpdGFsMSQwIgYDVQQDDBtESUdlVEFMU0lHTiBRVUFMSUZJRUQgQ0EgVjEwdjAQBgcq
hkjOPQIBBgUrgQQAIgNiAAT6uZGkAu81CD6CJQ13RopDinrnI2SZVFRI4t3FgJfO6ouKaltm3a4F
9tCz4juZoo7ECCQgy5ENvHDJFvW68QxB660AqapMeGrmgqeq0S1ENCd4gZ6Tbfo0gKyuLnX4Gib2j
qgF9MIIBeTASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFM6v5osadeLxOOcC8BatXupk
1Xu0MF0GCCsGAQUFBwEBBFEwTzBNBggrBgEFBQcwAoZBaHR0cDovL3Jvb3QtZWNkc2EuZGlnaXRh
bHNpZ24ucHQvRElHSVRBTFNJR05HTE9CQUxST09URUNEU0FDQS5wN2lwOQYDVR0gBDowODA2Bgsr
BgEEAYHHfAQBATAnMCUGCCsGAQUFBwIBFhlodHRwOi8vcGtpLmRpZ2I0YWxzaWduLnB0MB0GA1Ud
JQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBSBgNVHR8ESzBJMEegRaBDhkFodHRwOi8vcm9vdC1l
Y2RzYS5kaWdpdGFsc2lnbi5wdC9ES0UdJVEFMU0lHTkdMT0JBTFJPT1RFQ0RTQUNBLmNybDAdBgNV
HQ4EFgQU1x7k/OwS5Ut56vj8aU8MkSYls6IwDgYDVR0PAQH/BAQDAgEGMAoGCCqGSM49BAMDA2gA
MGUCMQC64F14UaJOL7e76h3fCHVlZcNF1uCtW9cmh/G5M1CTGow0VfPQbYxOejOFye/YpECMGRn
mmNWhCwwNB35gbHLGiUOH3xZYEA4nTvjAPfimyf+U9lx/tdm08c6C1/348iXAQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT ECDSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN QUALIFIED CA V1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

Valid from: *Fri Jan 22 11:14:49 CET 2021*

Valid to:	*Wed Jan 19 11:14:49 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:FA:B9:91:A4:02:EF:35:08:3E:82:25:0D:77:46:8A:43:8A:7A:E7:97:64:99:54:54:48:E2:DD:C5:80:97:CE:EA:8B:8A:68:8B:66:DD:AE:05:F6:D0:B3:E2:3B:99:A2:8E:C4:08:24:20:CB:91:0D:BC:70:FF:16:F5:BA:F1:0C:7C:EB:AD:00:A9:AA:4C:78:69:A0:A9:EA:B4:4B:51:0D:09:DE:20:67:A4:DB:7E:8D:20:2B:2B:8B:9D:7E:06:89:BD*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*CE:AF:4A:8B:1A:75:E2:F1:38:E7:02:F0:16:AD:5E:EA:64:D5:7B:B4*
Authority Info Access	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.crl*
Subject Key Identifier	*D7:1E:E4:FC:EC:12:E5:4B:79:EA:F2:7C:69:4F:0C:91:26:08:B3:A2*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*4A:2B:2B:0F:84:29:A7:7E:23:BC:AB:8F:FA:25:3F:4C:21:36:8C:B4:AA:2A:78:DB:C5:D4:17:C6:D1:D0:E1:05*

X509SubjectName

Subject CN:	*DIGITALSIGN QUALIFIED CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*1x7k/OwS5Ut56vJ8aU8MkSYIs6I=*

Service Status

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

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

Status Starting Time

2021-03-25T00:00:00Z

Scheme Service Definition URI

URI *[en]* *https://pki.digitalsign.pt/*

7.15.1 - Extension (critical): Qualifiers [QCSSCDStatusAsInCert, QCStatement, QCForESig, QCForESeal, QCQSCDManagedOnBehalf]

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 presence or absence of Secure Signature Creation Device (SSCD) support DO contain the machineprocessable information indicating whether or not the Qualified Certificate is supported by an SSCD.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Description

7.15.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.15.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

7.16 - Service (granted): DigitalSign Qualified TSA 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.*

Service Name

Name *[en]* *DigitalSign Qualified TSA G1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *518761864678796083844472466064387558743772037025*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGGDCCBACgAwIBAgIUWt4Wj2FBQFTa0QArS49vEVRg/6EwDQYJKoZIhvcNAQENBQAwYzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmlyYWRvcmEgRGlnaXRhbDEpMCYG
A1UEAwwfRElHSVRBTFNJR04gUVVBTEIGSUVEIFRTQSBDQSBHMTAeFw0yMTAyMjYxNTIwMjdaFw00
NjAxMTUxMDUwMzRaMHoxC2AJBgNVBAYTAlBUMRgwFgYDVQRhDA9WOVRQVC01MDcwMTU4NTExKjAo
BgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmlyYWRvcmEgRGlnaXRhbDElMCMGA1UEAwwcRGlnaXRh
bFNpZ24gUXVhbGlmaWVkIFRTQSBHMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK0k
37G1MTBznuXSy79VjLNNm5hcQayo3zBu3rZYXDGspSLFWRnA3p7cINK6eciIJ06Sscp+qmrJWGSWf
0W5WStKSN9vK9cljesWkG/l0/wgPlgIT63Crrv8hQHNJftpSDt39HMAYaDxXJmDTfXQ7OcITULv0
Z8EhktEGAH8FbRGpt8sb+Qmc5gEX32s7JG2H9ge/tyhsHu27M8jm6JBaqG/rsDfJSpFl5esIXa9/
2KVhsXaitnXO/N4J4OHedNSfBwHBqV+Za77OZDdMNX7Gy2HaLZOPlC9Mb+pOd9Iw5WFN85AmS1u3
yo7fbThOoHEdtW4rQs3oi2Dcqgx4N5QZq/0CAwEAAaOCAaswggGnMAwGA1UdEwEB/wQCMAAwHwYD
VR0jBBgwFoAUvLW/rC61RnHowVDsnsXnAcD3lwwgYkGCCsGAQUFBwEBBH0wezBJBggrBgEFBQcw
AoY9aHR0cDovL3F0c2EtZzEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZJRURUU0FD
QUcxLnA3YjAuBggrBgEFBQcwAYYiaHR0cDovL3F0c2EtZzEuZGlnaXRhbHNpZ24ucHQvb2NzcDBT
BgNVHSAETDBKMDYGCysGAQQBgcd8BAEBMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wa2kuZGlnaXRh
bHNpZ24ucHQwEAYOKwYBBAGBx3wEAgECAQIwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwTgYDVR0f
BEcwRTBDoEGgP4Y9aHR0cDovL3F0c2EtZzEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFM
SUZJRURUU0FDQUcxLmNybDAdBgNVHQ4EFgQU3aPAYY3N8TTtAOPv6t8c9UHs+REwDgYDVR0PAQH/
BAQDAgbAMA0GCSqGSIb3DQEBDQUAA4ICAQAOHr90AxRYsSLL7LIpJ9YFPo6Rp7fSjmIkyM1YR7y
uwzODP/LFCbLkU1fX+fQXYqFeBk4GhDQbEVcF4sC3QZfspfXElXFosZIr8TdV2b4vYbDa9bPVg+o
IzlcEtQuxjHY+bnqOECJgVfBS98wdgSZ2jczbYfiR6fT0m+isvm3wfjzxb0rmUy6Qx37zfcarKZB
f98653BJ5Ifqm9FaQba6oi3HqghVSdc0TDFTSJYe4F6odIIlMX31T3nDUPr8tijGwxqzr+VL+nZA
8edPba49aY8UvJlwSxqP+Mir0gdYAgCGKM9OXVsrgMFajE/0TtZOobecdmtYhHDYFpRLCIlFHHf
0IjKwZUTOIkcKdIhmXihcElsYDt4nfSXERXjytCK7dmbihzaa5u0mcy1HIlPav+pHBFQVrdBxV/Qt
XxMM39rU1/bqJ3mCCgwL+Wq84rN1rs2pLQuR6RX6Dv8TpkJRV7hi7Q68cAJo9gC2EVBzvNbhxBr4
RwrekQsUgC4R0hVuZraG7ov79SRvmDTzQR8KC7yCPFnJ80sCfjX+XFPD+ssGfE0MZGsm88wyCk7n
ZFX8k9ku/93NuhzKEMGpm5Bw/x9naJXT2dh3Y5k1RINaWepW4Q7G6zReiCXe3J+UDxnQR93pMGHu
5hf9blCanstjyKHKVRk9rzDw1B5pPxej9Q==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED TSA CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DigitalSign Qualified TSA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

Valid from: *Fri Feb 26 16:20:27 CET 2021*

Valid to: *Mon Jan 15 11:50:34 CET 2046*

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:24:DF:B1:B5:31:30:73:9E:E5:D2:CB:BF:55:24:B3:4D:9B:98:5C:41:AC:A8
:DF:30:6E:DE:B6:58:5C:31:AC:A5:22:C5:59:19:C0:DE:9E:DC:94:D2:BA:79:C8:94:D3:A4:AC:72:9F:A0:9A:B2:56:19:25:9F:D1:6E:56:4A:D2:92:37:DB:CA:F5:C2:63:7A:C5:A4:1B:F2:34:FF:
08:0F:96:09:53:EB:70:AB:AE:FF:21:40:73:49:7E:DA:52:0E:DD:FD:1C:C0:18:68:3C:57:26:60:D3:7D:74:3B:D1:C9:53:50:BB:F4:67:C1:21:2A:D1:06:00:7F:05:6D:11:A9:B7:CB:1B:F9:09:9
C:E6:01:17:DF:6B:3B:24:6D:87:F6:A7:BF:B7:28:6C:1E:ED:BB:33:C8:E6:E8:90:5A:A8:6F:EB:B0:37:C9:4A:91:65:E5:EB:08:5D:AF:7F:D8:A5:61:B1:76:A2:B6:75:CE:FC:DE:09:E3:41:DE:74
:D4:9F:07:01:C1:A9:5F:99:6B:BE:F4:64:37:4C:35:7E:C6:CB:61:DA:2D:9D:0F:20:2F:4C:6F:EA:4E:77:D8:B0:E5:61:4D:F3:90:26:4B:5B:B7:CA:8E:DF:6D:38:4E:A0:71:1D:B5:6E:2B:42:CD:
E8:8B:60:DC:AA:0C:78:37:94:19:AB:FD:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *BC:B5:BF:AD:C4:BA:D5:19:C7:A3:05:43:B2:7B:17:9C:07:03:DE:5C*

Authority Info Access

http://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.p7b

http://qtsa-g1.digitalsign.pt/ocsp

Certificate Policies

Policy OID: 1.3.6.1.4.1.25596.4.1.1

CPS pointer: http://pki.digitalsign.pt

Policy OID: 1.3.6.1.4.1.25596.4.2.1.2.1.2

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.crl*

Subject Key Identifier *DD:A3:C0:61:8D:CD:F1:34:ED:00:E3:EF:EA:DF:1C:F5:41:EC:F9:11*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BA:AB:49:4E:BD:06:B3:43:C4:3F:34:87:40:69:F6:D5:D6:61:D9:7B:63:B4:32:6F:BF:2C:D8:65:02:49:2C:31*

X509SubjectName

Subject CN: *DigitalSign Qualified TSA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *3aPAYY3N8TTtAOPv6t8c9UHs+RE=*

Service Status

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

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

Status Starting Time

2021-03-25T00:00:00Z

7.17 - Service (granted): DigitalSign Qualified TSA V1

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.*

Service Name

Name *[en]* *DigitalSign Qualified TSA V1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *488141604512698919887271549117539492817617275583*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDyTCCA0+gAwIBAgIUVYEGzkPX1LPqZOARtFctEu3Hyr8wCgYIKoZIzj0EAwMwYzELMAkGA1UE
BhMCUFOxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEoMCYGA1UE
AwwfREIlHSVRBTFNJR0dpUVV8TEIGSUVEIFRTQSBDQSBWMTAeFw0yMTAyMjYxNTA4NTdaFw00NjAx
MTUxMTA3NTBaMHoxC2AJBgNVBAYTAlBUMRgwFgYDVQRhDA9WQVRQVC01MDcwMTU4NTExKjAoBgNV
BAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDElMCMGA1UEAwwcRGlnaXRhbFNp
Z24gUXVhbGlmaWVkIFRTQSBWMTB2MBAGByqGSM49AgEGBSuBBAAiA2IABJjIFsgWwAsM/cjIFOWk
VykfchcGkI0ywUBZzylc7nAmvc74Oz0Il8tVSfNTn/MRWcdYFAmdRnznomVN5jwpdveRD/+zACuuD
8dgzVMNtbejWswGXlPplJEJdgeDLMbioHaOCAaswggGnMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUDSMrFhIXIkvtx/alHRpfG5g02gcwgYkGCCsGAQUFBwEBBH0wezBJBggrBgEFBQcwAoY9aHR0
cDovL3F0c2EtdjEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZjRURUU0FDQVYxLnA3
YiAuBggrBgEFBQcwAYYiaHR0cDovL3F0c2EtdjEuZGlnaXRhbHNpZ24ucHQvb2NzcDBTBgNVHSAE
TDBKMDYGCysGAQQBgcd8BAEBMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wa2kuZGlnaXRhbHNpZ24u
cHQwEAYOKwYBBAGBx3wEAgICAQIwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwTgYDVR0fBEcwRTBD
oEGgP4Y9aHR0cDovL3F0c2EtdjEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZjRURU
U0FDQVYxLmNybDAdBgNVHQ4EFgQU3M791/shfZak7pLDwrE1k+wsH6wwDgYDVR0PAQH/BAQDAgbA
MAoGCCqGSM49BAMDA2gAMGUCMDkpZvshBh06zGobwYf5MSbqYWNknZ2x4eWJC2as8TmO1hr0DON1
+YCctsKQU0pkTAIxAMnh17GXSxxMsIj5Qwlt9Q32Rbrwht4Bp6rC1057zWqo54O4B+1pUTvd98aN
PD9WLg==

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA384withECDSA*
Issuer CN:	*DIGITALSIGN QUALIFIED TSA CA V1*
Issuer O:	*DigitalSign Certificadora Digital*
Issuer C:	*PT*
Subject CN:	*DigitalSign Qualified TSA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject 2.5.4.97:	*VATPT-507015851*
Subject C:	*PT*
Valid from:	*Fri Feb 26 16:08:57 CET 2021*
Valid to:	*Mon Jan 15 12:07:50 CET 2046*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:82:48:16:C8:16:C0:0B:0C:FD:C8:E5:14:E5:A4:57:29:1F:72:17:06:90:8D:32:C1:40:76:CE:F2:5C:EE:60:26:BD:CE:F8:3B:3D:08:23:CB:55:4A:13:53:9F:F3:11:59:C7:58:14:09:9D:46:7C:E8:99:53:79:8F:0A:5D:C9:E4:43:FF:EC:C0:0A:EB:C3:F1:D8:33:54:C3:6D:6D:E2:56:B3:01:97:94:FA:65:8C:42:5D:81:E0:CB:31:B8:A8:1D*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*0D:23:2B:16:12:17:96:4B:ED:C7:F6:A5:1D:1A:5F:1B:98:34:DA:07*
Authority Info Access	*http://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.p7b* *http://qtsa-v1.digitalsign.pt/ocsp*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.2.2.1.2*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.crl*
Subject Key Identifier	*DC:CE:FD:D7:FB:21:7D:96:A4:EE:92:C3:C2:B1:35:93:EC:2C:1F:AC*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F3:24:19:96:B1:05:5B:1D:82:70:05:41:D4:8D:9A:EB:D0:00:21:C7:E2:C8:CD:C1:BC:B5:F9:C4:87:C8:C7:E2*

X509SubjectName

Subject CN:	*DigitalSign Qualified TSA V1*

Subject O: *DigitalSign Certificadora Digital*

Subject 2.5.4.97: *VATPT-507015851*

Subject C: *PT*

X509SKI

X509 SK I *3M791/shfZak7pLDwrE1k+wsH6w=*

Service Status

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

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

Status Starting Time

2021-03-25T00:00:00Z

7.18 - Service (recognisedatnationallevel): DIGITALSIGN CA G1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

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

Service Name

Name *[en]* *DIGITALSIGN CA G1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *570806727660964086140439467596184100247562728 95*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGvDCCBKSgAwIBAgIUCf+V/PG3aAwjiPsiEtoNborfXv8wDQYJKoZIhvcNAQENBQAwYjELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEnMCUG
A1UEAwweRlHSVRBTFNJR04gR0xPQkFMIFlPT1QgUlNBIENBMB4XDTIxMDEyMjEwMTM0MFoXDTMz
MDExOTEwMTM0MFowVTELMAkGA1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmlj
YWRvcmEgRGlnaXRhbDEaMBgGA1UEAwwRREHSVRBTFNJR04gQ0EgRzEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDfXQWQfBci8x/etk26O7Rh5ZHgf5cOYVk5RPHLjJntCcX6eRp5Y7iH
RF9BEGtMwsLwVZmd8Hjbc1i2akDZ4vJhCKf8tDMpQqtorvz08LovzReYPZok53pAduEPzglNI9JG
1JtatBZ5iQxREhbACdBaSrCjRtd82w/wen2ce/hKy4B1JHLR4Y6dYb34TcetX7DK7/jkjKizKeAL
UfB8cy+fjKpfuGoHCwPzd2Mg7kLqYuC9K2HD6viYUKfiDJgVA6En548G5vSSrownvJLEZAzUsvYH
y6EVLcBdQYvxb2+0oQHg92HzwoPG+h7Yk2BK9nxiIM8ctGeuryl5fbgKLX+52HX1BqOY0vkPoV4U
sVcmiEbLhcTaDGfGtfXv9j85K3HaglI2dJXWAU1DtxPEBx2F/FtxHRCTh4X/00HP0XygQHjUS2EuG
CzBMu91A6S+wKV0XsLXjQ65J5D1827jyApkQpH9bgrHj/aEijcM/kZqPX9mpSZXjH9tC6/khr7mL
xVm1Kookiz7/kS//W655MhbBn9CV+Aub+ceuSpBVVQeEq44JMy0hyr0Zvajz3VjhHf5aYGay5edGi
0WzR1NTsHoZKD8g8YNn1m1hI3IzQH0Tks803Kst5d5gyp82lfW4s9ywNn+k1kodbKYoCBelNMuEA
kXoi9H+rpLrcG33tNrm9kQIDAQABo4IBdTCCAXEwEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSME
GDAWgBS1Nrw8jBqrLPZZGS2DFNq7JRXWhjBZBggrBgEFBQcBAQRNMEswSQYIKwYBBQUHMAKGPWh0
dHA6Ly9yb290LXJ2YS5kaWdpdGFsc2lnbi5wdC9ESUdlVEFMU0lHTkdMT0JBTFJPT1RSU0FDQS5w
N2IwQQYDVR0gBDowODA2BgsrBgEEAYHHfAQBATAnMCUGCCsGAQUFBwIBFhlodHRwOi8vcGtpLmRp
Z2I0YWxzaWduLnB0MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBOBgNVHR8ERzBFMEOg
QaA/hj1odHRwOi8vcm9vdC1yc2EuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05HTE9CQUxST09U
UlNBQ0EuY3JsMB0GA1UdDgQWBBQRucfjuAMQxKos941uhLFg1GRVjAOBgNVHQ8BAf8EBAMCAQYw
DQYJKoZIhvcNAQENBQADggIBAB3ssszzegqwl+NJsp33m5M9aBMBu++++qfCuA/LqCSQZc48I9nlhT
LHJOViNzP6a7eMRZWds4ZUA2/R9KK0ASmOnNS1C0R1rEvsJvWU4z1P5yVGapxmLgjfOTOXfKBpGU
6npXC+qjJKDvHxUceZQfU+R50zfPsTc/AQSxDIIMGCfLM3SZSZV4sSQEBXjNGbmKWHW44foiRR2J
DQYKoZIhvcNAQENBQADggIBAB3ssszzegqwl+NJsp33m5M9aBMBu++++qfCuA/LqCSQZc48I9nlhT
LHJOViNzP6a7eMRZWds4ZUA2/R9KK0ASmOnNS1C0R1rEvsJvWU4z1P5yVGapxmLgjfOTOXfKBpGU
6npXC+qjJKDvHxUceZQfU+R50zfPsTc/AQSxDIIMGCfLM3SZSZV4sSQEBXjNGbmKWHW44foiRR2J
JIDRAzrm8x0C6jrF0Sr4VtSx0n6yyLJ8l951f8KV+xRs2EFh4i+0RFOQ4sTxyaYPPkEVZjXmsdOr
XAVuh+KaVTG0IwPdkWHsUagJctfPT0CVs2e2RiSkjvF/L5PJXW/KUC+o59vqLDlszCXL055usrQh
4BCgInr4161l/1bHmPCvaF2zQacxiY4YW8Gn9clCZARbKbMo62/atbhNQfIYxDc8Y36KdBH31fab
kBWev2gq9PlhMCtygM575oYexo4+yjKm7VntlnK+D56aCqRrZriwQHYHPdpUWOyV+raoV5KRUCpx
XoTkRbcs21esjLYtjelUrWLjTCco2OpOnwmcPRKp2siSzVhxWqcGAs7AwzcWdgpsznYgtCGtMlnL
kMCYSHyuiqBZ6BXC+vexJeaPVSQ8gZfZsasvjfqYiLrdroYu55Ez0FYk3Tb9diFUVE2Uw3pSWArI
eJw3s0IohtUXFMtp1X5dQ0Y1

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT RSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C:	*PT*
Subject CN:	*DIGITALSIGN CA G1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*
Valid from:	*Fri Jan 22 11:13:40 CET 2021*
Valid to:	*Wed Jan 19 11:13:40 CET 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:DF:5D:05:90:7C:17:22:F3:1F:DE:B6:4D:BA:3B:B4:61:E5:91:E0:7F:97:0E:61:59:39:44:F1:CB:8C:99:ED:09:C5:FA:79:1A:79:63:B8:87:44:5F:41:10:6B:4C:C2:C2:F0:57:39:9D:F0:78:DB:73:58:B6:6A:40:D9:E2:F2:61:08:A7:FC:B4:33:29:42:AB:68:AE:FC:F4:F0:BA:2F:CD:17:98:3D:9A:24:E7:7A:40:76:E1:0F:CE:02:0D:23:D2:46:D4:9B:5A:B4:16:79:89:0C:51:12:16:C0:09:D0:5A:4A:B0:A3:46:D7:7C:DB:0F:F0:7A:7D:9C:7B:F8:4A:CB:80:75:24:72:D1:E1:8E:9D:61:8D:F8:4D:C7:AD:5F:B0:CA:EF:F8:E4:8C:A8:B3:29:E0:0B:51:F0:7C:73:2F:9F:8C:AA:5F:B8:6A:07:0B:03:F3:77:63:20:EE:42:EA:62:E0:BD:2B:61:C3:EA:F8:98:52:47:E3:0C:98:15:03:A1:27:E7:8F:06:E6:F4:92:AE:8C:27:BC:92:C4:64:0C:D4:B2:F6:07:C8:A1:15:2D:C0:5D:41:8B:F1:6F:6F:B4:A1:01:E0:F7:61:F3:C2:83:C6:FA:1E:D8:93:60:4A:F6:7C:62:20:CF:1C:B4:67:AE:AF:29:79:7D:B8:0A:2D:7F:B9:D8:75:F5:06:A3:98:D2:F9:0F:A1:5E:14:B1:57:26:B8:46:CB:85:C4:DA:0C:67:C6:B5:F5:EF:F6:3F:39:2B:71:DA:80:8D:9D:25:75:80:53:50:ED:C4:F1:01:C7:61:7F:16:DC:47:44:24:E1:E1:7F:F4:D0:73:F4:5F:28:10:1E:35:12:D8:4B:86:0B:30:4C:BB:DD:40:E9:2F:B0:29:5D:17:B0:B5:E3:43:AE:49:48:3D:7C:DB:B8:F2:02:99:34:A4:7F:5B:82:B1:E3:FD:A1:22:8D:C3:3F:91:9A:8F:5F:D9:A9:49:95:E3:1F:DB:42:EB:F9:21:AF:B9:8B:C5:59:B5:2A:8A:24:8B:3E:FF:91:2F:FF:5B:AE:79:32:16:C1:9F:D0:95:F8:0B:9B:F9:C7:AE:4A:90:55:55:07:84:AB:8E:09:33:2D:21:CA:BD:19:BD:A2:73:DD:68:E1:1D:26:98:19:AC:B9:79:D1:A2:D1:6C:D1:D4:D4:EC:1E:86:4A:0F:C8:3C:60:D9:F5:9B:58:48:DC:8C:D0:1F:44:E4:B3:CD:37:2A:CB:79:77:98:32:A7:CD:88:7D:6E:2C:F7:2C:0D:9F:E9:35:92:87:5B:29:8A:02:05:E9:4D:32:E1:00:91:7A:22:F4:7F:AB:A4:BA:DC:1B:7D:ED:36:B9:BD:91:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*B5:36:BC:3C:8C:1A:AB:2C:F6:59:19:2D:83:14:DA:93:25:15:D6:86*
Authority Info Access	*http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.crl*
Subject Key Identifier	*11:B9:C7:DC:8E:E0:0C:43:12:A8:B3:DE:35:BA:12:C5:83:51:91:56*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*95:1B:52:3C:9B:7F:D5:9A:F6:FA:E2:E0:54:D9:7F:2B:93:71:A4:1D:F7:52:D6:32:95:B3:BB:93:F3:C5:05:9C*

X509SubjectName

Subject CN:	*DIGITALSIGN CA G1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*EbnH3I7gDEMSqLPeNboSxYNRkVY=*

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

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

Status Starting Time *2023-01-20T11:39:50Z*

7.18.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.18.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.19 - Service (recognisedatnationallevel): DIGITALSIGN CA V1

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

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

Service Name

Name *[en]* *DIGITALSIGN CA V1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *183136785991872580233738707653933416685281504757*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDdzCCAv2gAwIBAgIUIBOjM2cqbV/0ryZ9KpY18bmUbfUwCgYIKoZIzj0EAwMwZDELMAkGA1UE
BhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEpMCcGA1UE
AwwgREIHSVRBTFNjR04gR0xPQkFMIFjPT1QgRUNEU0EgQ0EwHhcNMjEwMTIyMTAxNjEwWhcNMzMw
MTE5MTAxNjEwWjBVMQswCQYDVQQGEwJQVDEqMCgGA1UECgwhRGlnaXRhbFNpZ24gQ2VydGlmaWNh
ZG9yYSBEaWdpdGFsMRowGAYDVQQDDBFESUdlVEFMUI0lHTiBDQSBWMTB2MBAGByqGSM49AgEGBSuB
BAAiA2IABNuj5SlzLS67suHp1ZP6680z3xlwXECTW9mHdwyuW2cSG7fwcu5GbfAEVPulYQ3znAE4
hiMSWKAYtrDkTa+pc7ojLQ93RxPkc54mgnhSL5mA6qoc0bpYI1eMs3i3J93eyKOCAX0wggF5MBIG
A1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUzq9Kixp14vE45wLwFq1e6mTVe7QwXQYIKwYB
BQUHAQEEUTBPME0GCCsGAQUFBzAChkFodHRwOi8vcm9vdC1IY2RzYS5kaWdpdGFscZlnbi5wdC9E
SUdJVEFMU0lHTkdMT0JBTFJPT1RFQ0RTQUNBLnA3YjBBBgNVHSAEOjA4MDYGCysGAQQBgcd8BAEB
MCcwIQYIKwYBBQUHAgEWGWh0dHA6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwHQYDVR0lBBYwFAYIKwYB
BQUHAwIGCCsGAQUFBwMEMFIGA1UdHwRLMEkwR6BFoEOGQWh0dHA6Ly9yb290LWVjZHNhLmRpZ2I0
YWxzaWduLnB0L0RjR0lUQUxTSUdOR0xPQkFMUk9PVEVDRFNBQOEuY3JsMB0GA1UdDgQWBBSgOIMf
LJhHSXmojpbA+cePugPeLDAOBgNVHQ8BAf8EBAMCAQYwCgYIKoZIzj0EAwMDaAAwZQIxAIC6E5nm
AzhBgRoNNr+AMuRMVr7AxXFARPu4xgPwo5ee+rZ8mrYJXTGBu5alrh9OOQIwf6Hatua9fOWa4K4S
LreRlzxoaaeYIEHnVxu26+0G2xDh80lrHN0XZi7ut1fFq3G9
-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT ECDSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C:	*PT*
Subject CN:	*DIGITALSIGN CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*
Valid from:	*Fri Jan 22 11:16:10 CET 2021*
Valid to:	*Wed Jan 19 11:16:10 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:DB:89:E5:22:33:2D:2E:BB:B2:E1:E9:D5:93:FA:EB:CD:33:DF:19:70:5C:40:93:5B:D9:87:77:0C:AE:5B:67:12:1B:B7:F0:72:EE:46:6D:F0:04:54:FB:88:61:0D:F3:9C:01:38:86:23:12:58:A0:18:B6:B0:E4:4D:AF:A9:73:BA:09:2D:0F:77:47:13:E4:73:9E:26:82:78:52:2F:99:80:EA:AA:1C:D1:BA:58:97:57:8C:B3:78:B7:27:DD:DE:C8*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*CE:AF:4A:8B:1A:75:E2:F1:38:E7:02:F0:16:AD:5E:EA:64:D5:7B:B4*
Authority Info Access	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.crl*
Subject Key Identifier	*A0:40:83:1F:2C:98:47:49:79:A8:8E:96:C0:F9:C7:8F:BA:03:DE:2C*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C1:8C:8D:E1:0A:7B:02:AB:2A:70:0F:3E:95:EE:53:50:1D:C0:15:01:2F:AA:C1:97:B2:D6:4B:F2:EE:6D:FE:77*

X509SubjectName

Subject CN:	*DIGITALSIGN CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*oECDHyyYR0l5qI6WwPnHj7oD3iw=*

Service Status

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

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

Status Starting Time *2023-01-20T11:41:49Z*

7.19.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.19.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.20 - Service (recognisedatnationallevel): DIGITALSIGN TSA CA G1

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

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

Service Name

Name *[en]* *DIGITALSIGN TSA CA G1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *50237675565034491978700540231108212884312647895 6*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGtjCCBJ6gAwIBAgIUV/9aU6Dm4Gv52h5BcjncFHcaGGwwDQYJKoZIhvcNAQENBQAwYjELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEnMCUG
A1UEAwweRElHSVRBTFNJR04gR0xPQkFMIFJPT1QgUlNBIENBMB4XDTIxMDEyMjEwMTQxMVoXDTQ2
MDExNTEwNTAzNFowWTELMAkGA1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmlj
YWRvcmEgRGlnaXRhbDEeMBwGA1UEAwVRElHSVRBTFNJR04gVFNBIENBIEcxMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEA9BelH63V815UEyi5SSf8vEu0CWb28tAoITjNbTAPTri2I/E2
C9/iAZVpxzc4A3L7VH7pJ/QmFa9Wlwess2Gs1jykRgLslNIDQIH4WA/3Lvnfw6Ur1OURZ6AFptFK
fjfXsm8avsUlxRQP5S44AfjJbn1wQdOXlsqGOV7doP+AVXUiwcx7Kj/3uayJknETPBNHXqcIKNA3o
GbKKcM/1ir/9IyTcK0Ch6KZordQyHGTXCwf1+IvtEVIxviKA+op1s43tSjP606DuimYTEzxL2Ob
CKe17Ns61a6K2mr+wgBDUhOgbrsopkKjtfODAX44OuGEw/nJoYk3Jdxu+kYd6rw82azAlhojCOx2
z6hgK43mQjVHH6aVujj0pB/0Ft7BkbR9Am2M2uD2ARbKuVWeYkz1vU49faEBDC0R2rwiuYK5bNOg
/wsy31ITxp5+o2rdcm3SKfLwslHLsYzcnvesIMAv6QXWy+rEH1JD9HRcvG/y8P1N5E+M9H5/T5Kk
+PgDO1zsfwkpC3F1kPfkPW/+2EI7kbSsSQHMt5L1QpcM+K93OiED23Ii81JYtg5iIjIHN4o1VOUt
4T42O5KqLo26KfNw6ZHA+dm0GDFtEagYyGCwp3J7NfioXwRrmDNY6idxfVGUv0bOeFJ5VmsMuLYJ
nqpMxnjxkTroZSmrJdGWYFujjG8CAwEAAaOCAWswggFnMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYD
VR0jBBgwFoAUtTa8PIwaqyz2WRktgxTakyUV1oYwWQYIKwYBBQUHAQEETTBLMEkGCCsGAQUFBzAC
hj1odHRwOi8vcm9vdC1yc2EuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05HTE9CQUxST09UUlNB
Q0EucDdiMEEGA1UdIAQ6MDgwNgYLKwYBBAGBx3wEAQEwjzAlBggrBgEFBQcCARYZaHR0cDovL3Br
aS5kaWdpdGFsc2lnbi5wdDATBgNVHSUEDDAKBggrBgEFBQcCDBOBgNVHR8ERzBFMEOgQaA/hj1o
dHRwOi8vcm9vdC1yc2EuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05HTE9CQUxST09UUlNBQ0Eu
Y3jsMB0GA1UdDgQWBBQP81Q0AMxVktE0xA6m/fka6uMlVTAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZI
hvcNAQENBQADggIBAFth7fUaGRVobM4PVOwHdTTEyVKk8EPAIK0RpdZWjtcxqmLFO2+i/gGTQLaP
0A8rCBZ4+Lra/DVCINrcLeioHdcyxiodD04tXpYQsSeXoRK92RPyDDauxlTOOCcCh9EJOcERYKM5
KK0DvlzZjsACRbjpZPOoZKpv+i6Daq95n6HRhSMgDDS6Bogt8cElnui4UGUUdIC1uuB6pJ7xYLqh
WO+ZDKM7eNDlOd64EtYCY8rozNBK3U7zzXnYypPVdr575+TdXf7hsbtzoPzxHfdCo9+b0WWmggqT
tZw+kHZBVvUMqYMBT2TxnQNrnNt7oFMLlnPSNjwXwwbkyuAex0KQDHVQbqBO02+akr7I0dHASn72k
XifYKpWvhJW0kIWUSHFeZzWZJf4lf6uwjta/VpY8uK+3eVZsQDAQ91TQL2W3HUNEWR26Z8r8UVY9
hghe0WW52jjZzREQceZTF3sUcFkSIFN6orWs74z71/hEbcpNk9M5LQRlGe9gYld6K/RF/ae1j8oD
cMLqV+XH0aNUR142+itRMJLAMBslwi4+AODqnOgbxubkMvX/6YapjIZ74ltWrZ1Z7qh96Oig57IV
4+hh4pGNsAmUjGa5kae4endPH/xqzlxWDThkLZp8K4FV+C+WuG0RFBHkTOMyvvEiRwW6MNQS3oF
o3GjjkCE370+tk/X
-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT RSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN TSA CA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

Valid from: *Fri Jan 22 11:14:11 CET 2021*

Valid to: *Mon Jan 15 11:50:34 CET 2046*

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:F4:17:A5:1F:AD:D5:F3:5E:54:13:28:B9:49:27:FC:BC:4B:B4:09:66:F6:F2:D0:28:95:38:CD:6D:30:0F:4E:B8:B6:27:F1:36:0B:DF:E2:01:95:69:C7:37:38:03:72:FB:54:7E:E9:27:F4:26:15:AF:56:97:07:AC:B3:61:AC:D6:3C:A4:46:02:EC:94:D9:43:40:81:F8:58:0F:F7:2E:F9:DF:C3:A5:2B:D4:E5:11:67:A0:05:A6:D1:4A:7E:37:D7:B2:6F:1A:BE:C5:25:C5:14:0F:E7:9E:00:7E:32:5B:9F:5C:10:75:05:E2:B2:A1:8E:57:B7:68:3F:E0:15:5D:48:B0:73:1E:CA:8F:FD:EE:6B:22:64:9C:44:CF:04:D1:D7:A9:C2:0A:34:0D:E8:19:82:8A:70:CF:F5:8A:BF:FD:97:24:DC:28:40:A1:E8:A6:68:AD:D4:32:1C:64:D7:0B:07:F5:FA:5B:ED:11:59:71:BE:22:B0:FA:8A:75:B3:8D:ED:B1:28:CF:EB:4E:83:BA:29:98:4C:4C:F1:2F:63:9B:08:A7:B5:EC:DB:3A:D5:AE:8A:DA:6A:FE:C2:00:43:52:13:A0:6E:BB:28:A6:42:A3:B5:F3:83:01:7E:38:3A:E1:84:C3:F9:C9:A1:89:37:25:DC:6E:FA:46:1D:EA:BC:3C:D9:AC:C0:96:1A:09:08:EC:76:CF:A8:60:2B:8D:E6:42:35:47:1F:A6:95:BA:38:F4:A4:1F:F4:15:3E:C1:91:B4:7D:02:6D:8C:DA:E0:F6:01:16:CA:B9:55:9E:62:4C:F5:BD:4E:3D:7D:A1:01:0C:2D:11:DA:8C:22:B9:82:B9:6C:D3:A0:FF:0B:32:DF:57:D3:C6:94:BE:A3:6A:DD:72:6D:D2:29:F2:F0:B0:81:CB:B1:8C:DC:9E:F7:AC:94:C0:2F:E9:05:D6:CB:EA:C4:1F:52:43:F4:74:5C:BC:6F:F2:F0:FD:4D:E4:4F:8C:F4:74:BF:4F:92:A4:F8:F8:03:3B:5C:EC:7F:09:29:0B:71:75:90:F8:9F:90:F5:BF:FB:61:2D:D7:B9:1B:4A:C4:90:1C:CB:79:2F:54:29:70:CF:8A:F7:73:A2:10:3D:B7:8B:1D:49:62:D8:39:8A:58:C7:37:8A:35:54:E5:2D:E1:3E:36:3B:92:AA:2E:8D:BA:29:F3:70:E9:91:C0:F9:D9:B4:18:31:6D:11:A8:18:CB:60:B0:A7:72:7B:35:F8:A8:5F:04:6B:98:33:58:EA:27:71:7D:51:94:BF:46:CE:78:52:79:56:6B:0C:B8:B6:09:9E:AA:4C:C6:78:F1:91:3A:E8:65:29:AB:25:D1:96:60:5B:A3:8C:6F:02:03:01:00:01

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

Authority Key Identifier *B5:36:BC:3C:8C:1A:AB:2C:F6:59:19:2D:83:14:DA:93:25:15:D6:86*

Authority Info Access *http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.p7b*

Certificate Policies *Policy OID: 1.3.6.1.4.1.25596.4.1.1*

CPS pointer: http://pki.digitalsign.pt

Extended Key Usage *id_kp_timeStamping*

CRL Distribution Points *http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.crl*

Subject Key Identifier *0F:F3:54:34:00:CC:55:92:D1:34:C4:0E:A6:FD:F9:00:EA:E3:25:55*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *38:BD:3C:34:D9:D9:3D:71:F8:F3:31:55:67:56:CB:4B:E1:52:E1:C9:9B:50:EB:17:7F:8A:68:E8:D0:1F:5C:D6*

X509SubjectName

Subject CN: *DIGITALSIGN TSA CA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

X509SKI

X509 SK I *D/NUNADMVZLRNMQOpv35AOrjJVU=*

Service Status

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

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

Status Starting Time

2023-01-20T14:10:14Z

7.21 - Service (recognisedatnationallevel): DIGITALSIGN TSA CA V1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA

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

Service Name

Name *[en]* *DIGITALSIGN TSA CA V1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *372092575080251664300315856246267264929396744379*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDcjCCAvegAwIBAgIUQS01R/lxPzU5THeZdYla9cW04LswCgYIKoZIzj0EAwMwZDELMAkGA1UE
BhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDEpMCcGA1UE
AwwgRElHSVRBTFNjR04gR0xPQkFMIFJPT1QgRUNEU0EgQ0EwHhcNMjEwMTIyMTAxNjQzWhcNNDYw
MTE1MTEwNzUwWjBZMQswCQYDVQQGEwJQVDEqMCgGA1UECgwhRGlnaXRhbFNpZ24gQ2VydGlmaWNh
ZG9yYSBEaWdpdGFsMR4wHAYDVQQDDBVESUdlVEFMU0lHTiBUU0EgQ0EgVjEwdjAQBgcqhkjOPQIB
BgUrgQQAIgNiAARjDVVmR/uMN2YZ1Esp+Fh3jzLq8Uw4aMDs6c/szgsNEufoyY64/HRsXluJ0PC
Jw3akawtsYG1Ubid9xm24HJbtb8Q5vnhn0COH+pej1Pj+6LvahVg0KR0rsFPOfzFSkCjggFzMIIB
bzASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFM6vSosadeLxOOcC8BatXupk1Xu0MF0G
CCsGAQUFBwEBBFEwTzBNBggrBgEFBQcwAoZBaHR0cDovL3Jvb3QtZWNkc2EuZGlnaXRhbHNpZ24u
cHQvRElhSVRBTFNjR05HTE9CQUxST09URUNEU0FDQS5wN2IwQQYDVR0gBDowODA2BgsrBgEEAYHH
fAQBATAnMCUGCCsGAQUFBwIBFhlodHRwOi8vcGtpLmRpZ2l0YWxzaWduLnB0MBMGA1UdJQQMMAoG
CCsGAQUFBwMIMFIGA1UdHwRLMEkwR6BFoEOGQWh0dHA6Ly9yb290LWVjZHNhLmRpZ2l0YWxzaWdu
LnB0L0RjR0lUQUxTSUdOR0xPQkFMUk9PVEVDRFNBQ0EuY3JsMB0GA1UdDgQWBBS3NBnRWhFPGoQ+
vdS6IOUMctg2kDAOBgNVHQ88BAf8EBAMCAQYwCgYIKoZIzj0EAwMDaQAwZgIxALHtpPEe2bEx4s/n
3yJvvRQGgrgZcTcO9sNYuWsXAUMn3DncmCviy3tn/OL3QMBZIAIxAK5Mwv0FDujF1SXjm1ME5g4v
ZckwmxhlS2AdXWwq071v50xfRNh010mrGssE89tszg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT ECDSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN TSA CA V1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

Valid from: *Fri Jan 22 11:16:43 CET 2021*

Valid to: *Mon Jan 15 12:07:50 CET 2046*

Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:49:0D:55:66:47:FB:8C:37:66:19:D4:4B:29:F8:58:77:27:32:EA:05:4C:38:68:C0:EC:E9:CF:EC:CE:0B:0D:12:E7:E0:C9:82:3A:E3:F1:D1:B1:79:6E:27:43:C2:27:0D:DA:91:AC:2D:B1:81:B5:51:B8:9D:F7:19:B6:E0:72:5B:B5:BF:10:E6:F9:E1:9F:40:8E:1F:EA:5E:8F:53:E3:FB:A2:EF:6A:15:60:D0:A4:74:AE:C1:4F:39:FC:C5:4A:40*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*CE:AF:4A:8B:1A:75:E2:F1:38:E7:02:F0:16:AD:5E:EA:64:D5:7B:B4*
Authority Info Access	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.crl*
Subject Key Identifier	*B7:34:19:D1:5A:11:4F:1A:84:3E:BD:D4:BA:20:E5:0C:71:F8:36:90*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C8:11:BD:06:D0:9F:43:F0:03:C4:96:F7:C2:8B:9D:5D:64:77:EF:ED:FF:E1:69:B4:18:A5:B7:B4:8B:6B:B9:D6*

X509SubjectName

Subject CN:	*DIGITALSIGN TSA CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*tzQZ0VoRTxqEPr3UuiDlDHH4NpA=*

Service Status

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

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

Status Starting Time

2023-01-20T14:16:59Z

7.22 - Service (withdrawn): DIGITALSIGN VALIDATION SERVICE

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

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

Service Name

Name *[en]* *DIGITALSIGN VALIDATION SERVICE*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *192452120927927221446359284431972560629527021002*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIHkjCCBXqgAwIBAgIUIbXaAGLo2KYsrcMQdu6Jb19ZBcowDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmlyYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gUVBTEIGSUVEtENBIEcxMB4XDTIyMTAwMzE2NDM0OFoXDTI1MTAw
MjE2NDM0OFowggELMQswCQYDVQQGEwJQVDFDMEEGA1UECww6Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjEYMBYGA1UEYQwPVkFUUFQtNTA3
MDE1ODUxMTIwMAYDVQQKDClESUdlYEFMU0lHTiAtIENFUlRjRkIDQURPUkEgRElhSVRBTCwgUy5B
LjEhMB8GCSqGSIb3DQEJARYSc3ZzQGRpZ2l0YWxzaWduLn80MRDwGwYDVQQLDBR5ZW1vdGVRU0NE
TWFuYWdlbWVudDEnMCUGA1UEAwweRElhSVRBTFNJR04gVkFMSURBVEIPTiBTRVJWSUNFMlBljAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt3fw+5pHureuEanFa18BUMTC13gVS6WOzXQCUGCz
F+QluS1t+qlsm7q/7PSrk7eAE1BYKavbUluNp69yzct16DoOSzVKa7ol0UurytyKlytSh5vWGuGf
yF2JmITGxRJ0jPYFbMuCQzk+zYfRLlnv4NpYTquBT4/llk1CM6TM/YEP3YeqvFWP0MW3CbxOXT
Gyx/remce260sMboT+HnKkWU7vn3pUsNMvGgMkraBR9I3pmmg3YvVpbk6dihwa/RkMkVpCfBsOmS
L166ISc8GFHwudU7vRlAh2OIXM3F8EwAT3jihdl/NDHW0/YqWauoY+JYXBcXkZEPlxwLR/oCkwID
AQABo4ICljCCApIwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRzS5fFAHBQEfJo5f/ovzVxnIxjp
FDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRwczovL3FjYS1nMS5kaWdpdGFsc2ln
bi5wdC9ESUdlYEFMU0lHTlFVQUxlRklFRENBRzEucDdlMC4GCCsGAQUFBzABhjodHRwczovL3Fj
YS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMB0GA1UdEQQWMBSBEnN2c0BkaWdpdGFsc2lnbi5wdDBf
BgNVHSAEWDBWMDcGCysGAQQBgcd8BAEBMCgwJgYIKwYBBQUHAgEWGmh0dHBzOi8vcGtpLmRpZ2l0
YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEGMAkGBwQAi+xAAQMwHQYDVR0IBBYwFAYIKwYBBQUH
AwIGCCsGAQUFBwMEMIGBBggrBgEFBQcBAwSBrzCBrDAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgG
BgQAjkYBATAIBgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYBBgIwagYGBACORgEFMGAwLhYoaHR0
cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX2VuLnBkZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6
ZzEuZGlnaXRhbHNpZ24ucHQvUERTX3B0LnBkZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6
Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIhSVRBTFNJR05RVUFrM5UZIRURDQUcxLmNybDAdBgNV
HQ4EFgQUu3Qu7EqeNtrMtmR+WZ9OEgEtchMwDgYDVR0PAQH/BAQDAgZAMA0GCSqGSIb3DQEBDQUA
A4ICAQArhutlMARKYYFRZxbi5I4LwWyv9c55r/aUPmNabQNOmFCbFu+Ceq939I2lrCZYGaPgk2UP
JR75O2ROot3LNqY3lsN7HqMl4T647nkVXFxa/ycUseXTTGWGcartyR/pmj+WjuXR3mHOI4dQGEL/
ji0mPf+Tzz1VTPCKGK2P9vyID5nj6+0sT1s32Ag5nw8K6NXT2hb/vjM3vWOFjKnDQs9qwXlQaxOG
PXqyWain3pZ546o5b+PfPlyUgkyaAkjzrdm1xisfetOFp1TbyacAJu/KNry+RlO59wIoYgfBZ3f6
hxbMurF6GjSABwnUO1CNh+JdsO+TMRrCDtpsRw7zVhlRginIJ3wFxAjpx8jVuWTWDOUx3a7JHdUv
f4QS4x29CCDboiKltOC688WtfQGIrajjij2V7ElN7g2CcB1Q3Pb2DsDJbTqOlejTGMtUeBpG+eR+
tLeKPXnCdJjGJTQvGzLP0zdQ9MGmmqf3GbGXpjOP0mnAOVO2Q37adGm0fIQbI3uHfCvCmvMwYPG
cYfC1EGqVNKwYwFnpR6ycED2/yrNKckYiXvfmiehvUfFGCte45Rkf2+1wzlp/6uOwhVb1BG5nww
gxhqZx+BHs+oPV7kR9YN+OAcYA3PIRIAyGp/E3IMO2gzoOmU/aKCZN5T4IT6Afjqn1HdiRme5Vf4
QfuCLQ==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN VALIDATION SERVICE*

Subject OU: *RemoteQSCDManagement*

Subject E: *svs@digitalsign.pt*

Subject O: *DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*

Subject 2.5.4.97: *VATPT-507015851*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *PT*

Valid from: *Mon Oct 03 18:43:48 CEST 2022*

Valid to: *Thu Oct 02 18:43:48 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:B7:77:F0:FB:9A:47:BA:B7:AE:11:A9:C5:6B:5F:01:50:C4:C2:D7:78:15:4B:A5:
8E:CD:74:02:50:60:B3:17:E4:08:B9:2D:6D:FA:A2:2C:9B:BA:BF:EC:F4:AB:93:B7:80:13:50:58:29:AB:DB:52:5B:8D:A7:AF:72:CD:CB:75:E8:3A:0E:4B:35:4A:6B:BA:08:D1:4B:AB:CA:DC:8A:
27:2B:52:87:9B:D6:1A:E1:9F:C8:5D:89:8A:62:13:1B:14:49:D2:33:D8:15:B3:2E:09:0C:E4:FB:36:1F:3C:B2:27:BF:83:69:61:3A:AE:05:3E:3F:88:89:64:D4:23:3A:4C:CF:D8:10:FD:D8:7A:A
B:C5:58:FD:0C:5B:70:9B:C4:E5:D3:1B:2C:7F:AD:E9:9C:78:6E:B4:B0:C6:E8:4F:E1:E7:2A:45:94:EE:F9:F7:A5:48:0D:32:F1:A0:32:4A:DA:05:1F:48:DE:99:A6:83:76:2F:56:96:E4:E9:D8:A1:
C1:AF:D1:90:C9:15:A4:27:C1:B0:E9:92:2F:5E:BA:21:27:3C:18:51:F0:B9:D5:3B:BD:19:40:87:63:88:5C:CD:C5:F0:4C:00:4F:78:E3:85:D2:3F:34:31:D6:D3:F6:2A:59:AB:A8:63:E2:58:5C:1
7:17:91:91:0F:97:1C:0B:47:FA:02:93:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*svs@digitalsign.pt*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*BB:74:2E:EC:4A:9E:36:DA:CC:B6:64:7E:59:9F:4E:12:01:2D:72:13*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B4:52:77:CA:89:52:DE:51:A1:3F:DA:AC:55:3E:E7:0E:91:97:9E:56:88:E0:97:98:60:74:9A:82:3E:38:2C:8E*

X509SubjectName

Subject CN:	*DIGITALSIGN VALIDATION SERVICE*
Subject OU:	*RemoteQSCDManagement*
Subject E:	*svs@digitalsign.pt*
Subject O:	*DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*
Subject 2.5.4.97:	*VATPT-507015851*
Subject OU:	*Certificate Profile - Qualified Certificate - Organization*
Subject C:	*PT*

X509SKI

X509 SK I	*u3Qu7EqeNtrMtmR+WZ9OEgEtchM=*

Service Status

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

Service status description [en] *undefined.*

Status Starting Time *2025-10-27T13:00:00Z*

7.22.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.22.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.22.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

Service Name

Name [en] *DIGITALSIGN VALIDATION SERVICE*

Service digital identities

X509SubjectName

Subject CN: *DIGITALSIGN VALIDATION SERVICE*

Subject OU: *RemoteQSCDManagement*

Subject E: *svs@digitalsign.pt*

Subject O: *DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*

Subject 2.5.4.97: *VATPT-507015851*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *PT*

X509SKI

X509 SK I *u3Qu7EqeNtrMtmR+WZ9OEgEtchM=*

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

Status Starting Time *2023-01-20T14:20:16Z*

7.22.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.22.3.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.23 - Service (granted): DIGITALSIGN QUALIFIED TSA CA V1

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.*

Service Name

Name *[en]* *DIGITALSIGN QUALIFIED TSA CA V1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *406165019569313429111155873387146621197990421518*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDejCCAwGgAwIBAgIURyURwwNs1mL/hiW23WsJrnWO5A4wCgYIKoZIzj0EAwMwZDELMAkGA1UE
BhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEpMCcGA1UE
AwwgRElhSVRBTFNJR04gR0xPQkFMIFJPT1QgRUNEU0EgQ0EwHhcNMjEwMTIyMTAxNTMxWhcNNDYw
MTE1MTEwNzUwWjBjMQswCQYDVQQGEwIQVDEqMCcGA1UECgwhRGlnaXRhbFNpZ24gQ2VydGlmaWNh
ZG9yYSBEaWdpdGFsMSgwJgYDVQQDDB9ESUdJVEFMU0lHTiBRVUFMSUZJRUQgVFNBIENBIFYxMHYw
EAYHKoZIzj0CAQYFK4EEACIDYgAECc5+UEEva6QANJyKOFPQfY6ciFEbWzTb1jMtAw+9Pi4e6p9X
kpNukPeEtLOeaIrRhngeK4DW/1B4Ct0K/DtuoguWF+jAD4WhOdOLI35+9N7I5JnoZPuPCTnk1x4m
ggsCoAIBczCCAW8wEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBTOr0qLGnXi8TJnAvAW
rV7gZNV7tDBdBggrBgEFBQcBAQRRMEBwTQYIKwYBBQUHMAKGQWh0dHA6Ly9yb290LWVjZHNhLmRp
Z2I0YWxzaWduLnB0L0RJR0lUQUxTSUdOR0xPQkFMUk9PVEVDRFNBQ0EucDdfMEEGA1UdIAQ6MDgw
NgYLKwYBBAGBx3wEAQEwJzAlBggrBgEFBQcCARYZaHR0cDovL3BraS5kaWdpdGFsc2lnbi5wdDAT
BgNVHSUEDDAKBggrBgEFBQcDCDBSBgNVHR8ESzBJMEegRaBDhkFodHRwOi8vcm9vdC1lY2RzYS5k
aWdpdGFsc2lnbi5wdC9lESUdJVEFMU0lHTkdMT0JBTFJPT1RFQ0RTQUNBLmNybDAdBgNVHQ4EFgQU
DSMrFhIXIkvtx/alHRpfG5g02gcwDgYDVR0PAQH/BAQDAgEGMAoGCCqGSM49BAMDA2cAMGQCMFGk
Q6ftD9YTrYMo7L73dpQRAg1Ozd5s4lQS9VASgPB49k10S7eMAPQNDPj7ZuHidwIwG9Lrnn6U29dq
+6p1J7WWjr7sMkYZLRsLJej3hsBj7XQAQTLfzwOOMf1WcztOmn6b

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT ECDSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN:	*DIGITALSIGN QUALIFIED TSA CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*
Valid from:	*Fri Jan 22 11:15:31 CET 2021*
Valid to:	*Mon Jan 15 12:07:50 CET 2046*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:09:CE:7E:50:41:2F:6B:A4:00:34:9C:8A:38:53:D0:7D:8E:9C:88:51:1B:5B:34:DB:D6:33:2D:03:0F:BD:3E:2E:1E:EA:9F:57:92:93:6E:90:F7:84:B4:B3:9E:68:8A:D1:86:78:1E:2B:80:D6:FF:50:78:0A:DD:0A:FC:3B:6E:A2:AB:96:17:E8:C0:0F:85:A1:39:D3:8B:97:7E:7E:F4:DE:E5:E4:99:E8:64:FB:8F:09:39:E4:D7:1E:26:82:0B:02*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*CE:AF:4A:8B:1A:75:E2:F1:38:E7:02:F0:16:AD:5E:EA:64:D5:7B:B4*
Authority Info Access	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.crl*
Subject Key Identifier	*0D:23:2B:16:12:17:96:4B:ED:C7:F6:A5:1D:1A:5F:1B:98:34:DA:07*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*BD:23:18:F6:4D:CC:52:92:38:BC:C7:1C:94:94:8F:7B:94:79:A3:6E:30:DD:A6:5A:52:0A:35:6F:9E:FB:5A:D9*

X509SubjectName

Subject CN:	*DIGITALSIGN QUALIFIED TSA CA V1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*DSMrFhIXlkvtx/alHRpfG5g02gc=*

Service Status

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

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

Status Starting Time

2024-01-31T14:54:38Z

7.24 - Service (granted): DIGITALSIGN QUALIFIED TSA CA 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.*

Service Name

Name *[en]* *DIGITALSIGN QUALIFIED TSA CA G1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *119735550504264623372372204748242882141846385103*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGwDCCBKigAwIBAgIUFPkqtgahV/V4ie93mmMuUL66Mc8wDQYJKoZIhvcNAQENBQAwYjELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEnMCUG
A1UEAwweRlHSVRBTFNJR04gR0xPQkFMIFJPT1QgUlNBIENBMB4XDTIxMDEyMjEwMTMwOVoXDTQ2
MDExNTEwNTAzNFowYzELMAkGA1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmlj
YWRvcmEgRGlnaXRhbDEoMCYGA1UEAwwfRElHSVRBTFNJR04gUUVBTElGSUVEIFRTQSBDQSBHMTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAOIwX99PizBeqFIThdsu4RiINZ7lzDKbDC1h
Hl6kSAf08K0CS3ErcxJRKv8f2zaqKWPGJCte8YzdfVjWsdAxmHVdn+C4JPsQHTaY7varePNtGulm
ACs2//WUz4IGtKZAmKL+Cj4MFo3z65szGl6MVgXmnmPkSuxmLGpwsNr8p2n2QBkON9QJMZyiF2Ul
Kf6egdYw54IgwwofNCP52T5ZqYfXMA2PZDHEgpgwoefCsINCrbuL6Ss8JBle4he0mSEvLrDh1C
StR+2PCALFNhhuzS+Dv4iCdOPCtrnVGzWuPHAkqmojH8Vnz4eiL5PdtUAEf0mZe/tB7RKbSUZgh1J
m6f+g356uiCfDEH9oTCvc2vR2D2XYJTLyH7tmK3f3dOzm0+16Uca7l/Y16hfDVig73B08WPMxAlu
XdaGJNvI8PP9NiQHZ91Xnstbgc4rU55OGkrnhk+Ut8yxYF5NsXCoJdhjpRXb5pZIved3TANVH9d9
ItQeHLAYCA79DgSXfADRgBFBZbmcMpAxHJ7nF/Y7Dz3Ez4Dz1vgichBYoVGPCbzVOiET6JI/+X+n
IkbMy/rGnTNAnHVXu11sIQNaUyvwCPeAXE4mPeHtxpooM3FbvH7i39oq/XM96V/JcN+tUS68kKSX
igUW33W6yPUn5kr/tlp7X94Rlw04+DgahKz7rWbFAgMBAAGjggFrMIIBZzASBgNVHRMBAf8ECDAG
AQH/AgEAMB8GA1UdIwQYMBaAFLU2vDyMGqss9IkZLYMU2pMIFdaGMFkGCCsGAQUFBwEBBE0wSzBJ
BggrBgEFBQcwAoY9aHR0cDovL3Jvb3QtcnNhLmRpZ2I0YWxzaWduLnB0L0RjR0lUQUxTSUdOR0xP
QkFMUk9PVFJTQUNBLnA3YjBBBgNVHSAEOjA4MDYGCysGAQQBgcd8BAEBMCcwJQYIKwYBBQUHAgEW
GWh0dHA6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwEwYDVR0lBAwwCgYIKwYBBQUHAwgwTgYDVR0fBEcw
RTBDoEGgP4Y9aHR0cDovL3Jvb3QtcnNhLmRpZ2I0YWxzaWduLnB0L0RjR0lUQUxTSUdOR0xPQkFM
Uk9PVFJTQUNBLmNybDAdBgNVHQ4EFgQUvLW/rcS61RnHowVDsnsXnAcD3IwwDgYDVR0PAQH/BAQD
AgEGMA0GCSqGSIb3DQEBDQUAA4ICAQAGg3W05oENzVZhbmplgSUGLzfD6jnJ0N0Nl4r85noCNuZ
LRqTRmPHgLbxLdkIOBN5eK9Jt3FI78xmViiAQiLznkB5lfAKY4yWu0CtqFB7fC0al4kX9h+jewAu
BFB7BPlp0DxXZZn1ffLa1pHYoOzFXXjom90UKXjJhcoa2qAGXAqlrMaB/ud3fU4cXXbYsejI+CpA
X4Y/36flWn1Q3MDSsd0rjpz1w9DOZkm1v7yaPith5StDQ6Rf3MGoLBL7g7PZ+eFEYafhdOYPstd0
hyoeh6bpBm2e2XfKM5iVuUnNFfQDE1LpWJSp+9rk3R3508i6dccguU6LkJXyG11UpTCM4mTAYn
6adzI5yWZuYUAzhQAEVe3egzf9zYr1vWyEPxtDLu+sVBZF0+pbtpq3Nvrd3jq71eD11j5V+xEaHJ
ADPJ7a+0xloGDC+cu76dUPnKg9VVkCaQ5T1FGhdHvpeaFZpANbOmpjdn6ZEs1Z4eumMMT+0W/0Wx
qwQYDIFZAEfruTKYVl/+PRiHa8bKudKroH+kUN4QEa+Te+gYx4UQ9q++V4EKt4Y4x7Zud4i9iGUV
milz8sG2IA/NGVhTwL2MLRdI5Tk3ViIwmJi0diY288+jRQABKoIih/OHg17bucLy6Ba72rZf2XI
BbZIlvLHReVB+k2dWNGd1D2/G/odNw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN GLOBAL ROOT RSA CA*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN QUALIFIED TSA CA G1*

Subject O: *DigitalSign Certificadora Digital*

Subject C: *PT*

Valid from: *Fri Jan 22 11:13:09 CET 2021*

Valid to: *Mon Jan 15 11:50:34 CET 2046*

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:E2:30:5F:DF:4F:8B:30:5E:A8:52:13:85:DB:2E:E1:18:A5:35:9E:E5:CC:32:9B:
0C:2D:61:1E:5E:A4:48:07:F4:F0:AD:02:4B:71:2B:73:12:51:2A:FF:1F:DB:36:AA:29:63:C6:24:2B:5E:F1:8C:DD:7D:58:D6:B1:D0:31:98:75:5D:9F:E0:B8:24:FB:10:1D:36:98:EE:F6:AB:78:F
3:6D:1A:E9:66:00:2B:36:FF:F5:94:CF:82:06:B4:A6:40:98:A2:FE:0A:3E:0C:16:8D:F3:EB:9B:33:1A:5E:8C:56:05:E6:9E:63:E4:4A:EC:66:2C:6A:70:B0:DA:FC:A7:69:F6:40:19:0E:37:D4:09:3
1:9C:A2:17:65:25:29:FE:9E:81:D6:30:E7:82:20:C3:0A:1F:34:23:D2:D9:3E:76:AB:F6:0F:5C:C0:36:3D:90:C7:7F:38:29:83:0A:1E:7C:2B:08:34:2A:DB:B9:4E:92:B0:18:C1:95:EE:21:7B:49:
92:12:F2:EB:0E:15:42:4A:D4:7E:D8:F0:80:2C:53:61:86:EC:D2:F8:3B:F8:88:27:4E:3C:2B:66:54:6C:D6:B8:F1:C0:92:A9:A8:8C:7F:15:9F:3E:1E:88:BE:4F:76:D5:00:11:F3:A6:65:EF:ED:F3:
B4:4A:6D:25:19:82:1D:49:9B:A7:FE:83:7E:7A:BA:20:9F:0C:41:FD:A1:30:AF:73:6B:D1:D8:3D:97:60:94:CB:C8:7E:ED:98:AD:DF:DD:D3:B3:9B:4F:B5:E9:47:1A:EC:8F:D8:D7:A8:5F:0D:58:
A0:EF:70:74:F1:63:CC:C4:D2:2E:5D:D6:86:24:DB:E5:F0:F3:FD:36:24:07:67:DD:57:9E:CB:5B:81:CE:2B:53:94:8E:1A:4A:E7:86:4F:94:B7:CC:B1:60:5E:4D:81:70:A8:25:D8:63:A5:15:DB:4
A:96:65:BD:E7:77:4C:03:55:1F:D7:7D:96:D4:1E:1C:B0:18:08:04:FD:0E:04:97:7C:00:D1:80:11:41:65:B9:9C:32:90:31:1C:9E:E7:17:F6:3B:0F:3D:C4:CF:80:F3:D6:F8:22:72:10:58:A1:51:
8F:09:BC:D5:3A:21:13:E8:99:7F:F9:7F:A7:8A:46:CC:CB:FA:C6:9D:33:40:9C:75:57:BB:5D:6C:51:03:5A:53:2B:F0:08:F7:80:5C:4E:26:3D:E1:ED:C6:9A:28:33:71:5B:BC:7E:E2:DF:DA:2A:F
D:73:D:E9:5F:C9:70:DF:AD:51:2E:BC:90:AE:57:8A:05:16:DF:75:BA:C8:F5:27:E6:4A:FF:B6:5A:7B:5F:DE:11:97:0D:38:F8:38:1A:84:AC:FB:AD:66:C5:02:03:01:00:01
```

Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*B5:36:BC:3C:8C:1A:AB:2C:F6:59:19:2D:83:14:DA:93:25:15:D6:86*
Authority Info Access	*http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.p7b*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: http://pki.digitalsign.pt*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.crl*
Subject Key Identifier	*BC:B5:BF:AD:C4:BA:D5:19:C7:A3:05:43:B2:7B:17:9C:07:03:DE:5C*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*2B:B4:02:D9:03:E1:C1:57:43:E9:98:06:D1:D0:46:CF:BF:45:E3:7D:DD:31:26:07:56:6F:46:49:96:E2:07:50*

X509SubjectName

Subject CN:	*DIGITALSIGN QUALIFIED TSA CA G1*
Subject O:	*DigitalSign Certificadora Digital*
Subject C:	*PT*

X509SKI

X509 SK I	*vLW/rcS61RnHowVDsnsXnAcD3Iw=*

Service Status

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

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

Status Starting Time

2024-02-02T12:52:14Z

7.25 - Service (granted): DIGITALSIGN VALIDATION SERVICE_01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

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

Service Name

Name *[en]* *DIGITALSIGN VALIDATION SERVICE_01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *289517737356129378793437755195882912374518235593*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIkjCCBnggAwIBAgIUMrZsoc/83G4kWxOm2DXsg4MAwckwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIHSVRBTFNJR04gUVVBTEIgSUVEIENBIEcxMB4XDTI1MDcxNjE3MDIyMVoXDTI4MDky
OTE3MDIyMVowggELMQswCQYDVQQGEwJQVDFDMEEGA1UECww6Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjEYMBYGA1UEYQwPVkFUUFQtNTA3
MDE1ODUxMTIwMAYDVQQKDClESUdlYEFMU0lHTiAtIENFUlRjRkIDQURPUkEgRElHSVRBTCwgUy5B
LjEhMB8GCSqGSIb3DQEJARYSc3ZzQGRpZ2l0YWxzaWduLn80MRQwGwYDVQQLDBRSZW1vdGVRU0NE
TWFuYWdlbWVudDEnMCUGA1UEAwweRElHSVRBTFNJR04gVkFMSURBVEIPTiBTRVJWSUNFMIICIjAN
BgkghkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0uvrBsz85sir+++G3+Fqflo8rKn7VKUODwDwI8jT
7q5EFumLwckGWBsDbJqew+j9vBRP5Jx6KJSMpLlK8/8IWwxWNl9wBy1kM7h8LwogWPTPXZ++HbVan
jfneoiGVpDn33KZ5DC6ckf4ZU2XNfs29ura7hxt5UgLvpENWyJYn3ZFOx8x9QDTGGq+X6sCZlZrA
ip1UyOTEzY9RNwnQj+se33B0HIBVB6MR7a1LVvn0/nINeWFXudGHv+fK9wCj6U+ziYCmvv8MJx9M
a/geDp8rP8rJNIuUaU8tdEXyhd2TRb+AvesZixOZq3f2QRQaWPISpHCQLydtdUJ8HtL81CFo95Kv
+j00FWuzIT7HSS5hyJK4AN0RZdqCy3JKzZoaFmcF8FOpvMNzuRoXwjxFskIMhBA0ZzXahNdBbKIB
+6ncqYbJUe0ujCk1J9RpYXf49mw8+Qb/QTHN3q/0z58RnPeyRvowjNPFZylKP1Bo1ZyyZRCjjAv
Sut17D5TKtpAmAGqJHB9K59H20O0eRP0yvrFnetx34MUucpJCxH9PnHesDmpuKLu4BCdl+jZK/VP
BM3lYZADdlDoAo30OVGvmWaNiSu8rzjbQSQfKdGC1mE1WrHuZ5t9tDzzPcmg22bMJW6lO9cin7EA
V8f8EAbzZZMk3NU2ZW88pNt2/QOUyUcrN20CAwEAAaOCApYwggKSMAwGA1UdEwEB/wQCMAAwHwYD
VR0jBBgwFoAUc0nxQBwUBHyaEn/6L81czyMY6RQwgYYGCCsGAQUFBwEBBHoweDBGBggrBgEFBQcw
AoY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFMSUZJRURDQUcx
LnA3YjAuBggrBgEFBQcwAYYiaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvb2NzcDAdBgNV
HREEFjAUgRJzdnNAZGlnaXRhbHNpZ24ucHQwXwYDVR0gBFgwVjA3BgsrBgEEAYHHfAQBATAoMCYG
CCsGAQUFBwIBFhpodHRwczovL3Bra55kaWdpdGFsc2lnbi5wdDAQBg4rBgEEAYHHfAQCAQEBBjAJ
BgcEAIvsQAEDMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDCBvAYIKwYBBQUHAQMEga8w
gawwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJ
BgcEAI5GAQYCMGoGBgQAjkYBBTBgMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BE
U19Ibi5wZGYTAmVuMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19wdC5wZGYT
AnBOMEsGA1UdHwREMEIwOKA+oDyGOmhhdHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0LORJR0lU
QUxTSUdOUVVBTEIGSUVEQ0FHM55jcmwwHQYDVR0OBBYEFGzsqzgBhxYF2BZG2JeV2TCh1cXdMA4G
A1UdDwEB/wQEAwIGODANBgkqhkiG9w0BAQ0FAAOCAgEAetyIUqnfTb6FfjnP8EUDwD8UvwcS++m9
jPwEGzS+mTdafzfQlcGF6TYxg1QkQg+GCevdApUpG+vs/+ncUHTt/1uADDFyf6YpUujT8cfzaUf
1VfrmAVB4l5dJg3WRo88dMDR4Ln56u65FpCuYWojlGp2Wa6/zcLoMSjFZo7N1bBumI54WLw6qsIS
4cuh31TQNC2q5qVV1tLLw3ZNOpr3zeyQLPMDAykqTxBVHDe1CahNFpO0TI47f+2b1YtWyyXkeYrc
FSlryUFLIX/xRJTtlmFfjluBqany8S0qHkms4xWEMA/awVeMaCPf81L7XOT4eokby7YE+XmEz3Iw
nSypVfWMMB+/lERnlOpfoxWeANNA9XhbDfrM0a9MQot2t5gaNYH5nibrjX95eXNbsjoc+6hb95Ro
fj8xXNiO5ZEN4ApBMwwClQeU5HuxfRIPqfrxu5PNGw32VWnPATLr6pVU07kSgh0oCcK1LyoVRYsi
4LEcK5lhAjr1HP1eL2VNXkjPmPGVYxXoPGjNBVZ6PStJCdMaztdrxiUx9dbzCXAwtRyHYFrhQS
BEK3sOLkuYYjKkIAE+BYBOD9FYgDTOYqMSw4tdgy57k0VcMdN5yJIH865o5biZ3VipxW3cBtscHy
oygiKUtl+7dQ0cGY3sFJiIeghMyuNRBzhVOpO0HjRc=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *DIGITALSIGN VALIDATION SERVICE*

Subject OU: *RemoteQSCDManagement*

Subject E: *svs@digitalsign.pt*

Subject O: *DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*

Subject 2.5.4.97: *VATPT-507015851*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *PT*

Valid from: *Wed Jul 16 19:02:21 CEST 2025*

Valid to: *Fri Sep 29 19:02:21 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:D2:EB:EB:06:CC:FC:E6:C8:AB:FB:EF:86:DF:E1:6A:7C:8A:3C:AC:A9:FB:54:A5
:0E:0F:00:F0:23:C8:D3:EE:AE:44:16:E9:8B:C1:C9:06:58:1B:03:6C:9A:9E:C3:EB:BD:BC:14:4F:E4:9C:7A:28:94:8C:A4:B9:4A:F3:FF:16:C3:15:8D:97:DC:01:CB:59:0C:EE:1F:0B:C2:88:16:3
D:33:D7:67:EF:87:6D:56:A7:8D:F9:DE:A2:21:95:A4:39:F7:DE:46:52:0C:2E:9C:91:FE:36:53:65:CD:7E:CD:BD:BA:B6:BB:87:1B:52:52:02:EF:A4:43:56:C8:96:27:DD:91:74:C7:CC:7D:40:3
4:C6:1A:AF:97:EA:CD:99:95:9A:CD:8A:9D:54:C8:E4:C4:CD:8F:51:37:09:D0:8F:EB:1E:DF:70:74:1C:80:55:07:A3:11:ED:AD:4B:56:F9:F4:FE:72:0D:79:61:57:B9:D1:87:BF:E7:CA:F7:00:A3:
E9:4F:B3:B9:80:A6:BE:FF:0C:27:1F:4C:6B:F8:1E:0E:9F:2B:3F:CA:C9:36:5B:94:69:4F:2D:74:45:F2:85:DD:93:45:BF:80:BD:EB:19:8B:13:99:AB:77:F6:41:14:1A:58:F2:12:A4:70:90:2F:27:
6D:75:42:7C:1E:D2:FC:D4:21:68:F7:92:AF:FA:3D:34:15:6B:B3:95:3E:C7:49:2E:61:C8:92:B8:00:DD:11:65:DA:82:CB:72:4A:CD:9A:1A:16:67:05:F0:53:A9:BC:C3:73:B9:1A:17:C2:3C:45:
B2:42:0C:84:10:34:67:35:DA:84:D7:41:6C:A9:41:FB:A9:DC:A9:86:C9:51:ED:2E:8C:29:35:27:D4:7F:A5:85:DF:E3:D9:B0:F3:E4:1B:FD:04:C7:37:7A:BF:D3:3E:7C:46:73:DE:C9:1B:E8:C2:
33:4F:15:9C:BB:28:FD:41:A3:56:72:FD:94:42:26:30:2F:4A:EB:75:EC:3E:53:2A:DA:40:98:01:A0:24:70:7D:2B:9F:47:D8:43:B4:79:13:F4:CB:2A:C5:9D:EB:71:DF:B3:14:B9:CA:63:0B:11:F
D:3E:71:DE:B0:39:A9:B8:A2:EE:E0:10:9D:23:E2:59:2B:F5:4F:04:CD:E5:61:90:03:76:50:E8:02:8D:F4:39:51:AF:99:66:8D:89:2B:BC:AF:32:5B:41:24:1F:29:D1:82:D6:61:35:5A:B1:EE:67:
9B:7D:B4:3C:F3:3D:C9:A0:DB:66:CC:25:6E:88:3B:D7:22:9F:B1:00:57:C7:FC:10:06:F3:65:93:24:DC:D5:36:65:6F:3C:A4:DB:76:FD:03:94:C9:47:2B:37:6D:02:03:01:00:01
```

Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*svs@digitalsign.pt*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*6C:EC:AB:38:01:87:16:05:D8:16:46:D8:97:95:D9:30:A1:D5:C5:DD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*CF:02:09:CD:EF:63:BC:A0:1B:89:FF:C1:3B:BE:3B:2F:8E:CB:9E:CD:4E:8E:B9:7E:52:1E:A6:B6:51:6C:F4:BB*

X509SubjectName

Subject CN:	*DIGITALSIGN VALIDATION SERVICE*
Subject OU:	*RemoteQSCDManagement*
Subject E:	*svs@digitalsign.pt*
Subject O:	*DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*
Subject 2.5.4.97:	*VATPT-507015851*
Subject OU:	*Certificate Profile - Qualified Certificate - Organization*
Subject C:	*PT*

X509SKI

X509 SK I	*bOyrOAGHFgXYFkbYl5XZMKHVxd0=*

Service Status

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

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

Status Starting Time

2025-10-27T13:00:00Z

7.25.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.25.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.26 - Service (granted): DIGITALSIGN PRESERVATION SERVICE

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service type description *[en]* *A preservation service for qualified electronic signatures.*

Service Name

Name *[en]* *DIGITALSIGN PRESERVATION SERVICE*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *285874882518916401114017508593443659740645008183*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIIIDCCBnygAwIBAgIUMhMStZuAbLtaL/C4nhPG+L9tozcwDOYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIHSVRBTFNJR04gUVbTEIGSUVEiEMBiEcxMB4XDTI1MDcxODA5MDY0N1oXDTI4MDcx
NzA5MDY0N1owggENMQswCQYDVQQGEwJQVDFDMEEGA1UECww6Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjEYMBYGA1UEYQwPVkFUUFQtNTA3
MDE1ODUxMTIwMAYDVQQKDClESUdlYEFMU0IHTiAtIENFUlRjRkIDQURPUkEgREIHSVRBTCwgUy5B
LjEhMB8GCSqGSIb3DQEJARYSc3ZzQGRpZ2l0YWxzaWduLn80MRQwGwYDVQQLDBRSZW1vdGVRU0NE
TWFuYWdlbWVudDEpMCcGA1UEAwwgREIHSVRBTFNJR04gUFJFU0VSVkFUSU9OIFNFUlZJQ0UwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCxbu5L7u2exPttgha7mU9ZReu++Vo17A1IYKnz
TitWShglHIYT3/mKzj7Mmx8WPpCDqxOZ0a6kiAmvMbuCzMfe+XctRdZwSxg4N9sqAo/cZMfZiQde
YGG0PGYpJrHznFoMFlv9RGXgWd3sKnpbD3pcnaLsN/gwvbcZk2KzVYf/tmKX0+XHDEUdQ5kDw4P
UeAYT6Fvc8Mtssz5Wh4S9sfkkrqU/X+zuApuXs935/W8tNMUlK4HwMLWGnINLlecjdcW0IPgoNfla
UytBFnYW0P9I3Jzkht4p7HIRJEko45tNEkEtu2wJ+cMdRbE7R+96I2mDUv2nw5tXfhPOEVu3rKMSD
k8Rw0m+GmkEbxI1x/WXneqit5VwXnnKwZvvqzXuNn7XOk2Z/zhMgs0u0Si4 3/E7hvEhaAW+Z9/jd
ifmgABeDKbqSyg6uE9G2T4xjwWIP0hF8xNbUe2VbbVAs/1YiwTMmt1nDf0j6eLmNvkD8pndZjXBL
m8gzw4Yu8G2DhHbOCVUf6l/cBoKjXBXOfBSKH/kRcYCG0Qw3+YA+eGw07bEWrzZGzJpeTuBXpwM/
pBLvQT76QYGBrD4zAxzX00M8oRCK+xmKt9R4kD6xbkm6+H3Aslo9C2a5hMpTZ/mE4W8aoFucxa7o
uk/y1wEWT2xViCMaVnQUi8uaGzTP+UAh/i9IlwIDAQABo4ICIjCCAplwDAYDVR0TAQH/BAIwADAf
BgNVHSMEGDAWgBRzSfFAHBQEfJoSf/ovzVxnlxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUF
BzAChjpodHRwczovL3fjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0IHTiFVQUxjRkIFRENB
RzEucDdiMC4GCCsGAQUFBzABhiJodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMB0G
A1UdEQQWMBSBEnN2c0BkaWdpdGFsc2lnbi5wdDBfBgNVHSAEWDBWMDcGCysGAQQBgcd8BAEBMCgw
JgYIKwYBBQUHAgEWGmh0dHBzOi8vcGtpLmRpZ2l0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEG
MAkGBwQAi+xAAQMwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMIGBBggrBgEFBQcBAwSB
rzCBrDAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYBATAIBgYEAI5GAQQwEwYGBAICORgEG
MAkGBwQAjkYBBgIwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQv
UERTX2VuLnBkZhMCZW4wLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX3B0LnBk
ZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIH
SVRBTFNJR05RVUFMSUZjRURDQUcxLmNybDAdBgNVHQ4EFgQU0yYMVYAiBZywR/ogh4dwJ7fubD8w
DgYDVR0PAQH/BAQDAgZAMA0GCSqGSIb3DQEBDQUAA4ICAQCZWKmYt/dtfughj+KQAcvKTgBf3re
9ZWmZNjbrg+TvDMcuJmbSHFn1p4VTuaWzwjHWz1INnuqF3m99CSfMvGb0rbVs/3xCB8A3drnH255t
ogzygHnBY75TIKK+A3DpA/KCZs49IM+FY8LhPaKKE1yofYf8ydH2+PYaGMujVbkLIobB8N3wJfRXj
1+5UHd5QAJlaImlZp+36AKC4WzpfbkBPsy7+Yu+T26QaL+2VKsQ0u8jQKesf/Gk26s/a8+DtW4f2
xw8sEIfo2cvKKdnL+9rNiL7p1WEAYFiYYPlfZ7zh7vkttYxsWOQmQ3emnBOdI0yTeyHGfNDAAwPs
EwsnxNbraXwXJPlfX1gIL8sEcPA9wQQ2XWobotkFZcaESWUQ04kWNLGP0xAxRRMe9Pgm8EOlDdrB
eCF6gVi87x9c2Yp1DGN+PciAcghtlW9T0/eMuwKxmltkvFrVwsUb7io0TDfnuN2zGiLUPSxl7Dn1
ritLpyMCDI7TsGKnSczl1rpNOwftJWoYQgrC+UmaV2P3T+KGIA5MjAxRpCi+Luy4K56NJlvdHOUvC
Shmd9MJsndjXpmLUwaXYv5383qfZMO6eOg4zine/x0/XplsPA/Xra5sXyDvQH9x0KsAjINj6sSla
PXwMlgTF/iOu1/IRFxTh3Courw1wF4btdaB+AfpqgJgFzQ==

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA512withRSA*
Issuer CN:	*DIGITALSIGN QUALIFIED CA G1*
Issuer O:	*DigitalSign Certificadora Digital*
Issuer C:	*PT*
Subject CN:	*DIGITALSIGN PRESERVATION SERVICE*
Subject OU:	*RemoteQSCDManagement*
Subject E:	*svs@digitalsign.pt*
Subject O:	*DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*
Subject 2.5.4.97:	*VATPT-507015851*
Subject OU:	*Certificate Profile - Qualified Certificate - Organization*
Subject C:	*PT*
Valid from:	*Fri Jul 18 11:06:47 CEST 2025*
Valid to:	*Mon Jul 17 11:06:47 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:B1:6E:EE:4B:EE:ED:9E:C4:FB:6D:AA:16:BB:99:4F:59:45:EB:BE:F9:5A:35:EC:0D:65:60:A9:F3:4E:2B:56:4A:18:08:1C:86:13:DF:F9:8A:CE:3E:CC:9B:1F:16:3E:90:83:AB:13:99:D1:AE:A4:88:09:AF:31:BB:82:CC:C7:DE:F9:77:2D:45:D6:70:4B:18:38:37:DB:2A:02:8F:DC:64:C7:D9:89:07:5E:60:61:B4:3C:66:29:26:B1:F3:9C:5A:0C:16:5B:FD:44:65:E0:59:DD:EC:2A:7A:5B:0F:7A:5C:9D:A2:EC:37:F8:30:BD:B7:19:93:62:B3:CD:56:1F:FE:D9:8A:5F:4F:97:1C:31:14:75:0E:64:0F:0E:0F:51:E0:18:4F:A1:6F:73:C3:2D:B2:CC:F9:5A:1E:12:F6:C7:E4:92:B8:14:FD:7F:B3:B8:0A:6E:5E:CF:77:E7:F5:BC:B4:D3:14:2B:81:F0:30:B5:86:9C:83:4B:95:E0:A3:75:C5:B4:20:FB:2B:35:F9:5A:53:2B:41:16:76:16:D0:FF:48:DC:9C:E4:86:DE:29:EC:72:11:24:49:28:E3:9B:4D:12:41:2D:BB:6C:09:F9:C3:1D:45:B1:3B:47:EF:7A:97:69:B3:52:FD:A7:C3:9B:57:84:F3:84:56:ED:EB:28:C4:83:93:C4:70:D2:6F:86:9A:41:18:C4:8D:71:FD:65:E7:7A:A8:AD:E5:5C:17:9E:72:B0:66:FB:EA:CD:7B:8D:9F:B5:CE:93:66:7F:CE:13:20:B3:4B:B4:4A:2E:37:FC:4E:E1:BC:48:5A:01:6F:99:F7:F8:DD:89:F9:AA:00:17:83:29:BA:92:CA:AE:AE:13:D1:B6:4F:8C:49:C1:62:0F:D2:11:7C:C4:D6:D4:7B:65:5B:6D:50:2C:FF:56:22:C1:33:26:B7:59:C3:7F:48:FA:78:B9:8D:BE:40:FC:A6:77:59:8D:70:4B:9B:C8:33:C3:86:2E:F0:6D:83:84:76:CE:09:55:1F:E8:8F:DC:F2:82:A3:5C:15:CE:7C:14:8A:1F:F9:11:71:80:86:D1:0C:37:F9:80:3E:78:6C:34:ED:B1:16:AF:36:46:CC:9A:5E:4E:E0:57:A7:03:3F:A4:12:EF:41:3E:FA:41:81:BC:AC:3E:33:03:1C:D7:D3:43:3C:A1:10:8A:FB:19:8A:B7:D4:78:90:3E:B1:6E:49:BA:F8:7D:C0:B2:5A:3D:0B:66:B9:84:CA:53:67:F9:84:E1:6F:1A:A0:5B:9C:C5:AE:E8:BA:4F:F2:D7:01:16:4F:6C:55:88:23:1A:56:74:14:8B:CB:9A:1B:34:CF:F9:40:21:FE:2F:48:97:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*svs@digitalsign.pt*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*

CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*D3:26:0C:55:80:22:05:9C:B0:47:FA:20:87:87:70:27:B7:EE:6C:3F*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*96:44:A3:FA:30:0A:17:10:6C:D0:4B:33:4C:EA:39:E7:12:71:F2:9C:1F:EF:1D:21:E0:76:3A:84:A9:04:4D:DC*

X509SubjectName

Subject CN:	*DIGITALSIGN PRESERVATION SERVICE*
Subject OU:	*RemoteQSCDManagement*
Subject E:	*svs@digitalsign.pt*
Subject O:	*DIGITALSIGN - CERTIFICADORA DIGITAL, S.A.*
Subject 2.5.4.97:	*VATPT-507015851*
Subject OU:	*Certificate Profile - Qualified Certificate - Organization*
Subject C:	*PT*

X509SKI

X509 SK I	*0yYMVYAiBZywR/ogh4dwJ7fubD8=*

Service Status

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

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

Status Starting Time

2025-11-06T16:00:00Z

7.26.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

7.26.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

8 - TSP: ACIN iCloud Solutions, Lda

TSP Name

Name	*[en]*	*ACIN iCloud Solutions, Lda*

TSP Trade Name

Name	*[en]*	*Global Trusted Sign*
Name	*[en]*	*VATPT-511135610*
Name	*[en]*	*ACIN-iCloud Solutions, Lda*

PostalAddress

Street Address	*[en]*	*Estrada Regional 104, n 42-A*
Locality	*[en]*	*Ribeira Brava*
State Or Province	*[en]*	*Madeira*
Postal Code	*[en]*	*9350-203 Ribeira Brava*
Country Name	*[en]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:info@globaltrustedsign.com*
URI	*[en]*	*https://pki.globaltrustedsign.com/*

TSP Information URI

URI	*[pt]*	*https://pki.globaltrustedsign.com/*
URI	*[en]*	*https://pki.globaltrustedsign.com/en*
URI	*[en]*	*https://pki.globaltrustedsign.com/*

8.1 - Service (withdrawn): Global Trusted Sign Certification Authority 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.*

Service Name

Name *[en]* *Global Trusted Sign Certification Authority 01*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *124892040465876533503730265851908818859*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGOjCCBCggAwIBAgIQXfVVAYyJRVZZjc/ZEzuHqzANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UE
BhMCUFQxIzAhBgNVBAoMGkFDSU4taUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTwwOgYDVQQDDDNHbG9iYWwgVHJ1c3RlZCBTaWduIFjvb3QgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkgMDEwHhcNMTcwODExMTU0MDA5WhcNMjMwODExMTU0MDA5WjCBiTEL
MAkGA1UEBhMCUFQxIzAhBgNVBAoMGkFDSU4gaUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQL
DBNHbG9iYWwgVHJ1c3RlZCBTaWduMTcwNQYDVQQDDC5HbG9iYWwgVHJ1c3RlZCBTaWduIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IDAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwExx
vkL2uvr1R5fCsLQ+/MH5qciKjgMkZXldC1WP8JUG+CBMKrILgRx90nQazDJF3/yd1zICID/pv3j1
+t38SGY/aGzJag9Tgk+5cbTnquiQfsWfvgHHVTNBBd+vkY/pot4yOrKaqiPzCzDpo/XNTgdHdAc4
QehGyyrF6ojYKYlhbgITPc93hy/hgKqrPWzajzUQ035Rr2udX6C44fIi4xwRYKXjcDFcfRulkY55
foPsXoHpfcAitDByujLyvhfyUgBSlUrQ7ZP7gYhk3r3yI0BayvMfuOmVzRPtTYNK5XxKUVarNndQ
taGgoO936t9rhikWuuN747VxJJEEMnVeBQIDAQABo4IBnTCCAZkwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFOaVbwEt+Xki5wA5GYgVuOqLRZmLMB8GA1UdIwQYMBaA
FKaYfkCRhNncKttOL4ICM5XTdC5BMFcGA1UdIARQME4wTAYOKwYBBAGDIH4BAQEBAQAwOjA4Bggr
BgEFBQcCARYsaHR0cHM6Ly9wa2kuZ2xvYmFsdHJ1c3RlZHNpZ24uY29tL2luZGV4Lmh0bWwwTwYI
KwYBBQUHAQEEQzBBMDBGCCsGAQUFBzAChjNodHRwczovL3BraS5nbG9iYWx0cnVzdGVkc2lnbi5j
b20vcm9vdC9ndHNfcm9vdC5jcnQwgYsGA1UdHwSBgzCBgDA9oDugOYY3aHR0cHM6Ly9wa2kuZ2xv
YmFsdHJ1c3RlZHNpZ24uY29tL3lyb3QuZ3Rzc3Jvb3RfY3JsLmNybDAroD2gO4Y5aHR0cHM6Ly9w
a2kwMi5nbG9iYWx0cnVzdGVkc2lnbi5jb20vcm9vdC9ndHNfcm9vdF9jcmwuY3JsMA0GCSqGSIb3
DQEBCwUAA4ICAQA1WslrVuxZk8L87r9stgCx0sQPbq0PcTs2T/067xsdlIKTkbSfMQW4WH9PHkLj
vDa6bZgEwfIE/jHMBHd+YH/Ab4gueodG4vP9h+lCoAjfuO+EzzUrKIBWshqQq5NF4SciQoOTmh8o
gtwktgvwascpez2GfrheY4bb2CfA7hwOX6puehy/GhjGrrM9HumiHFR/QyPrfa6ms05KaiuwwUChK
j4RTnvP9yGJKyKhk1BR/4gPj5CKz5vYqzCbTCpkYTKnJ7mz+OIHJ2+TC/KPRFrJ0cDNlvbGcedV9
NNBs7Z431oVtiKO0z0EkOgQ9FkyJtRCnTLVQI9QAYng+z92qIMm84zow5TE6gEDvdY+YoGKslepP
BLsfmpfsO4j8PgCl5hiHAqWiKL5L8VXUAet4jPwqJdDx5/2TDQD2999L3TF7DiMV+YVZPG3gv8m0
lIMqTGQygsKGpoXvbp2P/UBRUk6y489gKsnLFtcva0D/ofv5kZfxrpbfDEIAdYjKnRCOc8ce5oVA
CQJh2qRXiDsn8tLWrWk8WR8LGCFIA15cbLkssurfTsKoHkJEK51t/VJyHGvXO7Ay69upuZY3Xy6hL
7RmpNt/1G/cN0OfmnEofxWVXZBN3URqz9o55mNaqmYRQPbX/mXN3zJ8P2TvNT+dZxRoRQ+JbX0y7
xHvRTVVGSd84ww==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Root Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN-iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign Certification Authority 01*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Fri Aug 11 17:40:09 CEST 2017*

Valid to: *Fri Aug 11 17:40:09 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:C0:4C:71:BE:42:F6:BA:FA:F5:47:97:C2:B0:B4:3E:FC:C1:F9:A9:C8:8A:8E:03:
24:65:79:5D:0B:55:8F:F2:35:06:F8:20:4C:2A:B2:0B:81:1C:7D:D2:74:1A:CC:32:45:DF:FC:9D:D7:32:02:20:3F:E9:BF:78:F5:FA:DD:FC:48:66:3F:68:6C:C9:6A:0F:53:82:4F:B9:71:B4:E7:AA
:E8:90:7E:C5:9F:BE:01:C7:55:33:41:05:DF:AF:91:8F:E9:A2:DE:32:3A:B2:9A:AA:23:F3:0B:30:E9:A3:F5:CD:4E:07:47:74:07:38:41:E8:46:CB:2A:C5:EA:82:58:29:89:61:6E:09:53:3D:CF:7
7:87:2F:E1:80:AA:AB:3D:6C:DA:27:35:10:D3:7E:51:AF:6B:9D:5F:A0:B8:E1:F2:22:E3:1C:11:60:A5:E3:70:31:5C:7D:1B:A5:91:8E:79:7E:83:EC:5E:81:E9:7C:60:22:B4:30:72:BA:32:F2:BE:
17:F2:52:00:52:95:4A:D0:ED:93:FB:81:88:64:DE:BD:F2:23:40:5A:CA:F3:1F:B8:E9:95:CD:13:ED:4D:83:4A:E5:7C:4A:51:56:AB:36:77:50:B5:A1:A0:A0:EF:77:EA:DF:6B:86:29:16:BA:E3:7
B:E3:B5:71:94:91:04:32:75:5E:05:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *E6:95:6F:01:2D:F9:79:22:E7:00:39:19:88:15:B9:0A:8B:45:99:8B*

Authority Key Identifier *A6:98:7C:A0:91:84:D9:DC:5E:DB:4E:2F:82:02:33:95:D3:74:2E:41*

Certificate Policies *Policy OID: 1.3.6.1.4.1.50302.1.1.1.1.1.0*

CPS pointer: https://pki.globaltrustedsign.com/index.html

Authority Info Access *https://pki.globaltrustedsign.com/root/gts_root.crt*

CRL Distribution Points *https://pki.globaltrustedsign.com/root/gts_root_crl.crl*

https://pki02.globaltrustedsign.com/root/gts_root_crl.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *09:75:38:16:9F:89:D9:EC:F7:70:E1:16:27:0E:C7:E1:20:07:AD:15:50:52:82:02:20:F4:B3:8E:5C:0B:11:81*

X509SubjectName

Subject CN: *Global Trusted Sign Certification Authority 01*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *5pVvAS35eSLnADkZiBW5CotFmYs=*

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

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

Status Starting Time *2025-04-16T17:33:00Z*

8.1.1 - Extension (critical): Qualifiers [QCStatement, QCForWSA, QCForESig, QCForESeal, QCSSCDStatusAsInCert]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.4*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

8.1.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.1.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.1.5 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Global Trusted Sign Certification Authority 01*

Service digital identities

X509SubjectName

Subject CN: *Global Trusted Sign Certification Authority 01*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *5pVvAS35eSLnADkZiBW5CotFmYs=*

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

Status Starting Time *2018-01-03T01:00:00Z*

8.1.5.1 - Extension (critical): Qualifiers [QCStatement, QCForWSA, QCForESig, QCForESeal, QCSSCDStatusAsInCert]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.4*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

8.1.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.1.5.4 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.2 - Service (withdrawn): Global Trusted Sign Timestamping Authority 001 (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.*

Service Name

Name *[en]* *Global Trusted Sign Timestamping Authority 001 (Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *323517174479790416047104647920400512 36*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEITCCA32gAwIBAgIQGFa20ciRxuFaT6FpdYg5jDANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UE
BhMCUFOxlzAhBgNVBAoMGkFDSU4gaUNsb3VklFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTcwNQYDVQQDDC5HbG9iYWwgVHJ1c3RlZCBTaWduIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5IDAxMB4XDTE4MDEwNTE2MDE0NVoXDTIxMDEwNTE2MDE0NVowgYkxCzAJBgNV
BAYTAlBUMSMwIQYDVQQKDBpBQ0lOLWIDbG91ZCBTb2x1dGlvbnMsIExkYTEcMBoGA1UECwwTR2xv
YmFsIFRydXN0ZWQgU2lnbjE3MDUGA1UEAwwuR2xvYmFsIFRydXN0ZWQgU2lnbiBUaW1c3RhbXBp
bmcgQXV0aG9yaXR5IDAwMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM+goLP30wll
jgat73Xi27jSX12c+ggN0piXmkAl/i4nti7utfhMAfQYmfRX6q5qF4PUamLkrKbsUaPLjDpyv/sP
eOUT8TR0WK8eOb5oh08VVEg/ih1O7nlUXZmgK2x5DDJGR4oUh4ejxm1a00jt5QpVBalMmCwm3ebx
7ZaNsf7THgMhR/hpwVYIv34PgF7ZgRxknpBVH+NNApiTigrG0DCRVNa7zUmH8I4dja3TdpfQBcAc
OhNE54tIlt5XVo7bl5QXDAogLCLVjNq4BvkieD21unXqZGCtnkxKzN9e+LecyxhrZCQFDkZus+ap
bLu3jqaO7oBr0UY3dOipBR1sZtkCAwEAAaOB9jCB8zAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/
BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFPS0tO8wxyFBt68qUleIwsnfxqyRMB8GA1UdIwQYMBaA
FQaVbwEt+Xki5wA5GYgVuQqLRZmLMIGIBgNVHR8EgYAwfjB8oHqgeIY5aHR0cHM6Ly9wa2kuZ2xv
YmFsdHJ1c3RlZHNpZ24uY29tL3N1YmNhL2d0c19zdWJjYV9jcmwuY3JshjtodHRwczovL3BraTAy
Lmdsb2lhbHRydXN0ZWRzaWduLmNvbS9zdWJjYS9ndHNfc3ViY2FfY3JsLmNybDANBgkqhkiG9w0B
AQsFAAOCAQEAn6wA9TlsyN1kGlpWnJyxBsNpmgu0rieAct9Ir/rdYJK+DvFIJtse4vcH/D+VKaQ8
UR/Vqrg4QYTGOEGjDYa+nOv6GRfC5Aq5c+KzCJ+ASdd5WkCBcAGf6aGFdIAQCrdKG9vEsmjS4PE
ACQssIFIkJ2vW816QCuieQmpSUeh7gGijx8JgNoITdlEJYaIS6Gwx4SuxVERrYd2eXEIPlUNAbhV
x/juz16WDqWlHEOaO0vwgZSZWd9g0ECjLTRSrkhbgqrmgH1i4KewBsRtBjJUpFvOIUZTRgImytMY
ILlWyougGQUF448loYRDvlEkDMAKGf9sLQW2Imwo237HFUBnEg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign Timestamping Authority 001*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN-iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Fri Jan 05 17:01:45 CET 2018*

Valid to: *Tue Jan 05 17:01:45 CET 2021*

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:CF:A0:A0:B3:F7:D3:09:65:8E:06:AD:EF:75:E2:DB:B8:D2:5F:5D:9C:FA:0A:8D:D2:98:97:9A:40:08:FE:2E:27:B6:2E:EE:B5:FB:4C:01:F4:18:99:F4:57:EA:AE:6A:17:83:D4:6A:62:E4:AC:A6:EC:51:A3:CB:8C:3A:72:BF:FB:0F:78:E5:13:F1:34:74:58:AF:1E:39:BE:68:87:4F:15:54:48:3F:8A:1D:4E:EE:79:54:5D:99:A0:2B:6C:79:0C:32:46:47:8A:14:87:87:A3:C6:6D:5A:D3:48:ED:E5:0A:55:05:A2:0C:98:2C:26:DD:E6:F1:ED:96:8D:B1:FE:D3:1E:03:21:47:F8:69:C1:56:08:BF:7E:0F:80:5E:D9:81:1C:64:9E:90:55:1F:E3:4D:02:92:13:8A:0A:C6:D0:30:91:54:D6:BB:CD:49:87:F2:2E:1D:8D:AD:D3:76:97:D0:05:C0:1C:3A:13:44:E7:8B:48:96:D4:97:56:8E:DB:97:94:17:0C:0A:20:2C:22:D5:8C:DA:B8:06:F9:22:78:3D:B5:BA:75:EA:64:60:AD:9E:4C:4A:CC:DF:5E:F8:B7:9C:CB:18:6B:64:24:05:0E:46:6E:B3:E6:A9:6C:BB:B7:8E:A6:90:EE:80:6B:D1:46:37:74:E8:A9:05:1D:6C:66:D9:02:03:01:00:01*

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *F4:B4:B4:EF:30:C7:21:41:B7:AF:2A:52:57:A5:C2:C9:DF:C6:AC:91*

Authority Key Identifier *E6:95:6F:01:2D:F9:79:22:E7:00:39:19:88:15:B9:0A:8B:45:99:8B*

CRL Distribution Points *https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl*

https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *BC:B7:A9:6C:61:8E:21:4D:AF:AA:97:CE:D1:2A:06:CE:91:6E:39:36:67:0E:46:2F:A5:CD:0D:44:2A:B7:91:92*

X509SubjectName

Subject CN: *Global Trusted Sign Timestamping Authority 001*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN-iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *9LS07zDHIUG3rypSV6XCyd/GrJE=*

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

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

Status Starting Time *2021-02-24T00:00:00Z*

8.2.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Global Trusted Sign Timestamping Authority 001 (Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN: *Global Trusted Sign Timestamping Authority 001*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN-iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *9LS07zDHIUG3rypSV6XCyd/GrJE=*

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

Status Starting Time *2018-02-07T01:00:00Z*

8.3 - Service (withdrawn): Global Trusted Sign Timestamping Authority 001 (new 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.*

Service Name

Name *[en]* *Global Trusted Sign Timestamping Authority 001 (new Qualified TSA)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *630087639396681225212878969629693114 3*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEITCCA32gAwIBAgIQBL2BMOSuYUBamUPbenJPRzANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UE
BhMCUFOxIzAhBgNVBAoMGkFDSU4gaUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTcwNQYDVQQDDC5HbG9iYWwgVHJ1c3RlZCBTaWduIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5IDAxMB4XDTE4MDMwMjEyMzAxOVoXDTIzMDMwMjEyMzAxOVowgYkxC2AJBgNV
BAYTAlBUMSMwIQYDVQQKDBpBQ0lOIGlDbG9lZCBTb2x1dGlvbnMsIExkYTEcMBoGA1UECwwTR2xv
YmFsIFRydXN0ZWQgU2lnbjE3MDUGA1UEAwwuR2xvYmFsIFRydXN0ZWQgU2lnbiBUaW1lc3RhbXBp
bmcgQXV0aG9yaXR5IDAwMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALm7DeDpumD
1MvBjL3V+7VC13VHKlhteLL+NpYxXFLkjq93oFumX5wlsoqtVfU50p6gOVTl52deq5z6wi6sTZAJ
5OD2xNmQp/hA6nSlxh9OOigoVzP5/ocPX68SdNh9uSvruJo5hLSshioTfRJZEDiR4gPdgcmDqR6
6Xf5gCW4qLfW43whHaQlKprQ7Xts3cB4uUQqqxSKMOvli9mPpGhgk15/oRPD38mzkyGS6ZMNsPJa
xRx7FMMvPaggyMJcFxJo7Fj9njlR5sQioT7/x91cE0KyW8Yc+ECQODJU7f3p4KO+W5ok5Pz16Tnb
2nAXmeAydcPtr61FHAygYlpjxgMCAwEAAaOB9jCB8zAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/
BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFCSj7vKaAk7TFKwGrHKFRTnvrbgWtMB8GA1UdIwQYMBaA
FQaVbwEt+Xki5wA5GYgYuQqLRZmLMIGIBgNVHR8EgYAwfjB8oHqgeHY5aHR0cHM6Ly9wa2kuZ2xv
YmFsdHJ1c3RlZHNpZ24uY29tL3N1YmNhL2d0c19zdWJjYV9jcmwuY3JshjtodHRwczovL3BraTAy
Lmdsb2lhbHRydXN0ZWRzaWduLmNvbS9zdWJjYS9ndHNfc3ViY2FhY3JsLmNybDANBgkqhkiG9w0B
AQsFAAOCAQEAVGl6f1TKLsVk0+EsknesJROv8cBDLgzYDjCaIlfYpaJ0845bxpdK/B7K/qKpKIlj
FnYitZYpR2oFFBZdWHi1C17Oc4C/5wDa6x5iYkzhpq5XietsZ8bjSiMhfo4jEdgPIfo0sd0Ys00c
Kh+UcAstlgxhoQtHRgmf0v23jR+bzGxSkBr6l3zJtGgEvZ2GtmxAlES XnMwaU0mJwK6HShQBi6tP
8EB2qWF+skjlpYjqeBGfXx+40+vOQZBbX9+OoNVlNN4tPvX7qExeCDKpkis0zPM9rpRlkXr25/js
52eQtJQuBarsaLwUn2/Qjz2MKPlnvTxmZ0xpOlBgTSG32ID0CA==
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Certification Authority 01*

Issuer OU:	*Global Trusted Sign*
Issuer O:	*ACIN iCloud Solutions, Lda*
Issuer C:	*PT*
Subject CN:	*Global Trusted Sign Timestamping Authority 001*
Subject OU:	*Global Trusted Sign*
Subject O:	*ACIN iCloud Solutions, Lda*
Subject C:	*PT*
Valid from:	*Fri Mar 02 13:30:19 CET 2018*
Valid to:	*Thu Mar 02 13:30:19 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:B2:26:EC:37:83:A6:E9:83:D4:CB:C1:8C:BD:D5:FB:B5:42:D7:75:47:28:88:6D:78:B2:FE:36:96:31:5C:52:E4:8E:AF:77:A0:5B:A6:5F:9C:25:B2:8A:AD:55:F5:39:D2:9E:A0:41:54:C8:E5:97:5E:AB:9C:FA:C2:2E:AC:4D:90:09:E4:E0:F6:C4:D9:90:A7:F8:40:EA:74:A5:C6:1F:4E:3A:28:28:57:33:F9:FE:87:0F:5F:AF:12:74:D8:7F:F6:E4:AF:AE:E2:68:E6:12:D2:B2:18:AB:7D:34:49:64:40:E2:47:88:0F:76:07:26:0E:A4:7A:E9:77:F9:A8:25:B8:80:B7:D6:E3:7C:21:1D:A4:25:2A:9A:D0:ED:7B:6C:DD:C0:78:B9:44:2A:AB:14:8A:30:EB:C8:8B:D9:8F:A4:68:60:93:5E:7F:A1:13:C3:DF:C9:B3:93:21:92:E9:93:0D:B0:F2:5A:C5:1C:7B:14:C3:2F:3D:AA:A0:C8:C2:5C:17:12:68:EC:5B:FD:9E:32:11:E6:C4:22:A1:3E:FF:C7:DD:5C:13:42:B2:5B:C6:1C:F8:40:90:38:32:54:ED:FD:E9:E0:A3:BE:5B:9A:24:E4:FC:F5:E9:39:DB:DA:70:17:99:E0:32:75:C3:ED:AF:AD:45:1C:0C:A0:60:8A:63:C6:03:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*24:89:EE:F2:9A:02:44:C5:2B:01:AB:1C:A1:51:4E:7B:EB:6E:05:AD*
Authority Key Identifier	*E6:95:6F:01:2D:F9:79:22:E7:00:39:19:88:15:B9:0A:8B:45:99:8B*
CRL Distribution Points	*https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl* *https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*33:E7:1E:50:6C:C3:5E:7B:DF:27:7A:BA:CF:42:20:3E:B3:60:58:E3:1E:C1:C6:78:FC:19:BD:E4:67:68:F1:D0*

X509SubjectName

Subject CN:	*Global Trusted Sign Timestamping Authority 001*
Subject OU:	*Global Trusted Sign*
Subject O:	*ACIN iCloud Solutions, Lda*
Subject C:	*PT*

X509SKI

X509 SK I	*JInu8poCRMUrAascoVFOe+tuBa0=*

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

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

Status Starting Time *2025-02-28T00:00:00Z*

8.3.1 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Global Trusted Sign Timestamping Authority 001 (new Qualified TSA)*

Service digital identities

X509SubjectName

Subject CN: *Global Trusted Sign Timestamping Authority 001*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *JInu8poCRMUrAascoVFOe+tuBa0=*

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

Status Starting Time *2018-07-08T23:00:00Z*

8.4 - Service (deprecatedatnationallevel): Global Trusted Sign NQ Certification Authority 02

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

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

Service Name

Name *[en]* *Global Trusted Sign NQ Certification Authority 02*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *168192306089547979096668908311603559873*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGRTCCBC2gAwIBAgIQfoio7VQCn8ZclgCOCs+9wTANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UE
BhMCUFQxIzAhBgNVBAoMGkFDSU4taUNsb3VklFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTwwOgYDVQQDDDNHbG9iYWwgVHJ1c3RlZCBTaWduIFjvb3QgQ2VydGlm
aWNhdGlvbiBBdXRob3IpdHkgMDEwHhcNMTkwMzIzMDk0NjU0WhcNMjUwMzIzMDk0NjU0WjCBjDEL
MAkGA1UEBhMCUFQxIzAhBgNVBAoMGkFDSU4gaUNsb3VklFNvbHV0aW9ucywgTGRhMRwwGgYDVQQL
DBNHbG9iYWwgVHJ1c3RlZCBTaWduMTowOAYDVQQDDDFHbG9iYWwgVHJ1c3RlZCBTaWduIE5RIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5IDAyMIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2rS7R3k4LiCOegV1EOq0uYY2jITO04pNZr/+WWGqft2K/QZSienj6kPDn4T4fXxf5LSK35yCmvrSL
0IRU5Czf8BnQ6PBT/5a7xGYkxteC+1YwjvzAjzSEoNrzZ+7QJuNMzFSWpZqJoJMHsJAobMKuroCda
2lmmn+xTk3Y8vg/cTbFLJhi9JEBBOVmaOBbmOR4lFgpU31n4GWIUX/v2t19da7CzvCauxeDXNVJo
XBUFdnIdLPz/DWtosSHoP9FUSVk9aXB48CUy+2OABPbTgJdqEgUWtygzu1D48kvBRjJHDR/IeOxS
11CjTQKBbBjtGqNdsSP+yWyaJ2ffv52WJLu2OI0AQABo4IBnTCCAZkwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAR8EBAMCAQYwHQYDVR0OBBYEFMZCmZMjCqcvIMS3u0FM6/cF2sbcMBBGA1UdIwQY
MBaAFKaYfKCRhNncXttOL4ICM5XTdC5BMFcGA1UdIARQME4wTAYOKwYBBAGDiH4BAQEBAQAwOjA4
BggrBgEFBQcCARYsaHR0cHM6Ly9wa2kuZ2xvYmFsdHJ1c3RlZHNpZ24uY29tL2luZGV4Lmh0bWww
TwYIKwYBBQUHAQEEQzBBMD8GCCsGAQUFBzAChjNodHRwczovL3Bra55nbG9hYWx0cnVzdGVkc2ln
bi5jb20vcm9vdC9ndHNfcm9vdC5jcnQwgYsGA1UdHwSBgzCBgDA9oDugOYY3aHR0cHM6Ly9wa2ku
Z2xvYmFsdHJ1c3RlZHNpZ24uY29tL3Jvb3QvZ3RzX3jvb3RfY3J5sLmNybDAoD2gO4Y5aHR0cHM6
Ly9wa2kwMi5nbG9iYWx0cnVzdGVkc2lnbi5jb20vcm9vdC9ndHNfcm9vdF9jcmwuY3JsMA0GCSqG
SIb3DQEBCwUAA4ICAQAzFkPzCYwkF5uOOrPnUePANcYeV9rjGuDgOGFU37vXvY6V9/RGru74vUqf
Pq0JkEBoAnpvq+i24n2URN0HbwVnUW8zTXhnVm8vYXdAVUgG/9B076/HIu8EfX/Xt2mHt/rpnvzl
rs7FltyxT5fkXrNgNxBuG4FlgOyiIwy3ahadgXVZOUCntBRjzFXQEN7TQS01DtPmqMPlTT9RAyiz
+m+4XchQEoj1IP0N3lasl3fWAZ1MHxLghK96+XlCvA2ZL/Th+InB780B9DtPt9bnXPYr1WbkPWd1
KFuLY//v8ybc1efypOUKxGPAOF52XK3lrnUQCJqaP6WXG2kQDIh8Vvh3V0qOu6jOj0AGXI8iQUdH
INkIu8OzFMDnnVvx+xpdYB+jpz8LbsfVediNVKRBXaOLVUjeeEWDXrR5ieVGbukIC4AYLkPYju9ru
cl4KEwW6hMyklUeYf5mJKwF0g18okHQe+oFW5c2dT4wnlCD9+WTXz5v9QrK9ei5LnS3U/CSEBQVX
mXizKPJBFaA6eKhyDHU8BBQXtYo0/FyKyJGGCfxYzol0LR5uu4O2YTOSMkjoXdja+gHKtZMU1cMO
UuWulqsmmwvsdVcLjT4qTXCQaI3vSHhuF/5GFm73w4uwIeD4tzl5J7YCprAVYKB3cCE4d318/dHl
QKBVZDUU0dqQr1OWTw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Root Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN-iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign NQ Certification Authority 02*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Sat Mar 23 10:46:54 CET 2019*

Valid to: *Sun Mar 23 10:46:54 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:DA:B4:BB:47:79:38:2E:20:8E:7A:05:75:10:EA:B4:B9:86:36:26:24:CE:D3:8A:
4D:66:BF:FE:59:61:9D:B5:02:BF:41:94:A2:7A:78:FA:90:F0:E7:E1:3E:1F:5F:17:F9:2D:22:B7:E7:20:A6:BE:B4:8B:D2:54:54:E4:2C:DF:F0:19:D0:E8:F0:53:FF:96:BB:C4:66:24:C6:D7:82:F8:
86:30:8E:FC:C0:8F:34:84:A0:D9:D9:FB:B4:09:B8:D3:33:15:25:A9:66:A2:68:24:C1:EC:24:0A:1B:30:AB:AB:A0:27:5A:DA:59:A6:9F:EC:53:93:76:3C:BE:0F:DC:4D:B1:4B:26:18:BD:24:40:4
1:39:59:9A:38:16:E6:39:1E:25:16:0A:54:DF:59:F8:19:69:54:5F:FB:F6:B7:5F:5D:6B:B0:B3:BC:26:AE:C5:E0:D7:35:52:68:5C:15:05:76:72:1D:2C:FC:FF:0D:6B:68:B1:21:E8:3F:D1:54:49:5
9:3D:69:70:78:F0:25:32:FB:63:80:04:F6:D3:80:97:60:12:05:16:B7:28:33:BB:50:F8:F2:4B:C1:46:22:47:0D:1F:C8:78:EC:52:D7:50:A3:4D:02:81:6C:19:63:B4:68:0D:76:C4:8F:FB:25:B2:
68:9D:9F:7E:FE:76:58:92:E3:D9:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *C6:42:99:93:23:0A:A7:2F:20:C4:B7:BB:41:4C:EB:F7:05:DA:C6:DC*

Authority Key Identifier *A6:98:7C:A0:91:84:D9:DC:5E:DB:4E:2F:82:02:33:95:D3:74:2E:41*

Certificate Policies

Policy OID: 1.3.6.1.4.1.50302.1.1.1.1.1.0

CPS pointer: https://pki.globaltrustedsign.com/index.html

Authority Info Access *https://pki.globaltrustedsign.com/root/gts_root.crt*

CRL Distribution Points	*https://pki.globaltrustedsign.com/root/gts_root_crl.crl* *https://pki02.globaltrustedsign.com/root/gts_root_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*9C:76:F3:D1:40:DF:2B:F4:1A:D1:3C:06:2D:4F:A0:36:13:12:2B:0B:FD:4D:AE:57:23:EB:29:D8:CD:E7:C2:7B*

X509SubjectName

Subject CN:	*Global Trusted Sign NQ Certification Authority 02*
Subject OU:	*Global Trusted Sign*
Subject O:	*ACIN iCloud Solutions, Lda*
Subject C:	*PT*

X509SKI

X509 SK I	*xkKZkyMKpy8gxLe7QUzr9wXaxtw=*

Service Status

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

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

Status Starting Time

2025-05-08T11:00:00Z

8.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.4.3 - History instance n.1 - Status: recognisedatnationallevel

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

Service Name

Name *[en]* *Global Trusted Sign NQ Certification Authority 02*

Service digital identities

X509SubjectName

Subject CN: *Global Trusted Sign NQ Certification Authority 02*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *xkKZkyMKpy8gxLe7QUzr9wXaxtw=*

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

Status Starting Time *2020-05-19T23:00:00Z*

8.4.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.4.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.5 - Service (granted): Global Trusted Sign Certification Authority 03

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]* *Global Trusted Sign Certification Authority 03*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *399305944939663004918108980440818680 22*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGQjCCBCgAwIBAgIQHgpaTrJFmTxeuS8xSNsM9jANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UE
BhMCUFQxIzAhBgNVBAoMGkFDSU4taUNsb3VklFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTwwOgYDVQQDDDNHbG9iYWwgVHJ1c3RlZCBTaWduIFjvb3QgQ2VydGlm
aWNhdGlvbiBBdXRob3IpdHkgMDEwHhcNMjAwNTExMTA1NTQ1WhcNMjgwNTExMTA1NTQ1WjCBiTEL
MAkGA1UEBhMCUFQxIzAhBgNVBAoMGkFDSU4gaUNsb3VklFNvbHV0aW9ucywgTGRhMRwwGgYDVQQL
DBNHbG9iYWwgVHJ1c3RlZCBTaWduMTcwNQYDVQQDDC5HbG9iYWwgVHJ1c3RlZCBTaWduIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IDAzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtfAh
RJm/Db9EMAc+ajhjBA9y2ElVujyVv5iEHbCAfY1dlv2j+ZIl+V3AkzAmpIAxUBuQOOJSnIxRqXgD
1KKDXJE2Ilg6isdf+m7RxKkb2a5aoF43ZxNe0gENpeGze9wuAAb1WMBz4UoBcA6suct6eFMh35G
a5NaD7rlaQsuLe7KBOhcDHOnbFqlGIZTyyIeEgwRaN7SQtZng+/rf+M8NtOZLw7QKDv6kXOHGxZ/
5RWEZ1VfajS65m9rzb6CSfWc0AcGRiwvh993hQHI6zLvKx09oDyycYNvpKPLB1A1y8iqPgLHtbR6
XQcl35gC7GAH/fWy5aUpnWHC0lWL44T57jQIDAQABo4IBnTCCAZkwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFP1LZrmejz10uyZ5ThzfkCKDYinFMB8GA1UdIwQYMBaA
FKaYfKCRhNncXttOL4ICM5XTdC5BMFcGA1UdIARQME4wTAYOKwYBBAGDiH4BAQECAQAwOjA4Bggr
BgEFBQcCARYsaHR0cHM6Ly9wa2kuZ2xvYmFsdHJ1c3RlZHNpZ24uY29tL2luZGV4Lmh0bWwwTwYI
KwYBBQUHAQEEQzBBMD8GCCsGAQUFBzAChjNodHRwczovL3BraS5nbG9iYWx0cnVzdGVkc2Inbi5j
b20vcm9vdC9ndHNfcm9vdC5jcnQwgYsGA1UdHwSBgzCBgDA9oDugOYY3aHR0cHM6Ly9wa2kuZ2xv
YmFsdHJ1c3RlZHNpZ24uY29tL3JvbXQvZ3RzX3JvbXRfY3JsLmNybDA7oD2gO4Y5aHR0cHM6Ly9w
a2kwMi5nbG9iYWx0cnVzdGVkc2Inbi5jb20vcm9vdC9ndHNfcm9vdF9jcmwuY3JsMA0GCSqGSIb3
DQEBCwUAA4ICAQAwFRjiXhM8ZfG5nrUhGO2ms+X81ne5DQbrJmFMVsKNJk0gWXQl86o7nTYYjBZp
3gOFHBP15MO9QG0pjpWdpktQSWmybTCaD7Lvs+Qsx5vZ3UodlInfmD9zdcDD35IowQEVW+0ni/Nor
pfDDbdpZnQNr1RB170jE0gM+XOH0MHpgMpvze3Oga+dKYXh3DEEFVXyH0aui2a9Kt+qN2zFZfiqB
Sp6YGAkfIZuTuLYiOZTLQBAZ4KB7a031qf4020Ij61s+tl4oS2mnWIVYt4zzDE/7pcQrTx/hoYFMK
+aYuya/nuULS7VpH2HBnqToY8fnr/OWsAU+o8Vv3Kso4u5Qnhq++DQKJCn3x8PuuXd2HqkPDBXpB
0I3+Y66JlpwAsGU6+1ngZlcrnGEN+ERukgvm98H+3Kj90q7jGLgVGfaKCfARMEWsXkxfnL/a5LBs
AEvnfG1tTu31VtGPSo9hnB1QEGAvhQzgfRfFMth1URMcKsJgjLjNAwBpcFDvKDLgOgry2re0kqH4
wdK7NF93d/LdwIQkFWUO8ic3auWaSePc7t+tY103Z7QDKuv3788izixcILX3CworVDLId6YiWbKM
Ck5Xl3iCyzGd9Kqa/EjOKfoYRs4EMa3oEnqcHvhmOieHOWktzGwPuuk2/9Y8iCw4aV4iWE9IFyW8
xYUog5tsYws3Fw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Root Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN-iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign Certification Authority 03*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Mon May 11 12:55:45 CEST 2020*

Valid to: *Thu May 11 12:55:45 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:B5:F0:21:44:99:BF:0D:BF:44:30:07:3E:8E:18:81:03:DC:B6:10:85:6E:8F:25:
6F:E6:21:07:6C:20:1F:63:57:65:BF:68:FE:64:82:3E:57:70:24:CC:09:A9:94:0C:7F:50:1B:90:38:E2:79:9E:5C:51:81:78:03:D6:42:8A:0D:72:44:D8:92:2A:EA:2B:1D:7F:E9:BB:47:12:A4:6F:
36:B9:6A:81:78:DD:9C:4D:7B:48:04:36:97:86:CD:EF:70:B8:00:1B:D5:63:01:CF:85:28:05:C0:3A:B2:E7:2D:6D:E1:4C:87:7E:46:6B:93:5A:0F:BA:E5:69:0B:2E:2D:EE:CA:04:E8:5C:0C:73:A
7:6C:5A:A5:18:86:53:CB:22:1E:12:0C:11:68:DE:D2:42:D6:67:83:EF:EB:7F:E3:3C:36:D3:99:2F:0E:D0:28:3B:FA:91:73:87:1B:16:7F:E5:15:84:67:55:5F:68:9B:3A:4A:6F:6B:CD:BE:82:49:
F5:9C:D0:07:06:46:2C:2F:87:DF:77:85:01:E5:EB:32:EF:2B:1D:3D:A0:3C:B2:71:83:6F:A4:A3:CB:07:50:35:CB:C8:AA:3E:02:C7:B5:B4:7A:5D:07:25:DD:28:02:EC:60:07:FD:F5:B2:49:A5:2
9:9D:61:C2:D1:62:F8:E1:3E:7B:25:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *FD:4B:66:B9:9E:27:3D:74:BB:26:79:4E:1C:CF:90:22:83:62:29:C5*

Authority Key Identifier *A6:98:7C:A0:91:84:D9:DC:5E:DB:4E:2F:82:02:33:95:D3:74:2E:41*

Certificate Policies

Policy OID: 1.3.6.1.4.1.50302.1.1.1.2.1.0

CPS pointer: https://pki.globaltrustedsign.com/index.html

Authority Info Access *https://pki.globaltrustedsign.com/root/gts_root.crt*

CRL Distribution Points	*https://pki.globaltrustedsign.com/root/gts_root_crl.crl* *https://pki02.globaltrustedsign.com/root/gts_root_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*47:2A:2B:23:2F:E9:D8:6B:08:8F:AD:83:C2:5E:37:04:27:DA:00:6E:7D:6D:FA:0C:F9:B3:B7:27:D0:07:D3:A8*

X509SubjectName

Subject CN:	*Global Trusted Sign Certification Authority 03*
Subject OU:	*Global Trusted Sign*
Subject O:	*ACIN iCloud Solutions, Lda*
Subject C:	*PT*

X509SKI

X509 SK I	*/UtmuZ4nPXS7JnlOHM+QIoNiKcU=*

Service Status

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

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

Status Starting Time

2020-05-19T23:00:00Z

8.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

8.5.4 - Extension (critical): Qualifiers [QCStatement, QCSSCDStatusAsInCert, QCForESig, QCForESeal, QCForWSA]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.3*

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.4*

Description

8.6 - Service (granted): Global Trusted Sign Timestamping Authority 002

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.*

Service Name

Name *[en]* *Global Trusted Sign Timestamping Authority 002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *451034786659162858477070181732104960 08*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGVDCCBDygAwIBAgIQIe6dMCTpDH5iz/msP/EMCDANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UE
BhMCUFQxIzAhBgNVBAoMGkFDSU4taUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTwwOgYDVQQDDDNHbG9iYWwgVHJ1c3RlZCBTaWduIFJvb3QgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkgMDEwHhcNMjIwNzE0MTExMDM2WhcNMzAwNzE0MTExMDM2WjCBiTEL
MAkGA1UEBhMCUFQxIzAhBgNVBAoMGkFDSU4gaUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQL
DBNHbG9iYWwgVHJ1c3RlZCBTaWduMTcwNQYDVQQDDC5HbG9iYWwgVHJ1c3RlZCBTaWduIFRpbWVz
dGFtcGluZyBBdXRob3JpdHkgMDAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAteD8
zCsckHab+rGTiXCRNPCgNfBZccb34LUtFB3Qa07qFcz25gDfPhgo2q7T++BBfFHCtbkrA9tY9kYU
V82OwJqeK8tySHc5BpT0tdmVEU0kGqxKekvCRDC6UTa8B8vVJiOfF/S88V70KdfuQaTKgITFTLmH
no/5vLJZsxbNFVv9dEi7dfO25KCAC/xlVoq1A3FCUV/S3bOzotVE8WY9/ma52yaNogRG4HQEUZd
0mTe4mishDyPVC5T/q4hGC3vgEaY7OlvQ4+sq3IlvgCknUKuNb0fVoSxiM2f2/XAaTnTH89KfjvT
WBBxTfqP3RRFwg5cg8rdsGTeT3s4ZvYh2wIDAQABo4IBrzCCAaswDgYDVR0PAQH/BAQDAgbAMBYG
A1UdJQEB/wQMMAoGCCsGAQUFBwMIMB0GA1UdDgQWBBSKB5LOvWhp83OXnwk0jSkqwG9wCzAfBgNV
HSMEGDAWgBSmmHygkYTZ3F7bTi+CAjOV03QuQTBXBgNVHSAEUDBOMEwGDisGAQQBg4h+AQEBAQEA
MDowOAYIKwYBBQUHAgEWLGh0dHBzOi8vcGtpLmdsb2JhbHRtYydXNDZWRzaWduLmNvb59pbmRleC5o
dG1sMAkGA1UdEwQCMAAwTwYIKwYBBQUHAQEEQzBBMD8GCCsGAQUFBzAChjNodHRwczovL3BraS5n
bG9iYWx0cnVzdGVkc2lnbi5jb20vcm9vdC9ndHNfcm9vdC5jcnQwgYsGA1UdHw5BgzCBgDA9oDug
OYY3aHR0cHM6Ly9wa2kuZ2xvYmFsdHJl1c3RlZHNpZ24uY29tL3Jvb3QvZ3RzX3jvb3RfY3JsLmNy
bDAoD2gQ4Y5aHR0cHM6Ly9wa2kwMi5nbG9iYWx0cnVzdGVkc2lnbi5jb20vcm9vdC9ndHNfcm9v
dF9jcmwuY3JsMA0GCSqGSib3DQEBCwUAA4ICAQAc11/fVaYDrDkxq9a2iqQnS+OlMSYh7nC1nPNF
vIV8x/oRiWNmV+jBdGXDmJlt81pT/pFgJGbEv13i6WgMASayYx+A8oiuD9Tjw95fs4Ej5XwwtFHb
Uww4yZ074q/Pd0bUzAUjqQeTXX1CoUsA6OrcSbUewJT/K3ldIje15MeHb7zEuZqfUiyHGMd0H8z2
wRAYMNgFZUYy0OyHB9EjRNCHxbgHUBmsN754vsr01Z8nxeD5usjPgoTejPsTa/UYbGLO67E9iyGT
QISV5DGUhIMUyJKz6ebenIgUTWXTeNEpqSCLO5Z5W/EsOIj7N/vmwRlcjMg6xUg0fUlYJlgaXWhf
WOoUA2bAViitiOEtnRcx9Ytdg3iUsfabesgwnjVXqUVak5po0A+DGk2QtrnORLLgdiq6LsskV99k
E27IirykESpcK2s6Gk4jZdeGaH6hE/U3wlMQwL0thru4v6fS0KgvFTYFmT5xyjOivXlzIlC1pwST
EgO/FDeDYaKMoAggXYZ/RGAluW0WShmpri/UzCSAPG9vgBCtrc8JscM3UVFra2ObcFUnpGWaqfKA
AG6XNXqQBioGygIjuOELhRvac2Pn6/19RlabLMeSVDcYcffCNxoLQNaUq5/mo8br0N+ATOE/gee
absk8beAmhHEK36s9hiUBf28M/GW33c9XDo12w==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Root Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN-iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign Timestamping Authority 002*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Thu Jul 14 13:10:36 CEST 2022*

Valid to: *Sun Jul 14 13:10:36 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:B5:E0:FC:CC:2B:1C:90:76:9B:FA:B1:93:89:70:91:34:F0:A0:35:F0:59:71:C6:
F7:E0:B5:2D:14:1D:D0:6B:4E:E0:15:CC:F6:E6:A0:DF:3E:18:28:DA:AE:D3:FB:E0:41:7C:51:C2:B5:B9:2B:03:DB:58:F6:46:14:57:CD:90:C0:9A:9E:2B:CB:72:48:77:12:06:94:F4:B5:D9:95:1
1:4D:24:1A:AC:4A:7A:4B:C2:44:30:BA:51:36:BC:07:CB:D5:26:23:9F:14:94:BC:F1:5E:F4:29:D7:EE:41:A4:CA:82:54:C5:4C:B9:87:9E:8F:F9:BC:B9:49:66:CC:5B:34:55:6F:F5:D1:0B:ED:D7
:CE:DB:92:82:00:2F:F1:95:5A:2A:D4:0D:C5:09:45:7F:4B:76:CE:CE:8B:55:13:C5:98:F7:F9:9A:E7:3C:9A:36:B8:11:1B:81:D0:11:46:5D:D2:64:DE:E2:68:AC:B4:3C:8F:54:2E:53:FE:AE:21:1
8:2D:EF:A8:46:98:EC:E2:2F:43:8F:AC:83:79:65:BE:00:A4:9D:42:AE:35:BD:1F:56:84:B1:88:CD:9F:DB:F5:C0:69:39:D3:1F:CF:4A:7E:3B:D3:58:10:71:4D:FA:8F:DD:14:45:C2:0E:5C:83:CA
:DD:B0:64:DE:4F:7B:38:66:F6:21:DB:02:03:01:00:01
```


Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *8A:07:92:CE:BD:68:69:F3:73:97:9F:09:34:8D:29:2A:C0:6F:70:0B*

Authority Key Identifier *A6:98:7C:A0:91:84:D9:DC:5E:DB:4E:2F:82:02:33:95:D3:74:2E:41*

Certificate Policies

Policy OID: 1.3.6.1.4.1.50302.1.1.1.1.1.0

CPS pointer: https://pki.globaltrustedsign.com/index.html

Basic Constraints *IsCA: false*

Authority Info Access *https://pki.globaltrustedsign.com/root/gts_root.crt*

CRL Distribution Points

https://pki.globaltrustedsign.com/root/gts_root_crl.crl

https://pki02.globaltrustedsign.com/root/gts_root_crl.crl

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E6:4A:47:C6:8E:B4:2E:E6:D5:55:35:D7:0F:95:E1:CA:DD:2F:E6:C5:60:FD:BD:6F:E6:3E:CF:51:62:98:74:FC*

X509SubjectName

Subject CN: *Global Trusted Sign Timestamping Authority 002*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *igeSzr1oafNzl58JNI0pKsBvcAs=*

Service Status

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

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

Status Starting Time

2023-01-17T17:30:42Z

8.7 - Service (recognisedatnationallevel): Global Trusted Sign NQ Certification Authority 03

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

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

Service Name

Name *[en]* *Global Trusted Sign NQ Certification Authority 03*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *121058224641007306570347270578850088292*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGRTCCBC2gAwIBAgIQWxL3SsvKc+BizITh DXFZDANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UE
BhMCUFQxIzAhBgNVBAoMGkFDSU4taUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQLDBNHbG9i
YWwgVHJ1c3RlZCBTaWduMTwwOgYDVQQDDDNHbG9lYWwgVHJ1c3RlZCBTaWduIFJvb3QgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkgMDEwHhcNMjIwNzE0MTAzODExWhcNMzAwNzE0MTAzODExWjCBjDEL
MAkGA1UEBhMCUFQxIzAhBgNVBAoMGkFDSU4gaUNsb3VkIFNvbHV0aW9ucywgTGRhMRwwGgYDVQQL
DBNHbG9lYWwgVHJ1c3RlZCBTaWduMTowOAYDVQQDDDFHbG9lYWwgVHJ1c3RlZCBTaWduIE5RIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5IDAzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0tORBPNjssrDz9SNdPpm43hxAYEmtv5Yk/LNx6lYpUPkecC3uJazsPoMmZPZF+2SGSwP+TYiWWr3
t4Zi5NEtrmL8WaOuJRwjZY5dY0lDb+Gm1ummjPExyeqyJUid9DHCxHsd0tno/l0gPpah5PY5yHsj
gybNNOiPLtRXiGfDdm+pF4Za2jr9OIJyUbmg3gp6vrxvur6/78d+PKdGHeB68sRzbODVPl++YhaV
stRIU9PrlkSueyJU5uRtqC1oMxWJcUB5cNefDQ82XCp1DX+0yYLJFVMNPR9229Gx1ZLV8W3QAAtx
c/qogM9e1FtsgLVLYCD1PUr4A8gOx8a5lKzbLQIDAQABo4IBnTCCAZkwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFHp77AqF9btGkuC9dssAmXnSt6MWMB8GA1UdIwQY
MBaAFKaYfKCRhNncXttOL4ICM5XTdC5BMFcGA1UdIARQME4wTAYOKwYBBAGDIH4BAQEBAQAwOjA4
BgqrBgEFBQcCARYsaHR0cHM6Ly9wa2kuZ2xvYmFsdHJ1c3RlZHNpZ24uY29lZluZGV4Lmh0bWww
TwYIKwYBBQUHAQEEQzBBMD8GCCsGAQUFBzAChjNodHRwczovL3Bra55nbG9lYWx0cnVzdGVkc2ln
bi5jb20vcm9vdC9ndHNfcm9vdC5jcnQwgYsGA1UdHwSBgzCBgDA9oDugOYY3aHR0cHM6Ly9wa2ku
Z2xvYmFsdHJ1c3RlZHNpZ24uY29tL3Jvb3QvZ3RzX3jvb3RtY3jSLmNybDA/oD2gO4Y5aHR0cHM6
Ly9wa2kwMi5nbG9lYWx0cnVzdGVkc2lnbi5jb20vcm9udC9ndHNfcm9udF9jcmwuY3jsMA0GCSqG
SIb3DQEBCwUAA4ICAQA8fnJpjKREV3oQcc6i1nNfzzIEPuQVDjYajlH1GeRqW/oHSH8CATabspec
cVEn/D6KUpwUZxsZKVwV3yOP/0TqBn5mlvrVoPd9FEHZEUsJOL0oGV6CQbedyUPZr+/zl6nlGZPr
y5NokAkOZw3jiNa2NphN12mFHGUw7HIHN7V4M8yZiBj2a7a1PHAruYR/BnsE/ld4ZIGGc8NTNY+r
VOzYcIG/LIIF0BIFCJ4jy8MgGhOoZAyfKuh555EXcEaBnpXiWfILtj/FUE4u338Thnqtt DcDfwsW
Rx4seZa+1h2UZwxzMw6NgmueTrtNjt0gID3w6tD7Ujw/0fGsWMXRb486aDzpQqsO3Up+Hnm7DiLo
tVR+Dy2qXV3xE+P8nEmxgh3dAQNzkjfhNeA94V3Ttpbnpigb+k5gr7dovYM1uu45MY2V/zSdZXMo
jCx2FgqDwuXlz2EOTZPPBDS5n9a3dUbw8XlmktT52XE2r/9cQlseU0NtD5JpuD5TxOJWa3t4mg4a
uqxVdArU8zHcIS28/6I1/7yyqGqlxrlq5un7LFZ6SBeNZH+c35/FeqqyCqPvKhJ1xfRNmLonfss
cHYAfnovV3dPY/+c/yR071ajewg+i24TuqZfCjTL2KFWc/8VZSQtKPwKVqP8pZDwvUNGb0MBzYSe
SY0UZ4G/c/JFJqCeYw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Global Trusted Sign Root Certification Authority 01*

Issuer OU: *Global Trusted Sign*

Issuer O: *ACIN-iCloud Solutions, Lda*

Issuer C: *PT*

Subject CN: *Global Trusted Sign NQ Certification Authority 03*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

Valid from: *Thu Jul 14 12:38:11 CEST 2022*

Valid to: *Sun Jul 14 12:38:11 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:D2:D3:91:04:F3:49:B2:CA:C3:CF:D4:8D:74:FA:66:E3:78:71:01:81:26:B6:FE:
58:93:F2:CD:C7:A9:58:A5:43:E4:79:C0:B7:B8:96:B3:B0:FA:0C:99:93:D9:17:ED:92:19:2C:0F:F9:36:22:59:6A:F7:B7:86:62:E4:D1:2D:AE:62:FC:59:A3:AE:25:1C:23:65:8E:5D:63:49:43:6F
:E1:A6:D6:E9:A6:24:F1:31:C9:EA:B2:25:48:9D:F4:31:C2:C4:7B:1D:D2:D9:E8:FE:5D:20:3E:96:A1:E4:F6:39:C8:7B:23:83:26:CD:34:E8:8F:2E:D4:57:88:67:C3:76:6F:A9:17:86:5A:DA:3A:F
D:40:82:72:51:B9:A0:DE:AA:7A:BE:BC:6F:BA:BE:BF:EF:C7:7E:3C:A7:46:1D:E0:7A:F2:C4:73:6C:E0:D5:3C:8F:BE:62:16:95:B2:D4:65:53:D1:68:96:44:AE:7B:22:54:E6:E4:6D:80:2D:68:33
:15:89:71:40:52:70:D7:9F:0D:0F:36:5C:2A:75:0D:7F:B4:C9:82:C9:15:53:0D:3F:AF:76:DB:D1:B1:D5:92:D5:F1:6D:CE:00:0B:71:73:FA:A8:80:CF:5E:D4:5B:6C:80:B5:4B:60:27:75:3D:4A:
F8:03:C8:0E:C7:C6:B9:94:AC:DB:2D:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Subject Key Identifier *7A:7B:EC:0A:85:F5:BB:46:92:E0:BD:76:CB:00:99:79:D2:B7:A3:16*

Authority Key Identifier *A6:98:7C:A0:91:84:D9:DC:5E:DB:4E:2F:82:02:33:95:D3:74:2E:41*

Certificate Policies

Policy OID: 1.3.6.1.4.1.50302.1.1.1.1.1.0

CPS pointer: https://pki.globaltrustedsign.com/index.html

Authority Info Access *https://pki.globaltrustedsign.com/root/gts_root.crt*

CRL Distribution Points

https://pki.globaltrustedsign.com/root/gts_root_crl.crl

https://pki02.globaltrustedsign.com/root/gts_root_crl.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A1:C5:7E:3D:13:AF:EC:2F:FD:24:F0:12:10:17:D6:E7:FD:12:2F:85:C7:8E:24:F1:A7:71:8F:AD:0C:BD:D7:8D*

X509SubjectName

Subject CN: *Global Trusted Sign NQ Certification Authority 03*

Subject OU: *Global Trusted Sign*

Subject O: *ACIN iCloud Solutions, Lda*

Subject C: *PT*

X509SKI

X509 SK I *envsCoX1u0aS4L12ywCZedK3oxY=*

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

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

Status Starting Time *2023-01-20T11:12:08Z*

8.7.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

8.7.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9 - TSP: Agência para a Reforma Tecnológica do Estado, I. P.

.

TSP Name

Name	*[pt]*	*Agência para a Reforma Tecnológica do Estado, I. P.*
Name	*[en]*	*Agência para a Reforma Tecnológica do Estado, I. P.*
Name	*[pt]*	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Name	*[en]*	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

TSP Trade Name

Name	*[en]*	*ARTE*
Name	*[en]*	*VATPT-508184509*
Name	*[en]*	*AMA*

PostalAddress

Street Address	*[en]*	*Rua de Santa Marta n.º 55*
Locality	*[en]*	*Lisboa*
State Or Province	*[en]*	*Lisboa*
Postal Code	*[en]*	*1150 - 294 Lisboa*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Rua de Santa Marta n.º 55*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1150 - 294 Lisboa*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:arte@arte.gov.pt*
URI	*[en]*	*https://www.arte.gov.pt/*

TSP Information URI

URI *[en]* *https://www.arte.gov.pt/*

9.1 - Service (granted): Chave Móvel Digital 00001

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]* *Chave Móvel Digital 00001*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5445717213426110391*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIAzCCBeugAwIBAgIIS5MS8/V+T7cwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXI0aWZpY2HDpBOjbyBFbGVjdHLDs25pY2EgZG8g
RXNOYWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDQwHhcNMTgwMzI2MTEwODMyWhcNMzAwMzI2MTEwODMyWjCB6TELMAkGA1UEBhMCUFQxQjBABgNV
BAoMOUFNOSAtIEFHw4pOO0lBIFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1JTkITVFJBVElWQSBJ
LiBQLjEcMBoGA1UECwwTQ2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViUlNFc3RhZG8x
YjBgBgNVBAMMWUVDIGRlIENoYXZlIE3Ds3ZlbCBEaWdpdGFsIGRlIEFzc2luYXR1cmEgRGlnaXRh
bCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENpZGFkw6NvIDAwMDAxMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEA7vDxrTDdrIccFXbmDSTPvNuYn7Oj52Bts7a6t6FBPS+F41oLAJ
UcT0yEhPMxIgY7giYWkR9bwuBOWi6Brk1+KYZ8gySfp8sA3vHmph+LD0OhuxrhfLuRdf/w8JA0c
Y8lnuIZNtdIq1IQ39U+HQACECzPMcjoaTGpX2RuAnWxnD9PbRYE1DAcKztRb/G659NQ5zK5HA8Dj
RUmE23Z+lOltQjHFb5V91m9Y8U+H4vAfidTomOpxGCzuJCneKRLsSzOMZjleVbbknPWUrCmu/xXA
0M6oFK17X/4hZdK9vT/ERMrRtOOejD/DN8dqRQtNUecUH9VH20qcPkkXWW7wOKIG5Eqfl643oM8o
5Ox071FW62PLArt51NRGtKk25FqtbBTh/Ghw0kKiHukocjwRTLiHo4m9mPWwceZmvdhUlyi3Pjc0
YoaRC59NjNzejzKfV9fQmT6WIDTlOpBLKB5cETBB5ZcgaVvligh8v8X2NAA9sTZQaXoZV/D15/
x3v2+Xc/nH/d2U4EN0rU4bNRteAgWb6XuUCOrZaGfzajgR+OdbqZOihEcoenKDUiGvy4HWGwTDJW
A+odlX5FwRZShYDnzXs5O2KbwUsXagD+OMf4hdEOVDj3wd4otB8izmF/b8uv9YzjRqcl+o1LIG6Q
MgDDxcAtWkGhIpqEkwiAMjECAwEAAaOCAhAwggIMMEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcw
AYYwaHR0cDovL29jc3Aucm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMB0GA1Ud
DgQWBBQRjenPzHSh7jhsblzWIKVWg67YOjASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaA
FBi2DK7+AWFpRLZB68+kOHPC+506MIH+BgNVHSAEgfYwgfMwVQYLYIRsAQEBAgQAAQkwRjBEBggr
BgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz
L2NwLmh0bWwwZgYKYIRsAQEBAgQABzBYMFYGCCsGAQUFBwIBFkpodHRwOi8vcGtpLmNhcnRhb2RI
Y2lkYWRhby5wdC9wdWJsaWNvL3BvbGl0aWNhcy4cGMvY2NfZWNfY2lkYWRhb19kcGMuaHRtbDAy
BgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cuc2NlZS5nb3YucHQvcGNlcnQwVwYDVR0f
BFAwTjBMoEqgSlZGaHR0cDovL3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9scmMvY2Nf
ZWNfY2lkYWRhb19jcmwwMDRfY3JsLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQAD
ggIBACX90Ydp7bQNnM4iIJuwqHNxqXmQx/yioUCKno8kyqCsZgTk7M6fb4I/vgBlzG1ARXrEGL
xk3b7pqBa+Omg4/To5j1VY/nXfp3A7mBgbGNh9tWJLdO3rNXTN2bAHJbfeBJmDZTzSJvgEOHNCxf
7Jw+CXeplpkK75Za8VAfEk1ftWAX8OxqyzyPD+J2+erNyk0UIxx5q0B11Lz8JZgQjKjUbI44MiAc
qZrgn+/ZEmljbSuHrVHhYiqmu8x0JNcuh+lXRqMsOvnWvP4CfbXdZYi8ZIivVQhjC1g9edScTQKU
CtvEv+UiujPww7IKDwp9OUxP/dwLJFu3A3dKMyGwrBQXRKYnHOPQ5PR/UGlNLKMh6nw0k3sOMn/Y
u0fXJ1rt8He48iz+lHjKsRHBb9jK6IL0hwBXk+mjYQ8jrBOlOjJCUg+yxOkXuoLWd2NRE7GbzkNR
2GJXDenb6OidIONwHqbrzFBpfM9LmV6Cz+pnD0Ca/7qnbf1acwTCEt/EDCJvb5UF8ZGRq6gHXWLt
f6Fq8ubikKJDVegI1xSHFyKykeCDbZfn49pL4gcrUjSS3Rr/M4dKXLhbeIrErGBxUs+tBeGJU8d4
14+VWgMKaIdIiaM5e4/tt+yMim6Wy+pTLiuJSAy8ZtyjIl2ichI6GsKPgTI51I+96NDaZMbpPb63/
DIVD

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 004*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00001*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

Valid from: *Mon Mar 26 13:08:32 CEST 2018*

Valid to: *Tue Mar 26 12:08:32 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:EE:F0:F1:AD:30:DD:AC:87:1C:15:76:E6:0D:24:CF:BC:DB:9F:62:7E:CE:26:2E:76:06:DB:38:6B:AB:7A:14:13:D2:F8:5E:35:A0:B0:09:51:C4:F4:CB:48:4F:33:12:20:63:B8:22:61:68:A4:47:D6:F0:B8:13:96:88:A0:68:93:5F:8A:61:9F:20:C9:2B:69:F2:C0:37:BC:79:A9:87:E2:C3:D1:08:6E:C6:B8:5F:2E:E4:5D:7F:FC:3C:24:0D:1C:63:C9:67:B8:86:4D:B5:D2:2A:D7:54:37:F5:4F:87:40:00:84:0B:33:CC:72:3A:1A:4C:6A:57:D9:1B:80:9D:6C:67:0F:D3:DB:45:81:35:0C:07:0A:CE:D4:5B:FC:6E:B9:F4:D4:39:CC:AE:47:03:C0:E3:45:49:84:DB:76:7E:94:E2:2D:42:31:C5:6F:95:7D:D6:6F:58:F1:4F:87:E2:F0:1F:89:D4:E8:98:EA:71:18:2C:EE:24:29:DE:29:12:EC:4B:33:8C:66:39:5E:55:B6:E4:9C:F5:94:AC:29:AE:FF:15:C0:D0:CE:A8:14:AD:7B:5F:FE:21:65:D2:BD:BD:3F:C4:44:CA:D1:B4:E3:9E:8C:3F:C3:37:C7:6A:45:0B:4D:51:E7:14:1F:D5:47:DB:4A:9C:3E:49:17:59:6E:F0:38:A9:46:E4:4A:9F:97:AE:37:A0:CF:28:E4:EC:50:EF:51:56:EB:63:CB:02:BB:79:D4:D4:46:B4:A9:36:E4:5A:AD:6C:14:E1:FC:68:70:D2:42:A2:1E:E9:28:72:3C:11:4C:B8:87:A3:89:BD:98:F5:B0:71:E6:66:BD:D8:54:97:28:B7:3C:97:34:62:86:BC:0B:9F:4D:8C:DC:DE:27:32:A2:15:5F:5F:42:64:FA:5A:50:D3:94:EA:41:2C:A0:52:70:44:C1:05:26:46:72:06:95:BE:58:A0:87:CB:FC:5F:63:40:03:DB:13:D9:06:97:A1:95:7F:0F:54:BF:C7:7B:F6:F9:77:3F:9C:7F:DD:D9:4E:04:37:4A:D4:E1:B3:51:B5:E0:20:59:BE:97:B9:40:8E:AD:96:86:7F:36:A3:81:1F:8E:75:BA:99:3A:28:44:72:87:A7:28:35:22:1A:FC:B8:1D:61:B0:4C:32:56:03:EA:1D:95:7E:45:C1:16:52:85:80:E7:CD:7B:39:3B:62:9B:C1:4B:17:6A:00:FE:38:C7:F8:85:D1:0E:55:42:77:C1:DE:28:B4:1F:22:CE:61:7F:6F:CB:AF:F5:8C:E3:46:A7:25:FA:8D:4B:94:6E:90:32:A0:C3:C5:C0:2D:5A:41:A1:96:9A:84:93:08:80:32:31:02:03:01:00:01

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Subject Key Identifier *11:8D:E9:CF:CC:74:A1:EE:38:6C:6C:8C:D6:20:A5:56:AB:AE:D8:42*

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

Authority Key Identifier *19:76:0C:AE:FE:01:61:69:44:B6:41:EB:CF:A4:38:73:C2:FB:9D:3A*

Certificate Policies

Policy OID: 2.16.620.1.1.1.2.4.0.1.9

CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html

Policy OID: 2.16.620.1.1.1.2.4.0.7

CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html

Policy OID: 2.5.29.32.0

CPS pointer: http://www.scee.gov.pt/pcert

CRL Distribution Points *http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl004_crl.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *11:9F:0F:E4:C3:CE:62:1A:53:B6:C4:F4:FF:56:11:A1:C9:25:0C:4F:7B:A3:DE:45:F4:85:5F:F2:9F:4C:46:15*

X509SubjectName

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00001*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

X509SKI

X509 SK I *EY3pz8x0oe44bGyM1iClVquu2EI=*

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

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

Status Starting Time *2018-06-11T23:00:00Z*

9.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

9.2 - Service (granted): Chave Móvel Digital 00002

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]* *Chave Móvel Digital 00002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *4888358685188713580*

X509 Certificate	-----BEGIN CERTIFICATE----- MIIH8TCCBdmgAwIBAgIQ9bwUxVebGwwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw MDUwHhcNMTkwNTI5MTA0ODA5WhcNMzEwNTI5MTA0ODA5WjCB6TELMAkGA1UEBhMCUFQxQjBABgNV BAoMOUFNQSAtIEFHw4pOQ0lBIFBBUkEgQSBNT0RFUk5lWkHDh8ODTyBBRE1JTkITVFJBVEIWQSBj LiBQLjEcMBoGA1UECwwTQ2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3VRUNFc3RhZG8x YjBgBgNVBAMMWUVDIGRlIENoYXZlIE3Ds3ZlbCBEaWdpdGFsIGRlIEFzc2luYXR1cmEgRGlnaXRh bCBRdWFsaWZpY2FkYSBkbyBDYXJ0w6NvIGRlIENpZGFkw6NvIDAwMDAyMIICIjANBgkqhkiG9w0B AQEFAAOCAg8AMIICCgKCAgEA6om1x4cU+qtwaBZAbwdsGuKXveXxcpYN/sRKKQPStBaBHolDnC/9 0ghHMEwO95HH8UBKMahVbW+T7kG7UomUczrTy4pjCRWnIWbBQNmgcSSwK67iaENEZZWENuGUJBtm b2ZUqK8baW3eYN9Yq8xL3vPGD3WAaDiGcPjxc/3BxyfLHlddzfDNPyX7qOEEy4ZPkNGkaCAObri4 XrnBNRQ8sE0imiLAj821fab/DZBNbCd8WJU2MwOK0grOjmzqxJhVt5HDcz2pT6Aqh6bvxwHuQ7lb gcGXusbpU62W9/Rb71bq9QHkGaCJEe/l0YNzWOy2dWSzUh8issu1sHKU8a0oyU7fbl0fmnsndKi0 M7mD9EqFm+3QU4LW0Gxe/hlppqwkmGucRr+qd72hVUf9EmYkzAPGDs26tp3xN+fzGLczU7/4binW HfEREmHuVpO6vB47vr1HnMB5Ui2gzOKcGz4OlEI/itI1lCdEvYxn+a6Z45zlVn8Zzpo7DEjwL5a 1mLBKy6lelk0zOdf2Tf1foaldeb2AUqdaNut2pbXF7tWjcPQgeaRB7DDZ6hLIVvhkcz8I4AXHYr2 lXt58CL6HT/TFJKeMjjE0M1w9oEwiwIkX359/80p+lIKM8g8OTNFpF88YxhAKeowZ+jc3hj5J8A0 oewdjD7hNXJVgmISw3v0lG8CAwEAAaOCAf4wggH6MEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcw AYYwaHR0cDovL29jc3Aucm9vdC5jYXJ0YW9kZWNpZGFkYW8ucHVucHVibGljby9vY3NwMB0GA1Ud DgQWBBT1cz4tidak1oA+3c/ZZAmAIKbvnDA5BgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaA FPbLg7KPA2BajGRcfZHRTrU5ZuEpMIHsBgNVHSAEgeQwgeEwVQYLYIRsAQEBAgQAAQkwRjBEBggr BgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz L2NwLmh0bWwwVQYKYIRsAQEBAgQABzBHMEUGCCsGAQUFBwIBFjodHRwczovL3BraS5jYXJ0YW9k ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGlj YXMvY3BzLmh0bWwwMQYEVR0gADApMCcgCCsGAQUF BwIBFhtodHRwczovL3d3dy5zY2VlLmdvdi5wdC9yZXAwVwYDVR0fBFAwTjBMoEqgSIZGaHR0cDov L3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9scmMvY2NtZWNfY2lkYWRhb19jcmwwMDVf Y3JsLmNvbDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBADHCWQMScOXXILBxN0hf 6GTHhDdStX6wioULIJ2scxI3qQzEwyGvWNV258AcNjpy+e12d6Nfo1SmrPLqrRZl5E0Of0BE6rM O6m290FblgN4Vw9dScrZgGlyEndtiAfcGLOKkyzHdFcjlKziRfmvdwlr5HIFx3LeDB/PMnVTF6bm VVIJg14LyV43uVr6qAPP7GlB8gO8zTUtF5aYRDjEaLhsL7wBSlmhp4VacXtw57rJg4HkSCyHssh5 ziVnWPgXS4LPdkhwcWGUWP6hNeUUNSZ7iIImitd3rvVYEHHFpjC8PHNn31g6jfnNSlYrZSiVGe7i gbcabUB P6uHnhzT7eYe5DlIy3G4ApR6U6F8oAfnM7U/xcp2DPa3OA7rXgnTo7BgfAAapFOHZjtQSA WUu8I1N/l81goz5n2vzztLCC7BDDF1IYj9rWfbT/EdFCvYf6LYUskfki78IGaWWBNJG5T2F5/xTp HYkeXOzpB/iB6b/uH7adyQsLz+jqnvpmSPBWGLims/SLWBTeNnideZuq6el1604aphQ1H+u2Y3Ap dlq/PgUBbT4X/MKPv3S4tfeJOlLgg4GXc0cy4y/98FHtbxkfTsve1FiypFVdUOTrv0vXy6IrgE/l BLNd/l+kngVm5QBJ4nNelp269Ya5WlOe9KRMVZga30RSElPxSeirmZ2e -----END CERTIFICATE-----
Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Cartão de Cidadão 005*
Issuer OU:	*ECEstado*
Issuer O:	*SCEE - Sistema de Certificação Electrónica do Estado*
Issuer C:	*PT*
Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00002*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*
Valid from:	*Wed May 29 12:48:09 CEST 2019*
Valid to:	*Thu May 29 12:48:09 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:EA:89:B5:C7:87:14:FA:AB:70:68:16:40:6F:07:6C:1A:E2:97:BD:E5:F1:72:9C: 8D:FE:C4:4A:29:03:EC:B4:16:81:1E:89:43:9C:2F:FD:D2:08:47:30:4C:0E:F7:91:C7:F1:40:4A:31:AB:55:6D:6F:93:EE:41:BB:52:89:94:73:3A:D3:CB:8A:63:09:15:A7:21:66:C1:40:D9:A0:71 :24:B0:2B:AE:E2:68:43:44:65:95:84:36:E1:94:24:1B:66:6F:66:54:A8:AF:1B:69:6D:DE:00:DF:58:AB:CC:4B:DE:F3:C6:0F:75:80:68:38:86:70:FB:F1:73:FD:C1:C7:27:CB:1C:B7:5D:CD:F0:C D:3F:25:FB:A8:E1:04:CB:86:4F:90:D1:A4:68:20:0E:6E:B8:B8:5E:B9:C1:35:14:3C:B0:4D:22:9A:22:C0:27:CD:B5:7D:A6:FF:0D:90:4D:6C:27:7C:58:95:36:33:03:8A:D2:0A:CE:8E:6C:EA:C 4:98:55:B7:91:C3:73:3D:A9:4F:A0:2A:87:A6:EF:C7:01:EE:43:B2:1B:81:C1:97:BA:C6:E9:53:AD:96:F7:F4:5B:EF:56:EA:F5:01:E4:19:A0:89:11:EF:E5:D1:83:73:58:EC:B6:75:64:B3:52:1F:2 2:82:CB:B5:B0:72:94:F1:AD:28:C9:4E:DF:6E:5D:1F:9A:7B:27:74:A8:B4:33:B9:B3:F4:4A:85:9B:ED:D0:53:82:D6:D0:6C:5E:FE:19:69:A6:0C:24:98:6B:9C:46:BF:AA:77:BD:A1:55:47:FD:12 :66:24:CC:03:C6:0E:CD:BA:B6:9D:F1:37:E7:F3:18:B7:33:53:BF:F8:6E:29:D6:1D:F1:11:12:61:EE:56:93:BA:BC:1E:3B:BE:BD:47:9C:C0:52:52:E6:60:CD:02:9C:1B:3E:34:94:49:7F:8A:D8: A2:D4:80:9D:12:F6:31:9F:E6:BA:67:84:B3:95:59:FC:67:3A:68:4F:41:23:C0:B4:9A:D6:62:C1:2B:2E:88:78:89:34:CC:E7:5F:D9:37:F5:7E:86:A5:75:E6:F6:01:4A:9D:68:DB:AD:DA:96:D7:1 7:BB:56:25:C3:D0:81:E6:91:07:B0:C3:67:A8:4B:21:5B:E1:91:CC:FC:97:80:17:1D:8A:F6:21:7B:79:F0:22:FA:1D:3F:D3:14:92:9E:32:38:C4:D0:CD:70:F6:81:30:8B:02:24:5F:7E:7D:FF:CD: 29:F8:82:0A:33:C8:3C:39:33:45:A4:5F:3C:63:18:40:29:EA:30:67:E8:DC:DE:18:F9:27:C0:34:A1:EC:1D:8C:3E:E1:35:72:55:82:69:52:C3:7B:F4:94:6F:02:03:01:00:01*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Subject Key Identifier	*F5:73:3E:2D:89:D6:A4:D6:80:3E:DD:CF:D9:64:09:80:20:A6:EF:9C*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*F6:CB:83:B2:8F:03:60:5A:8C:64:5C:7D:91:D1:4E:B5:39:66:E1:29*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.9* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl005_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*18:91:1C:E2:3E:93:98:A8:B8:E7:5A:30:BA:D3:62:BD:B1:45:6A:A9:97:BB:6F:5B:3B:16:EB:ED:7C:95:7A:FE*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00002*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*

X509SKI

X509 SK I	*9XM+LYnWpNaAPt3P2WQJgCCm75w=*

Service Status

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

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

Status Starting Time

2019-06-23T23:00:00Z

9.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

9.3 - Service (granted): Chave Móvel Digital 00003

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]* *Chave Móvel Digital 00003*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *453404888397271453*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIH8TCCBdmgAwIBAgIIBkrRWABYUZ0wDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlBUMUAw
PgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBdZXJ0aWZpY2HDp8OjbyBFbGVjdHLDs25pY2EgZG8g
RXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBDaWRhZMOjbyAw
MDYwHhcNMjAwMjA2MTYxNzIzWhcNMzIwMjA2MTYxNzIzWjCB6TELMAKGA1UEBhMCUFQxOjBABgNV
BAoMOUFNQSAtIEFHw4pOQ0lBIFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1JTkITVFJBVElWQSBJ
LiBQLjEcMBoGA1UECwwTQ2FydMOjbyBkZSBDaWRhZMOjbzEUMBIGA1UECwwLc3ViRUNFc3RhZG8x
YjBgBgNVBAMMWUVDIGRlIENoYXZlIE3Ds3ZlbCBEaWdpdGFsIGRlIEFzc2luYXR1cmEgRGlnaXRh
bCBRdWFsaWZpY2FkYSBkbyBOYX0w6NvIGRlIENpZGFkw6NvIDAwMDAzMlICjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEArnX3onYP0IEuGZL1io3fhuIOOB6xN1LB2DuKDJWfM/EfhmLpwLIM
lcO4dOyY0uNYL+B3/jaXl6VltXvzC87pOqOKygytcx7FOxNVPKyKOCSrEZY0506VhvHmXZH1GDJ
7HHBjQNeRAjaHwkO0QSRHAf0gUs2LIMJjl8ZYXjRYxFftX1Lw1UuifLxfrHqmomI5gTUFgXcKEyV
7AREvtL51A70bIZ4hy3TK2n7gjlf7rqIMRj28G3QprpYGFR0EHgME+rsAKuL2jSaIOA70aHwsjp7
oW4Fs8h7WY4/HIuysXU3AueLsqeuQArEuGQOd5+uBVNUiPI3+rYvrXvekm2fn1E0qlLmCFIpOpnH
dUrBD9OAMIVjkE/+7u2CdYYXghZN2zZq7jpfktpFuSg+36/NjdqpsqyFiiSaEGZcBwno2KRp/Lxt
szYruM3t/OMvwRpjagigz61OcV+bS7LAVnGqSld9FUbpbpmYL2vJgz1P06Qc0j0I5TwuTfCbyNP
z4pXlG2ju346rXRw7k6TH7iBmrzQVf2nyyIU8w+qLW3INQd/WYRm07EPD6DbzcbfVUHI0r6H/aH
I5wsh5QB7QKAM1Ri6fMMLmjIbUWI68SaIRSp+yEQKgbjZOlbjr/4EBnkveZYW/CYLSe57HOwaTqTn
3gTtrdeLDN7pxTWhxZzKmAECAwEAAaOCAf4wggH6MEwGCCsGAQUFBwEBBEAwPjA8BggrBgEFBQcw
AYYwaHR0cDovL29jc3Aucm9vdCSjYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9vY3NwMB0GA1Ud
DgQWBBRqxuWzerwGdO/nkKaW2HDDt5qDpDA5BgNVHRMBAf8ECDAGAOH/AgEAMB8GA1UdIwQYMBaA
FDZbSRCplLktoGstc+S2S3tzlbA8MIHsBgNVHSAEgeQwgeEwVQYLYIRsAQEBAgQAAQkwRjBEBggr
BgEFBQcCARY4aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz
L2NwLmh0bWwwVQYKYIRsAQEBAgQABzBHMEUGCCsGAQUFBwIBFjlodHRwczovL3BraS5jYXJ0YW9k
ZWNpZGFkYW8ucHQvcHVibGljby9wb2xpdGlJYXMvY3BzLmh0bWwwMQYEVR0gADApMCcGCCsGAQUF
BwIBFhtodHRwczovL3d3dy5zY2VLmdvdl5wdC9yZXAwVwYDVR0fBFAwTjBMoEagSIZGaHR0cDov
L3BraS5jYXJ0YW9kZWNpZGFkYW8ucHQvcHVibGljby9scmMvY2NfZWNfY2lkYWRhb19jcmwwMDZf
Y3JsLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAHdC7aTZPmWiHHM3SAEJ
z4ntUt8tB9/xiKE7DQEGfq2k/SnOgmHlOm21K4Nnv8NE0APY+kaKSk5XLQbulISiLMXW5Cdevac/
yEygIHPZfozgbNQZq6Dp7ETXcpdKKaLjmwPDtWznjEiCIBiQjKVYSepC8ctVi619BFLa4Vd8XdB+Q
5scWpoUc89BTpxrjCxEpynA9bRnhAIZku5xEhOQny8fqsdLLhTH5rg+2OMKscXXx5skHw60yNj0N
liwQ3b6C88am0w1CDxOgJj7CpFKlpVrZptFjJN3dP5C6Gowo++BS96aVtwVGWU9s5YOGdFldXEV3
KwHY8ZIrJq4i81ifXPcltLzW19FQHNma/Pnhwc4yMGlo39DHJuQ4rHN17WL6F6fRc5ordVYI9gLD
Xb1YnCOY9IzKPOFooVu4ceiToGrjL675JXfVhIlHGnYqbIr5TAD7594QkZkKyipARgE4ViE5BX
GFe+QtOO75OEqxlhWICZKf6OTmVMdg2X6E64TMg63Qcalch963hTTuYk7f0Hyq+S+8G/Vgp/mS3
e+dWGRK7CBhf/1+8BB3aEHtEzmWJ3ddMLzzjHexEV0uTlkSdoNbCnpe9tueVemmCirqoKiBr8Z12
VTEKxrTv3lRiL3dWPnDkjEfShjdorfxYNQkZuqjtV6Tdyw3TIV6TN53R

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 006*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00003*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*
Valid from:	*Thu Feb 06 17:17:23 CET 2020*
Valid to:	*Fri Feb 06 17:17:23 CET 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:AE:75:F7:A2:76:0F:D0:81:2E:19:92:F5:8A:8D:DF:86:E2:0E:38:1E:B1:37:52:C1:D8:3B:8A:0C:95:9F:33:F1:1F:86:62:E9:C0:B2:0C:95:C3:B8:74:EC:98:D2:E3:58:2F:E0:77:FC:96:97:97:A5:49:96:D5:EF:CC:2F:3B:A5:0A:8E:2B:28:32:B5:CC:7B:14:EC:4D:54:F2:B2:28:ED:92:AC:46:58:D3:9D:3A:56:18:C7:99:76:47:D4:60:C9:EC:71:C1:8D:03:5E:44:08:DA:1F:09:0E:D1:04:91:1C:07:F4:81:4B:36:2C:83:23:26:2F:19:63:18:D1:63:11:5F:B5:7D:48:C3:55:2E:89:F2:F1:7E:B1:EA:9A:89:A5:E6:04:D4:16:05:DC:28:4C:95:EC:04:44:BE:D2:F9:D4:0E:F4:6E:56:78:87:2D:D3:2B:69:FB:80:92:1F:EE:BA:A5:31:12:76:F4:6D:D0:A6:BA:58:18:54:50:10:78:0C:13:EA:EC:00:AB:8B:DA:34:9A:20:E0:3B:41:A1:F0:B2:3A:7B:A1:6E:05:B3:C8:7B:59:8E:3F:1C:8B:B2:B3:15:37:02:E7:8B:B2:A7:AE:40:0A:C4:B8:64:0E:77:9F:AE:05:53:54:88:F2:77:FA:B6:2F:AD:7B:DE:92:6D:9F:9F:51:34:AA:52:E6:08:52:29:42:99:C7:75:4A:C1:0F:D3:B0:32:55:63:90:4F:FE:EE:ED:82:75:86:17:82:16:4D:DB:36:6A:EE:3A:5F:92:DA:45:B9:28:3E:DF:AF:CD:8D:DA:A9:B2:AC:85:8A:24:9A:10:66:5C:07:09:E8:D8:A4:69:FC:BC:6D:B3:36:2B:8B:CD:ED:FC:93:8C:BF:04:69:8D:AB:22:83:3E:B5:39:C5:7E:6D:24:CB:01:59:C6:A9:22:1D:F4:55:1B:A5:BA:66:60:BD:AF:26:AC:F5:3F:4E:90:73:48:F4:97:94:F0:B9:37:C2:6F:23:4F:CF:8A:57:94:6D:A3:BB:7E:39:EA:B5:D1:C3:B9:3A:4C:7E:C8:06:6A:F3:41:57:F6:9F:2C:B8:53:CC:3E:A8:B5:B7:20:D4:1D:FD:66:11:9B:4E:C4:3C:3E:83:6F:37:1B:7D:55:07:23:4A:FA:1F:F6:87:97:9C:2C:87:94:01:ED:02:80:33:54:65:E8:53:0C:2E:68:C8:B5:45:A5:EB:C4:9A:21:14:A9:FB:21:10:2A:06:C9:65:09:5B:26:BE:04:06:79:2F:79:96:16:FC:26:0B:49:E4:BB:1C:EC:1A:4E:A4:E7:DE:04:ED:AD:D7:8B:0C:DE:E9:C5:35:A1:C5:9C:CA:98:01:02:03:01:00:01*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Subject Key Identifier	*6A:C6:E5:B3:7A:BC:06:74:EF:E7:90:A6:96:D8:70:C3:B7:9A:83:A4*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*36:5B:49:10:A9:94:B9:2D:A0:6B:2D:73:E4:B3:4B:7B:73:21:B0:3C*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.9* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl006_crl.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C9:FF:C6:F3:15:7F:55:9C:7B:59:72:27:03:62:AF:A9:94:85:CC:D1:29:3C:0A:B1:58:EA:ED:AF:0D:B9:AF:67*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00003*
Subject OU:	*subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

X509SKI

X509 SK I *asbls3q8BnTv55Cmlthww7eag6Q=*

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

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

Status Starting Time *2020-03-18T12:00:00Z*

9.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

9.3.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *CN=EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00003, OU=subECEstado, OU=Cartão de Cidadão, O=AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P., C=PT*

Service digital identities

X509SubjectName

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00003*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

X509SKI

X509 SK I *asbls3q8BnTv55Cmlthww7eag6Q=*

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

Status Starting Time *2020-03-16T00:00:00Z*

9.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

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

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

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

Criteria list assert=all

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

9.4 - Service (granted): Chave Móvel Digital 00004

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]* *Chave Móvel Digital 00004*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *150116946838775167975445535883915522737*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH+TCCBeGgAwIBAgIQcO946SfwVbhtLNkftrVysTANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UE
BhMCUFQxQDA+BgNVBAoMN1NDRUUgLSBTaXN0ZW1hIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOz
bmljYSBkbyBFc3RhZG8xETAPBgNVBAsMCEVDRXN0YWRvMSAwHgYDVQQDDBdDYXJl0w6NvIGRlIENp
ZGFkw6NvIDAwNjAeFw0yMTExMTgxNTQxMTFaFw0zMzExMTgxNTQxMTFaMHtpMQswCQYDVQQGEwJQ
VDFCMEAGA1UECgw5QU1BIC0gQUFiDik5DSUEgUEFSQSBBIE1PREVSTkIaQcOHw4NPIEFETlIOSVNU
UkFUSVZBIEkuIFAuMRwwGgYDVQQLDBNDYXJ0w6NvIGRlIENpZGFkw6NvMRQwEgYDVQQLDAtzdWJF
Q0VzdGFkbzFiMGAGA1UEAwxZRUMgZGUgQ2hhdmUgTcOzdmVsIERpZ2lOYWwgZGUgQXNzaW5hdHVy
YSBEaWdpdGFsIFI1YWxpZmlj YWRhIGRvIENhcnTDo28gZGUgQ2lkYWTDo28gMDAwNDQwggIiMA0G
CSqGSib3DQEBAQUAA4ICDwAwggIKAoICAQDueKCfikKE+RNTG8uYvl6G9Eebe08PFqLYOakKbtS0
Drps0ziPgN1EZnjvLS63Xgd+TBpxtW5vhcY9SkisK5zAZKAUjMDYiupDtqmJnkSayyBMLTXzwpOF
4fzY3ti0HxoPp+MNKVjrnx7twrKtSzAM4PNtdU+Nhi/obGBYAOL5Ygo25IFHhO5d1I5k90Dkzv+LU
eDtKKDbHyEdptLjjDVf6U1fdhmKvGrOPb/4NFfhPqOXMmPNfNp966e/Futhbij30LD5scaBbDJXE
0pq0OfqfRIUn7IGs+MMQs28/1g5OZj++g9ip3+dwznhgCc2S4d5IXWw59uoAzksNLEfLxCD4OO9o
YWZ3Yc+ZujK0r7MIBsIPiY6cW6XsAMoI5bHJZVxvIEp+3dUchv1sVQwJ1uYTMLWNp6M0co7TX+bp
h9TOKj1IisV15PLhfGIWPMGDvInwO7UdLXQVPIXMjUE33Tp T0/r4y0wdyLvfAB126zN6LJX8u7NN
DL2g3g0G68SfELku9cVhxtrN5EaVS1uRIRqRAPoFRAM+5HmjqLF/vlt1pXYsvTtNxcwWjUFg16F0
kkTOqIBAwnlvWUUF8mBHlz06yFUmmGHP1sPeQkUS(0RK6lzfU86IZ9IOIDPuMK+wlgQH9RRPKPH
9c075Tp7crbtNfiA6INvdHH5Y5PMcsKW6wIDAQABo4IB/jCCAfowEgYDVR0TAQH/BAgwBgEB/wIB
ADAfBgNVHSMEGDAWgBQ2W0kQqZS5LaBrLXPks0t7cyGwPDBMBggrBgEFBQcBAQRAMD4wPAYIKwYB
BQUHMAGGMGh0dHA6Ly9vY3NwLnJvb3QuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDCB
7AYDVR0gBIHkMIHhMFUGCCZEbAEBAQIEAAEJMEYwRAYIKwYBBQUHAgEWOGh0dHBzOi8vcGtpLmNh
cnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL3BvbGl0aWNhcy9jcC5odG1sMDEGBFUdIAAwKTAnBggr
BgEFBQcCARYbaHR0cHM6Ly93d3cuc2NlZS5nb3YucHQvcmVwMFUGCmCEbAEBAQIEAAcwRzBFBggr
BgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz
L2Nwcy5odG1sMFcGA1UdHwRQME4wTKBKoEiGRmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJjL2NjX2VjX2NpZGFkYW9fY3JsMDA2X2NybC5jcmwwHQYDVR0OBBYEFKEDpYKG
w+F+MvelBI5SaNENnCSsMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAozZsHfov
OQrtSrwZ+MTivEExhV9gvlBDYHJNGVNKNWpV4IPwud0vjYQ5iiF2Xye9oNnudMX7NQQ0182Y0aas
8Ber04xXU2DGh/tmqX3BPqUmrDspVG/PTygbfIe3ldqxxHfVr6y2jJL3EYzDWRt2TvBgYPNYZNo9
pDccu1mpolimzjYtO5LPsvC/dJexymD65da0It7tO0a9r3NousDlku4dUd3JftnjRRQP8K7t7Qlua
xQ5rksFakYRmW2FLfU+7M+IOPdILp8lHzva27cZJxTp/bQYwCva45js85OglgyNQVt+tGZ0L1QgV
XkK55a9IGz+uGZuVSEOD3hd2filyNYoBQBdPhr38E4Fzp8tbdsKFA/qgz0hIK9dIUnPYfKL5IxBy
Twws4NmbNWbPz47wb6MDKdMTVZcONnPFpKhvmypOzDDk0cbjQY78qSjBXx31g7wZ4+GH9uUBO+
gB1EuXf/f2S2bvmqYlvpAEe+MH9trKM3edjgq0/wmMhgwlN/vFWNZJ/ttqIfrDmhefBZR6CzF7h
Ot6wFh1Ce6S7aBXEimjaZQAg62QYIKrbNsa3v3SMzE6hYFCSF9UBVo62IlICug28WeCyLXfjFqZS
rrQX9/YVnZKtqtysN+vJlFESkEw8eZFy/YvV++85QMjzSiwshbul5ybDMoHsSm26hak=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 006*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00004*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

Valid from: *Thu Nov 18 16:41:11 CET 2021*

Valid to: *Fri Nov 18 16:41:11 CET 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:EE:78:A0:9F:22:42:84:F9:13:53:1B:CB:98:BE:5E:86:F4:47:9B:7B:4F:0F:16:A
2:D8:39:A9:24:6E:D4:B4:0E:BA:6C:D3:38:8F:80:DD:44:66:78:EF:2D:2E:B7:5E:07:7E:4C:1A:71:B5:6E:6F:85:C6:3D:4A:48:AC:2B:9C:C0:64:A0:14:8C:C0:D8:8A:EA:43:B6:A9:89:9E:44:9
A:CB:20:4C:2D:35:F3:C2:93:85:E1:FC:D8:DE:D8:B4:1F:1A:0F:A7:E3:0D:29:58:E6:C7:BB:70:AC:AB:52:CC:03:38:3C:DB:5D:53:E3:61:BB:FA:1B:18:16:00:38:BE:58:AA:8D:B9:20:51:E1:3
B:97:75:97:99:3D:D0:39:33:BF:E2:D4:78:3B:57:28:36:C7:C8:47:69:B4:B2:63:0D:58:7A:53:57:DD:86:62:AF:1A:B3:8F:6F:FE:0D:15:F8:4F:A8:E5:CC:98:F3:5F:36:9F:7A:E9:EF:C5:BA:D8:
5B:8A:3D:F4:2C:3E:6C:09:A0:5B:0E:35:C4:D2:98:34:39:FA:9F:46:55:27:EC:91:AC:F8:C3:10:B3:6F:3F:D6:0E:4E:64:9F:BE:B3:D8:A9:DF:E7:70:CE:78:60:09:CD:92:E1:DE:65:5D:6C:39:F
6:EA:00:CE:4B:0D:2C:47:CB:C4:20:F8:D0:EF:68:61:66:77:61:CF:99:B8:92:B4:AF:B3:08:06:C9:4F:89:8E:9C:5B:A5:EC:00:CA:08:E5:B1:C9:65:5C:6F:20:4A:7E:DD:D5:1C:86:FD:6C:55:0C
:09:D6:E6:13:30:B5:8D:A7:A3:34:72:8E:D3:5F:E6:E9:87:D4:CE:2A:3D:48:96:C5:75:E4:F2:E1:7C:62:16:3C:C1:83:BC:89:F0:3B:B5:1D:2D:74:15:3C:85:CC:26:E1:37:DD:3A:53:D3:FA:F8:
CB:4C:1D:C8:BB:DF:00:1D:76:EB:33:7A:2C:95:FC:BB:B3:4D:0C:BD:A0:DE:0D:06:EB:C4:9F:10:B9:2E:F5:C5:61:C6:DA:CD:E4:46:95:4B:5B:91:21:1A:91:00:FA:05:44:03:3E:48:79:A3:AB:
B1:7F:BC:BB:75:A5:76:2C:BD:3B:4D:C5:CC:16:25:41:60:D7:A1:74:92:44:CE:82:2F:00:C2:79:6F:59:48:BF:17:C9:81:1E:5C:F4:EB:21:54:9A:61:87:3F:5B:0F:79:09:14:48:9D:11:2B:A9:73
:7D:4F:3A:95:9F:49:0C:80:CF:B8:C2:BE:C2:58:10:1F:D4:51:3C:A3:C7:F5:CD:3B:E5:3A:7B:72:B6:ED:35:F8:80:E8:83:6F:74:71:F9:63:93:CC:72:C2:96:EB:02:03:01:00:01
```


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

Authority Key Identifier *36:5B:49:10:A9:94:B9:2D:A0:6B:2D:73:E4:B3:4B:7B:73:21:B0:3C*

Authority Info Access *http://ocsp.root.cartaodecidadao.pt/publico/ocsp*

Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.9* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl006_crl.crl*
Subject Key Identifier	*A1:03:A5:82:86:C3:E1:7E:32:F7:88:F0:8E:52:68:D1:0D:9C:24:AC*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*59:43:43:32:11:12:0C:59:CA:BA:00:9A:34:44:BE:E0:84:98:70:8A:34:5A:73:1E:AE:FB:5F:46:B7:0D:19:8F*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00004*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*

X509SKI

X509 SK I	*oQOlgobD4X4y94jwjlJo0Q2cJKw=*

Service Status

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

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

Status Starting Time

2021-12-06T11:43:31Z

9.4.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.4.2 - Extension (not critical): Qualifiers [QCStatement, QCQSCDManagedOnBehalf, 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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

9.4.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00004*

Service digital identities

X509SubjectName

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00004*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

X509SKI

X509 SK I *oQOlgobD4X4y94jwjlJo0Q2cJKw=*

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

Status Starting Time *2021-12-06T11:29:20Z*

9.4.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.5 - Service (granted): Chave Móvel Digital 00005

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]* *Chave Móvel Digital 00005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *160558550848698927986948208694566905179*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH+TCCBeGgAwIBAgIQeMpzvDc1OlCeZy73gyDIWzANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UE
BhMCUFQxQDA+BgNVBAoMN1NDRUUgLS8TaXN0ZW1hIGRlIENlcnRpZmlYcOnw6NvIEVsZWNOcsOz
bmljYSBkbyBFc3RhZG8xETAPBgNVBAsMCEVDRXN0YWRvMSAwHgYDVQQDDBdDYXl0w6NvIGRlIENp
ZGFkw6NvIDAwNzAeFw0yMzA1MzAxNTIzMDlaFw0zNTA1MzAxNTIzMDlaMIHpMQswCQYDVQQGEwJQ
VDFCMEAGA1UECgw5QU1BIC0gQUfDik5DSUEgUEFSQSBBIE1PREVSTklaQcOHw4NPIEFETUlOSVNU
UkFUSVZBIEkuIFAuMRwwGgYDVQQLDBNDYXl0w6NvIGRlIENpZGFkw6NvMRQwEgYDVQQLDAtzdWJF
QDVzdGFkbzFiMGAGA1UEAwxZRUlMgZGUgQ2NhdmUgTcOzdmVsIERpZ2l0YWwgZGUgQXNzaW5hdHVy
YSBEaWdpdGFsIFF1YWxpZmljYWRhIGRvIENhcnTDo28gZGUgQ2lkYWTDo28gMDAwMDUwggIiMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDB8pKk/PmR932byVCkorjaeY3m8ckmHCadtO3S0ZuS
sx9BmjAFvGCamUnPtsI+m/OTrt8oIFmAbRWDsnp1WvmpI4OAVpeuJu/gnwnUTDv06wNMsyPrIizr
ryINk0QOg9ej/nWID/xPK7gxoTNmj4CiFRzhujogHHtqGJjlyczbO7QE9wtcHGGHejyNk27kT3MLG
N5Loeh4JfD6xzxdaNMpIBDxA75s4VaxV2x5lcXGE+JqzBzmhBTpKkyaQAAccDCAB8xbMVOYTlodc
YwRNji7w Y3yRECgbpdI5lqHhGffxgjLEUs3OeH1CuhykdRrKXX4DtwULD0oz3Ujs/HEF3i0fxKWR
xPlSCizupTHbNzyo9VTAjlWDaEeqZmWygFfG8+E5BEEoPcLZ7wkQAe2TWhXTqzC5RwDt0r45eNLU
iYvjzZeKudHv1A9ZfaL4P5VPXVGMsR9iUqxPTRphaUcxtiew1IU3TT3Qg8kMizym6Ph0Ik259E48
tGLAkuK9cRwsBeo7V8bqQKtp67hFSUW/F1SeZyNyg+fVq7YdwEQPhB3dA82O4gGnMyOOOTr6N1ID
YkGsNRaTQEq9RL6D9DBGT2yBGkvWSCppKmwQ5R/xkWJoieWM6j8uu1qXLt76HKahAbYMDUw//YTj
gQJPCXj2xz7nkN/sW6FCrd/2RE7u5zd31wIDAQABo4IB/jCCAfowEgYDVR0TAQH/BAgwBgEB/wIB
ADAfBgNVHSMEGDAWgBQUnBJGPKkdgfhXhCdlyxMcSPFIzzBMBggrBgEFBQcBAQRAMD4wPAYIKwYB
BQUHMAGGMGh0dHA6Ly9vY3NwLnJvb3QuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDCB
7AYDVR0gBIHkMIHhMFUGC2CEbAEBAQIEAAEJMEYwRAYIKwYBBQUHAgEWOGh0dHBzOi8vcGtpLmNh
cnRhb2RlY2lkYWRhby5wdC9wdWjsaWNvL3BvbGl0aWNhcy9jcC5odG1sMDEGBFUdIAAwKTAnBggr
BgEFBQcCARYbaHR0cHM6Ly93d3cuc2NlZS5nb3YucHQvcmVwMFUGCmCEbAEBAQIEAAcwRzBFBggr
BgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz
L2Nwcy5odG1sMFcGA1UdHwRQME4wTKBKoEiGRmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJjL2NjX2VjX2NpZGFkYW9fY3JsMDA3X2NybC5jcmwwHQYDVR0OBBYEFLn24cQF
quvZtoLiWfRUcvPTKcxHRMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEATOloDLAw
UQUSOvz1pQrHQE3XkI0BytcCWbG+MSjrFxK/7Uk3R6CMaiOmnf0oLOr4Yp8E9+ifmcB1GG++mEw+
jfSxmif8bmVyarspXyYxhplFRY1sU1mTO4eBol4N/kpVWLsAfG3N/ZE4xrPLgCvpf/Ep52VFzJ0X
LMYLigiyiPq0kzNuZdo7UQlZHbB/boQnnTtQpxbWdzSu/xHVe//QRtZAx/mzOlH5mjObuM6x9bYq
o0BDzdLdcQ7AJl/im51s5JTzfZHoS52GjAlZfxcQErtAfjxu58ebZTKyHrBUsll7OppWYksEzhV2W
02S+TO7/65i3OKabHttqnQb+9cYVYp/GRBGhpLQDsERktGorS2XnzBFhOAE/PXANcGZ3mYXeMDhcR
/1Sc0AgYH6OhfOtcgAkdcTsiMUCl+dxfEd3J/yEqmUOdDH9ecamiGgVO6u/XlXYuxsmyZOgM0Cay
StibrwF55vqax6GOrWBBmKFs5jUtxNI0+g6CzlzBGUN/DjABkK/bta7Iw37JQQZxJMgINvetdCoT
NKqF7q0ujpQ5sna9gLeSjNLLukf9e1BiKMaA2Y0ielAQKf4QBf1adHx3IFzvX7+x2AZo2JP3Arrp
AUXXY5ncLe7WqX3Dy5ra05YmgYB8/QH3G2nc5d3BegOlr+NVj4T1xaHM4oaqGEq+q38=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 007*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00005*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

Valid from:	*Tue May 30 17:23:09 CEST 2023*
Valid to:	*Wed May 30 17:23:09 CEST 2035*
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:C1:F2:92:A4:FC:F9:91:F7:7D:9B:C9:50:A4:A2:B8:DA:79:8D:E6:F1:C9:26:1C:26:9D:84:ED:D2:D1:9B:92:B3:1F:41:9A:30:05:BC:60:9A:99:49:CF:B6:C2:3E:9B:F4:13:AE:DF:28:20:59:80:6D:15:83:B2:7A:75:5A:F9:A9:97:8D:00:56:97:AE:26:EF:ED:9F:09:D4:4C:3B:F4:EB:03:4C:B3:23:EB:22:2C:EB:AE:F2:4D:93:44:0E:AB:D7:89:FE:75:88:0F:FC:4F:2B:B8:31:A1:33:66:8F:80:A2:15:1C:E1:BA:3A:20:1C:7B:6A:18:92:72:73:36:F4:ED:01:3D:C2:D7:07:18:61:DE:27:23:64:DB:B9:13:DC:C2:C6:37:92:E8:7A:1E:09:7C:3E:B1:CF:17:5A:34:CA:48:04:3C:40:EF:9B:00:55:AC:55:DB:1E:65:71:71:84:F8:9A:B3:07:39:A1:05:3A:4A:93:26:90:00:07:1C:0C:20:01:F3:16:CC:54:E6:13:96:87:5C:63:04:4D:8E:2E:F0:63:7C:91:10:28:1B:A5:D2:39:96:A1:E1:19:F7:F1:82:32:C4:52:CD:CE:78:7D:42:BA:1C:A4:75:1A:CA:5D:7E:03:B7:05:0B:0F:4A:33:DD:42:6C:FC:71:05:DE:2D:1F:C4:A5:91:C4:F2:12:0A:2C:EE:A5:31:D8:37:3C:A8:F5:54:C0:8C:95:83:68:47:AA:66:65:82:80:57:C6:F3:E1:39:04:41:28:3D:C2:D9:EF:09:10:01:ED:93:5A:15:D3:AB:30:B9:47:00:ED:D2:BE:39:78:D2:D4:89:8B:C9:CD:97:8A:B9:D1:EF:D4:0F:59:7D:A2:F8:3F:95:4F:5D:51:8C:B1:1F:62:52:AC:4F:4D:1A:61:69:47:31:B6:27:B0:D6:55:37:4D:3D:D0:83:C9:0C:8B:3C:A7:E8:F8:74:22:4D:B9:F4:4E:3C:B4:62:C0:92:E2:BD:71:1C:2C:05:EA:3B:57:C6:EA:40:AB:69:EB:B8:45:49:45:BF:17:54:9E:67:23:72:83:E7:D5:AB:B6:1D:C0:44:0F:84:1D:DD:03:CD:8E:E2:01:A7:33:24:0E:39:3A:FA:37:59:43:62:41:AC:35:16:93:40:4A:BD:44:BE:83:F4:30:46:4F:6C:81:1A:4B:D6:48:2A:69:2A:6C:10:49:1F:F1:91:62:68:89:E5:8C:EA:3F:2E:BB:5A:97:2E:DE:FA:1C:A6:A1:01:B6:0C:0D:4C:3F:FD:84:C9:81:02:4F:09:78:F6:C7:3E:E7:90:DF:EC:5B:A1:42:AD:DF:F6:44:4E:EE:E7:37:77:D7:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*14:9C:12:46:3C:A9:1D:81:F8:57:84:27:65:CB:13:1C:48:F1:65:CF*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.9* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl007_crl.crl*
Subject Key Identifier	*B9:F6:E1:C4:05:AA:EB:D9:B6:82:E2:59:F4:54:72:F3:D3:2B:11:D1*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*04:E1:5A:53:99:3E:63:2F:BF:A4:EF:F8:F2:DE:AF:A9:18:13:77:54:CB:99:DE:76:DB:0C:B8:CF:E7:38:F4:04*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00005*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*

X509SKI

X509 SK I	*ufbhxAWq69m2guJZ9FRy89MrEdE=*

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

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

Status Starting Time *2023-09-12T10:00:56Z*

9.5.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.5.2 - Extension (not critical): Qualifiers [QCStatement, QCQSCDManagedOnBehalf, 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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

9.6 - Service (granted): ECCE-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.*

Service Name

Name *[en]* *ECCE-TSA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *90313582736903220885852895936510726947*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFOzCCBCOgAwIBAgIQQ/HDahr6JuNnt7AoQ0yTlzANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE
BhMCUFQxOTA/BgNVBAoMOEFNQSAtIEFHw4pOQ0lBlFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1J
TklTVFJBVElWQSBjLlAuMQ0wCwYDVQQLDARTQ0VFMREwDwYDVQQLDAhFQ0VzdGFkbzERMA8GA1UE
AwwIRUNDRVEwMDIwHhcNMjUwMjIwMjI0MzUyWhcNMzAwMjIwMjI0MzUyWjCBtjELMAkGA1UEBhMC
UFQxOTA/BgNVBAoMOEFNQSAtEFHw4pOQ0lBlFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1JTkIT
VFJBVElWQSBjLlAuMQ0wCwYDVQQLDARTQ0VFMREwDwYDVQQLDAhFQ0VzdGFkbzEvMCDGA1UECwwm
RW50aWRhZGUgQ2VydGlmaWNhZG9yYSBDb211bSBkbyBFc3RhZG8xETAPBgNVBAMMCEVDQ0UtVFNB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAh37wo1HGnxFe6X2teuzwPT5LEm4ebA3/
GQ8pFTOM4Wd/OK4ZoiTNRhs9nXCwOcXdXHjFNta2HIPKdUDWwLP+NrDI6aKTTjNe1QCFg1SKb0T7
MU5x9OEw8ZheU4b8pAPDPorkUcNzTxhkwg8Nk2BvMMZu0vooqo25qtQpz2KFFOyyBGy47CRiD1Y9
x2s8ESfo2M/1hjv5q2f0SR3hPSczq6VOQ4I3r+CQdE1jA+XdVmjqIUokpEZSzvbxGE+yVlZhxIDL
hbAy92eCFHAC7tiS7YaIP/IKxgIHHs4nzpc0JInvtnNZmPhLwdLIKxcAhMKHY7olwt9oPXD6Lbd6
vt9OUQIDAQABo4IBcjCCAW4wGAYIKwYBBQUHAQMEDDAKMAgGBgQAjkYBATAOBgNVHQ8BAf8EBAMC
BsAwFgYDVR0IAQH/BAwwCgYIKwYBBQUHAwgwHQYDVR0OBBYEFjs4S89Ar/iMWS5DBPGX+Xg2Mu4j
MB8GA1UdIwQYMBaAFC4HERAYTGit0nltWgPUt9TsLNeCMDsGA1UdIAQ0MDIwMAYEVR0gADAoMCYG
CCsGAQUFBwIBFhpodHRwOi8vd3d3LmVjY2UuZ292LnB0L2RwYzBmBggrBgEFBQcBAQRaMFgwIwYI
KwYBBQUHMAGGF2h0dHA6Ly9vY3NwLmVjY2UuZ292LnB0MDEGCCsGAQUFBzAChiVodHRwOi8vdHJ1
c3QuZWNjZS5nb3YucHQvZWNjZXEwMDIuY3J0MAkGA1UdEwQCMAAwOgYDVR0fBDMwMTAvoC2gK4Yp
aHR0cDovL2NybHMuZWNjZS5nb3YucHQvY3Jscy9lY2NlcTAwMi5jcmwwdQYJKoZIhvcNAQELBQAD
ggEBAJ4EgiuM78CGjbD22HTmsx/RQWC5peKDAWpTM8o133xL21EQ0ntys0d2TFh4osRm/Mfnh7/0
O6omFvw/ghEO0DjSsnfiPKiL9RRV6YHlvAshEr7szbokvTogUfdzukhNRNg+4oKORxt4uZadxSkl
H3TbNGhdRZNC7ItJMjxQDgGoixP/egW83dqJ/tnUYZtYSywXt/MRD9xiWE4MoQmNF0m22fHuQLau
8rjOIEtSjIA3g2C6scN1pXH33oZfNp6Uj3iwE5XxGx9G+K9OkYWEcaC51kOP7KyOt6oyN4gbc4k
4wXvgTlNEaSuA2frALO8DXHTijM1kjuXYI2oux4s+g=

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ECCEQ002*
Issuer OU:	*ECEstado*
Issuer OU:	*SCEE*
Issuer O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*
Issuer C:	*PT*
Subject CN:	*ECCE-TSA*
Subject OU:	*Entidade Certificadora Comum do Estado*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*
Subject C:	*PT*
Valid from:	*Thu Feb 20 23:43:52 CET 2025*
Valid to:	*Wed Feb 20 23:43:52 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:02:82:01:01:00:87:7E:F0:A3:51:C6:9F:11:5E:E9:7D:AD:7A:EC:F0:3D:3E:4B:12:6E:1E:6C:0D:FF:19:0F:29:15:33:8C:E1:67:7F:38:AE:19:A2:24:CD:46:1B:3D:9D:70:B0:39:C5:DD:5C:78:C5:36:D6:B6:1C:83:CA:75:40:D6:C0:B3:FE:36:B0:E5:E9:A2:93:4E:33:5E:D5:00:85:83:54:8A:6F:44:FB:31:44:B1:F4:E1:30:F3:68:5E:BB:86:FC:A4:03:C3:3E:8A:E4:51:C3:73:4F:18:64:C2:0F:0D:93:60:6F:30:C6:6F:D2:FA:28:AA:8D:92:AA:D4:29:CF:62:85:3C:EC:B2:04:6C:B8:EC:24:62:0F:56:3D:C7:6B:3C:11:27:E8:D8:CF:F5:86:3B:F9:AB:67:F4:49:1D:E1:3D:27:33:83:A5:4E:3B:89:77:AF:E0:8E:74:4D:63:03:E5:DD:56:68:EA:21:4A:24:A4:46:79:CE:F6:F1:18:4F:B2:56:56:61:C4:80:CB:85:B0:32:F7:67:82:14:70:02:EE:D8:92:ED:86:88:3F:F2:0A:C6:09:47:1E:CE:27:CE:97:34:24:89:EF:B6:73:59:98:F8:4B:C1:D2:C8:2B:17:00:84:C2:87:63:BA:25:C2:DF:68:3D:70:FA:2D:B7:7A:BE:DF:4E:51:02:03:01:00:01*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*9B:38:4B:CF:40:AF:F8:8C:59:2E:43:04:F1:97:F9:78:36:32:EE:23*
Authority Key Identifier	*2E:07:11:10:18:4C:68:AD:D2:79:6D:5A:03:D4:B7:D4:EC:2C:D7:82*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecceq002.crt*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/ecceq002.crl*
Key Usage:	*digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *10:46:0E:2D:49:96:C0:43:9E:C0:AC:15:56:58:EE:88:20:5C:20:27:8D:A0:A7:47:2B:FD:BE:1A:6C:39:D4:86*

X509SubjectName

Subject CN: *ECCE-TSA*

Subject OU: *Entidade Certificadora Comum do Estado*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*

Subject C: *PT*

X509SKI

X509 SK I *mzhLz0Cv+IxZLkME8Zf5eDYy7iM=*

Service Status

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

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

Status Starting Time

2025-03-01T00:00:00Z

9.7 - Service (granted): ECCEQ002

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]* *ECCEQ002*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *85276328393010455966344034778770832980*

X509 Certificate	-----BEGIN CERTIFICATE----- MIIF4TCCA8mgAwIBAgIQQCefmcKziPxntzBpvrv+VDANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UE BhMCUFQxOTA/BgNVBAoMOEFNQSAtIEFHw4pOQ0lBIFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1J TklTVFJBVEIWQSBjLIAuMQ0wCwYDVQQLDARTQ0VFMREwDwYDVQQLDAhFQVzdGFkbzERMA8GA1UE AwwIRUNDRSAwMDQwHhcNMjUwMjIwMTMzODQ5WhcNMzEwMjIwMTMzODQ5WjCBhTELMAkGA1UEBhMC UFQxOTA/BgNVBAoMOEFNQSAtIEFHw4pOQ0lBIFBBUkEgQSBNT0RFUk5JWkHDh8ODTyBBRE1JTkIT VFJBVEIWQSBjLIAuMQ0wCwYDVQQLDARTQ0VFMREwDwYDVQQLDAhFQVzdGFkbzERMA8GA1UEAwwI RUNDRVEwMDIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2Grn+URhHlpJdq13isSPq TbEQ7gYB0hTq+xjt4ZZpY9KL2xUegUwSjDCeNBWIsgOi+T1j8Ez4sK585RZAgJasllt0daGsC8oj KOdw89E3QNt7H8hRH80GfrFSNubmeivqsBqc6S/wPqn0uTynctkVacHmG474Kpe2b5DIGdEp9mAD ejLjmtT9UDvH1YNMp7SettETp+T3O5g81OuGT537bn2yc9ItofRvxYUS2aesw3SNT3PgGo9esRqE KdnnMZvGskmZI1Rd9rqVqZ1OCtIFzx6QRNlSOK8CzqxtfRka9MnUVq1L/OffgY4D5Q2gplBCfiy whGDp8MsctN4QUEvAgMBAAGjggFjMIIBRTASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQWBBQu BxEQGExordJ5bVoD1LfU7CzXgJAfBgNVHSMEGDAWgBRK6ad2WCWq5O8Tq0UW1AtSnlPYJjAOBgNV HQ8BAf8EBAMCAQYwOwYDVR0gBDQwMjAwBgRVHSAAMCgwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cu c2NlZS5nb3YucHQvcmVwMGYGCCsGAQUFBwEBBFowWD4jBggrBgEFBQcwAYYXaHR0cDovL29jc3Au ZWNjZS5nb3YucHQwMQYIKwYBBQUHMAKGJWh0dHA6Ly90cnVzdC5lY2NILmdvdi5wdC9lY2NILTAw NC5jcnQwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybHMuZWNjZS5nb3YucHQvY3Jscy9FQ0NF LTAwNC5jcmwwDQYJKoZIhvcNAQELBQADggIBAFXgoXQEyLaMDMAzZUGEE48T8om9nL4+vX8joN6C +++te8N8oDbCQ+08Ooc0Cd3oY1Uk9edYskTqBTON7H7z168EsCuQjcc+KYYVxH/3YohYApmlDQ/ Krv0gVdIgFqhtk9/+T22GxxPM0GW07+DQF9Xb1icLkpFEAYOAFxoDfpZ7Hi6u0CkuDsAepcc3XhD LcmjUqbyjgsrDuRrUs6l9mcOcEh/W1UJsGZWD0fIVlGRdCEb9k2Nrjuifg8S99QutXcvQKSjBVas CRa7mixBn9TGZODkPA3Bey5lG5eMzE7aTcY9FT07SuJmKzfnRp2uqYQ+ts1LjHnqj9/FgDR6k5a3 I5Pe0OldLqFepdrgSxQpv5sEifEHDvefmz5zHIt8dlWdrkw2T8akpYao8xroZwD282AYpeEpVxhj stnA9nVmmfG7qqLDyOuJkfXHAiG7ZztQCcvLrTOYNKk24nMJZRlad4brR+hQBWWNkN3oxCoMyrwS N/AwPpCR7iueyGrYKxo7tOpcqBjpGVUAOGzwBXEY+cYKQhd163YdNtvMjYz4LYeECLHSHLahzyg7 BioCPmORnfl8CqGYdmCD4aLrrK5lkmRrMBSyVA2EN5trvjWkIQBOy9vtRNXWyFHI7FwZ26RlzP1E 41xLq9XY697a+AVU83D9vxC6VWH5qKBLqvjP -----END CERTIFICATE-----
Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ECCE 004*
Issuer OU:	*ECEstado*
Issuer OU:	*SCEE*
Issuer O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*
Issuer C:	*PT*
Subject CN:	*ECCEQ002*
Subject OU:	*ECEstado*
Subject OU:	*SCEE*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*
Subject C:	*PT*
Valid from:	*Thu Feb 20 14:38:49 CET 2025*
Valid to:	*Thu Feb 20 14:38:49 CET 2031*
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:B6:1A:B9:FE:51:18:47:96:92:5D:AB:5D:E2:B1:23:EA:4D:B1:10:EE:06:01:D2:14:EA:FB:18:ED:E1:96:69:63:D2:8B:DB:15:1E:81:4C:12:8C:30:9E:34:15:88:B2:03:A2:F9:3D:63:F0:4C:F8:B0:AE:7C:E5:16:40:80:96:AC:22:5B:74:75:A1:AC:0B:CA:23:28:E7:70:F3:D1:37:40:DB:7B:1C:18:51:1C:1D:06:7E:B1:52:36:E6:E6:7A:28:EA:B0:1A:9C:E9:2F:F0:3E:A9:F4:B9:3C:A7:72:D9:15:69:C1:E6:18:8E:F8:2A:97:B6:6F:90:C8:19:D1:29:F6:60:03:7A:32:E3:9A:D4:FD:50:3B:C7:D5:83:4C:A7:B4:9E:B6:D1:13:A7:E4:F7:3B:98:3C:D4:EB:86:4F:9D:FB:6E:7D:B2:73:D8:ED:A1:F4:6F:C5:85:12:D9:A7:AC:C3:74:8D:4F:73:E0:1A:8F:5E:B1:1A:84:29:D9:E6:31:9B:C6:B2:49:99:97:57:D1:77:DA:EA:56:06:75:38:2B:65:17:3C:7A:41:13:65:48:E2:BC:0B:3A:B1:B5:F4:64:6B:D3:27:51:5A:B5:2F:F3:9F:16:06:38:0F:94:36:AA:92:01:09:FF:F2:C2:11:83:A7:C3:2C:72:D3:78:41:41:2F:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*2E:07:11:10:18:4C:68:AD:D2:79:6D:5A:03:D4:B7:D4:EC:2C:D7:82*
Authority Key Identifier	*4A:E9:A7:76:58:25:AA:E4:EF:13:AB:45:16:D4:0B:52:9E:53:D8:26*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.scee.gov.pt/rep*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-004.crt*

CRL Distribution Points *http://crls.ecce.gov.pt/crls/ECCE-004.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D4:00:7A:68:F8:20:6D:72:07:34:5D:00:0C:D5:1D:88:81:C8:58:B4:31:A9:2C:1D:8B:57:BB:3B:71:D4:8A:86*

X509SubjectName

Subject CN: *ECCEQ002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*

Subject C: *PT*

X509SKI

X509 SK I *LgcREBhMaK3SeW1aA9S31Ows14I=*

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

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

Status Starting Time *2025-06-11T11:00:00Z*

9.7.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.7.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.7.3 - Extension (not critical): Qualifiers [QCStatement, QCForESig, QCForESeal, QCWithQSCD]

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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.2*

Description

Policy Identifier:

Identifier [OIDAsURI] *0.4.0.194112.1.3*

Description

Description

9.7.4 - History instance n.1 - Status: granted

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

Service Name

Name [en] *ECCEQ002*

Service digital identities

X509SubjectName

Subject CN: *ECCEQ002*

Subject OU: *ECEstado*

Subject OU: *SCEE*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I.P.*

Subject C: *PT*

X509SKI

X509 SK I *LgcREBhMaK3SeW1aA9S31Ows14I=*

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

Status Starting Time *2025-03-01T00:00:00Z*

9.7.4.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.7.4.2 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.8 - Service (granted): Chave Móvel Digital 00006

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]* *Chave Móvel Digital 00006*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *554286591274982108980380120644656043 90*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIH+TCCBeGgAwIBAgIQKbMr426c8Ef2dpHsRa7PljANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UE
BhMCUFQxQDA+BgNVBAoMN1NDRUUgLSBTaXN0ZW1fIGRlIENlcnRpZmljYcOnw6NvIEVsZWN0csOz
bmljYSBkbyBFc3RhZG8xETAPBgNVBAsMCEVDRXN0YWRvMSAwHgYDVQQDDBdDYXJ0w6NvIGRlIENp
ZGFkw6NvIDAwNzAeFw0yNTAzMjYxMjEwMzIaFw0zNzAzMDcxMDQ4MzVaMIHpMQswCQYDVQQGEwJQ
VDFCMEAGA1UECgw5QU1BIC0gQUFDIkI5DSUEgUEFSQSBBIE1PREVSTkIaQcOHw4NPIEFETUlOSVNU
UkFUSVZBIEkuIFAuMRwwGgYDVQQLDBNDYXJ0w6NvIGRlIENpZGFkw6NvMRQwEgYDVQQLDAtzdWJF
Q0VzdGFkbzFiMGAGA1UEAwxZRUMgZGUgQ2hhdmUgTcOzdmVsIERpZ2lOYWwgZGUgQXNzaW5hdHVy
YSBEaWdpdGFsIFF1YWxpZmlj YWRhIGRvIENhcnTDo28gZGUgQ2lkYWTDo28gMDAwMDYwggIMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCmWV0KTS2z8TYxaVFCnWZZQjnHoZiMI6iVyNnWKNhh
TElrDYMFUddlt6U/7LG3cbuYEq59SczXCrUxwibM+WcwZQIAc6U4QAmSQWP4+Z0rUbzKcuJxpjE
iN3o+Qm1N+TBj11RZAyhcCFAC8yFOL/zQxnHXgJSMzxzRF23qN2x9E85Vch9LjCsztIQyfTWFHj4
HZDTp/wPjZpMgZtfPTGbR5k3lrTLvS7xju9QhzvLAu8oMLRQWCRc3oRd9RLa3M20fIFmigXeOEqn
to1eB0PznmCjVlAPqjuz4F5GtARwlVNuQG8imDeyljcCNQUlytmKkY97y8L91wERMPpyka32XOkh
h1tiyhE/34HLMjP+agonWzqnWIT0y0rRJ2njPias4X1gpffOkZvpWcuKy8T805rUGfEjr6o7co54
Gn4gfRND9DVcayQmRrx7rzFYjqXegZvL6RWm6DM+rj305l+jnIwlF9x1QYWKF+nwgSg6rNmDht1J
zgy6cOaUE+aZy4lAQXjcGomDp2F/PifyF51epg3bbkykcHRoEUkA4tEYF8H9fRRT0bX28Hngzb4M
MP8joC X6M3pAplyt1faFbYjyPPJ1NU2kIv3DSE1kX5eec6p/EiGqfOc3xNFxRj11Ijk0igDhaAB
evPiBYPv9kf9Sl0VTmnO8ar8dwRpINWE6wIDAQABo4IBjCCAfowEgYDVR0TAQH/BAgwBgEB/wIB
ADAfBgNVHSMEGDAWgBQUnBJGPKdgfhXhCdlyxMcSPFlzzBMBggrBgEFBQcBAQRAMD4wPAYIKwYB
BQUHMAGGMGh0dHA6Ly9vY3NwLnJvb3QuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vb2NzcDCB
7AYDVR0gBIHkMIHhMFUGC2CEbAEBAQIEAAEjMEYwRAYIKwYBBQUHAgEWOGh0dHBzOi8vcGtpLmNh
cnRhb2RlY2lkYWRhby5wdC9wdWJsaWNvL3BvbGl0aWNhcy9jcC5odG1sMDEGBFUdIAAwKTAnBggr
BgEFBQcCARYbaHR0cHM6Ly93d3cuc2NlZS5nb3YucHQvcmVwMFUGCmCEbAEBAQIEAAcwRzBFBggr
BgEFBQcCARY5aHR0cHM6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0L3B1YmxpY28vcG9saXRpY2Fz
L2Nwcy5odG1sMFcGA1UdHwRQME4wTKBKoEiGRmh0dHA6Ly9wa2kuY2FydGFvZGVjaWRhZGFvLnB0
L3B1YmxpY28vbHJlL2NlX2V1X2NpZGFkYW9fY3lsMDA3X2NyDC5jcmwwHQYDVR0OBBYEFJKMzpns
FgejZ57xycYjvrDWZgPUMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAnovSJaOK
MZpknuI1QEYSRZvHkpzppeTcmgO1UaeB+98e9vcbVAiKWVoozNHqEjj/U0twTH/gW53bx1aUtJY8
fz+RcaqUzFOgkIh8ZhuWWYxLBTe5IfmLqfAQFmEBzqQiT0out2gR+EJlxW/PH8lhGSznGhPxvNac
PIjujOeySUWHV0cZ15iucnMCd/7ySrLBI4ouVPJ13MJmtF1OTZuo4XD/5ocWsGCVlhKUoVWm/tu
T9DRxHViW6VdUxto+/r/7YeJ0d4OJqzGeP+M9ZEgQn2NjBtCGO4hBYCKSQL1ZpJp6wTsH1xlygRa
qbD5FBZqb/RE9jCAOYHlkHJfYS0mQgueN2yNefdp23ks0+Gog49sO1PhKJBzOxRPo2QHycSqm3ud
CB2bXC6gIcUI3Yelg5oVfnDj766Lhij7YSe/EwVO2Ez3kfk4zP0HcNHB1NxpnjWye4rZsMsLnB
z3ZT9XIMNVGYSyD9Uz6UuRPg/33mUXdwj7n+lO5mRSHrrjEyd6luQcBRMXs8b59Yomecdrcp Q
OVPOpN7YGFIj40esa/tmUNSCrY7cqxinuQ3vZfPBZjHW6bjcRLAvsQs9VKx9e/hbXgG3yPMA1anS
WZXp5i/0rdSbre9Th4S03eNJX3O0KxdCGw9K8CGkALJvq5YcTh8dpSWU93jmj9yf1MQ=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *Cartão de Cidadão 007*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C:	*PT*
Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00006*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*
Valid from:	*Wed Mar 26 13:10:39 CET 2025*
Valid to:	*Sat Mar 07 11:48:35 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:A6:59:5D:0A:4D:2D:B3:F1:36:31:69:51:42:9D:66:59:42:39:C7:A1:98:8C:97:A8:95:C8:D9:D6:28:D8:61:4C:49:6B:0D:83:05:51:D7:48:B7:A5:3F:EC:B1:B7:71:BB:98:12:AE:7D:49:C6:F3:5C:2A:D4:C7:08:9B:33:E5:9C:C1:94:25:01:CE:94:E1:00:26:49:05:8F:E3:E6:74:AD:46:F3:29:CB:89:C6:98:C4:88:DD:E8:F9:09:B5:37:E4:C1:8F:5D:51:64:0C:A1:70:21:40:0B:CC:85:38:BF:F3:43:19:C7:5E:02:52:33:3C:73:44:5D:B7:A8:DD:B1:F4:4F:39:55:CB:7D:2E:30:AC:CE:D9:50:C9:F4:D6:14:78:F8:1D:90:D3:A7:FC:0F:8D:9A:4C:A9:9B:5F:3D:31:9B:47:99:37:22:B4:CB:BD:2E:F1:8E:EF:50:87:3B:CB:02:EF:28:30:B4:50:58:24:5C:DE:84:5D:F5:12:DA:DC:CD:B4:7C:81:66:8A:05:DE:38:4A:A7:B6:8D:5E:04:E3:F3:9E:60:A3:56:50:0F:AA:3B:B3:E0:5E:46:1A:D0:11:C1:53:6E:40:6F:22:9B:47:B2:22:37:02:35:05:08:CA:D9:8A:91:8F:7B:C8:12:FD:D7:01:11:30:FA:72:91:AD:F6:5C:E9:21:B7:5B:62:CA:11:3F:DF:81:CB:32:33:FE:6A:0A:27:5B:3A:A7:58:84:F4:CB:4A:D1:27:69:C9:3E:26:AC:E1:7D:60:A5:F7:CE:91:98:E9:59:CB:8A:CB:C4:FC:D3:9A:D4:19:F1:23:AF:AA:3B:72:8E:78:1A:7E:2A:7D:13:43:F4:35:5C:6B:24:26:46:BC:7B:AF:31:58:8E:A5:DE:81:9B:CB:E9:15:A6:E8:33:3E:AE:3D:F4:E6:5F:A3:9C:8C:25:17:DC:75:41:85:8A:17:E9:F0:81:28:3A:AC:D9:83:86:DD:49:CE:0C:BA:70:E6:94:13:E6:99:CB:89:40:41:72:5C:1A:89:83:A7:61:7F:3E:27:F2:17:9D:5E:A6:0D:DB:6E:4C:A4:70:74:68:11:49:00:E2:D1:18:17:C1:FD:7D:14:53:D1:B5:F6:F0:79:E0:CD:BE:0C:30:F0:63:A0:25:FA:33:7A:40:A6:5C:AD:D5:F6:85:6D:88:F2:3C:FF:E5:D4:D5:36:90:8B:F7:0D:21:35:91:7E:5E:79:CE:A9:FC:49:46:81:F3:9C:DF:13:45:C5:18:F5:D4:88:E4:D2:28:03:85:A0:01:7A:F3:E2:05:83:EF:F6:47:FD:4A:5D:15:4E:69:CE:F1:AA:FC:77:04:69:20:D5:84:EB:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*14:9C:12:46:3C:A9:1D:81:F8:57:84:27:65:CB:13:1C:48:F1:65:CF*
Authority Info Access	*http://ocsp.root.cartaodecidadao.pt/publico/ocsp*
Certificate Policies	*Policy OID: 2.16.620.1.1.1.2.4.0.1.9* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cp.html* *Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: https://pki.cartaodecidadao.pt/publico/politicas/cps.html*
CRL Distribution Points	*http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl007_crl.crl*
Subject Key Identifier	*92:8C:CE:99:EC:16:07:A3:67:9E:F1:C9:C6:23:BE:B0:D6:66:03:D4*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1A:EA:D5:90:1F:50:A0:52:A3:07:26:D8:F6:99:32:7D:06:69:D4:A8:FA:00:6F:C9:3D:F9:B8:5A:61:8B:7F:A4*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00006*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*

Subject C: *PT*

X509SKI

X509 SK I *kozOmewWB6NnnvHJxiO+sNZmA9Q=*

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

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

Status Starting Time *2025-06-09T15:00:00Z*

9.8.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.8.2 - Extension (not critical): Qualifiers [QCStatement, QCQSCDManagedOnBehalf, 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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

Description

9.8.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *Chave Móvel Digital 00006*

Service digital identities

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00006*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.*
Subject C:	*PT*

X509SKI

X509 SK I	*kozOmewWB6NnnvHJxiO+sNZmA9Q=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2025-05-08T11:00:00Z*

9.8.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.9 - Service (granted): CMD00007

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]*	*CMD00007*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*156656901778166022664089017382317961684468322882*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIG7DCCBk6gAwIBAgIUG3C9CaTV/ukj0NRGoiq5A2/DUkIwCgYIKoZIzj0EAwIwgYQxCzAJBgNV
BAYTAlBUMUI4wPgYDVQQKDDdTQ0VFIC0gU2lzdGVtYSBkZSBDZXj0aWZpY2HDpBOjbyBFbGVjdHLD
s25pY2EgZG8gRXN0YWRvMREwDwYDVQQLDAhFQ0VzdGFkbzEgMB4GA1UEAwwXQ2FydMOjbyBkZSBD
aWRhZMOjbyAwMDgwHhcNMjUwOTE3MTQ0NTI2WhcNMzcwOTE3MTQ0NTI1WjCB5TELMAkGA1UEBhMC
UFQxPjA8BgNVBAoMNUFnw6puY2lhIHBhcmEgYSBSZWZvcm1hIFRlY25vbMOzZ2ljYSBkbyBFc3Rh
ZG8sIEkuIFAuMRwwGgYDVQQLDBNDYXj0w6NvIGRlIENpZGFkw6NvMRQwEgYDVQQLDAtzdWJfQ0Vz
dGFkbzFlMGAGA1UEAwxZRUMgZGUgQ2hhdmUgTcOzdmVsIERpZ2l0YWwgZGUgQXNzaW5hdHVyYSBE
aWdpdGFsIFF1YWxpZmlqYWRhIGRvIENhcnTDo28gZGUgQ2lkYWTDo28gMDAwMDcwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDHoqPo6nBCjA+cPQwROBhPjm2HXOu6/BWvtEqM9X0FeIIh
LgPAUK5DROgRLGOXaVjlzDqpKQIhtPawRYXAFtfLseZhaCaQPKQpDTqkgFh8xKieKOqID22GM7ob
9WiM+5xUXOYpjqO00knm8qZja+TL85Y8kyu5J68cbuvMcb0KMdOP6hENmdf5UTJB5nHwEo6uch8
vSWzb9SxCPqWlLwtR9N74bUBlUQlqPlf6dJNvnPi5hlC/TqejySntvvEA7vzmv2svB4n5EMPkRyZ
svy0YIZvXtOqlS5akQA89dobdH+7xHSh2F9vmZj6eygd4J3m1LRwrFV+CZ8hglnF9F3InBqdeudn
0HrLMU9hWcimIMIQAgjzj6jWe8a9Esw1TMiDGF3sY7siv/6bTZgqxBW9swza/v6caAgjCd/4D9Nq
vBRQxX+L6nCtNEp/+WcHPuT7YnzNeyLifOJyHZa94UgdT0ebhp6GiYMtghmo/nH/nZOBjWZuDrE7
zyWSTeQ3rVRFOOq5LWjHg6dr+V0AUyqH/porcAH6j2JyoS1SzlP/ciKIBh7W5RijPBoCl/mH1zR
SPFxhCEPvO+Ovsw0as9Eq5pL1WMcQ6UuKAiNQX1jr7t4TjW1zA3KMynLmFpepRiDpfl0j8gzdvtw
vnCaWTnIQAF1unf+3bnUlEAlzUg5KwlDAQABo4ICbjCCAmowEgYDVR0TAQH/BAgwBgEB/wIBADAf
BgNVHSMEGDAWgBSrAIAr+zNE+T34Xvne/7FzZ5lj/CBrAYIKw7BBQUHAQEEgZ8wgZwwXwYIKwYB
BQUHMAKGU2h0dHA6Ly9wa2kyLmNhcnRhb2RlY2lkYWRhby5wdC9lbnRpZGFkZS1jZXj0aWZpY2Fj
YW8tY2MvY2VydGlmaWNhZG9zL0NDX1jvb3QwMDguY3J0MDkGCCsGAQUFBzABhi1odHRwOi8vb2Nz
cC5yb290LnBraTluY2FydGFvZGVjaWRhZGFvLnB0L29jc3AwgesGA1UdIASB4zCB4DAyBgRVHSAA
MCowKAYIKwYBBQUHAgEWHGhdHBzOi8vd3d3LnNjZWUuZ29ZLnB0L3JlcC8wVAYKYIRsAQEBAgQA
BzBGMEQGCCsGAQUFBwIBFjhodHRwOi8vcGtpLmNhcnRhb2RlY2lkYWRhby5wdC9wdWlsaWNvL3Bv
bGl0aWNhcy9jcHMuaHRtbDBUBgtghGwBAQECBAABBDBFMEMGCCsGAQUFBwIBFjdodHRwOi8vcGtp
LmNhcnRhb2RlY2lkYWRhby5wdC9wdWlsaWNvL3BvbGl0aWNhcy9jcC5odG1sMGcGA1UdHwRgMF4w
XKBaoFiGVmhdHA6Ly9wa2kyLmNhcnRhb2RlY2lkYWRhby5wdC9lbnRpZGFkZS1jZXj0aWZpY2Fj
YW8tY2MvbGlzdGEtcmV2b2dhY2FvL0NDX1jvb3QwMDguY3JsMB0GA1UdDgQWBBSPrjhiqh5jQI0a3
vbmYvLhoNHc4cDAOBgNVHQ8BAf8EBAMCAQYwCgYIKoZIzj0EAwIDgYsAMIGHAkEEE+ZsyAEE1rPl
JR48MOO8LEyDrpQ325NvjWTqjrs6+6BmsSHL0my6o5tUKCJwXxV4j2cYxQa3jRsEpCcrUyBguAJC
Ad95SO5eY2Rac9YZDcwvxuw2Gu9hL74Dn+mldfoGnc0lJT8Rw9GClIxoUw5vVXuYt00h/0hcBau4
HnjpegRQaTwh

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer CN: *Cartão de Cidadão 008*

Issuer OU: *ECEstado*

Issuer O: *SCEE - Sistema de Certificação Electrónica do Estado*

Issuer C: *PT*

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00007*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Agência para a Reforma Tecnológica do Estado, I. P.*

Subject C: *PT*

Valid from: *Wed Sep 17 16:45:26 CEST 2025*

Valid to: *Thu Sep 17 16:45:25 CEST 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:C7:A2:A3:E8:EA:70:42:24:0F:9C:3D:0C:11:38:18:4F:8E:6C:C7:5C:EB:BA:FC:
15:AF:B4:4A:8C:F5:7D:05:78:82:21:2E:03:CD:50:AE:43:44:E8:11:2C:64:17:69:58:C9:CC:3A:A9:29:02:21:B4:F6:B0:45:85:C0:16:D7:CB:B1:E6:61:68:26:90:3C:A4:29:0D:3A:A4:80:58:7
C:C4:A8:9E:28:EA:A5:0F:6D:86:33:BA:1B:F5:68:8C:F9:2C:63:51:74:18:A6:3A:BE:D3:49:27:9B:CA:99:8D:AF:93:2F:CE:5B:F2:4C:AE:E4:9E:BC:71:BB:AF:31:C6:F4:28:C7:4E:3F:A8:44:36:
67:5F:E5:44:FF:F1:29:C7:C0:4A:3A:B9:C8:7C:BD:25:B3:6F:D4:B1:08:FA:96:94:BC:2D:47:D3:7B:E1:B5:01:21:44:25:A8:F2:1F:E9:D2:4D:BE:73:E2:E6:19:42:FD:3A:9E:8F:24:A7:B6:FB:C4
:03:BB:F3:9A:FD:AC:BC:1E:27:E4:43:0F:91:1C:99:B2:FC:B4:62:56:6F:5E:D3:AA:95:2E:5A:91:00:3C:F5:DA:1B:74:7F:BB:C4:74:A1:D8:5F:6F:99:98:FA:7B:28:1D:E0:9D:E6:D4:B4:70:AC:5
5:7E:09:9F:21:82:59:C5:F4:5D:E5:9C:1A:9D:7A:E7:67:D0:7A:CB:31:4F:61:59:C8:A6:20:C2:10:02:08:F3:8F:A8:D6:7B:C6:BD:12:CC:35:4C:C8:83:18:5D:EC:63:BB:22:BF:FE:9B:4D:9A:A0
:C4:15:BD:B3:0C:DA:FE:FE:9C:68:08:23:09:DF:F8:0F:D3:6A:BC:14:50:C5:7F:BB:EA:70:AD:34:4A:7F:F9:67:07:3E:E4:FB:62:7C:CD:7B:22:E2:7C:E2:72:1D:96:BD:E1:48:1D:4F:47:9B:86:9
E:86:89:83:2D:82:19:A8:FE:71:FF:9D:93:81:8D:66:6E:3A:B1:3B:CF:25:92:4D:E4:37:AD:54:45:3B:4A:B9:2D:68:C7:83:A7:6B:F9:5D:00:53:2A:87:FE:9A:2B:70:01:FA:8F:62:72:A1:2D:52:
CC:99:4F:FD:C8:BA:94:18:7B:5B:94:62:8C:F0:68:0A:5F:E6:1F:5C:D1:48:F1:71:84:21:0F:BC:EF:8E:BE:CC:34:6A:CF:44:AB:9A:4B:D5:63:1C:43:A5:2E:28:08:8D:41:7D:63:AF:BB:78:4E:35
:B5:CC:0D:CA:33:29:CB:98:5A:5E:A5:18:83:A5:F2:34:8F:CA:B3:77:2B:70:BE:70:9A:59:39:C8:40:01:75:BA:77:FE:DD:B9:D4:94:40:25:CD:48:39:2B:02:03:01:00:01
```


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

Authority Key Identifier *AB:00:80:2B:FB:33:44:F9:3D:F8:5E:F9:DE:FF:B1:73:67:99:62:FE*

Authority Info Access *http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/certificados/CC_Root008.crt*

http://ocsp.root.pki2.cartaodecidadao.pt/ocsp

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.scee.gov.pt/rep/* *Policy OID: 2.16.620.1.1.1.2.4.0.7* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cps.html* *Policy OID: 2.16.620.1.1.1.2.4.0.1.4* *CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/cp.html*
CRL Distribution Points	*http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/lista-revogacao/CC_Root008.crl*
Subject Key Identifier	*8F:8E:18:AA:87:98:D0:23:46:B7:BD:B9:98:BC:B8:68:34:77:38:70*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*9C:0B:D1:03:92:D1:BC:A3:86:74:40:37:33:16:A8:62:B9:62:AB:BF:FB:A5:B9:8F:8A:8F:52:09:38:3F:0A:B2*

X509SubjectName

Subject CN:	*EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00007*
Subject OU:	*subECEstado*
Subject OU:	*Cartão de Cidadão*
Subject O:	*Agência para a Reforma Tecnológica do Estado, I. P.*
Subject C:	*PT*

X509SKI

X509 SK I	*j44YqoeY0CNGt725mLy4aDR3OHA=*

Service Status

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

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

Status Starting Time

2025-10-08T18:00:00Z

9.9.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

9.9.2 - Extension (not critical): Qualifiers [QCStatement, QCQSCDManagedOnBehalf, 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.*

Criteria list assert=atLeastOne

Policy Identifier:

Identifier *[OIDAsURI]* *0.4.0.194112.1.2*

Description

Description

9.9.3 - History instance n.1 - Status: granted

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

Service Name

Name *[en]* *CMD00007*

Service digital identities

X509SubjectName

Subject CN: *EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00007*

Subject OU: *subECEstado*

Subject OU: *Cartão de Cidadão*

Subject O: *Agência para a Reforma Tecnológica do Estado, I. P.*

Subject C: *PT*

X509SKI

X509 SK I *j44YqoeY0CNGt725mLy4aDR3OHA=*

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

Status Starting Time *2025-10-07T16:00:00Z*

9.9.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

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

10 - TSP: NOS COMUNICAÇÕES, S.A.

.

TSP Name

Name	*[en]*	*NOS COMUNICAÇÕES, S.A.*
Name	*[pt]*	*NOS COMUNICAÇÕES, S.A.*

TSP Trade Name

Name	*[en]*	*NOS*
Name	*[en]*	*VATPT-502604751*
Name	*[en]*	*Lleidanetworks Serveis Telemàtics, S.A.*

PostalAddress

Street Address	*[en]*	*Rua Actor António Silva, nº9, Campo Grande*
Locality	*[en]*	*Lisboa*
State Or Province	*[en]*	*Lisboa*
Postal Code	*[en]*	*1600-404 Lisboa*
Country Name	*[en]*	*PT*

PostalAddress

Street Address	*[pt]*	*Rua Actor António Silva, nº9, Campo Grande*
Locality	*[pt]*	*Lisboa*
State Or Province	*[pt]*	*Lisboa*
Postal Code	*[pt]*	*1600-404 Lisboa*
Country Name	*[pt]*	*PT*

ElectronicAddress

URI	*[en]*	*mailto:comunicacao.corporativa@nos.pt*
URI	*[en]*	*https://www.nos.pt*

TSP Information URI

URI *[en]* *https://www.nos.pt/empresas/profissionais-empresas/aplicacoes-negocio/Pages/NOS-Comunicacoes-Registadas-Pro.aspx*

10.1 - Service (deprecatedatnationallevel): Delegated RA (Registration Authority) - Verification Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/RA

Service type description *[en]* *A registration service that verifies the identity and, if applicable, any specific attributes of a subject for which a certificate is applied for, and whose results are passed to the relevant certificate generation service.*

Service Name

Name *[en]* *Delegated RA (Registration Authority) - Verification Authority*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5379122206984586969*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGvjCCBaagAwIBAgIISqZ7Jb67RtkwDQYJKoZIhvcNAQELBQAwgZIxC2AJBgNVBAYTAkVTMR4w
HAYDVQQKExVGaXJtYXByb2Zlc2lvbmFsIFMuQS4xIjAgBgNVBAsTGUNlcnRpZmlpYWRvcyBDdWFs
aWZpY2Fkb3MxEjAQBgNVBAUTCUE2MjYzNDA2ODErMCkGA1UEAxMiQUMgRmlybWFwcm9mZXNpb25h
bCAtIENVQUxjRkIDQURPUzAeFw0xODAyMTkxMjM3MDBaFw0yMzAyMTgxMjM3MDBaMIHRMQswCQYD
VQQGEwJFUzEPMA0GA1UECAwGTExFSURBMTEwLwYDVQQKDChMbGVpZGFuZXR3b3JrcyBTZXJ2ZWlz
IFRlbGVtw6B0aWNzLCBTLkEuMRgwFgYDVQRhDA9WQVRFUy1BMjUzNDUzMzExHTAbBgNVBAsMFFRF
Q0hOSUNBTCBERVBBUlRNRU5UMRIwEAYDVQQFEwlBMjUzNDUzMzExMTAvBgNVBAMMKExsZWlkYW5l
dHdvcmtzIFNlcnZlaXMgVGVsZW3DoHRpY3MslFMuQS4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDZHCJmq3VQiypncEMq9AjfvGlhY2/7siKr2kYToqrRMBWszQ8KnFjY8NRyFdS1xcjn
Y+dh55i4Ycy0pPgZy2todigN+bbGgbI0P0dPT92oIThyfiGyEkYylWQLwya7lqmagoZ0gGHYShSAZ
r2ssNu2bDsxHKp4dpedjMTFbp4eqQD89nSk7Mcd5WK0Cm0Zt7DTR3P/TuXS+bIo8FAIOrUW3tClp
LRYgj97YdcIDWduja/v5Xa0//CRaYMmd1SZMi9gqSw7eRmDQQs5c/RDtnpkbiBcDcUpxihrg/Q6E
uaIyuCQSk2kc/4h4+DeMW3bWb1Az1/KvzpoHn2NIxHARr/s9AgMBAAGjggLVMIIC0TB6BggrBgEF
BQcBAQRuMGwwPAYIKwYBBQUHMAKGMCh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vY3Vh
bGlmaWNhZG9zLmNydDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AuZmlybWFwcm9mZXNpb25hbC5j
b20wHQYDVR0OBBYEFINzCjfrGBdmqucHp3zcmkHEsq1GMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUjHHMkwdv0dWGaH2COkHZTAL4Il0wfQYJKwYBBQUHAQMEcTBvMAgGBgQAjkYBATALBgYEAI5G
AQMCAQ8wEwYGBACORgECMAkGBwQAjkYBBgIwOQYJKwYBBAGCORgEFMDcwNRYvaHR0cHM6Ly93d3cuZmly
bWFwcm9mZXNpb25hbC5jb20vY3BzL3kc19lbi5w2GYTAmVuMIIBEgYDVR0gBIIBCTCCAQUwgfcG
CysGAQQB5nkKAQoCMIHnMC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LmZpcm1hcHJvZmVzaW9uYWwu
Y29tL2NwczCBswYIKwYBBQUHAgIwgaYMgaPDiXN0ZSBlcyB1biBDZXJ0aWZpY2Fkby8Db3Jwb3Jh
dGl2byBkZSBTZWxsbyBFbXByZXNhcmlhbCBjdWFsaWZpY2Fkby4gRGlyZWNjac0zbiBkZWwgcHJl
c3RhZG9yIGRlIHNlcnZpY2lvcyBkZSBjb25maWFuemE6IFBhc2VvIGRlIGxhIEJvbmFub3ZhNLCA0
Ny4gMDgwMTcgQmFyY2Vsb25hMAkGBwQAi+xAAQEwQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL2Ny
bC5maXJtYXByb2Zlc2lvbmFsLmNvbS9jdWFsaWZpY2Fkb3MuY3JsMA4GA1UdDwEB/wQEAwIF4DAd
BgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwDQYJKoZIhvcNAQELBQADggEBAKYDU8gk5Nu8
9t+Ngb0tYdPfaP31hA2QakI5VSPPKbidcf5NZgWN5pXG0MNBkgxu2okYTeeFgMy2GXFGifmtOo3
We9hp8eb7OCSpZnzfiGJ4mUXpXqGc6KIy3l+FQXiKEfYmcWiAgNE3NLvdTQN/5BkddMWBCTOAanS
ln+vZwyWxHwc9pmyyYR5bgGJQUyi9PECkZgMbJWxBn5ptlkda3MYGj2p27Ogq0nj7EdLb3tAxPij
5ESZOI2ViKDpAWkrnCp60bjZfGnDFnplYP7md9gCrAEumYPEg9se0Qg2F7OImwib+9+kpss1bUPz
ex7lYm6Dhqh0ul4uUfeMgv9+9qo=

-----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: *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:01:01:01:05:00:03:82:01:0F: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:D1:30:15:AC:CD:0F:0A:9C:58:D8:F0:D4:72:15:D4:B5:C5:C8:E7:63:E7:61:E7:99:78:61:CC:B4:A4:F8:19:CB:67:E8:76:28:0D:F9:B6:C6:81:B2:0E:3F:47:4F:4F:DD:A8:95:38:72:7E:21:B2:12:46:32:59:02:F0:C9:AE:C8:AA:66:A0:A1:9D:2A:18:76:12:85:20:19:AF:6B:2C:36:ED:9B: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:02:9B:46:6D:EC:34:D1:DC:FF:D3:B9:74:BE:6C:BA:3C:14:09:4E:AD:45:B7:B4:22:29:2D:16:20:8F:DE:D8:75:C9:43:59:DB:89:6B:F8:F9:5D:AD:3F:FC:24:5A:60:C9:9D:D5:26:4C:8B:D8:2A:4B:0E:DE:46:60:D0:42: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:EE: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/deprecatedatnationallevel

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

Status Starting Time

2025-02-28T00:00:00Z

10.1.1 - History instance n.1 - Status: recognisedatnationallevel

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/RA

Service Name

Name *[en]* *Delegated RA (Registration Authority) - Verification Authority*

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/recognisedatnationallevel*
Status Starting Time	*2021-01-25T00:00:00Z*

11 - Signature node - Id: id-2d073691b535c94a543045b954d84f6f

.

Signing Time

2026-07-01T11:11:43Z

TSL Scheme Operator certificate fields details

Version:

3

Serial Number:

129179134488490223641223067489262815787

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIExjCCA66gAwIBAgIQYS7/D337SVpmO2CCEzbKKzANBgkghkiG9w0BAQsFADB/MQswCQYDVQQG
EwlQVDE6MDgGA1UECgwxQ2VudHJvIGRlIEdlc3TDo28gZGEgUmVkZSBlbmZvcm3DoXRpY2EgZG8g
R292ZXJubzENMAsGA1UECwwEU0NFRTERMA8GA1UECwwIRUNFc3RhZG8xEjAQBgNVBAMMCUVDQ0VO
UTAwMTAeFw0yNDA1MDgxMTIyNDJaFw0yNzA1MDgxMTIyNDJaMGcxCzAJBgNVBAYTAlBUMSgwIgYD
VQQKDB9HYWJpbmV0ZSBOYWNpb25hbCBkZSBTZWd1cmFuw6dhMS4wLAYDVQQDDCVQT1JUVUdVRVNF
IFRSVVNUIExjU1QgU0NlRU1FIE9QRVJBVE9SMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA3ILzhMTUwHxQCrpfTq6dgg6j+xyY/gptE7nsgNSK7RBkkjnsp77mY++ItweTCE/334glDa5z
Csv6/59XK3lM6eJpXFVhqwbLvNT9KVgT3YEvek9fvy/DhCdmEisAv51M9b+K92WHkVaLpoURYYa9
+k6sjF1iEDZ4hKBqtU7Gg5jgO00F7ghbzqFf4tnepWjRcRjrzQxD87tQYdGhErueM56bq0LL+jHF
enQC1Z2C+QkoHMrirbHHfZlwn9eKGihipvvvbjWX2t4gtU5Seo7Pv0VrL1xyIJeO9dIkoNtaja8q
yIZw4SvUg0imLdaYD9UfRlMEwewZ7PncNMxcvhqIQwIDAQABo4IBVDCCAVAwCQYDVR0TBAIwADAO
BgNVHQ8BAf8EBAMCBkAwEQYDVR0lBAowCAYGBACRNwMAMB0GA1UdDgQWBBSE/HUkA1hcvLjaBsVQ
w08yjWDX2zAfBgNVHSMEGDAWgBTeXZmFcW676uJV4ZaHFfMVbaFm2zA7BgNVHSAENDAyMDAGBFUd
IAAwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5lY2NlLmdvdi5wdC9kcGMwZgYIKwYBBQUHAQEE
WjBYMCMGCCsGAQUFBzABhhodHRwOi8vb2NzcC5lY2NlLmdvdi5wdDAxBggrBgEFBQcwAoYlaHR0
cDovL3RydXN0LmVjY2UuZ292LnB0L2VjY2UtMDAyLmNydDA7BgNVHR8ENDAyMDCgLqAshipodHRw
Oi8vY3Jscy5lY2NlLmdvdi5wdC9jcmxzL2VjY2VucTAwMS5jcmwwDQYJKoZIhvcNAQELBQADggEB
ANOzm11ltTG4BVmpPlWlE+rmqRxN2HVbQEWjiwJN9HVg/SAIe7AI9cJV6yr914AMVuIrI0P3zAex
b35Y3bwoQYeJGcBO878A6brr2atA1wjHlYlFMyUZv+qJsbMwYQGndkjeEKOfkc8XOtJmDbs3scB
jG8MQpcUgLedWvB6wy63GL/o947Udj6zUy81ijMXBk8Iwt T6iY7CJND0CMdEn0M3hJu01/4HN/sl
pgUzR8AcR9vZapcXEtKtdYyqmRrU/30EBEP6+dn/GcNsHlkkybtvTWaMIgsPjjsBacaDffZ8cdM
lruc2j2wuWkaaWum0gyZ7yoNU1dKfwabRtyPbOw=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA256withRSA

Issuer CN:

ECCENQ001

Issuer OU:

ECEstado

Issuer OU:

SCEE

Issuer O:

Centro de Gestão da Rede Informática do Governo

Issuer C:

PT

Subject CN:

PORTUGUESE TRUST LIST SCHEME OPERATOR

Subject O:

Gabinete Nacional de Segurança

Subject C:

PT

Valid from:

Wed May 08 13:22:42 CEST 2024

Valid to:

Sat May 08 13:22:42 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:DC:82:F3:84:C4:D4:C0:7C:50:0A:BA:5F:4E:AE:9D:82:0E:89:FB:1C:98:FE:0A:
6D:13:B9:EC:80:D4:8A:ED:10:64:92:39:EC:A7:BE:E6:63:EF:88:B7:07:93:08:4F:F7:DF:88:25:0D:AE:73:0A:CB:FA:FF:9F:57:2B:79:4C:E9:E2:69:5C:55:61:AB:06:CB:BC:D4:FD:29:58:13:D
D:81:2F:7A:4F:5F:BF:2F:C3:84:27:66:12:2B:00:BF:9D:4C:F5:BF:8A:F7:65:87:91:56:8B:A6:85:11:61:86:BD:FA:4E:AC:8C:5D:62:10:36:78:84:AF:2A:B5:4E:C6:83:98:EA:3B:4D:05:EE:08:
5B:CE:A1:5F:E2:D9:DE:A5:62:51:71:18:EB:CD:0C:43:F3:BB:50:61:D1:A1:12:BB:9E:31:2E:9B:AB:42:CB:F8:91:C5:7A:74:02:D5:9D:82:F9:09:28:1C:CA:E2:AD:B1:C7:7D:99:70:9F:D7:8A:
1A:28:62:A6:FB:EF:6C:95:97:DA:DE:20:B5:4E:52:7A:BE:CF:BF:45:6B:2F:5C:72:94:97:8E:F5:D2:24:A0:DB:5A:8D:AF:2A:C8:86:70:E1:2B:D4:83:48:A6:2D:D6:98:0F:D5:1F:44:83:04:C1:E
C:19:EC:F9:DC:34:CC:5C:BE:1A:A5:43:02:03:01:00:01
```


Basic Constraints

IsCA: false

Extended Key Usage

id-tsl-kp-tslSigning

Subject Key Identifier

84:FC:75:24:03:58:5C:BC:B8:DA:06:C5:50:C3:4F:32:8D:60:D7:67

Authority Key Identifier	*DE:5D:99:85:71:6E:BB:EA:E2:55:E1:96:87:15:F3:15:6D:A1:66:DB*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://www.ecce.gov.pt/dpc*
Authority Info Access	*http://ocsp.ecce.gov.pt* *http://trust.ecce.gov.pt/ecce-002.crt*
CRL Distribution Points	*http://crls.ecce.gov.pt/crls/eccenq001.crl*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*13:B3:14:74:C9:D6:E1:B5:D0:ED:FF:4B:19:63:05:1F:F2:FF:E9:1D:EE:DD:1B:C5:16:52:A4:DB:FC:8C:F7:F0*