



PORTUGAL (PORTUGAL) : Trusted List

Tsl Id: TrustServiceStatusList

Valid until nextUpdate value: 2012-10-23T00:00:01Z

TSL Scheme Information

TSL Id	<i>TrustServiceStatusList</i>
TSLTag	<i>http://uri.etsi.org/02231/TSLTag</i>
TSLVersionIdentifier	<i>3</i>
TSLSequenceNumber	<i>6</i>
TSLType	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic</i>

SchemeOperatorName

Name *[en]* *National Security Cabinet of Portugal*

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

PostalAddress

StreetAddress *[en]* *Rua da Junqueira, 69*

Locality *[en]* *Lisbon*

StateOrProvince *[en]* *Lisbon*

PostalCode *[en]* *1300-342 Lisboa*

CountryName *[en]* *PT*

PostalAddress

StreetAddress *[pt]* *Rua da Junqueira, 69*

Locality *[pt]* *Lisbon*

StateOrProvince *[pt]* *Lisbon*

PostalCode *[pt]* *1300-342 Lisboa*

CountryName *[pt]* *PT*

ElectronicAddress

URI *http://www.gns.gov.pt*

URI *mailto:geral@gns.gov.pt*

SchemeName

Name [en] *PT:Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.*

Name [pt] *PT:Relação das Entidades Certificadoras que estão registadas ou credenciadas pela Autoridade Credenciadora, no cumprimento das disposições previstas na Directiva 1999/93/CE do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999, relativa ao quadro comunitário para as assinaturas electrónicas.*

SchemeInformationURI

URI [en] <http://www.gns.gov.pt/gns/en/tsl>

URI [pt] <http://www.gns.gov.pt/gns/pt/tsl/>

StatusDeterminationApproach

<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate>

SchemeTypeCommunityRules

URI <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common>

URI <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/PT>

SchemeTerritory

PT

PolicyOrLegalNotice

TSLLegalNotice [en] *The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for Portugal is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in Portugal laws.*

TSLLegalNotice [pt] *O quadro jurídico aplicável à presente implemntação desta TSL (Trusted-Service Status List) é a Directiva 1999/93/CE do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999, relativa ao quadro comunitário para as assinaturas electrónicas e sua aplicação nas leis de Portugal, nomeadamente, o Decreto-Lei n.º 290-D/99, de 2 de Agosto.*

HistoricalInformationPeriod

7306

PointersToOtherTSL

OtherTSLPointer

Service digital identities

Certificate fields details

Version 3

SerialNumber 1208925819615896178901234

Subject GIVENNAME: *Karel Lodewijk M*

Subject SURNAME: *De Vriendt*

Subject CN: *Karel Lodewijk M De Vriendt*

Subject OU: *NA*

Subject O: *European Commission*

Subject L: *BE*

Subject C: *BE*

NotBefore *Wed Dec 23 11:35:56 CET 2009*

NotAfter *Sun Dec 23 11:35:56 CET 2012*

PublicKey
30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:BD:E8:90:6A:9E:30:A6:02:4E:37:2C:3B:99:0C:CB:B9:94:D1:8A:EF:F5:10:9C:90:4B:0E:45:2A:37:62:5B:FD:24:D0:48:12:67:44:97:21:09:8F:43:9C:AB:6A:60:6F:5C:B9:26:43:47:1B:C8:52:4B:2C:A8:EF:D6:A4:5B:BF:23:97:CE:F4:8E:26:BC:B1:83:F6:1E:28:B7:C:F:C6:91:19:ED:6C:49:77:0A:73:25:44:A6:49:90:07:5C:48:7C:2E:AA:7B:8D:A5:F6:99:E3:21:86:20:FB:25:47:2F:69:6D:19:1F:5D:27:9E:9D:E2:40:A3:42:31:8A:ED:D0:27:02:03:01:00:01

BasicConstraints *IsCA: false*

AuthorityInfoAccess
http://ocsp.luxtrust.lu
http://ca.luxtrust.lu/LTQCA.crt

CertificatePolicies
Policy OID: 1.3.171.1.1.2.4.1
CPS text: [LuxTrust Qualified Certificate on CCSD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualified Electronic Signature.]
CPS pointer: http://repository.luxtrust.lu
Policy OID: 0.4.0.1456.1.1

QCStatements - crit. = false
id_etsi_qcs_QcCompliance
id_etsi_qcs_LimiteValue
Value: not readable
Currency: not readable
id_etsi_qcs_QeSSCD

AuthorityKeyIdentifier *8D:90:A3:07:DD:1A:13:77:99:4C:92:AB:4D:43:DE:3F:CD:29:64:05*

CRLDistributionPoints *http://crl.luxtrust.lu/LTQCA.crl*

SubjectKeyIdentifier *4C:03:3B:25:5E:DC:85:79*

KeyUsage *nonRepudiation*

SHA256 Cert. hash *D5:49:51:FE:BB:C5:9D:2C:2E:C0:1A:CC:D9:2C:CD:8C:9D:2C:74:44:C2:E5:51:BA:7E:C0:DE:62:2C:74:14:8C*

TSLLocation https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

TSLType <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/schemes>

SchemeOperatorName

Name [*en*] *European Commission*

SchemeTypeCommunityRules

URI <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CompiledList>

SchemeTerritory *EU*

MimeType *application/vnd.etsi.tsl+xml*

ListIssueDateTime *2012-04-23T00:00:01Z*

NextUpdate

dateTime *2012-10-23T00:00:01Z*

DistributionPoints

URI <http://www.gns.gov.pt/NR/rdonlyres/AE2B69CF-4869-4CDC-820C-8C5C0FE1736E/0/TSLPT.xml>

1 - TSP: ECCE - State Common Certification Service Provider

TSPName

Name [en] *ECCE - State Common Certification Service Provider*

Name [pt] *ECCE - Entidade Certificadora Comum do Estado*

TSPTradeName

Name [en] *CEGER - Management Center for the Electronic Government Network*

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

PostalAddress

StreetAddress [en] *Rua Almeida Brandão, 7*

Locality [en] *Lisboa*

StateOrProvince [en] *Lisboa*

PostalCode [en] *1200-602 Lisboa*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Rua Almeida Brandão, 7*

Locality [pt] *Lisboa*

StateOrProvince [pt] *Lisboa*

PostalCode [pt] *1200-602 Lisboa*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:certificacao@ecce.gov.pt*

URI *http://www.ecce.gov.pt*

TSPInformationURI

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

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

Subject CN:	<i>ECCE</i>
Subject OU:	<i>ECEstado</i>
Subject O:	<i>SCEE</i>
Subject C:	<i>PT</i>
NotBefore	<i>Mon Jul 03 16:27:00 CEST 2006</i>
NotAfter	<i>Sat Jun 23 10:49:47 CEST 2018</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:13:1B:4B:6F:6B:24:3D:C3:ED:B9:FE:AE:F4:10:C9:73:31:0D:7C:BA:BC:1A:71:4E: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</i>
BasicConstraints	<i>IsCA: true</i>
SubjectKeyIdentifier	<i>59:0B:66:CC:FA:7B:16:98:68:0E:F6:5C:00:F3:B9:AD:E9:A6:3A:74</i>
AuthorityKeyIdentifier	<i>71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80</i>
CertificatePolicies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.ecee.gov.pt/dpc</i>
AuthorityInfoAccess	<i>https://ocsp.ecee.gov.pt</i>
CRLDistributionPoints	<i>http://crls.ecee.gov.pt/crls/ARL.crl</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2007-07-04T00:00:00Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://www.ecee.gov.pt</i>
URI	<i>[pt] http://www.ecee.gov.pt</i>
ServiceInformationExtensions	
Extension - critical=true	
Qualification Element	
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert</i>

Qualifier

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

2.16.620.1.1.1.2.10

2 - TSP: ECCC - National Identification Card Certification Service Provider

TSPName

Name [en] *ECCC - National Identification Card Certification Service Provider*

Name [pt] *ECCC - Entidade Certificadora do Cartão de Cidadão*

TSPTradeName

Name [en] *ITIJ, I.P. - Justice Information Technology Institute*

Name [pt] *ITIJ, I.P. - Instituto das Tecnologias de Informação na Justiça*

PostalAddress

StreetAddress [en] *Av. Casal Ribeiro, 16*

Locality [en] *Lisboa*

StateOrProvince [en] *Lisboa*

PostalCode [en] *1049-068 Lisboa*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Av. Casal Ribeiro, 16*

Locality [pt] *Lisboa*

StateOrProvince [pt] *Lisboa*

PostalCode [pt] *1049-068 Lisboa*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:correio@mail.itij.mj.pt*

URI *http://www.cartaodecidadao.pt/*

TSPInformationURI

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

Issuer OU:	<i>ECEstado</i>
Issuer CN:	<i>Cartão de Cidadão 001</i>
Subject C:	<i>PT</i>
Subject O:	<i>Cartão de Cidadão</i>
Subject OU:	<i>subECEstado</i>
Subject CN:	<i>EC de Assinatura Digital Qualificada do Cartão de Cidadão 0001</i>
NotBefore	<i>Mon Jan 29 22:29:39 CET 2007</i>
NotAfter	<i>Sat Mar 30 22:39:39 CET 2013</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:5A: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:87:0C: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</i>
BasicConstraints	<i>IsCA: true - Path length: 0</i>
SubjectKeyIdentifier	<i>F0:86:CB:A6:B8:F5:AF:07:F0:F9:42:BA:47:CA:90:EE:82:78:B8:15</i>
AuthorityKeyIdentifier	<i>B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E</i>
CertificatePolicies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.scee.gov.pt/pcert</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.1.2</i> <i>CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.7</i> <i>CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html</i>
CRLDistributionPoints	<i>http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_cr1001_crl.crl</i>
AuthorityInfoAccess	<i>http://ocsp.root.cartaodecidadao.pt/publico/ocsp</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2007-01-30T09:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://pki.cartaodecidadao.pt/</i>

URI *[pt]* <http://pki.cartaodecidadao.pt/>

ServiceInformationExtensions

Extension - critical=true

Qualification Element

Qualifier <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier 2.16.620.1.1.1.2.4.1.0.1.1

2.2 - Service: ECCC 2 (CA-Qualified Certificates)

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

ServiceName

Name *[en]* ECCC 2 (CA-Qualified Certificates)

Name *[pt]* ECCC 2 (EC-Certificados Qualificados)

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

Certificate fields details

Version 3

SerialNumber 2366735987959252941

CertificatePolicies

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**CRLDistributionPoints**http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl**AuthorityInfoAccess**<http://ocsp.root.cartaodecidadao.pt/publico/ocsp>**KeyUsage**

keyCertSign - cRLSign

SHA256 Cert. hash

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

ServiceStatus<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited>**StatusStartingTime**

2008-01-17T09:00:01Z

SchemeServiceDefinitionURIURI [en] <http://pki.cartaodecidadao.pt/>URI [pt] <http://pki.cartaodecidadao.pt/>**ServiceInformationExtensions**

Extension - critical=true

Qualification Element

Qualifier

<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSCSDStatusAsInCert>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

2.16.620.1.1.1.2.4.1.0.1.1

2.3 - Service: ECCC 3 (CA-Qualified Certificates)**ServiceTypeIdentifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**ServiceName**

Name [en] ECCC 3 (CA-Qualified Certificates)

Subject C:	<i>PT</i>
NotBefore	<i>Tue Feb 17 17:03:47 CET 2009</i>
NotAfter	<i>Sun Apr 19 18:13:47 CEST 2015</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:8A:E3:03:B7: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:FCE1:68:1C:7A:0C:76:74:95: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:FE: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</i>
BasicConstraints	<i>IsCA: true - Path length: 0</i>
SubjectKeyIdentifier	<i>3B:D4:87:EE:75:17:95:A8:66:CE:23:8E:E7:1E:25:19:DB:4B:23:7C</i>
AuthorityKeyIdentifier	<i>B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E</i>
CertificatePolicies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.scee.gov.pt/pcert</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.1.2</i> <i>CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.7</i> <i>CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html</i>
CRLDistributionPoints	<i>http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_cr1001_crl.crl</i>
AuthorityInfoAccess	<i>http://ocsp.root.cartaodecidadao.pt/publico/ocsp</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2009-02-19T09:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://pki.cartaodecidadao.pt/</i>
URI	<i>[pt] http://pki.cartaodecidadao.pt/</i>
<u>ServiceInformationExtensions</u>	
Extension - critical=true	
<u>Qualification Element</u>	
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert</i>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

2.16.620.1.1.1.2.4.1.0.1.1

2.4 - Service: ECCC 4 (CA-Qualified Certificates)

ServiceTypeIdentifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

ServiceName

Name [*en*] *ECCC 4 (CA-Qualified Certificates)*

Name [*pt*] *ECCC 4 (EC-Certificados Qualificados)*

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*

Certificate fields details

Version *3*

SerialNumber *2016756349056267015*

X509Certificate

```
-----BEGIN CERTIFICATE-----
MIHGCjCCBOKgAwIBAgIIg/z1NigDMwewDQYJKoZIhvcNAQEFBQAwYQxiDAEgNBAMMF0NhenTD
o28gZGUGQ2lkYWYwMjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
c3RlbnVlZGUGQ2lkYWYwMjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
UFQwHhcNMTEwMzEzMTQzMTUwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEw
BAoMEQhcnTDo28gZGUGQ2lkYWYwMjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
QyBkZSBBCiNpbmF0dXJhcnRzZjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
byAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
nhanMCDrcCjOxd893S7ygfX08Ghsnc4DhYTXaD4Sx2sp8R5MjylFvaBbYgybYVmm3Jvflv
3mYryzQFJopVqnKQ3YfuGjzmHkpr7E6axmoxDNpj4nPmSHUx6DQYQiyiGMfbkXlu6TbqBUrxG
mEWBvJUTAvLuK-dehN8WwXnN1CipcnVP=FFWwyyeF8qoN9bvN2APwuHbblcD9icVnWcYj4q+WT9
C0wO3qLPSnkibXlmXOCs4wVcTLE9Xk7szZG5FfWdPwvJ0j2HXfkbZsbkpxmmMFXPdlfBZ
abv4EkykIplOIDAQABo4ChDCCAgAwEgYDVDR0TARQIBAgwBqEBwIBADAQOBgNVHQ8BAQ8BAQ
AQYwHQYDVROBBYFQovXivBw9jk0MN/B04bdJnpWm0MB8GA1UdIwQYMBAfLjNmLLPRWrbkVv
O2P7jain4W2eMIIBeQYDVROgBIBaDCCAQWQwMgYEVROgADAQMGCCGAQUFBwIFhcodHRwOi8v
d3d5LnNjZWUz292LnB0L3BjZXJ0MjYyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
gallAaB0AHQAcaA6AC8ALwBwAGsAaQAAGMAyQBvAHQAyQBvAGQAyQBvAGQAyQBvAGQAyQBvAGQA
cABOAC8AcABIAAGIAb4BpAGMAbwAAIAAbwBAAGkAdABpAGMAyQBvAGQAyQBvAGQAyQBvAGQAyQBv
AGIAlQBIAQMAxwBjAGkAZAABGAQAYQBvAFRAyQBvAHMAcQBvAHMAcQBvAHMAcQBvAHMAcQBv
AQEBAGQABzBYMFYGCCGAQUFBwIFBkpodHRwOi8vc3RlbnVlZGUGQ2lkYWYwMjYyODIyMDA5
aWVnL3BjZXJ0MjYyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
hkZodHRwOi8vc3RlbnVlZGUGQ2lkYWYwMjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAw
X2NybDAwMjYyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
cm9udC5yY3RlbnVlZGUGQ2lkYWYwMjYyODIyMDA5MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
j4w+OSNDagVa=7ZEVS8POVghWg8BY5V79L.RmvezZ1kRahh6B5yOoz2pl4Cns5qUrhkyD3qvN
izMzGjFfPknbphdnDRh6fzYLX37eF0jJ3ike/V6yQsIHj5ymZ9egE5EjemKHK3Y9TpuJc
rFCCREBWE0Hm4YC6s7Rsz4x6y60Jc4B8I+9KlvuZhesOUiY+nnTlw5UorPDQUBAmHcyemEpMv5
EtpxoD9gUlEszj17wDMdgcMOCbTZyFribBhEGEYztZ2cbgQhKz5ANSysm4MB0C746YwKwQY4i
9/889sLTJyHk6Gx4+aICMNY7awpLpWQymwMippBk2smg9DRK8GZZikcyYoLFFG3uMkKv1
dsHm2aY5Hoadp2nfo10YAcosxy174zAdEUdA3PujiVr=2lB9KTVAI4d4SMEShJZCGXpCml_e0
PdY8Mump6Bw3T8yndV3V167RPlvl6Solrh0VB03LwFavGDUWkkKhp52mAlGWOK14zCDBRRP
HB9fW9B7dw/SwwGgTlKUS/nTId+zeE9Y2LWReiaEhw8JovexKTQ2ksFXnunUJXoHdKm4Yp5d
aoICPr55bwn0SKOj7ZOIHsorXeXAxopvRjpdLjh9aq0C2pYlZKtkHu5hyv9St+Usalj=Dfg=
-----END CERTIFICATE-----
```

SigAlg *SHA1withRSA*

SigAlgOID	1.2.840.113549.1.1.5
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
NotBefore	Tue Mar 16 15:31:14 CET 2010
NotAfter	Sun May 15 16:41:14 CEST 2016
PublicKey	30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:B3:73:B4:7C:E7:B4:3E:2C:55:BE:50:4F:51:F8:52:0F:04:9E:19:5A:9C:0: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:AA:C4:33:69:8F:89:CF:99:28:9F:51:7E:83:41:84:22:AB:28:86:31:FE:A4:5E:5B:B A:4D:BA:81:52:BC:46:98:45:81:BC:95:13:02:F2:EE:2B:47:5E:84:DF:16:38: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:0 F: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:08:D0:FE:3D:36:1D:72: 5F:CS: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
BasicConstraints	IsCA: true - Path length: 0
SubjectKeyIdentifier	EA:A7:BD:72:2F:07:0F:63:93:43:0D:FC:1D:38:6D:D2:67:A5:69:B4
AuthorityKeyIdentifier	B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E
CertificatePolicies	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
CRLDistributionPoints	http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_cr1001_crl.crl
AuthorityInfoAccess	http://ocsp.root.cartaodecidadao.pt/publico/ocsp
KeyUsage	keyCertSign - cRLSign
SHA256 Cert. hash	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
ServiceStatus	http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited

StatusStartingTime 2010-03-16T00:00:00Z

SchemeServiceDefinitionURI

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

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

ServiceInformationExtensions

Extension - critical=true

Qualification Element

Qualifier http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert

Criteria list assert=all

PolicyIdentifier nodes:

Identifier 2.16.620.1.1.1.2.4.1.0.1.1

2.5 - Service: ECCC 5 (CA-Qualified Certificates)

ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC

ServiceName

Name [en] ECCC 5 (CA-Qualified Certificates)

Name [pt] ECCC 5 (EC-Certificados Qualificados)

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

Certificate fields details

Version 3

SerialNumber 341054323862704202

X509Certificate

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

MIIHGCBOkGAWIBAgIIBLurG7ykeEowDOYJKoZihvcNAQEFBQAwgYQxIDAeBgNVBAMMF0Nhcnd...
3RIBWEGZGUgQ2VudGhmaWNhW6D28gRWxY3RyW7NuuWNhGRVIEVzdGFkbnZELMkGA1UEBHMCMC...

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

SigAlg

SHA1withRSA

SigAlgOID

1.2.840.113549.1.1.5

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

NotBefore

Tue Apr 05 16:55:47 CEST 2011

NotAfter

Sun Jun 04 17:05:47 CEST 2017

PublicKey

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:02:07:9A:47:29:6B:E7:4B:D0:B4:0D:00...

BasicConstraints

IsCA: true - Path length: 0

SubjectKeyIdentifier

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

AuthorityKeyIdentifier

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

CertificatePolicies

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**CRLDistributionPoints**http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.crl**AuthorityInfoAccess**<http://ocsp.root.cartaodecidadao.pt/publico/ocsp>**KeyUsage**

keyCertSign - cRLSign

SHA256 Cert. hash

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

ServiceStatus<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited>**StatusStartingTime**

2011-04-05T00:00:00Z

SchemeServiceDefinitionURIURI [en] <http://pki.cartaodecidadao.pt/>URI [pt] <http://pki.cartaodecidadao.pt/>**ServiceInformationExtensions**

Extension - critical=true

Qualification ElementQualifier <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier 2.16.620.1.1.1.2.4.1.0.1.1

2.6 - Service: ECCC 6 (CA-Qualified Certificates)**ServiceTypeIdentifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**ServiceName**

Name [en] ECCC 6 (CA-Qualified Certificates)

Subject C:	<i>PT</i>
NotBefore	<i>Tue Feb 28 13:57:21 CET 2012</i>
NotAfter	<i>Sun Apr 29 15:07:21 CEST 2018</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:82:3C:75:ED:41:88:49:09:50: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:B7:30: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</i>
BasicConstraints	<i>IsCA: true - Path length: 0</i>
SubjectKeyIdentifier	<i>97:95:84:45:B6:B6:63:B9:B4:F6:3D:9D:ED:FB:B7:21:9E:84:E5:6B</i>
AuthorityKeyIdentifier	<i>B2:67:30:B2:CF:45:6A:E3:91:B5:6F:3B:63:FB:8D:A8:A7:E1:6D:9E</i>
CertificatePolicies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.scee.gov.pt/pcert</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.1.2</i> <i>CPS text: [http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assq_pc.html]</i> <i>Policy OID: 2.16.620.1.1.1.2.4.0.7</i> <i>CPS pointer: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.html</i>
CRLDistributionPoints	<i>http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_cr1001_crl.crl</i>
AuthorityInfoAccess	<i>http://ocsp.root.cartaodecidadao.pt/publico/ocsp</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2012-02-28T00:00:00Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://pki.cartaodecidadao.pt/</i>
URI	<i>[pt] http://pki.cartaodecidadao.pt/</i>
<u>ServiceInformationExtensions</u>	
Extension - critical=true	
<u>Qualification Element</u>	
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert</i>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier	<i>2.16.620.1.1.1.2.4.1.0.1.1</i>
-------------------	-----------------------------------

3 - TSP: ECM Justiça - Ministry of Justice Certification Service Provider

TSPName

Name [en] *ECM Justiça - Ministry of Justice Certification Service Provider*

Name [pt] *ECM Justiça - Entidade Certificadora do Ministério da Justiça*

TSPTradeName

Name [en] *ITIJ, I.P. - Justice Information Technology Institute*

Name [pt] *ITIJ, I.P. - Instituto das Tecnologias de Informação na Justiça*

PostalAddress

StreetAddress [en] *Av. Casal Ribeiro, 16*

Locality [en] *Lisboa*

StateOrProvince [en] *Lisboa*

PostalCode [en] *1049-068 Lisboa*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Av. Casal Ribeiro, 16*

Locality [pt] *Lisboa*

StateOrProvince [pt] *Lisboa*

PostalCode [pt] *1049-068 Lisboa*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:correio@mail.itij.mj.pt*

URI *http://www.itij.mj.pt*

TSPInformationURI

URI [en] *http://icp.itij.mj.pt*

3.1 - Service: ECM Justiça (CA-Qualified Certificates)

ServiceTypeIdentifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

ServiceName

Name *[en] ECM Justiça (CA-Qualified Certificates)*

Name *[pt] ECM Justiça (EC-Certificados Qualificados)*

Service digital identities

X509SubjectName

Subject CN: *Justica*

Subject OU: *ECEstado*

Subject O: *SCEE*

Subject C: *PT*

Certificate fields details

Version *3*

SerialNumber *81644356235450830107306268853290411122*

X509Certificate

```
-----BEGIN CERTIFICATE-----
MIIGDzCCA/egAwIBAgIQPWhjEHh0n5G6P8b+bAkcjANBgkqhkiG9w0BAQUFADAzMQswCQYDVQOQ
EwJQVFNMAAsGA1UECgwEU0FRFRTEVMBMGAIUEAwMRUNSW6RKN0YWRvMB4XDTAzMDkxMzA5MTI1
OVoXDTE5MDkxMzA5MTI1OVoQTElMAKGA1UEBmMUFQNDIAlBgNVBAAwMBFNDRIUAETAPBgNVBAsM
CEVDRXN0YWRvMRAsDgYDVQQDDAdkKXN0aWNBMIICiANBgkqhkiG9w0BAQEFAAOCAg8AMIICgKcK
AgEAr5bP3YChO77DDEuF72KLUGUU4QUiQnjinfaDAWIGVDeUZE5rrO19wgez497c4DgQX8g9
tPR6AIm8mgfoZcq4jEhHNoFQPL3p8wk+3lSizzHzpDop02nC9xFqAEx4bP4bs2DzrwEtxg9im
7vMMoE9uxFNRL3LbryQUoKONDzvwIuz2E43pL1/6DUj9OxQH5oKU7ndQ6v+2idf+fy+ubhS3G
ePfv8TKLmrhKu6Xdtrefy5Y9NPLueONREgVlho1GaWkngsXIBYI+2ycAp12jtV87JqmWbEZF1
zIaxGeANdwyqmCs8RdlimeUES14ERQkaW4M2sbxrofgcAwEByIQPLh3YyA81s0OimN1
dQc7ZINq4OXBg32lyXTix9Vtxy22vp9gDtVnizw3LpbiVvR0qk+RepMzw8D4x2mr56vBw/w
gPuty9HPg3S2KyBGL957Ka+uz8+JV+S3IKOuWHzWa16CDOnRppNsZJVC/6HFnzj2/dlx05v
gPRxOuGmwP+mtEUKaAh5bCNW1oOu50rc5d+yRtSjeuBLQjCz50Ksh9gBISZnp6kmToul6Oa/OG
EsbxogOTUjGVHucOWzooO9hSnnJQh5DxwsALhC7otQYkiBGZi9wzupb9po+Esg0B+ovkQd
oDUCAwEAaAOCAQ8wggELMA8GA1UdEwEBwQFMAMBAA8wHQYDVROBBYEF12oMg0trQ9W7pXP9WO1f
qOr5ALMBGAIUdlwQYMBaAFHP/Nd71d5FHRKc4ZKucvCps4+AMAAGAIUdDwEBwQEAWBBY7
BgNVHSAENDAYMDAGBFUdIAAwKDAmBegrBgEFBQCARyaaHR0cDovL3d3dy51Y2VlLmdvd5tdC9k
cGMwNAYIKwYBBQUHAQEEDAmCQCQCcSQAQUFBAhhdhHRwezovL29jc3AuZWlnZS5nb3YucHQw
NQYDVROBBGAIUdAgoCigJoYkAHR0cDovL2NybmMuZWlnZS5nb3YucHQwY3Jscy9BUkwwY3JsMA0G
CSqGSIb3DQEBBQUAA4ICAQAx66b18sA3b763563tx2BfinzjwEfyfBMT28SLHLy3TApCvzOqhrf
hyLHNKqYKSP7z74U8J0bAnkDVx6Yks0RbvYEHuZQ7IDej194S1vargp6i2MqNihSL1QeVAO
QfXuWmQ0hNqjly9+X6CWrmORal3mlf8mgfPzXhuBC6hKkZZg7pWHEEzygRk+0MY3ErvEh
Skst8dyBAqXTZJuWBgOufOQwHn77cOgp1A9GAg0l35Kf4O1532YAQgErerFXmoAVON/EB
/VzPdNjMPLUSgoszV0ErInds01eSjAntuFvxtm75YV72iO2Jxi1CVX+i7+IbluSjN+cpuk9uO
ht13fwEp7hEEVcNxy4wgAilcTdsU43TKvLwbsa/6eNS873skIM++NP7517rN73YE/7m7HOvfp8
3RUgBbCjC3eg4YqaFYKpbywCegiM1VDCHUGXORhkmJEKtrt2A6MB+C/3v+/C3hQQOVfSb9luKMU
CIW3yISW2kd5owZ2F+VnQY5sh6rsuNEIdYV6n5EKPTT6FVeIPB+xs8ortfMSzeuB9hg22zgiE
BkjmFdvdpRgZQuLdx8pwTbdq/bILUBsgV4BIX2YAEtzjVA8/Jyc2kShSHNRFArsmSGSJJp
jPEKk5IEXORUGIGbjntz=
-----END CERTIFICATE-----
```

SigAlg *SHA1withRSA*

SigAlgOID *1.2.840.113549.1.1.5*

Issuer CN: *ECRaizEstado*

Issuer O: *SCEE*

Issuer C: *PT*

Subject CN:	<i>Justica</i>
Subject OU:	<i>ECEstado</i>
Subject O:	<i>SCEE</i>
Subject C:	<i>PT</i>
NotBefore	<i>Thu Sep 13 11:12:59 CEST 2007</i>
NotAfter	<i>Fri Sep 13 11:12:59 CEST 2019</i>
PublicKey	<i>30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00: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:68:29:4E: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:B1:7B: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:ES:75:07:BB:67:12:0D:AB:83:97:06:0D:F6:93:25:D3:C6:2C:7D:56:DC:72:B7:68: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:CS: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</i>
BasicConstraints	<i>IsCA: true</i>
SubjectKeyIdentifier	<i>BD:A8:32:0D:2B:43:D5:BB:A5:73:FD:58:ED:5F:A9:0A:DD:E6:B0:0B</i>
AuthorityKeyIdentifier	<i>71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80</i>
CertificatePolicies	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.ecee.gov.pt/dpc</i>
AuthorityInfoAccess	<i>https://ocsp.ecee.gov.pt</i>
CRLDistributionPoints	<i>http://crls.ecee.gov.pt/crls/ARL.crl</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>A7:EF:72:5D:FB:42:FE:17:F8:10:8E:5C:EA:A0:08:48:B9:D3:2B:56:56:8B:AF:59:C4:5A:88:32:CE:95:63:E4</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2007-09-14T09:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://icp.itij.mj.pt</i>
URI	<i>[pt] http://icp.itij.mj.pt</i>
ServiceInformationExtensions	
Extension - critical=true	
Qualification Element	

Qualifier

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert

Qualifier

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

2.16.620.1.1.1.2.10

4 - TSP: ECAR - Assembly of the Republic Certification Service Provider

TSPName

Name [en] *ECAR - Assembly of the Republic Certification Service Provider*

Name [pt] *ECAR - Entidade certificadora da Assembleia da Republica*

TSPTradeName

Name [en] *Assembly of the Republic*

Name [pt] *Assembleia da República*

PostalAddress

StreetAddress [en] *Palácio de S. Bento*

Locality [en] *Lisboa*

StateOrProvince [en] *Lisboa*

PostalCode [en] *1249-068 Lisboa*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Palácio de S. Bento*

Locality [pt] *Lisboa*

StateOrProvince [pt] *Lisboa*

PostalCode [pt] *1249-068 Lisboa*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:ecar.correio@ar.parlamento.pt*

URI *http://www.parlamento.pt*

TSPInformationURI

URI [en] *http://www.ecar.parlamento.pt/*

4.1 - Service: ECAR (CA-Qualified Certificates)

ServiceTypeIdentifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

ServiceName

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*

Certificate fields details

Version *3*

SerialNumber *153011951768217544694210381804578517321*

X509Certificate

```
-----BEGIN CERTIFICATE-----
MIIGDCCA/SgAwIBAgIQcx0HrEQg8JHWTP7DzOxSTANBgkqhkiG9w0BAQUFADAzMQswCOYDVQOQ
EwJQVjDENMAsGA1UECgwEU0NFRTYVMBMGAIUEAwwwMRUNSYWl6RXNOYWRwMB4XDTA3MTIwNzExNTIy
N1oXDTE5MTIwNzExNTIyN1owPjELMAkGA1UEBhMCU0QDTALBgNVBAs0BTFNDRUUmEETAPBgNVBAsT
CEVDRXNOYWRwMQ0wCwwYDQOODEwRF00FSMIIChANBgkqhkiG9w0BAQEFAAOCAg8AMITCCgKCAgEA
5yQzGup+79iU7TPh3AP65FPzjIDBciUraqdqQLxa4B5CgV2TIOK+E7E1E2J1fvcj9DC/Isaa2
C3uDo97FQkBJWoTnY/Gx/f4QyMTLGI7oELWrbQA2jVkrRd74IDbnPyX2+kh78c7hAuhLbbC5ilP2
jBd0KYXsevGpmXb+JLpmZCbEurl0j9zqPSretvDeRo/ZISGO0qTyA0wPuHP1jrffimsNFoLEu
jBd5q3i7oYbs3wxcZUacVqwn7epuuy5Plz5j3rRANxPpcidLCarlgcSeTIPFIDB08OZq1Nczj
EuU6l9KsmwEEDVedyOfcNZLKtUgmaYm95vZed3A6ns4cFKZ4DzZ0x2cleZB28mk7oOHZsM
JcNjym56tcZVCzsg48Bsr04Yua2DmWUfeW0zVdzKIKfSLmWVZgtADnDuVUrzQMXxVYUelU
aNP9GsjOm2KQWV0pHtw1uBKb9MmMfkgCHiA9e90HDK0YqEx6BAdvRRRf13VRND0z1FsKsp3zD
o53LHnqDLrkKp8Mb7q75yfcjBESIRJ80qw7Lgknoe15DTHYTC08rpYru9Y9wkwjrvulXrMQfC
aKe052C2o6GeresivWdpylchdrg8ZyZThZBOZde3B2UT6GMQbpoGri3lu4Ls2GT4IEyYD7f1W8C
AwEAAQCAQ8wggELMA8GA1UdEwEBwQFMAMBAI8wHQYDVR0OBByEFg7nTv4CDK2dnC0Lk2RZKIJ
Lgf+MB8GA1UdIwQ1MBAFHR7Nq71d3PHRKeAZCkovCpe4+AMAGA1UdDwEBwQEAwIBBjA7BGNV
HSAENDAwMDAGBGFUdIAAwKDAmbggrBgEFBQCARyaaHR0cDovL3d3dy51Y2VlLmdvdj5wdC9kcGMw
NAYIKwYBBQUHAEQEKDAMCQCcGAQUFBzABhhhdHRwczovL29jc2AuzWNlZS5nb3YucHQwNQYD
VIR0BC4wLDAqoCigJoYkaHR0cDovL2NybgMuZWZWNlZS5nb3YucHQwY3Jscy9BUkwuY3JsMA0GCsQg
Sib3DQEBBQUAA4ICAQArApE4PrW82IMVsgta+J3FzpeHYXBpveuasGxg0YpzOwnQX+8rITQIDgce
xopRqjznFCU9PeLuzpVEJG0mHrBlgp3fEgcg6YCM2kiEmEW5+4G5fpyvYgzISfSzaQ0nkWc0WIT
CWWHYclldipe87gHKSipeU1UExLEi0Rjdyo6kavC2VUPA09HmPELUI1BzrT3aIV0YVYbNRcoR
80NbaKhcXpGDDDKU02kueh50WtNRclUm708NWyJ416C68DzW5L0vBMReQQZyknMkPULVirgY4AK
8RX+80+By0zImMx3lPd15k412ioPqOw+4D4Z6Dc76Vqq/08EBISFUSRA5Y+rgsIHnq9ZBoAqr
b5ocGwP1A7DcoIXA915Y0kh0wRAOi1Ka9uwb/jip785LB7HjwMGL0Za8ox4URdlnJK4vNvgdG
8na/qCY1J9DmdeYKH3O6stvtv4IU6m+3qevM260yg+o5Pfa9IDKp6JJ/cBH/D+RozDcrulQj
4wZLRK2WesB+qSwYFD+xbgiteBr0u7Uy3W8JUGsh5L6+07HIMap61ZdaN8KVsqaAogilGdR58E
O33Ahl2EPHbrja7diz05BuEcgtDpphks5DbGILV7Hmg6c9mUR++BzVUfw9T+IVAoHbW7q80
2e0CXHvPKha7Abzda==
-----END CERTIFICATE-----
```

SigAlg *SHA1withRSA*

SigAlgOID *1.2.840.113549.1.1.5*

Issuer CN: *ECRaizEstado*

Issuer O: *SCEE*

Issuer C: *PT*

Subject CN:	ECAR
Subject OU:	ECEstado
Subject O:	SCEE
Subject C:	PT
NotBefore	Fri Dec 07 12:52:27 CET 2007
NotAfter	Sat Dec 07 12:52:27 CET 2019
PublicKey	30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00: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:33:48: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:DB: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:01:8D: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:BI: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
BasicConstraints	IsCA: true
SubjectKeyIdentifier	6E:E7:25:3B:F8:08:32:B6:76:70:B4:2C:AD:91:64:A2:09:2E:07:FE
AuthorityKeyIdentifier	71:7F:35:DE:F5:77:71:6D:1D:12:9C:E1:90:A4:BA:F0:A9:83:8F:80
CertificatePolicies	Policy OID: 2.5.29.32.0 CPS pointer: http://www.ecee.gov.pt/dpc
AuthorityInfoAccess	https://ocsp.ecee.gov.pt
CRLDistributionPoints	http://crls.ecee.gov.pt/crls/ARL.crl
KeyUsage	keyCertSign - cRLSign
SHA256 Cert. hash	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
ServiceStatus	http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited
StatusStartingTime	2007-12-08T00:00:01Z
SchemeServiceDefinitionURI	
URI	[en] http://www.ecar.parlamento.pt/
URI	[pt] http://www.ecar.parlamento.pt/
ServiceInformationExtensions	
Extension - critical=true	
Qualification Element	

Qualifier

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert

Qualifier

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

2.16.620.1.1.1.2.10

5 - TSP: MULTICERT S.A.**TSPName**

Name [en] *MULTICERT S.A.*

Name [pt] *MULTICERT S.A.*

TSPTradeName

Name [en] *MULTICERT - Serviços de Certificação Electrónica S.A.*

Name [pt] *PT:MULTICERT - Serviços de Certificação Electrónica S.A.*

PostalAddress

StreetAddress [en] *Estrada Casal do Canas, Lote 6*

Locality [en] *Alfragide*

StateOrProvince [en] *Lisboa*

PostalCode [en] *2720-092 Amadora*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Estrada Casal do Canas, Lote 6*

Locality [pt] *Alfragide*

StateOrProvince [pt] *Lisboa*

PostalCode [pt] *2720-092 Amadora*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:info@multicert.com*

URI *http://www.multicert.com*

TSPInformationURI

URI [en] *https://pki.multicert.com/index.html*

5.1 - Service: Multicert (CA-Qualified Certificates)

ServiceTypeIdentifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

ServiceName

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

Name *[pt]* *Multicert (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*

Certificate fields details

Version *3*

SerialNumber *120007005*

X509Certificate

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

```
MIIFmzCCBQSAwIBAgIEBycpXTANBgkqhkiG9w0BAQUFAADBIMQswCQYDVOQGEwJVUzEYMBYGA1UE
CMMPR1RFENvcnBvcnF0aW9uMScwJQYDVQQLEz5HVEUgQ3hZLXUlcncvzdCB7b2x1dGhvbmsiEjUu
Yy4kZiAhBgNVBAMTGFkafRSBDeWJicjRydXN0EEdsb2hucBSh290MB4XDTEASMDhwOTE3NDAA00VaX
DTE4MDgzMjE2NDAAwMlowgheCzAJBgNVBAYTAIBUMUJwQAYDVQQKDDINVLVUxLUSTINFUQgLSBTZXI2
acOnb3MgZGU2VydGlmawWnHw6fDo28gRWx1Y3Ryw7NuaWNhIFMuQ54xLzAtBgNVBAsMUkVudGll
bnRpZGFkZSBKZSBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBkZXBk
AocCAQCv8akRYT1dInFVQZ4O3k9Vc90im0YPI09s8RpiXmrfGAZD3iFXuixiZbULj0-xjAw8ia
7qd8j7V/Bly0fK1rscyDxaN3Ssy9p51HKs49w6f5gal-LharQOJE16/1PjX9fAcCGccZa
7de8Rum0FmEwmqap5b8nzNdyfLzyB2SOWCqCUIjgpP18jgU1LvwTcYsdkauBajMPlslG0fz3wRTS
X17ACbj5BESQuReFAfuEDlqO26Bjlic2vqA3jw7PdZv8h8WIXfLb9cSthBFJ49C68pafe
ugrnejocOBES+pYhl+GzyhupG6OYEG92QLraSe7AW23GLkx0NmlrzAIDXZnNxB5CgmnWbfiwN
BCdEX8SxqrBtarvF9JZEKvPMV/eQ+2muZKICeJFdUnRNnW0ESBQ3jsCwvqxtPVqk89NAjkb7
tBzLzHbQ2e/vzHUlgztsN3iz0YFIWhEervPaXBgsGDYRitVegnaAqRWH54616NXhWQgIHEfFo
sbMzultInYNg8eHscG2ndITe50igCxCn3Hjx0RcaXRKScsb4lJceQRbJ0raqUZYWLnk61E
IsdYxmpKzeFizAoxg6SjYFS3k8fwaF/KgkxU02DduR7IGW4knWng4vnbTSKUT5V2cxgDcX7
vwfupQIDAQAB4IBzCCAAswEgYDVR0TAQH/BAgwBgEB/wIBATBTBgNVHSAETDBKMEGCCSGAQQB
sT4BADA7MDkGCCGAQUFBwIwBF11odHRwOi8vY3hZLXUlcncvzdCB7b2x1dGhvbmsiEjUuMm9u
dG9veS5jZm0wDgYDVR0PAQH/BAQDAgEGMIGIBG9NVHSMFgYEwrf5pHcWdTElMAkGA1UEBhMCVVX
GDAWBgNVBAAoITD0dURSBD63jw63jhdGhvbG9uMScwJQYDVQQLEz5HVEUgQ3hZLXUlcncvzdCB7
b2x1dGhvbmsiEjUuMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9u
BD4wPDA6fDgNoY0aHR0cDovL3d3dy5wdWJsaWVudHMdH11c3QuY29L2NnaS1jaW4vQ1JMLzlwMTgy
Y2RwLm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9uMm9u
jmhHule8DQJEqw5MQMY60Bqkb46ALIErnx84IKP952PubjXewSxAsi93CpQAIUtlbv/wqD36Qc
p81ztCLrvKuWx81=ALmpBEJa+p85mMgeSy8lW45BwHlpVm5hwjWROInIapiT4HZXLj5ZPfbJv
b1M0msAD0x0nEq2/5=
```

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

SigAlg *SHA1withRSA*

SigAlgOID *1.2.840.113549.1.1.5*

Issuer CN: *GTE CyberTrust Global Root*

Issuer OU: *GTE CyberTrust Solutions, Inc.*

Issuer O: *GTE Corporation*

Issuer C:	<i>US</i>
Subject CN:	<i>MULTICERT - Entidade de Certificação 001</i>
Subject OU:	<i>Entidade de Certificação Credenciada</i>
Subject O:	<i>MULTICERT - Serviços de Certificação Electrónica S.A.</i>
Subject C:	<i>PT</i>
NotBefore	<i>Mon Feb 09 18:40:49 CET 2009</i>
NotAfter	<i>Sun Aug 12 18:40:02 CEST 2018</i>
PublicKey	<i>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:B1: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:D9:23:96:0A:AB:82:50:9A:60:3F:5F:09:81:4D:4B:BF:04:DC:62:C7:64:6A:ED: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:F0:D0:42:75:F:C4:B1:AA:B0:6D:6A:BB:CS:F4:96:44:29:5A:4C:57:F7:90: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:DD: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:33:78:56:42:DD:47:12:21:68:B2:13:53:BA:5B:88:9D:A3:6A: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</i>
BasicConstraints	<i>IsCA: true - Path length: 1</i>
CertificatePolicies	<i>Policy OID: 1.3.6.1.4.1.6334.1.0</i> <i>CPS pointer: http://cybertrust.omniroot.com/repository.cfm</i>
CRLDistributionPoints	<i>http://www.public-trust.com/cgi-bin/CRL/2018/cdp.crl</i>
SubjectKeyIdentifier	<i>7F:33:72:7F:4C:DA:34:C8:0E:A7:75:CB:2E:83:98:1B:06:B8:A6:90</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>BC:77:08:F4:E8:16:3E:43:27:4B:13:55:FA:3F:C8:A8:D5:50:16:4D:DE:68:4E:98:1C:F1:38:D1:59:DF:AD:AD</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</i>
StatusStartingTime	<i>2009-05-27T00:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] https://pki.multicert.com</i>
URI	<i>[pt] https://pki.multicert.com</i>
ServiceInformationExtensions	
Extension - critical=true	
Qualification Element	
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert</i>

Qualifier

<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier

1.3.6.1.4.1.25070.1.1.1.1.0.1.2

Service history instance n.1

ServiceTypeIdentifier

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

ServiceName

Name [en] Multicert (CA-Qualified Certificates)

Name [pt] Multicert (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

X509SKI fzNyf0zaNMgOp3XLLoOYGwa4ppA=

Certificate fields details

Version 3

SerialNumber 120007005

X509Certificate

```
-----BEGIN CERTIFICATE-----
MIIFmzCCBQSGAwIBAgIEBypXTANBgkqhkiG9w0BAQUFAADBIMQswCQYDVQQGEwJVUzEYMBYGA1UE
ChMPRIRFIENvcnBvemF0aW9uMSwwZjYyOQQLExSHVUeUgQ3liZXUlc3VzZCBTb2x1dGlvbnMsIElu
Yy4xLzAhBgNVBAMTGkdURSBDeWJleRydXN0IEsh2hbCBsb290MB4XDTA5MDIwOTE3NDAAOVoX
DTE=MIIDgXMFJENDAwMlowghexCzAIBGNVBAYTAIBUMUWUQAAYDVOQKDDINVLXUSUNFUJQGLSBTZXJ2
ac0h3MgZGUgQ2YyYdGmaWNBw6iDo28gRWaY3Ryw7NaaWNhIFMuOS4kLzAtEgNVBASMKVudGik
YWRUIGRiENlenRpzmliYc0mw6NviENyZWRlbnNpYWRhMTMwMQYDVQDDCpNVUxUSUNFUJQGLSBF
bnRlZGZlZSBKZSBkZDZlOaWZpY2HDp8OjbyAwMDEwggIiMA0GCSCGQSB3DQEBAAUAA4ICDAwAggIK
A0CAQCVSakRYT1dNnFVQZ4O3k9Vc90fm0YPI09s8tpiXmrFGAzD3iFXUxiZbULU0+xjAw8ia
7qdJ7V/B1y0/cK1rscyDxxN3sqy9p5f1HKy4/vq6f5gal=LbarQOIE16/PljX9FaCfGecZa
7dc8Rum0FmEwmq5b8nZNdylgyB2SOWCquCUIpgP18gU1lvwTcYsdkauBajMPISG0Fzt5wRTS
X17ACby5IcsQmReFAfueDlq20eBlilc2yqA3w7IzVdh88WXLlB99cSbfBF49C68paie
ugrncjocOBE5+pYbl+GzyhupG6OYEG92QLrauSe7AW23GLkx0BnmlrzAIDXznNRB5CgmnWBfwN
BCdXSSXqrBtarvF9IZEKVPmV/eQ+2muZKICeJfUnRnNw0ESBQ0jsCwqxxtPvqk89NAjkb7
ttBzUzHbQ2e/vzHUgzzfS3iz0YFIWhtEervPaXBqsGDYRitVeg/nAaQRWHS4616NXhWQg1HEiFo
shMzululYNqu8eHscG52ndIFPc5GigCxcn3Hjx0Ra3aXRSCsb4JjCQRbilOraqUizyWLnk61E
IsdYxmpKzeFzAoXig6sYfS3k8fwaF/KghU02DduR7IGW4knWng4vnb1SKU7SV2cxgDAX7
vwfupQIDAQAAB4BzCCAASwEgYDVRR0TAQHBAQwEgEBwIBATBTEgNVISAETDBKMEgGCCSAAQOB
s14BADA7MDKGCSCGAUFBw1BF11odHRwOi8vY3liZXUlc3VzZCB3bW5pcm9vdC5jb20vcnVwb3Np
dG9yeS5jZm0wDgYDVROPAQHBAQDAgEGMIGIBGNVHSMegYewf65pHewdTELMAGAIUEBhMCVVMx
GDAWBgNVBAAoTD0dURSBDb3Jwb3JhdGlvbHJENmCUGA1UECXMURIRFIEN5YmVvYVh1c3QgU29sdXRp
b25zLlCBjbmMuMSMwIQYDVQDExpHVEUgQ3liZXUlc3VzZCBHbG9YwWgUm9vdllCAaUwRQYDVR0f
BD4wPDA6oDgNoY0aHR0cDovL3d3dy5ydWJsaWwudHJ1c3QuY29uL2NaS1iaW4wQ1JMLzlwMTgY
Y2RwLmNybDAdBgNVHQEFQGUzNvY29zaNMGOp3XLLoOYGwa4ppAwDQYIKoZIbveNAQEFBQADgYEA
jmhHJue8DQIEagw5MQMY60Bqkb46ALIErnx84kP952PubiXewSXAs193CpQAIFulib/wqD36Qc
8Q8IzClrKuWx8l=ALmpBEJa=p85mMgeS8y81W45BwHlpVm5hwjWROlnApiT4HZXLj5ZPthbJv
b1M0msAD0x0nElq2/Is=
-----END CERTIFICATE-----
```

SigAlg	<i>SHA1withRSA</i>
SigAlgOID	<i>1.2.840.113549.1.1.5</i>
Issuer CN:	<i>GTE CyberTrust Global Root</i>
Issuer OU:	<i>GTE CyberTrust Solutions, Inc.</i>
Issuer O:	<i>GTE Corporation</i>
Issuer C:	<i>US</i>
Subject CN:	<i>MULTICERT - Entidade de Certificação 001</i>
Subject OU:	<i>Entidade de Certificação Credenciada</i>
Subject O:	<i>MULTICERT - Serviços de Certificação Electrónica S.A.</i>
Subject C:	<i>PT</i>
NotBefore	<i>Mon Feb 09 18:40:49 CET 2009</i>
NotAfter	<i>Sun Aug 12 18:40:02 CEST 2018</i>
PublicKey	<i>30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:95:F1:A9:11:61:3D:5D:7C:D9:C5:55:06:78:3B:79:3D:55:CF:74:7E:6D:18:3D:F3:BD:B1:FF:2D:A6:25:E6:AC:51:80:CC:3D:E2:15:75:31:89:96:DE: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:D9:23:96:0A:AB:82:50:9A:60:3F:5E:09:81:4D:4B:BF:04:DC:62:C7:94:6A:E0:5A:8C:C3:C8:B2:51:B4:17:37:F7:CF: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:C4:B1:AA:B0:6D:6A:BB:C5:F4:96:44:29:5A:4C:57:F7:90: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:DD: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:AS:CI:AA:CI: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:CI: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</i>
BasicConstraints	<i>IsCA: true - Path length: 1</i>
CertificatePolicies	<i>Policy OID: 1.3.6.1.4.1.6334.1.0</i> <i>CPS pointer: http://cybertrust.omnirroot.com/repository.cfm</i>
CRLDistributionPoints	<i>http://www.public-trust.com/cgi-bin/CRL/2018/cdp.crl</i>
SubjectKeyIdentifier	<i>7F:33:72:7F:4C:DA:34:C8:0E:A7:75:CB:2E:83:98:1B:06:B8:A6:90</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>BC:77:08:F4:E8:16:3E:43:27:4B:13:55:FA:3F:C8:A8:D5:50:16:4D:DE:68:4E:98:1C:F1:38:D1:59:DF:AD:AD</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision</i>
StatusStartingTime	<i>2009-02-10T00:00:01Z</i>

6 - TSP: British Telecom

TSPName

Name [en] *British Telecom*

Name [pt] *British Telecom*

TSPTradeName

Name [en] *British Telecommunications plc*

Name [pt] *British Telecommunications plc*

PostalAddress

StreetAddress [en] *BT Trust Service, P.O. Box 641,*

Locality [en] *Cardiff*

StateOrProvince [en] *Cardiff*

PostalCode [en] *CF1 1YL*

CountryName [en] *UK*

PostalAddress

StreetAddress [pt] *BT Trust Service, P.O. Box 641,*

Locality [pt] *Cardiff*

StateOrProvince [pt] *Cardiff*

PostalCode [pt] *CF1 1YL*

CountryName [pt] *UK*

ElectronicAddress

URI *mailto:support@trustwise.com*

TSPInformationURI

URI [en] *http://www.globalservices.bt.com*

6.1 - Service: BT/DigitalSign (CA-Qualified Certificates)

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*

NotBefore: *Thu Aug 14 02:00:00 CEST 2008*

NotAfter: *Fri Aug 14 01:59:59 CEST 2015*

PublicKey:
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:85:57:8C: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:83:DF:33:6B:C5:B3:72:6C:BE:3E:9F:32:5F:6C:C8:0C:76:68:E1:DA: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

BasicConstraints: *IsCA: true - Path length: 0*

CertificatePolicies:
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>]

CRLDistributionPoints: *<http://onsitecrl.trustwise.com/BTClass2CA-G2.crl>*

SubjectKeyIdentifier: *A1:83:72:1A:3D:9E:9F:22:E6:DE:82:C7:90:C9:51:01:FF:83:29:6B*

AuthorityKeyIdentifier: *6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4*

KeyUsage: *keyCertSign - cRLSign*

SHA256 Cert. hash: *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*

ServiceStatus: *<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited>*

StatusStartingTime: *2009-04-22T23:00:01Z*

6.2 - Service: DigitalSign (LRA in Portugal)

ServiceTypeIdentifier<http://uri.etsi.org/TrstSvc/Svctype/RA>**ServiceName**

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*

Certificate fields details

Version 3

SerialNumber 129306905431624887482487812001666232948

X509Certificate

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

MIIFFDCCBHGAWlBAGlQYUcap4Wb5VWhWJkplyTydDANBqkqkiG9w0BAQUFADB0MqswCOYDVOQG
 EwJHQEnMCUGA1UEChMeQnJpdGlzaCBUZWx1Y29ibXVuaWNhdGlvbnMgeGsjMR8wHQYDVQQLExZW
 ZXJpU2lnbiBUcnVzdCB0ZXR3b3JrMRswGQYDVQQDEJCVCBDbGFzcyAyIENBIC0gRzlwHhcNMjgw
 ODEMDAwMDAwWhcNMjUwODEzMTU5WjCCATxGzAJBgNVBAYTAkdCMScwJQYDVQQKEx5Ccmll
 aXNoIEFibGVyY21idW5pY290aW9uecyBwbGMApA8BgNVBAsTlnx5SQAIEpZ20YVWxTaWduEjE
 cnRpZmlYYSRvcmlEgRGlbnXRhbCAoU0FQIMDcwMTU4NTEpMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVz
 dCB0ZXR3b3JrMTwwOgYDVQQLEZnUzXJlcyBvZiB1c2UgYXQgaHR0cHM6Ly93dScudHI1c3R3aXNl
 LmNvbS9ycGEGKGMpMDgXNTAzBgNVBAsTLENsYXNzdlJlTGwFuYWdlZCB0S0kgSW5kaXpZHVhbCBT
 dWJzY3pYmVyiENBMSQwlgYDVQQDExtVC9EaWdpdGFsU2lnbiBRdWFSaWZpZWQgQ0EwggEiMA0G
 CsqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ+zFQINPEI3EQtTaBQDNLbBZIHIM30wExctq/ZuH
 YHhL0PV8TlxzqVaLjYjvCOVV+LhhNpmRlnZGyO9pyCbo0aapOwVWx9L-E3-4SwrKOleFYCINPrd
 Ryd3aBGAMVCuaIzcutolxqJpTczHLv4pi70eNw9zIRiXDMbz+o9LchNaf3HFrTp7mTaAg5i8Q
 Mcyj+VcMDsUQF+Fajl0vFAdltDEibClhixptE4xYpIMAR0S16D3zNrxNybL4+nzJfBmGmdmjh
 CqQgILBge6hokqBf4H9aLbmrNfwTmfY1uKEDZuXZpS2TvASozZAlhOTcs9oRuYXxLGEAgMB
 AAGiggfMIHWDASBGNVHRMBAIECDAGAQH/AgEAMHIGA1UdIARrMGkwZwYlYlZlA1Yb4RQEHFfw
 WDApBgggBgEFBQcCARydaHR0cHM6Ly93dScudHI1c3R3aXNlLnVhbGMApA8BgNVBAsTlnx5SQA
 HkodiHR0cHM6Ly93dScudHI1c3R3aXNlLnVhbGMApA8BgNVBAsTlnx5SQAIEpZ20YVWxTaWduEjE
 L29ue2l0ZWVybC50cnVzdHdpc2UuY291L0U02hc3MyQ0EIRzluY3IsMA4GA1UdDwEBwQEAsIB
 BJA8BgIghkgBhvCAQEEBAMCAQYwKAYDVR0RCBwH6QdMBsxGTAxBGNVBAMTEGJ0MjA0OGMyUHVI
 MS0yMDIwHQYDVROBBYEFKGDcho9np8i56CzSDUQH/gYhMB8GA1UdIwQYMBaAFG7BXz93s3m
 2wjK09I0D07V7P0MA0GCSqGSIb3DQEBAQUAA4IBAQAAMK5Zsjsx5bduPHMp1thpGHj7PGbXW3To
 Yk8n2C9QLX9KZ4IIZ1sUXmpX+uf31/bs6KImdwofMcejNw9W28vszeC+EmrYATneAQW3Cq
 5yL9lyKd65gmuuqpc8q7b7B0GJdibfsgX6MxvC8evmOybr1AYOramCwVHaTQmCJ+Xp4IPyblj
 naWWxQkxcARUd4QjhbGSCbYac9nqrFYaks2UIYNwcl1ee7hXcWbEqNYG4k2W5Eq7NYcArEl.dnw
 hLC8h0K0mXgqaCbQ60aRbLrc1Xe+B72MFXPKsqEILPsTzzYy8a84Iq9VhDv/qnydMMBJUX6esj
 eL2v

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

SigAlg *SHA1withRSA*

SigAlgOID *1.2.840.113549.1.1.5*

Issuer CN: *BT Class 2 CA - G2*

Issuer OU: *VeriSign Trust Network*

Issuer O:	<i>British Telecommunications plc</i>
Issuer C:	<i>GB</i>
Subject CN:	<i>BT/DigitalSign Qualified CA</i>
Subject OU:	<i>Class 2 Managed PKI Individual Subscriber CA</i>
Subject OU:	<i>Terms of use at https://www.trustwise.com/rpa (c)08</i>
Subject OU:	<i>VeriSign Trust Network</i>
Subject OU:	<i>LRA - DigitalSign Certificadora Digital (PT507015851)</i>
Subject O:	<i>British Telecommunications plc</i>
Subject C:	<i>GB</i>
NotBefore	<i>Thu Aug 14 02:00:00 CEST 2008</i>
NotAfter	<i>Fri Aug 14 01:59:59 CEST 2015</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:85:57:8C:0E:C3:10:17: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:83:DF:33:6B:C5:B3:72:6C:BE:3E:9F:32:5F:6C:C8:0C:76:68:E1:DA: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</i>
BasicConstraints	<i>IsCA: true - Path length: 0</i>
CertificatePolicies	<i>Policy OID: 2.16.840.1.113733.1.7.23.2</i> <i>CPS pointer: https://www.trustwise.com/cps</i> <i>CPS text: [https://www.trustwise.com/rpa]</i>
CRLDistributionPoints	<i>http://onsitecrl.trustwise.com/BTClass2CA-G2.crl</i>
SubjectKeyIdentifier	<i>A1:83:72:1A:3D:9E:9F:22:E6:DE:82:C7:90:C9:51:01:FF:83:29:6B</i>
AuthorityKeyIdentifier	<i>6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision</i>
StatusStartingTime	<i>2009-04-22T23:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://www.digitalsign.pt</i>

7 - TSP: DigitalSign**TSPName**

Name [en] *DigitalSign*

Name [pt] *DigitalSign*

TSPTradeName

Name [en] *DigitalSign - Certificadora Digital, S.A.*

Name [pt] *DigitalSign - Certificadora Digital, S.A.*

PostalAddress

StreetAddress [en] *Largo Pe. Bernardino Ribeiro Fernandes, 26*

Locality [en] *Nespereira - Guimarães*

StateOrProvince [en] *Guimarães*

PostalCode [en] *4835-489 Nespereira - Guimarães*

CountryName [en] *PT*

PostalAddress

StreetAddress [pt] *Largo Pe. Bernardino Ribeiro Fernandes, 26*

Locality [pt] *Nespereira - Guimarães*

StateOrProvince [pt] *Guimarães*

PostalCode [pt] *4835-489 Nespereira - Guimarães*

CountryName [pt] *PT*

ElectronicAddress

URI *mailto:geral@digitalsign.pt*

URI *http://www.digitalsign.pt*

TSPInformationURI

URI [en] *http://www.digitalsign.pt/ECDIGITALSIGN/cps/*

Subject OU:	<i>VeriSign Trust Network</i>
Subject O:	<i>DigitalSign - Certificadora Digital</i>
Subject C:	<i>PT</i>
NotBefore	<i>Fri Jun 13 02:00:00 CEST 2008</i>
NotAfter	<i>Tue Jun 12 01:59:59 CEST 2018</i>
PublicKey	<i>30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:ES: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:F5:86:07:9B: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:5A: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</i>
BasicConstraints	<i>IsCA: true - Path length: 0</i>
SubjectKeyIdentifier	<i>BB:1F:44:1D:EC:22:F7:A0:F5:2B:F2:8F:23:90:59:F8:B2:99:20:AA</i>
CertificatePolicies	<i>Policy OID: 2.16.840.1.113733.1.7.23.2</i> <i>CPS pointer: https://www.trustwise.com/cps</i> <i>CPS text: [https://www.trustwise.com/rpa]</i>
CRLDistributionPoints	<i>http://onsitecrl.trustwise.com/BTClass2CA-G2.crl</i>
AuthorityKeyIdentifier	<i>6A:BB:05:7C:FD:DE:CD:E6:DB:08:CA:3B:D9:4E:24:3D:3B:57:B3:F4</i>
KeyUsage	<i>keyCertSign - cRLSign</i>
SHA256 Cert. hash	<i>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</i>
ServiceStatus	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision</i>
StatusStartingTime	<i>20011-12-19T00:00:01Z</i>
SchemeServiceDefinitionURI	
URI	<i>[en] http://www.digitalsign.pt/ECDIGITALSIGN/cps/</i>
URI	<i>[pt] http://www.digitalsign.pt/ECDIGITALSIGN/cps/</i>
ServiceInformationExtensions	
Extension - critical=true	
Qualification Element	
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert</i>
Qualifier	<i>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson</i>

Criteria list assert=all

PolicyIdentifier nodes:

Identifier	<i>2.16.840.1.113733.1.7.44.2</i>
-------------------	-----------------------------------

BasicConstraints	<i>IsCA: false</i>
ExtendedKeyUsage	<i>id_kp_emailProtection</i>
SubjectKeyIdentifier	<i>C5:DC:BD:8A:2A:BC:57:53:82:33:D0:F4:6F:82:C5:6D:89:20:EF:D4</i>
AuthorityKeyIdentifier	<i>59:0B:66:CC:FA:7B:16:98:68:0E:F6:5C:00:F3:B9:AD:E9:A6:3A:74</i>
CertificatePolicies	<i>Policy OID: 2.16.620.1.1.1.2.10</i> <i>CPS pointer: http://www.ecce.gov.pt/dpc</i> <i>CPS text: [O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito]</i>
QCStatements - crit. = false	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_QcSSCD</i>
CRLDistributionPoints	<i>http://crls.ecce.gov.pt/crls/crl.crl</i> <i>http://crls.ecce.gov.pt/crls/crl.crl</i>
KeyUsage	<i>nonRepudiation</i>
SHA256 Cert. hash	<i>C2:A4:62:45:42:2E:7D:1C:7C:CC:9F:51:FB:DD:EB:03:B5:F4:09:A2:DC:22:54:71:9F:2F:F1:3B:31:BD:91:03</i>