Belgique/België (Belgium): Trusted List

Scheme name

BE: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.

Legal Notice

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.

Scheme territory	BE
Scheme status determination approach	EUappropriate
Scheme type community rules	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon http://uri.etsi.org/TrstSvc/TrustedList/schemerules/BE
Issue date	2018-09-12T00:00:00.000Z
Next update	2019-03-12T00:00:00.000Z
Historical information period	65535 days
Sequence number	38
Scheme information URIs	https://tsl.belgium.be/

Scheme Operator

Scheme operator name	FOD Economie, KMO, Middenstand en Energie - Kwaliteit en Veiligheid
Scheme operator street address	NG III - Koning Albert II-laan 16
Scheme operator postal code	1000
Scheme operator locality	Brussels
Scheme operator state	Brussels
Scheme operator country	BE
Scheme operator contact	http://economie.fgov.be mailto:be.sign@economie.fgov.be

Trust Service Providers

Certipost n.v./s.a.

Service provider trade name	VATBE-0475396406
Information URI	http://repository.eid.belgium.be http://www.certipost.be/dpsolutions/en/e-certificates-legal-info.html
Service provider street address	Muntcentrum
Service provider postal code	1000
Service provider locality	Brussels
Service provider state	Brussels
Service provider country	BE

CN=Belgium Root CA, C=BE

Type	CA/QC
Status	withdrawn
Status starting time	2016-09-06T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	11702928888893786435059652017684464596 8
Signature algorithm	SHA1withRSA
Issuer	CN=Belgium Root CA, C=BE
Valid from	Sun Jan 26 23:00:00 UTC 2003
Valid to	Sun Jan 26 23:00:00 UTC 2014
Subject	CN=Belgium Root CA, C=BE
Public key	Sun RSA public key, 2048 bits modulus: 25327272471742424753108761113025515413507712904874083939907073553139389403581555633427000903307438065008396155423372038139338001129228397387437566169146147569101132153735147576372578550015244598849082833749686618262398710652224019389731334957158067691632442561241462450868417538609485432931629806056877222374520561111218990450541853348409938502314444513897535102557574950367954722638103130021380872795033334967224942002004934838812373471384411526579026650775354589375802255665011941485467556333747329602589496041615986077417544850696324111877604954193498318303560891627721798430948172071644141969017225065301229219951 public exponent: 65537
Subject key identifier	10f00c569b61ea573ab635976d9fddb9148edbe6
Authority key identifier	10f00c569b61ea573ab635976d9fddb9148edbe6
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited

SHA1 Thumbprint dfdfac8947bdf75264a9233ac10ee3d12833dacc
SHA256 Thumbprint 7c7ed4240bb253bb35c376e12e00b027f1659df9d8267422a93eed75edc7adfb

Extension (critical: true)

Additional service information

RootCA-QC

Extension (critical: true)

Qualifications

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.1.1.1.2.1

Policy OID: 2.16.56.1.1.1.7.1

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=Belgium Root CA, C=BE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
25327272471742424753108761113025515413507712904874083939907073553139389403581555633427000903307438065008396155423372038139338001129228397387437566169146147569101132153735147
57637257855001524459884908283374968661826239871065222401938973133495715806769163244256124146245086841753860948543293162980605687722237452056111121899045054185334840993850231
44445138975351025575749503679547226381031300213808727950333349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
77417544850696324111877604954193498318303560891627721798430948172071644141969017225065301229219951
 public exponent: 65537
 Validity: [From: Sun Jan 26 23:00:00 UTC 2003,
             To: Sun Jan 26 23:00:00 UTC 2014]
 Issuer: CN=Belgium Root CA, C=BE
 SerialNumber: [    580b056c 5324dbb2 5057185f f9e5a650]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 10 F0 0C 56 9B 61 EA 57   3A B6 35 97 6D 9F DD B9  ...V.a.W:.5.m...
0010: 14 8E DB E6                                        ....
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.56.1.1.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 3A 2F   2F 72 65 70 6F 73 69 74  . http://reposit
0010: 6F 72 79 2E 65 69 64 2E   62 65 6C 67 69 75 6D 2E  ory.eid.belgium.
0020: 62 65                                              be

]]  ]
]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]
```

```
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 10 F0 0C 56 9B 61 EA 57   3A B6 35 97 6D 9F DD B9  ...V.a.W:.5.m...
0010: 14 8E DB E6                                        ....
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: C8 6D 22 51 8A 61 F8 0F   96 6E D5 20 B2 81 F8 C6  .m"Q.a...n. ....
0010: DC A3 16 00 DA CD 6A E7   6B 2A FA 59 48 A7 4C 49  ......j.k*.YH.LI
0020: 37 D7 73 A1 6A 01 65 5E   32 BD E7 97 D3 D0 2E 3C  7.s.j.e^2......<
0030: 73 D3 8C 7B 83 EF D6 42   C1 3F A8 A9 5D 0F 37 BA  s......B.?..].7.
0040: 76 D2 40 BD CC 2D 3F D3   44 41 49 9C FD 5B 29 F4  v.@..-?.DAI..[).
0050: 02 23 22 5B 71 1B BF 58   D9 28 4E 2D 45 F4 DA E7  .#"[q..X.(N-E...
0060: B5 63 45 44 11 0D 2A 7F   33 7F 36 49 B4 CE 6E A9  .cED..*.3.6I..n.
0070: 02 31 AE 5C FD C8 89 BF   42 7B D7 F1 60 F2 D7 87  .1.\....B...`...
0080: F6 57 2E 7A 7E 6A 13 80   1D DC E3 D0 63 1E 3D 71  .W.z.j......c.=q
0090: 31 B1 60 D4 9E 08 CA AB   F0 94 C7 48 75 54 81 F3  1.`........HuT..
00A0: 1B AD 77 9C E8 B2 8F DB   83 AC 8F 34 6B E8 BF C3  ..w........4k...
00B0: D9 F5 43 C3 64 55 EB 1A   BD 36 86 36 BA 21 8C 97  ..C.dU...6.6.!..
00C0: 1A 21 D4 EA 2D 3B AC BA   EC A7 1D AB BE B9 4A 9B  .!..-;........J.
00D0: 35 2F 1C 5C 1D 51 A7 1F   54 ED 12 97 FF F2 6E 87  5/.\.Q..T.....n.
00E0: 7D 46 C9 74 D6 EF EB 3D   7D E6 59 6E 06 94 04 E4  .F.t...=..Yn....
00F0: A2 55 87 38 28 6A 22 5E   E2 BE 74 12 B0 04 43 2A  .U.8(j"^..t...C*

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDlDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBgkqhkiG9w0BAQUFADAn
MQswCQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ2l1bSBSb290IENBMB4XDTAzMDEy
NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowJzELMAkGA1UEBhMCQkUxGDAWBgNVBAMT
D0JlbGdpdW0gUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMihcekcRkJ5eHFvna6pqKsot03HIOswkVp19eLSz8hMFJhCWK3HEcVAQGpa+XQS
J4fpnOVxTiIs0RIYqjBeoiG52bv/9nTrMQHnO35YD5EWTXaJqAFPrSJmcPpLHZXB
MFjqvNll2Jq0iOtJRlLf0lMVdssUXRlJsW9q09P9vMIt7EU/CT9YvvzU7wCMgTVy
v/cY6pZifSsofxVsY9LKyn0FrMhtB20yvmi4BUCuVJhWPmbxMOjvxKuTXgfeMo8S
dKpbNCNUwOpszv42kqgJF+qhLc9s44Qd3ocuMws8dOIhUDiVLlzg5cYx+dtA+mqh
pIqTm6chBocdJ9PEoclMsG8CAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4AQEBMC4wLAYIKwYBBQUHAgEW
IGh0dHA6Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBQQ8AxW
m2HqVzq2NZdtn925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth6lc6tjWXbZ/duRSO2+YwDQYJKoZIhvcNAQEFBQADggEBAMhtIlGKYfgP
lm7VILKB+MbcoxYA2s1q52sq+llIp0xJN9dzoWoBZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0AiMiW3Ebv1jZKE4tRfTa57VjRUQRDSp/
M382SbTObqkCMa5c/ciJv0J71/Fg8teH9lcuen5qE4Ad3OPQYx49cTGxYNSeCMqr
8JTHSHVUgfMbrXec6LKP24OsjzRr6L/D2fVDw2RV6xq9NoY2uiGMlxoh1OotO6y6
7Kcdq765Sps1LxxcHVGnH1TtEpf/8m6HfUbJdNbv6z195lluBpQE5KJVhzgoaiJe
4r50ErAEQyo=
-----END CERTIFICATE-----
```

CN=Belgium Root CA2, C=BE

Type	CA/QC
Status	granted
Status starting time	2016-06-30T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	3098404661496965511
Signature algorithm	SHA1withRSA
Issuer	CN=Belgium Root CA2, C=BE
Valid from	Thu Oct 04 10:00:00 UTC 2007
Valid to	Wed Dec 15 08:00:00 UTC 2021
Subject	CN=Belgium Root CA2, C=BE

Public key	Sun RSA public key, 2048 bits modulus: 25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533 47188304070237411505371354690003523602796504748268436965740013155524363953296559605768293726462748683867807979476223046936921095 00887975787577283413392923336546545109817976430306701793579151560621584351236063583342307 52621584351236063583342307104976244322177652181265270572535288593688668361490384043063624052887014382463758810568004079588144865 46438584605327134008224091466795027147972455421015549428678366393080491 58535662204430622722091644041294798682626345622247703196611536459503012648921426461410998536799349 11536459503012648921426461410998536799349 public exponent: 65537
Subject key identifier	858aebf4c5bbbe0e590394ded6800115e3109c39
Authority key identifier	858aebf4c5bbbe0e590394ded6800115e3109c39
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	51cca0710af7733d34acdc1945099f435c7fc59f
SHA256 Thumbprint	9f9744463be13714754e1a3becf98c08cc205e4ab32028f4e2830c4a1b2775b8

Extension (critical: true)

Additional service information

RootCA-QC

Extension (critical: true)

Qualifications

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.9.1.1.2.1

Policy OID: 2.16.56.9.1.1.7.1

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=Belgium Root CA2, C=BE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533471883040702374115053713546900035236027965047
48268436965740013155524363953296559605768293726462748683867807979476223046936921095008879757875772834133929233365465451098179764303067017935791515652621584351236063583342307
10497624432217765218126527057253528859368866836149038404306362405288701438246375881056800407958814486546438584605327134008224091466795027147972455421015549428678366393080491
58535662204430622722091644041294798682626345622247703196611536459503012648921426461410998536799349
 public exponent: 65537
 Validity: [From: Thu Oct 04 10:00:00 UTC 2007,
             To: Wed Dec 15 08:00:00 UTC 2021]
 Issuer: CN=Belgium Root CA2, C=BE
 SerialNumber: [    2affbe9f a2f0e987]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 85 8A EB F4 C5 BB BE 0E   59 03 94 DE D6 80 01 15  ........Y.......
0010: E3 10 9C 39                                        ...9
]
```

```
]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.56.9.1.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 3A 2F   2F 72 65 70 6F 73 69 74  . http://reposit
0010: 6F 72 79 2E 65 69 64 2E   62 65 6C 67 69 75 6D 2E  ory.eid.belgium.
0020: 62 65                                              be

]]  ]
]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 85 8A EB F4 C5 BB BE 0E   59 03 94 DE D6 80 01 15  ........Y.......
0010: E3 10 9C 39                                        ...9
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 51 D8 85 DD BB 57 6F CC   A0 6C B5 A3 20 9C 53 09  Q....Wo..l.. .S.
0010: F3 4A 01 0C 74 BF 2B B3   9A 9A BA 18 F2 0B 88 AC  .J..t.+.........
0020: 1C B3 33 AF CE E5 13 01   27 92 84 58 9A 10 B9 F7  ..3.....'..X....
0030: CC 14 92 6B 74 16 8A 96   E8 51 EF BF FA 4A 25 A7  ...kt....Q...J%.
0040: 89 B6 63 2B 5D 94 58 D1   CF 11 72 B6 1E B9 39 41  ..c+].X...r...9A
0050: 16 4D 29 BC 35 53 0B DA   DE 8E 0E CD A9 95 77 25  .M).5S........w%
0060: CA 94 5A E9 B2 69 AE D8   C0 13 BE 98 FC 96 9C 84  ..Z..i..........
0070: 7F 55 13 E6 3C 87 E3 BC   20 A4 A4 36 68 6B 4D 60  .U..<... ..6hkM`
0080: 66 1C F9 BF AC 80 94 66   2E B9 41 8A D3 65 D3 84  f.......f..A..e..
0090: 80 02 EF 50 1D 5E 46 DC   F7 C9 BA B5 34 7C 2A F3  ...P.^F.....4.*.
00A0: C6 D8 5F 5F 54 9D DB 4D   CD 11 E7 FD 14 02 83 66  .._T..M.......f
00B0: 5E C8 A6 00 12 A0 5F BE   CE 14 FE BB 1F A7 61 F7  ^....._.......a.
00C0: AB 4A F1 06 14 9F CA 49   42 C2 A9 BC ED 85 B1 AB  .J.....IB.......
00D0: 81 41 E6 0D C5 42 69 53   87 39 9D 4C 1F 00 0E 3E  .A...BiS.9.L...>
00E0: 07 0D 75 57 44 A8 53 B4   36 76 64 99 DC 6E EB 3D  ..uWD.S.6vd..n.=
00F0: 46 6E 14 5D 5E 47 53 8D   78 4D E0 27 BB 8E 85 76  Fn.]^GS.xM.'...v

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIIKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTIwHhcNMDcxMDA0MTAwMDAw
WhcNMjExMjE1MDgwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2ll
bSBSb290IENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi790hqc/7bIYLS2X+an7mEoj39WN4IzGMhwWLQdC1i22bi+n9fzGhYJdld61
IgDMqFNAn68KNaJ6x+HK92AQZw6nUHMXU5WfIp8MXW+2QbyM69odRr2nlL/zGsvU
+40OHjPIltfsjFPekx40HopQcSZYtF3CiInaYNKJIT/e1wEYNm7hLHADBGXvmAYr
XR5i3FVr/mZkIV/4L+HXmymvb82fqgxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y
HewApDgglVrH1Tdjuk+bqv5WRi5j2Qsj1Yr6tSPwiRuhFA0m2kHwOI8w7QUmecFL
TqG4flVSOmlGhHUCAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4CQEBMC4wLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBSFiuv0xbu+DlkD
lN7WgAEV4xCcOTARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAUhYrr9MW7
vg5ZA5Te1oABFeMQnDkwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGyloyCc
UwnzSgEMdL8rs5qauhjyC4isHLMzr87lEwEnkoRYmhC598wUkmt0FoqW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTlBFk0pvDVTC9rejg7NqZV3JcqUWumyaa7YwBO+mPyW
nIR/VRPmPIfjvCCkpDZoa01gZhz5v6yAlGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9fVJ3bTc0R5/0UAoNmXsimABKgX77OFP67H6dh96tK8QYUn8pJQsKpvO2F
sauBQeYNxUJpU4c5nUwfAA4+Bw11V0SoU7Q2dmSZ3G7rPUZuFF1eR1ONeE3gJ7uO
hXY=
-----END CERTIFICATE-----
```

CN=Belgium Root CA3, C=BE

Type	CA/QC
Status	granted
Status starting time	2016-06-30T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	4260689877497748905
Signature algorithm	SHA1withRSA
Issuer	CN=Belgium Root CA3, C=BE
Valid from	Wed Jun 26 12:00:00 UTC 2013
Valid to	Fri Jan 28 12:00:00 UTC 2028
Subject	CN=Belgium Root CA3, C=BE
Public key	Sun RSA public key, 4096 bits modulus: 689236842520400737293007329444355412322945976773189586843778935274893310124994701480157281209710914089287785990112639173313973887322735841404218927092481342245128960306942910996978037963366658748767743816676204871284733442749926896979727669941268727926916185454970539243310520698751355644372183719952899271297720759475324004770387044092331280439040222928977901876514295420628487235605720754718154655536547406721199374512288034894793897815898733743613360808422998466573314449092648772434298473182128687579464777943923944626874903980284954943444633165097044418808053302806567480397310165318173570984027495063931197729837576456850924507587304797255602129815800963894248447037937123270920368663080351919425068313464980278629369152701697759736384202776541620591588545291932466321499552953337556325973237815480592810613680950380979980022929206175039044753321633938140477949569594213821975729473102508366454723047943333937457964148701121644586439773493445613256431505451689600807046471898622121897269823517896969688074733205559734650561444823679292519060900635654581417970980552285817902789069514772158596504768735853434600634865427052445967408799471479389419032516498345380244525442401294961866201789300874794189231821802278084190173776931 public exponent: 65537
Subject key identifier	b8bc6c008f5b19859d25019cf019dc408ed0382b
Authority key identifier	b8bc6c008f5b19859d25019cf019dc408ed0382b
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	fd6b835c99b99e6ff84fcd0e6266a3610786a717
SHA256 Thumbprint	a8d14e945e3e5156bcae5e39737cf6a1b1f51028bbbf982f50ce5f4c05568b4d

Extension (critical: true)

Additional service information

RootCA-QC

Extension (critical: true)

Qualifications

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.10.1.1.2.1
Policy OID: 2.16.56.10.1.1.7.1

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Belgium Root CA3, C=BE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
689236842520400737293007329444355412322945976773189586843778935274893310124994701480157281209710914089287785990112639173313973887322735841404218927092481342245128960306942910996978037963366658748767743816676204871284733442749926896979727669941268727926916185454970539243310520698751355644372183719952899271297720759475324004770387044092331280439040222292897790187651429542062848723560572075471815465553654740672119937451228803489479389781589873374361336080842299846657331444909264877243429847318212868757946477794392394462687490398028495494344463316509704441880805330280656748039731016531817357098402749506393119772983757645685092450758730479725560212981580096389424844703793712327092036866308035191942506831346498027862936915270169775973638420277654162059158854529193246632149955295333755632597323781548059281061368095038097998002292920617503904475332163393814047794956959421382197572947310250836645472304794333393745796414870112164458643977349344561325643150545168960080704647189862212189726982351789696968807473320555973465056144482367929251906090063565458141797098055228581790278906951477215859650476873585343460063486542705244596740879947147938941903251649834538024452544240129496186620178930087479418923182180227808419017377693 1
 public exponent: 65537
 Validity: [From: Wed Jun 26 12:00:00 UTC 2013,
             To: Fri Jan 28 12:00:00 UTC 2028]
 Issuer: CN=Belgium Root CA3, C=BE
 SerialNumber: [    3b2102de 965b1da9]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B8 BC 6C 00 8F 5B 19 85   9D 25 01 9C F0 19 DC 40  ..l..[...%.....@
0010: 8E D0 38 2B                                        ..8+
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.56.10.1.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 3A 2F   2F 72 65 70 6F 73 69 74  . http://reposit
0010: 6F 72 79 2E 65 69 64 2E   62 65 6C 67 69 75 6D 2E  ory.eid.belgium.
0020: 62 65                                              be

]]  ]
]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B8 BC 6C 00 8F 5B 19 85   9D 25 01 9C F0 19 DC 40  ..l..[...%.....@
0010: 8E D0 38 2B                                        ..8+
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 45 62 3B FF 98 A5 FE 55   CC B1 11 A7 1C 92 0C 78  Eb;....U.......x
0010: 2F C5 EF 16 42 05 3D 7C   E3 12 70 E7 02 D0 82 91  /...B.=...p.....
0020: 13 94 FE 4E 67 D6 38 D5   2B E3 83 3A 7F 90 E2 42  ...Ng.8.+..:...B
0030: 60 E8 D7 7B 2B 8E FE CD   35 DC AD 27 B5 B4 1D A0  `...+...5..'....
0040: 54 CB 32 68 23 7D B1 CC   B8 A6 12 D7 D6 A4 F8 F2  T.2h#7..........
0050: C4 E1 0A 35 2D A2 8C 5F   22 84 72 72 97 65 7F 5E  ...5-.._".rr.e.^
0060: 07 71 43 C2 62 50 12 4C   26 A9 65 4D 0C 9C 06 F3  .qC.bP.L&.eM....
```

```
0070: 7E 9C F1 9B 8F 48 93 F0   36 25 6C 40 87 15 D5 44  .....H..6%l@...D
0080: 7C 0E BB 74 CC 1A 24 38   5B F5 72 55 AC 31 8F 04  ...t..$8[.rU.1..
0090: 0C 3B C4 E7 78 10 E8 99   B9 A4 5E C2 3D 6C 8D 0E  .;..x.....^.=l..
00A0: C5 65 21 D8 0E 5D 2A 5A   AE D2 C6 2F 13 47 73 F3  .e!..]*Z.../.Gs.
00B0: 10 F1 AF D6 64 99 9A 98   70 F2 0A 8B 30 99 95 A3  ....d...p...0...
00C0: F5 66 C4 A5 0A 2E 52 DF   58 27 DC 45 0F F9 F7 76  .f....R.X'.E...v
00D0: D6 AE 99 5E 05 3E E7 4F   EA 82 88 7F D1 45 1A 1D  ...^.>.O.....E..
00E0: 1A 5E 74 F4 01 11 2F C5   61 CD 88 41 9D 97 8E 19  .^t.../.a..A....
00F0: 9E 4F 03 3E F4 B9 3B B6   7C C7 78 7A 77 76 00 A8  .O.>..;...xzwv..
0100: 39 F7 1E C8 F5 1A 56 45   A2 5C C5 9C 34 0B EF 90  9.....VE.\..4...
0110: 35 44 2E F5 DF 26 94 71   C1 C4 5F 4B 92 AC E6 86  5D...&.q.._K....
0120: 9F 39 F8 FC D5 1C C6 51   B9 A9 C2 5D AE B0 E7 82  .9.....Q...]....
0130: 47 07 56 13 C8 0F BD B7   D6 35 04 02 F0 C2 6A B8  G.V......5....j.
0140: 39 79 1D D7 AE CD 47 AC   4D 75 2A 5D E1 24 C8 03  9y....G.Mu*].$..
0150: A8 E9 89 C5 DE 0D 2A 19   C2 C8 F4 D5 EE B2 38 B5  ......*.......8.
0160: 7A 04 54 67 B0 78 5C 2B   C6 E7 69 53 07 B5 A0 77  z.Tg.x\+..iS...w
0170: FC 15 17 34 B7 7F 89 80   99 84 C6 25 71 FE 37 F9  ...4.......%q.7.
0180: 6B 04 11 8A B9 32 79 5E   77 09 6A 58 85 50 AC 46  k....2y^w.jX.P.F
0190: 3F A5 66 37 26 9A 2D 41   79 22 54 EA 0B D0 86 1C  ?.f7&.-Ay"T.....
01A0: F2 D2 5C E8 03 A2 4B 76   1B DA 4D C0 59 B6 B7 B0  ..\...Kv..M.Y...
01B0: 1C A7 00 26 7A 09 0C 36   98 1C 81 37 7E AA 4D B2  ...&z..6...7..M.
01C0: 96 31 1A 4F CC 1F F7 9D   E3 50 01 5E 75 BA 4D DE  .1.O.....P.^u.M.
01D0: D5 FF DE 2F AE BC 73 8E   99 68 D0 3B 12 60 DA 55  .../..s..h.;.`.U
01E0: 4A 90 2F 9B 91 66 B6 16   B4 C1 0D DA E5 11 65 5A  J./..f........eZ
01F0: 2E B6 3E 33 EC 5E 21 CB   6B 0B 45 A7 3F BB B8 C6  ..>3.^!.k.E.?...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFjjCCA3agAwIBAgIIOyEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTMwHhcNMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBMzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKjyAZ2L
g8kHoIX7JLc3BeZ1Tzy9MEv7Bnr59xcJezc/xJJdO4V3bwMltKFfNvqsQ5H/GQAD
FJ0GmTLLPDI5AoeUjBubRZ9hwruUuQ11+vhtoVhuEuZUxofEIU2yJtiSOONwpo/G
Ib9C4YZ5h+7ltDpC3MvsFyyordpzgwqSHvFwTCmls5SpU05UbF7ZVPcfVf24A5Ig
HLpZTgQfAvnzPlm++eJY+sNoNzTBoe6iZphmPbxuPNcJ6slV8qMQQk50/g+KmoPp
HX4AvoTr4/7TMTvuK8jS1dEn+fdVKdx9qo9ZZRHFW/TXEn5SrNUu99xhzlE/WBur
rVwFoKCWCjmO0CnekJlw0NTr3HBTG5D4AiDjNFUYaIcGJk/ha9rzHzY+WpGdoFZx
hbP83ZGeoqkgBr8UzfOFCY8cyUN2db6hpIaK6Nuoho6QWnn+TSNh5Hjui5miqpGx
S73gYlT2Qww16h8gFTJQ49fiS+QHlwRw5cqFuqfFLE3nFFF9KIamS4TSe7T4dNGY
2VbHzpaGVT4wy+fl7gWsfaUkvhM4b00DzgDiJ9BHiKytNLmzoa3Sneij/CKur0dJ
5OdMiAqUpSd0Oe8pdIbmQm1oP5cjckiQjxx7+vSxWtacpGowWK8+7oEsYc+7fLt3
GD6q/O5Xi440Pd/sFJmfqRf3C1PPMdBqXcwjAgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVgOAoBATAuMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5iZTAdBgNV
HQ4EFgQUuLxsAI9bGYWdJQGc8BncQI7QOCswEQYJYIZIAYb4QgEBBAQDAgAHMB8G
A1UdIwQYMBaAFLi8bACPWxmFnSUBnPAZ3ECO0DgrMA0GCSqGSIb3DQEBBQUAA4IC
AQBFYjv/mKX+VcyxEacckgx4L8XvFkIFPXzjEnDnAtCCkROU/k5n1jjVK+ODOn+Q
4kJg6Nd7K47+zTXcrSe1tB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpdl
f14HcUPCYlASTCapZU0MnAbzfpzxm49Ik/A2JWxAhxXVRHwOu3TMGiQ4W/VyVawx
jwQMO8TneBDombmkXsI9bI0OxWUh2A5dKlqu0sYvE0dz8xDxr9ZkmZqYcPIKizCZ
laP1ZsSlCi5S31gn3EUP+fd21q6ZXgU+50/qgoh/0UUaHRpedPQBES/FYc2IQZ2X
jhmeTwM+9Lk7tnzHeHp3dgCoOfceyPUaVkWiXMWcNAvvkDVELvXfJpRxwcRfS5Ks
5oafOfj81RzGUbmpwl2usOeCRwdWE8gPvbfWNQQC8MJquDl5HdeuzUesTXUqXeEk
yAOo6YnF3g0qGcLI9NXusji1egRUZ7B4XCvG52lTB7Wgd/wVFzS3f4mAmYTGJXH+
N/lrBBGKuTJ5XncJaliFUKxGP6VmNyaaLUF5IlTqC9CGHPLSXOgDokt2G9pNwFm2
t7AcpwAmegkMNpgcgTd+qk2yljEaT8wf953jUAFedbpN3tX/3i+uvHOOmWjQOxJg
2lVKkC+bkWa2FrTBDdrlEWVaLrY+M+xeIctrC0WnP7u4xg==
-----END CERTIFICATE-----
```

CN=Belgium Root CA4, C=BE

Type	CA/QC
Status	granted
Status starting time	2016-06-30T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	5706940941790920504
Signature algorithm	SHA256withRSA
Issuer	CN=Belgium Root CA4, C=BE
Valid from	Wed Jun 26 12:00:00 UTC 2013
Valid to	Fri Oct 22 12:00:00 UTC 2032
Subject	CN=Belgium Root CA4, C=BE

Public key	Sun RSA public key, 4096 bits modulus: 6224115906824122031433393414467734255795749661242697041972796971 3589761663492552027516102528196645068474513261170454526640944182 0354245698609366890086847476742643168250121823522568805311895801 3272845856830766072936328678029599339864160757582078179782933477 1277758427264740541256591774911244974410560636250890042978670882 3655369589600664996359169269749224840725363125898523192670130240 3094481995663975256487988599594079751375649124722315558398958459 8625577661561495707877863985269083424382019627610669355576767590 3287437086963541879185923650029046515083278917967647521237597009 7723059779987931314312946138958009529327069795639742850540854481 1668100588053087190204290004659595000540204476361567140374287384 5557572387796136829835237636572157056930341887317395041724077153 2738123406566311692859096140881485975714355900153034684151459890 4885138299612865991395755715162815883415449288903178308408884400 9310182142365979807396066210319470759450039107508536195377707761 0756884183843432860457151575734269893011244632427230932999271471 6298828392876694701362548042681113710329345462526205188173283210 4879637264017398565292090224855096446539393723135313244013015486 7925044711328249031368163390477454073402140822040781939631335114 29055306278731837 public exponent: 65537
Subject key identifier	67e8f14e4fb3b5f3076f089c0c83d97ad95be749
Authority key identifier	67e8f14e4fb3b5f3076f089c0c83d97ad95be749
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	6b97f89956592a9b2010197527b0dc4ca5ac9be0
SHA256 Thumbprint	702dd5c1a093cf0a9d71fadd9bf9a7c5857d89fb73b716e867228b3c2beb968f

Extension (critical: true)

Additional service information

RootCA-QC

Extension (critical: true)

Qualifications

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.12.1.1.2.1

Policy OID: 2.16.56.12.1.1.7.1

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=Belgium Root CA4, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
6224115906824122031433393414467734255795749661242697041972796971358976166349255202751610252819664506847451326117045452664094418203542456986093668900868474767426431682501218235225688053118958013272845856830766072936328678029599339864160757582078179782933477352256880531189580132728458568307660729363286780295993398641607575820781797829334771277758427264740541256591774911244974410560636250890042978670882365536958960066499635916926974922484072536312589852319267013024030944819956639752564879885995940797513756491247223155583989584598625577661561495707877863985269083424382019627610669355576767590374922484072536312589852319267013024030944819956639752564879885995940797513756491247223155583989584598625577661561495707877863985269083424382019627610669355576767590374922484072536312589852319267013024030944819956639752564879885995940797513756491247223155583989584598625577661561495707877863985269083424382019627610669355576767590
```

```
0869635418791859236500290465150832789179676475212375970097723059779987931314312946138958009529327069795639742850540854481166810058805308719020429000465959500054020447636156714037428738455575723877961368298352376365721570569303418873173950417240771532738123406566311692859096140881485975714355900153034684151459890488513829961286599139575571516281588341544928890317830840888440093101821423659798073960662103194707594500391075085361953777077610756884183843432860457151575734269893011244632427230932999271471629882839287669470136254804268111371032934546252620518817328321048796372640173985652920902248550964465393937231353132440130154867925044711328249031368163390477454073402140822040781939631335114290553062787318371 public exponent: 65537
 Validity: [From: Wed Jun 26 12:00:00 UTC 2013,
             To: Fri Oct 22 12:00:00 UTC 2032]
 Issuer: CN=Belgium Root CA4, C=BE
 SerialNumber: [    4f33208c c594bf38]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 67 E8 F1 4E 4F B3 B5 F3   07 6F 08 9C 0C 83 D9 7A  g..NO....o.....z
0010: D9 5B E7 49                                        .[.I
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.56.12.1.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 3A 2F   2F 72 65 70 6F 73 69 74  . http://reposit
0010: 6F 72 79 2E 65 69 64 2E   62 65 6C 67 69 75 6D 2E  ory.eid.belgium.
0020: 62 65                                              be

]]  ]
]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 67 E8 F1 4E 4F B3 B5 F3   07 6F 08 9C 0C 83 D9 7A  g..NO....o.....z
0010: D9 5B E7 49                                        .[.I
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 5E DC 24 00 66 B3 70 55   9F 4B 97 79 C5 5A 46 8A  ^.$.f.pU.K.y.ZF.
0010: 0E F3 30 38 4D AC D4 DC   AC 4D FA 1C 19 4C 32 77  ..08M....M...L2w
0020: A7 34 D6 AB 12 37 9D 81   85 1A A9 69 21 16 2D E4  .4...7.....i!.-.
0030: 97 01 F3 D0 2B E7 F9 EC   CD 61 5C B3 55 13 C5 4C  ....+....a\.U..L
0040: 7F 55 6D 73 48 1E F9 58   23 28 E5 8B 27 EE 1D D0  .UmsH..X#(..'...
0050: 20 24 F1 52 00 2B 9E 4D   52 4A D2 6E EE 29 9F EA   $.R.+.MRJ.n.)..
0060: 2C 7C 3F C7 7B 48 DF 10   22 B2 AB DC 6B 85 B9 F8  ,.?..H.."...k...
0070: CB 16 7F 77 9A A3 F1 14   A3 F9 A3 E6 0A 85 FF 91  ...w............
0080: A3 83 66 6B A0 F8 07 F3   63 E4 D7 78 98 23 9F C7  ..fk....c..x.#..
0090: 84 40 63 BC CC 32 68 57   F8 5D 52 EA 2D 91 FF 1E  .@c..2hW.]R.-...
00A0: 41 77 AE 46 1A 02 BA F8   A9 06 6E EF 1E A1 00 F7  Aw.F......n.....
00B0: 8E 8D B9 5B 51 52 66 B3   B4 B5 11 F4 29 1B 49 9D  ...[QRf.....).I.
00C0: 69 95 65 A6 A8 A0 BE 40   A1 2B 5B 3B C1 7A CC 2B  i.e....@.+[;.z.+
00D0: 5B 1C DA 46 85 BD 52 7E   EA 09 29 A2 3B D7 5D 90  [..F..R...).;.].
00E0: 41 D5 44 78 9B 91 44 2F   3E 7F 24 19 D1 BF B8 E9  A.Dx..D/>.$.....
00F0: A6 45 0B 1B 8C 5B 80 44   D0 8C 59 2E 27 1D CE 93  .E...[.D..Y.'...
0100: 4F 0E DD 26 09 1E 66 36   62 A8 F9 76 DA 27 EC 58  O..&..f6b..v.'.X
0110: 9B 11 FF 0F D5 B8 93 00   E2 44 A8 B7 F8 7A A9 05  .........D...z..
0120: 7D 12 09 68 E0 29 51 94   49 37 CB 36 CA 91 C2 64  ...h.)Q.I7.6...d
0130: 2C A9 3A 94 0F 74 FE EE   3A 2A CA 92 0B 93 20 51  ,.:..t..:*.... Q
0140: E1 63 11 1D FD F2 25 EA   A4 3A 53 F0 1C C8 32 8B  .c....%..:S...2.
0150: CC CC 79 4A EE 9C 53 24   0E 5C 59 73 76 6B C3 8C  ..yJ..S$.\Ysvk..
0160: 85 80 80 FC A6 FA 76 A2   17 22 2F 0D 2A CA B3 54  ......v.."/.*..T
0170: C5 C9 7D 7E B9 0C CD A0   58 0F 2B 8E 27 09 5A 8A  ........X.+.'.Z.
0180: 28 A8 B8 54 2A E6 7A B5   25 80 E8 87 F6 4D 1A FB  (..T*.z.%....M..
0190: 31 F4 2C 54 38 70 C1 49   3A 9A F1 08 68 12 41 73  1.,T8p.I:...h.As
01A0: 23 96 1F C5 E0 C9 8E AE   B8 7B AF 19 EF 02 90 AF  #.............. 
01B0: 98 93 85 F6 4E 21 3E EC   6B 90 7B 86 15 27 F3 0E  ....N!>.k....'..
01C0: 19 D4 B7 57 57 99 C0 F9   96 4A EF BE 6B 33 8E 16  ...WW....J..k3..
01D0: BC 28 66 92 0F 28 EC 23   6E CB 8B 6E CD 31 B7 A0  .(f..(.#n..n.1..
01E0: 70 59 6D 97 14 FD 36 E4   10 E1 FC E0 FA 50 4E 15  pYm...6......PN.
01F0: B3 2C E7 9D 40 A4 6F 80   1B 4B DE 3B 51 7E 8D 18  .,..@.o..K.;Q...
```

]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFjjCCA3agAwIBAgIITzMgjMWUvzgwDQYJKoZIhvcNAQELBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTQwHhcNMTMwNjI2MTIwMDAw
WhcNMzIxMDIyMTIwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBNDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJiQrvrH
Hm+O4AU6syN4TNHWL911PFsY6E9euwVml5NAWTdw9p2mcmEOYGx424jFLpSQVNxx
xoh3LsIpdWUMRQfuiDqzvZx/4dCBaeKL/AMRJuL1d6wU73XKSkdDr5uH6H2Yf19z
SiUOm2x4k3aNLyT+VryF11b1Prp67CBk63OBmG0WUaB+ExtBHOkfPaHRHFA04Mig
oVFt3gLQRGh1V+H1rm1hydTzd6zzpoJHp3ujWD4r4kLCrxVFV0QZ44usvAPlhKoe
cF0feiKtegS1pS+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7MMpf8MEygX
WMb+WrynTetWnIV6jTzZA1RmaZuqmIMDvWTA7JNkiDJQOJBWQ3Ehp+Vn7li1MCIj
XlEDYJ2wRmcRZQ0bsUzaM/V3p+Q+j8S3osma3Pc6+dDzxL+Og/lnRnLlDapXx28X
B9urUR5H03Ozm77B9/mYgIeM8Y1XntlCCELBeuJeEYJUqc0FsGxWNwjsBtRoZ4dv
a1rvzkXmjJuNIR4YILg8G4kKLhr9JDrtyCkvI9Xm8GDjqQIJ2KpQiJHBLJA0gKxl
Yem8CSO/an3AOxqTNZjWbQx6E32OPB/rsU28ldadi9c8yeRyXLWpUF4Ghjyoc4Od
rAkXmljnkzLMC459xGL8gj6LyNb6UzX0eYA9AgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVgOAwBATAuMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5iZTAdBgNV
HQ4EFgQUZ+jxTk+ztfMHbwicDIPZetlb50kwEQYJYIZIAYb4QgEBBAQDAgAHMB8G
A1UdIwQYMBaAFGfo8U5Ps7XzB28InAyD2XrZW+dJMA0GCSqGSIb3DQEBCwUAA4IC
AQBe3CQAZrNwVZ9Ll3nFWkaKDvMwOE2s1NysTfocGUwyd6c01qsSN52BhRqpaSEW
LeSXAfPQK+f57M1hXLNVE8VMf1Vtc0ge+VgjKOWLJ+4d0CAk8VIAK55NUkrSbu4p
n+osfD/He0jfECKyq9xrhbn4yxZ/d5qj8RSj+aPmCoX/kaODZmug+AfzY+TXeJgj
n8eEQGO8zDJoV/hdUuotkf8eQXeuRhoCuvipBm7vHqEA946NuVtRUmaztLUR9Ckb
SZ1plWWmqKC+QKErWzvBeswrWxzaRoW9Un7qCSmiO9ddkEHVRHibkUQvPn8kGdG/
uOmmRQsbjFuARNCMWS4nHc6TTw7dJgkeZjZiqPl22ifsWJsR/w/VuJMA4kSot/h6
qQV9Eglo4ClRlEk3yzbKkcJkLKk6lA90/u46KsqSC5MgUeFjER398iXqpDpT8BzI
MovMzHlK7pxTJA5cWXN2a8OMhYCA/Kb6dqIXIi8NKsqzVMXJfX65DM2gWA8rjicJ
WoooqLhUKuZ6tSWA6If2TRr7MfQsVDhwwUk6mvEIaBJBcyOWH8XgyY6uuHuvGe8C
kK+Yk4X2TiE+7GuQe4YVJ/MOGdS3V1eZwPmWSu++azOOFrwoZpIPKOwjbsuLbs0x
t6BwWW2XFP025BDh/OD6UE4VsyznnUCkb4AbS947UX6NGA==
-----END CERTIFICATE-----

CN=Certipost Public CA for Qualified Signatures, O=Certipost n.v./s.a., C=BE

Type	CA/QC
Status	withdrawn
Status starting time	2016-12-14T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	904
Signature algorithm	SHA256withRSA
Issuer	CN=Verizon Global Root CA, OU=OmniRoot, O=Verizon Business, C=US
Valid from	Wed Jan 11 19:45:06 UTC 2012
Valid to	Tue Jan 11 19:44:34 UTC 2022
Subject	CN=Certipost Public CA for Qualified Signatures, O=Certipost n.v./s.a., C=BE
Public key	Sun RSA public key, 2048 bits modulus: 20583708081178068867195678561473200619452921905927961291793273671328005822028265845465542836756717140506081882114668638826442932484074478170330701774649713666715833210650528515435727743179164568714309427414922655427737007468372319167639662905481587399501992029174676515494584699514099891322542890739713299134792579834056665407461968770656502958366334026477026985672010148944735034154896679171316339669903378855401615391971540384786406392311131067913663589486493118066042504737642498346914368670309047269922309076138772412256664686136790625895780242652401177074998149327839849236823966793860428091543634245433429423 81 public exponent: 65537
Subject key identifier	0e3733c7286ebfce5fe62ae698908bacc1e62844
CRL distribution points	http://cdp1.public-trust.com/CRL/Omniroot2034.crl

Authority key identifier	4c3811b898005b5a2b703eaa78e4d5676767a77e
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	05e88c57c47c3b510aed61a8c9d427ffe2925c01
SHA256 Thumbprint	4671a19c0fb1e221aeda10c7d745b7e5bf4faaffafc63fc2e2f8add187adab69

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Certipost Public CA for Qualified Signatures, O=Certipost n.v./s.a., C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
20583708081178068867195678561473200619452921905927961291793273671328005822028265845465542836756717140506081882114668638826442932484074478170330701774649713666715833210650528
51543572774317916456871430942741492265542773700746837231916763966290548158739950199202917467651549458469951409989132254289073971329913479257983405666540746196877065650295836
63340264770269856720101489447350341548966791713163396699033788554016153919715403847864063923111310679136635894864931180660425047376424983469143686703090472699223090766138772
41225666468613679062589578024265240117707499814932783984923682396679386042809154363424543342942381
 public exponent: 65537
 Validity: [From: Wed Jan 11 19:45:06 UTC 2012,
             To: Tue Jan 11 19:44:34 UTC 2022]
 Issuer: CN=Verizon Global Root CA, OU=OmniRoot, O=Verizon Business, C=US
 SerialNumber: [    0388]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4C 38 11 B8 98 00 5B 5A   2B 70 3E AA 78 E4 D5 67  L8....[Z+p>.x..g
0010: 67 67 A7 7E                                        gg..
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://cdp1.public-trust.com/CRL/Omniroot2034.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 24 68 74 74 70 73 3A   2F 2F 77 77 77 2E 63 65  .$https://www.ce
0010: 72 74 69 70 6F 73 74 2E   63 6F 6D 2F 73 68 6F 77  rtipost.com/show
0020: 70 6F 6C 69 63 79                                  policy

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0E 37 33 C7 28 6E BF CE   5F E6 2A E6 98 90 8B AC  .73.(n.._.*.....
0010: C1 E6 28 44                                        ..(D
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 73 F0 57 07 07 F3 34 DE   48 53 1E 3E 0A 88 33 07  s.W...4.HS.>..3.
```

```
0010: 6C 55 49 D2 75 85 54 92   F2 80 19 1C 86 5D D7 F4  lUI.u.T......]..
0020: 10 35 18 31 AC 35 F8 8D   4B 0F 6D 66 4B 15 4C 28  .5.1.5..K.mfK.L(
0030: 91 12 78 3B C4 B3 42 65   A8 44 46 A2 10 8C F6 38  ..x;..Be.DF....8
0040: A0 AA EB 8D 42 18 10 E1   21 AC 5B 2C 0D C9 7C 35  ....B...!.[,...5
0050: 6A D2 0C 7E 9D 83 EC 5B   22 36 B4 DC AF 2D F2 87  j......["6...-..
0060: 6B F9 7F 16 77 0B 25 7B   A3 66 52 4B EA 44 BC 58  k...w.%..fRK.D.X
0070: 6F B9 FA 9D 65 49 60 67   AE 3F 46 13 DC AB 56 55  o...eI`g.?F...VU
0080: EF 86 AC 26 E3 41 45 9E   D2 E8 81 77 3F 1C C0 28  ...&.AE....w?..(
0090: 33 7D 62 DA 7C BC 9C 35   72 CD 51 A1 2F F4 08 9F  3.b....5r.Q./...
00A0: FA 68 94 BC 1E 30 5C F3   AD D1 8F 7F 52 B1 C2 FF  .h...0\.....R...
00B0: CD 95 BE 29 A9 EF 2E FB   C3 69 F0 82 27 F1 4D B9  ...).....i..'.M.
00C0: A0 3C D1 56 23 1D 61 EC   9E 4D 59 8C 55 81 5A 5A  .<.V#.a..MY.U.ZZ
00D0: 62 6C 93 73 21 5A F6 52   84 8A AF 97 01 96 7E B4  bl.s!Z.R.......
00E0: 79 80 91 A5 E2 2B 7B 19   27 B7 9A 29 AF A3 27 72  y....+..'..)..'r
00F0: 28 A9 09 73 9B 93 A7 3F   E0 48 8F 9E B5 98 8A F8  (..s...?.H......

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIELTCCAxWgAwIBAgICA4gwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAoMEFZlcml6b24gQnVzaW5lc3MxETAPBgNVBAsMCE9tbmlSb290MR8w
HQYDVQQDDBZWZXJpem9uIEdsb2JhbCBSb290IENBMB4XDTEyMDExMTE5NDUwNloX
DTIyMDExMTE5NDQzNFowYjELMAkGA1UEBhMCQkUxHDAaBgNVBAoTE0NlcnRpcG9z
dCBuLnYuL3MuYS4xNTAzBgNVBAMTLENlcnRpcG9zdCBQdWJsaWMgQ0EgZm9yIFF1
YWxpZmllZCBTaWduYXR1cmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAow3rmuZKZMnGhQRGeEzZK4THeq59CIqK6BseSxLmZ3sh8znY0FBNK4OXmFEj
0Y99QnIyAJxnU5bcvSSBFQKPwtD5cFcmpcyP7BROi6/MyJCE6BMD8wcS61CJfLlm
8/p/VRF9KsDfa6fMd/W1ghbq78Owa22+UgXpFr27eqBCsUzEiZya5cILWXMOhmP+
ZE3Oi7pLZ/Dh+50tn/R+P0IVBBIypiycnx/u4Q/1oEqMyy+DF1iuMfCbCpE2Pbwz
0R+SCqlFNeRO9dlfmJ5XlpSr5K7dKXJP8DgoMw8Cu5fGLU8z2qwqx+3ZvOXdxDNF
e2g8HHX4WdMymhSzbmnLjGVYrQIDAQABo4HyMIHvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwRQYDVR0gBD4wPDA6BgRVHSAAMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3
LmNlcnRpcG9zdC5jb20vc2hvd3BvbGljeTAOBgNVHQ8BAf8EBAMCAQYwHwYDVR0j
BBgwFoAUTDgRuJgAW1orcD6qeOTVZ2dnp34wQgYDVR0fBDswOTA3oDWgM4YxaHR0
cDovL2NkcDEucHVibGljLXRydXN0LmNvbS9DUkwvT21uaXJvb3QyMDM0LmNybDAd
BgNVHQ4EFgQUDjczxyhuv85f5irmmJCLrMHmKEQwDQYJKoZIhvcNAQELBQADggEB
AHPwVwcH8zTeSFMePgqIMwdsVUnSdYVUkvKAGRyGXdf0EDUYMaw1+I1LD21mSxVM
KJESeDvEs0JlqERGohCM9jigquuNQhgQ4SGsWywNyXw1atIMfp2D7FsiNrTcry3y
h2v5fxZ3CyV7o2ZSS+pEvFhvufqdZUlgZ64/RhPcq1ZV74asJuNBRZ7S6IF3PxzA
KDN9Ytp8vJw1cs1RoS/0CJ/6aJS8HjBc863Rj39SscL/zZW+KanvLvvDafCCJ/FN
uaA80VYjHWHsnk1ZjFWBWlpibJNzIVr2UoSKr5cBln60eYCRpeIrexknt5opr6Mn
ciipCXObk6c/4EiPnrWYivg=
-----END CERTIFICATE-----
```

CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE

Type	CA/QC
Status	withdrawn
Status starting time	2016-12-14T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	48357032784596390676244 85
Signature algorithm	SHA1withRSA
Issuer	CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
Valid from	Tue Jul 26 10:00:00 UTC 2005
Valid to	Sun Jul 26 10:00:00 UTC 2020
Subject	CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE

Public key	Sun RSA public key, 2048 bits modulus: 21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291 71019845110836298509487347392598926445178040669341963245499642913192950780187748886826305662589231481198165241 31929507801877488868263056625892314811981652410138907899996057327037799082855868763511239453871155320357733059447691386874174245 63514185255502148282975915843232278470198050293821835164764560721 13503509849133047234960429392298749219309319677503350490197904821 80175721305618158877519196536509324816209488739023225409035382932 01748046544492990321822776933466895853040481157184268960104728191756821 91756828175665531985013380898309970472809711974749172360391497320021423618781243205030580718750539861465 00214236187812432050305807187505398614653 public exponent: 65537
Subject key identifier	f078f9077710bbdc1ea1ae79fb3010dbc634f817
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	742cdf1594049cbf17a2046cc639bb3888e02e33
SHA256 Thumbprint	058a40323ec8c46262c3052a5d357b91ac24d3da26351b3ff4407e99f7a4e9b4

Extension (critical: true)

Additional service information

RootCA-QC

Extension (critical: true)

Qualifications

Qualifier: NotQualified

Assert: atLeastOne

Policy OID: 0.3.2062.7.1.1.112.1

Policy OID: 0.3.2062.7.1.1.140.1

Policy OID: 0.3.2062.7.1.1.111.1

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524
10138907899996057327037799082855868763511239453871155320357733059447691386874174245635141852555021482829759158432322784701980502938218351647645607213503509849133047234960429
39229874921930931967750335049019790482801757213056181588775191965365093248162094887390232254090353829320174804654449299032182277693346689585304048115718426896010472819175682
81756655319850133808983099704728097119747491723603914973200214236187812432050305807187505398614653
 public exponent: 65537
 Validity: [From: Tue Jul 26 10:00:00 UTC 2005,
             To: Sun Jul 26 10:00:00 UTC 2020]
 Issuer: CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
 SerialNumber: [    04000000 00010552 64c425]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[2]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
```

```
 [CertificatePolicyId: [0.3.2062.7.1.0.1.2.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 22 68 74 74 70 3A 2F   2F 77 77 77 2E 65 2D 74  ."http://www.e-t
0010: 72 75 73 74 2E 62 65 2F   43 50 53 2F 51 4E 63 65  rust.be/CPS/QNce
0020: 72 74 73 20                                        rts

]]  ]
]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[5]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F0 78 F9 07 77 10 BB DC   1E A1 AE 79 FB 30 10 DB  .x..w......y.0..
0010: C6 34 F8 17                                        .4..
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 6C E1 D8 5F 74 58 E9 70   49 D6 CA 0D 2C 58 DA CA  l.._tX.pI...,X..
0010: 64 B6 51 4F C3 06 64 01   E9 8A 73 1D 9E CF 46 78  d.QO..d...s...Fx
0020: BF 3B 85 86 E2 3D 4A 18   94 2A 81 77 6F 82 F8 6F  .;...=J..*.wo..o
0030: F4 EE 22 FC 9D 18 21 72   60 BB 18 80 82 95 FB F9  .."...!r`.......
0040: F7 95 24 81 66 C1 B5 C3   B5 D2 B6 76 8B 3B 81 5C  ..$.f......v.;.\
0050: B8 A1 0E 2B 01 14 8B 80   09 40 EE F8 60 4C 19 E4  ...+.....@..`L..
0060: 17 CD 27 01 B3 63 12 05   A4 08 C9 B4 BF 9E 50 4E  ..'..c........PN
0070: B5 DE 0F 92 33 66 75 D0   3D E7 23 7C EA 25 71 7C  ....3fu.=.#..%q.
0080: FE 3E 2E 36 79 A1 E5 29   50 23 35 05 95 78 BB 9F  .>.6y..)P#5..x..
0090: 79 64 DC 57 48 27 2C E2   5C 33 CD C2 BB 7E 68 77  yd.WH',.\3....hw
00A0: A7 2F A3 49 17 72 E1 00   84 6B 7D 7A AF 39 0B 2C  ./.I.r...k.z.9.,
00B0: D5 D8 57 64 32 6C 84 0A   6A 76 3A D3 AC CD 9D B1  ..Wd2l..jv:.....
00C0: E7 37 DC EC 0C 2F C5 57   60 DF 88 F5 43 B1 01 64  .7.../.W`...C..d
00D0: 26 B4 27 82 10 B2 A3 50   EF 97 E6 7F BF 91 87 B3  &.'....P........
00E0: DB 90 A9 2A E2 7A 34 6C   73 49 F4 E8 8D 2E 6B 8A  ...*.z4lsI....k.
00F0: DD A1 8A 7F 63 D0 BF 58   1E AF CC 3F 92 50 2D D1  ....c..X...?.P-.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID3jCCAsagAwIBAgILBAAAAAABBVJkxCUwDQYJKoZIhvcNAQEFBQAwXDELMAkG
A1UEBhMCQkUxHDAaBgNVBAoTE0NlcnRpG9zdCBzLmEuL24udi4xLzAtBgNVBAMT
JkNlcnRpG9zdCBFLVRydXN0IFByaW1hcnkgUXVhbGlmaWVkIENBMB4XDTA1MDcy
NjEwMDAwMFoXDTIwMDcyNjEwMDAwMFowXDELMAkGA1UEBhMCQkUxHDAaBgNVBAoT
E0NlcnRpG9zdCBzLmEuL24udi4xLzAtBgNVBAMTJkNlcnRpG9zdCBFLVRydXN0
IFByaW1hcnkgUXVhbGlmaWVkIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAriDSeNuaoHKcBFIlLG1S2NcniTOg4bLV+zB1ay1/HGeODucfEt8XeRi7
tBtv+D11G55nN/Dx+g917YadAwShKHAtPLJroHNR4zWpdKUIPpSFJzYqqnJk/Hfu
dpQccuu/Msd3A2olggkFr19gPH+sG7yS6Dx0Wc7xfFQtOK6W8KxvoTMMIVoBuiMg
W6CGAtVT3EkfqDKzrztGO7bvnzmzOAvneor2KPmnb1ApyHlYi0nSpdiFflbxaRV4
RBE116VUPqtmJdLb4xjxLivicSMJN2RDQnQylnfel6LploacJUQJ1AGdUX4ztwlE
5YCXDWRbdxiXpUupnhCdh/pWp88KfQIDAQABo4GgMIGdMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTwePkHdxC73B6hrnn7MBDbxjT4
FzBIBgNVHSAEQTA/MD0GCQQQDgcBAAECADAwMC4GCCsGAQUFBwIBFiJodHRwOi8v
d3d3LmUtdHJ1c3QuYmUvQ1BTL1FOY2VydHMgMBEGCWCGSAGG+EIBAQQEAwIABzAN
BgkqhkiG9w0BAQUFAAOCAQEAbOHYX3RY6XBJ1soNLFjaymS2UU/DBmQB6YpzHZ7P
Rni/O4WG4j1KGJQqgXdvgvhv9O4i/J0YIXJguxiAgpX7+feVJIFmwbXDtdK2dos7
gVy4oQ4rARSLgAlA7vhgTBnkF80nAbNjEgWkCMm0v55QTrXeD5IzZnXQPecjfOol
cXz+Pi42eaHlKVAjNQWVeLufeWTcV0gnLOJcM83Cu35od6cvo0kXcuEAhGt9eq85
CyzV2FdkMmyECmp2OtOszZ2x5zfc7AwvxVdg34j1Q7EBZCa0J4IQsqNQ75fmf7+R
h7PbkKkq4no0bHNJ9OiNLmuK3aGKf2PQv1ger8w/klAt0Q==
-----END CERTIFICATE-----
```

Society for Worldwide Interbank Financial Telecommunication SCRL

Service provider trade name	VATBE-0413330856
Information URI	http://www.swift.com/pkirepository
Service provider street address	Avenue Adèle 1

Service provider postal code	1310
Service provider locality	La Hulpe
Service provider state	Brussels
Service provider country	BE

SWIFTNet PKI Certification Authority

Type	CA/QC
Status	granted
Status starting time	2017-10-11T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	1007235709
Signature algorithm	SHA1withRSA
Issuer	O=SWIFT
Valid from	Sat Jun 15 11:51:47 UTC 2002
Valid to	Wed Jun 15 12:21:47 UTC 2022
Subject	O=SWIFT
Public key	Sun RSA public key, 2048 bits modulus: 27134891449536663670091338916364605667193647212683610465365919934994474903020635584331677653228200210928489182501819079634477925849223359099983741305164508178246344443502931307261967832450338861324550609449630768200966983969376986503711769404215924828428075011899626639351963633260617226195373584394852072888957304178117531351056971116345766894660348212101363444293023928141534285009070263864185204364271348993003240734092537017732631174312798422848480577617459936682837566698589952098721105585848777111378534843596652764240089811159449759859139013698249064619618572718739685639915967136410239131574955455289383883587 public exponent: 65537
Subject key identifier	3e30b33b359757fff140db1b4501382e15a79eb2
Authority key identifier	3e30b33b359757fff140db1b4501382e15a79eb2
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	d9a235c88c875b171174d1076b596af9e0a0363d
SHA256 Thumbprint	cfa61bf3895cfe4244fbe684aedc88feaddd14d6aa3c73f5688f2c1e52c9a604

Extension (critical: true)

Additional service information

ForeSeals

Extension (critical: true)

Qualifications

Qualifier: QCNoQSCD

Criterial List Description

Assert: atLeastOne

Policy OID: 1.3.21.6.3.10.200.7

Qualifier: NotQualified

Criterial List Description

Assert: none

The decoded certificate:

```
[
[
 Version: V3
 Subject: O=SWIFT
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
27134891449536663670091338916364605667193647212683610465365919934994474903020635584331677653228200210928489182501819079634477925849223359099983741305164508178246344443502931
30726196783245033886132455060944963076820096698396937698650371176940421592482842807501189962663935196363326061722619537358439485207288895730417811753135105697111634576689466
03482121013634442930239281415342850090702638641852043642713489930032407340925370177326311743127984228484805776174599366828375666985899520987211055858487771113785348435966527
64240089811159449759859139013698249064619618572718739685639915967136410239131574955455289383883587
 public exponent: 65537
 Validity: [From: Sat Jun 15 11:51:47 UTC 2002,
             To: Wed Jun 15 12:21:47 UTC 2022]
 Issuer: O=SWIFT
 SerialNumber: [    3c09327d]

Certificate Extensions: 8
[1]: ObjectId: 1.2.840.113533.7.65.0 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 10 30 0E 1B 08 56 35   2E 30 3A 34 2E 30 03 02  ..0...V5.0:4.0..
0010: 04 90                                              ..


[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 3E 30 B3 3B 35 97 57 FF   F1 40 DB 1B 45 01 38 2E  >0.;5.W..@..E.8.
0010: 15 A7 9E B2                                        ....
]

]

[3]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [CN=CRL1, O=SWIFT]
]]

[5]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[7]: ObjectId: 2.5.29.16 Criticality=false
PrivateKeyUsage: [
From: Sat Jun 15 11:51:47 UTC 2002, To: Wed Jun 15 12:21:47 UTC 2022]

[8]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 3E 30 B3 3B 35 97 57 FF   F1 40 DB 1B 45 01 38 2E  >0.;5.W..@..E.8.
0010: 15 A7 9E B2                                        ....
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: BE CD 22 54 79 F9 BF D6   7E E7 EC 99 A5 E3 63 18  .."Ty........c.
0010: 80 CB 07 4E 87 4E A5 CD   AD F3 D7 9E ED CB B3 78  ...N.N.........x
0020: CE FD 20 2C C3 D5 F1 F3   1B 1A 42 CB 8B 62 A7 9B  .. ,......B..b..
0030: A3 D1 34 D6 C3 92 5F 03   1C 1D 39 5C FB D0 34 53  ..4..._...9\..4S
```

```
0040: CF 93 5A 36 6D 15 D4 8B   3A 0E CB F6 B2 3F 97 02  ..Z6m...:....?..
0050: 1A DA 39 12 49 40 9B CC   5B 51 92 33 38 A5 54 4E  ..9.I@..[Q.38.TN
0060: C3 06 09 4E 77 70 E0 88   B3 93 32 AC C1 A4 8A F2  ...Nwp....2.....
0070: D9 D7 C7 F7 AB 0F 71 B8   D7 AE E5 01 37 D6 E4 4F  ......q.....7..O
0080: 42 A2 DE D6 16 DD FF 81   03 17 6C 5C 7E F5 C2 C6  B.........l\....
0090: 86 57 8E C7 D7 44 91 BA   09 5D 05 5D 87 1E F3 86  .W...D...].]....
00A0: BB F3 E7 3E 9C 55 53 B9   4A 18 49 01 2B 21 3D 55  ...>.US.J.I.+!=U
00B0: E3 31 DA B3 B5 62 42 00   2B 1D 55 0A CE 8B 2B 83  .1...bB.+.U...+.
00C0: D9 46 A0 B5 17 BA 4E 66   88 33 07 0D E2 31 CD BA  .F....Nf.3...1..
00D0: 7B AD ED 45 C1 DA C1 A8   FE 86 7E BC 82 40 E4 D4  ...E.........@..
00E0: 2E AC 78 80 91 FE C3 28   ED 42 F6 47 7C 6B 7C E0  ..x....(.B.G.k..
00F0: CA 50 B5 C3 7E 4B 39 AF   70 97 86 79 CB 0C 9E 09  .P...K9.p..y....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDkDCCAnigAwIBAgIEPAkyfTANBgkqhkiG9w0BAQUFADAQMQ4wDAYDVQQKEwVT
V0lGVDAeFw0wMjA2MTUxMTUxNDdaFw0yMjA2MTUxMjIxNDdaMBAxDjAMBgNVBAoT
BVNXSUZUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1vMie2UrDYQy
2yk3+hjuqgqSc8br8qtqzXHsB7Zt99PenOdTFAsAnFyshdMVIGgwmyJb8X3QpFEJ
nh6is3o+JrHfkDPsO7ISroFc9lAD7TEGQEnfiCMNJnJRH8Oce0bLKmBfqv/Gwrsp
/SZRzFUlJu+PILZaZ3uwVuxQ1ZLkKWlQVGSQJudNhh2qeWDU3D3SusRBNS37d4h5
zg3ZV3nmDWuQb0K866KRjiYRRY7rau/amjUYegkJe3bhK18yRlYprz25AS3XWl7a
zOpKv9obTQINRgg/wNwNdqwSF2rZLt/bZg8UnlomKWq7MTQfN/cHniGOQbfNtINL
MWblH5aTQwIDAQABo4HxMIHuMBEGCWCGSAGG+EIBAQQEAwIABzAyBgNVHR8EKzAp
MCegJaAjpCEwHzEOMAwGA1UEChMFU1dJRlQxDTALBgNVBAMTBENSTDEwKwYDVR0Q
BCQwIoAPMjAwMjA2MTUxMTUxNDdagQ8yMDIyMDYxNTEyMjE0N1owCwYDVR0PBAQD
AgEGMB8GA1UdIwQYMBaAFD4wszs1l1f/8UDbG0UBOC4Vp56yMB0GA1UdDgQWBBQ+
MLM7NZdX//FA2xtFATguFaeesjAMBgNVHRMEBTADAQH/MB0GCSqGSIb2fQdBAAQQ
MA4bCFY1LjA6NC4wAwIEkDANBgkqhkiG9w0BAQUFAAOCAQEAvs0iVHn5v9Z+5+yZ
peNjGIDLB06HTqXNrfPXnu3Ls3jO/SAsw9Xx8xsaQsuLYqebo9E01sOSXwMcHTlc
+9A0U8+TWjZtFdSLOg7L9rI/lwIa2jkSSUCbzFtRkjM4pVROwwYJTndw4IizkzKs
waSK8tnXx/erD3G4167lATfW5E9Cot7WFt3/gQMXbFx+9cLGhleOx9dEkboJXQVd
hx7zhrvz5z6cVVO5ShhJAShPVXjMdqztWJCACsdVQrOiyuD2UagtRe6TmaIMwcN
4jHNunut7UXB2sGo/oZ+vIJA5NQurHiAkf7DKO1C9kd8a3zgylC1w35LOa9wl4Z5
ywyeCQ==
-----END CERTIFICATE-----
```

QuoVadis Trustlink BVBA

Service provider trade name	VATBE-0537698318
Information URI	https://www.quovadisglobal.be/Repository.aspx?sc_lang=en-GB
Service provider street address	Schaliënhoevedreef 20 boxT
Service provider postal code	2800
Service provider locality	Mechelen
Service provider state	Antwerpen
Service provider country	BE

QuoVadis BE PKI Certification Authority

Type	CA/QC
Status	withdrawn
Status starting time	2017-11-30T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	609679183321230578642917563116990405939188292251
Signature algorithm	SHA256withRSA
Issuer	CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
Valid from	Tue Jan 28 13:31:54 UTC 2014
Valid to	Wed Mar 17 18:33:33 UTC 2021

Subject	CN=QuoVadis Belgium Issuing CA G1, O=QuoVadis Trustlink BVBA, C=BE
Public key	Sun RSA public key, 4096 bits modulus: 97839640499375085962331984385066460254733880605256647363902160732102443656154852856590692595277855257563778420931571542568909508097863188313682143846785967742550551892529594210244365615485285659069259527785525756377842093157154256890950809786318831368214384678596774255055189252959464789355362156150906056393460135609950257208816552322058565456762152598983343579241207167353021311043823546160995023349465819732001393426014237052576853073064817439203850489307475026119919108600127180985930937572274379190999324023048980609635572348358816072484994067170269394212885704794032888031826978293616900979564841015208237311036093100150907292007819407536844165622944133156471883193565917716336391354589201137377636219363681450601184436862019672700673253280529883042295074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669381028717945085604658219831940595283416191753140348941632069250736324234157157004129102669072961997392759148097836830663187572932975564250918605529635852688494190304072707741879985054593570602546547329191019290607044365007087591103957060761678635733849787122519130799704308147165599948849072838313070703058851956878669387044135529569895785662937077766970294625223703430
public exponent: 65537
Subject key identifier	f80f651c7a6319aabf446fa6491221f37a5de30d
CRL distribution points	http://crl.quovadisglobal.com/qvrca.crl
Authority key identifier	8b4b6dedd329b90619ec3939a9f097846acbefdf
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	89c89b25fa25bafa839fbd9fc1d29caf6481bf28
SHA256 Thumbprint	27ebacd86dd3bf86143da4342861031a57cf3fa414d40a86e669c3f4f1d8cf24

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=QuoVadis Belgium Issuing CA G1, O=QuoVadis Trustlink BVBA, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
97839640499375085962331984385066460254733880605256647363902160732102443656154852856590692595277855257563778420931571542568909508097863188313682143846785967742550551892529594
64789355362156997209060563934601356099502572088165523220585654567621525989833435792412071673530213110438235461609950233494658197320013934260142370525768530730648174392038504
89307475026119919108600127180985930937572274379190999324023048980609635572348358816072484994067170269394212885704794032888031826978293616900979564841015208237311036093100150
81851223324633173258785905907612479870628855689431012390109729200781940753684416562294413315647188319356591771633913545892011373776362193636814506011844368620196727006732532
80529883042295074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669
38102871794508560465821983194059528341619175314034894163206925073632423415715700412910266907296199739275914809783683066318757293297556425091860552963585268849419030407270774
18799850545935706025465473291910192906070443650070875911039570607616786357338497871225191307997043081471655999488490728383130707030588519568786693870441355295698957856629370777669702946252237034
 public exponent: 65537
 Validity: [From: Tue Jan 28 13:31:54 UTC 2014,
             To: Wed Mar 17 18:33:33 UTC 2021]
 Issuer: CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
 SerialNumber: [    6acaf5c9 85274c50 27ba2928 3006d6e4 c4f15a9b]

Certificate Extensions: 7
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.quovadisglobal.com,
```

```
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://trust.quovadisglobal.com/qvrca.crt]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 8B 4B 6D ED D3 29 B9 06   19 EC 39 39 A9 F0 97 84  .Km..)....99....
0010: 6A CB EF DF                                        j...
]

]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.quovadisglobal.com/qvrca.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F8 0F 65 1C 7A 63 19 AA   BF 44 6F A6 49 12 21 F3  ..e.zc...Do.I.!.
0010: 7A 5D E3 0D                                        z]..
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 4E 04 84 57 BF 82 C8 BE   65 FA B0 95 94 6D E3 B8  N..W....e....m..
0010: D5 58 5D 73 3E 15 FA 26   80 08 C3 22 C2 0F 0B CA  .X]s>..&..."....
0020: 58 D5 48 F1 49 B3 90 43   4A 0A 66 F9 53 D1 6F B8  X.H.I..CJ.f.S.o.
0030: 54 DC 51 90 6C 7D DA 1D   AB E4 F3 F0 F0 54 06 06  T.Q.l........T..
0040: 25 70 E8 A8 11 6B 2A 86   C9 66 B9 1E 99 23 82 49  %p...k*..f...#.I
0050: F2 40 B5 B5 CB 9F 3B 8C   CD 63 3E 4E D7 1C 5C 1C  .@....;..c>N..\.
0060: 06 97 DF 54 AF 10 D5 1F   E1 47 75 9D EF A3 74 2D  ...T.....Gu...t-
0070: C3 27 D8 43 6F F7 F0 52   4E FC 41 91 93 E9 A8 E2  .'.Co..RN.A.....
0080: D9 C6 1E 7A D6 21 F9 09   06 A8 22 0E 89 82 8A 2C  ...z.!....".....,
0090: B5 D4 C7 DA 1F 33 6E 09   AB 79 96 A8 13 F8 40 38  .....3n..y....@8
00A0: 2C 5A 0A 10 EC B9 4B 03   E3 F0 34 EB FD 66 8B FD  ,Z....K...4..f..
00B0: D0 D6 98 0F A0 F4 20 C9   FF 75 5D 44 EC 44 A1 2C  ...... ..u]D.D.,
00C0: AF 55 66 25 BD 5B E0 EE   3D 22 9A 08 0B 9C 49 22  .Uf%.[..="....I"
00D0: BB 75 4D B5 9C 7E 54 B4   1D F4 10 6B 3A D3 2C BA  .uM...T....k:.,.
00E0: 84 D1 B7 27 F5 45 71 0B   AF BB 7B 83 26 A2 36 4D  ...'.Eq.....&.6M
00F0: 3E 47 0F A8 5B 37 C2 4C   2B EC F5 B3 97 9D 1C 4E  >G..[7.L+......N

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFjzCCBHegAwIBAgIUasr1yYUnTFAnuikoMAbW5MTxWpswDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxJTAj
BgNVBAsTHFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxLjAsBgNVBAMTJVF1
b1ZhZGlzIFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTI4MTMz
MTU0WhcNMjEwMzE3MTgzMzMzWjBYMQswCQYDVQQGEwJCRTEgMB4GA1UEChMXUXVv
VmFkaXMgVHJ1c3RsaW5rIEJWQkExJzAlBgNVBAMTHlF1b1ZhZGlzIEJlbGdpdW0g
SXNzdWluZyBDQSBHMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAO/S
7zDGARkRKs9BxEzbGZoDK3e9m5SV6JzMaLUpFkzXzzkyRJbMphLgSOl6VtYAA+fg
H9dawUV1fr2qLoBtp74tpNl1GdXIYI++WM0j/sgy2JnhTDOpcLV++zP8eN+SP5Oo
wiDTqTxjQASSt+fmRvmgCIsGLCS3g67DSN/xCPdymefuoQWNNaxDnkIpArmRKElH
jH+JS4jxjxtHhOlGgEFbPw41DyRPtFL3nDwQeTEgGvpxDUkuTD03lMdeHvGy3zZe
pAm/pmhVx9z7L6fNrgIu+rW6CSD5deO59M8N4oXs5L8dsVv3mh1DHp5kyoY+qZAw
T7NqKEbT8GkqoRs4uBXLuRPTCl6le1thTETBCrZRKLl9aZ8AP0NkAlo5Rl0PR7LS
XeZtzKhp37p9dxOOy16LurdVf0XMvjVUZ2LP+X+ZgDZmYm4FfoxKihrHXnaTAckL
+nTsDQ49cYQvfgOGHH6+hrYJdR/ypa3Yf1s1YrNz5s+gSarp6eGWyDvNcugQ4TDW
J46Cr8EOgo7x3Vkk8+RAHtSB0MFuBaupqVRgdVAVqU3wF7B2puwxxmGcvQbgLGkH
1+bplVk/c6q/zICWWeD4SjTSChpbCnldJzkV2tKRFImlf9bv87G0x7WJoLSnLsa/
Qs1YhKGjX9MndQnvSFuwrJLvtzXPC2XaXYxXoJknAgMBAAGjggEoMIIBJDASBgNV
HRMBAf8ECDAGAQH/AgEAMHEGCCsGAQUFBwEBBGUwYzAqBggrBgEFBQcwAYYeaHR0
cDovL29jc3AucXVvdmFkaXNnbG9iYWwuY29tMDUGCCsGAQUFBzAChilodHRwOi8v
dHJ1c3QucXVvdmFkaXNnbG9iYWwuY29tL3F2cmNhLmNydDARBgNVHSAECjAIMAYG
BFUdIAAwDgYDVR0PAQH/BAQDAgEGMB8GA1UdIwQYMBaAFItLbe3TKbkGGew5Oanw
l4Rqy+/fMDgGA1UdHwQxMC8wLaAroCmGJ2h0dHA6Ly9jcmwucXVvdmFkaXNnbG9i
YWwuY29tL3F2cmNhLmNybDAdBgNVHQ4EFgQU+A9lHHpjGaq/RG+mSRIh83pd4w0w
DQYJKoZIhvcNAQELBQADggEBAE4EhFe/gsi+ZfqwlZRt47jVWF1zPhX6JoAIwyLC
```

DwvKWNVI8UmzkENKCmb5U9FvuFTcUZBsfdodq+Tz8PBUBgYlcOioEWsqhslmuR6Z
I4JJ8kC1tcufO4zNYz5O1xxcHAaX31SvENUf4Ud1ne+jdC3DJ9hDb/fwUk78QZGT
6aji2cYeetYh+QkGqCIOiYKKLLXUx9ofM24Jq3mWqBP4QDgsWgoQ7LlLA+PwNOv9
Zov90NaYD6D0IMn/dV1E7EShLK9VZiW9W+DuPSKaCAucSSK7dU21nH5UtB30EGs6
0yy6hNG3J/VFcQuvu3uDJqI2TT5HD6hbN8JMK+z1s5edHE4=
-----END CERTIFICATE-----

QuoVadis BE PKI Certification Authority G2

Type	CA/QC
Status	granted
Status starting time	2018-02-08T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	37086194365877306047544927857258417826279931451 7
Signature algorithm	SHA256withRSA
Issuer	CN=QuoVadis Enterprise Trust CA 1 G3, O=QuoVadis Limited, C=BM
Valid from	Mon Jun 13 12:22:05 UTC 2016
Valid to	Sat Jun 13 12:22:05 UTC 2026
Subject	CN=QuoVadis Belgium Issuing CA G2, O=QuoVadis Trustlink BVBA, OID.2.5.4.97=NTRBE-0537698318, C=BE
Public key	Sun RSA public key, 4096 bits modulus: 623088369958782373989038775437907047721515535194850369628492892867626590968760013487140595039804690588476583228163560342281325406918046605165432002116706169653521048417532557931231131550972290003119722826836304026898294102318795786104267603483402033307062071907725800429830346155840706133863659522208361534393413846926578696826895714227903391959565967406530088771729767950440929656043216301458534589881617252192037684023672312080578911531264538787094518573480249000064877305531406065948039128854366518032256227604949718044388445919353619902272978753999638960838408864058539228388888479106605465459304370381737882803810163755318282895848388976932482946581771780007339197149254499947922990967256608264691415787505237699654446749447000128867835773633689728589749900455455319090699985484921038680916093288098301753746986699829404622404868071877704062572758631087788200363289569649080722571785143125565781944574264061476509602921155725032494954347404540188432827496460397682941622995610157763156443595757370452444868333800151563706382102943186592677922050256250273430059031604111004357902651789701181087824146360347223046255190611473747043852317503717497250927026791542693181089165688800622906042384672374815917738285418783956236392611131 public exponent: 65537
Subject key identifier	87c9bc3197127a73bb7ec03d4551b401259551ab
CRL distribution points	http://crl.quovadisglobal.com/qventca1g3.crl
Authority key identifier	6c26bd605529294e663207a0ff638b835a4b34c6
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	a8884570c16ec0337170e5058f960d74aaf67a78
SHA256 Thumbprint	d90b40132306d1094608b1b9a2f6a9e23b45fe121fef514a1c9df70a815ad95c

Extension (critical: true)

Additional service information

ForeSignatures

Extension (critical: true)

Additional service information

ForeSeals

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=QuoVadis Belgium Issuing CA G2, O=QuoVadis Trustlink BVBA, OID.2.5.4.97=NTRBE-0537698318, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
623088369958782373989038775437907047721515535194850369628492892867626590968760013487140595039804690588476583228163560342281325406918046605165432002116706169653521048417532557932131135509722900031197228268363040268982941023187957861042676034834020333070620719077258004298303461558407061338636595222083615343934138469265786968268957142279033919595659674065300887717297679504409296560432163014585345898816172521920376840236723120805789115312645387870945185734802490000648773055314060659480391288543665180322562276049497180443884459193536199022729787539996389608384088640585392283888884791066054654593043703817378828038101637553182828958483889769324829465817717800073391971492544999479229909672566082646914157875052376996544467494447000128867835773633689728589749900045545531909069998548492103868091609328809830175374698669982940462240486807187770406257275863108778820036328956964908072257178514312556578194457426406147650960292115572503249495434740454018843282749646039768294162299561015776315644359575737045244486833380015156370638210294318659267792205025625027343005903160411100435790265178970118108782414636034722304625519061147374704385231750371749725092702679154269318108916568880062290604238467237481591773828541878395623639261113
 public exponent: 65537
 Validity: [From: Mon Jun 13 12:22:05 UTC 2016,
             To: Sat Jun 13 12:22:05 UTC 2026]
 Issuer: CN=QuoVadis Enterprise Trust CA 1 G3, O=QuoVadis Limited, C=BM
 SerialNumber: [    40f60653 43c04cb6 71e9c825 0e90ebd5 8dd86e55]

Certificate Extensions: 7
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://trust.quovadisglobal.com/qventca1g3.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.quovadisglobal.com]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 6C 26 BD 60 55 29 29 4E   66 32 07 A0 FF 63 8B 83  l&.`U))Nf2...c..
0010: 5A 4B 34 C6                                        ZK4.
]

]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.quovadisglobal.com/qventca1g3.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 87 C9 BC 31 97 12 7A 73   BB 7E C0 3D 45 51 B4 01  ...1..zs...=EQ..
0010: 25 95 51 AB                                        %.Q.
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
```

```
0000: A7 67 CB E3 94 A6 46 5B   5D 0E 02 E9 B3 7E 64 CC  .g....F[].....d.
0010: 5C EB A6 75 7C 27 5C 3E   8A 26 E9 9C 77 24 F3 C3  \..u.'\>.&..w$..
0020: E4 4D 3F 9C C6 30 C2 77   02 86 06 DB 5E 1E 28 82  .M?..0.w....^.(.
0030: 38 09 6F 65 27 C5 89 BA   58 5F 5A 9F 16 0C 5F 50  8.oe'...X_Z..._P
0040: 13 A7 B1 19 61 C7 EE F7   44 92 6B A4 95 E7 66 80  ....a...D.k...f.
0050: 95 95 83 41 96 96 20 50   45 4B 09 83 52 3B EC C1  ...A.. PEK..R;..
0060: BE 41 0A B1 3F 0A 80 DF   B9 12 3E 17 3E 16 E9 DC  .A..?.....>.>...
0070: 99 9A CF 26 0E 0E E6 AD   C4 80 FB 79 71 B1 D2 14  ...&.......yq...
0080: 8F 4F C5 DF 17 C2 F4 2F   77 04 7A 9B 18 C3 56 43  .O...../w.z...VC
0090: B6 84 CD FA 32 1C 73 5C   6A 50 AB 10 BA B6 06 E7  ....2.s\jP......
00A0: 9F 41 AB 7B 26 C0 0E 8E   20 BE 9A E2 18 91 18 1E  .A..&... .......
00B0: 84 59 FF 45 76 A7 17 50   5C 30 CE 05 52 B8 6F 2E  .Y.Ev..P\0..R.o.
00C0: 08 B7 51 85 A9 A7 86 B2   FF 32 F6 1C EF EB 22 89  ..Q......2....".
00D0: 9C BA 0E 64 DF BC BA 3C   2F DA 0D D6 14 C4 C2 D7  ...d...</.......
00E0: 17 0E 5D 9F 77 F8 03 90   30 AC 78 EE BF 1D B7 33  ..].w...0.x....3
00F0: E7 13 3B 49 DC 0C C4 D1   BB 24 8C E1 38 C5 C2 70  ..;I.....$..8..p
0100: BD 36 00 B5 16 49 35 72   BD AC 46 DA 37 0D 51 9D  .6...I5r..F.7.Q.
0110: 2E 78 24 79 F5 39 FD F8   DE D8 73 CB 5E CC 9A 54  .x$y.9....s.^..T
0120: 8A 3E 8E F8 A0 EE 21 B0   8D 67 0D 0C 9E EC 1F A2  .>....!..g......
0130: 2A 24 B3 8B 50 48 4D 38   25 1A DC 0E 34 4A D0 A8  *$..PHM8%...4J..
0140: 78 2B D3 F1 C8 EA D0 5A   F2 1F F5 7F 79 15 65 8A  x+.....Z....y.e.
0150: EE F4 D0 29 39 81 99 29   45 38 71 3A AE 21 1F 99  ...)9..)E8q:.!..
0160: A0 57 F1 A6 9D 94 22 39   88 64 03 D5 23 05 C0 F0  .W....“9.d..#...
0170: 38 C4 58 F0 22 77 AC BE   E4 7C 08 2E 9F 59 92 74  8.X."w.......Y.t
0180: 0A B7 91 7D A9 6D D1 C3   1C DD 60 9A D6 4D D8 59  .....m....`..M.Y
0190: 17 C8 8C DC 1B 89 A7 00   AD 53 4E E7 2C 19 68 DE  .........SN.,.h.
01A0: A7 6A 6E BA 16 73 76 20   80 15 12 6E A8 35 8E 1C  .jn..sv ...n.5..
01B0: 4E A1 AA EA C0 D7 FE A9   8E 03 DB 02 E6 8C FD E5  N...............
01C0: D8 AE 4F B4 D9 E4 94 F4   88 9B 9C 00 B0 28 1A DE  ..O.........(..
01D0: 79 77 44 0A B2 37 A3 85   8C A3 7D 84 E0 7E 56 4B  ywD..7........VK
01E0: 44 ED C2 F6 38 5B 4A 86   1B 8C 2D 08 1A B8 D0 62  D...8[J...-....b
01F0: 64 36 DA 6E 82 A5 D9 C8   12 5F 2A AB 05 87 8E 75  d6.n....._*....u

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGiTCCBHGgAwIBAgIUQPYGU0PATLZx6cglDpDr1Y3YblUwDQYJKoZIhvcNAQEL
BQAwVDELMAkGA1UEBhMCQk0xGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxKjAo
BgNVBAMMIVF1b1ZhZGlzIEVudGVycHJpc2UgVHJ1c3QgQ0EgMSBHMzAeFw0xNjA2
MTMxMjIyMDVaFw0yNjA2MTMxMjIyMDVaMHMxCzAJBgNVBAYTAkJFMRkwFwYDVQRh
DBBOVFJCRS0wNTM3Njk4MzE4MSAwHgYDVQQKDBdRdW9WYWRpcyBUcnVzdGxpbmsg
QlZCQTEnMCUGA1UEAwweUXVvVmFkaXMgQmVsZ2l1bSBJc3N1aW5nIENBIEcyMIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAmLsm3G2sWV/LTr0gC5iOXSSL
DXGEdSFvK7dsEU4wgvy3kv2sL1bpx4g9UjmoQuUiLVfvuIWOSmcunFA9CoTf+vK4
uTxqvYjOVdd6dAjUx4D+xgGGdQdONKFNv+V6PPZ7KziNO/QfJWZhw31sRv/3vybb
ZdVFcaEoGhisYw6GpJ+nQfzyTuvwnjyFdNsS5qA4YgNXrmHcH91PMrM3pesCa0iA
hB24snUAJjyggJWXLR3rUm7QXgOulkfQtFEPwvq66kmVt6To45h8CvmCcwqDLPp/
H1N2oMuTfEnxqDFwUP4pRHcCzUt9CWNdk8wUyyUWnWd5/YMFI2rMK5tdycfuwzxv
LJn4LOUEqn0hvxtV4w1Q15MV7ipM1AiPpaWXE1WU7BNFcKO2aPWygQnkJOEKW7fg
Aq0QG0FdqqGb12v1c06EQvRi5D5SJQNq15A5cpqy8XdaeXkANP/IlAMI1cnsPMBS
IySuQ00zQVqHiIv+q3kls3oz7PV1aglrZ3pJXp9BZGPdcZjhJh5JkVaF8zQ6qrLP
a+YO8/ud2Bklt6I0E4EY/637VhcPYTlfxmvZIPfHjM8HWdjBg2c/i+sd5CsIfeeU
OWlUZV3jZbtgQijhe3meejHpbYzggZKM0jUU8/p6vsvzBKRhqj2bgABByUcFaLHH
LTBX3BKrSpS+hjgan7kCAwEAAaOCATIwggEuMHYGCCsGAQUFBwEBBGowaDA6Bggr
BgEFBQcwAoYuaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9xdmVudGNh
MWczLmNydDAqBggrBgEFBQcwAYYeaHR0cDovL29jc3AucXVvdmFkaXNnbG9iYWwu
Y29tMB0GA1UdDgQWBBSHybwxlxJ6c7t+wD1FUbQBJZVRqzASBgNVHRMBAf8ECDAG
AQH/AgEAMB8GA1UdIwQYMBaAFGwmvWBVKSlOZjIHoP9ji4NaSzTGMBEGA1UdIAQK
MAgwBgYEVR0gADA9BgNVHR8ENjA0MDKgMKAuhixodHRwOi8vY3JsLnF1b3ZhZGlz
Z2xvYmFsLmNvbS9xdmVudGNhMWczLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZI
hvcNAQELBQADggIBAKdny+OUpkZbXQ4C6bN+ZMxc66Z1fCdcPoom6Zx3JPPD5E0/
nMYwwncChgbbXh4ogjgJb2UnxYm6WF9anxYMX1ATp7EZYcfu90SSa6SV52aAlZWD
QZaWIFBFSwmDUjvswb5BCrE/CoDfuRI+Fz4W6dyZms8mDg7mrcSA+3lxsdIUj0/F
3xfC9C93BHqbGMNWQ7aEzfoyHHNcalCrELq2BuefQat7JsAOjiC+muIYkRgehFn/
RXanF1BcMM4FUrhvLgi3UYWpp4ay/zL2HO/rIomcug5k37y6PC/aDdYUxMLXFw5d
n3f4A5AwrHjuvx23M+cTO0ncDMTRuySM4TjFwnC9NgC1Fkk1cr2sRto3DVGdLngk
efU5/fje2HPLXsyaVIo+jvig7iGwjWcNDJ7sH6IqJLOLUEhNOCUa3A40StCoeCvT
8cjq0FryH/V/eRVliu700Ck5gZkpRThxOq4hH5mgV/GmnZQiOYhkA9UjBcDwOMRY
8CJ3rL7kfAgun1mSdAq3kX2pbdHDHN1gmtZN2FkXyIzcG4mnAK1TTucsGWjep2pu
uhZzdiCAFRJuqDWOHE6hqurA1/6pjgPbAuaM/eXYrk+02eSU9IibnACwKBreeXdE
CrI3o4WMo32E4H5WS0TtwvY4W0qGG4wtCBq40GJkNtpugqXZyBJfKqsFh451
-----END CERTIFICATE-----
```

Zetes S.A./N.V.

Service provider trade name	VATBE-0408425626
Information URI	https://repository.tsp.zetes.com
Service provider street address	Straatsburgstraat 3
Service provider postal code	1130
Service provider locality	Haren

Service provider state	Brussels
Service provider country	BE

Zetes TSP PKI certification authority

Type	CA/QC
Status	granted
Status starting time	2016-06-30T22:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	4044494821122691399
Signature algorithm	SHA256withRSA
Issuer	CN=ZETES TSP ROOT CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE
Valid from	Fri May 20 17:20:29 UTC 2016
Valid to	Wed May 20 17:20:29 UTC 2026
Subject	CN=ZETES TSP QUALIFIED CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE
Public key	Sun RSA public key, 4096 bits modulus: 796670963707404071432065818493803891702809240590462420290375347747994588113208099700729051785414484823482525435876673110437515420735604726572971351905453910263879782247724079533201420434980906125965224730804606662799039976870403500931229888155317082614573594704517179372017197856526130176823910307008895492699896270264105325707292486709403261729124934205264059173193364705541586249507683415359327192536525709342120955928411872179790740473158323149626825194303559561225493008161461440799137419524601916152077655659687136786182992996855987043403957104672173646950330802423343213508073306982585360184966777581336760412791331765639203806282433736523279259847931051729072468470236770944148214553513939620511218083182177840750610896383923573133536872261434818526596231169060655010327374464747028050258051208770260865253192866646123025398160614262520735143117298693992724870873712485454606901345087223985476499537104029642559990594063568574302420354537223370647609793591407046929694019477470638647390455920090693898311187309030812183921530631483626309588304299585290362437034578598825004653047384241045855121661319645975335646628176987427562630329145631982930345735549926310183701470429519753966691572749129654680349494485283853717680609119 public exponent: 65537
Subject key identifier	e2b4db5f6a0f025054d51defd27672722195462b
CRL distribution points	http://crl.tsp.zetes.com/ZETESTSPROOTCA001.crl
Authority key identifier	38bc5c3054dce2bb20efee6f41a0316e5cfd8b75
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	1698dc47f4f5ff956c560324e1965aa7ed38e29d
SHA256 Thumbprint	d628417a992140d3bd98b310d6de33d04a91c49221841dbf0f52c81fd2fafab5

Extension (critical: true)

Additional service information

ForeSignatures

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=ZETES TSP QUALIFIED CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
796670963707404071432065818493803891702809240590462420290375347747994588113208099700729051785414484823482525435876673110437515420735604726572971351905453910263879782247724079533201420434980906125965224730804606662799039976870403500931229888155317082614573594704517179372017197856526130176823910307008895492699896270264105325707292486709403261729124934205264059173193364705541586249507683415359327192536525709342120955928411872179790740473158323149626825194303559561225493008161461440799137419524601916152077655659687136786182992996855987043403957104672173646950330802423343213508073306982585360184966777581336760412791331765639203806282433736523279259847931051729072468470236770944148214555313939620511218083182177840750610896383923573133536872261434818526596231169060655010327374464747028050258051208770260865253192866646123025398160614262520735143117298693992724870873712485454606901345087223985476499537104029642559990594063568574302420354537223370647609793591407046929694019477470638647390455920090693898311187309030812183921530631483626309588304299585290362437034578598825004653047384241045855121661319645975335646628176987427562630329145631982930345735549926310183701470429519753966691572749129654680349494485283853717680609119
 public exponent: 65537
 Validity: [From: Fri May 20 17:20:29 UTC 2016,
             To: Wed May 20 17:20:29 UTC 2026]
 Issuer: CN=ZETES TSP ROOT CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE
 SerialNumber: [    3820ee9c 74ecd147]

Certificate Extensions: 7
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://crt.tsp.zetes.com/ZETESTSPROOTCA001.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.tsp.zetes.com]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 38 BC 5C 30 54 DC E2 BB   20 EF EE 6F 41 A0 31 6E  8.\0T... ..oA.1n
0010: 5C FD 8B 75                                        \..u
]

]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.tsp.zetes.com/ZETESTSPROOTCA001.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 73 3A   2F 2F 72 65 70 6F 73 69  . https://reposi
0010: 74 6F 72 79 2E 74 73 70   2E 7A 65 74 65 73 2E 63  tory.tsp.zetes.c
0020: 6F 6D                                              om

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 2E 0C 2C 5A 45 54 45   53 20 54 53 50 20 43 50  0..,ZETES TSP CP
0010: 53 20 66 6F 72 20 4E 43   50 2B 20 61 6E 64 20 51  S for NCP+ and Q
0020: 43 50 2B 20 63 65 72 74   69 66 69 63 61 74 65 73  CP+ certificates

]]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E2 B4 DB 5F 6A 0F 02 50   54 D5 1D EF D2 76 72 72  ..._j..PT....vrr
0010: 21 95 46 2B                                        !.F+
]
]
```

```
]
 Algorithm: [SHA256withRSA]
 Signature:
0000: A8 7C 4D 53 16 D5 F8 35   E4 4F F2 02 A7 B6 1C BC  ..MS...5.O......
0010: DF 47 85 B2 54 AC 53 8B   9A D1 2D 35 F3 70 56 75  .G..T.S...-5.pVu
0020: 2F 8B CE EB 40 9B 34 00   EF ED A9 62 95 90 9A C5  /...@.4....b....
0030: 90 A3 1A 5C 04 7A 3C 53   6C 9E 87 E4 70 2B 36 64  ...\.z<Sl...p+6d
0040: D8 52 05 9C E5 10 79 7A   EC B6 AD A4 00 60 F9 B8  .R....yz.....`..
0050: F3 F0 1B F4 CD 51 AA 80   13 B1 66 2A 2B 27 90 DF  .....Q....f*+'..
0060: D1 60 7F D9 D0 0E ED A8   40 7A 52 4B 5F 3C A3 BE  .`......@zRK_<..
0070: 16 04 A8 90 1E 50 50 EA   B7 C1 8E CC C5 12 D7 A6  .....PP.........
0080: 12 0B 65 38 B2 3B AE 75   7F 18 27 C8 86 AD 2B 1D  ..e8.;.u..'...+.
0090: 50 5D C6 10 11 79 5F 3F   52 C2 8B F7 26 E2 44 94  P]...y_?R...&.D.
00A0: F5 66 46 EE B6 F6 6F 1C   CE 28 E5 DF 86 E4 71 FC  .fF...o..(....q.
00B0: AC 78 A0 FB 45 F8 AA EE   F6 FB 04 8D 59 C8 6E 98  .x..E.......Y.n.
00C0: AD D4 3F CE 33 3C BF 98   26 FA 60 71 F7 F3 A6 64  ..?.3<..&.`q...d
00D0: B7 8D C1 C5 04 E2 B0 6B   80 D7 3D DD 7C 79 67 F0  .......k..=..yg.
00E0: 10 DB F5 C4 F4 27 CE DC   AD 4B 44 F3 83 C4 99 A6  .....'...KD.....
00F0: 0B A7 04 9B B8 9E 8A C0   DA 32 86 80 F7 84 E9 5D  .........2.....]
0100: 51 AC 7F 57 D1 95 A3 94   A1 66 B6 90 A7 45 71 A3  Q..W.....f...Eq.
0110: FA A9 09 68 55 53 12 81   0E D3 99 2A 2A 9E 56 47  ...hUS.....**.VG
0120: 5B 7D BF 4A B9 2C 9D 9D   ED 0A 71 69 B8 45 62 50  [..J.,....qi.EbP
0130: E8 72 6C 72 31 8F 45 68   D2 BD 5A 84 AD EC CB 2F  .rlr1.Eh..Z..../
0140: CF 21 A1 89 4B 7C 1B B9   E6 07 B8 33 D5 DF 20 8F  .!..K......3.. .
0150: 78 56 3E 9A D7 FC 8E 1D   8A 50 09 AA 82 A6 A9 B4  xV>......P......
0160: 86 C4 3A AF 98 AF 3B 5D   E9 AE 46 AA 19 60 2C 96  ..:...;]..F..`,.
0170: A8 67 A5 F7 B9 2E C3 E6   45 A0 8B BD ED 70 73 A4  .g......E....ps.
0180: E6 5D B8 FF 04 A7 A2 D6   93 5B 82 11 A9 94 03 66  .].......[.....f
0190: 62 F9 18 1C F5 BE F8 04   2A E0 E1 82 E6 0E FD 6C  b.......*......l
01A0: 08 45 C5 6B 7C 37 E9 10   7A 92 5A 3C 13 62 3F 78  .E.k.7..z.Z<.b?x
01B0: B3 5A 85 1E 2E 45 3A 58   86 C2 B2 B8 4B 6C 64 E3  .Z...E:X....Kld.
01C0: F5 FB 4D 91 66 82 DB 5F   B1 E6 64 1C 2B 6E F0 3C  ..M.f._..d.+n.<
01D0: 24 CA 74 49 99 24 B3 7C   E1 4B F0 C8 CA 60 22 8A  $.tI.$...K...`".
01E0: 83 C4 3D C4 3D A8 CC 9B   C2 4A 96 8D B6 E2 D1 81  ..=.=....J......
01F0: E6 48 37 E2 B4 78 D6 C1   D5 D8 EC DB 28 0D 6A 3B  .H7..x......(.j;

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIG5jCCBM6gAwIBAgIIOCDunHTs0UcwDQYJKoZIhvcNAQELBQAwYTELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMR4wHAYDVQQDDBVaRVRFUyBUU1AgUk9PVCBDQSAwMDEwHhcNMTYw
NTIwMTcyMDI5WhcNMjYwNTIwMTcyMDI5WjBmMQswCQYDVQQGEwJCRTEkMCIGA1UE
CgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMQwwCgYDVQQFEwMwMDExIzAh
BgNVBAMMGlpFVEVTIFRTUCBRVUFMSUZJRUQgQ0EgMDAxMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAw0ePE++btk1uYouqDgClGmrIekzMp8kFfDsZWrD7
IwQCpMs5YJv+LiGkLHOhG0U8RQYy9rWxy3wEpMgo4uPViBNSc/gM0jjCJBq3nuLc
mXUJIaqPmEcTfk8fWwJGTBZ22/HAEDKdBGl42iNziiArq86//GyHlAnogIZg/1MJ
CjEFf0XyjXSx9oTfH8Qyg1oogtI00WgG9KZs4Ik4pgcyEKrMqvD8EGHNWhwMyGdG
eX4sBI5cJxai2nqp+39wLkzJ/S4V5ZJNNcGDAzvjQiORz5zx/+2+/9M0wPIbNxtU
pn+7BM7az3tfQWYOIEDP3/hI8pwBq+C5M12I9P2VkQqckQ/33ROSv1c0I4gZSUKx
iTM7IrxLo9bvJi8s/9A9VtGmqxbEuYs4WduEEhQX+hhTBopQ0Erzi9plTMpv58Ij
fMCc+DUoLnaCuvkb6wdUnKVfbZsK4rTAoIL0K2idTEf9PAP39F9UElsLtAeDHR5e
RsWw7RVarop8Drx9cMOaXqKyvUJyAdYLBHi2UrgvKKFVaf7s6lrRbqr6PMnP4fni
PGxnrnxVl4CUdwtNhH7odlM6UX55lzikPilx9jGFYrliTq5SYgQhg0IoVx5RifZP
pCh6gF1O4DJyCGA6XlTnOYoKPWg/ih7WqfhY50nFvwar0esA5RUqHfF4GgFrqcC6
118CAwEAAaOCAZswggGXMHEGCCsGAQUFBwEBBGUwYzA6BggrBgEFBQcwAoYuaHR0
cDovL2NydC50c3AuemV0ZXMuY29tL1pFVEVTVFNQUk9PVENBMDAxLmNydDAlBggr
BgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4EFgQU4rTb
X2oPAlBU1R3v0nZyciGVRiswEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAW
gBQ4vFwwVNziuyDv7m9BoDFuXP2LdTB9BgNVHSAEdjB0MHIGBFUdIAAwajAsBggr
BgEFBQcCARYgaHR0cHM6Ly9yZXBvc2l0b3J5LnRzcC56ZXRlcy5jb20wOgYIKwYB
BQUHAgIwLgwsWkVURVMgVFNQIENQUyBmb3IgTkNQKyBhbmQgUUNQKyBjZXJ0aWZp
Y2F0ZXMwPwYDVR0fBDgwNjA0oDKgMIYuaHR0cDovL2NybC50c3AuemV0ZXMuY29t
L1pFVEVTVFNQUk9PVENBMDAxLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcN
AQELBQADggIBAKh8TVMW1fg15E/yAqe2HLzfR4WyVKxTi5rRLTXzcFZ1L4vO60Cb
NADv7alilZCaxZCjGlwEejxTbJ6H5HArNmTYUgWc5RB5euy2raQAYPm48/Ab9M1R
qoATsWYqKyeQ39Fgf9nQDu2oQHpSS188o74WBKiQHlBQ6rfBjszFEtemEgtlOLI7
rnV/GCfIhq0rHVBdxhAReV8/UsKL9ybiRJT1ZkbutvZvHM4o5d+G5HH8rHig+0X4
qu72+wSNWchumK3UP84zPL+YJvpgcffzpmS3jcHFBOKwa4DXPd18eWfwENv1xPQn
ztytS0Tzg8SZpgunBJu4norA2jKGgPeE6V1RrH9X0ZWjlKFmtpCnRXGj+qkJaFVT
EoEQ05kqKp5WR1t9v0q5LJ2d7QpxabhFYlDocmxyMY9FaNK9WoSt7MsvzyGhiUt8
G7nmB7gz1d8gj3hWPprX/I4dilAJqoKmqbSGxDqvmK87XemuRqoZYCyWqGel97ku
w+ZFoIu97XBzpOZduP8Ep6LWk1uCEamUA2Zi+Rgc9b74BCrg4YLmDv1sCEXFa3w3
6RB6klo8E2I/eLNahR4uRTpYhsKyuEtsZOP1+02RZoLbX7HmZBwrbvA8JMp0SZkk
s3zhS/DIymAiioPEPcQ9qMybwkqWjbbi0YHmSDfitHjWwdXY7NsoDWo7
-----END CERTIFICATE-----
```

Portima s.c.r.l. c.v.b.a.

Service provider trade name	VATBE-0428775335
Information URI	https://www.portisign.be/fr/support
Service provider street address	Chaussée de La Hulpe 150 Boîte 16

Service provider postal code	1170
Service provider locality	Watermael-Boitsfort
Service provider state	Bruxelles
Service provider country	BE

PortiSign Users CA10

Type	CA/QC
Status	granted
Status starting time	2017-11-30T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	10018
Signature algorithm	SHA512withRSA
Issuer	CN=PortiSign Root CA, O=Portima s.c.r.l. c.v.b.a., OU=Security, STREET=Terhulpsesteenweg 150 Chaussée de la Hulpe, ST=Brussels, L=B-1170 Brussels, C=BE, EMAILADDRESS=security@portima.com, OID.2.5.4.20=0032 2 6614411
Valid from	Fri Jun 16 07:00:00 UTC 2017
Valid to	Wed Jun 16 07:00:00 UTC 2027
Subject	CN=PortiSign Users CA10 for Qualified Certificates, O=Portima s.c.r.l. c.v.b.a., C=BE
Public key	Sun RSA public key, 4096 bits modulus: 782233571000725055147082781552042919680656300016314134547210087187896597355883887363164778406749004104583252789170049053462777714543027813377832723686044148297352247511982636804558743064752710630104634643441610162613039330225863323756100715267856761208706636837217301282415148754586082947664708595343550515928240986856058903703273900457384328845246582324465256168787803317124987401334246273109581908305132021138452361508649991025080884452757399342104474102818209912607082416506142142548046418536894649736248961822380119351693256776860981717710315130994214488579044776384353133485605624724691954270326766137348088134498204776137926317383153071214096171523556146900789668617910941260655137015095840626016492911537726053232950941626095777957264249178084496030530417805736533411517930551846466538852567469967216248296246542336754461809399742692428777177711371704185511312868332076490508021626286376058134404749628647471462878938327392198840836357505581846785829429904695853208321937749429380971096036088821922356572408455806004360404411754521896456192611389416577140546599199984286425617514602780604465263348085101519821412158692760937791849160981740144608807504711070975278811081421505339688532082871955110727690279813674328209071723559 public exponent: 65537
Subject key identifier	49a4cc366ed611d7
CRL distribution points	http://crl.portisign.be/crl/root.crl
Authority key identifier	4fe2be327047b2b3
Key usage	keyCertSign cRLSign

Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	e72570644a41bdfd3fb11e408f13a2e355bf4dc7
SHA256 Thumbprint	676d7a24f3cf04400390144adc407f338b2eb447d0127d897a5a91c7ab694b09

Extension (critical: true)

Additional service information

ForeSignatures

Extension (critical: true)

Qualifications

Qualifier: QCNoQSCD

Criterial List Description

Assert: atLeastOne

Policy OID: 1.3.6.1.4.1.10438.3.2.4.10.1

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=PortiSign Users CA10 for Qualified Certificates, O=Portima s.c.r.l. c.v.b.a., C=BE
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
782233571000725055147082781552042919680656300016314134547210087187896597355883887363164778406749004104583252789170049053462777714543027813377832723686044148297352247511982636804558743064752710630104634643441610162613039330225863323756100715267856761208706636837217301282415148754586082947664708595343550515928240986856058903703273900457384328845246582324465256168787803317124987401334246273109581908305132021138452361508649991025080884452757399342104474102818209912607082416506142142548046418536894649736248961822380119351693256776860981717710315130994214488579044776384353133485605624724691954270326766137348088134498204776137926317383153071214096171523556146900789668617910941260655137015095840626016492911537726053232950941626095777957264249178084496030530417805736533411517930551846466538852567469967216248296246542336754461809399742692428777177711371704185511312868332076490508021626286376058134404749628647471462878938327392198840836357505581846785829429904695853208321937749429380971096036088821922356572408455806004360404411754521896456192611389416577140546599199984286425617514602780604465263348085101519821412158692760937791849160981740144608807504711070975278811081421505339688532082871955110727690279813674328209071723559
 public exponent: 65537
 Validity: [From: Fri Jun 16 07:00:00 UTC 2017,
            To: Wed Jun 16 07:00:00 UTC 2027]
 Issuer: CN=PortiSign Root CA, O=Portima s.c.r.l. c.v.b.a., OU=Security, STREET=Terhulpsesteenweg 150 Chaussée de la Hulpe, ST=Brussels, L=B-1170 Brussels, C=BE,
EMAILADDRESS=security@portima.com, OID.2.5.4.20=0032 2 6614411
 SerialNumber: [    2722]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4F E2 BE 32 70 47 B2 B3                            O..2pG..
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.portisign.be/crl/root.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 49 A4 CC 36 6E D6 11 D7                            I..6n...
]
]

]
```

```
 Algorithm: [SHA512withRSA]
 Signature:
0000: 70 AA 23 B3 D1 2F 9E 27   D3 33 B7 79 45 FC 8A 4E  p.#../.'.3.yE..N
0010: 6E F8 03 DF 72 B4 F6 87   87 A1 05 28 95 F9 B6 30  n...r......(...0
0020: E4 E9 C7 EE 9F D2 42 4F   B6 72 B6 DD 59 8B A1 D3  ......BO.r..Y...
0030: F1 6C C9 EB F5 66 65 F0   08 21 1F 8E 0C D2 D2 4B  .l...fe..!.....K
0040: 1E 8A 05 9A 6E 44 DA 7A   8A D7 DE 62 55 2F BF 9C  ....nD.z...bU/..
0050: F0 89 F5 B5 F3 32 68 A0   69 0A 88 70 BC B8 DD A5  .....2h.i..p....
0060: 82 A9 5B D8 F0 22 D2 0A   10 D1 89 30 67 E5 03 8F  ..[.."......0g...
0070: E0 F3 95 8E 00 FC 9A B2   95 80 88 09 3C 8E DC 4C  ............<..L
0080: B2 C3 DA 4B 40 DD A0 CD   78 7A 1A 62 C5 42 53 D0  ...K@...xz.b.BS.
0090: 79 8D DD 46 54 91 B8 DD   06 E2 A9 3A 10 F2 45 B1  y..FT......:..E.
00A0: 56 DA 52 9B 3D 8E EC C1   0F E9 FD B0 B9 38 EC 80  V.R.=........8..
00B0: 29 0F 1A 57 38 F3 C9 E8   85 03 B4 EC 2E E9 51 57  )..W8.........QW
00C0: D8 C7 1B 22 39 56 01 10   51 7E AA 00 7A EA 48 8C  ..."9V..Q...z.H.
00D0: 7F 78 72 CE 69 D6 DD 21   DF 3D 3C 0B 84 C0 42 74  .xr.i..!.=<...Bt
00E0: EA B3 1F 5E 86 CD 2D 71   DF 1C 73 15 2C 38 F9 54  ...^..-q..s.,8.T
00F0: 78 14 A4 2D 60 C0 E4 CA   E0 0D 2D C0 84 CB 3D 8E  x..-`.....-...=.
0100: 19 E8 2F B8 84 27 E6 22   58 2C 5B FF 88 42 95 49  ../..'."X,[..B.I
0110: 57 2D CB CE ED DD B0 FE   B2 B4 D5 87 83 B5 04 E7  W-..............
0120: 8A 78 41 AE F3 04 1E DF   73 97 01 6F 2F F2 49 1F  .xA.....s..o/.I.
0130: CB B5 7D 5C 51 97 77 E4   B3 2C FC 7D 4A F9 8E EC  ...\Q.w..,..J...
0140: BE BF B3 C0 44 33 B4 33   C5 B9 12 80 E8 31 D7 83  ....D3.3.....1..
0150: 95 08 31 7F C0 49 D0 08   53 33 BA 2A 43 B5 56 31  ..1..I..S3.*C.V1
0160: D5 8B 35 CC 04 B6 12 43   89 2D 9B 21 34 47 AD 64  ..5....C.-.!4G.d
0170: 20 77 04 9C EE 6B 67 B8   D6 37 FF 76 B8 E1 79 AB   w...kg..7.v..y.
0180: 9D C1 E8 71 FA 57 7A 15   1C C2 37 77 F7 BF 25 41  ...q.Wz...7w..%A
0190: B8 D6 F0 51 4D E0 22 39   CD 36 D5 97 32 41 61 71  ...QM."9.6..2Aaq
01A0: 65 16 32 F8 4B 8B 99 8D   95 DC 43 C9 C0 0C 50 1E  e.2.K.....C...P.
01B0: B5 65 E2 90 D0 EE 91 8B   26 D1 A8 23 C0 E5 7D 74  .e......&..#...t
01C0: 47 41 57 F2 30 4C 73 C6   6A F9 0E 65 70 79 08 4B  GAW.0Ls.j..epy.K
01D0: 3D 34 CD 71 F4 D1 7B 59   22 3F 4B 77 A8 37 40 F1  =4.q...Y"?Kw.7@.
01E0: 45 5D 26 6E 3C 67 43 7D   10 EE 23 84 AB 4E 96 98  E]&n<gC...#..N..
01F0: E7 90 EF 18 78 2F FE C4   63 C4 9B 9D 7B 2A CE E9  ....x/..c....*..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGfjCCBGagAwIBAgICJyIwDQYJKoZIhvcNAQENBQAwggEBMRcwFQYDVQQUEw4w
MDMyIDIgNjYxNDQxMTEjMCEGCSqGSIb3DQEJARYUc2VjdXJpdHlAcG9ydGltYS5j
b20xCzAJBgNVBAYTAkJFMRgwFgYDVQQHEw9CLTExNzAgQnJ1c3NlbHMxETAPBgNV
BAgTCEJydXNzZWxzMTQwMgYDVQQJDCtUZXJodWxwc2VzdGVlbndlZyAxNTAgQ2hh
dXNzw6llIGRlIGxhIEh1bHBlMREwDwYDVQQLEwhTZWN1cml0eTEiMCAGA1UEChMZ
UG9ydGltYSBzLmMuci5sLiBjLnYuYi5hLjEaMBgGA1UEAxMRUG9ydGlTaWduIFJv
b3QgQ0EwHhcNMTcwNjE2MDcwMDAwWhcNMjcwNjE2MDcwMDAwWjBrMQswCQYDVQQG
EwJCRTEiMCAGA1UEChMZUG9ydGltYSBzLmMuci5sLiBjLnYuYi5hLjE4MDYGA1UE
AxMvUG9ydGlTaWduIFVzZXJzIENBMTAgZm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0
ZXMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC/vZqvr6Iw2cbgBPDd
Y+4efCPQZUwtV/feKWGad+WidY462J1cXE5nuxC7Q1ubuXb4fwiXN6ZP/e9gDI+V
ORZavsM9Sw2MQLEaMMrqk0lFV/nZsRaYUhcIxvqpz8y4ayh+Mjfc1+BUqzKiwwF4
nvs+vZD+sDVolGRKy3cKyg+kAzV51mK+1bSMHFIiX8fMMP2ZxzF2uVM99zDM3MXB
r3LTHJgfxQjoz1Rk+8Mfx9SKXhwhtFTRkfCqqXlw/cufWhX4Ki/7D3TXfNmE0jrO
RTlY0JnZsJk+oXeig8hdtlQWbuNbLVZ8fUYK3uPnL81OJbMItkvyWcjpIllXYae1
hxIKZcDyaSxx27hNySgDiElWUMg9KuEmhkHcK4fw3JOBeUHBAw6yMgwY7jAPn8Fj
cvQdctwa3tr23a/ugC/Sj7XbZyclGjpcD7PkKVEB8uoowTc4RWnAU8R3vzlUxyLd
S+DEUs3a35odnnM7sYrsUhnxl+GLPzq7TgPx+bTk7AB+3MnfPKXhBXMrA3UPhEpX
ytHPhaa9Bd8rpv+0mzkVrI+6qCAwPyKeSAcw57oIakcg50E6ahk8P7RiX7LDNFWL
4FKNRin90rpIWLu6st2VHpQASiRi0adJoCvi294i+EpXlt1WmEsjhX4jxXwFhK/i
TW4/3QKJUVuptAzgcF/3drLUJwIDAQABo4GTMIGQMA8GA1UdEwEB/wQFMAMBAf8w
EQYDVR0OBAoECEmkzDZu1hHXMBEGA1UdIAQKMAgwBgYEVR0gADATBgNVHSMEDDAK
gAhP4r4ycEeyszALBgNVHQ8EBAMCAQYwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDov
L2NybC5wb3J0aXNpZ24uYmUvY3JsL3Jvb3QuY3JsMA0GCSqGSIb3DQEBDQUAA4IC
AQBwqiOz0S+eJ9Mzt3lF/IpObvgD33K09oeHoQUolfm2MOTpx+6f0kJPtnK23VmL
odPxbMnr9WZl8AghH44M0tJLHooFmm5E2nqK195iVS+/nPCJ9bXzMmigaQqIcLy4
3aWCqVvY8CLSChDRiTBn5QOP4POVjgD8mrKVgIgJPI7cTLLD2ktA3aDNeHoaYsVC
U9B5jd1GVJG43QbiqToQ8kWxVtpSmz2O7MEP6f2wuTjsgCkPGlc488nohQO07C7p
UVfYxxsiOVYBEFF+qgB66kiMf3hyzmnW3SHfPTwLhMBCdOqzH16GzS1x3xxzFSw4
+VR4FKQtYMDkyuANLcCEyz2OGegvuIQn5iJYLFv/iEKVSVcty87t3bD+srTVh4O1
BOeKeEGu8wQe33OXAW8v8kkfy7V9XFGXd+SzLPx9SvmO7L6/s8BEM7QzxbkSgOgx
14OVCDF/wEnQCFMzuipDtVYx1Ys1zAS2EkOJLZshNEetZCB3BJzua2e41jf/drjh
eaudwehx+ld6FRzCN3f3vyVBuNbwUU3gIjnNNtWXMkFhcWUWMvhLi5mNldxDycAM
UB61ZeKQ0O6RiybRqCPA5X10R0FX8jBMc8Zq+Q5lcHkISz00zXH00XtZIj9Ld6g3
QPFFXSZuPGdDfRDuI4SrTpaY55DvGHgv/sRjxJudeyrO6Q==
-----END CERTIFICATE-----
```

PortiSign Users CA11

Type	CA/QC
Status	granted
Status starting time	2017-11-30T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	10019
Signature algorithm	SHA512withRSA
Issuer	CN=PortiSign Root CA, O=Portima s.c.r.l. c.v.b.a., OU=Security, STREET=Terhulpsesteenweg 150 Chaussée de la Hulpe, ST=Brussels, L=B-1170 Brussels, C=BE, EMAILADDRESS=security@portima.com, OID.2.5.4.20=0032 2 6614411
Valid from	Fri Jun 16 07:00:00 UTC 2017
Valid to	Wed Jun 16 07:00:00 UTC 2027
Subject	CN=PortiSign Users CA11 for Qualified Certificates, O=Portima s.c.r.l. c.v.b.a., C=BE
Public key	Sun RSA public key, 4096 bits modulus: 849634259409079725533274052509037539102614120902461338260113147435263251475770989207559810718699257932792983730766606293270025049761465100568418825473084562192693028965685595236345251387469981087738209828176080359959583894483657440571364507398666029142222887964445202177453470474667742391804194881594263766124324783295395182265925085784245055822607410675601677470070056396999987258494074069518897150912978061463034784490877348514329138250487204294562708026913838203450630481360161560165597090343236034176004095114531455561227344091147666956810822609697202463449670498214146450493791069598478645128200728335785222832968136812790859774787811720774939883089610788191855578655014935170809225396094091875081854822708916333768406362775536327484401830050821562493983458620132979674927405291792159728579175563686151980574201671017390764384702456631403833204971656466088439203244281952196356091495514481779627765115140709972510276820807882249814189340670178677313624264480632034117924516418771156711815870489262274445550103040911421326280336828884236894344471510438644931121773180266156106767329363613006961641856271861881724634655675630111995800486827579105998743437389823508734797301557373674608772681751178764118064633067654636539287413393 public exponent: 65537
Subject key identifier	460abbf7bde34e95
CRL distribution points	http://crl.portisign.be/crl/root.crl
Authority key identifier	4fe2be327047b2b3
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	2ed230c5fc0d5936d4926766e798fe0efd024c99
SHA256 Thumbprint	4bd119b7adcc710e1db224b1178ca2ab809a5131ce86bc10832a2f9e77d31ea9

Extension (critical: true)

Additional service information

ForeSignatures

Extension (critical: true)

Qualifications

Qualifier: QCNoQSCD

Criterial List Description

Assert: atLeastOne

Policy OID: 1.3.6.1.4.4.10438.3.2.4.10.1

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=PortiSign Users CA11 for Qualified Certificates, O=Portima s.c.r.l. c.v.b.a., C=BE
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
849634259409079725533274052509037539102614120902461338260113147435263251475770989207559810718699257932792983730766606293270025049761465100568418825473084562192693028965685595236345251387469981087738209828176080359959583894483657440571364507398666029142222887964445202177453470474667742391804194881594263766124324783295395182265925085784245055822607410675601677470070056396999987258494074069518897150912978061463034784490877348514329138250487204294562708026913838203450630481360161560165597090343236034176004095114531455612273440911476669568108226096972024634496704982141464504937910695984786451282007283357852228329681368127908597747878117207749398830896107881918555786550149351708092253960940918750818548227089163337684063627755363274844018300508215624939834586201329796749274052917921597285791755636861519805742016710173907643847024566314038332049716564660884392032442819521963560914955144817796277651151407099725102768208078822498141893406701786773136242644806320341179245164187711567118158704892622744455501030409114212326280336828884236894344471510438644931121773180266156106767329363613006961641856271861881724634655675630111995800486827579105998743437389823508734797301557373674608772681751178764118064633067654636539287413393
 public exponent: 65537
 Validity: [From: Fri Jun 16 07:00:00 UTC 2017,
              To: Wed Jun 16 07:00:00 UTC 2027]
 Issuer: CN=PortiSign Root CA, O=Portima s.c.r.l. c.v.b.a., OU=Security, STREET=Terhulpsesteenweg 150 Chaussée de la Hulpe, ST=Brussels, L=B-1170 Brussels, C=BE,
EMAILADDRESS=security@portima.com, OID.2.5.4.20=0032 2 6614411
 SerialNumber: [    2723]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4F E2 BE 32 70 47 B2 B3                            O..2pG..
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.portisign.be/crl/root.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 46 0A BB F7 BD E3 4E 95                            F.....N.
]
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: 4E 3D 99 D8 2D 8E D9 F0   FF C9 6A BC 8A 1E 6A A0  N=..-.....j...j.
0010: DA C9 13 D5 B7 4E F4 65   57 EC A6 F6 16 CE 65 71  .....N.eW.....eq
0020: 49 30 DB BC F7 82 83 F1   6C CD 6B AD 42 A0 3D D3  I0......l.k.B.=.
0030: 19 8A 28 65 A2 64 FE 32   8D 01 DC 4A 4E 43 28 EA  ..(e.d.2...JNC(.
0040: D1 DB B2 40 A6 B2 C6 DD   99 B5 7F 37 EC 66 0E EB  ...@.......7.f..
0050: 04 6F 9C BD EE 6A 7E 79   31 BF 83 86 3F 97 38 EF  .o...j.y1...?.8.
0060: 12 81 23 63 D0 2D 6A B1   E5 4D 9C 65 70 D0 8B 23  ..#c.-j..M.ep..#
0070: B7 6C BF 50 73 46 A3 F1   1F 82 F2 18 4E 73 3B 9F  .l.PsF......Ns;.
0080: 77 86 E9 19 6F F4 E2 FB   D1 40 BB 71 2D 6A D7 9B  w...o....@.q-j..
0090: 7B 05 E9 6E 2A 3F 60 93   A9 30 56 7C CB 95 8C 1F  ...n*?`..0V.....
00A0: 18 0E 00 F3 61 B3 79 F1   DF CF 2A C4 AF 24 2B C8  ....a.y...*..$+.
00B0: A2 17 2C BB 38 61 D6 6A   51 D5 DD 58 8F B6 A1 65  ..,.8a.jQ..X...e
00C0: FD 73 51 88 C3 D4 9B 1A   C0 EC AF DA 84 62 23 B2  .sQ..........b#.
00D0: 33 1B 23 B6 14 38 EE DE   F1 CF 93 D2 8F DB 0F B6  3.#..8..........
00E0: FD 66 8B 72 7F EF BE 1F   6A 89 1F A4 CA E4 5D FC  .f.r....j.....].
00F0: 70 25 1E C2 98 F6 8D DC   99 18 D8 B7 39 A1 E1 6E  p%..........9..n
0100: 3C 97 62 19 EC 35 A1 2F   44 07 11 CC BC D2 44 AC  <.b..5./D.....D.
0110: B6 68 91 41 5B 19 45 CA   EC 92 EB 13 96 29 55 3C  .h.A[.E......)U<
0120: 2D 02 E9 D2 F1 3D CD D5   7F AF 5A 06 F7 41 EE D7  -.....=....Z..A..
0130: B9 33 BF 38 04 A3 7A 19   0B ED 4D B5 C6 55 19 60  .3.8..z...M..U.`
0140: 16 68 43 89 8E 3A E0 D8   FB 96 E3 D1 B8 22 30 1A  .hC..:........"0.
0150: FF D9 CE 20 9A ED 6A 65   DA 86 9D 6C 74 D7 16 2A  ... ..je...lt..*
```

```
0160: E4 EC 52 2E 71 C1 C0 27   7B 92 2C 1C 0E 1C BA 68  ..R.q..'..,....h
0170: 67 D1 8B AF 16 C3 E1 28   8F 48 D8 FA 1E A4 23 D0  g......(.H....#.
0180: 81 92 0D F1 F0 8B D9 20   C6 25 B8 19 A2 9D 59 60  ....... .%....Y`
0190: D0 EF A2 BB 2C B4 A1 F7   D0 0A D0 0D 2D A9 A7 A0  ....,.......-...
01A0: 9E A2 1C 41 1F 9D 48 7D   0F 43 A4 FA EA DD 41 32  ...A..H..C....A2
01B0: C4 C1 30 09 C3 F5 70 9E   FA 43 F5 C6 A0 13 97 3C  ..0...p..C.....<
01C0: 08 45 23 4C 68 58 38 5E   D1 E6 3D CA 8E 24 0F 3F  .E#LhX8^..=..$.?
01D0: 4C 35 B7 98 2A 79 34 32   72 D3 04 8D F5 2C BB AD  L5..*y42r....,..
01E0: 01 B8 C1 AD FE 07 19 E2   A0 30 D9 E9 5E D8 D9 83  .........0..^...
01F0: C7 5B 6E DD 8F 54 49 BE   9E 49 1A B8 DC 9C E2 76  .[n..TI..I.....v

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGfjCCBGagAwIBAgICJyMwDQYJKoZIhvcNAQENBQAwggEBMRcwFQYDVQQUEw4w
MDMyIDIgNjYxNDQxMTEjMCEGCSqGSIb3DQEJARYUc2VjdXJpdHlAcG9ydGltYS5j
b20xCzAJBgNVBAYTAkJFMRgwFgYDVQQHEw9CLTExNzAgQnJ1c3NlbHMxETAPBgNV
BAgTCEJydXNzZWxzMTQwMgYDVQQJDCtUZXJodWxwc2VzdGVlbndlZyAxNTAgQ2hh
dXNzw6llIGRlIGxhIEh1bHBlMREwDwYDVQQLEwhTZWN1cml0eTEiMCAGA1UEChMZ
UG9ydGltYSBzLmMuci5sLiBjLnYuYi5hLjEaMBgGA1UEAxMRUG9ydGlTaWduIFJv
b3QgQ0EwHhcNMTcwNjE2MDcwMDAwWhcNMjcwNjE2MDcwMDAwWjBrMQswCQYDVQQG
EwJCRTEiMCAGA1UEChMZUG9ydGltYSBzLmMuci5sLiBjLnYuYi5hLjE4MDYGA1UE
AxMvUG9ydGlTaWduIFVzZXJzIENBMTEgZm9yIFF1YWxpZmllZCBDZXJ0aWZpY2F0
ZXMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDQQwk4LiTPrp2kCIU/
Cbiikj47XWm0pyjXH4gthbFPESrcitPegf/RtQKLX7WbRvaAeP56aYHeVw1t/12V
cPJYtuqrgJe1ZHCVLLmS8JF1NHidx2hLVou0xhlSQvimx0uSq0LaZW9iDCU7D2ag
KJ4B/lPeCclpXrWDEP00xbYEsZa+ntnd+D0Vi5I8/oCPFiA6Z3FRgYboQ7/FQXkM
6vJw/MkTQqMr4YOs+XLPdUjBblyEcTGoJ4jKlpPYKSMqdbC6NBhMfwWmfjovmWKh
tw8zp4DoMhVPZVUco0AxRNJTdoz4BgOif3IiO7pRtKxacF8DUtPIjDfnvJfS9ciB
TOBVN/qmME7MgiV7OaPDQOVCCMHVvqVGr+RuM8+p3lK5+c3rynHIyc2jhHXbr4Zg
rC5pKnu0Tk3WkPY6E7X4g8GHxQrwpiCp8ZQlqyUUXlhFsxlhvGnyac+YCNTLu1Om
FdGZGfOQM+8SmlB66KObw79kSVhQOf9tbEkoAnSErERo9duHA3KABUUDza57wgqi
6FZZ6pD/aVeAtsBGnjibn12VI1EG/IRm7Jyj7OQKcC5ns4MwvO/z9+N0Wq3MECkh
/+sSzUevqi6cLhK41R/4hkPpAUbJxEogvD9VZbYgxH40kgOpQvzer7fIJ5/5DaVb
p3TvzBpKqETBDQtN7jG1RgOikQIDAQABo4GTMIGQMA8GA1UdEwEB/wQFMAMBAf8w
EQYDVR0OBAoECEYKu/e9406VMBEGA1UdIAQKMAgwBgYEVR0gADATBgNVHSMEDDAK
gAhP4r4ycEeyszALBgNVHQ8EBAMCAQYwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDov
L2NybC5wb3J0aXNpZ24uYmUvY3JsL3Jvb3QuY3JsMA0GCSqGSIb3DQEBDQUAA4IC
AQBOPZnYLY7Z8P/JaryKHmqg2skT1bdO9GVX7Kb2Fs5lcUkw27z3goPxbM1rrUKg
PdMZiihlomT+Mo0B3EpOQyjq0duyQKayxt2ZtX837GYO6wRvnL3uan55Mb+Dhj+X
OO8SgSNj0C1qseVNnGVw0Isjt2y/UHNGo/EfgvIYTnM7n3eG6Rlv9OL70UC7cS1q
15t7BeluKj9gk6kwVnzLlYwfGA4A82GzefHfzyrEryQryKIXLLs4YdZqUdXdWI+2
oWX9c1GIw9SbGsDsr9qEYiOyMxsjthQ47t7xz5PSj9sPtv1mi3J/774faokfpMrk
XfxwJR7CmPaN3JkY2Lc5oeFuPJdiGew1oS9EBxHMvNJErLZokUFbGUXK7JLrE5Yp
VTwtAunS8T3N1X+vWgb3Qe7XuTO/OASjehkL7U21xlUZYBZoQ4mOOuDY+5bj0bgi
MBr/2c4gmulqZdqGnWx01xYq5OxSLnHBwCd7kiwcDhy6aGfRi68Ww+Eoj0jY+h6k
I9CBkg3x8IvZIMYluBminVlg0O+iuyy0offQCtANLamnoJ6iHEEfnUh9D0Ok+urd
QTLEwTAJw/VwnvpD9cagE5c8CEUjTGhYOF7R5j3KjiQPP0w1t5gqeTQyctMEjfUs
u60BuMGt/gcZ4qAw2ele2NmDx1tu3Y9USb6eSRq43Jzidg==
-----END CERTIFICATE-----
```

Connect Solutions

Service provider trade name	VATBE-0843871294
Information URI	https://www.aangetekende.email/ae/logon.aspx
Service provider street address	Zandstraat 187
Service provider postal code	3550
Service provider locality	Heusden-Zolder
Service provider country	BE

Aangetekende.email

Type	EDS/Q
Status	granted
Status starting time	2018-02-08T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	167182972227906586217881844147 30
Signature algorithm	SHA256withRSA
Issuer	CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
Valid from	Tue Jun 06 09:40:25 UTC 2017
Valid to	Thu Jun 06 09:40:25 UTC 2019
Subject	SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions, L=Heusden-Zolder, C=BE
Public key	Sun RSA public key, 2048 bits modulus: 22786999722609582425701063646852183642223123604098378972866899584206259405863671525808018022668465651753042776036196630535005264224575736208594601930249570413531293193306785175367745479855052777394742532389876463178777151442775416063970660384793828153918812314909295417801991364937382493148487476857088326560843966433239809355806833624420929177714898791541340007096075624291567915693748188284974659841271912727321559814873806248854930647488327256254693922822006502238251646938345410580498062718231663773703164520451544644735620778095939548811627269448261992539906191044487222714578168514490549523545295887546456004858613 1 public exponent: 101
Subject key identifier	d54269260da49bf911110e9ec5bd9dbce611b9c6
CRL distribution points	http://crl.e-szigno.hu/qoca2016.crl
Authority key identifier	b1188fb2b938d29e67377b7815593baffa0017b2
Key usage	nonRepudiation
Basic constraints	CA=false
SHA1 Thumbprint	bc705e20694b2bac449a70ee2619ebda676f1083
SHA256 Thumbprint	2b297c7856a00d7b80048ceefedb41634e5da84b5923c42107eb0ec1357ec743

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions,
L=Heusden-Zolder, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
22786999722609582425701063646852183642223123604098378972866899584206259405863671525808018022668465651753042776036196630535005264224575736208594601930249570413531293193306785175367745479855052777394742532389876463178777151442775416063970660384793828153918812314909295417801991364937382493148487476857088326560843966433239809355806833624420929177714898791541340007096075624291565937481882849746598412719127273215598148738062488549306474883272562546939228220065022382516469383454105804980627182316637737031645204515446447356207780959395488116272694482619925399061910444872227145781685144905495235452958875464560048586131
 public exponent: 101
 Validity: [From: Tue Jun 06 09:40:25 UTC 2017,
             To: Thu Jun 06 09:40:25 UTC 2019]
 Issuer: CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
 SerialNumber: [    d303bb56 6c667eae 2af4688a 0a]

Certificate Extensions: 8
[1]: ObjectId: 1.3.6.1.5.5.7.1.3 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 81 A5 30 81 A2 30 08   06 06 04 00 8E 46 01 01  ...0..0......F..
0010: 30 15 06 06 04 00 8E 46   01 02 30 0B 13 03 48 55  0......F..0...HU
0020: 46 02 01 01 02 01 06 30   0B 06 06 04 00 8E 46 01  F......0......F.
0030: 03 02 01 0A 30 08 06 06   04 00 8E 46 01 04 30 53  ....0......F..0S
0040: 06 06 04 00 8E 46 01 05   30 49 30 24 16 1E 68 74  .....F..0I0$..ht
0050: 74 70 73 3A 2F 2F 63 70   2E 65 2D 73 7A 69 67 6E  tps://cp.e-szign
0060: 6F 2E 68 75 2F 71 63 70   73 5F 65 6E 13 02 45 4E  o.hu/qcps_en..EN
0070: 30 21 16 1B 68 74 74 70   73 3A 2F 2F 63 70 2E 65  0!..https://cp.e
0080: 2D 73 7A 69 67 6E 6F 2E   68 75 2F 71 63 70 73 13  -szigno.hu/qcps.
0090: 02 48 55 30 13 06 06 04   00 8E 46 01 06 30 09 06  .HU0......F..0..
00A0: 07 04 00 8E 46 01 06 02                            ....F...
```

```
[2]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://qoca2016-ocsp1.e-szigno.hu,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.e-szigno.hu/qoca2016.crt]
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B1 18 8F B2 B9 38 D2 9E   67 37 7B 78 15 59 3B AF  .....8..g7.x.Y;.
0010: FA 00 17 B2                                        ....
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.e-szigno.hu/qoca2016.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.21528.2.1.1.81.2.2]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1A 68 74 74 70 3A 2F   2F 63 70 2E 65 2D 73 7A  ..http://cp.e-sz
0010: 69 67 6E 6F 2E 68 75 2F   71 63 70 73              igno.hu/qcps

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 01 04 1A 82 01 00   51 75 61 6C 69 66 69 65  0.......Qualifie
0010: 64 20 63 65 72 74 69 66   69 63 61 74 65 20 28 42  d certificate (B
0020: 72 6F 6E 7A 65 29 2C 20   74 68 65 20 70 72 69 76  ronze), the priv
0030: 61 74 65 20 6B 65 79 20   72 65 73 69 64 65 73 20  ate key resides
0040: 69 6E 20 61 20 71 75 61   6C 69 66 69 65 64 20 73  in a qualified s
0050: 69 67 6E 61 74 75 72 65   20 63 72 65 61 74 69 6F  ignature creatio
0060: 6E 20 64 65 76 69 63 65   20 28 51 53 43 44 29 2E  n device (QSCD).
0070: 20 52 65 74 65 6E 74 69   6F 6E 20 70 65 72 69 6F   Retention perio
0080: 64 20 6F 66 20 6D 61 74   65 72 69 61 6C 20 69 6E  d of material in
0090: 66 6F 72 6D 61 74 69 6F   6E 3A 20 31 30 20 79 65  formation: 10 ye
00A0: 61 72 73 2E 20 4C 69 6D   69 74 20 6F 6E 20 74 68  ars. Limit on th
00B0: 65 20 76 61 6C 75 65 20   6F 66 20 74 72 61 6E 73  e value of trans
00C0: 61 63 74 69 6F 6E 73 3A   20 48 55 46 20 31 4D 2E  actions: HUF 1M.
00D0: 20 54 68 65 20 73 75 62   6A 65 63 74 20 6F 66 20   The subject of
00E0: 74 68 65 20 63 65 72 74   69 66 69 63 61 74 65 20  the certificate
00F0: 69 73 20 6E 6F 74 20 61   20 6E 61 74 75 72 61 6C  is not a natural
0100: 20 70 65 72 73 6F 6E 2E                            person.

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 02 0A 1E 82 02 06   00 4D 00 69 00 6E 01 51  0........M.i.n.Q
0010: 00 73 00 ED 00 74 00 65   00 74 00 74 00 20 00 74  .s...t.e.t.t. .t
0020: 00 61 00 6E 00 FA 00 73   00 ED 00 74 00 76 00 E1  .a.n...s...t.v..
0030: 00 6E 00 79 00 20 00 28   00 42 00 72 00 6F 00 6E  .n.y. .(.B.r.o.n
0040: 00 7A 00 29 00 2C 00 20   00 61 00 20 00 6D 00 61  .z.).,. .a. .m.a
0050: 00 67 00 E1 00 6E 00 6B   00 75 00 6C 00 63 00 73  .g...n.k.u.l.c.s
0060: 00 6F 00 74 00 20 00 6D   00 69 00 6E 01 51 00 73  .o.t. .m.i.n.Q.s
0070: 00 ED 00 74 00 65 00 74   00 74 00 20 00 61 00 6C  ...t.e.t.t. .a.l
0080: 00 E1 00 ED 00 72 00 E1   00 73 00 2D 00 6C 00 E9  .....r...s.-.l..
0090: 00 74 00 72 00 65 00 68   00 6F 00 7A 00 F3 00 20  .t.r.e.h.o.z...
00A0: 00 65 00 73 00 7A 00 6B   00 F6 00 7A 00 20 00 28  .e.s.z.k...z. .(
00B0: 00 4D 00 41 00 4C 00 45   00 29 00 20 00 76 00 E9  .M.A.L.E.). .v..
00C0: 00 64 00 69 00 2E 00 20   00 41 00 20 00 72 00 65  .d.i... .A. .r.e
00D0: 00 67 00 69 00 73 00 7A   00 74 00 72 00 E1 00 63  .g.i.s.z.t.r...c
00E0: 00 69 00 F3 00 73 00 20   00 61 00 64 00 61 00 74  .i...s. .a.d.a.t
00F0: 00 6F 00 6B 00 61 00 74   00 20 00 61 00 20 00 73  .o.k.a.t. .a. .s
0100: 00 7A 00 6F 00 6C 00 67   00 E1 00 6C 00 74 00 61  .z.o.l.g...l.t.a
0110: 00 74 00 F3 00 20 00 61   00 20 00 74 00 61 00 6E  .t... .a. .t.a.n
0120: 00 FA 00 73 00 ED 00 74   00 76 00 E1 00 6E 00 79  ...s...t.v...n.y
0130: 00 20 00 6C 00 65 00 6A   00 E1 00 72 00 74 00 E1  . .l.e.j...r.t..
0140: 00 74 00 F3 00 6C 00 20   00 73 00 7A 00 E1 00 6D  .t...l. .s.z...m
0150: 00 ED 00 74 00 6F 00 74   00 74 00 20 00 31 00 30  ...t.o.t.t. .1.0
0160: 00 20 00 E9 00 76 00 69   00 67 00 20 01 51 00 72  . ...v.i.g. .Q.r
0170: 00 7A 00 69 00 20 00 6D   00 65 00 67 00 2E 00 20  .z.i. .m.e.g...
0180: 00 54 00 72 00 61 00 6E   00 7A 00 61 00 6B 00 63  .T.r.a.n.z.a.k.c
0190: 00 69 00 F3 00 73 00 20   00 6C 00 69 00 6D 00 69  .i...s. .l.i.m.i
01A0: 00 74 00 3A 00 20 00 31   00 4D 00 20 00 46 00 74  .t.:. .1.M. .F.t
01B0: 00 2E 00 20 00 41 00 20   00 74 00 61 00 6E 00 FA  ... .A. .t.a.n..
01C0: 00 73 00 ED 00 74 00 76   00 E1 00 6E 00 79 00 20  .s...t.v...n.y.
01D0: 00 61 00 6C 00 61 00 6E   00 79 00 61 00 20 00 4E  .a.l.a.n.y.a. .N
01E0: 00 45 00 4D 00 20 00 74   00 65 00 72 00 6D 00 E9  .E.M. .t.e.r.m..
01F0: 00 73 00 7A 00 65 00 74   00 65 00 73 00 20 00 73  .s.z.e.t.e.s. .s
0200: 00 7A 00 65 00 6D 00 E9   00 6C 00 79 00 2E        .z.e.m...l.y..

]]  ]
 [CertificatePolicyId: [0.4.0.194112.1.3]
[]  ]
 [CertificatePolicyId: [0.4.0.2042.1.2]
[]  ]
]
```

```
[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Non_repudiation
]

[7]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@connect-solutions.be
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
]

[8]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D5 42 69 26 0D A4 9B F9   11 11 0E 9E C5 BD 9D BC  .Bi&............
0010: E6 11 B9 C6                                        ....
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 83 5A 98 06 2C B2 B1 29   98 85 42 D6 98 03 ED F1  .Z..,..)..B.....
0010: 14 5C 79 CA 60 86 F0 D5   AD AA 08 CB 1A D3 32 28  .\y.`.........2(
0020: 0B 90 D1 F9 20 C0 E8 C5   54 0C EF 89 75 40 CD C0  .... ...T...u@..
0030: 9B 74 BF E7 93 00 A4 EA   02 CA D2 7C 13 4E D2 44  .t...........N.D
0040: 2A 50 E7 43 8C 84 F4 95   E5 2E 50 76 94 E0 49 15  *P.C......Pv..I.
0050: 31 7F 5D FB D2 0C 4E 2C   5C 71 A8 E3 99 87 BE 20  1.]...N,\q..... 
0060: 36 2C DF AE 0E 52 34 57   99 77 31 4B D6 F7 01 B7  6,...R4W.w1K....
0070: 86 DA 10 E9 11 18 A5 9B   AA 8D A2 9E A7 BC 20 49  .............. I
0080: 1D 3E D9 D8 1E 92 A5 05   EC 63 62 51 C7 33 60 FE  .>.......cbQ.3`.
0090: 02 A2 08 C7 59 B8 E1 EB   36 38 C7 99 F4 CB A8 0C  ....Y...68......
00A0: 7A 2C 93 6C C4 D8 16 06   81 25 3D E8 C8 58 F8 F4  z,.l.....%=..X..
00B0: F7 9C 81 E6 B9 8C 92 5E   21 42 C3 33 FA 16 A0 1D  .......^!B.3....
00C0: 09 E4 6A 96 5C 4A FC AB   50 AC 85 3E B3 B3 03 C0  ..j.\J..P..>....
00D0: 1B C6 50 96 0D 3C EA 0E   62 91 7D 64 11 D9 64 A4  ..P..<..b..d..d.
00E0: 04 97 DF F2 37 2E A0 DC   14 D3 36 E2 85 86 B8 81  ....7.....6.....
00F0: 50 C5 41 62 F7 F7 49 E1   E5 22 90 91 02 AF 74 D0  P.Ab..I.."....t.
0100: D5 00 A4 7A 74 4D FE 56   73 DC 10 EA E1 7B 6F E8  ...ztM.Vs.....o.
0110: 28 6C 8E 52 77 21 CE E0   64 C8 DF BF 23 E3 AF 95  (l.Rw!..d...#...
0120: AD 4A A6 8E C5 B0 68 E7   2F 39 1C E4 D2 46 85 32  .J....h./9...F.2
0130: 5B E3 B5 50 2D 4D E1 E1   E3 52 82 FA EE 87 43 8F  [..P-M...R....C.
0140: 92 64 B7 F6 8E 8B DB C6   36 EE DE DD ED 49 DB A6  .d......6....I..
0150: AF 16 1C 28 6D CE 2C 89   CB 45 AA 8F A6 B1 32 7D  ...(m.,..E....2.
0160: FD 81 E2 CE A9 CB 78 56   2A E0 7A DC E8 41 6A 89  ......xV*.z..Aj.
0170: 82 D2 0B 15 D1 6F CD E1   FF 07 F3 F6 A9 3E 23 60  .....o.......>#`
0180: F4 D3 E0 AA 8B 01 0F 79   A8 BB 47 10 C0 28 EB FE  .......y..G..(..
0190: CF 1A 1C 23 80 B5 09 37   A7 C4 4F C9 36 8B C7 3E  ...#...7..O.6..>
01A0: 63 4C DC 3D 9D 77 AA BD   5F B4 43 0B 92 D9 61 BA  cL.=.w.._.C...a.
01B0: 5E A3 02 67 C3 48 BA D2   B2 52 A3 D3 EE E9 B1 DC  ^..g.H...R......
01C0: DE 20 6B FE 3C 78 A6 C1   91 D4 92 7E 2F 8D 75 B5  . k.<x....../.u.
01D0: 69 C4 1C 87 05 AF E3 42   CF 68 ED 6E 2F 84 67 AB  i......B.h.n/.g.
01E0: EB 4D 83 24 FF F9 42 78   41 EE BE 28 B6 19 70 19  .M.$..BxA..(..p.
01F0: FB 26 8D 3A A5 28 C9 FB   8A 15 C0 F3 E8 50 2E EF  .&.:.(.......P..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIKZDCCCEygAwIBAgIOANMDu1ZsZn6uKvRoigowDQYJKoZIhvcNAQELBQAwgYgx
CzAJBgNVBAYTAkhVMREwDwYDVQQHDAhCdWRhcGVzdDEWMBQGA1UECgwNTWljcm9z
ZWMgTHRkLjEcMBoGA1UEYQwTVkFUSFUtMjM1ODQ0OTctMi00MTEwMC4GA1UEAwwn
UXVhbGlmaWVkIGUtU3ppZ25vIE9yZ2FuaXphdGlvbiBDQSAyMDE2MB4XDTE3MDYw
NjA5NDAyNVoXDTE5MDYwNjA5NDAyNVowgcoxCzAJBgNVBAYTAkJFMRcwFQYDVQQH
DA5IZXVzZGVuLVpvbGRlcjEaMBgGA1UECgwRQ29ubmVjdCBTb2x1dGlvbnMxGTAX
BgNVBGEMEFZBVEJFLTA4NDM4NzEyOTQxGjAYBgNVBAMMEUNvbm5lY3QgU29sdXRp
b25zMSgwJgYJKoZIhvcNAQkBFhlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJlMSUw
IwYDVQQFExwxLjMuNi4xLjQuMS4yMTUyOC4yLjMuMi4zMTcxMIIBIDANBgkqhkiG
9w0BAQEFAAOCAQ0AMIIBCAKCAQEAtIH/tYGL7zmhmealJw+px2Izm3aQQZUSmXWl
+NmHC5dyQbPtFS03NV2GDpJ5NZpuMbQtEdBX3memt4WEuzSaD4ygBdaC5tac5Kna
eRLI0LoALp3n4oPfNPvfhPgGmRZvYkn0zZtGNCGjPG120Nb2iUSdfgVVhGcvorDa
TmTijCO8T623RmWyZKARQa9ngVOdkViUxzOG/tPvAZhnlagJhHZiiLOyW53lkZJU
ezHqvUK+NF5yg9Ztf63pBDz2ngRHTuxrYJMXZ9Xc7QjhMvxKOe5Ex4gszalYLev1
xONRT1M+fB8jKSNORgA6RMzVORyj1kKZiLXrbXlbLqz+INu9kwIBZaOCBYgwggWE
MA4GA1UdDwEB/wQEAwIGQDCCA5QGA1UdIASCA4swggOHMIIDbgYOKwYBBAGBqBgC
AQFRAgIwggNaMCYGCCsGAQUFBwIBFhpodHRwOi8vY3AuZS1zemlnbm8uaHUvcWNw
czCCARIGCCsGAQUFBwICMIIBBBqCAQBRdWFsaWZpZWQgY2VydGlmaWNhdGUgKEJy
b256ZSksIHRoZSBwcml2YXRlIGtleSByZXNpZGVzIGluIGEgcXVhbGlmaWVkIHNp
Z25hdHVyZSBjcmVhdGlvbiBkZXZpY2UgKFFTQ0QpLiBSZXRlbnRpb24gcGVyaW9k
IG9mIG1hdGVyaWFsIGluZm9ybWF0aW9uOiAxMCB5ZWFycy4gTGltaXQgb24gdGhl
IHZhbHVlIG9mIHRyYW5zYWN0aW9uczogSFVGIDFNLiBUaGUgc3ViamVjdCBvZiB0
aGUgY2VydGlmaWNhdGUgaXMgbm90IGEgbmF0dXJhbCBwZXJzb24uMIICGAYIKwYB
BQUHAgIwggIKHoICBgBNAGkAbgFRAHMA7QB0AGUAdAB0ACAAdABhAG4A+gBzAO0A
dAB2AOEAbgB5ACAAKABCAHIAbwBuAHoAKQAsACAAYQAgAG0AYQBnAOEAbgBrAHUA
bABjAHMAbwB0ACAAbQBpAG4BUQBzAO0AdABlAHQAdAAgAGEAbADhAO0AcgDhAHMA
LQBsAOkAdAByAGUAaABvAHoA8wAgAGUAcwB6AGsA9gB6ACAAKABNAEEATABFACkA
IAB2AOkAZABpAC4AIABBACAAcgBlAGcAaQBzAHoAdAByAOEAYwBpAPMAcwAgAGEA
ZABhAHQAbwBrAGEAdAAgAGEAIABzAHoAbwBsAGcA4QBsAHQAYQB0APMAIABhACAA
dABhAG4A+gBzAO0AdAB2AOEAbgB5ACAAbABlAGoA4QByAHQA4QB0APMAbAAgAHMA
egDhAG0A7QB0AG8AdAB0ACAAMQAwACAA6QB2AGkAZwAgAVEAcgB6AGkAIABtAGUA
ZwAuACAAVAByAGEAbgB6AGEAawBjAGkA8wBzACAAbABpAG0AaQB0ADoAIAAxAE0A
IABGAHQALgAgAEEAIAB0AGEAbgD6AHMA7QB0AHYA4QBuAHkAIABhAGwAYQBuAHkA
YQAgAE4ARQBNACAAdABlAHIAbQDpAHMAegBlAHQAZQBzACAAcwB6AGUAbQDpAGwA
```

eQAuMAkGBwQAi+xAAQMwCAYGBACPegECMB0GA1UdDgQWBBTVQmkmDaSb+RERDp7F
vZ285hG5xjAfBgNVHSMEGDAWgBSxGI+yuTjSnmc3e3gVWTuv+gAXsjA/BgNVHREE
ODA2gRlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJloBkGCCsGAQUFBwgDoA0wCwYJ
KwYBBAGBqBgCMDQGA1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwuZS1zemlnbm8u
aHUvcW9jYTIwMTYuY3JsMG4GCCsGAQUFBwEBBGIwYDAtBggrBgEFBQcwAYYhaHR0
cDovL3FvY2EyMDE2LW9jc3AxLmUtc3ppZ25vLmh1MC8GCCsGAQUFBzAChiNodHRw
Oi8vd3d3LmUtc3ppZ25vLmh1L3FvY2EyMDE2LmNydDCBsgYIKwYBBQUHAQMEgaUw
gaIwCAYGBACORgEBMBUGBgQAjkYBAjALEwNIVUYCAQECAQYwCwYGBACORgEDAgEK
MAgGBgQAjkYBBDBTBgYEAI5GAQUwSTAkFh5odHRwczovL2NwLmUtc3ppZ25vLmh1
L3FjcHNfZW4TAkVOMCEWG2h0dHBzOi8vY3AuZS1zemlnbm8uaHUvcWNwcxMCSFUw
EwYGBACORgEGMAkGBwQAjkYBBgIwDQYJKoZIhvcNAQELBQADggIBAINamAYssrEp
mIVC1pgD7fEUXHnKYIbw1a2qCMsa0zIoC5DR+SDA6MVUDO+JdUDNwJt0v+eTAKTq
AsrSfBNO0kQqUOdDjIT0leUuUHaU4EkVMX9d+9IMTixccajjmYe+IDYs364OUjRX
mXcxS9b3AbeG2hDpERilm6qNop6nvCBJHT7Z2B6SpQXsY2JRxzNg/gKiCMdZuOHr
NjjHmfTLqAx6LJNsxNgWBoElPejIWPj095yB5rmMkl4hQsMz+hagHQnkapZcSvyr
UKyFPrOzA8AbxlCWDTzqDmKRfWQR2WSkBJff8jcuoNwU0zbihYa4gVDFQWL390nh
5SKQkQKvdNDVAKR6dE3+VnPcEOrhe2/oKGyOUnchzuBkyN+/I+Ovla1Kpo7FsGjn
Lzkc5NJGhTJb47VQLU3h4eNSgvruh0OPkmS39o6L28Y27t7d7Unbpq8WHChtziyJ
y0Wqj6axMn39geLOqct4VirgetzoQWqJgtILFdFvzeH/B/P2qT4jYPTT4KqLAQ95
qLtHEMAo6/7PGhwjgLUJN6fET8k2i8c+Y0zcPZ13qr1ftEMLktlhul6jAmfDSLrS
slKj0+7psdzeIGv+PHimwZHUkn4vjXW1acQchwWv40LPaO1uL4Rnq+tNgyT/+UJ4
Qe6+KLYZcBn7Jo06pSjJ+4oVwPPoUC7v
-----END CERTIFICATE-----

Aangetekende.email

Type	EDS/Q
Status	granted
Status starting time	2018-02-08T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	167185797760092878653607018365 54
Signature algorithm	SHA256withRSA
Issuer	CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
Valid from	Tue Jun 06 09:51:07 UTC 2017
Valid to	Thu Jun 06 09:51:07 UTC 2019
Subject	SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions, L=Heusden-Zolder, C=BE
Public key	Sun RSA public key, 2048 bits modulus: 21357749065365006902756428275314780447624043197914727096014355796040183720986486759720494772670902123072513544197750740762148710806657534540981355055815543638101442508000153322324035045672339876642752533920315501280008750951453581436177174747416470621567446406267117434677809980509033160026107293765007659083456515207538789868460357792992571664803607230069995979416860355830874854558853749009444456669821613000805329366786591777632040268264993165823385325197679216889778061454587863379743666599019114810100871957367134323512970007464420144073879137201840335830864920121703020528027918191798466752086376540978742542353 public exponent: 101
Subject key identifier	ab08b52fbf3728c56e89144d87bc1218ab8d71fc
CRL distribution points	http://crl.e-szigno.hu/qoca2016.crl
Authority key identifier	b1188fb2b938d29e67377b7815593baffa0017b2
Key usage	nonRepudiation
Basic constraints	CA=false
SHA1 Thumbprint	293dda07109176ea0f44643283570136070ef93e
SHA256 Thumbprint	dc65ff59b1c0b545fb89b87c58fc861bbab22d534a050ccbd76d846dd12c3cfc

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions,
L=Heusden-Zolder, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
21357749065365006902756428275314780447624043197914727096014355796040183720986486759720494772670902123072513544197750740762148710806657534540981355055815543638101442508000153
32232403504567233987664275253392031550128000875095145358143617717474741647062156744640626711743467780998050903316002610729376500765908345651520753878986846035779299257166480
36072300699959794168603558308748545588537490094444566698216130008053293667865917776320402682649931658233853251976792168897780614545878633797436665990191148101008719573671343
23512970007464420144073879137201840335830864920121703020528027918191798466752086376540978742542353
 public exponent: 101
 Validity: [From: Tue Jun 06 09:51:07 UTC 2017,
             To: Thu Jun 06 09:51:07 UTC 2019]
 Issuer: CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
 SerialNumber: [    d304a50f 65130be7 0ac249cd 0a]

Certificate Extensions: 8
[1]: ObjectId: 1.3.6.1.5.5.7.1.3 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 81 A5 30 81 A2 30 08   06 06 04 00 8E 46 01 01  ...0..0......F..
0010: 30 15 06 06 04 00 8E 46   01 02 30 0B 13 03 48 55  0......F..0...HU
0020: 46 02 01 01 02 01 06 30   0B 06 06 04 00 8E 46 01  F.......0......F.
0030: 03 02 01 0A 30 08 06 06   04 00 8E 46 01 04 30 53  ....0......F..0S
0040: 06 06 04 00 8E 46 01 05   30 49 30 24 16 1E 68 74  .....F..0I0$..ht
0050: 74 70 73 3A 2F 2F 63 70   2E 65 2D 73 7A 69 67 6E  tps://cp.e-szign
0060: 6F 2E 68 75 2F 71 63 70   73 5F 65 6E 13 02 45 4E  o.hu/qcps_en..EN
0070: 30 21 16 1B 68 74 74 70   73 3A 2F 2F 63 70 2E 65  0!..https://cp.e
0080: 2D 73 7A 69 67 6E 6F 2E   68 75 2F 71 63 70 73 13  -szigno.hu/qcps.
0090: 02 48 55 30 13 06 06 04   00 8E 46 01 06 30 09 06  .HU0......F..0..
00A0: 07 04 00 8E 46 01 06 02                            ....F...


[2]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://qoca2016-ocsp1.e-szigno.hu,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.e-szigno.hu/qoca2016.crt]
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B1 18 8F B2 B9 38 D2 9E   67 37 7B 78 15 59 3B AF  .....8..g7.x.Y;.
0010: FA 00 17 B2                                        ....
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.e-szigno.hu/qoca2016.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.21528.2.1.1.81.2.2]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1A 68 74 74 70 3A 2F   2F 63 70 2E 65 2D 73 7A  ..http://cp.e-sz
0010: 69 67 6E 6F 2E 68 75 2F   71 63 70 73              igno.hu/qcps

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 01 04 1A 82 01 00   51 75 61 6C 69 66 69 65  0.......Qualifie
0010: 64 20 63 65 72 74 69 66   69 63 61 74 65 20 28 42  d certificate (B
0020: 72 6F 6E 7A 65 29 2C 20   74 68 65 20 70 72 69 76  ronze), the priv
0030: 61 74 65 20 6B 65 79 20   72 65 73 69 64 65 73 20  ate key resides
0040: 69 6E 20 61 20 71 75 61   6C 69 66 69 65 64 20 73  in a qualified s
0050: 69 67 6E 61 74 75 72 65   20 63 72 65 61 74 69 6F  ignature creatio
0060: 6E 20 64 65 76 69 63 65   20 28 51 53 43 44 29 2E  n device (QSCD).
0070: 20 52 65 74 65 6E 74 69   6F 6E 20 70 65 72 69 6F   Retention perio
0080: 64 20 6F 66 20 6D 61 74   65 72 69 61 6C 20 69 6E  d of material in
0090: 66 6F 72 6D 61 74 69 6F   6E 3A 20 31 30 20 79 65  formation: 10 ye
00A0: 61 72 73 2E 20 4C 69 6D   69 74 20 6F 6E 20 74 68  ars. Limit on th
00B0: 65 20 76 61 6C 75 65 20   6F 66 20 74 72 61 6E 73  e value of trans
00C0: 61 63 74 69 6F 6E 73 3A   20 48 55 46 20 31 4D 2E  actions: HUF 1M.
00D0: 20 54 68 65 20 73 75 62   6A 65 63 74 20 6F 66 20   The subject of
00E0: 74 68 65 20 63 65 72 74   69 66 69 63 61 74 65 20  the certificate
00F0: 69 73 20 6E 6F 74 20 61   20 6E 61 74 75 72 61 6C  is not a natural
0100: 20 70 65 72 73 6F 6E 2E                            person.

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 02 0A 1E 82 02 06   00 4D 00 69 00 6E 01 51  0........M.i.n.Q
0010: 00 73 00 ED 00 74 00 65   00 74 00 74 00 20 00 74  .s...t.e.t.t. .t
0020: 00 61 00 6E 00 FA 00 73   00 ED 00 74 00 76 00 E1  .a.n...s...t.v..
```

```
0030: 00 6E 00 79 00 20 00 28   00 42 00 72 00 6F 00 6E  .n.y. .(.B.r.o.n
0040: 00 7A 00 29 00 2C 00 20   00 61 00 20 00 6D 00 61  .z.),. .a. .m.a
0050: 00 67 00 E1 00 6E 00 6B   00 75 00 6C 00 63 00 73  .g...n.k.u.l.c.s
0060: 00 6F 00 74 00 20 00 6D   00 69 00 6E 01 51 00 73  .o.t. .m.i.n.Q.s
0070: 00 ED 00 74 00 65 00 74   00 74 00 20 00 61 00 6C  ...t.e.t.t. .a.l
0080: 00 E1 00 ED 00 72 00 E1   00 73 00 2D 00 6C 00 E9  .....r...s.-.l..
0090: 00 74 00 72 00 65 00 68   00 6F 00 7A 00 F3 00 20  .t.r.e.h.o.z...
00A0: 00 65 00 73 00 7A 00 6B   00 F6 00 7A 00 20 00 28  .e.s.z.k...z. .(
00B0: 00 4D 00 41 00 4C 00 45   00 29 00 20 00 76 00 E9  .M.A.L.E.). .v..
00C0: 00 64 00 69 00 2E 00 20   00 41 00 20 00 72 00 65  .d.i... .A. .r.e
00D0: 00 67 00 69 00 73 00 7A   00 74 00 72 00 E1 00 63  .g.i.s.z.t.r...c
00E0: 00 69 00 F3 00 73 00 20   00 61 00 64 00 61 00 74  .i...s. .a.d.a.t
00F0: 00 6F 00 6B 00 61 00 74   00 20 00 61 00 20 00 73  .o.k.a.t. .a. .s
0100: 00 7A 00 6F 00 6C 00 67   00 E1 00 6C 00 74 00 61  .z.o.l.g...l.t.a
0110: 00 74 00 F3 00 20 00 61   00 20 00 74 00 61 00 6E  .t... .a. .t.a.n
0120: 00 FA 00 73 00 ED 00 74   00 76 00 E1 00 6E 00 79  ...s...t.v...n.y
0130: 00 20 00 6C 00 65 00 6A   00 E1 00 72 00 74 00 E1  . .l.e.j...r.t..
0140: 00 74 00 F3 00 6C 00 20   00 73 00 7A 00 E1 00 6D  .t...l. .s.z...m
0150: 00 ED 00 74 00 6F 00 74   00 74 00 20 00 31 00 30  ...t.o.t.t. .1.0
0160: 00 20 00 E9 00 76 00 69   00 67 00 20 01 51 00 72  . ...v.i.g. .Q.r
0170: 00 7A 00 69 00 20 00 6D   00 65 00 67 00 2E 00 20  .z.i. .m.e.g...
0180: 00 54 00 72 00 61 00 6E   00 7A 00 61 00 6B 00 63  .T.r.a.n.z.a.k.c
0190: 00 69 00 F3 00 73 00 20   00 6C 00 69 00 6D 00 69  .i...s. .l.i.m.i
01A0: 00 74 00 3A 00 20 00 31   00 4D 00 20 00 46 00 74  .t.:. .1.M. .F.t
01B0: 00 2E 00 20 00 41 00 20   00 74 00 61 00 6E 00 FA  ... .A. .t.a.n..
01C0: 00 73 00 ED 00 74 00 76   00 E1 00 6E 00 79 00 20  .s...t.v...n.y.
01D0: 00 61 00 6C 00 61 00 6E   00 79 00 61 00 20 00 4E  .a.l.a.n.y.a. .N
01E0: 00 45 00 4D 00 20 00 74   00 65 00 72 00 6D 00 E9  .E.M. .t.e.r.m..
01F0: 00 73 00 7A 00 65 00 74   00 65 00 73 00 20 00 73  .s.z.e.t.e.s. .s
0200: 00 7A 00 65 00 6D 00 E9   00 6C 00 79 00 2E        .z.e.m...l.y..

]]  ]
 [CertificatePolicyId: [0.4.0.194112.1.3]
[]  ]
 [CertificatePolicyId: [0.4.0.2042.1.2]
[]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Non_repudiation
]

[7]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@connect-solutions.be
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
]

[8]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: AB 08 B5 2F BF 37 28 C5   6E 89 14 4D 87 BC 12 18  .../.7(.n..M....
0010: AB 8D 71 FC                                        ..q.
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 26 C5 45 3F 68 EC 05 F9   FC D0 F9 35 F8 AA 71 1B  &.E?h......5..q.
0010: 63 60 11 CA 80 3F C1 33   59 D5 17 E0 5A 60 A8 7C  c`...?.3Y...Z`..
0020: EE 0B E7 47 A8 35 3F B2   CB 89 32 4C 4A CB EE 4F  ...G.5?...2LJ..O
0030: 14 96 6D 5E 2A 3D F1 7C   83 6E 78 86 11 47 AF B3  ..m^*=...nx..G..
0040: 6F 5A ED F5 58 DA 9B 76   DE 9A 89 1B B5 54 2D E9  oZ..X..v.....T-.
0050: 64 1E C7 B0 D4 0E DA 32   8F F3 94 66 F1 EB C4 F9  d......2...f....
0060: 53 4F DD 60 54 A8 29 46   9D 40 40 29 2F F7 23 0B  SO.`T.)F.@@)/.#.
0070: 9A 2F 78 49 CE 91 5D 83   BF 7B E2 CA F7 50 B5 65  ./xI..]......P.e
0080: 03 12 0C 74 40 1A E5 0B   DE DC AC BE E5 6D A8 EB  ...t@........m..
0090: 66 89 FC 14 32 DE DF 53   22 24 A2 8D E7 8F 14 96  f...2..S"$......
00A0: F7 D6 3B 12 CC 13 2C 0E   B7 EB 10 3C 9A 00 9D D0  ..;...,....<....
00B0: 1F 8B 1D 5E 85 17 D7 81   1A 36 04 08 18 25 10 B5  ...^.....6...%..
00C0: BE 8D C7 76 41 91 7A 84   E9 E9 E9 D0 48 C8 F6 3E  ...vA.z.....H..>
00D0: AE 2E 8C 00 CB 6B 23 E3   85 C9 75 7E EC D9 2D 70  .....k#...u...-p
00E0: C4 7D 5F DE 96 30 33 EE   7F E9 AD 64 54 6B 65 DB  ._..03....dTke.
00F0: E9 85 90 D9 6D 51 02 00   CB 60 1A 14 CF B4 63 DF  ....mQ...`....c.
0100: D9 58 21 E2 D6 F9 93 2C   89 F4 4F 2B D2 A7 AB DC  .X!....,..O+....
0110: 37 0E 78 11 53 A5 33 49   41 27 B5 A9 E8 45 F2 60  7.x.S.3IA'...E.`
0120: AC 84 E6 0C AB 07 80 99   00 92 25 9E 21 24 F7 4F  ..........%.!$.O
0130: 38 E6 F5 01 86 12 68 73   BD 58 E2 DC 18 59 44 EC  8.....hs.X...YD.
0140: 13 B4 65 5F 76 7B DB 49   1C 45 86 D4 57 F7 46 43  ..e_v..I.E..W.FC
0150: D5 A4 DE 64 DE F8 51 65   D3 D3 B1 73 71 A8 0B 79  ...d..Qe...sq..y
0160: 84 F9 04 1E 13 53 70 DB   1A 16 0F CF B0 A7 11 74  .....Sp........t
0170: 9A 1E A7 73 5C 34 02 5F   C9 1E C1 B3 05 17 9A 2A  ...s\4._.......*
0180: 2A 93 5D BC CA 6B F8 86   55 AB E5 C5 C3 7B B5 C4  *.]..k..U.......
0190: FE 19 5D DA 3F 3A 8D CE   AC 7B B5 D9 C6 59 20 66  ..].?:.......Y f
01A0: B6 FE F4 1E 2B D5 15 BE   93 0E EB 69 6C BB 7B 6D  ....+......il..m
01B0: FA 3D EC 44 75 19 22 46   3B 12 B5 7B 18 E7 A6 9D  .=.Du."F;.......
01C0: 48 30 64 78 A2 4D 50 AE   59 96 FA 9E 1E 4F 0D 02  H0dx.MP.Y....O..
01D0: BF A2 98 E5 19 83 3E A2   16 B9 D5 70 18 66 75 3F  ......>....p.fu?
01E0: 95 FD 1F 1E 8C E0 87 7C   AA C3 07 42 3E 95 91 80  ...........B>...
01F0: 8E 07 A6 52 51 C8 CA E5   16 A0 D2 CC A3 B4 1A F4  ...RQ...........

]
```

The certificate in PEM format:


```
-----BEGIN CERTIFICATE-----
MIIKZDCCCEygAwIBAgIOANMEpQ9lEwvnCsJJzQowDQYJKoZIhvcNAQELBQAwgYgx
CzAJBgNVBAYTAkhVMREwDwYDVQQHDAhCdWRhcGVzdDEWMBQGA1UECgwNTWljcm9z
ZWMgTHRkLjEcMBoGA1UEYQwTVkFUSFUtMjM1ODQ0OTctMi00MTEwMC4GA1UEAwwn
UXVhbGlmaWVkIGUtU3ppZ25vIE9yZ2FuaXphdGlvbiBDQSAyMDE2MB4XDTE3MDYw
NjA5NTEwN1oXDTE5MDYwNjA5NTEwN1owgcoxCzAJBgNVBAYTAkJFMRcwFQYDVQQH
DA5IZXVzZGVuLVpvbGRlcjEaMBgGA1UECgwRQ29ubmVjdCBTb2x1dGlvbnMxGTAX
BgNVBGEMEFZBVEJFLTA4NDM4NzEyOTQxGjAYBgNVBAMMEUNvbm5lY3QgU29sdXRp
b25zMSgwJgYJKoZIhvcNAQkBFhlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJlMSUw
IwYDVQQFExwxLjMuNi4xLjQuMS4yMTUyOC4yLjMuMi4zMTcxMIIBIDANBgkqhkiG
9w0BAQEFAAOCAQ0AMIIBCAKCAQEAqS+bNG78ONSeZ1tH594qKYrWTBylk43vXT11
S1MburD78q/jVS/+P3PnCudzxBeOpLi9Xg77VVWBdya5+2ek2XGyw8Q6Hgpp+kdB
PQURIg19BKSjUnrPMrujK8BxBTnmA20oeelzbXkQuM3uWr3CtsAXwgazMjfsxKW9
sJXsHXScNiA6b0aw/7mhSPYbFk0IAIwcKprkcHm2XXhgw8I+QFvK4V7YYuP9mHdh
Mcv2T+oJo+k34HjPzPygLyP9aXvOBoVZCz+SO3nM4iDbtjIFpRhqHjsGEq0prTs9
rluWOAN8DoNFLgMS3TXq19YyWrB/7HJWRXzyVIDusLBapOvAEQIBZaOCBYgwggWE
MA4GA1UdDwEB/wQEAwIGQDCCA5QGA1UdIASCA4swggOHMIIDbgYOKwYBBAGBqBgC
AQFRAgIwggNaMCYGCCsGAQUFBwIBFhpodHRwOi8vY3AuZS1zemlnbm8uaHUvcWNw
czCCARIGCCsGAQUFBwICMIIBBBqCAQBRdWFsaWZpZWQgY2VydGlmaWNhdGUgKEJy
b256ZSksIHRoZSBwcml2YXRlIGtleSByZXNpZGVzIGluIGEgcXVhbGlmaWVkIHNp
Z25hdHVyZSBjcmVhdGlvbiBkZXZpY2UgKFFTQ0QpLiBSZXRlbnRpb24gcGVyaW9k
IG9mIG1hdGVyaWFsIGluZm9ybWF0aW9uOiAxMCB5ZWFycy4gTGltaXQgb24gdGhl
IHZhbHVlIG9mIHRyYW5zYWN0aW9uozogSFVGIDFNLiBUaGUgc3ViamVjdCBvZiB0
aGUgY2VydGlmaWNhdGUgaXMgbm90IGEgbmF0dXJhbCBwZXJzb24uMIICGAYIKwYB
BQUHAgIwggIKHoICBgBNAGkAbgFRAHMA7QB0AGUAdAB0ACAAdABhAG4A+gBzAO0A
dAB2AOEAbgB5ACAAKABCAHIAbwBuAHoAKQAsACAAYQAgAG0AYQBnAOEAbgBrAHUA
bABjAHMAbwB0ACAAbQBpAG4BUQBzAO0AdABlAHQAdAAgAGEAbADhAO0AcgDhAHMA
LQBsAOkAdAByAGUAaABvAHoA8wAgAGUAcwB6AGsA9gB6ACAAKABNAEEATABFACkA
IAB2AOkAZABpAC4AIABBACAAcgBlAGcAaQBzAHoAdAByAOEAYwBpAPMAcwAgAGEA
ZABhAHQAbwBrAGEAdAAgAGEAIABzAHoAbwBsAGcA4QBsAHQAYQB0APMAIABhACAA
dABhAG4A+gBzAO0AdAB2AOEAbgB5ACAAbABlAGoA4QByAHQA4QB0APMAbAAgAHMA
egDhAG0A7QB0AG8AdAB0ACAAMQAwACAA6QB2AGkAZwAgAVEAcgB6AGkAIABtAGUA
ZwAuACAAVAByAGEAbgB6AGEAawBjAGkA8wBzACAAbABpAG0AaQB0ADoAIAAxAE0A
IABGAHQALgAgAEEAIAB0AGEAbgD6AHMA7QB0AHYA4QBuAHkAIABhAGwAYQBuAHkA
YQAgAE4ARQBNACAAdABlAHIAbQDpAHMAegBlAHQAZQBzACAAcwB6AGUAbQDpAGwA
eQAuMAkGBwQAi+xAAQMwCAYGBACPegECMB0GA1UdDgQWBBSrCLUvvzcoxW6JFE2H
vBIYq41x/DAfBgNVHSMEGDAWgBSxGI+yuTjSnmc3e3gVWTuv+gAXsjA/BgNVHREE
ODA2gRlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJloBkGCCsGAQUFBwgDoA0wCwYJ
KwYBBAGBqBgCMDQGA1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwuZS1zemlnbm8u
aHUvcW9jYTIwMTYuY3JsMG4GCCsGAQUFBwEBBGIwYDAtBggrBgEFBQcwAYYhaHR0
cDovL3FvY2EyMDE2LW9jc3AxLmUtc3ppZ25vLmh1MC8GCCsGAQUFBzAChiNodHRw
Oi8vd3d3LmUtc3ppZ25vLmh1L3FvY2EyMDE2LmNydDCBsgYIKwYBBQUHAQMEgaUw
gaIwCAYGBACORgEBMBUGBgQAjkYBAjALEwNIVUYCAQECAQYwCwYGBACORgEDAgEK
MAgGBgQAjkYBBDBTBgYEAI5GAQUwSTAkFh5odHRwczovL2NwLmUtc3ppZ25vLmh1
L3FjcHNfZW4TAkVOMCEWG2h0dHBzOi8vY3AuZS1zemlnbm8uaHUvcWNwcxMCSFUw
EwYGBACORgEGMAkGBwQAjkYBBgIwDQYJKoZIhvcNAQELBQADggIBACbFRT9o7AX5
/ND5NfiqcRtjYBHKgD/BM1nVF+BaYKh87gvnR6g1P7LLiTJMSsvuTxSWbV4qPfF8
g254hhFHr7NvWu31WNqbdt6aiRu1VC3pZB7HsNQO2jKP85Rm8evE+VNP3WBUqClG
nUBAKS/3IwuaL3hJzpFdg7974sr3ULVlAxIMdEAa5Qve3Ky+5W2o62aJ/BQy3t9T
IiSijeePFJb31jsSzBMsDrfrEDyaAJ3QH4sdXoUX14EaNgQIGCUQtb6Nx3ZBkXqE
6enp0EjI9j6uLowAy2sj44XJdX7s2S1wxH1f3pYwM+5/6a1kVGtl2+mFkNltUQIA
y2AaFM+0Y9/ZWCHi1vmTLIn0TyvSp6vcNw54EVOlM0lBJ7Wp6EXyYKyE5gyrB4CZ
AJIlniEk90845vUBhhJoc71Y4twYWUTsE7RlX3Z720kcRYbUV/dGQ9Wk3mTe+FFl
09Oxc3GoC3mE+QQeE1Nw2xoWD8+wpxF0mh6nc1w0Al/JHsGzBReaKiqTXbzKa/iG
VavlxcN7tcT+GV3aPzqNzqx7tdnGWSBmtv70HivVFb6TDutpbLt7bfo97ER1GSJG
OxK1exjnpp1IMGR4ok1QrlmW+p4eTw0Cv6KY5RmDPqIWudVwGGZ1P5X9Hx6M4Id8
qsMHQj6VkYCOB6ZSUcjK5Rag0syjtBr0
-----END CERTIFICATE-----
```


Aangetekende.email

Type	EDS/Q
Status	granted
Status starting time	2018-02-08T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	167188733894607427019297771870 82
Signature algorithm	SHA256withRSA
Issuer	CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
Valid from	Tue Jun 06 09:58:01 UTC 2017
Valid to	Thu Jun 06 09:58:01 UTC 2019
Subject	SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions, L=Heusden-Zolder, C=BE

Public key	Sun RSA public key, 2048 bits modulus: 24859440349058275244465543481669119891509867887407136347306008122383500635157452210483314205298254091229867863859444317438853115267447924906233495305588553904033177799999576101174959997325511547038100344909773556671623541259145328479195969023532832086396173597280418753794986343084828941545834485626152460124797779634125687969346509643982191579077813865234440793724645864923524004350810053143570250124385979993063282825209989239356134304137611603744508468363886858384523117286653022023158025921311415205774272828062858760601600861186906139777682521040235171258708200462492916095087954796508690394493025493769970770423 public exponent: 101
Subject key identifier	2ae3817682ffe94c44acebb2fb531fa8ab8b8806
CRL distribution points	http://crl.e-szigno.hu/qoca2016.crl
Authority key identifier	b1188fb2b938d29e67377b7815593baffa0017b2
Key usage	nonRepudiation
Basic constraints	CA=false
SHA1 Thumbprint	c57a90d3eb806696929b1d133602e6b7f4d4193a
SHA256 Thumbprint	97eea98d2d5ff304994021319f4370c539c1db804697a8c833a3e400345032cf

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=1.3.6.1.4.1.21528.2.3.2.3171, EMAILADDRESS=info@connect-solutions.be, CN=Connect Solutions, OID.2.5.4.97=VATBE-0843871294, O=Connect Solutions,
L=Heusden-Zolder, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
24859440349058275244465543481669119891509867887407136347306008122383500635157452210483314205298254091229867863859444317438853115267447924906233495305588553904033177799999576
10117495999732551154703810034490977355667162354125914532847919596902353283208639617359728041875379498634308482894154583448562615246012479777963412568796934650964398219157907
78138652344407937246458649235240043508100531435702501243859799930632828252099892393561343041376116037445084683638868583845231172866530220231580259213114152057742728280628587
60601600861186906139777682521040235171258708200462492916095087954796508690394493025493769970770423
 public exponent: 101
 Validity: [From: Tue Jun 06 09:58:01 UTC 2017,
             To: Thu Jun 06 09:58:01 UTC 2019]
 Issuer: CN=Qualified e-Szigno Organization CA 2016, OID.2.5.4.97=VATHU-23584497-2-41, O=Microsec Ltd., L=Budapest, C=HU
 SerialNumber: [    d30597ee 762bdb53 c5242dc9 0a]

Certificate Extensions: 8
[1]: ObjectId: 1.3.6.1.5.5.7.1.3 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 81 A5 30 81 A2 30 08   06 06 04 00 8E 46 01 01  ...0..0......F..
0010: 30 15 06 06 04 00 8E 46   01 02 30 0B 13 03 48 55  0......F..0...HU
0020: 46 02 01 01 02 01 06 30   0B 06 06 04 00 8E 46 01  F......0......F.
0030: 03 02 01 0A 30 08 06 06   04 00 8E 46 01 04 30 53  ....0......F..0S
0040: 06 06 04 00 8E 46 01 05   30 49 30 24 16 1E 68 74  .....F..0I0$..ht
0050: 74 70 73 3A 2F 2F 63 70   2E 65 2D 73 7A 69 67 6E  tps://cp.e-szign
0060: 6F 2E 68 75 2F 71 63 70   73 5F 65 6E 13 02 45 4E  o.hu/qcps_en..EN
0070: 30 21 16 1B 68 74 74 70   73 3A 2F 2F 63 70 2E 65  0!..https://cp.e
0080: 2D 73 7A 69 67 6E 6F 2E   68 75 2F 71 63 70 73 13  -szigno.hu/qcps.
0090: 02 48 55 30 13 06 06 04   00 8E 46 01 06 30 09 06  .HU0......F..0..
00A0: 07 04 00 8E 46 01 06 02                            ....F...


[2]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://qoca2016-ocsp1.e-szigno.hu,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.e-szigno.hu/qoca2016.crt]
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B1 18 8F B2 B9 38 D2 9E   67 37 7B 78 15 59 3B AF  .....8..g7.x.Y;.
0010: FA 00 17 B2                                        ....
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
```

```
 [DistributionPoint:
    [URIName: http://crl.e-szigno.hu/qoca2016.crl]
]]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.21528.2.1.1.81.2.2]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1A 68 74 74 70 3A 2F   2F 63 70 2E 65 2D 73 7A  ..http://cp.e-sz
0010: 69 67 6E 6F 2E 68 75 2F   71 63 70 73              igno.hu/qcps

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 01 04 1A 82 01 00   51 75 61 6C 69 66 69 65  0.......Qualifie
0010: 64 20 63 65 72 74 69 66   69 63 61 74 65 20 28 42  d certificate (B
0020: 72 6F 6E 7A 65 29 2C 20   74 68 65 20 70 72 69 76  ronze), the priv
0030: 61 74 65 20 6B 65 79 20   72 65 73 69 64 65 73 20  ate key resides
0040: 69 6E 20 61 20 71 75 61   6C 69 66 69 65 64 20 73  in a qualified s
0050: 69 67 6E 61 74 75 72 65   20 63 72 65 61 74 69 6F  ignature creatio
0060: 6E 20 64 65 76 69 63 65   20 28 51 53 43 44 29 2E  n device (QSCD).
0070: 20 52 65 74 65 6E 74 69   6F 6E 20 70 65 72 69 6F   Retention perio
0080: 64 20 6F 66 20 6D 61 74   65 72 69 61 6C 20 69 6E  d of material in
0090: 66 6F 72 6D 61 74 69 6F   6E 3A 20 31 30 20 79 65  formation: 10 ye
00A0: 61 72 73 2E 20 4C 69 6D   69 74 20 6F 6E 20 74 68  ars. Limit on th
00B0: 65 20 76 61 6C 75 65 20   6F 66 20 74 72 61 6E 73  e value of trans
00C0: 61 63 74 69 6F 6E 73 3A   20 48 55 46 20 31 4D 2E  actions: HUF 1M.
00D0: 20 54 68 65 20 73 75 62   6A 65 63 74 20 6F 66 20   The subject of
00E0: 74 68 65 20 63 65 72 74   69 66 69 63 61 74 65 20  the certificate
00F0: 69 73 20 6E 6F 74 20 61   20 6E 61 74 75 72 61 6C  is not a natural
0100: 20 70 65 72 73 6F 6E 2E                             person.

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 02 0A 1E 82 02 06   00 4D 00 69 00 6E 01 51  0........M.i.n.Q
0010: 00 73 00 ED 00 74 00 65   00 74 00 74 00 20 00 74  .s...t.e.t.t. .t
0020: 00 61 00 6E 00 FA 00 73   00 ED 00 74 00 76 00 E1  .a.n...s...t.v..
0030: 00 6E 00 79 00 20 00 28   00 42 00 72 00 6F 00 6E  .n.y. .(.B.r.o.n
0040: 00 7A 00 29 00 2C 00 20   00 61 00 20 00 6D 00 61  .z.).,. .a. .m.a
0050: 00 67 00 E1 00 6E 00 6B   00 75 00 6C 00 63 00 73  .g...n.k.u.l.c.s
0060: 00 6F 00 74 00 20 00 6D   00 69 00 6E 01 51 00 73  .o.t. .m.i.n.Q.s
0070: 00 ED 00 74 00 65 00 74   00 74 00 20 00 61 00 6C  ...t.e.t.t. .a.l
0080: 00 E1 00 ED 00 72 00 E1   00 73 00 2D 00 6C 00 E9  .....r...s.-.l..
0090: 00 74 00 72 00 65 00 68   00 6F 00 7A 00 F3 00 20  .t.r.e.h.o.z...
00A0: 00 65 00 73 00 7A 00 6B   00 F6 00 7A 00 20 00 28  .e.s.z.k...z. .(
00B0: 00 4D 00 41 00 4C 00 45   00 29 00 20 00 76 00 E9  .M.A.L.E.). .v..
00C0: 00 64 00 69 00 2E 00 20   00 41 00 20 00 72 00 65  .d.i... .A. .r.e
00D0: 00 67 00 69 00 73 00 7A   00 74 00 72 00 E1 00 63  .g.i.s.z.t.r...c
00E0: 00 69 00 F3 00 73 00 20   00 61 00 64 00 61 00 74  .i...s. .a.d.a.t
00F0: 00 6F 00 6B 00 61 00 74   00 20 00 61 00 20 00 73  .o.k.a.t. .a. .s
0100: 00 7A 00 6F 00 6C 00 67   00 E1 00 6C 00 74 00 61  .z.o.l.g...l.t.a
0110: 00 74 00 F3 00 20 00 61   00 20 00 74 00 61 00 6E  .t... .a. .t.a.n
0120: 00 FA 00 73 00 ED 00 74   00 76 00 E1 00 6E 00 79  ...s...t.v...n.y
0130: 00 20 00 6C 00 65 00 6A   00 E1 00 72 00 74 00 E1  . .l.e.j...r.t..
0140: 00 74 00 F3 00 6C 00 20   00 73 00 7A 00 E1 00 6D  .t...l. .s.z...m
0150: 00 ED 00 74 00 6F 00 74   00 74 00 20 00 31 00 30  ...t.o.t.t. .1.0
0160: 00 20 00 E9 00 76 00 69   00 67 00 20 01 51 00 72  . ...v.i.g. .Q.r
0170: 00 7A 00 69 00 20 00 6D   00 65 00 67 00 2E 00 20  .z.i. .m.e.g...
0180: 00 54 00 72 00 61 00 6E   00 7A 00 61 00 6B 00 63  .T.r.a.n.z.a.k.c
0190: 00 69 00 F3 00 73 00 20   00 6C 00 69 00 6D 00 69  .i...s. .l.i.m.i
01A0: 00 74 00 3A 00 20 00 31   00 4D 00 20 00 46 00 74  .t.:. .1.M. .F.t
01B0: 00 2E 00 20 00 41 00 20   00 74 00 61 00 6E 00 FA  ... .A. .t.a.n..
01C0: 00 73 00 ED 00 74 00 76   00 E1 00 6E 00 79 00 20  .s...t.v...n.y.
01D0: 00 61 00 6C 00 61 00 6E   00 79 00 61 00 20 00 4E  .a.l.a.n.y.a. .N
01E0: 00 45 00 4D 00 20 00 74   00 65 00 72 00 6D 00 E9  .E.M. .t.e.r.m..
01F0: 00 73 00 7A 00 65 00 74   00 65 00 73 00 20 00 73  .s.z.e.t.e.s. .s
0200: 00 7A 00 65 00 6D 00 E9   00 6C 00 79 00 2E        .z.e.m...l.y..

]]  ]
 [CertificatePolicyId: [0.4.0.194112.1.3]
[]  ]
 [CertificatePolicyId: [0.4.0.2042.1.2]
[]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Non_repudiation
]

[7]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@connect-solutions.be
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
]

[8]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 2A E3 81 76 82 FF E9 4C   44 AC EB B2 FB 53 1F A8  *..v...LD....S..
0010: AB 8B 88 06                                        ....
]
]
```

```
]
 Algorithm: [SHA256withRSA]
 Signature:
0000: CD 8D 7B B1 28 CF 00 D2   B8 49 20 87 DF AA 17 1A  ....(....I .....
0010: D9 C2 C3 40 0A FD EE EB   C0 CB 2A C8 04 BD E2 4B  ...@......*....K
0020: D1 1E B5 A3 01 A6 FB 51   AD F9 21 E2 3A AD C9 B1  .......Q..!.:...
0030: C1 CF 9E 98 93 17 B0 27   61 06 45 1E 34 59 B8 25  .......'a.E.4Y.%
0040: 19 FD 0B F8 60 E6 3E 06   75 3C A6 23 9D F2 F1 B8  ....`.>.u<.#....
0050: E6 89 BE 25 BA CA B9 4D   53 65 3A 2F 51 28 3E AC  ...%...MSe:/Q(>.
0060: 41 AE CB 43 30 9D 50 3C   30 41 2E 0E 9D EF 6F 88  A..C0.P<0A....o.
0070: 8A 55 64 C2 95 54 B0 0C   8F 3D 17 2F 9D D6 D9 B1  .Ud..T...=./....
0080: 15 1B 06 0E 10 E3 BD 0A   11 61 6D B2 10 CA 3F 9D  .........am...?.
0090: 24 44 D6 80 CC EA 65 56   00 A0 3E 38 D5 FD 9E C7  $D....eV..>8....
00A0: A8 27 FD 30 F4 F7 10 9F   97 C1 EA 51 94 4C F5 3F  .'.0.......Q.L.?
00B0: 3C C7 DC DD 57 8B ED 65   7A 01 28 04 BE 41 88 11  <...W..ez.(..A..
00C0: 28 63 74 89 87 BC 25 0A   5C 0C A4 64 36 06 21 10  (ct...%.\..d6.!.
00D0: 0E 95 86 E3 99 6A 3E 8D   0B 30 7E 0C D4 B2 DC A2  .....j>..0......
00E0: 46 6D F9 D7 A1 8E 85 5F   EF DB 94 D6 FD 04 4F 17  Fm....._......O.
00F0: D9 42 35 DA 8C F4 D9 AF   60 25 7B 51 13 BE 2F 0C  .B5.....`%.Q../.
0100: 2F 0D 5D DE A5 26 DA B2   FB 02 F0 67 68 4B 9C 33  /.]..&.....ghK.3
0110: BA F4 B7 AC 88 A8 15 63   5A 69 54 C5 B3 60 0A 9D  .......cZiT..`..
0120: CA E4 8B CF 43 B6 6E B1   86 4A DE 71 86 BD A0 40  ....C.n..J.q...@
0130: CE 46 B9 F8 36 28 5C CD   7A 0A 68 C1 4F 67 4D 3A  .F..6(\.z.h.OgM:
0140: D2 81 85 60 96 02 33 24   A5 A2 D8 A0 1D C0 BD D3  ...`..3$........
0150: 7F 0F DF C8 C1 57 F5 EC   9B 51 7E 54 4B BE EE 71  .....W...Q.TK..q
0160: 40 B8 DD 7A 4D A4 76 CD   96 CB 41 C7 F8 72 0F 27  @..zM.v...A..r.'
0170: C7 A7 62 5D 64 87 22 88   9A C6 72 FC B9 65 F4 6C  ..b]d."...r..e.l
0180: 11 BD 45 48 A1 A5 48 32   05 94 0F 02 4F 11 F0 78  ..EH..H2....O..x
0190: 28 86 A9 CC 01 07 79 BE   76 A6 5E 98 A0 2E 0A 9C  (.....y.v.^.....
01A0: 38 B4 62 01 88 6C 9D BF   A2 0E 38 FC 8C 71 92 04  8.b..l....8..q..
01B0: B3 2A D4 86 E2 C2 54 F9   DD 35 BB 26 D3 B7 EE 7A  .*....T..5.&...z
01C0: E4 6A F1 FB F1 F6 0D 3E   C5 DC E5 41 A4 86 AC 00  .j.....>...A....
01D0: 8A 2C 0A 45 A1 37 69 F4   6E 45 6F DA D6 08 0E 1F  .,.E.7i.nEo.....
01E0: C3 69 99 7D 51 D2 1A A6   17 CA 90 82 D9 E7 BF DF  .i..Q...........
01F0: 2F B3 C3 6A E7 D8 C8 51   16 37 96 D5 4A 2A A0 2B  /..j...Q.7..J*.+

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIKZDCCCEygAwIBAgIOANMFl+52K9tTxSQtyQowDQYJKoZIhvcNAQELBQAwgYgx
CzAJBgNVBAYTAkhVMREwDwYDVQQHDAhCdWRhcGVzdDEWMBQGA1UECgwNTWljcm9z
ZWMgTHRkLjEcMBoGA1UEYQwTVkFUSFUtMjM1ODQ0OTctMi00MTEwMC4GA1UEAwwn
UXVhbGlmaWVkIGUtU3ppZ25vIE9yZ2FuaXphdGlvbiBDQSAyMDE2MB4XDTE3MDYw
NjA5NTgwMVoXDTE5MDYwNjA5NTgwMVowgcoxCzAJBgNVBAYTAkJFMRcwFQYDVQQH
DA5IZXVzZGVuLVpvbGRlcjEaMBgGA1UECgwRQ29ubmVjdCBTb2x1dGlvbnMxGTAX
BgNVBGEMEFZBVEJFLTA4NDM4NzEyOTQxGjAYBgNVBAMMEUNvbm5lY3QgU29sdXRp
b25zMSgwJgYJKoZIhvcNAQkBFhlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJlMSUw
IwYDVQQFExwxLjMuNi4xLjQuMS4yMTUyOC4yLjMuMi4zMTcxMIIBIDANBgkqhkiG
9w0BAQEFAAOCAQ0AMIIBCAKCAQEAxOy5JaSmHfhFrjG7SMhFi0ixd2DKh2UJZZS6
b/m0QgHBttD8j7ozwRcXw2FmEjp0fsMkhGoyeGY6ns2b6DWmWrkGhEZKUbfgkPwQ
CcRAh8h1Sth69Rjbqrwf/cdl65vwWB6VMscmej+Zdf05jVeyTV/QbvLGq5ATbj6
witJkKDVpSDqgf9opUBGSoK+hgAF8CbmPDY1OyY2vhUNM+cvEyC9WTBt+8rvMlW2
s2HyvYI3fPPpOUYUqvrBX2EzLcqq+z32eeZMLeETKR2l3Itb9bWrsyBxioxtl441
5UHjCIJwgwDv6JoXtVvXcGcRyXNIdhIOLhg3Lvgwzy3gLuvh9wIBZaOCBYgwggWE
MA4GA1UdDwEB/wQEAwIGQDCCA5QGA1UdIASCA4swggOHMIIDbgYOKwYBBAGBqBgC
AQFRAgIwggNaMCYGCCsGAQUFBwIBFhpodHRwOi8vY3AuZS1zemlnbm8uaHUvcWNw
czCCARIGCCsGAQUFBwICMIIBBBqCAQBRdWFsaWZpZWQgY2VydGlmaWNhdGUgKEJy
b256ZSksIHRoZSBwcml2YXRlIGtleSByZXNpZGVzIGluIGEgcXVhbGlmaWVkIHNp
Z25hdHVyZSBjcmVhdGlvbiBkZXZpY2UgKFFTQ0QpLiBSZXRlbnRpb24gcGVyaW9k
IG9mIG1hdGVyaWFsIGluZm9ybWF0aW9uOiAxMCB5ZWFycy4gTGltaXQgb24gdGhl
IHZhbHVlIG9mIHRyYW5zYWN0aW9uczogSFVGIDFNLiBUaGUgc3ViamVjdCBvZiB0
aGUgY2VydGlmaWNhdGUgaXMgbm90IGEgbmF0dXJhbCBwZXJzb24uMIICGAYIKwYB
BQUHAgIwggIKHoICBgBNAGkAbgFRAHMA7QB0AGUAdAB0ACAAdABhAG4A+gBzAO0A
dAB2AOEAbgB5ACAAKABCAHIAbwBuAHoAKQAsACAAYQAgAG0AYQBnAOEAbgBrAHUA
bABjAHMAbwB0ACAAbQBpAG4BUQBzAO0AdABlAHQAdAAgAGEAbADhAO0AcgDhAHMA
LQBsAOkAdAByAGUAaABvAHoA8wAgAGUAcwB6AGsA9gB6ACAAKABNAEEATABFACkA
IAB2AOkAZABpAC4AIABBACAAcgBlAGcAaQBzAHoAdAByAOEAYwBpAPMAcwAgAGEA
ZABhAHQAbwBrAGEAdAAgAGEAIABzAHoAbwBsAGcA4QBsAHQAYQB0APMAIABhACAA
dABhAG4A+gBzAO0AdAB2AOEAbgB5ACAAbABlAGoA4QByAHQA4QB0APMAbAAgAHMA
egDhAG0A7QB0AG8AdAB0ACAAMQAwACAA6QB2AGkAZwAgAVEAcgB6AGkAIABtAGUA
ZwAuACAAVAByAGEAbgB6AGEAawBjAGkA8wBzACAAbABpAG0AaQB0ADoAIAAxAE0A
IABGAHQALgAgAEEAIAB0AGEAbgB6AHMA7QB0AHYA4QBuAHkAIABhAGwAYQBuAHkA
YQAgAE4ARQBNACAAdABlAHIAbQDpAHMAegBlAHQAZQBzACAAcwB6AGUAbQDpAGwA
eQAuMAkGBwQAi+xAAQMwCAYGBACPegECMB0GA1UdDgQWBBQq44F2gv/pTESs67L7
Ux+oq4uIBjAfBgNVHSMEGDAWgBSxGI+yuTjSnmc3e3gVWTuv+gAXsjA/BgNVHREE
ODA2gRlpbmZvQGNvbm5lY3Qtc29sdXRpb25zLmJloBkGCCsGAQUFBwgDoA0wCwYJ
KwYBBAGBqBgCMDQGA1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwuZS1zemlnbm8u
aHUvcW9jYTIwMTYuY3JsMG4GCCsGAQUFBwEBBGIwYDAtBggrBgEFBQcwAYYhaHR0
cDovL3FvY2EyMDE2LW9jc3AxLmUtc3ppZ25vLmh1MC8GCCsGAQUFBzAChiNodHRw
Oi8vd3d3LmUtc3ppZ25vLmh1L3FvY2EyMDE2LmNydDCBsgYIKwYBBQUHAQMEgaUw
gaIwCAYGBACORgEBMBUGBgQAjkYBAjALEwNIVUYCAQECAQYwCwYGBACORgEDAgEK
MAgGBgQAjkYBBDBTBgYEAI5GAQUwSTAkFh5odHRwczovL2NwLmUtc3ppZ25vLmh1
L3FjcHNfZW4TAkVOMCEWG2h0dHBzOi8vY3AuZS1zemlnbm8uaHUvcWNwcxMCSFUw
EwYGBACORgEGMAkGBwQAjkYBBgIwDQYJKoZIhvcNAQELBQADggIBAM2Ne7EozwDS
uEkgh9+qFxrZwsNACv3u68DLKsgEveJL0R61owGm+1Gt+SHiOq3JscHPnpiTF7An
YQZFHjRZuCUZ/Qv4YOY+BnU8piOd8vG45om+JbrKuU1TZTovUSg+rEGuy0MwnVA8
MEEuDp3vb4iKVWTClVSwDI89Fy+d1tmxFRsGDhDjvQoRYW2yEMo/nSRE1oDM6mVW
AKA+ONX9nseoJ/0w9PcQn5fB6lGUTPU/PMfc3VeL7WV6ASgEvkGIEShjdImHvCUK
XAykZDYGIRAOlYbjmWo+jQswfgzUstyiRm3516GOhV/v25TW/QRPF9lCNdqM9Nmv
YCV7URO+LwwvDV3epSbasvsC8GdoS5wzuvS3rIioFWNaaVTFs2AKncrki89Dtm6x
hkrecYa9oEDORrn4NihczXoKaMFPZ0060oGFYJYCMySlotigHcC9038P38jBV/Xs
m1F+VEu+7nFAuN16TaR2zZbLQcf4cg8nx6diXWSHIoiaxnL8uWX0bBG9RUihpUgy
BZQPAk8R8HgohqnMAQd5vnamXpigLgqcOLRiAYhsnb+iDjj8jHGSBLMq1IbiwlT5
```

3TW7JtO37nrkavH78fYNPsXc5UGkhqwAiiwKRaE3afRuRW/a1ggOH8NpmX1R0hqm
F8qQgtnnv98vs8Nq59jIURY3ltVKKqAr
-----END CERTIFICATE-----

Universign

Service provider trade name	VATBE-0673755466
Information URI	https://www.universign.com/en/certifications
Service provider street address	Rue des Anciens Etangs 40
Service provider postal code	1190
Service provider locality	Forest
Service provider state	Bruxelles
Service provider country	BE

Universign CA Hardware

Type	CA/QC
Status	granted
Status starting time	2018-05-03T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	140703056120414465291844983464117439126
Signature algorithm	SHA256withRSA
Issuer	CN=Universign Primary CA hardware, OU=0002 43912916400026, O=Cryptolog International, C=FR
Valid from	Wed May 31 14:54:32 UTC 2017
Valid to	Mon May 31 14:54:32 UTC 2027
Subject	CN=Universign CA hardware, OID.2.5.4.97=NTRBE-0673755466, O=Universign, C=BE
Public key	Sun RSA public key, 2048 bits modulus: 21729125281410544028392057685307155520980647366368115207122468602254825140651316431170147687829671225094546345236707508641637139714659552369478824024350286615846070368087853266859245056446324844451498669338904750040693159215272852668952311094753935148676601338187465924926582480109462770992021078556028501309990386809667405908834036829464612777742141866370019865645929850537978151015619674281056534647727961035135832447269952935386678440281846938981960963446612368988657861606469692846586255093601129463658007964748011454618238514869647514516393075923760992850022321674681702487092693622616979687785683895829317709317 public exponent: 65537
Subject key identifier	3e42fc11d1400c09d03a4cefab3b4c57153aab0d
CRL distribution points	http://crl.universign.eu/universign_primary_ca_hardware.crl
Authority key identifier	4dd9fca82dc7c85aa4ad5f49ae68a4dc9e8a1222
Key usage	keyCertSign cRLSign

Basic constraints CA=true; PathLen=0
SHA1 Thumbprint 4cce938e8ffdfc3edc9ced852ae65b6c24bfda23
SHA256 Thumbprint 6c1f4bf5b489362291e0f1c154828c99677e4715d6517b842d5f2d21d5e12448

Extension (critical: true)

Additional service information

ForeSignatures

Extension (critical: true)

Qualifications

Qualifier: QCNoQSCD

Criterial List Description

Assert: atLeastOne

Policy OID: 1.3.6.1.4.1.15819.5.1.3.1

Extension (critical: true)

Qualifications

Qualifier: NotQualified

Criterial List Description

Assert: none

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Universign CA hardware, OID.2.5.4.97=NTRBE-0673755466, O=Universign, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
21729125281410544028392057685307155520980647366368115207122468602254825140651316431170147687829671225094546345236707508641637139714659552369478824024350286615846070368087853
26685924505644632484445149866933890475004069315921527285266895231109475393514867660133818746592492658248010946277099202107855602850130999038680966740590883403682946461277774
21418663700198656459298505379781510156196742810565346477279610351358324472699529353866784402818469389819609634466123689886578616064696928465862550936011294636580079647480114
54618238514869647514516393075923760992850022321674681702487092693622616979687785683895829317709317
 public exponent: 65537
 Validity: [From: Wed May 31 14:54:32 UTC 2017,
             To: Mon May 31 14:54:32 UTC 2027]
 Issuer: CN=Universign Primary CA hardware, OU=0002 43912916400026, O=Cryptolog International, C=FR
 SerialNumber: [    69da6c43 7f077791 b991dbe7 99188a96]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4D D9 FC A8 2D C7 C8 5A   A4 AD 5F 49 AE 68 A4 DC  M...-..Z.._I.h..
0010: 9E 8A 12 22                                        ..."
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.universign.eu/universign_primary_ca_hardware.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1A 68 74 74 70 3A 2F   2F 64 6F 63 73 2E 75 6E  ..http://docs.un
0010: 69 76 65 72 73 69 67 6E   2E 65 75 2F              iversign.eu/

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
```

```
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 3E 42 FC 11 D1 40 0C 09   D0 3A 4C EF AB 3B 4C 57  >B...@...:L..;LW
0010: 15 3A AB 0D                                        .:..
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 02 66 AD AF 77 73 B1 86   F8 B0 81 EB 86 DF A8 43  .f..ws.........C
0010: 8D 5F 27 4D FD C2 C8 87   7A 73 25 D6 91 CF 17 EB  ._'M....zs%.....
0020: 04 B3 98 C8 67 91 D7 98   66 C2 E0 AD 10 8A 86 D6  ....g...f.......
0030: 76 94 7D 58 C2 0B D4 0F   2B C8 DD 81 51 A7 83 72  v..X....+...Q..r
0040: 0B 54 31 FE D9 92 AD 6E   23 CF 5B BB 89 32 37 F7  .T1....n#.[..27.
0050: C4 83 E6 D8 A9 D3 7E 02   58 00 C8 FD F3 85 5A 1F  ........X.....Z.
0060: E5 FE A5 75 2C B2 3A 08   DF 16 9D 27 5F F5 37 09  ...u,.:....'_.7.
0070: 93 DE D3 01 66 84 3C 6C   D4 6E 5D 7B CC CC DB F8  ....f.<l.n].....
0080: 08 C1 B4 C7 51 93 47 9F   DC 53 4D 2D 5A 8B C5 24  ....Q.G..SM-Z..$
0090: F7 DC F4 22 08 B0 BE 19   1B EF 99 60 DD 52 96 A5  ..."....... `.R..
00A0: C0 C5 C5 B9 D8 19 CF 24   1B 6F 1A 97 A2 50 1B 79  .......$.o...P.y
00B0: BC 8D 91 83 C6 0C 00 27   70 18 78 2E D6 EF BA D7  .......'p.x.....
00C0: B1 9E 29 9A CC 95 97 6D   B9 AA 60 1C 07 AB 5E D0  ..)....m..`...^.
00D0: 30 6E 36 4D E5 85 EB 35   0F 4E BA 07 7B 78 1C A9  0n6M...5.N...x..
00E0: 35 E2 B2 CF 1B C7 7B 7F   12 4E B2 7B AC 51 2C 6A  5........N...Q,j
00F0: FF 04 B6 15 7D D9 75 10   28 30 1E 7E FE B8 AA A3  ......u.(0......

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIEUTCCAzmgAwIBAgIQadpsQ38Hd5G5kdvnmRiKljANBgkqhkiG9w0BAQsFADB2
MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwx
HDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxJzAlBgNVBAMTHlVuaXZlcnNp
Z24gUHJpbWFyeSBDQSBoYXJkd2FyZTAeFw0xNzA1MzExNDU0MzJaFw0yNzA1MzEx
NDU0MzJaMF4xCzAJBgNVBAYTAkJFMRMwEQYDVQQKEwpVbml2ZXJzaWduMRkwFwYD
VQRhExBOVFJCRS0wNjczNzU1NDY2MR8wHQYDVQQDExZVbml2ZXJzaWduIENBIGhh
cmR3YXJlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArCC5WukzPz9n
DOGZ9BL6ffG81d0w6eir1/y9tGus9+RaqlWfgARU/CFMGbMigZOsCEyZ0QnANIqL
uMMdwwlOlFv6oM704Cp29qk+0K/ctGJkNSSIal1FQVM1ZlZbqjlFoZ75iHhb6aUL
JSZVU7drKlBrlpYFJ1Slcw+HYajOgJle0yE4uW2v8HcESbnqMJGxa3pVS84grEQL
iESwWvsbe0K8/H60UtBh8zy7OuPzJA6nwq5rbfgjvNc4WM6pQ4Kp5uAb2tAVDYWk
dWXtfxr5Ym3RWa3zl232VwVbuFcoHnBWdIuXE6RwEqR5ZKuZiWYMrFaGOlH6unRG
9JZNTd5uBQIDAQABo4HyMIHvMA4GA1UdDwEB/wQEAwIBBjBMBgNVHR8ERTBDMEGg
P6A9hjtodHRwOi8vY3JsLnVuaXZlcnNpZ24uZXUvdW5pdmVyc2lnbl9wcmltYXJ5
X2NhX2hhcmR3YXJlLmNybDAdBgNVHQ4EFgQUPkL8EdFADAnQOkzvqztMVxU6qw0w
OwYDVR0gBDQwMjAwBgRVHSAAMCgwJgYIKwYBBQUHAgEWGmh0dHA6Ly9kb2NzLnVu
aXZlcnNpZ24uZXUvMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUTdn8
qC3HyFqkrV9Jrmik3J6KEiIwDQYJKoZIhvcNAQELBQADggEBAAJmra93c7GG+LCB
64bfqEONXydN/cLIh3pzJdaRzxfrBLOYyGeR15hmwuCtEIqG1naUfVjCC9QPK8jd
gVGng3ILVDH+2ZKtbiPPW7uJMjf3xIPm2KnTfgJYAMj984VaH+X+pXUssjoI3xad
J1/1NwmT3tMBZoQ8bNRuXXvMzNv4CMG0x1GTR5/cU00tWovFJPfc9CIIsL4ZG++Z
YN1SlqXAxcW52BnPJBtvGpeiUBt5vI2Rg8YMACdwGHgu1u+617GeKZrMlZdtuapg
HAerXtAwbjZN5YXrNQ9Ougd7eBypNeKyzxvHe38STrJ7rFEsav8EthV92XUQKDAe
fv64qqM=
-----END CERTIFICATE-----
```

Universign CA hardware

Type	CA/QC
Status	granted
Status starting time	2018-05-03T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	140703056120414465291844983464117439126
Signature algorithm	SHA256withRSA
Issuer	CN=Universign Primary CA hardware, OU=0002 43912916400026, O=Cryptolog International, C=FR
Valid from	Wed May 31 14:54:32 UTC 2017
Valid to	Mon May 31 14:54:32 UTC 2027
Subject	CN=Universign CA hardware, OID.2.5.4.97=NTRBE-0673755466, O=Universign, C=BE

Public key	Sun RSA public key, 2048 bits modulus: 21729125281410544028392057685307155520980647366368115207122468602254825140651316431170147687829671225094546345236707508641637139714659552369478824024350286615846070368087853266859245056446324844451498669338904750040693159215272852668952311094753935148676601338187465924926582480109462770992021078556028501309990386809667405908834036829464612777742141866370019865645929850537978151015619674281056534647727961035135832447269952935386678440281846938981960963446612368988657861606469692846586255093601129463658007964748011454618238514869647514516393075923760992850022321674681702487092693622616979687785683895829317709317 public exponent: 65537
Subject key identifier	3e42fc11d1400c09d03a4cefab3b4c57153aab0d
CRL distribution points	http://crl.universign.eu/universign_primary_ca_hardware.crl
Authority key identifier	4dd9fca82dc7c85aa4ad5f49ae68a4dc9e8a1222
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	4cce938e8ffdfc3edc9ced852ae65b6c24bfda23
SHA256 Thumbprint	6c1f4bf5b489362291e0f1c154828c99677e4715d6517b842d5f2d21d5e12448

Extension (critical: true)

Additional service information

ForeSeals

Extension (critical: true)

Qualifications

Qualifier: QCNoQSCD

Criterial List Description

Assert: atLeastOne

Policy OID: 1.3.6.1.4.1.15819.5.1.3.5

Extension (critical: true)

Qualifications

Qualifier: NotQualified

Criterial List Description

Assert: none

The decoded certificate:


```
[
[
 Version: V3
 Subject: CN=Universign CA hardware, OID.2.5.4.97=NTRBE-0673755466, O=Universign, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
21729125281410544028392057685307155520980647366368115207122468602254825140651316431170147687829671225094546345236707508641637139714659552369478824024350286615846070368087853266859245056446324844451498669338904750040693159215272852668952311094753935148676601338187465924926582480109462770992021078556028501309990386809667405908834036829464612777742141866370019865645929850537978151015619674281056534647727961035135832447269952935386678440281846938981960963446612368988657861606469692846586255093601129463658007964748011454618238514869647514516393075923760992850022321674681702487092693622616979687785683895829317709317
 public exponent: 65537
 Validity: [From: Wed May 31 14:54:32 UTC 2017,
             To: Mon May 31 14:54:32 UTC 2027]
 Issuer: CN=Universign Primary CA hardware, OU=0002 43912916400026, O=Cryptolog International, C=FR
 SerialNumber: [    69da6c43 7f077791 b991dbe7 99188a96]
```

```
Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4D D9 FC A8 2D C7 C8 5A   A4 AD 5F 49 AE 68 A4 DC  M...-..Z.._I.h..
0010: 9E 8A 12 22                                        ..."
]

]

[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.universign.eu/universign_primary_ca_hardware.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1A 68 74 74 70 3A 2F   2F 64 6F 63 73 2E 75 6E  ..http://docs.un
0010: 69 76 65 72 73 69 67 6E   2E 65 75 2F              iversign.eu/

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 3E 42 FC 11 D1 40 0C 09   D0 3A 4C EF AB 3B 4C 57  >B...@...:L..;LW
0010: 15 3A AB 0D                                        .:..
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 02 66 AD AF 77 73 B1 86   F8 B0 81 EB 86 DF A8 43  .f..ws.........C
0010: 8D 5F 27 4D FD C2 C8 87   7A 73 25 D6 91 CF 17 EB  ._'M....zs%.....
0020: 04 B3 98 C8 67 91 D7 98   66 C2 E0 AD 10 8A 86 D6  ....g...f.......
0030: 76 94 7D 58 C2 0B D4 0F   2B C8 DD 81 51 A7 83 72  v..X....+...Q..r
0040: 0B 54 31 FE D9 92 AD 6E   23 CF 5B BB 89 32 37 F7  .T1....n#.[..27.
0050: C4 83 E6 D8 A9 D3 7E 02   58 00 C8 FD F3 85 5A 1F  ........X.....Z.
0060: E5 FE A5 75 2C B2 3A 08   DF 16 9D 27 5F F5 37 09  ...u,.:....'_.7.
0070: 93 DE D3 01 66 84 3C 6C   D4 6E 5D 7B CC CC DB F8  ....f.<l.n].....
0080: 08 C1 B4 C7 51 93 47 9F   DC 53 4D 2D 5A 8B C5 24  ....Q.G..SM-Z..$
0090: F7 DC F4 22 08 B0 BE 19   1B EF 99 60 DD 52 96 A5  ..."........`.R..
00A0: C0 C5 C5 B9 D8 19 CF 24   1B 6F 1A 97 A2 50 1B 79  .......$.o...P.y
00B0: BC 8D 91 83 C6 0C 00 27   70 18 78 2E D6 EF BA D7  .......'p.x.....
00C0: B1 9E 29 9A CC 95 97 6D   B9 AA 60 1C 07 AB 5E D0  ..)....m..`...^.
00D0: 30 6E 36 4D E5 85 EB 35   0F 4E BA 07 7B 78 1C A9  0n6M...5.N...x..
00E0: 35 E2 B2 CF 1B C7 7B 7F   12 4E B2 7B AC 51 2C 6A  5........N...Q,j
00F0: FF 04 B6 15 7D D9 75 10   28 30 1E 7E FE B8 AA A3  ......u.(0......

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIEUTCCAzmgAwIBAgIQadpsQ38Hd5G5kdvnmRiKljANBgkqhkiG9w0BAQsFADB2
MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwx
HDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxJzAlBgNVBAMTHlVuaXZlcnNp
Z24gUHJpbWFyeSBDQSBoYXJkd2FyZTAeFw0xNzA1MzExNDU0MzJaFw0yNzA1MzEx
NDU0MzJaMF4xCzAJBgNVBAYTAkJFMRMwEQYDVQQKEwpVbml2ZXJzaWduMRkwFwYD
VQRhExBOVFJCRS0wNjczNzU1NDY2MR8wHQYDVQQDExZVbml2ZXJzaWduIENBIGhh
cmR3YXJlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArCC5WukzPz9n
DOGZ9BL6ffG81d0w6eir1/y9tGus9+RaqlWfgARU/CFMGbMigZOsCEyZ0QnANIqL
uMMdwwlOlFv6oM704Cp29qk+0K/ctGJkNSSIal1FQVM1ZlZbqjlFoZ75iHhb6aUL
JSZVU7drKlBrlpYFJ1Slcw+HYajOgJle0yE4uW2v8HcESbnqMJGxa3pVS84grEQL
iESwWvsbe0K8/H60UtBh8zy7OuPzJA6nwq5rbfgjvNc4WM6pQ4Kp5uAb2tAVDYWk
dWXtfxr5Ym3RWa3zl232VwVbuFcoHnBWdIuXE6RwEqR5ZKuZiWYMrFaGOlH6unRG
9JZNTd5uBQIDAQABo4HyMIHvMA4GA1UdDwEB/wQEAwIBBjBMBgNVHR8ERTBDMEGg
P6A9hjtodHRwOi8vY3JsLnVuaXZlcnNpZ24uZXUvdW5pdmVyc2lnbl9wcmltYXJ5
X2NhX2hhcmR3YXJlLmNybDAdBgNVHQ4EFgQUPkL8EdFADAnQOkzvqztMVxU6qw0w
OwYDVR0gBDQwMjAwBgRVHSAAMCgwJgYIKwYBBQUHAgEWGmh0dHA6Ly9kb2NzLnVu
aXZlcnNpZ24uZXUvMBIGA1UdEwEB/wQIMAYBAf8CAQAwHwYDVR0jBBgwFoAUTdn8
qC3HyFqkrV9Jrmik3J6KEiIwDQYJKoZIhvcNAQELBQADggEBAAJmra93c7GG+LCB
64bfqEONXydN/cLIh3pzJdaRzxfrBLOYyGeR15hmwuCtEIqG1naUfVjCC9QPK8jd
gVGng3ILVDH+2ZKtbiPPW7uJMjf3xIPm2KnTfgJYAMj984VaH+X+pXUssjoI3xad
J1/1NwmT3tMBZoQ8bNRuXXvMzNv4CMG0x1GTR5/cU00tWovFJPfc9CIIsL4ZG++Z
YN1SlqXAxcW52BnPJBtvGpeiUBt5vI2Rg8YMACdwGHgu1u+617GeKZrMlZdtuapg
HAerXtAwbjZN5YXrNQ9Ougd7eBypNeKyzxvHe38STrJ7rFEsav8EthV92XUQKDAe
```

fv64qqM=
-----END CERTIFICATE-----

Belgian Mobile ID SA/NV

Service provider trade name	VATBE-0541659084
Information URI	https://www.itsme.be/legal/document-repository
Service provider street address	Sinter-Goedeleplein 5
Service provider postal code	1000
Service provider locality	Brussel
Service provider country	BE

itsme Sign Validation

Type	QESValidation/Q
Status	granted
Status starting time	2018-09-12T00:00:00.000Z

Service digital identity (X509)

Version	3
Serial number	595659758488486612421071900640167610102289542121
Signature algorithm	SHA256withRSA
Issuer	CN=QuoVadis Belgium Issuing CA G2, O=QuoVadis Trustlink BVBA, OID.2.5.4.97=NTRBE-0537698318, C=BE
Valid from	Wed May 23 08:14:29 UTC 2018
Valid to	Sun May 23 08:24:00 UTC 2021
Subject	CN=itsme Sign Validation Service, O=Belgian Mobile ID, OID.2.5.4.97=NTRBE-0541659084, C=BE
Public key	Sun RSA public key, 2048 bits modulus: 24042985253419460845608706676127477354171692694704811249127925515135912261895969830768156599797472218908209770913785996594858943324977374211076321250415069913923581889120958125051774067628778859373226922500228869985258833257032879388459344278480970450219249938718602538349068924960120931613403200903198561274994300148263009329937414224787080368718526603055697632323765912341922569808655187743369207171481322294902854177650749645056678834957046898383892072644395448844075923079357793671956486297603342926850683073947338041981892327513462860511688735203356746879407863908700665249631726025678432189576265938134944564251 public exponent: 65537
Subject key identifier	e276edb08270e286e783a26d479f777c40cd082b
CRL distribution points	http://crl.quovadisglobal.com/qvbecag2.crl
Authority key identifier	87c9bc3197127a73bb7ec03d4551b401259551ab
Key usage	nonRepudiation
Basic constraints	CA=false
SHA1 Thumbprint	24a8f49699a6ddfe4170de8cb00b8e69a452a366

SHA256 Thumbprint 16722a5e323b14c47439683ae5f5d0ad077ba8bac0f68c6b5fcee49f5f91b74f

Extension (critical: true)

Additional service information

ForeSignatures

Extension (critical: true)

Additional service information

ForeSeals

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=itsme Sign Validation Service, O=Belgian Mobile ID, OID.2.5.4.97=NTRBE-0541659084, C=BE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
24042985253419460845608706676127477354171692694704811249127925515135912261895969830768156599797472218908209770913785996594858943324977374211076321250415069913923581889120958
12505177406762877885937322692250022886998525883325703287938845934427848097045021924993871860253834906892496012093161340320090319856127499430014826300932993741422478708036871
85266030556976322327659123419225698086551877433692071714813222949028541776507496450566788349570468983838920726443954488440759230793577936719564862976033429268506830739473380
41981892327513462860511688735203356746879407863908700665249631726025678432189576265938134944564251
 public exponent: 65537
 Validity: [From: Wed May 23 08:14:29 UTC 2018,
             To: Sun May 23 08:24:00 UTC 2021]
 Issuer: CN=QuoVadis Belgium Issuing CA G2, O=QuoVadis Trustlink BVBA, OID.2.5.4.97=NTRBE-0537698318, C=BE
 SerialNumber: [    68564eae c9d8893c a1e5a792 6d9199d3 533c2be9]

Certificate Extensions: 10
[1]: ObjectId: 1.2.840.113583.1.1.9.1 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 26 30 24 02 01 01 86   1F 68 74 74 70 3A 2F 2F  .&0$.....http://
0010: 74 73 2E 71 75 6F 76 61   64 69 73 67 6C 6F 62 61  ts.quovadisgloba
0020: 6C 2E 63 6F 6D 2F 62 65                            l.com/be


[2]: ObjectId: 1.2.840.113583.1.1.9.2 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 05 30 03 02 01 01                               ..0....


[3]: ObjectId: 1.3.6.1.5.5.7.1.3 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 75 30 73 30 15 06 08   2B 06 01 05 05 07 0B 02  .u0s0...+.......
0010: 30 09 06 07 04 00 8B EC   49 01 02 30 08 06 06 04  0.......I..0....
0020: 00 8E 46 01 01 30 13 06   06 04 00 8E 46 01 06 30  ..F..0......F..0
0030: 09 06 07 04 00 8E 46 01   06 02 30 3B 06 06 04 00  ......F...0;....
0040: 8E 46 01 05 30 31 30 2F   16 29 68 74 74 70 73 3A  .F..010/.)https:
0050: 2F 2F 77 77 77 2E 71 75   6F 76 61 64 69 73 67 6C  //www.quovadisgl
0060: 6F 62 61 6C 2E 63 6F 6D   2F 72 65 70 6F 73 69 74  obal.com/reposit
0070: 6F 72 79 13 02 65 6E                               ory..en


[4]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://trust.quovadisglobal.com/qvbecag2.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://uw.ocsp.quovadisglobal.com]
]

[5]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 87 C9 BC 31 97 12 7A 73   BB 7E C0 3D 45 51 B4 01  ...1..zs...=EQ..
0010: 25 95 51 AB                                        %.Q.
]

]

[6]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.quovadisglobal.com/qvbecag2.crl]
]]

[7]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.8024.1.450]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 28 68 74 74 70 3A 2F   2F 77 77 77 2E 71 75 6F  .(http://www.quo
0010: 76 61 64 69 73 67 6C 6F   62 61 6C 2E 63 6F 6D 2F  vadisglobal.com/
```

```
0020: 72 65 70 6F 73 69 74 6F   72 79                    repository

]]  ]
 [CertificatePolicyId: [0.4.0.194112.1.1]
[]  ]
]

[8]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 emailProtection
 1.3.6.1.4.1.311.10.3.12
]

[9]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Non_repudiation
]

[10]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E2 76 ED B0 82 70 E2 86   E7 83 A2 6D 47 9F 77 7C  .v...p.....mG.w.
0010: 40 CD 08 2B                                        @..+
]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 86 6C 54 D7 F0 F8 26 AA   04 09 68 23 AA F9 42 F1  .lT...&...h#..B.
0010: 0A C2 1A FE ED D5 10 58   C0 FD D3 1F 6A 5C B1 35  .......X....j\.5
0020: 1C B4 13 0E 79 05 45 91   C7 79 8E A6 8D 68 C4 35  ....y.E..y...h.5
0030: D7 8C 8D 3D 61 64 42 CC   72 6C 63 A3 67 38 C0 F8  ...=adB.rlc.g8..
0040: 28 61 8F 5E E3 1F A9 F6   BE BE D2 93 D3 8F C4 4F  (a.^...........O
0050: 90 9B EE 80 3E F1 85 3C   C1 FB 7B 76 4D 01 01 D6  ....>..<...vM...
0060: 07 B7 13 74 D5 F1 68 73   AF A0 D7 2A 0C 84 DD B9  ...t..hs...*....
0070: 55 C4 18 02 5C 4C CB 88   0C A5 F4 29 34 5A 85 72  U...\L.....)4Z.r
0080: 1D E7 8B 74 F3 DC 62 32   13 7C C8 48 BF 59 82 AA  ...t..b2...H.Y..
0090: BB 33 95 85 34 6C 85 63   00 2B B1 6A CA 2B AD 72  .3..4l.c.+.j.+.r
00A0: F6 7B 2F 3A 57 7C F2 16   BA 7C C5 81 80 D1 32 FB  ../:W.........2.
00B0: C3 06 AF 8A C1 25 B7 F4   DB D4 2F CC 83 F7 D1 94  .....%..../.....
00C0: 6F D7 87 99 2C 80 F2 84   D7 8E 45 CB 40 27 E8 45  o...,.....E.@'.E
00D0: E6 52 93 1C 3B 59 8B 9F   4B CC 9D 3F 1D F3 02 52  .R..;Y..K..?...R
00E0: EE F0 EB 1C 07 39 39 DF   B0 0D 9E AA 57 AD E9 D6  .....99.....W...
00F0: F0 6F 51 89 4E 8A 6A A5   9F 76 49 F9 F9 64 42 6E  .oQ.N.j..vI..dBn
0100: BD 4A DA 79 92 C2 BE 33   77 F1 4A 49 F2 10 D0 69  .J.y...3w.JI...i
0110: EB 78 A0 01 B8 A5 74 DD   87 A9 1D F4 AC 6E ED 93  .x....t......n..
0120: BD E6 4E 50 B6 31 69 A0   DC B9 05 A1 B6 18 2F 48  ..NP.1i......./H
0130: 6E 86 5F 99 D1 3E 46 88   92 DD 7B AC DE 0B 73 F0  n._..>F.......s.
0140: B2 08 47 F5 AE 5B E9 7B   3D 03 06 02 37 C8 45 FF  ..G..[..=...7.E.
0150: C7 09 F2 FC 9A 05 51 38   0D 02 F1 5D EB EC F0 94  ......Q8...]....
0160: AC E0 33 F1 A6 A8 6F 2B   CF DA 9B DD 0A 28 9B 97  ..3...o+.....(..
0170: A4 24 0D 81 EF 9E 44 2F   C6 E7 62 38 38 D7 66 87  .$....D/..b88.f.
0180: 6A CF 1A 63 06 B1 20 06   0E E5 D4 BD 24 61 B7 2E  j..c.. .....$a..
0190: 5D AD FE 35 6B 32 4E 6D   71 CF 34 CD 78 89 58 D3  ]..5k2Nmq.4.x.X.
01A0: 61 CE 67 A7 5F 07 D1 D5   84 AC 93 81 B5 67 11 A6  a.g._........g..
01B0: AB 5F BD D5 82 A3 16 20   FB 13 6D 5C C1 1C 6A 5A  ._..... ..m\..jZ
01C0: 35 31 54 24 8E F0 08 42   5F E9 4E C0 AD 5C 8C 2F  51T$...B_.N..\./
01D0: 56 89 78 E3 6D 54 B0 F6   08 CC 5C E5 0C 1D C1 0B  V.x.mT....\.....
01E0: 69 5D EE F2 E9 79 86 2B   C9 92 6D 2D B7 3E A8 79  i]...y.+..m-.>.y
01F0: F1 C9 DF 32 FF 59 7C 79   7C 3E 1B D2 75 55 F8 C1  ...2.Y.y.>..uU..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGxTCCBK2gAwIBAgIUaFZOrsnYiTyh5aeSbZGZ01M8K+kwDQYJKoZIhvcNAQEL
BQAwczELMAkGA1UEBhMCQkUxGTAXBgNVBGEMEE5UUkJFLTA1Mzc2OTgzMTgxIDAe
BgNVBAoMF1F1b1ZhZGlzIFRydXN0bGluayBCVkJBMScwJQYDVQQDDB5RdW9WYWRp
cyBCZWxnaXVtIElzc3VpbmcgQ0EgRzIwHhcNMTgwNTIzMDgxNDI5WhcNMjEwNTIz
MDgyNDAwWjBsMQswCQYDVQQGEwJCRTEZMBcGA1UEYQwQTlRSQkUtMDU0MTY1OTA4
NDEaMBgGA1UECgwRQmVsZ2lhbiBNb2JpbGUgSUQxJjAkBgNVBAMMHWl0c21lIFNp
Z24gVmFsaWRhdGlvbiBTZXJ2aWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvnUGd+OGmt8QXoP19QSTDCkAuE1tOOfDQteF19yFw39oLHbEeCGQd+mm
7NHGLVJiuVYPV6Wzw+pJ3i60QNfqr+xrcOUeDaQLPTJFHGWHcuao/EsOSG4yXjf1
op8SlqBgs5qYdp8jXauLRonK29G0nsiZ90jPqVOyPK1DSu6+BQDSmYfaYu7lxHbV
esCuWEtMQeX5awzmLQmRgnT71AeZVdE6eYZ498CC6/Kic3UH3AWeHodlQDHQETOK
21Rfq6tusvvc2zT2fJXc7R8RYYzPkfuWnklD2kWXblDg90o8o8N3inDpkWsq/8Ri
lGWwNQHhoevdCjgWbwwyKwAbfrnEGwIDAQABo4ICVjCCAlIwdwYIKwYBBQUHAQEE
azBpMDgGCCsGAQUFBzAChixodHRwOi8vdHJ1c3QucXVvdmFkaXNnbG9iYWwuY29t
L3F2YmVjYWcyLmNydDAtBggrBgEFBQcwAYYhaHR0cDovL3V3Lm9jc3AucXVvdmFk
aXNnbG9iYWwuY29tMB0GA1UdDgQWBBTidu2wgnDihueDom1Hn3d8QM0IKzAfBgNV
HSMEGDAWgBSHybwxlxJ6c7t+wD1FUbQBJZVRqzBaBgNVHSAEUzBRMEQGCisGAQQB
vlgBg0IwNjA0BggrBgEFBQcCARYoaHR0cDovL3d3dy5xdW92YWRpc2dsb2JhbC5j
b20vcmVwb3NpdG9yeTAJBgcEAIvsQAEBMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6
Ly9jcmwucXVvdmFkaXNnbG9iYWwuY29tL3F2YmVjYWcyLmNybDAOBgNVHQ8BAf8E
BAMCBkAwHwYDVR0lBBgwFgYIKwYBBQUHAwQGCisGAQQBgjcKAwwwEwYKKoZIhvcv
AQEJAgQFMAMCAQEwNAYKKoZIhvcvAQEJAQQmMCQCAQGGH2h0dHA6Ly90cy5xdW92
YWRpc2dsb2JhbC5jb20vYmUwgYEGCCsGAQUFBwEDBHUwczAVBggrBgEFBQcLAjAJ
BgcEAIvsSQECMAgGBgQAjkYBATATBgYEAI5GAQYwCQYHBACORgEGAjA7BgYEAI5G
AQUwMTAvFilodHRwczovL3d3dy5xdW92YWRpc2dsb2JhbC5jb20vcmVwb3NpdG9y
eRMCZW4wDQYJKoZIhvcNAQELBQADggIBAIZsVNfw+CaqBAloI6r5QvEKwhr+7dUQ
WMD90x9qXLE1HLQTDnkFRZHHeY6mjWjENdeMjT1hZELMcmxjo2c4wPgoYY9e4x+p
9r6+0pPTj8RPkJvugD7xhTzB+3t2TQEB1ge3E3TV8Whzr6DXKgyE3blVxBgCXEzL
```

```
iAyl9Ck0WoVyHeeLdPPcYjITfMhIv1mCqrszlYU0bIVjACuxasorrXL2ey86V3zy
Frp8xYGA0TL7wwavisElt/Tb1C/Mg/fRlG/Xh5ksgPKE145Fy0An6EXmUpMcO1mL
n0vMnT8d8wJS7vDrHAc5Od+wDZ6qV63p1vBvUYlOimqln3ZJ+flkQm69Stp5ksK+
M3fxSknyENBp63igAbildN2HqR30rG7tk73mTlC2MWmg3LkFobYYL0huhl+Z0T5G
iJLde6zeC3PwsghH9a5b6Xs9AwYCN8hF/8cJ8vyaBVE4DQLxXevs8JSs4DPxpqhv
K8/am90KKJuXpCQNge+eRC/G52I4ONdmh2rPGmMGsSAGDuXUvSRhty5drf41azJO
bXHPNM14iVjTYc5np18H0dWErJOBtWcRpqtfvdWCoxYg+xNtXMEcalo1MVQkjvAI
Ql/pTsCtXIwvVol4421UsPYIzFzlDB3BC2ld7vLpeYYryZJtLbc+qHnxyd8y/1l8
eXw+G9J1VfjB
-----END CERTIFICATE-----
```

Trusted List Signer

Subject	C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
Issuer	C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
Not before	Wed Feb 19 13:37:52 UTC 2014
Not after	Tue Feb 11 13:37:52 UTC 2025
Serial number	12597032158223217295
Version	3
Public key SHA1 Thumbprint	8f914035f0200880afe97b0eab85b5921ea98421
Public key SHA256 Thumbprint	f7cf32405bc6553c92fec8364bf58d56b153324ad58ad6cb7aace1037d5d3e41

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
24300999668952271336930030093714651766559690911903216193281992404510245187371320819543733804448624693522397655805338290368738930744837629562942067296575129066040125015273157
93517280217865321819160740775732194727930458919922521995692540951807923171115060769731590712346286509664439160107000534884146909041751636242027382031023466107500619524409877
27283427021323280307639992049788147229043339760080834570290066311843665221921835557433177168179986865374356704032605187207885089432302544936253416592529324143468606089203473
20921304607665880177501274313091120751308363261034368874146407550848866631307165625943996664160511
 public exponent: 65537
 Validity: [From: Wed Feb 19 13:37:52 UTC 2014,
             To: Tue Feb 11 13:37:52 UTC 2025]
 Issuer: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
 SerialNumber: [    aed1a601 8711328f]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
 CA:false
 PathLen: undefined
]

[2]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 0.4.0.2231.3.0
]

[3]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
 Non_repudiation
]

[4]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5F EF 8E 69 5D FB F4 97   5A F1 07 08 0E 52 19 50  _..i]...Z....R.P
0010: AA D7 90 51                                        ...Q
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 16 9B 23 CA D4 FE 95 B8   BA 24 C7 93 8E D7 F3 7F  ..#......$......
0010: 2A 9E DC 7A 14 9E 62 0C   2B 3E 89 A1 03 D7 8D BE  *..z..b.+>......
0020: CA 3B BF C1 05 54 E0 9F   2B 8D 2E 14 AA C7 4E F3  .;...T..+.....N.
0030: 03 8C E2 C7 F2 2E 33 0B   45 1B 0A EB 4B 1A 67 9A  ......3.E...K.g.
0040: 36 BB EB 4B 22 3D 10 AC   54 72 B5 30 F5 58 8B 8F  6..K"=..Tr.0.X..
0050: 67 1A 41 8D 05 3C 66 3F   FE 68 B9 2B E1 B4 26 CA  g.A..<f?.h.+..&.
0060: A8 09 E1 7C C9 67 D0 4C   BE 2D D8 BF 5F 23 43 12  .....g.L.-.._#C.
0070: 52 8E F1 A9 5D A5 A9 50   D2 CD 9E 11 0D 4E EC CA  R...]..P.....N..
0080: BF C7 FF D2 F0 67 D8 89   E6 A6 0E DC C2 08 F6 AB  .....g..........
0090: CA A1 67 FD EB D5 99 87   11 34 83 98 47 63 57 8A  ..g......4..GcW.
```

```
00A0: 2F 62 BB 80 29 7E 7C 8F   0C 27 45 D8 1A 71 3B 60  /b..)....'E..q;`
00B0: 42 90 7C F3 EC D9 0E D0   29 DC 55 49 C5 1F 67 79  B.......).UI..gy
00C0: F0 9D BE 35 76 9E E3 7E   F9 48 00 DA FF 1D DA EF  ...5v....H......
00D0: 5C F1 CE CE 6C 67 7B 74   BE 8E F6 B4 02 7E F0 56  \...lg.t.......V
00E0: 6F 0E BF 87 D9 E4 5D 22   52 02 32 97 4B 5B AF 9C  o.....]"R.2.K[..
00F0: 00 6D AB 77 D0 69 B1 F0   C4 D7 3C AC 84 0F 90 B9  .m.w.i....<.....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIJAK7RpgGHETKPMA0GCSqGSIb3DQEBBQUAMIGHMS0wKwYD
VQQDEyRCZWxnaWFuIFRydXN0ZWQgTGlzdCBTY2hlbWUgT3BlcmF0b3IxSTBHBgNV
BAoTQEZQUyBFY29ub215LCBTTUVzLCBTZWxmLWVtcGxveWVkIGFuZCBFbmVyZ3kg
LSBRdWFsaXR5IGFuZCBTYWZldHkxCzAJBgNVBAYTAkJFMB4XDTE0MDIxOTEzMzc1
MloXDTI1MDIxMTEzMzc1MlowgYcxLTArBgNVBAMTJEJlbGdpYW4gVHJ1c3RlZCBM
aXN0IFNjaGVtZSBPcGVyYXRvcjFJMEcGA1UEChNARlBTIEVjb25vbXksIFNNRXMs
IFNlbGYtZW1wbG95ZWQgYW5kIEVuZXJneSAtIFF1YWxpdHkgYW5kIFNhZmV0eTEL
MAkGA1UEBhMCQkUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAgEFk
oDPTYDvGk+/IPnGSPm58NRE7mpzLHk8lxpYnTAtbMhn7FWru9GlNi+blYYNOEmzN
2E5KO9+7AAAMmx2x8zmEMwc3oUQ7E0WN5Gl+Y+7n6NtX50D/4Sbw4IjVvwwRRru8
Coj5vq5Hz3JKTgft8teEpwb5vSFZh6+o9irdX342RJU4AtG78sxZvzIqpa3WsddM
f5XDyjnGK3dRgkDuOaBxWEexuUiN4LvO+MacwoaxEqLhEZ6TALGWS2WmNEW3OlUd
f7nc0Tz/lnyQsuFn01c4pg56hjyxLtpjyHwNwbTDx+cjBpBveOT9Nb6UfKFHknC5
AfrIOWnFLXUmyKD/AgMBAAGjTDBKMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgbAMB0G
A1UdDgQWBBRf745pXfv0l1rxBwgOUhlQqteQUTARBgNVHSUECjAIBgYEAJE3AwAw
DQYJKoZIhvcNAQEFBQADggEBABabI8rU/pW4uiTHk47X838qntx6FJ5iDCs+iaED
142+yju/wQVU4J8rjS4UqsdO8wOM4sfyLjMLRRsK60saZ5o2u+tLIj0QrFRytTD1
WIuPZxpBjQU8Zj/+aLkr4bQmyqgJ4XzJZ9BMvi3Yv18jQxJSjvGpXaWpUNLNnhEN
TuzKv8f/0vBn2Inmpg7cwgj2q8qhZ/3r1ZmHETSDmEdjV4ovYruAKX58jwwnRdga
cTtgQpB88+zZDtAp3FVJxR9nefCdvjV2nuN++UgA2v8d2u9c8c7ObGd7dL6O9rQC
fvBWbw6/h9nkXSJSAjKXS1uvnABtq3fQabHwxNc8rIQPkLk=
-----END CERTIFICATE-----
```

The public key in PEM format:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwIBBZKAz02A7xpPvyD5x
kj5ufDURO5qcyx5PJcaWJ0wLWzIZ+xVq7vRpTYvm5WGDThJszdhOSjvfuwAADJsd
sfM5hDMHN6FEOxNFjeRpfmPu5+jbV+dA/+Em8OCI1b8MEUa7vAqI+b6uR89ySk4H
7fLXhKcG+b0hWYevqPYq3V9+NkSVOALRu/LMWb8yKqWt1rHXTH+Vw8o5xit3UYJA
7jmgcVhHsblIjeC7zvjGnMKGsRKi4RGekwCxlktlpjRFtzpVHX+53NE8/5Z8kLLh
Z9NXOKYOeoY8sS7aY8h8DcG0w8fnIwaQb3jk/TW+lHyhR5JwuQH6yDlpxS11Jsig
/wIDAQAB
-----END PUBLIC KEY-----
```