

# 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* 2018-02-08T00:00:00.000Z

*Next update* 2018-07-30T00:00:00.000Z

*Historical information period* 65535 days

*Sequence number* 36

*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*Status* withdrawn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* 117029288888937864350596520176844645968

*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:  
2532727247174242475310876111302551541350771290487408393990707355  
3139389403581555633427000903307438065008396155423372038139338001  
1292283973874375661691461475691011321537351475763725785500152445  
9884908283374968661826239871065222401938973133495715806769163244  
2561241462450868417538609485432931629806056877222374520561111218  
9904505418533484099385023144445138975351025575749503679547226381  
0313002138087279503333496722494200200493483881237347138441152657  
9026650775354589375802255665011941485467556333747329602589496041  
6159860774175448506963241118776049541934983183035608916277217984  
30948172071644141969017225065301229219951  
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
444451389753510255757495036795472263810313002138008727950333349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
774175448506963241118776049541934983183035608916277217984309481720716444141969017225065301229219951
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]

```

---

## Belgique/België (Belgium): Trusted List

---

```
[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 .l.\....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 l.`.....HuT...
00A0: 1B AD 77 9C E8 B2 8F DB 83 AC 8F 34 68 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+eWmUDANBqkqkhiG9w0BAQUFADAN
M0swcQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ21lLmB5S290IENBMB4XDTAzMDUy
NjIzMDAwMFoXDTE0MDEyMjIzMDAwMFowZELMAkGA1UEBhMCkUuGDAWBgNVBAMT
D0JlbgdwdW0gUm9vdCBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMi.hcekCRKJ5eHFvna6pqqKsot03HIOswkVp19eLSz8hMFJhCwK3HEcVAQGa+X0S
J4fpn0VxTiIIs0RIYqjBeoiG52bv/9nTrMQHn035YSEWtXaJqAFPrSjmcPpLHZXB
MFjqvNlL2Jq0i0tJrLLf0lMVdssUXRLJsw9q09P9vMI7EU/CT9YvzvU7wCMgTVy
v/cY6pZ1f5sofxVsY9LKyn0FmMtB20yvmi4BUcuJhWpmbxM0jvxKuTXgfeMo8S
dKpbNCNUwOpszv42kqgJF+qhLc9s44Qd3ocuMws8d0IhUDiVLlZg5cYx+dtA+mqh
pIqTm6chBocdJ9PEocLmsG8CAwEAAa0BuzCBuDA0BgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAEOzA5MDCGBWA4AQEBMCAwLAYIKwYBBQUHAGew
IGh0dHA6Ly9yZXBvc2l0b3J3JmVpZC51ZWxnaXVtLmJlMB0GA1UdDgQWBQ08Axw
m2HqVzq2Nzdt925F17b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth61c6tjWxbZ/diurS02+YwDQYJKoZIhvcNAQEFBQADggEBAMhtILGKYfgP
lm7VILKB+MbcoxYA2s1q52sq+llIp0xJN9dzoWbZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0A1M1w3EbV1jZKE4tRfTa57VjRU0RD5p/
M3825bT0bqkCMA5c/ciJv0J71/Fg8teH9Lcuen5qE4Ad30PQYx49cTGxYNSeCMqr
8JTHSHVUgFmbrXec6lKP240sjzRr6L/D2fVDw2RV6x9NoY2u1GMLxoh10ot06y6
7Kcdq765Sp1LxxCHVGNHITtEpf/8m6HFubJdNbv6z1951luBpQE5KJVhzgoaiJe
4r50ErAE0yo=
-----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:  
2505202035897286929802442931365977782136110157856742564234839581  
6436795380283967224876983130034020316820575216355360416605004533  
4718830407023741150537135469000352360279650474826843696574001315  
5524363953296559605768293726462748683867807979476223046936921095  
0088797578757728341339292333654654510981797643030670179357915156  
5262158435123606358334230710497624432217765218126527057253528859  
3688668361490384043063624052887014382463758810568004079588144865  
4643858460532713400822409146679502714797245542101554942867836639  
3080491585356622044306227220916440412947986826263456222477031966  
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
4826843696574001315524363953296559605768293726462748683867807979476223046936921095008879757875772834133929233365465451098179764303067017935791515652621584351236063583342307
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
]
```

## Belgique/België (Belgium): Trusted List

```
]

[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 50 94 58 D1 CF 11 72 B6 1E B9 39 41 ..c+).X...r...9A
0050: 16 40 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-----
MIIDjjCCAnagAwIBAgIIVKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMakGA1UE
BHMCOkUxGTAxBG9NBAMTEEEJLbGdpdW0gUm9vCBDDQTIwHhcNMDCxMDA0MTA0MDAw
WhcNMjExMDgwMDAwMjE0MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
bSBSb290IENBMjCCASIdDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi790hqC/7bIYLS2X+an7mEoj39WN4IzGMhwLQdC1i22bi+n9fzGhYJdld61
IgdMqFNA68KNaJ6x+HK92AQZw6nUHMxU5wfIp8MXW+2QbyM69odRr2nLL/zGsvU
+400HjPILtfsjFPekx40Hop0cSZYf3CiInaYnkJIT/e1wEYnm7hLHADBGXvmAYr
XR5i3FVr/mZkIV/4L+HXmymvb82fqqxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y
HewApDgg1VrH1Tdjuk+bqv5WR15j2Qsj1Yr6tSPwiRuhFA0m2khw0I8w7QUmecFL
TqG4f1V50mLGHUCAwEAa0BuzCBuDA0BgNVHQ8BAF8EBAMCAQYwDwYDR0TAQH/
BAUwAwEB/zBCBgNVHSAE0zA5MdcGBWA4COEBMCAwLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC51ZWxnaXVtLmJlM0GA1UdDgQWBBSFiuuv0xbu+dLk0
LN7WgAEV4xcccOTARBg1ghkgBhvCAQEEBAMCAAcwHwYDR0jBBgwFoAUHyrr9MMW
vg5ZA5Te1oABFeM0NdKwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyCc
UwnzSgEMdL8rs5qauhjyC4isHLMzr87LEwEnkoRYmhCS98wUkmt0F0qW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTLBFk0pvDVTc9rejj7NqZV3JcqUwumyaa7YwB0+mPyW
nIR/VRPmPIfjvCCKpDZoa01gZhz5v6yALGYuuUGK02ThIAC71AdXkbc98m6tTR8
KvPG2F9fJ3bTc0R5/0UA0NmXsImABKgX770FP67H6d96tK8QYUn8pJQsKpv02F
sauB0eYxUjU4c5nUwFAA4+Bw11V0S0U7Q2dmS23G7rPUZuFF1eR10NeE3gJ7u0
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:  
6892368425204007372930073294443554123229459767731895868437789352  
7489331012499470148015728120971091408928778599011263917331397388  
7322735841404218927092481342245128960306942910996978037963366658  
7487677438166762048712847334427499268969797276699412687279269161  
8545497053924331052069875135564437218371995289927129772075947532  
4004770387044092331280439040222928977901876514295420628487235605  
7207547181546555365474067211993745122880348947938978158987337436  
1336080842299846657331444909264877243429847318212868757946477794  
3923944626874903980284954943444633165097044418808053302806567480  
3973101653181735709840274950639311977298375764568509245075873047  
9725560212981580096389424844703793712327092036866308035191942506  
8313464980278629369152701697759736384202776541620591588545291932  
4663214995529533375563259732378154805928106136809503809799800229  
2920617503904475332163393814047794956959421382197572947310250836  
6454723047943333937457964148701121644586439773493445613256431505  
4516896008070464718986221218972698235178969696880747332055597346  
5056144482367929251906090063565458141797098055228581790278906951  
4772158596504768735853434600634865427052445967408799471479389419  
0325164983453802445254424012949618662017893008747941892318218022  
78084190173776931  
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:
68923684252040073729300732944435541232294597677318958684377893527489331012499470148015728120971091408928778599011263917331397388732273584140421892709248134224512896030694291
09969780379633666587487677438166762048712847334427499268969797276699412687279269161854549705392433105206987513556443721837199528992712977207594753240047703870440923312804390
40222928977901876514295420628487235605720754718154655536547406721199374512288034894793897815898733743613360808422998466573314449092648772434298473182128687579464777943923944
62687490398028495494344463316509704441880805330280656748039731016531817357098402749506393119772983757645685092450758730479725560212981580096389424844703793712327092036866308
0351919425068313464980278629369152701697759736384202776541620591588545291932466321499552953375563259732378154805928106136809503809799800229292061750390447533216339381404779
49569594213821975729473102508366454723047943333937457964148701121644586439773493445613256431505451689600807046471898622121897269823517896969688074733205559734650561444823679
2925190609006356545814179709805522858179027890695147721585965047687358534346006348654270524459674087994714793894190325164983453802445244240129496186620178930087479418923182
1802278084190173776931
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 ...[...%.....@
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 ...[...%.....@
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 '...+...S.'.....
0040: 54 CB 32 68 23 7D B1 CC B8 A6 12 D7 D6 A4 F8 F2 T.2h#.....
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 .q.c.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 ...>..0....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 .0>...;...xzwv...
0100: 39 F7 1E C8 F5 1A 56 45 A2 5C 5E 9C 34 0B EF 90 9.....\..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...].
0140: 39 79 1D 07 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 08 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 .1.0.....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-----
MIIFjjCCA3agAwIBAglI0yEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BHMCCkxkGTAxBG9NBWAMTEEEJLbGpdwQ0Um9vdbCDDQTMwHhcNMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwMjA0MQswCQYDVQQGEWJCRTEZMBCGAIUEAxMQQmVsZ211
bSB5b290IENBMzCCAIwDQYJKoZIhvcNAQEBBQADAgIPADCCAgCggIBAKjYAZ2L
g8KH0IX7JLc3BeZ1Tzy9MEv7Bnr59xcJezc/xJJd04V3bwM1tKFfNvqsQ5H/GQAD
FJ0GmTLPLD15AoeUjBubRZ9hwrUuQ11+vhtoVhuEuZuxofEUIU2yJti500Nwpo/G
Ib9C4YZSh+71tDpC3MvsFyyordpZgwgShvFWtCmL55SpU05Ubf7ZVPcfVf24A5IG
HLpZTgQfAvnzPlm++eJY+sNoNzTBoe6iZphmPbxuPncJ6sLV8MQQK50/g+KmoPp
HX4AvoTr4/7TMTvuK8j51dEn+fdvKdx9qo9ZZRHFW/TXEn55rNUu99xhzLE/wBur
rVwFoKcWcjm00CnekJlw0NTr3HBTG5D4A1dJNFUYaIcGJK/ha9rzHzY+WpGdoFZx
hbP83ZGeoqkgBr8Uzf0FCY8cyUN2db6hpIak6Nuoho60Wnn+TSNh5Hju5i5mqGx
S73gYLTQww16h8gFTJQ49fiS+QHLwRw5cqFuqfLE3nFFF9KIam54TSe7T4dNGY
2VhZpaGVT4wy+fL7gWsfauKvM4b00DzgdIj9BHiKytNLMzoa3Snejj/Ckur0dJ
50dMiAqUpSd00e8pdIbmQm1oP5cjk1Qjxx7+vSxWtaccGowWK8+7oEsYc+7fL7L3
GD6q/05xi440Pd/sFmfqRf3C1PPMdBqXcwgAgMBAAGjgbswgbgwgDgYDVR0PAAQ/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVwA0BATAUwCwG
CCsGAQUFBwIBFIBodHRwOi8vcmlvb3NpdG9yeS51awQumVsZ211b55iZTAdBgNV
HQ4EFgQUuLxsA19bGYWdJQgC8BncQ1700CswEQYJYIZIAyB40gEBBAQDAgAHMB8G
A1UdIwQYBAAFLi8bACPWxmFnsUBnPAZ3EC00DgrMA0GCsG5Ib3DQEBBQUAA4IC
AQBFIjv/mKX+VcyxEacckgx4L8XvFKIFPXzjEnDnAtCCKR0U/k5n1jJVk+0D0n+Q
4kJg6Nd7K47+zTXcrSe1tB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpdl
f14HcUPCYLA5TCapZU0MnAbzfpzxm49Ik/A2JWxhXVRHw0u3TMG1Q4W/VyVawx
jwQM08TneBDombmkXsI9bI00xWUj2A5dKlqu0sYvE0dz8xDr9ZkmZqYcPIKiZCZ
laP1zS5Lc15531gn3EUP+fd21q6ZxgU+50/qgoH/0UuaHRpedPQ8ES/FYc2IQZ2X
jhmeTmW+9Lk7tnzHeHp3dgCo0fceyPUaVkwjWmWcNvkvDVELvXfJpRxcwRf55Ks
5oaF0fj81RzGUbmpwL2us0eCRwdWE8PvbFwNQC8MjqudL5HdeuzUesTXUqXeEk
yAO06YnF3g0qGcL19NXusji1egRUZ7B4XCvG52LTB7Wgd/wVFzS3f4mAmYTGJXH+
N/LrBBGKuTJ5XncJa1iFUKxGP6VmYaaLUF5ILTqC9CGHPLSX0gDokt2G9pNwFm2
t7AcPwAmegkMnpgcgTd+qk2YlEaT8wF953jUAFedpbN3tX/3i+uvH00mWj00xJg
2LVKkC+bkWaZFTBDdrLEWValrY+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:  
  6224115906824122031433393414467734255795749661242697041972796971  
  35225688053118958013272845856830766072936328678029599339864160757582078179782933477127775842726474054125659177491124497441056063625089004297867088236553695896006649963591692  
  69749224840725363125898523192670130240309448199566397525648798859959407975137564912472231555839895845986255776615614957078778639852690834243820196276106693555767675903287437
```

# Belgique/België (Belgium): Trusted List

08696354187918592365002904651508327891796764752123759700977230597799879313143129461389580095293270697956397428505408544811668100588053087190204290004659595000540204476361567  
14037428738455575723877961368298352376365721570569303418873173950417240771532738123406566311692859096140881485975714355900153034684151459890488513829961286599139575571516281  
5883415449288903178308408884400931018214236597980739606621031947075945003910750853619537707761075688418384343286045715157573426989301124463242723093299927147162988283928766  
9470136254804268113710329345462526205188173283210487963726401739856529209022485509644653939372313531324401301548679250447113282490313681633904774540734021408220407819396313  
3511429055306278731837  
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 58 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 8B E9 A.Dx..D/>\$.S.....  
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 0..&..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... Q  
0140: E1 63 11 1D FD F2 25 EA A4 3A 53 F0 1C 8C 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 l.,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...

1

*The certificate in PEM format:*

-----BEGIN CERTIFICATE-----
MIIFjjCCAgAwIBAgIITzGjMjMwUvzgwDQYJKoZIhvcNAQELBQAwKDELMAkGA1UE
BHMCMQKUGTAXBgNVBAMTEEJlbgdwdW0gUm9vdCBDQ0QwHhcnMTMwNjI2MTIwMDAw
WhcNMzIxMDYyMTIwMDAwWjAoMQswCQYDVQ0GEwJCRTEZMBcGA1UEAxMQQmVsZ21l
bSB5b290IENBNDCCAIiwDQYJKoZIhvcNAQEBBQADggIPADCCAgOAgCgGIBAJiQrvrH
Hm+04AU6syN4TNH9L1PFsY6E9euwVmL5NAWtdw9p2mcmEYOYGx424jFLpSQVnxx
xoh3LsIpdWUMRQfuiDqzvZx/4dCBaeKL/AMRJuL1d6wU73XKSkd0r5uH6H2Yf19z
SiU0m2x4k3aNLyT+VryF11b1Prp67CBk630BmG0WUaB+ExtBHOkfPaHRFA04Mig
oVfT3gLQRgh1V+H1rm1hydTzd6zppoJHp3ujWD4r4kLCrxVfV0QZ44usvAPLhKoe
cF0feiktegS1pS+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7Mmpf8MEyGx
WMb+WrynTetWnIV6jTzZAIrmaZuqmIMDvMTA7JNkiDJQ0JBWQ3Ehp+Vn7Li1MCIj
XLEDYJ2wRmcRZQ0bsUzaM/V3p+Q+j853osma3Pc6+dDzxL+Og/LnRnLdDapXx28X
B9urUR5H030zm77B9/mYgIeM8Y1XntLCELEBeuJeEYJUqc0FsGxWnwjsBtRoZ4dv
a1rvzKxMjJuNIR4YILg8G4kKlhr9JDrtYckvI9Xm8GDjQIJJ2KpQIjHBLJA0gKxL
Yem8CS0/an3A0xqTNzjWbQx6E320PB/rsu28ldadi9c8yeRyXLWpUF4Ghjyoc40d
rAkXmLjnkzLMC459xGL8gj6Lynb6UzX0eYA9AgMBAAGjgbswbgwDgYDR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQDYDR0gBDSwOTA3BgVgOAwBATAuMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmlvb3NpdG9yeS51aWQ0YmVsZ21lbn55iZTAaBgNV
HQ4EFgQUZ+JxTk+ztfMhwiCdIPZetLb50kwEQYJYIZIAyb40gEBBAQDAgAHMB8G
A1UdIwQYBAAFGfo8U5Ps7XzB28InAyD2XrZw+dJMA0GCSqGSIb3DQEBCwUAA4IC
AQBe3CAZrNwZ9L3nFwkaKdVmw0E2s1NysTfocUwyd6c01qs5N52BhRqpaSEW
LeSXAfP0K+f57M1hXLNVE8VMf1Vtc0ge+VgjKOWLj+4d0CAk8VIAK55NukrSbu4p
n+osfD/He0jFEckYq9xrhbna4yxZ/d5qj8RSj+aPmCoX/ka0DZmug+AfzY+TXeJgJ
n8eEQG08zDJoV/hduUotkF8eQXeuRhoCuvipBm7vHqEA946NuVtRumaztLUR9Ckb
SZ1pLWmqKC+QKERwzvBeswrWzaRow9Un7qCSm109ddkEHRHibkUQvPn8kgdG/
u0mmR0sbjFuARNCMwS4nHc6TTw7dJgkeZjZ1qPL22i fswJsr/vuJMA4kSot/h6
qQV9Egl04C1R1Ek3ybkKcJkLk6LA90/u46Ksq5CSMgUeFjER398iXqpDpT8BzI
MovMzHLK7pxTJA5cWXN2a80MhYCA/Kb6dqIXIi8NksqzVMXJfX65DM2gWA8rjicJ
WoooolhUKuZ6tSWA6I f2TRr7MfQsVDhwWUk6mvEiaBjBcy0WH8XgyY6uuHuvGe8C
K+Yk4X2TiE+7GuQe4YVJ/MOGdS3V1eZwPmWSu++a00FtwoZpIPK0wjbsuLbs0x
t6BwWw2XFP025BDh/OD6UE4VsyZnnUckb4Ab5947UX6NGA==
-----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:
2058370808117806886719567856147320061945292190592796129179327367
1328005822028265845465542836756717140506081882114668638826442932
4840744781703307017746497136667158332106505285154357277431791645
6871430942741492265542773700746837231916763966290548158739950199
2029174676515494584699514099891322542890739713299134792579834056
6654074619687706565029583663340264770269856720101489447350341548
9667917131633966990337885540161539197154038478640639231113106791
3663589486493118066042504737642498346914368670309047269922309076
6138772412256664686136790625895780242652401177074998149327839849
23682396679386042809154363424543342942381
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://cdpl.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 .shttps://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.....

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIELTCCAxiGwAwIBAgICA4gwDQYKozIhvcNAQELBQAwXDELMAKGA1UEBHMCMVVMx
GTAXBgNVBAoMEFZlcm16b24gQnVzaW5lc3MxETAPBgNVBAsMCE9tbnlsb290MR8H
QYDVQQDBDBZWZjcm9uIEEdsb2JhbCBSb290IENBMB4XDTEyMDUxMTE5NDUwN1oX
DTIyMDUxMTE5NDUwN1oXELMAKGA1UEBHMCMVVMxGTAXBgNVBAoMEFZlcm16b24g
QnVzaW5lc3MxETAPBgNVBAsMCE9tbnlsb290MR8HQAQwIjANBgkqhkiG9w0BAQFA
FAAQCAQ8AMIIBCgKC
AQEAow3rmuZKZMnGhQRGeEzK4THeq59CIqK6BseSxLmZ3sh8znY0FBNK40XmFEj
0Y99QnIYAxnU5bcvS5BFQKpwtD5cFcmP7BR0i6/MyJCE6BMD8wcS61CJfLtm
8/p/VRf9KsdFaf6fMd/Wlghbq780wa22+UgXpFr27eqBCsUzEiZya5cILWXM0hmP+
ZE30i7pLZ/Dh+50tn/R+P0IVBBiYpIycnx/u4Q/loEqMyy+DFliuMfCbCpE2Pbwz
0R+SCqLfnER09d1fmJ5XlpSr5K7dKXJP8Dg0Mw8Cu5fGLU8z2qqqx+3Zv0XdDNF
e2g8HX4wdMymhSzbmLjGVYrQIDAQABo4HyMIHvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwRQYDVRR0gBD4wPDA6BgRVHSAAMDImAYIKwYBBQUHAgEwJGh0dHBz0i8vd3d3
LmNlcnRpcG9zdC5jb29vc2hvvd3BvbG1jeTA0BgNVHQ8BAF8EBAMCAQYwHwYDVR0j
BBgwFoAUAUTDgRuJgAw1orrcD6qe0TVZ2dnp34w0gYDVR0fBDswOTA3oDwgM4Yxahr0
cDovL2NkcDEucHVi1bG1jLXRydXN0LmNvbS59DUkwvT21uaXJvb3QyMDM0LmNybDA0
BgnVH04EFgQUUDjczxyhu85f51rmmJCLrMhmKEQwDQYKozIhvcNAQELBQADggEg
AHPwVwcH8zTeSFMePggIMwdsVUnSdYVUkvKAGRYGxdF0EDUyMawL+I1LD21mSxVM
KJSEdVes0JlqERGoHcM9jigquuN0hg04SGsWyyWxwLatIMfp2D7FsiNrTcry3y
h2v5fxZ3Cyv7o2ZSS+pEvFhvuFqdZULgZ64/RhPcqlZV74asJuNBRZ756IF3PxxzA
KDN9Ytp8vJwLcs1RoS/0CJ/6aJ58HjBc863Rj39SscL/zZW+KanvLvDafCCJ/FN
uaA80VYjHMHsnk1ZjFwBwLpibJNzIvr2UoSkR5c8ln60eYCRpeIreXkntSopr6Mn
ciipCX0bk6c/4EiPnrWiyvg=
-----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 4835703278459639067624485
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:  
2198165027276639742335246370299919491834299685174947076499863829  
7101984511083629850948734739259892644517804066934196324549964291  
3192950780187748886826305662589231481198165241013890789999605732  
7037799082855868763511239453871155320357733059447691386874174245  
6351418525550214828297591584323227847019805029382183516476456072  
1350350984913304723496042939229874921930931967750335049019790482  
8017572130561815887751919653650932481620948873902322540903538293  
2017480465444929903218227769334668958530404811571842689601047281  
9175682817566553198501338089830997047280971197474917236039149732  
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:
    21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524101389078999960573270377990828558687635112394538711553203577330594476913868741742456351418525550214828297591584323227847019805029382183516476456072135035098491330472349604293922987492193093196775033504901979048280175721305618158877519196536509324816209488739023225409035382932017480465444929903218227769334668958530404811571842689601047281917568281756655319850133808983099704728097119747491723603914973200214236187812432050305807187505398614653
    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 [
```

# Belgique/België (Belgium): Trusted List

```
[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.Q0..d...s...Fx
0020: BF 3B 85 86 E2 3D 4A 18 94 2A 81 77 6F 82 F8 6F ;...=J...*.w.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 B8 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-----
MIID3jCCAsagAwIBAgILBAAAAAABBVJKxClUwDQYJKoZIhvcNAQEFBQAwXDELMAkG
A1UEBHMCCkUxHDAaBgNVBAoTE0NlcnRpcG9zdCBzLmEuL24ud14xLzAtBgNVBAMT
JkNlcnRpcG9zdCBFLVRydXN0IFByaW1hcnkgUXVhbGlmawVklENBMB4XDTA1MDcy
NjEwMDAwMFoXDTEwMDcyNjEwMDAwMFoXDELMAkG1UEBHMCCkUxHDAaBgNVBAoT
E0NlcnRpcG9zdCBzLmEuL24ud14xLzAtBgNVBAMTJkNlcnRpcG9zdCBFLVRydXN0
IFByaW1hcnkgUXVhbGlmawVklENBMB4XDTA1MDcyNjEwMDAwMFoXDTEwMDAwMFoX
DElG1S2NcniT0g4bLV+zBlay1/HGe0DucfEt8XeRi7
tBtv+d1lG55nN/Dx+g917YadAwShKHATPLJroHNR4zWpdKUIPpSFJzYqqnJk/Hfu
dpQccuu/Msd3A2oLggkFr19gPH+sG7yS6Dx0Wc7x fFQtOK6W8KxvoTMMIVoBuiMg
W6CGAtVT3EkfQDKzrttG07bnz0Avneor2Kpmb1ApyHLYi0nSpdiFfLbxaRV4
RBE116VUPqtmJdLb4xjLivi.cSMJN2RDQnQyLnfeL6LpLoacJUQJ1AGdUX4ztwLE
5YCXDWrbdxixPlUpnhCdh/plWp88KfQIDAQABo4GgMIGdMA41UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWB8TwePkHdxC73B6hrnn7MBDbxjT4
FzBIBGNVHSAEQTA/MD0GC000DgcBAEAACADAwMC4GCCSQAQUFBwIBF1JodHRw018v
d3d3LmUtdHJlcn3QuYmUvQ1BTL1FOY2VydHMgMBEGCWC5AGG+EIBAQQEAwIABzAN
BgkqhkiG9w0BAQUFAAQCAQEAbOHYX3RY6XBj1soNLFjajymS2UU/DBmQB6YpZHZ7P
Rni/04W64j1KGJQqgXdvghv904i/30YIXJguxiAgpX7+feVJIFmwbXdtK2dos7
gVy4oQ4rARS LGALa7vhgTBnkF80nAbNjEgWkCMm0v55QTrXeD5IzZnXQPECjf0l
cXz+Pi42eahLKVAjNQWwLeLuFeWtcV0gnLOJcM83Cu35od6cvo0KxcuEAhGt9eq85
CyzV2FdKMyECmp20t0sZ2x5zfc7AwvxVdg34j1Q7EBZCa0J4IQsqN075fmf7+r
h7PbkKq4no0bHNJ90iNLmuK3aGkF2PQvIger8w/KLAT00==
-----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:  
2713489144953666367009133891636460566719364721268361046536591993  
4994474903020635584331677653228200210928489182501819079634477925  
8492233590999837413051645081782463444435029313072619678324503388  
6132455060944963076820096698396937698650371176940421592482842807  
5011899626639351963633260617226195373584394852072888957304178117  
5313510569711163457668946603482121013634442930239281415342850090  
7026386418520436427134899300324073409253701773263117431279842284  
8480577617459936682837566698589952098721105585848777111378534843  
5966527642400898111594497598591390136982490646196185727187396856  
39915967136410239131574955455289383883587  
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* cfa61bf3895cfe4244fbe684aedc88feadd14d6aa3c73f5688f2c1e52c9a604

### ***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: 0=SWIFT
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Key: Sun RSA public key, 2048 bits
modulus:
27134891449536663670091338916364605667193647212683610465365919934994474903020635584331677653228200210928489182501819079634477925849223359099983741305164508178246344443502931
30726196783245033886132455060944963076820096698396937698650371176940421592482842807501189962663935196363326061722619537358439485207288095730417811753135105697111634576689466
03482121013634442930239281415342850090702638641852043642713489930032407340925370177326311743127984228484805776174599366828375666985899520987211055858487771113785348435966527
64240089811159449759859139013698249064619618572718739685639915967136410239131574955455289383803587
public exponent: 65537
Validity: [From: Sat Jun 15 11:51:47 UTC 2002,
          To: Wed Jun 15 12:21:47 UTC 2022]
Issuer: 0=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, 0=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\..45
```

```
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..0
0080: 42 A2 DE D6 16 DD FF 81 03 17 6C 5C 7E F5 C2 C6 B.....\.....
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....
```

1

*The certificate in PEM format:*

```
-----BEGIN CERTIFICATE-----
MIIDkDCCAnigAwIBAgIEPAkyFTANBgkqhkiG9w0BAQUFADAQM04wDAYDVQQKEwVU
V01GVDAeFw0wMjA2MTUxMTUxNDdaFw0yMjA2MTUxMjIxNDdaMBAxDjAMBGNVBAOT
BVNXS0ZUMiIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlvMie2UrDYQy
2yk3+hjuqq5c8br8qtqzXhsB7Zt99Pen0TFAsAnFyshdMVIgqwyJb8X3QpFEJ
nh6is3o+JrHfKdPs07ISroF9LAD7TEG0EnfiCMNjNJRH80ce0bLKnBfQv/Gwrsp
/SZRzFUlJu+PILZaZ3uwVuxQ1ZLkKWLQVGSQJUDNhh2qewDU3D3S5sRBNS37d4h5
zg3ZV3nmDwuQb0K866KRjiYRRY7rau/amjUYegKJe3bhK18yRlYprz25AS3XWl7a
z0pKv9obTQINRgg/wNwNdgwSF2rZLtbZg8UnLomKwq7MTQfN/cHniG00bfntINL
MmbLH5aTQwIDAQABO4HxMIHuMBEGCWCAGG+EIABAQEAwIABzAyBgNVHR8EKzAp
MCEgJAJpceWzE0MAwGA1UEChMFUjldJRLQxDALBgNVBAMTBENSTDEwKwYDRVR0Q
BCQwIgoAPMjA2MTUxMTUxNDdaQ08yMDIyMDYxNTEyMjE0N1owCwYDRVR0PBAQ0
AgEGMB8GA1UdIwQYMBaAFD4wszs1L1f/8UDbG0UB0C4Vp56yMB0GA1UdDgQWB0B+
MLM7NzdX//FA2xtFATguFaeesjAMBGNVHRMEBTADAQH/MB0GCSGSIb2fQDBAAQ0
MA4bCFY1LjA6NC4wAwIEKdANBgkqhkiG9w0BAQUFAAOCAQEAvs0iVHn5v9Z+5+yZ
penJGIDLb06HTqXNrfPXnu3Ls3j0/SAsw9Xx8xsaQsulYqbo9E01s05XwMCHTLc
+9A0U8+TmjZtFdSL0g7L9rI/lwIa2jkSSUCbzFtRkM4pVR0wwYJTndw4IizkzKs
waSK8tnXx/erD3G4167LATfW5E9Cot7Wft3/gQMxbF+9cLGHle0x9dEkboJXQVd
hx7zhvrz5z6cV05ShhJASshPVXjMdzTzWJcACsdVQr0iyu2UagtRe6TmaIMwcn
4jHNunut7UXB2sGo/oz+v1JA5NqurHiAkf7DK01C9kd8a3zgyLC1w35L0a9wL4Z5
ywyecQ==
-----END CERTIFICATE-----
```

**QuoVadis Trustlink BVBA**

Service provider VATBE-0537698318  
trade name

Information URI [https://www.quovadisglobal.be/~media/Files/Repository/QV\\_RCA1\\_RCA3\\_CPCP\\_S\\_V4\\_16.ashx](https://www.quovadisglobal.be/~media/Files/Repository/QV_RCA1_RCA3_CPCP_S_V4_16.ashx)

Service provider Schaliënhoevedreef 20 boxT  
street address

Service provider 2800  
postal code

Service provider Mechelen  
locality

Service provider state Antwerpen

Service provider BE  
country

**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:  
9783964049937508596233198438506646025473388060525664736390216073  
2102443656154852856590692595277855257563778420931571542568909508  
0978631883136821438467859677425505518925295946478935536215699720  
9060563934601356099502572088165523220585654567621525989833435792  
4120716735302131104382354616099502334946581973200139342601423705  
2576853073064817439203850489307475026119919108600127180985930937  
5722743791909993240230489806096355723483588160724849940671702693  
9421288570479403288803182697829361690097956484101520823731103609  
3100150818512233246331732587859059076124798706288556894310123901  
0972920078194075368441656229441331564718831935659177163391354589  
2011373776362193636814506011844368620196727006732532805298830422  
9507472040779971787788316999945970815156831404655445754634094522  
5619263559926007219454491737036392400734256628057595967019737484  
9640740113884793702843399591566693810287179450856046582198319405  
9528341619175314034894163206925073632423415715700412910266907296  
1997392759148097836830663187572932975564250918605529635852688494  
1903040727077418799850545935706025465473291910192906070443650070  
8759110395706076167863573384978712251913079970430814716559994884  
9072838313070703058851956878669387044135529569895785662937077766  
97029462522370343  
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
6478935362156997209060563934601356099502572088165523220585654567621525989833435792412071673530213110438235461609950233494658197320013934260142370525768530730648174392038504
89307475026119919108600127180985930937572274379190999324023048980609635572348358816072484994067170269394212885704794032888031826978293616900979564841015208237311036093100150
81851223324633173258785905907612479870628855689431012390109729200781940753684416562294413315647188319356591771633913545892011373776362193636814506011844368620196727006732532
80529883042295074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669
3810287179450856046582198319405928341619175314034894163206925073632423415715700412910266907296199739275914809783683066318757293297556425091860552963585268849419030407270774
1879850545935706025465473291910192906070443650070875911039570607616786357338497871225191307997043081471655999488490728383130707030588519568786693870441355295698957856629370
776697029462522370343
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 [
[
```



YWwUY29tL3F2cmNhLmNybDAdBgNVHQ4EFgQU+A9LHhpjGaq/RG+mSRIh83pd4w0w  
DQYJKoZIhvcNAQELBQADggEBAE4EhFe/gsi+ZfqwLZrt47jVWF1zPhX6JoAIWYLC  
DwvKwNVI8UmzkENKcmb5U9FvuFTcUZBsfdodq+Tz8PBUBgYlCoIoEWSqhsLmuR6Z  
I4JJ8KC1tcuF04zNYz501xxcHAaX315vENUf4Ud1ne+jdC3DJ9hDb/fwUk78QZGT  
6ajI2cYeetYh+QkGqCIOiYKkLLXUx9ofM24Jq3mWqBP40DgsWgoQ7LLA+PwN0v9  
Zov90NaYD6D0IMn/dV1E7EshLK9VZ1W9W+DuPSKaCAucSSK7dU21nH5UtB30EGs6  
0yy6hNG3J/VFc0uvu3uDJqI2T5HD6hbN8JMK+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 370861943658773060475449278572584178262799314517  
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:  
6230883699587823739890387754379070477215155351948503696284928928  
6762659096876001348714059503980469058847658322816356034228132540  
6918046605165432002116706169653521048417532557931231131550972290  
0031197228268363040268982941023187957861042676034834020333070620  
7190772580042983034615584070613386365952220836153439341384692657  
8696826895714227903391959565967406530088771729767950440929656043  
2163014585345898816172521920376840236723120805789115312645387870  
9451857348024900006487730553140606594803912885436651803225622760  
4949718044388445919353619902272978753999638960838408864058539228  
3888884791066054654593043703817378828038101637553182828958483889  
7693248294658177178000733919714925449994792299096725660826469141  
5787505237699654446749444700012886783577363368972858974990045545  
5319090699985484921038680916093288098301753746986699829404622404  
8680718777040625727586310877882003632895696490807225717851431255  
6578194457426406147650960292115572503249495434740454018843282749  
6460397682941622995610157763156443595757370452444868333800151563  
7063821029431865926779220502562502734300590316041110043579026517  
8970118108782414636034722304625519061147374704385231750371749725  
0927026791542693181089165688800622906042384672374815917738285418  
78395623639261113  
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:
62308836995878237398903877543790704772151553519485036962849289286762659096876001348714059503980469058847658322816356034228132540691804660516543200211670616965352104841753255
79312311315509722900031197228268363040268982941023187957861042676034834020333070620719077258004298303461558407061338636595222083615343934138469265786968268957142279033919595
65967406530088771729767950440929656043216301458534589881617252192037684023672312080578911531264538787094518573480249000064877305531406065948039128854366518032256227604949718
04438844591935361990227297875399963896083840886405853922838888847910660546545930437038173788280381016375531828289584838897693248294658177178000733919714925449994792299096725
6608264691415787505237699654446749444700012886783577363368972858974990045545319090699985484921038680916093288098301753746986699829404622404868071877704062572758631087788200
36328956964908072257178514312556578194457426406147650960292115572503249495434740454018843282749646039768294162299561015776315644359575737045244486833380015156370638210294318
659267792205262502734300590316041110043579026517897011810878241463603472230462551906114737470438523175037174972509270267915426931810891656888006229060423846723748159177382
8541878395623639261113
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/qventcalg3.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 1&.`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/qventcalg3.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...=E0..
0010: 25 95 51 AB %.0.
]
]

]
Algorithm: [SHA256withRSA]
Signature:
```

## Belgique/België (Belgium): Trusted List

```
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$.
0020: E4 4D 3F 9C C6 30 C2 77 02 86 06 DB 5E 1E 28 82 .M?...0.w...^.(.
0030: 38 09 6F 65 27 C5 89 BA 58 5F 5A 9F 16 0C 5F 50 8.oe'...X.Z...P
0040: 13 A7 B1 19 61 C7 EE F7 44 92 6B A4 95 E7 66 80 ....a...D.k...f.
0050: 95 95 83 41 96 96 20 50 45 4B 09 83 52 3B EC C1 ...A...PEK..R;...
0060: BE 41 0A B1 3F 0A 80 DF B9 12 3E 17 3E 16 E9 DC .A..?...>...
0070: 99 9A CF 26 0E 0E E6 AD C4 80 FB 79 71 B1 D2 14 ...&.....yq...
0080: 8F 4F C5 DF 17 C2 F4 2F 77 04 7A 9B 18 C3 56 43 .0...../w.z...VC
0090: B6 84 CD FA 32 1C 73 5C 6A 50 AB 10 BA B6 06 E7 ....2.s\jP.....
00A0: 9F 41 AB 7B 26 C0 0E 8E 20 BE 9A E2 18 91 18 1E .A.&.....
00B0: 84 59 FF 45 76 A7 17 50 5C 30 CE 05 52 B8 6F 2E .Y.Ev..P\0..R.o.
00C0: 08 B7 51 85 A9 A7 86 B2 FF 32 F6 1C EF EB 22 89 ..Q.....2.....".
00D0: 9C BA 0E 64 DF BC BA 3C 2F DA 0D D6 14 C4 C2 D7 ...d....</.....
00E0: 17 0E 5D 9F 77 F8 03 90 30 AC 78 EE BF 1D B7 33 ...].w...0.x....3
00F0: E7 13 3B 49 DC 0C C4 D1 BB 24 8C E1 38 C5 C2 70 ...;I.....$.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$y.9....s.^...T
0120: 8A 3E 8E F8 A0 EE 21 80 8D 67 0D 0C 9E EC 1F A2 .>.....!..g.....
0130: 2A 24 B3 8B 50 48 4D 38 25 1A DC 0E 34 4A D0 A8 *$.PHM8%...4J..
0140: 78 2B D3 F1 C8 EA D0 5A F2 1F 5F 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 ..0.....(.
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 0D 62 D...8[J].....b
01F0: 64 36 DA 6E 82 A5 D9 C8 12 5F 2A AB 05 87 8E 75 d6.n....._*.....
```

]

### The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGiTCBHBGgAwIBAgIUQPYGUOPATLzX6cg1DpDr1Y3yb1UwDQYJKoZIhvcNAQEL
BQAwDELMAGKA1UEBHMCAQkxGTAXBgNVBAoMEHFF1b1ZhZGlzIEVpbWl0ZWQxKjAo
BgNVBAMM1V1b1ZhZGlzIEVudG9yYyHjpc2UgVHJlczQ0g00EgMSBHMzAeFw0xNjA2
MTMxMjIyMDVhFw0xNjA2MTMxMjIyMDVhMHMxZCZABGNVBAYTAkFMRkwFwYDVQRh
DBBOVFJCRS0wNTM3NjMkZmE4MSAwHGYDVQ0KDBRdW9WYWRpYyB1c2VzZGxpbmsG
QZLCQTEtMCA1UEAweUxvVmFkaXMGQmVsZ211bSBjC3N1aW5nIENBIEcyMIIC
IjANBgkqhkiG9w0BAQFAFAAOCAG8AMIIICGKCAgEAmLsm3G2sW/LTr0g5i0XSSL
DXGEdSfVk7dsEU4wgvy3kvs2L1bpx4g9UjmoQuU1LfvuIWO5mCunFA9COTf+vK4
uTxqVj0Vdd6dAjUx4D+xgGdQd0KNFNV+V6PPZ7KziNO/QfJWZh31sRv/3vybb
ZdVfCaEoGhisYw6GpJ+nQfzyTuvwnjyFdnS55qA4YgNXrmhC91PMrM3pesCa0iA
hB24snUAJjyggJwXLR3rUm7QXg0uLkF0tFEPwvq66kmVt6T045h8CvmCcwqDLPp/
H1N2oMuTFEnxqDFwUP4pRhcCzUt9CWndk8WjyUWnWd5/YMFI2rMK5tdycfuwzXv
LJn4L0UEqn0hvxtV4w1Q15MV7j1pM1AiPpaWKE1WU7BNFCk02aPwYgQnkJOEKW7fg
AqQ0G0Fdqq6b12v1c0E6QvRi15D55JQnQ15A5cpqy8XdaeXKANP/I1AMI1cnsPMBS
IYSu00z0VqHi1v+q3kLs3oz7PV1aglrZ3pJXp9BZGpdcZjhJh5JkvaF8z06qrLP
a+Y08/ud2Bk1t6I0E4EY/637VhcPYTLfxmVZIPFHjM8HWdJBg2c/i+sd5CsIfeeU
0WLUZV3jZbtq01jhe3meejHpbYzggZKM0jUu8/p6vszBKRhjq2bgABBYucFALHH
LTBX3BKrSpS+hjgan7kCAwEAa0CATIwggEuMHYGCCsGAQUFBwEBBGowaDA6Bggg
rBgEFQcwoAyuahR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmF5LmNvbS59xdmVudG9h
MwczLmNydDAqBggrBgEFBQcwAYYeaHR0cDovL29jC3AucXVdmFkaXNnbG9iYWw0
Y29tMB0GA1UdDgQWBBSHybwxLxJ6c7t+wD1FUBQ8JZVRqzASBGNVHRMBAf8ECDAG
AQH/AgEAMB8GA1UdIwQYMBaAFGmVwBVKSL0ZjIHoP9j4NaSzTGMBEGA1UdIAQK
MAGwBgYEVr0gADA9BgNVHR8ENjA0MDkqMKAUh1xodHRw018vY3JSLnF1b3ZhZGlz
Z2xvYmF5LmNvbS59xdmVudG9hMwczLmNydDA0BgNVHQ8BAf8EBAMCAQYwDQYJKoZI
hvcNAQELBQADggIBAKdny+0UpkZbXQ4C6bN+ZMxc66Z1fCdCpoom6Zx3JPPD5E0/
nMYwncChgbbXh4ogjgJb2UnxYm6WF9anxYMX1ATp7EZYcfu90SSa65V52aALZWD
QZawIFBFSwMDUjvsb5BcRfE/CoDfuRI+fz4W6dyZms8mDg7mrcSA+3LxsdIUj0/F
3xfC9C93BhbqGMNW07aEzfoYHhNcaLrELq2BuefQat7JsA0jiC+muIYkRgehFn/
RXanF1BCMM4FUrthVg13UYWpp4ay/zL2HO/rIomcuk5k37y6PC/aDdYUxMLXFw5d
n3f4A5AwRHzuvx23M+cT00ncDMTRuySM4TjFwnC9NgC1Fkk1cr2sRto3DVGdLngk
efU5/fjeZHLXsyaVio+jviG7iGwjWcNDJ7sH6IqJL0LUEhN0Ua3A40StCoeCvT
8cjQ0FryH/V/eRVLiu700C5gZkpRThx0q4hH5mgV/GmnZQ10YhkA9UjBcDw0MRy
8CJ3rL7kFagun1msdAq3kX2pbDHDH1gmtZN2FkXyZcG4mnAK1TTucsGwJep2pu
uhZzdiCAFRJquqDWOHEhqrA1/6pjgPbAuaM/eXYrk+02eSU9IibnACwKBReeXDE
CrI3o4Wmo32E4H5WS0TtwY4W0GG4wtCBq40GJKntpugqXzyBjFKqsFh451
-----END CERTIFICATE-----
```

## Zetes S.A./N.V.

Service provider VATBE-0408425626  
trade name

Information URI <https://repository.tsp.zetes.com>

Service provider Straatsburgstraat 3  
street address

Service provider 1130  
postal code

Service provider Haren  
locality



*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:  
7966709637074040714320658184938038917028092405904624202903753477  
4799458811320809970072905178541448482348252543587667311043751542  
0735604726572971351905453910263879782247724079533201420434980906  
1259652247308046066627990399768704035009312298881553170826145735  
9470451717937201719785652613017682391030700889549269989627026410  
5325707292486709403261729124934205264059173193364705541586249507  
6834153593271925365257093421209559284118721797907404731583231496  
2682519430355956122549300816146144079913741952460191615207765565  
9687136786182992996855987043403957104672173646950330802423343213  
5080733069825853601849667775813367604127913317656392038062824337  
3652327925984793105172907246847023677094414821455351393962051121  
8083182177840750610896383923573133536872261434818526596231169060  
6550103273744647470280502580512087702608652531928666461230253981  
6061426252073514311729869399272487087371248545460690134508722398  
5476499537104029642559990594063568574302420354537223370647609793  
5914070469296940194774706386473904559200906938983111873090308121  
8392153063148362630958830429958529036243703457859882500465304738  
4241045855121661319645975335646628176987427562630329145631982930  
3457355499263101837014704295197539666915727491296546803494944852  
83853717680609119  
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:
79667096370740407143206581849380389170280924059046242029037534774799458811320809970072905178541448482348252543587667311043751542073560472657297135190545391026387978224772407
95332014204349809061259652247308046066627990399768704035009312298881553170826145735947045171793720171978565261301768239103070088954926998962702641053257072924867094032617291
24934205264059173193364705541586249507683415359327192536525709342120955928411872179790740473158323149626825194303559561225493008161461440799137419524601916152077655659687136
78618299299685598704340395710467217364695033080242334321350807330698258536018496677758133676041279133176563920380628243373652327925984793105172907246847023677094414821455351
39396205112180831821778407506108963839235731335368722614348185265962311690606550103273744647470280502580512087702608652531928666461230253981606142625207351431172986939927248
7087371248545460690134508722398547649953710402964255990594063568574302420354537223370647609793591407046929694019477470638647390455920090693898311187309030812183921530631483
62630958830429958529036243703457859882500465304738424104585512166131964597533564662817698742756263032914563198293034573554992631018370147042951975396669157274912965468034949
4485283853717680609119
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://reposit
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+
]
]
```

---

## Belgique/België (Belgium): Trusted List

---

```
]
Algorithm: [SHA256withRSA]
Signature:
0000: A8 7C 4D 53 16 D5 F8 35 E4 4F F2 02 A7 B6 1C BC ..MS...5.0.....
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...y.z.....'
0050: F3 F0 1B F4 C0 51 AA 80 13 B1 66 2A 28 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 A0 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 88 F7 26 E2 44 94 P]...y_?R...&.D.
00A0: F5 66 4E 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 CA 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 [...]....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 CA 3A AF 98 AF 3B 5D E9 AE 46 AA 19 60 2C 96 .....;].F...`
0170: A0 67 A5 F7 B9 2E C3 E6 45 A0 8B BD ED 70 73 A4 ..g.....E.....ps.
0180: E6 50 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...KId.
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 $.t.I...K...`".
01E0: 83 CA 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.....(.];
```

]

### The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIG5jCCBM6gAwIBAgIIOCDunHTS0UcwDQYJKoZIhvcNAQELBQAwYTELMAkGA1UE
BhMCQKQxJDAiBgnVBAoMG1pFVEVTFNBICWhVQRCSR0wNDA4NDI1NjI2KTEwMDA0
A1UEBRMMDAaMR4wHAYDVQQDDDBvRVRFUyBUU1AgUK9PVCBDQ0SAwMDEwHhcnMTYw
NTIwMTcyMDI5WhcnMjYwNTIwMTcyMDI5WjBmMQswCQYDVQQGEwJCRTEKMCICA1UE
CgwbWkVURVMyMDU0EgKFMjZBVEJFLTA0MDg0MjU2MjYpMjYpMjYpMjYpMjYpMjYp
BgnVBAoMG1pFVEVTFNBICWhVQRCSR0wNDA4NDI1NjI2KTEwMDA0A1UEBRMMDAa
AQEFAAOCAg8AMIICGKCAgEAw0ePE++btk1uYouqDgClGmrIekzMP8kFfDsZwrD7
IwQcPm5YJv+LlGklH0hG0UBRQY9rWxy3wEpMgo4uPviBN5c/gM0jJCjBq3nuLc
mXUJ1aqPmEcTf8kFwJGTBZ22/HAEDKdBG142iZniaiAr8q6//GyH1AnogIZg/1MJ
CjEFf0XyJXSx9oTfh8Qygl0oogtI00Wg9KZs4Ik4pggyEKrMqvD8EGHNWhwMgDg
eX4sB15cJxai2nqp+39wLkzJ/54V5ZJNncGDAzvj0i0Rz5zx/+2+/9M0wPIbnxTU
pn+7BM7az3tFQWYOIEDP3/hI8pwBq+C5M12I9P2VkQck0/33R05v1c0I4gZSUkx
iTM7IrxLo9bvj18s/9A9vtGmqxbEuYs4WduEEhQX+hhTBop00Erzi9pLTPv58Ij
fMcC+DUoLnaCuvkb6wDunKvfbZsk4rTAoIL0K2idTEf9PAP39F9UElSLtAeDHR5e
R5W7RVarop8Drx9cM0aXqKyvUJyAdYLBH12UrgvKKFVaF7s6lRbqr6PMn4fni
PGxnrnxVL4CUdwtNH7odLM6UX55LziKpLlx9jGfYrLITq55Yg0hg0IoVx5RifZP
pCh6gF104DJyCGA6XLtn0YokPwg/ih7WqfhY50nFvwar0esA5RUqHff4GgFrqcC6
118CAwEAACA0CAZSwggGXmHEGCCsGAOUFBwEBBGUvYzA6BggRBgEFBQcwAoYuaHR0
cDovL2Nydc50c3AuemV0ZXMuY29tL1pFVEVTFNBICWhVQRCSR0wNDA4NDI1NjI2K
BgEFBQcwAYYZaHR0cDovL29jczAudHwLnlpLdGVzLmNvbTAdBgNVHQ4EFgQU4rTb
X2oPA1BU1R3v0nZyciGVR1swEgYDVR0TAQH/BAgwBgEB/wIBADAFBgNVHSMEGDAW
gBQ4vFwvNziuyDv7m9B0DFuXP2LdtB9B9NVHSAEdjB0MHIgBFUdIAAwaJAsBggr
BgEFBQcCARygaHR0cHM6Ly9yZXBvc2l0b3JlLnRzcC56ZXRlcj5jb20w0gYIKwYB
QUHAgiIwLgswKwVURVMyMDU0EgKFMjZBVEJFLTA0MDg0MjU2MjYpMjYpMjYpMjYp
Y2F0ZXMuPwYDVR0fBDgwNjY0oDkgMIYuaHR0cDovL2Nydc50c3AuemV0ZXMuY29t
L1pFVEVTFNBICWhVQRCSR0wNDA4NDI1NjI2KTEwMDA0A1UEBRMMDAaAQEFAAOCA
AQELBQADggIBAKh8TVMw1fg15E/yaqeZHLzfr4WwyVKxT15rRLTxzcFZL4v060Cb
NADv7a1lZCaxZcJGwEejxTbJ6H5HArNmTYUgWc5R85euy2raQAYPm48/Ab9M1R
qoATswYqYe039Fg9nQDUzo0HpsS188o74WBKI0HlBQ6rfBjzszFEtemEgtL0LI7
rnV/GCfThq0rHVBdxhArV8/UsKl9yb1RJt1ZkbtvZvHm4o5d+G5HH8rHig+0X4
qu72+w5NwchumK3UP84zPL+Yjvpgcfzpm53jchFBOKwa4DXPd18eWfENv1xPQn
ztyt50Tzg8SZpgunBJu4norA2jKGGPeE6V1RrH9X0ZwjLkFmtpCnRXGj+qkJaFVT
EoE005kqKp5WR1t9v0q5LJ2d70pxabhFYLDocmxyMY9FaNk9Wo5t7MsvzyGhiUt8
G7nmB7gz1d8gj3hwPprX/I4di1AJqoKmqb5GxDqvmK87XemuRqoZYCYwqGe197ku
w+ZFoIu97XBzp0ZduP8E6LWk1uCEamUA2Zi+Rgc9b74BCrg4YLMdv1sCEXFa3w3
6RB6kLo8E2I/eLNahR4uRTpYhsKyuEtsZOP1+02RZ0LbX7HmZBwrBvA8JMp0SZk
s3zhS/DlymA1ioPEPCQ9qMybkwqjbb10Yhm50f1thjWdXY7Ns0Dwo7
-----END CERTIFICATE-----
```

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

Service provider VATBE-0428775335  
trade name

Information URI <https://www.portisign.be/fr/support>

Service provider Chaussée de La Hulpe 150 Boîte 16  
street address

*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=Terhulpesteenweg 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:  
7822335710007250551470827815520429196806563000163141345472100871  
8789659735588388736316477840674900410458325278917004905346277771  
4543027813377832723686044148297352247511982636804558743064752710  
6301046346434416101626130393302258633237561007152678567612087066  
3683721730128241514875458608294766470859534355051592824098685605  
8903703273900457384328845246582324465256168787803317124987401334  
2462731095819083051320211384523615086499910250808844527573993421  
0447410281820991260708241650614214254804641853689464973624896182  
2380119351693256776860981717710315130994214488579044776384353133  
4856056247246919542703267661373480881344982047761379263173831530  
7121409617152355614690078966861791094126065513701509584062601649  
2911537726053232950941626095777957264249178084496030530417805736  
5334115179305518464665388525674699672162482962465423367544618093  
9974269242877717771137170418551131286833207649050802162628637605  
8134404749628647471462878938327392198840836357505581846785829429  
9046958532083219377494293809710960360888219223565724084558060043  
6040441175452189645619261138941657714054659919998428642561751460  
2780604465263348085101519821412158692760937791849160981740144608  
8075047110709752788110814215053396885320828719551107276902798136  
74328209071723559  
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:
7822335710007250551470827815520429196806563000163141345472100871878965973558838873631647784067490041045832527891700490534627771454302781337783272368604414829735224751198263
68045587430647527106301046346434416101626130393302258633237561007152678567612087066368372173012824151487545860829476647085953435505159282409868560589037032739004573843288452
46582324465256168787803317124987401334246273109581908305132021138452361508649991025080884452757399342104474102818209912607082416506142142548046418536894649736248961822380119
35169325677686098171771031513099421448857904477638435313348560562472469195427032676613734808813449820477613792631738315307121409617152355614690078966861791094126065513701509
58406260164929115377260532329509416260957779572642491780844960305304178057365334115179305518464665388525674699672162482962465423367544618093997426924287771777113717041855113
1286833207649050802162628637605813440474962864747146287893832739219884083635705581846785829429904695853208321937749429380971096036088821922356572408455806004360404411754521
89645619261138941657714054659919998428642561751460278060446526334808510151982141215869276093779184916098174014468080750471107097527881108142150533968853208287195511072769027
9813674328209071723559
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=Terhulpesteenweg 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 0..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...
]
]
]
```

# Belgique/België (Belgium): Trusted List

```
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 .....B0.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 58 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 ..S...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-----
MIIGfjCCBGAgaAwIBAgICJyIwDQYJKoZIhvcNAQENBQAwggEBMRcwFQYDVQQUEw4w
MDMyIDInGjYxNDQxMTEjMCEGCSqGSIb3DQEJARYUc2VjdXJpdHlAcG9ydGltYS5j
b20xCzAJBgNVBAYTAkFMRgwwFgYDVQOHEw9CLTEuZnZlbnRlLnZyXzA0MjE0MjE0
BAGTEjYdXNzZmZlbnRlLnZyXzA0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
dXNzZmZlbnRlLnZyXzA0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
dXNzZmZlbnRlLnZyXzA0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
UG9ydgltYSBzLmMuc15sLjBjLnYuY15hLjEaMBGGAUEAaMRU9ydgltTawduIFJv
b3Q0Q0EWhcNMTcWjE2MDcwMDAwHwNmjcwNjE2MDcwMDAwHwNmjcwNjE2MDcwMDAw
EwJCRTEiMCAgA1UECHZU9ydgltYSBzLmMuc15sLjBjLnYuY15hLjE4MDYGA1UE
AxMmVU9ydgltTawduIFVzZXZlZiE2MDcwMDAwHwNmjcwNjE2MDcwMDAwHwNmjcwNj
ZXMwgGSIb3DQEBAQUAA4IDwAwGAwIACAQcVzqvr6Iw2cbgBPDD
Y+4efCP0ZUwT/vfeKwGad+WidY462J1cXE5nuxC7Q1ubuXb4fwixN6ZP/e9gdI+V
ORZavsM9S2MQLaEMrqrk0LFV/nZsRaYUhcIxvqzp8y4ayh+Mjfc1+BUqzKiwwF4
nvs+vZD+sDVoLGRKy3cKyq+kA2V5ImK+1bSMHF1iX8fMMP2ZxZf2uVM99zDM3MXB
r3LTHJgFjQj0z1Rk+8Mfx9SKXhwhTfTRkfCqQXlw/cufWhX4K1/7D3TXfNmE0jr0
RTLY0JnZsJk+oXeig8hdtLQWbuNblVZ8fUYK3uPnL810bMItkvyWcjpILXYae1
hxIKZcDya5xx27hNySgdIElWUMg9KuEmhKcK4fw3J0BeUHBaw6yMgy7jAPn8Fj
cv0dctwa3tr23a/ugC/Sj7XbZycLgJpcD7PKKVEB8uooWtC4RWhAU8R3vzLUxyLd
5+DEUS3a35odnnM7sYrsUhnXl+GLPzq7TgPx+bTk7AB+3MnFPKXhBXMRA3UPhEpX
yTHPhaa9Bd8rpv+0mzkVrI+6qCAwPyKeSACw57oIakcg50E6ahk8P7RiX7LDFWL
4FKNRin90rPIWLu6st2VhQASiRi0adJoCv12941+EpXlt1WmEsjhX4jxXwFhK/i
TW4/3QKJUvuptAzgcf/3drLUJwIDAQABo4GTMIQ0MA8GA1UdEwEB/wQFMAMBAf8w
EQYDVRO0BAoECeMkzDZu1hHXMBEGA1UdIAQMAGwBgYEVR0gADATBgNVHSMEDDAK
gAhP4r4ycEeysZALBgNVHQ8EBAMCAQYwNQYDVRO0FBC4wLDAQoCigJoYkAHR0CDov
L2Nybc5wb3J0aXNpZ2ZuYmUvY3JsL3V3b3QyY3sMA0GCSqGSIb3DQEBAQUAA4IC
AQBwq10z0S+eJ9Mzt3lF/1p0bvgd33K09oeHoUoLfm2M0Tpx+6f0KJPtnK23VmL
odPxbMnr9WZ18AgH44M0tJLHooFmm5E2nqK1951VS+/nPCJ9bXzMmigaQqIcLy4
3awCqVvY8CLSDhDR1Tbn50QP4P0VjgD8mrKVgJPI7cTLLD2ktA3aDNeHoaYSVC
U9B5j1dGVJG430biqTo08kXvTpsmz207MEP6f2wuTjsgCKPgl488noh0007C7p
UVfyxss10VYBEFF+qgB66kiMf3hyzmmW3SHfPTwLhMBCd0qzH16GzS1x3xxzF5w4
+VR4FKQtYMDkyuANLcCEyZ0GegvUIQn51JYLFv/iEKVSVcty87t3bd+srtVh401
B0eKeEGu8w0e330XAW8v8kkfy7V9XFGXd+SzLpX9Svm07L6/s8BEM70zxbkSg0gX
140VCDf/wEnQCFMzuipDtVYx1Ys1zAS2Ek0JLZshNEetZCB3BJzua2e41jf/drjh
eaudwehx+Ld6FRzCN3f3vyvYBuNBwUU3gIjNnNtWXMkFhcWUWmVhL15mNldxDycAM
UB61ZeK006R1ybrQCPA5X10R0FX8jBMc8Zq+Q51ChKISz00zXh00xtZIj9Ld6g3
QPFFXSZuPgDdFRduI45rTpaY55DvGHv/sRjxJudeyr06Q==
-----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:  
8496342594090797255332740525090375391026141209024613382601131474  
3526325147577098920755981071869925793279298373076660629327002504  
9761465100568418825473084562192693028965685595236345251387469981  
0877382098281760803599595838944836574405713645073986660291422228  
8796444520217745347047466774239180419488159426376612432478329539  
5182265925085784245055822607410675601677470070056396999987258494  
0740695188971509129780614630347844908773485143291382504872042945  
6270802691383820345063048136016156016559709034323603417600409511  
4531455561227344091147666956810822609697202463449670498214146450  
4937910695984786451282007283357852228329681368127908597747878117  
2077493988308961078819185557865501493517080922539609409187508185  
4822708916333768406362775536327484401830050821562493983458620132  
9796749274052917921597285791755636861519805742016710173907643847  
0245663140383320497165646608843920324428195219635609149551448177  
9627765115140709972510276820807882249814189340670178677313624264  
4806320341179245164187711567118158704892622744455501030409114213  
2628033682888423689434447151043864493112177318026615610676732936  
3613006961641856271861881724634655675630111995800486827579105998  
7434373898235087347973015573736746087726817511787641180646330676  
54636539287413393  
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:
84963425940907972553327405250903753910261412090246133826011314743526325147577098920755981071869925793279298373076660629327002504976146510056841882547308456219269302896568559
5236345251387469981087738209828176080359959583894483657440571364507398666029142228879644452021774534704746677423918041948815942637661243247832953951822659250857842450558226
07410675601677470070056396999987258494074069518897150912978061463034784490877348514329138250487204294562708026913838203450630481360161560165597090343236034176004095114531455
56122734409114766695681082260969720246344967049821414645049379106959847864512820072833578522283296813681279085977478781172077493988308961078819185557865501493517080922539609
40918750818548227089163337684063627755363274844018300508215624939834586201329796749274052917921597285791755636861519805742016710173907643847024566314038332049716564660884392
0324428195219635609149551448177962776511514070997251027682080788224981418934067017867731362426448063203411792451641877115671181587048926227444550103040911421326280336828884
23689434447151043864493112177318026615610676732936361300696164185627186188172463465567563011199580048682757910599874343738982350873479730155737367460877268175117876411806463
3067654636539287413393
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=Terhulpesteenweg 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 0..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 68 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.yl...?.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 38 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 ...Ba.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..\*





*Version* 3  
*Serial number* 16718297222790658621788184414730  
*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:  
2278699972260958242570106364685218364222312360409837897286689958  
4206259405863671525808018022668465651753042776036196630535005264  
2245757362085946019302495704135312931933067851753677454798550527  
7739474253238987646317877715144277541606397066038479382815391881  
2314909295417801991364937382493148487476857088326560843966433239  
8093558068336244209291777148987915413400070960756242915659374818  
8284974659841271912727321559814873806248854930647488327256254693  
9228220065022382516469383454105804980627182316637737031645204515  
4464473562077809593954881162726944826199253990619104448722271457  
81685144905495235452958875464560048586131  
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:
22786999722609582425701063646852183642223123604098378972866899584206259405863671525808018022668465651753042776036196630535005264224575736208594601930249570413531293193306785
17536774547985505277739474253238987646317877715144277541606397066038479382815391881231490929541780199136493738249314848747685708832656084396643323980935580683362442092917771
48987915413400070960756242915659374818828497465984127191272732155981487380624885493064748832725625469392282200650223825164693834541058049806271823166377370316452045154464473
56207780959395488116272694482619925399061910444872227145781685144905495235452958875464560048586131
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...
```

# Belgique/België (Belgium): Trusted List

```
[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 40 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..ma
 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..l.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...l.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]
[ ] ]
]
```



```
eQAUMAKGBwQAi+xAQMwCAYGBACegECMB0GA1UdDgQWBTVQmkDaSb+RERdp7F
vZ285Hg5xjAFBgNVHSMEDAWgB5xGI+yuTjSmnc3e3gVWtu+gAXsjA/BgNVHREE
DDA2gRlpbmZvQGNvbm51Y3Qtc29sdXRpb25zLmJ1L0BkGCGSsGAQUBFwGDoA0wCwYj
KwYBBAGBqBqCMDQGA1UdHwQTMCSwKaAnoCWI2h0dHA6Ly9jcmwuZS1zemlnbm8u
aHUvcw9jYTIwMTYuY3JsMG4GCCsGAQUFBwEBBGiWYDA+BgEgEFBQcwAYYhaHR0
cDovL3FvY2EyMDE2LW9jczA3XmUtc3ppZ25vLmhlMCGCCsGAQUFBzAChNodHRW
O18vd3d3LmUtc3ppZ25vLmhlL3FvY2EyMDE2LmNyd0CBsgYIKwYBBQUHAQEgaUw
gaIwCAYGBACORgEBMBUGBqQjYkYBAjALEwNlVUYCAQEAQYwCwYGBACORgEAgEK
MAGBqGAjKYBBDBTbgYEA15GAQUwSTAKFh5odHRwc2ovL2NwLmUtc3ppZ25vLmhl1
L3FjcnHNfW4TAKVOMCEWG2h0dHBz018vY3AuZS1zemlnbm8uaHUvcWwNwCwMCSFw
EwYGBACORgEGMAKGBwQAjkyYBBGiwDQYJKoZIhvcNAQELBQADggIBAINamAYs rEp
mIVC1pgD7fEUXHnKYIbw1a2qCMsa0zIoC5DR+SDA6MVUD0+JdUDNwJt0v+eTAKTq
AsrSfBN00KQ0U0dDjIT0leUuUHaU4EKVMX9d+9IMTixccajjmYe+IDYs3640UjRX
mXcS9b3AbeG2hdPERRiLm6qNop6nvCBJHT7Z2B6SpQXsY2JRxzNg/gKiCMdZu0Hr
NjjHmFTLqAx6LJNsxNgWBoELPejIWPj095y85rmMkL4h0sMz+hagH0kqZcSvyr
UKyFP0za8AbxLCWDTzqDmKRfWQR2W5kBJff8jcuoNWU0zbiHya4gVDFQWL390nh
5SK0kQKvdNDVAKR6dE3+VnPcE0rhe2/oKgy0UnchzuBkyN+/I+0vLaIkpo7FsGjn
Lzk5NjGhTJb47VQLU3h4eNSgvruh00Pkm53906L28Y27t7d7Unbpq8WHChzIyJ
y0Wqj6axMn39geLQoct4Vi.rgetz0WqJgtILFdfVzeH/B/P2qT4jYPTT4KqLAQ95
qLtHEMAo6/7PGhwjgLUNJ6fET8k2i8c+Y0zcPZ13qr1ftEMLkLhlu6jAmfD5LrS
s1Kj0+7psdzeIGv+PHimwZHUkn4vJXW1ac0chwwV40LPA01uL4Rnq+tnGyT/+UJ4
Qe6+KLYZcBn7Jo06p5jJ+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 16718579776009287865360701836554  
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:  
2135774906536500690275642827531478044762404319791472709601435579  
6040183720986486759720494772670902123072513544197750740762148710  
8066575345409813550558155436381014425080001533223240350456723398  
7664275253392031550128000875095145358143617717474741647062156744  
6406267117434677809980509033160026107293765007659083456515207538  
7898684603577929925716648036072300699959794168603558308748545588  
5374900944445666982161300080532936678659177763204026826499316582  
3385325197679216889778061454587863379743666599019114810100871957  
3671343235129700074644201440738791372018403358308649201217030205  
28027918191798466752086376540978742542353  
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 dc65ff59b1c0b545fb89b87c58fc861bbab22d534a050ccbd76d846ddd12c3cfc

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
322324035045672339876642752533920315501280008750951453581436177174747416470621567446406267117434677809980509031600261072937650076590834565152075387898684603577929257166480
3607230069959794168603558308748545588537490094444566698216130008053293667865917776320402682649931658233853251976792168897780614545878633797436665990191148101008719573671343
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 ..HU.....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..g.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 IM.
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 40 00 69 00 6E 01 51 0.....M.i.n.O
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..
```

# Belgique/België (Belgium): Trusted List

```
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.t.e.t.t. .a.l
0080: 00 E1 00 ED 00 72 00 E1 00 73 00 2D 00 6C 00 E9 .r...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.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...
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.t.o.t.t. .l.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... .l.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..0
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 S0.`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 0C 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 9D 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!.....,0+....
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 .....%!.S.0
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...0..
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.....B>...
```

```
]
```

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIKZDCCCEyGawIBAgIOANMEp09LEwvncsJJzQowDQYJKoZIhvcNAQELBQAwYgYx
CzAJBgNVBAYTAkhhbWREwYDQVQ0HDAhCWRhcCzVzdDEWMBQGA1UECgwNTWljcm9z
ZWMgTHRKLjEcmBoGA1UEYQwTVkFUSUFUtmjM1ODQ00TctM100MTExMCA1UEAwWn
UXVhbGlmawVWIGUtU3ppZ25vIE9yZ2FuaXphdGlvbD1BD0SAyMDE2MzE3MDYw
NjA5NTwEwNl0xDTESMDYwNjA5NTwEwNl0wGcoxCzAJBgNVBAYTAkFMRcwFYQVQVQX
DA51ZXZvZGVuLWVpbGRlLjEaMBGGA1UECgwRQ29ubmVjdCBTb2x1dGlvbnMxGTAx
BgNVBGEtZmFzZVEJFlTAANDM4NzEyOTQxGjAYBgNVBAMtEUNvbm51Y3QGU29sdXRp
b25zMH5GwJgYJKoZIhvcNAQkBFhhlpbmZvQGVmb251Y3Qtc29sdXRpb25zLmJLMSUw
IwYDQ0FEExwLjMuNi4xLjQUMS4yMTUyOC4yLjMuMi4zMTCxMIIBIDANBgkqhkiG
9w0BAQEFAAOCAQAMIBCAKCAQEAQs+bNG780NSeZ1tH594qKYrWTByLk43vXT11
S1MburD78q/jVS/+P3PnCuDzXBeOpLi9Xg77VWVbDya5+2ek2XGyw806Hpp+kdB
PQURIg19BKSjUnrPMrUjK8BxBTnmA20oeelzbXkQuM3uWr3CtsAXwgaZMjfsxKW9
sJXsHXScnIA6b0aw/7mhSPYbFk0IAIwckPkrckhm2XXhgw8I+0FvK4V7YyuP9mHdh
Mcv2T+oJo+k34hjPzPygLyP9aXv0BoVZCz+S03nM41DbtjIFpRhgHsGEq0pRtS9
rLuW0AN8D0nFLgMS3TXq19YyWrb/7HJWRXzyVIDustLap0vAEQIBZa0CBYggwGE
MA4GA1UdDwEB/wQEAwIGQDCCASQGA1UdIASCA4swggOHMIIIDbgY0KwYBBAGBgBgC
AQFRAGIwggNaMCCsGAQFwIBFhpodHRw018Y3AuZS1zemlnbm8uaHUvcWVw
czCARIGCCsGAQFwIBFwIBBBQCAQBRdWfSAwZpZWQ0Y2VydGlmawNhdGUgKEJy
b256ZSkSIHR0ZS5Bwcm1ZXRyLIGtLeSBYzXNpZGVzIGUuIGEGcXVhbGlmawVkiHNP
Z25hdHVyZS5BjcmVhdGlvb1BkZXZpY2UgKFFFT00pL1BSZXRlbnRpb24gcGVyaW9k
IG9mIhdGvYafSvIGLuZm9ybwF0aW9u01AxCMB5ZWFycy4gTGtLtaX0q24gdGhL
IHZhbHVlIG9mIHRyYW5zYWN0aW9uczo5FVGIIDFNLIUaGUgc3ViamVjdBVzI0
aGUgY2VydGlmawNhdGUgXMGbm90IGEGbmF0dXJhbCBwZXJzb24uMIIICGAYIKwYB
BQUHAgIwggIKH0ICBnAGkAbGFRAMA70B0AGUAdAB0CAAdABhAG4A+gBzA00A
dAB2A0EAbgB5CAAKABCAHIAbwAhoAKQAsCAAYQAgA0YQBN0EAbgBrAHUA
bABjAHMAbW0CAABQBPAG4BUQZsA00AdABLAHQAdAAAGAEAbADhA00AcgDhAHMA
L0BSA0kAdABYAAGUAAAbvAhoA8wAGUAGUAgB6AGsA9gB6ACAABNAEETABFACKA
IAB2A0kAZABpAC4AIAABBACAAGBLAGcAaQbzAhoAdABYA0EAyWbPAPMAcAgAGEA
ZABhAHQAbwBrAGEAdAAAGAEIAIABzAhoAbwBsAGcA4QBSAHQAYQ0APMAIABhACAA
dABhAG4A+gBzA00AdAB2A0EAbgB5CAABABLAGoA4QBYAHQ4Q0BAPMAbAAgAHMA
egDhAG0A70B0AG8AdAB0CAAMQAwCAAA6Q0ZAGkAZwAGAVEAgB6AGkAIABtAGUA
ZwAuCAAAVABYAGEAbgB6AGEAawBjAGkA8wBzACAAbABPAG0AaQ0B0ADoAIAAxAE0A
IABGAHQALGAgAEAAIAB0AGEAbgD6AHMA70B0AHYA4QBUAHKAIAhAGwAYQ0uAHKA
YQAgAE4AR0BNAACAAdABLAHIAbQDpAHMAegBLAGHQAQZBsACAACwB6AGUAbQDpAGWA
eQAUmAKGBwQAi+xAQQMwCAYGACPEgECMB0GA1UdDgQNBBSrCLUvzcxwW6JFE2H
vBIYq41x/DAfBgNVHSMEGDAwGBSXGI+yuTjSnmC3e3gVWtUV+gAXsJA/BgNVHREE
DDA2gRlpbmZvQGVmb251Y3Qtc29sdXRpb25zLmJLb2BkGCCsGAQFwIBwDoA0wCwYJ
KwYBBAGBgBgCMDQGA1UdHwQtMCswKaAnoCWGI2h0dHA6L9jcmwuZS1zemlnbm8u
aHUvcW9jYTIwMTYyY3J5Mg4GCCsGAQFwIBwEBBGiWYDAtBggRBgEFBQcwAYYhaHR0
cDovL3FvY2EYMDZLW9jC3AxlMlU3c3ppZ25vLmhm1MC8GCCsGAQFwIBzAChINodHRw
018vd3d3LmU3c3ppZ25vLmhm1L3FvY2EYMDZLmNydDcBsgYIKwYBBQUHAQMegaUw
gaIwCAYGBACORgEBMBUGBgQAjkyYBAjALEwNlVUYCAQEAQYwCwYGBACORgEDAgEK
MagBgQAjkyYBDBTBGyEAI5GAQUwSTAKFh5odHRwczovL2NwLmU3c3ppZ25vLmhm1
L3FjCHfZw4TAKVOMCEWg2h0dHBz018vY3AuZS1zemlnbm8uaHUvcWVwCwMCSFUw
EwYGBACORgEGMAKGBwQAjkyYBBIwDQYJKoZIhvcNAQELBQADggIBACbFRt9o7AX5
/ND5NfiqcRtjYBHKgD/BM1nVF+BaYK87gvnR6g1P7LLiTJMSsvuTxSwbV4qPfF8
g254hhFH7NvWu31WNgbd6aiRu1VC3pZB7HsNQ02jKPSRm8evE+VNP3WBUcLG
nUBAKS/3IwuaL3hJzpfDg7974sr3ULVLAXImdEAA50ve3Ky+5W2o62aJ/BQy3t9T
1I51jeePFj31js5zBMsDrfrEdyaA33QH4sdXoU14EAnG0IGCU0tb6N3ZBkXqE
6en0EjI9j6uLowAy2s44XJdX7s251wxH1f3pYmH+5/6a1kVgtL2+mFkNLTUQIA
y2AaFM+0Y9/ZwCHI1vmTLIn0TyvSp6vcNw54EVO1M0LBJ7Wp6EXyYkY5gyrB4CZ
AJIlniEK90845vUBhhJoc71Y4twWUTsE7RLX3Z720kcRYbUv/dG09Wk3mTe+FFL
090xc3GoC3mE+Q0eE1Nw2x0wD8+wpX0hm6nc1w0A/LJHsGzBReaKiqTXbzKa/ig
VavLxcN7tctGV3apZqzq77tdnGWSBmtv70H1vVFb6TDutpbL7bfo97ER1GSJG
0xKlexjnpplIMGR4ok1QrLmW+p4eTw0Cv6KY5RmDpQIwUdVwGGZ1P5X9Hx6M4I8
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 16718873389460742701929777187082
Signature algorithm SHA256withRSA
Issuer CN=Qualified e-Signo 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:  
2485944034905827524446554348166911989150986788740713634730600812  
2383500635157452210483314205298254091229867863859444317438853115  
2674479249062334953055885539040331777999995761011749599973255115  
4703810034490977355667162354125914532847919596902353283208639617  
359728041875379498634308482894154583448562615246012479779634125  
6879693465096439821915790778138652344407937246458649235240043508  
1005314357025012438597999306328282520998923935613430413761160374  
4508468363886858384523117286653022023158025921311415205774272828  
0628587606016008611869061397776825210402351712587082004624929160  
95087954796508690394493025493769970770423  
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
  1011749599973255115470381003449097735566716235412591453284791959690235328320863961735972804187537949863430848289415458344856261524601247977963412568796934650964398219157907
  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-szigno
0060: 0F 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 .HU.....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 [
```

# Belgique/België (Belgium): Trusted List

```
[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 68 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 40 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. .l.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 5A 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... .l.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 ....
  ]
]
]
```



3TWJt037nrkavH78fYNPscX5UGkhqAiiwKRaE3afRuRW/a1gg0H8NpmXR0hqm
F8qGgtnnv98vs8Nq59jIURY3ltVKKqAr
-----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 13:37:15 UTC 2014
Not after Sat Feb 17 13:37:15 UTC 2024
Serial number 16398570047450317122
Version 3
Public key SHA1 8f914035f0200880afe97b0eab85b5921ea98421
Thumbprint
Public key SHA256 f7cf32405bc6553c92fec8364bf58d56b153324ad58ad6cb7aace1037d5d3e41
Thumbprint

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:
2430099668952271336930030093714651766559690911903216193281992404510245187371320819543733804448624693522397655805338290368738930744837629562942067296575129066040125015273157
93517280217865321819160740775732194727930458919922521995692540951807923171115060769731590712346286509664439160107000534884146909041751636242027382031023466107500619524409877
27283427021323280307639992049788147229043339760080834570290066311843665221921835557433177168179986865374356704032605187207885089432302544936253416592529324143468606089203473
20921304607665880177501274313091120751308363261034368874146407550848866631307165625943996664160511
public exponent: 65537
Validity: [From: Wed Feb 19 13:37:15 UTC 2014,
To: Sat Feb 17 13:37:15 UTC 2024]
Issuer: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
SerialNumber: [ e3936c93 26a30142]

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: 6F 23 D6 03 88 28 42 93 77 DD 38 11 EA 58 B3 53 o#...(B.w.8..X.S
0010: 22 A0 11 2B 8D 7C 64 00 DD B3 BD A6 5E BE 1D DA "...+..d.....^...
0020: C2 40 7A 70 67 90 52 79 83 CF 7B DE E1 90 89 48 .@zpg.Ry.....H
0030: 1E 0C 67 5D FC 12 45 22 D9 EA 18 5D A3 F2 68 BB ..g]..E"....].h.
0040: F4 D6 F9 7A B0 CE 9E 52 3E 90 87 03 6F 7C 65 C7 ...z...R>...o.e.
0050: 3F DF 40 38 71 BC 67 21 F8 22 42 60 07 EF 23 22 ?.@q.g!".B'..#"
0060: 68 60 D9 D6 A7 8F 85 5C 02 8B 06 B6 F4 E4 9D 8B h'.....\.....
0070: 59 D8 AF 86 85 17 AF 80 09 E8 AF 28 49 EC 0E E3 Y.....(I...
0080: B3 3C 16 CD A6 A1 17 04 E7 BA 7C A6 94 15 E5 AF <.....\.....
0090: 01 BD 2B 20 52 92 0E 08 85 68 1C F8 88 18 52 00 ..+ R....h....R.
00A0: 3B AE 93 99 EB 35 C5 3D 32 50 26 98 62 46 0E E9 ;...5.=2P&.bF..
00B0: 40 40 A7 57 51 6F C3 D7 9D 88 C1 A1 06 73 48 DE @@.WQo.....sK.
00C0: D1 3F E4 82 88 BA 0D 97 A0 9D CC 96 1F 65 86 8E .?.....e..
00D0: 9C F1 80 21 CA 9D 90 D7 A8 A7 08 B0 C9 92 C6 5C ...!.....\
00E0: D6 A5 2A 44 7A 3D 96 6C 16 9C 60 0D 59 F6 6F 41 ..\*Dz=..l...Y.oA
00F0: 64 49 4B 42 C9 BE B1 7B 2D 22 F9 1F F6 38 C9 9A dIKB....."....8..

1

*The certificate in PEM format:*

```
-----BEGIN CERTIFICATE-----
MIID3zCAseGAwIBAgIJA00TbJmowFCMA0GCSqGSIb3DQEBBQUAMIGHMS0wKwYD
VQ0DEyRCZwnaWfuIFrydXN0ZWQgTGlzdCBTY2hlLWUgT3BlcmF0b3IuSTBHBGNV
BAoTQEZQUyBfY29ub215LCBTUUVzLlCBTZWxMLWVtcGxveWVkaGFuZCBFbWVz3kg
LSBRdWfsaXR5IGFvZCBTYWZldHkxZzAJBgNVBAYTAkFMB4XDTE0MDIxOTZzMzcx
NVoXDTI0MDIxNzEzMzcxNVoYcXkLTAoBqNVBAMTJEJlbgGpYw4gVHJlc3RlZCBB
aXN0IFNjaGVtZSBBPcGVyYXRvcjFJMEcGA1UECHNARlBTEVYj25vbXksIFNNRXMs
IFNlbnV0eWVzZW0wZjZlY29ub215LWVzLWVzLWVzLWVzLWVzLWVzLWVzLWVzLWVz
MAkGA1UEBhMCQlUwggEiMA0GCSqGSIb3DQEBBQUAA4IBDwAwggEKAoIBAQQDAgEFk
oDPTYDvGk+/IPnGSPm58NRE7mpzLHk8LxpYnTAtbMhn7Fwru9GLNi+bLYYNOEmzN
2E5K09+7AAAMmx2x8zmEMwc3oUQ7E0WN5GL+Y+7n6NtX50D/4Sbw4IjVvwRRru8
Coj5vq5Hz3JKTgft8teEpwb5vSFZn6+o9irdX342RJU4AtG78sxZvzIqpa3WsdDM
f5XdyjnGK3dRgkDu0aBxwEexuUIN4LVO+MacwoaxEqLhEz6TALGWS2WmNEW30LUD
f7nc0Tz/lnyQsuFn01c4pg56hjyxLtpjYHwNwbTDx+cjBpBveOT9Nb6UfKfHKnC5
Afr10WnFLXUmykD/AqMBAAGjTDBKMAKGA1UdEwQCAAwCwYDVR0PBAQDAgBAMB0G
A1UdDgQWBRRf745pxFv011rxBwg0UhLQqteOUTARBgNVHSUECjAIBgYEAJJE3AwAw
DQYJKoZIhvcNAQEFBQADggEBAG8j1gOIKEKTD904EepYs1MioBERjXxkAN2zvaZe
vh3awKB6cGeQUnmDz3ve4ZCJSB4MZ138EKUj2eobXaPyaL01vL6sM6eUj6QhwNv
fGXHP99A0HG8ZyH4IkjgB+8jImhg2danj4vCAosGtvTknYtZ2K+GhRevGAno r y h J
7A7j s z w z a a h F w T n u n y m L B X l r w G 9 K y B S k g 4 I h W g c + I g Y U g A 7 r p 0 Z 6 z X F P T J Q j p h i
R g 7 p Q E C n V 1 F v w 9 e d i M G h B n L 3 t e / 5 I K I u g 2 X o J 3 M L h 9 L h o 6 c 8 Y A h y p 2 Q 1 6 i n C L D J
k s Z c 1 q U r H o 9 l m w n G A N w f Z v Q W R J S 0 L J v r F 7 L S L 5 H / Y 4 y Z o =
-----END CERTIFICATE-----
```

*The public key in PEM format:*

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAACQ8AMIIBCgKCAQEAWIBBZKAz02A7xpVvyD5x
kj5ufDUR05qcyx5PJcaWJ0wLWzIZ+XVq7vRpTYvm5WGDThJszdhOSjvfuwAADJsd
sfm5hDMHN6FE0XNFjeRpfmPu5+jbV+dA/+Em80CI1b8MEUa7vAqI+b6uR89ySk4H
7fLxhKcG+b0hWYevqPYq3V9+NkSVOALRu/LMwb8yKqWt1rHXTH+Vw8o5xi.t3UYJA
7jmgcVhHsblIjeC7zvzGnMKGsRK14RGeKwCx1ktlpjRFtZpVHX+53NE8/5Z8kLLh
Z9NXOKY0eoY8s57aY8h8DcG0w8fnIwaQb3jk/Tw+LHyhR5JwuQH6yD1pxS11Jsisg
/wIDAQAB
-----END PUBLIC KEY-----
```