#### Scheme name

BE:Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

### Legal Notice

The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for Belgium is Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in Belgian laws. The applicable legal national framework is the Belgian CSP act of 9 July 2001 to create a legal framework for the usage of electronic signatures and certification services.

Scheme territory

Scheme status **EUappropriate** 

determination approach

Scheme type http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon community rules

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/BE

Issue date 2014-10-09T00:00:00.000Z Next update 2015-02-23T00:00:00.000Z

Historical information 65535 days

period

Sequence number 19

Scheme information

http://tsl.belgium.be/

## Scheme Operator

FPS Economy, SMEs, Self-employed and Energy - Quality and Safety Scheme operator

name

Scheme operator NG III - Koning Albert II-laan 16

street address

1000 Scheme operator

postal code

Brussels Scheme operator

locality

Brussels Scheme operator

state

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

Certipost s.a./n.v.

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

Brussels

locality

Service provider state Brussels

Service provider country

BE

## CN=Belgium Root CA, C=BE

*Type* CA/QC

Status undersupervision

2003-01-26T23:00:00.000Z Status starting time

## Service digital identity (X509)

Version

Serial number 117029288888937864350596520176844645968

Signature algorithm SHA1withRSA

CN=Belgium Root CA, C=BE Issuer Mon Jan 27 00:00:00 CET 2003 Valid from Valid to Mon Jan 27 00:00:00 CET 2014 CN=Belgium Root CA, C=BE Subject Public key Sun RSA public key, 2048 bits

modulus:

2532727247174242475310876111302551541350771290487408393990707355 3139389403581555633427000903307438065008396155423372038139338001 12922839738743756616914614756910113215373514757637257855001524459884908283374968661826239871065222401938973133495715806769163244  $\frac{2561241462450868417538609485432931629806056877222374520561111218}{9904505418533484099385023144445138975351025575749503679547226381}$ 90266507753545893758022556650119414854675563337473296025894960416159860774175448506963241118776049541934983183035608916277217984

30948172071644141969017225065301229219951

public exponent: 65537

Subject key identifier 10f00c569b61ea573ab635976d9fddb9148edbe6 Authority key

10f00c569b61ea573ab635976d9fddb9148edbe6

identifier

Key usage keyCertSign

cRLSign

Basic constraints CA=true; PathLen=unlimited

SHA1 Thumbprint dfdfac8947bdf75264a9233ac10ee3d12833dacc

SHA256 Thumbprint 7c7ed4240bb253bb35c376e12e00b027f1659df9d8267422a93eed75edc7adfb

## Scheme Service Definition URI

en http://tsl.belgium.be/pages/SchemeServiceDefinition

#### Qualifications

Object Signing CA]

Qualifier: QCSSCDStatusAsInCert

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

```
RootCA-QC
The decoded certificate:
Subject: CN=Belgium Root CA. C=BF
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5
Key: Sun RSA public key, 2048 bits
5763725785500152445988490823374968661826239871065222401938973133495715806769163244256124146245086841753860948543293162980605687722237452056111121899045054185334840993850231
77417544850696324111877604954193498318303560891627721798430948172071644141969017225065301229219951
public exponent: 65537
Validity: [From: Mon Jan 27 00:00:00 CET 2003
          To: Mon Jan 27 00:00:00 CET 2014]
Issuer: CN=Belgium Root CA, C=BE
              580b056c 5324dbb2 5057185f f9e5a650
SerialNumber: [
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
CA:true
PathLen: 2147483647
[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [2.16.56.1.1.1]
[PolicvOualifierInfo: [
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
]] ]
[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 [
 S/MIME CA
```

```
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKevIdentifier [
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.
                                                    .....j.k*.YH.LI
0010: DC A3 16 00 DA CD 6A E7
                             6B 2A FA 59 48 A7 4C 49
0020: 37 D7 73 A1 6A 01 65 5E
                             32 BD E7 97 D3 D0 2E 3C 7.s.j.e^2.....<
                             C1 3F A8 A9 5D 0F 37 BA s.....B.?..].7.
0030: 73 D3 8C 7B 83 EF D6 42
                             44 41 49 9C FD 5B 29 F4 v.@..-?.DAI..[).
0040: 76 D2 40 BD CC 2D 3F D3
0050: 02 23 22 5B 71 1B BE 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
                             1D DC E3 D0 63 1E 3D 71 .W.z.j.....c.=q
0080: F6 57 2F 7A 7F 6A 13 80
                             F0 94 C7 48 75 54 81 F3 1.`.....HuT..
0090: 31 B1 60 D4 9E 08 CA AB
                             83 AC 8F 34 6B E8 BF C3 ..w.....4k...
00A0: 1B AD 77 9C E8 B2 8F DB
00B0: D9 F5 43 C3 64 55 FB 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.
```

#### The certificate in PEM format:

----BEGIN CERTIFICATE-

 ${\tt MIIDlDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBgkqhkiG9w0BAQUFADAnMarket} \\$ MOswCOYDVOOGEwJCRTEYMBYGA1UEAxMPOmVsZ2l1bSBSb290IENBMB4XDTAzMDEv NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowJzELMAkGA1UEBhMCQkUxGDAWBgNVBAMT D0JlbGdpdW0gUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB AMihcekcRkJ5eHFvna6pqKsot03HI0swkVp19eLSz8hMFJhCWK3HEcVAQGpa+XQS J4fpn0VxTiIs0RIYqjBeoiG52bv/9nTrMQHn035YD5EWTXaJqAFPrSJmcPpLHZXB MFjqvNll2Jq0i0tJRlLf0lMVdssUXRlJsW9q09P9vMIt7EU/CT9YvvzU7wCMgTVy v/cY6pZifSsofxVsY9LKyn0FrMhtB20yvmi4BUCuVJhWPmbxM0jvxKuTXgfeMo8S dKpbNCNUwOpszv42kqgJF+qhLc9s44Qd3ocuMws8d0IhUDiVLlzg5cYx+dtA+mqh VROTAOH/BAUWAWEB/zBCBqNVHSAEOzA5MDcGBWA4A0EBMC4wLAYIKwYBBOUHAqEW IGh0dHA6Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBQQ8AxW  $\verb|m2HqVzq2NZdtn925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU| \\$ EPAMVpth6lc6tiWXbZ/duRS02+YwD0YJKoZIhvcNA0EFB0ADagEBAMhtIlGKYfgP lm7VILKB+MbcoxYA2s1q52sq+llIp0xJN9dzoWoBZV4yveeX09AuPHPTjHuD79ZC wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0AiMiW3Ebv1jZKE4tRfTa57VjRUQRDSp/ M382SbT0bgkCMa5c/ciJv0J71/Fg8teH9lcuen5gE4Ad30P0Yx49cTGxYNSeCMgr 8JTHSHVUgfMbrXec6LKP240sjzRr6L/D2fVDw2RV6xq9NoY2uiGMlxoh10ot06y6 7 Kcdq 765 Sps1 LxxcHVGnH1TtEpf/8m6HfUbJdNbv6z195lluBpQE5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQE5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQE5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQE5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQe5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQe5KJVhzgoaiJender Sps1 LxxcHVfUbJdNbv6z195lluBpQe5KJVhzgoaiJender Sps1 Lxxc4r50ErAE0vo

----END CERTIFICATE----

## CN=Belgium Root CA2, C=BE

Type CA/QC

Status undersupervision

Status starting time 2007-10-04T10:00:00.000Z

## Service digital identity (X509)

Version 3

Serial number 3098404661496965511

Signature algorithm SHA1withRSA

Issuer CN=Belgium Root CA2, C=BE
Valid from Thu Oct 04 12:00:00 CEST 2007
Valid to Wed Dec 15 09:00:00 CET 2021
Subject CN=Belgium Root CA2, C=BE

Public key Sun RSA public key, 2048 bits

modulus:

2505202035897286929802442931365977782136110157856742564234839581 64367953802839672248769831300340203168205752163553604166050045334718830407023741150537135469000352360279650474826843696574001315 552436395329655960576829372646274868386780797947622304693692109500887975787577283413392923336546545109817976430306701793579151565262158435123606358334230710497624432217765218126527057253528859 3688668361490384043063624052887014382463758810568004079588144865 4643858460532713400822409146679502714797245542101554942867836639 3080491585356622044306227220916440412947986826263456222477031966

11536459503012648921426461410998536799349

public exponent: 65537

Subject key identifier 858aebf4c5bbbe0e590394ded6800115e3109c39 858aebf4c5bbbe0e590394ded6800115e3109c39

Authority key identifier

Key usage keyCertSign

cRLSign

CA=true; PathLen=unlimited Basic constraints

SHA1 Thumbprint 51cca0710af7733d34acdc1945099f435c7fc59f

SHA256 Thumbprint 9f9744463be13714754e1a3becf98c08cc205e4ab32028f4e2830c4a1b2775b8

## Scheme Service Definition URI

http://tsl.belgium.be/pages/SchemeServiceDefinition

## Qualifications

Qualifier: QCSSCDStatusAsInCert

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

[2]: ObjectId: 2.5.29.19 Criticality=true

BasicConstraints:[ CA:true

#### RootCA-QC

```
The decoded certificate:
Subject: CN=Belgium Root CA2, C=BE
Signature Algorithm: SHAlwithRSA, OID = 1.2.840.113549.1.1.5
Key: Sun RSA public key, 2048 bits
modulus:
10497624432217765218126527057253528859368866836149038404306362405288701438246375881056800407958814486546438584605327134008224091466795027147972455421015549428678366393080491
public exponent: 65537
Validity: [From: Thu Oct 04 12:00:00 CEST 2007,
        To: Wed Dec 15 09:00:00 CET 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
```

```
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.
11 1
[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
Kev CertSian
Crl_Sign
[5]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
 SSI CA
 S/MIME CA
 Object Signing CA]
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KevIdentifier [
0000: 85 8A EB F4 C5 BB BE 0E 59 03 94 DE D6 80 01 15 ......Y.....
Algorithm: [SHA1withRSA]
Signature:
0010: F3 4A 01 0C 74 BF 2B B3
0020: 1C B3 33 AF CE E5 13 01
0030: CC 14 92 6B 74 16 8A 96
                               E8 51 EF BF FA 4A 25 A7 ...kt....Q...J%.
                               CF 11 72 B6 1E B9 39 41 ..c+].X...r...9A
DE 8E 0E CD A9 95 77 25 .M).5S......%
0040: 89 B6 63 2B 5D 94 58 D1
0050: 16 4D 29 BC 35 53 0B DA
0060: CA 94 5A E9 B2 69 AE D8
                               CO 13 BE 98 FC 96 9C 84
                               20 A4 A4 36 68 6B 4D 60 .U..<....6hkM<sup>2</sup>
2E B9 41 8A D3 65 D3 84 f.....f..A..e..
0070: 7F 55 13 E6 3C 87 E3 BC
0080: 66 1C F9 BF AC 80 94 66
0090: 80 02 EF 50 1D 5E 46 DC
                               F7 C9 BA B5 34 7C 2A F3 ...P.^F....4.*.
                               CD 11 E7 FD 14 02 83 66 ..__T..M......f
CE 14 FE BB 1F A7 61 F7 ^...._a.
00A0: C6 D8 5F 5F 54 9D DB 4D
00B0: 5E C8 A6 00 12 A0 5F BE
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
00F0: 46 6E 14 5D 5E 47 53 8D 78 4D E0 27 BB 8E 85 76 Fn.]^GS.xM.'...v
```

#### The certificate in PEM format:

----BEGIN CERTIFICATE---

MIIDjjCCAnagAwIBAgIIKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTIwHhcNMDcxMDA0MTAwMDAw WhcNMjExMjE1MDgwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1 bSBSb290IENBMiCCASIwDOYJKoZIhvcNAOEBBOADagEPADCCAOoCagEBAMZzOh6S /3UPi790hqc/7bIYLS2X+an7mEoj39WN4IzGMhwWLQdC1i22bi+n9fzGhYJdld61  ${\tt IgDMqFNAn68KNaJ6x+HK92AQZw6nUHMXU5WfIp8MXW+2QbyM69odRr2nlL/zGsvU}$ +400HiPIltfsiFPekx40HopOcSZYtF3CiInaYNKJIT/e1wEYNm7hLHADBGXvmAYr XR5i3FVr/mZkIV/4L+HXmymvb82fqgxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y HewApDgglVrH1Tdjuk+bqv5WRi5j2Qsj1Yr6tSPwiRuhFA0m2kHw0I8w7QUmecFLine American AmeriTaG4flVSOmlGhHUCAwEAAaOBuzCBuDAOBaNVHO8BAf8EBAMCAOYwDwYDVR0TAOH/ BAUWAWEB/zBCBgNVHSAE0zA5MDcGBWA4CQEBMC4wLAYIKwYBBQUHAgEWIGh0dHA6  ${\tt Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBSFiuv0xbu+DlkD}$ lN7WgAEV4xCcOTARBglahkaBhvhCAOEEBAMCAAcwHwYDVR0iBBgwFoAUhYrr9MW7 vg5ZA5Te1oABFeMQnDkwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyCc UwnzSgEMdL8rs5qauhjyC4isHLMzr87lEwEnkoRYmhC598wUkmt0FoqW6FHvv/pK JaeJtmMrXZRY0c8RcrYeuTlBFk0pvDVTC9reig7NgZV3JcgUWumvaa7YwB0+mPvW nIR/VRPmPIfjvCCkpDZoa01gZhz5v6yAlGYuuUGK02XThIAC71AdXkbc98m6tTR8 KvPG2F9fVJ3bTc0R5/0UAoNmXsimABKgX770FP67H6dh96tK8QYUn8pJQsKpv02F sauBQeYNxUJpU4c5nUwfAA4+Bw11V0SoU7Q2dmSZ3G7rPUZuFF1eR10NeE3gJ7u0 ----END CERTIFICATE----

## CN=Belgium Root CA3, C=BE

Type CA/QC
Status undersupervision
Status starting time 2013-06-26T12:00:00.000Z

## Service digital identity (X509)

Version 3

Serial number 4260689877497748905

Signature algorithm SHA1withRSA

IssuerCN=Belgium Root CA3, C=BEValid fromWed Jun 26 14:00:00 CEST 2013Valid toFri Jan 28 13:00:00 CET 2028SubjectCN=Belgium Root CA3, C=BEPublic keySun RSA public key, 4096 bits

modulus:

7489331012499470148015728120971091408928778599011263917331397388 7322735841404218927092481342245128960306942910996978037963366658 7487677438166762048712847334427499268969797276699412687279269161 40047703870440923312804390402229289779018765142954206284872356057207547181546555365474067211993745122880348947938978158987337436 1336080842299846657331444909264877243429847318212868757946477794 3923944626874903980284954943444633165097044418808053302806567480 3973101653181735709840274950639311977298375764568509245075873047 97255602129815800963894248447037937123270920368663080351919425068313464980278629369152701697759736384202776541620591588545291932 466321499552953337556325973237815480592810613680950380979980022929206175039044753321633938140477949569594213821975729473102508366454723047943333937457964148701121644586439773493445613256431505451689600807046471898622121897269823517896969688074733205559734650561444823679292519060900635654581417970980552285817902789069514772158596504768735853434600634865427052445967408799471479389419 0325164983453802445254424012949618662017893008747941892318218022

78084190173776931 public exponent: 65537

 Subject key identifier
 b8bc6c008f5b19859d25019cf019dc408ed0382b

 Authority key
 b8bc6c008f5b19859d25019cf019dc408ed0382b

identifier

Key usage keyCertSign

cRLSign

Basic constraints CA=true; PathLen=unlimited

SHA1 Thumbprint fd6b835c99b99e6ff84fcd0e6266a3610786a717

SHA256 Thumbprint a8d14e945e3e5156bcae5e39737cf6a1b1f51028bbbf982f50ce5f4c05568b4d

## Scheme Service Definition URI

en http://tsl.belgium.be/pages/SchemeServiceDefinition

#### Qualifications

Qualifier: QCSSCDStatusAsInCert

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

#### RootCA-QC

```
The decoded certificate:
Version: V3
 ubject: CN=Belgium Root CA3, C=BE
Signature Algorithm: SHAlwithRSA, OID = 1.2.840.113549.1.1.5
    Sun RSA public key, 4096 bits
modulus:
40222928977901876514295420628487235665720754718154655536547406721199374512288034894793897815898733743613360808422998466573314449092648772434298473182128687579464777943923944
29251906090063565458141797098055228581790278906951477215859650476873585343460063486542705244596740879947147938941903251649834538024452544240129496186620178930087479418923182
1802278084190173776931
public exponent: 65537
Validity: [From: Wed Jun 26 14:00:00 CEST 2013,
          To: Fri Jan 28 13:00:00 CET 2028]
Issuer: CN=Belgium Root CA3, C=BE
SerialNumber: [ 3b2102de 965b1da9]
Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
[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]
[PolicvOualifierInfo: [
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
]] ]
[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 [
 S/MIME CA
 Object Signing CA]
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0010: 8E D0 38 2B
Algorithm: [SHA1withRSA]
Signature:
                       CC B1 11 A7 1C 92 0C 78 Eb;....U.....x
0010: 2F C5 EF 16 42 05 3D 7C 0020: 13 94 FE 4E 67 D6 38 D5
                       E3 12 70 E7 02 D0 82 91 /...B.=...p.....
2B E3 83 3A 7F 90 E2 42 ...Ng.8.+.....B
35 DC AD 27 B5 B4 1D A0 `...+...5..'...
0030: 60 E8 D7 7B 2B 8E FE CD
                       0040: 54 CB 32 68 23 7D B1 CC
0050: C4 E1 0A 35 2D A2 8C 5F
0060: 07 71 43 C2 62 50 12 4C
                       26 A9 65 4D 0C 9C 06 F3 .qC.bP.L&.eM...
0070: 7E 9C F1 9B 8F 48 93 F0
                       36 25 6C 40 87 15 D5 44 .....H..6%l@...D
0080: 7C 0E BB 74 CC 1A 24 38
                       5B F5 72 55 AC 31 8F 04 ...t..$8[.rU.1..
0090: 0C 3B C4 E7 78 10 E8 99
                       B9 A4 5E C2 3D 6C 8D 0E
                                         .;..x....^.=l..
00A0: C5 65 21 D8 0E 5D 2A 5A
                       AE D2 C6 2F 13 47 73 F3 .e!..]*Z.../.Gs.
                       70 F2 0A 8B 30 99 95 A3 ....d...p...0...
00B0: 10 F1 AF D6 64 99 9A 98
00C0: F5 66 C4 A5 0A 2E 52 DF
                       58 27 DC 45 0F F9 F7 76 .f...R.X'.E...v
                       EA 82 88 7F D1 45 1A 1D ...^.>.0....E..
61 CD 88 41 9D 97 8E 19 .^t.../.a..A....
00D0: D6 AE 99 5E 05 3E E7 4F
00E0: 1A 5E 74 F4 01 11 2F C5
00F0: 9E 4F 03 3E F4 B9 3B B6
                       7C C7 78 7A 77 76 00 A8
                                         .0.>..;...xzwv..
```

A2 5C C5 9C 34 0B EF 90 9.....VE.\..4...

0100: 39 F7 1E C8 F5 1A 56 45

```
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
0130: 47 07 56 13 C8 0F BD B7
                               D6 35 04 02 F0 C2 6A B8 G.V.....5...j.
0140: 39 79 1D D7 AE CD 47 AC
                               4D 75 2A 5D E1 24 C8 03 9y....G.Mu*].$..
0150: A8 E9 89 C5 DE 0D 2A 19
                               C2 C8 F4 D5 EE B2 38 B5
0160: 7A 04 54 67 B0 78 5C 2B
                               C6 E7 69 53 07 B5 A0 77 z.Tg.x\+..iS...w
                               99 84 C6 25 71 FE 37 F9
0170: FC 15 17 34 B7 7F 89 80
                                                       ...4.....%q.7.
0180: 6B 04 11 8A B9 32 79 5E
                               77 09 6A 58 85 50 AC 46
                                                       k....2y^w.jX.P.F
0190: 3F A5 66 37 26 9A 2D 41
                               79 22 54 EA 0B D0 86 1C ?.f7&.-Ay"T....
01A0: F2 D2 5C E8 03 A2 4B 76
                               1B DA 4D C0 59 B6 B7 B0 ..\...Kv..M.Y...
01B0: 1C A7 00 26 7A 09 0C 36
                               98 1C 81 37 7E AA 4D B2
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....
01F0: 2E B6 3E 33 EC 5E 21 CB
                               6B 0B 45 A7 3F BB B8 C6 ...>3.^!.k.E.?...
```

#### The certificate in PEM format:

---BEGIN CERTIFICATE----

MIIFjjCCA3agAwIBAgIIOyEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTMwHhcNMTMwNjI2MTIwMDA WhcNMigwMTI4MTIwMDAwWiAoMOswCOYDVOOGEwJCRTEZMBcGA1UEAxMOOmVsZ2l1 bSBSb290IENBMzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKjyAZ2L g8kHoIX7JLc3BeZ1Tzy9MEv7Bnr59xcJezc/xJJd04V3bwMltKFfNvqsQ5H/GQAD FJ0GmTLLPDI5AoeUiBubRZ9hwruUu011+vhtoVhuEuZUxofEIU2vJtiS00Nwpo/G Ib9C4YZ5h+7ltDpC3MvsFyyordpzgwqSHvFwTCmls5SpU05UbF7ZVPcfVf24A5Ig HLpZTgQfAvnzPlm++eJY+sNoNzTBoe6iZphmPbxuPNcJ6slV8qMQQk50/g+KmoPp HX4AvoTr4/7TMTvuK8iS1dEn+fdVKdx9go9ZZRHFW/TXEn5SrNUu99xhzlE/WBur rVwFoKCWCjm00CnekJlw0NTr3HBTG5D4AiDjNFUYaIcGJk/ha9rzHzY+WpGdoFZx hbP83ZGeoqkgBr8Uzf0FCY8cyUN2db6hpIaK6Nuoho6QWnn+TSNh5Hjui5miqpGx S73gYlT20ww16h8gFTJ049fiS+OHlwRw5cgFugfFLE3nFFF9KIamS4TSe7T4dNGY 2VbHzpaGVT4wy+fl7gWsfaUkvhM4b00DzgDiJ9BHiKytNLmzoa3Sneij/CKur0dJ 50dMiAqUpSd00e8pdIbmQmloP5cjckiQjxx7+vSxWtacpGowWK8+7oEsYc+7fLt3 GD6q/05Xi440Pd/sFJmfqRf3C1PPMdBqXcwjAgMBAAGjgbswgbgwDgYDVR0PAQH/ BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDsw0TA3BgVg0AoBATAuMCwG  ${\tt CCsGAQUFBwIBFiBodHRw0i8vcmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5iZTAdBgNVacables} \\$ H04EFq0UuLxsAI9bGYWdJ0Gc8Bnc0I700CswE0YJYIZIAYb40qEBBA0DAqAHMB8G A1UdIwQYMBaAFLi8bACPWxmFnSUBnPAZ3EC00DgrMA0GCSqGSIb3DQEBBQUAA4IC AQBFYjv/mKX+VcyxEacckgx4L8XvFkIFPXzjEnDnAtCCkR0U/k5n1jjVK+0D0n+Q 4kJg6Nd7K47+zTXcrSeltB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpdl f14HcUPCYlASTCapZU0MnAbzfpzxm49Ik/A2JWxAhxXVRHw0u3TMGiQ4W/VyVawx jwQM08TneBDombmkXsI9bI00xWUh2A5dKlqu0sYvE0dz8xDxr9ZkmZqYcPIKizCZlaP1ZsSlCi5S31gn3EUP+fd21g6ZXgU+50/ggoh/0UUaHRpedP0BES/FYc2I0Z2X jhmeTwM+9Lk7tnzHeHp3dgCo0fceyPUaVkWiXMWcNAvvkDVELvXfJpRxwcRfS5Ks 5oaf0fj81RzGUbmpwl2us0eCRwdWE8gPvbfWNQQC8MJquDl5HdeuzUesTXUqXeEk vAOo6YnF3aOaGcLI9NXusiileaRUZ7B4XCvG52lTB7Wad/wVFzS3f4mAmYTGJXH+ N/lrBBGKuTJ5XncJaliFUKxGP6VmNyaaLUF5IlTqC9CGHPLSX0gDokt2G9pNwFm2 t7AcpwAmegkMNpgcgTd+qk2yljEaT8wf953jUAFedbpN3tX/3i+uvH00mWjQ0xJg 2lVKkC+bkWa2FrTBDdrlEWVaLrY+M+xeIctrC0WnP7u4xg= ----END CERTIFICATE----

## CN=Belgium Root CA4, C=BE

Type CA/QC

Status undersupervision

Status starting time 2013-06-26T12:00:00.000Z

## Service digital identity (X509)

Version 3

Serial number 5706940941790920504

Signature algorithm SHA256withRSA

Issuer CN=Belgium Root CA4, C=BE
Valid from Wed Jun 26 14:00:00 CEST 2013
Valid to Fri Jan 28 13:00:00 CET 2028
Subject CN=Belgium Root CA4, C=BE

Public key Sun RSA public key, 4096 bits

modulus:

6224115906824122031433393414467734255795749661242697041972796971 3589761663492552027516102528196645068474513261170454526640944182 035424569860936689008684747674264316825012182352256880531189580112777584272647405412565917749112449744105606362508900429786708823655369589600664996359169269749224840725363125898523192670130240 3094481995663975256487988599594079751375649124722315558398958459 8625577661561495707877863985269083424382019627610669355576767590 32874370869635418791859236500290465150832789179676475212375970097723059779987931314312946138958009529327069795639742850540854481 16681005880530871902042900046595950005402044763615671403742873845557572387796136829835237636572157056930341887317395041724077153 2738123406566311692859096140881485975714355900153034684151459890 4885138299612865991395755715162815883415449288903178308408884400 9310182142365979807396066210319470759450039107508536195377707761075688418384343286045715157573426989301124463242723093299927147162988283928766947013625480426811137103293454625262051881732832104879637264017398565292090224855096446539393723135313244013015486 7925044711328249031368163390477454073402140822040781939631335114 29055306278731837

public exponent: 65537

Authority key identifier

Subject key identifier 67e8f14e4fb3b5f3076f089c0c83d97ad95be749 67e8f14e4fb3b5f3076f089c0c83d97ad95be749

Kev usage keyCertSign

cRLSign

CA=true; PathLen=unlimited Basic constraints

SHA1 Thumbprint cd4186bcd938ca5c19610f74c762b23acf07a564

SHA256 Thumbprint c3fbf37259af0954eeea4282dd1c7226a54e7150f7c29a2c495ba34dbfe09ca0

## Scheme Service Definition URI

http://tsl.belgium.be/pages/SchemeServiceDefinition

## Qualifications

Qualifier: QCSSCDStatusAsInCert

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

RootCA-QC

The decoded certificate:

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:

697492248407253631258985231926701302403094481995663975256487988599594079751375649124722315558398958459862557766156149570787786398526908342438201962761066935557676759032874375883415449288903178308408884490931018214236597980739606621031947075945003910750853619537770776107568841838434328604571515757342698930112446324272309329992714716298828392876694701362548042681113710329345462526205188173283210487963726401739856529209022485509644653939372313531324401301548679250447113282490313681633904774540734021408220407819396313 3511429055306278731837

public exponent: 65537

```
Validity: [From: Wed Jun 26 14:00:00 CEST 2013,
             To: Fri Jan 28 13:00:00 CET 2028]
Issuer: CN=Belgium Root CA4, C=BE
                 4f33208c c594bf38]
SerialNumber: [
Certificate Extensions: 6
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KevIdentifier [
0000: 67 E8 F1 4E 4F B3 B5 F3 07 6F 08 9C 0C 83 D9 7A g..NO.....z
[2]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen: 2147483647
[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicvId: [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.
11 1
[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 [
 SSI CA
 S/MIME CA
 Object Signing CA]
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
Algorithm: [SHA256withRSA]
Signature:
0000: 25 89 3C AB 51 CB A6 8F D8 75 21 12 99 34 82 A5 %.<.Q....u!..4..
0020: AB 69 B2 F9 9F A1 99 AE
                             3F EE AB 49 B8 43 8B 52 .i....?..I.C.R
                              3C 31 1B 07 E4 88 F2 40 ....a._ <1....@
0030: 7D A5 F8 BB 61 CF 5F 20
0040: 89 10 65 D5 AC 5D B6 99
                             E4 A0 03 04 73 14 28 9C ..e..].....s.(.
                              42 A2 17 A5 BD 0E DF 86 ..2$....B......
0050: B9 F1 32 24 BA FE 7E A7
0060: 00 60 03 49 9F 92 EE 8D
                              DE 55 F4 8F A2 BF 9A EB . `.I....U...
                              01 DF 1E 9F 25 DA 55 6A .x.q.....%.Uj
0070: CD 78 EF 71 93 CD C6 01
                              83 B5 EA 11 8F 89 62 22
0080: 96 E8 92 18 2B 0E B8 35
                                                      ....+..5.....b
                              A9 4D DB D7 E8 07 3A 22 0...\..g.M....:
0090: 4F 9A FE DD 5C 8C E1 67
00A0: 93 5A 3A 5A 9E 14 9C 2E
                              14 B0 54 E0 C7 F8 4D E7 .Z:Z.....T...M.
                              1D 03 16 99 C0 B3 92 4D .#....I......M
00B0: A7 23 91 D5 CC 09 1F 49
00C0: 99 50 DD 92 3D 82 F5 E3
                              12 B7 74 21 C0 74 F7 25 .P..=....t!.t.%
00D0: 9A 35 68 51 26 68 C9 71
                              28 1C CD 78 15 3B D5 D4 .5hQ&h.q(..x.;..
                              D2 5F 4C F0 74 1A A5 55 .^.@...._L.t..U
00E0: E7 5E D5 40 89 07 F1 04
00F0: C8 52 14 A6 A8 ED 51 F8
                              0D D1 0F C7 2F 8C FF 4F .R....Q..../..0
                              EA 71 72 88 8F 5A 96 B3 .P..)..:.qr..Z..
0100: E4 50 E8 C4 29 9E 19 3A
                              EC 7C 92 4F 9F E8 33 E1 .,.vt.0....0..3.
0110: B8 2C AD 76 74 C8 30 AC
0120: 90 F4 E2 E1 53 DC 2B 1F
                              87 OC C1 6F OD B0 E4 72
                              61 13 E0 25 9A 3E 12 9B ...jz.Rm.a..%.>..
0130: 0A A6 6A 7A 08 52 6D DE
                              44 67 9B 7F 9A 3A AB E4
0140: 18 CF 86 DE E4 AE D4 17
                                                      ........Dg...:..
0150: 4B 1D 79 C5 0B 30 6D A8
                              97 80 E9 4E 80 A6 BD 52 K.y..0m....N...R
0160: AD 2B C4 A6 43 97 2C 85
                              6C DA 7B 7C A3 F6 29 02 .+..C.,.l....)
                              8E A7 E5 D1 45 12 E8 8B ....=....E...
0170: 85 0C C4 EA F0 3D 1C 1B
0180: CA 66 10 0B 78 CO 5E E8
                                                      .f..x.^.k....im
                              6B D7 A4 C8 93 AA 69 6D
                              40 BF 3B 84 DD 02 4C 3D k....%.@.;...L=
CD 45 5B CE 7B 90 D9 5B ...+:.`7.E[....[
0190: 6B B7 03 D7 7C 8A 25 00
01A0: 8D 17 02 2B 3A 09 60 37
01B0: 64 D0 C0 6D 95 01 1B FB
                              0D CE B1 48 78 78 88 3F d..m.....Hxx.?
                              5F 3B 39 25 98 1E E4 F7 .C.'..._;9%...
F2 0A 37 EF 0B 6A FC 0F ..]...U...7..j.
01C0: 02 43 8D 27 8F F6 E0 01
01D0: 7B 7B 5D AF D8 B9 55 9B
                                                     ..]...U...7..j..
01E0: 47 BC 58 9E 22 6B AE B1
                              F8 21 67 A1 14 F6 9B D4 G.X."k...!g....
01F0: 3E 62 FA D8 D3 D8 E7 88
                              3E 9C 59 B6 A8 CB 4C 59 >b.....>.Y...LY
```

The certificate in PEM format:

-BEGIN CERTIFICATE

MIIFjjCCA3agAwIBAgIITzMgjMWUvzgwDQYJKoZIhvcNAQELBQAwKDELMAkGA1UE BhMCOkUxGTAXBqNVBAMTEEJlbGdpdW0qUm9vdCBDOTOwHhcNMTMwNiI2MTIwMDAv WhcNMjgwMTI4MTIwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1bSBSb290IENBNDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJiQrvrH Hm+04AU6svN4TNHWL911PFsY6E9euwVml5NAWTdw9p2mcmE0YGx424iFLpS0VNxx xoh3LsIpdWUMRQfuiDqzvZx/4dCBaeKL/AMRJuL1d6wU73XKSkdDr5uH6H2Yf19z SiUOm2x4k3aNLyT+VryF11b1Prp67CBk630BmG0WUaB+ExtBH0kfPaHRHFA04Mig oVFt3gLQRGh1V+H1rm1hydTzd6zzpoJHp3ujWD4r4kLCrxVFV0QZ44usvAPlhKoe cF0feiKtegS1pS+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7MMpf8MEygX  $\label{lem:wmb+wrynTetWnIV6jTzZA1RmaZuqmIMDvWTA7JNkiDJQ0JBWQ3Ehp+Vn7li1MCIj to the control of the control of$ X1EDYJ2wRmcRZQ0bsUzaM/V3p+Q+j8S3osma3Pc6+dDzxL+0g/lnRnLlDapXx28X B9urUR5H030zm77B9/mYgIeM8Y1XntlCCELBeuJeEYJUqc0FsGxWNwjsBtRoZ4dv alrvzkXmjJuNIR4YILg8G4kKLhr9JDrtyCkvI9Xm8GDjqQIJ2KpQiJHBLJA0gKxl Yem8CSO/an3A0xqTNZjWbQx6E320PB/rsU28ldadi9c8yeRyXLWpUF4Ghjyoc40d rAkXmljnkzLMC459xGL8gj6LyNb6UzX0eYA9AgMBAAGjgbswgbgwDgYDVR0PAQH/ CCsGAQUFBwIBFiBodHRw0i8vcmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5iZTAdBgNV HQ4EFgQUZ+jxTk+ztfMHbwicDIPZetlb50kwEQYJYIZIAYb4QgEBBAQDAgAHMB8G  $\verb|AludIwQYMBaAFGfo8U5Ps7XzB28InAyD2XrZW+dJMA0GCSqGSIb3DQEBCwUAA4IC| \\$ AQAliTyrUcumj9h1IRKZNIKlt2hAyNW1jdkYz+fJ57PD0qtpsvmfoZmuP+6rSbhD ilJ9pfi7Yc9fIDwxGwfkiPJAiRBllaxdtpnkoAMEcxQonLnxMiS6/n6nQqIXpb00 YiJPmv7dXIzhZ6lN29foBzoik1o6Wp4UnC4UsFTgx/hN56cjkdXMCR9JHQMWmcCz kk2ZUN2SPYL14xK3dCHAdPclmjVoUSZoyXEoHM14FTvV10de1UCJB/EE019M8HQa pVXIUhSmq01R+A3RD8cvjP9P5FDoxCmeGTrqcXKIj1qWs7gsrXZ0yDCs7HyST5/o M+GQ90LhU9wrH4cMwW8Ns0RyCqZqeghSbd5hE+Almj4SmxjPht7krtQXRGebf5o6q+RLHXnFCzBtqJeA6U6Apr1SrSvEpk0XLIVs2nt8o/YpAoUMx0rwPRwbjqfl0UUS 6IvKZhALeMBe6GvXpMiTqmlta7cD13yKJQBAvzuE3QJMPY0XAis6CWA3zUVbznuQ 2Vtk0MBtlQEb+w3OsUh4eIg/Ak0NJ4/24AFf0zklmB7k93t7Xa/YuVWb8go37wtq /A9HvFieImuusfghZ6EU9pvUPmL62NPY54g+nFm2qMtMWQ= ----END CERTIFICATE--

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

*Type* CA/OC

**Status** undersupervision

Status starting time 2012-01-11T19:45:06.000Z

## Service digital identity (X509)

Version Serial number 904

Signature algorithm SHA256withRSA

Issuer CN=Verizon Global Root CA, OU=OmniRoot, O=Verizon Business, C=US

Valid from Wed Jan 11 20:45:06 CET 2012 Valid to Tue Jan 11 20:44:34 CET 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 66540746196877065650295836633402647702698567201014894473503415489667917131633966990337885540161539197154038478640639231113106791 3663589486493118066042504737642498346914368670309047269922309076 6138772412256664686136790625895780242652401177074998149327839849

23682396679386042809154363424543342942381

public exponent: 65537

Subject key identifier 0e3733c7286ebfce5fe62ae698908bacc1e62844

CRL distribution

http://cdp1.public-trust.com/CRL/Omniroot2034.crl points

4c3811b898005b5a2b703eaa78e4d5676767a77e Authority key

identifier

Key usage keyCertSign cRLSign

Basic constraints CA=true; PathLen=0

SHA1 Thumbprint 05e88c57c47c3b510aed61a8c9d427ffe2925c01

4671a19c0fb1e221aeda10c7d745b7e5bf4faaffafc63fc2e2f8add187adab69SHA256 Thumbprint

```
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
public exponent: 65537
Validity: [From: Wed Jan 11 20:45:06 CET 2012,
          To: Tue Jan 11 20:44:34 CET 2022]
Issuer: CN=Verizon Global Root CA, OU=OmniRoot, O=Verizon Business, C=US
SerialNumber: [
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
[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 7F 63 65 .$https://www.ce
0010: 72 74 69 70 6F 73 74 2E 63 6F 6D 2F 73 68 6F 77 rtipost.com/show
0020: 70 6F 6C 69 63 79
]] ]
[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSigr
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
Algorithm: [SHA256withRSA]
Signature:
                         48 53 1E 3E 0A 88 33 07 s.W...4.HS.>..3.
0000: 73 F0 57 07 07 F3 34 DE
0010: 6C 55 49 D2 75 85 54 92
                         F2 80 19 1C 86 5D D7 F4 \UI.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
                         21 AC 5B 2C 0D C9 7C 35
0040: A0 AA EB 8D 42 18 10 E1
                                             ....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
                         AE 3F 46 13 DC AB 56 55 o...eI`g.?F...VU
0070: 6F B9 FA 9D 65 49 60 67
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
00A0: FA 68 94 BC 1E 30 5C F3
                         72 CD 51 A1 2F F4 08 9F 3.b...5r.Q./...
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
```

```
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..7.H.....
```

]

#### The certificate in PEM format:

----BEGIN CERTIFICATE----

 ${\tt MIIELTCCAxWgAwIBAgICA4gwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx}$ GTAXBqNVBAoMEFZlcml6b24qOnVzaW5lc3MxETAPBqNVBAsMCE9tbmlSb290MR8v HOYDVOODDBZWZXJpem9uIEdsb2JhbCBSb290IENBMB4XDTEvMDExMTE5NDUwNloX  ${\tt DTIyMDExMTE5NDQzNFowYjELMAkGA1UEBhMCQkUxHDAaBgNVBAoTE0NlcnRpcG9zerout} \\$ dCBuLnYuL3MuYS4xNTAzBqNVBAMTLENlcnRpcG9zdCB0dWJsaWMq00EqZm9vIFF1 YWxpZmllZCBTaWduYXR1cmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  ${\tt AQEAow3rmuZKZMnGhQRGeEzZK4THeq59CIqK6BseSxLmZ3sh8znY0FBNK40XmFEj}$ 0Y990nIvAJxnU5bcvSSBF0KPwtD5cFcmpcvP7BR0i6/MvJCE6BMD8wcS61CJfLlm 8/p/VRF9KsDfa6fMd/Wlghbq780wa22+UgXpFr27eqBCsUzEiZya5cILWXM0hmP+ ZE30i7pLZ/Dh+50tn/R+P0IVBBIypiycnx/u4Q/loEqMyy+DFliuMfCbCpE2Pbwz 0R+SCalFNeR09dlfmJ5XlpSr5K7dKXJP8DaoMw8Cu5fGLU8z2awax+3Zv0XdxDNF e2g8HHX4WdMymhSzbmnLjGVYrQIDAQABo4HyMIHvMBIGA1UdEwEB/wQIMAYBAf8C AQAwRQYDVR0gBD4wPDA6BgRVHSAAMDIwMAYIKwYBBQUHAgEWJGh0dHBz0i8vd3d3 LmNlcnRpcG9zdC5ib20vc2hvd3BvbGlieTA0BqNVH08BAf8EBAMCA0YwHwYDVR0i BBgwFoAUTDgRuJgAWlorcD6qe0TVZ2dnp34wQgYDVR0fBDsw0TA3oDWgM4YxaHR0 cDovL2NkcDEucHVibGljLXRydXN0LmNvbS9DUkwvT21uaXJvb3QyMDM0LmNybDAd BgNVHQ4EFgQUDjczxyhuv85f5irmmJCLrMHmKEQwDQYJKoZIhvcNAQELBQADggEB AHPwVwcH8zTeSFMePgqIMwdsVUnSdYVUkvKAGRyGXdf0EDUYMaw1+I1LD21mSxVM  ${\it KJESeDvEs0JlqERGohCM9jigquuNQhgQ4SGsWywNyXw1atIMfp2D7FsiNrTcry3y} \\$ h2v5fxZ3CyV7o2ZSS+pEvFhvufqdZUlgZ64/RhPcq1ZV74asJuNBRZ7S6IF3PxzA KDN9Ytp8vJw1cs1RoS/0CJ/6aJS8HjBc863Rj39SscL/zZW+KanvLvvDafCCJ/FN uaA80VYjHWHsnk1ZjFWBWlpibJNzIVr2UoSKr5cBln60eYCRpeIrexknt5opr6Mn ciipCXObk6c/4EiPnrWYivg= ----END CERTIFICATE----

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

Type CA/QC

Status undersupervision

Status starting time 2005-07-26T10:00:00.000Z

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 12:00:00 CEST 2005

 Valid to
 Sun Jul 26 12:00:00 CEST 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

## Qualifications

Qualifier: QCForLegalPerson

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

RootCA-QC

0060: 17 CD 27 01 B3 63 12 05

```
The decoded certificate:
Version: V3
Subject: CN=Certipost E-Trust Primary Qualified CA, Q=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
21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524
39229874921930931967759335049019790482801757213056181588775191965365993248162094887390232254090353829320174804654449299032182277693346689585304048115718426896010472819175682
public exponent: 65537
 Validity: [From: Tue Jul 26 12:00:00 CEST 2005,
           To: Sun Jul 26 12:00:00 CEST 2020]
Issuer: CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
                04000000 00010552 64c425]
SerialNumber: [
Certificate Extensions: 5
[1]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen: 2147483647
[2]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [0.3.2062.7.1.0.1.2.0]
[PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.1
qualifier: 0000: 16 22 68 74 74 70 3A 2F 2F 77 77 77 2E 65 2D 74 ."http://www.e-t
0010: 72 75 73 74 2E 62 65 2F 43 50 53 2F 51 4E 63 65 rust.be/CPS/QNce
0020: 72 74 73 20
11 1
[3]: ObjectId: 2.5.29.15 Criticality=true
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 [
0010: C6 34 F8 17
Algorithm: [SHAlwithRSA]
Signature:
0000: 6C E1 D8 5F 74 58 E9 70
                          49 D6 CA 0D 2C 58 DA CA l.
0010: 64 B6 51 4F C3 06 64 01
                          E9 8A 73 1D 9E CF 46 78 d.QO..d...s...Fx
0020: BF 3B 85 86 E2 3D 4A 18
                          94 2A 81 77 6F 82 F8 6F .;...=J..*.wo..o
0030: F4 EE 22 FC 9D 18 21 72
                          60 BB 18 80 82 95 FB F9 .."...!r`....
0040: F7 95 24 81 66 C1 B5 C3
                          B5 D2 B6 76 8B 3B 81 5C ...$.f.....v.;.\
0050: B8 A1 0E 2B 01 14 8B 80
                          09 40 EE F8 60 4C 19 E4 ...+....@..`L.
```

A4 08 C9 B4 BF 9E 50 4E ..'..c.....PN

```
....3fu.=.#..%q.
0080: FE 3E 2E 36 79 A1 E5 29
                               50 23 35 05 95 78 BB 9F
                                                        .>.6y..)P#5..x.
                               5C 33 CD C2 BB 7E 68 77 yd.WH',.\3....hw
0090: 79 64 DC 57 48 27 2C E2
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.....
                                                       ...*.z4lsI....k
00E0: DB 90 A9 2A E2 7A 34 6C
                               73 49 F4 E8 8D 2E 6B 8A
00F0: DD A1 8A 7F 63 D0 BF 58
                               1E AF CC 3F 92 50 2D D1 ....c..X...?.P-.
```

#### The certificate in PEM format:

----BEGIN CERTIFICATE----

MIID3jCCAsagAwIBAgILBAAAAAABBVJkxCUwDQYJKoZIhvcNAQEFBQAwXDELMAkG  $\verb|A1UEBhMCQkUxHDAaBgNVBAoTE0NlcnRpcG9zdCBzLmEuL24udi4xLzAtBgNVBAMT| \\$ JkNlcnRpcG9zdCBFLVRydXN0IFByaW1hcnkgUXVhbGlmaWVkIENBMB4XDTA1MDcy NjEwMDAwMFoXDTIwMDcyNjEwMDAwMFowXDELMAkGA1UEBhMCQkUxHDAaBgNVBAoT E0NlcnRpcG9zdCBzLmEuL24udi4xLzAtBgNVBAMTJkNlcnRpcG9zdCBFLVRydXN0 IFBvaW1hcnkgUXVhbGlmaWVkIENBMIIBIiANBgkghkiG9w0BA0EFAA0CA08AMIIB CgKCAQEAriDSeNuaoHKcBFIlLG1S2NcniT0g4bLV+zB1ay1/HGe0DucfEt8XeRi7 tBtv+D11G55nN/Dx+g917YadAwShKHAtPLJroHNR4zWpdKUIPpSFJzYqqnJk/Hfu dpQccuu/Msd3A2olggkFr19gPH+sG7yS6Dx0Wc7xfFQt0K6W8KxvoTMMIVoBuiMg W6CGAtVT3EkfqDKzrztG07bvnzmz0Avneor2KPmnb1ApyHlYi0nSpdiFflbxaRV4 RBE116VUPqtmJdLb4xjxLivicSMJN2RDQnQylnfel6LploacJUQJ1AGdUX4ztwlE5YCXDWRbdxiXpUupnhCdh/pWp88KfQIDAQABo4GgMIGdMA4GA1UdDwEB/wQEAwIB BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTwePkHdxC73B6hrnn7MBDbxjT4 FzBIBgNVHSAEQTA/MD0GCQ0QDgcBAAECADAwMC4GCCsGAQUFBwIBFiJodHRw0i8v d3d3LmUtdHJ1c3QuYmUvQ1BTL1F0Y2VydHMgMBEGCWCGSAGG+EIBAQQEAwIABzAN BgkqhkiG9w0BAQUFAAOCAQEAbOHYX3RY6XBJ1soNLFjaymS2UU/DBmQB6YpzHZ7P Rni/04WG4j1KGJQqgXdvgvhv904i/J0YIXJguxiAgpX7+feVJIFmwbXDtdK2dos7 gVy4oQ4rARSLgAlA7vhgTBnkF80nAbNjEgWkCMm0v55QTrXeD5IzZnXQPecjf0ol cXz+Pi42eaHlKVAjNQWVeLufeWTcV0gnL0JcM83Cu35od6cvo0kXcuEAhGt9eq85 CyzV2FdkMmyECmp2Ot0szZ2x5zfc7AwvxVdg34j1Q7EBZCa0J4IQsqNQ75fmf7+R h7PbkKkq4no0bHNJ90iNLmuK3aGKf2PQv1ger8w/klAt0Q= ----END CERTIFICATE----

# Society for Worldwide Interbank Financial Telecommunication SCRL

Service provider trade name VATBE-0413330856

**SWIFT** 

Information URI http://www.swift.com/index.page?lang=en

http://www.swift.com/pkirepository

Service provider Avenue Adèle 1

street address

Service provider

postal code

1310

Service provider

locality

La Hulpe

Service provider state Brussels

Service provider

country

## SWIFTNet PKI Certification Authority

Type CA/QC

Status undersupervision

Status starting time 2013-05-15T00:00:00.000Z

## Service digital identity (X509)

Version 3

Serial number 1007235709 Signature algorithm SHA1withRSA Issuer 0=SWIFT

Valid from Sat Jun 15 13:51:47 CEST 2002

Valid to Wed Jun 15 14:21:47 CEST 2022

Subject O=SWIFT

Public key Sun RSA public key, 2048 bits

modulus:

2713489144953666367009133891636460566719364721268361046536591993 4994474903020635584331677653228200210928489182501819079634477925 8492233590999837413051645081782463444435029313072619678324503388 61324550609449630768200966983969376986503711769404215924828428075011899626639351963633260617226195373584394852072888957304178117 5313510569711163457668946603482121013634442930239281415342850090 7026386418520436427134899300324073409253701773263117431279842284 84805776174599366828375666985899520987211055858487771113785348435966527642400898111594497598591390136982490646196185727187396856

39915967136410239131574955455289383883587

public exponent: 65537

Authority key

Subject key identifier 3e30b33b359757fff140db1b4501382e15a79eb2 3e30b33b359757fff140db1b4501382e15a79eb2

identifier Key usage

keyCertSign

cRLSign

Basic constraints

CA=true; PathLen=unlimited

SHA1 Thumbprint

d9a235c88c875b171174d1076b596af9e0a0363d

SHA256 Thumbprint

cfa61bf3895cfe4244fbe684aedc88feaddd14d6aa3c73f5688f2c1e52c9a604

## Qualifications

[DistributionPoint:

Qualifier: QCForLegalPerson

Assert: atLeastOne

Policy OID: 1.3.21.6.3.10.200.3

#### The decoded certificate:

```
Version: V3
Subject: 0=SWIFT
Signature Algorithm: SHAlwithRSA, OID = 1.2.840.113549.1.1.5
Key: Sun RSA public key, 2048 bits
```

```
public exponent: 65537
Validity: [From: Sat Jun 15 13:51:47 CEST 2002
          To: Wed Jun 15 14:21:47 CEST 20221
Issuer: 0=SWIFT
SerialNumber: [
               3c09327d1
Certificate Extensions: 8
[1]: ObjectId: 1.2.840.113533.7.65.0 Criticality=false
Extension unknown: DER encoded OCTET string =
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 [
```

```
[CN=CRL1, O=SWIFT]
[5]: ObjectId: 2.5.29.15 Criticality=false
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
From: Sat Jun 15 13:51:47 CEST 2002. To: Wed Jun 15 14:21:47 CEST 20221
[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]
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
                               1B 1A 42 CB 8B 62 A7 9B ...,....B..b..
0020: CE FD 20 2C C3 D5 F1 F3
                               1C 1D 39 5C FB D0 34 53 ..4.._..9\..4S
3A 0E CB F6 B2 3F 97 02 ..Z6m...:...?..
0030: A3 D1 34 D6 C3 92 5F 03
0040: CF 93 5A 36 6D 15 D4 8B
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....
                                D7 AE E5 01 37 D6 E4 4F
0070: D9 D7 C7 F7 AB 0F 71 B8
                               03 17 6C 5C 7E F5 C2 C6 B......l\....
0080: 42 A2 DE D6 16 DD FF 81
                               09 5D 05 5D 87 1E F3 86 .W...D...].]...
0090: 86 57 8E C7 D7 44 91 BA
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...+.
                               88 33 07 0D E2 31 CD BA .F....Nf.3...1..
00C0: D9 46 A0 B5 17 BA 4E 66
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..
                               70 97 86 79 CB 0C 9E 09 .P...K9.p..y....
00F0: CA 50 B5 C3 7E 4B 39 AF
```

#### The certificate in PEM format:

----BEGIN CERTIFICATE----

 ${\tt MIIDkDCCAnigAwIBAgIEPAkyfTANBgkqhkiG9w0BAQUFADAQMQ4wDAYDVQQKEwVT}$ V0lGVDAeFw0wMiA2MTUxMTUxNDdaFw0vMiA2MTUxMiIxNDdaMBAxDiAMBqNVBAoT BVNXSUZUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1vMie2UrDYQy 2yk3+hjuqgqSc8br8qtqzXHsB7Zt99Pen0dTFAsAnFyshdMVIGgwmyJb8X3QpFEJ nh6is3o+JrHfkDPs07ISroFc9lAD7TEG0EnfiCMNJnJRH80ce0bLKmBfqv/Gwrsp /SZRzFUlJu+PILZaZ3uwVuxQ1ZLkKWlQVGSQJudNhh2qeWDU3D3SusRBNS37d4h5 zOpKv9obTQINRgg/wNwNdqwSF2rZLt/bZg8UnlomKWq7MTQfN/cHniGOQbfNtINL MWblH5aTOwIDAOABo4HxMIHuMBEGCWCGSAGG+EIBAOOEAwIABzAvBqNVHR8EKzAp  ${\tt MCegJaAjpCEwHzE0MAwGa1UEChMFU1dJRlQxDTALBgNVBAMTBENSTDEwKwYDVR0Q}$  ${\tt BCQwIoAPMjAwMjA2MTUxMTUxNDdagQ8yMDIyMDYxNTEyMjE0N1owCwYDVR0PBAQD}$ AqEGMB8GA1UdIwOYMBaAFD4wszs1l1f/8UDbG0UB0C4Vp56vMB0GA1UdDq0WBB0+ MLM7NZdX//FA2xtFATguFaeesjAMBgNVHRMEBTADAQH/MB0GCSqGSIb2fQdBAAQQ MA4bCFY1LjA6NC4wAwIEkDANBgkqhkiG9w0BAQUFAA0CAQEAvs0iVHn5v9Z+5+yZ peNiGIDLB06HTqXNrfPXnu3Ls3i0/SAsw9Xx8xsaOsuLYgebo9E01sOSXwMcHTlc +9A0U8+TWjZtFdSL0g7L9rI/lwIa2jkSSUCbzFtRkjM4pVR0wwYJTndw4IizkzKs waSK8tnXx/erD3G4167lATfW5E9Cot7WFt3/gQMXbFx+9cLGhle0x9dEkboJXQVd hx7zhrvz5z6cVV05ShhJASshPVXiMdgztWJCACsdV0r0ivuD2UagtRe6TmaIMwcN 4jHNunut7UXB2sGo/oZ+vIJA5NQurHiAkf7DK01C9kd8a3zgylC1w35L0a9wl4Z5 -----END CERTIFICATE-----

## QuoVadis Trustlink BVBA

Service provider trade name

VATBE-0537698318

QuoVadis

Information URI

https://www.quovadisglobal.be/~/media/Files/Repository/QV\_RCA1\_RCA3\_CPCP

S V4 16.ashx

Service provider street address Steenbergen 8

Service provider postal code

3583

,

Service provider

Beringen

locality

Service provider state Limburg

Service provider country

BE

## **QuoVadis BE PKI Certification Authority**

*Type* CA/QC

Status undersupervision

Status starting time 2014-05-20T00:00:00.000Z

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 14:31:54 CET 2014

 Valid to
 Wed Mar 17 19:33:33 CET 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 0978631883136821438467859677425505518925295946478935536215699720906056393460135609950257208816552322058565456762152598983343579241207167353021311043823546160995023349465819732001393426014237055722743791909993240230489806096355723483588160724849940671702693 9421288570479403288803182697829361690097956484101520823731103609 $3100150818512233246331732587859059076124798706288556894310123901\\0972920078194075368441656229441331564718831935659177163391354589\\2011373776362193636814506011844368620196727006732532805298830422$ 95074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669381028717945085604658219831940595283416191753140348941632069250736324234157157004129102669072961997392759148097836830663187572932975564250918605529635852688494 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

```
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
81851223324633173258785905907612479870628855689431012390109729200781940753684416562294413315647188319356591771633913545892011373776362193636814506011844368620196727006732532
7776697029462522370343
public exponent: 65537
Validity: [From: Tue Jan 28 14:31:54 CET 2014,
          To: Wed Mar 17 19:33:33 CET 2021]
Issuer: CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
SerialNumber: [
              6acaf5c9 85274c50 27ba2928 3006d6e4 c4f15a9b1
Certificate Extensions: 7
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 accessMethod: 1.3.6.1.5.5.7.48.1
 accessLocation: URIName: http://ocsp.quovadisglobal.com,
 accessMethod: 1.3.6.1.5.5.7.48.2
 accessLocation: URIName: http://trust.quovadisglobal.com/qvrca.crt]
[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 8B 4B 6D ED D3 29 B9 06 19 EC 39 39 A9 F0 97 84 .Km..)....99....
0010: 6A CB EF DF
]
[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
Pathlen:0
]
[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
   [URIName: http://crl.quovadisglobal.com/qvrca.crl]
[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [2.5.29.32.0]
[6]: ObjectId: 2.5.29.15 Criticality=true
KevUsage [
Key_CertSign
Crl_Sign
1
[7]: ObjectId: 2.5.29.14 Criticality=false
SubjectKevIdentifier [
0000: F8 0F 65 1C 7A 63 19 AA BF 44 6F A6 49 12 21 F3 ..e.zc...Do.I.!.
0010: 7A 5D E3 0D
Algorithm: [SHA256withRSA]
Signature:
0000: 4E 04 84 57 BF 82 C8 BE
                        65 FA B0 95 94 6D E3 B8 N..W...e...m..
0010: D5 58 5D 73 3E 15 FA 26
                         80 08 C3 22 C2 0F 0B CA .X]s>..&..."
0020: 58 D5 48 F1 49 B3 90 43
0030: 54 DC 51 90 6C 7D DA 1D
                         4A 0A 66 F9 53 D1 6F B8 X.H.I..CJ.f.S.o.
                         AB E4 F3 F0 F0 54 06 06 T.Q.l.....T..
0040: 25 70 E8 A8 11 6B 2A 86
                         C9 66 B9 1E 99 23 82 49
                                            \$p\dots k*\dots f\dots \#. \mathtt{I}
0050: F2 40 B5 B5 CB 9F 3B 8C
                        CD 63 3E 4E D7 1C 5C 1C .@...;..c>N..\.
E1 47 75 9D EF A3 74 2D ...T....Gu...t-
0060: 06 97 DF 54 AF 10 D5 1F
0070: C3 27 D8 43 6F F7 F0 52
                         4E FC 41 91 93 E9 A8 E2 .'.Co..RN.A.....
                        06 A8 22 0E 89 82 8A 2C ...z.!..."....
0080: D9 C6 1E 7A D6 21 F9 09
0090: B5 D4 C7 DA 1F 33 6E 09
                         AB 79 96 A8 13 F8 40 38
                                           .....3n..y....@8
00A0: 2C 5A 0A 10 EC B9 4B 03
                         E3 F0 34 EB FD 66 8B FD ,Z....K...4..f..
                                            .......u]D.D.,
00B0: D0 D6 98 0F A0 F4 20 C9
                         FF 75 5D 44 EC 44 A1 2C
00C0: AF 55 66 25 BD 5B E0 EE
                         3D 22 9A 08 0B 9C 49 22 .Uf%.[..="....I
00D0: BB 75 4D B5 9C 7E 54 B4
                         1D F4 10 6B 3A D3 2C BA .uM...T....k:
```

2B EC F5 B3 97 9D 1C 4E >G..[7.L+.....N

....'.Eq.....&.6M

AF BB 7B 83 26 A2 36 4D

00F0: 84 D1 B7 27 F5 45 71 0B

00F0: 3E 47 0F A8 5B 37 C2 4C

### The certificate in PEM format:

--BEGIN CERTIFICATE-MIIFjzCCBHegAwIBAgIUasrlyYUnTFAnuikoMAbW5MTxWpswDQYJKoZIhvcNAQEL BqNVBAsTHFJvb30q02VvdGlmaWNhdGlvbiBBdXRob3JpdHkxLiAsBqNVBAMTJVF1 b1ZhZGlzIFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTI4MTMz  ${\tt MTU0WhcNMjEwMzE3MTgzMzMzWjBYMQswCQYDVQQGEwJCRTEgMB4GA1UEChMXUXVv}$ VmFkaXMqVHJ1c3RsaW5rIEJW0kExJzAlBqNVBAMTHlF1b1ZhZGlzIEJlbGdpdW0q SXNzdWluZyBDQSBHMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAO/S 7z DGARkRKs9BxEzbGZoDK3e9m5SV6JzMaLUpFkzXzzkyRJbMphLgS0l6VtYAA+fgH9dawUV1fr2qLoBtp74tpNl1GdXIYI++WM0j/sgy2JnhTD0pcLV++zP8eN+SP50o wiDTqTxjQASSt+fmRvmgCIsGLCS3g67DSN/xCPdymefuoQWNNaxDnkIpArmRKElH  ${\tt jH+JS4jxjxtHh0lGgEFbPw41DyRPtFL3nDwQeTEgGvpxDUkuTD03lMdeHvGy3zZe}$ pAm/pmhVx9z7L6fNrqIu+rW6CSD5de059M8N4oXs5L8dsVv3mh1DHp5kvoY+qZAw T7NqKEbT8GkqoRs4uBXLuRPTCl6le1thTETBCrZRKLl9aZ8AP0NkAlo5Rl0PR7LS XeZtzKhp37p9dx00y16LurdVf0XMvjVUZ2LP+X+ZgDZmYm4FfoxKihrHXnaTAckL +nTsDQ49cYQvfg0GHH6+hrYJdR/ypa3Yf1s1YrNz5s+gSarp6eGWyDvNcugQ4TDW J46Cr8E0go7x3Vkk8+RAHtSB0MFuBaupqVRgdVAVqU3wF7B2puwxxmGcvQbgLGkH 1+bplVk/c6q/zICWWeD4SjTSChpbCnldJzkV2tKRFImlf9bv87G0x7WJoLSnLsa/ Qs1YhKGjX9MndQnvSFuwrJLvtzXPC2XaXYxXoJknAgMBAAGjggEoMIIBJDASBgNV HRMBAf8ECDAGAQH/AgEAMHEGCCsGAQUFBwEBBGUwYzAqBggrBgEFBQcwAYYeaHR0

l4Rqy+/fMDgGA1UdHwQxMC8wLaAroCmGJ2h0dHA6Ly9jcmwucXVvdmFkaXNnbG9i YWwuY29tL3F2cmNhLmNybDAdBgNVHQ4EFgQU+A9lHHpjGaq/RG+mSRIh83pd4w0w DQYJKoZIhvcNAQELBQADggEBAE4EhFe/gsi+ZfqwlZRt47jVWF1zPhX6JoAIwyLC DwvKWNVI8UmzkENKCmb5U9FvuFTcUZBsfdodq+Tz8PBUBgYlcOioEWsqhslmuR6Z I4JJ8kC1tcuf04zNYz501xxcHAaX31SvENUf4Ud1ne+idC3DJ9hDb/fwUk780ZGT 6aji2cYeetYh+QkGqCIOiYKKLLXUx9ofM24Jq3mWqBP4QDgsWgoQ7L1LA+PwNOv9 Zov90NaYD6D0IMn/dV1E7EShLK9VZiW9W+DuPSKaCAucSSK7dU21nH5UtB30EGs6 0yy6hNG3J/VFcQuvu3uDJqI2TT5HD6hbN8JMK+z1s5edHE4=

cDovL29jc3AucXVvdmFkaXNnbG9iYWwuY29tMDUGCCsGAQUFBzAChilodHRw0i8v dHJ1c3OucXVvdmFkaXNnbG9iYWwuY29tL3F2cmNhLmNvdDARBqNVHSAECiAIMAYG BFUdIAAwDgYDVR0PAQH/BAQDAgEGMB8GA1UdIwQYMBaAFItLbe3TKbkGGew50anw

----END CERTIFICATE----

Trusted List Signer

C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Subject

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 14:38:04 CET 2014 Wed Jun 11 15:38:04 CEST 2025 Not after

Serial number 17004208314404367103

Version 3

Public key SHA1 8f914035f0200880afe97b0eab85b5921ea98421

Thumbprint

Public key SHA256

*Thumbprint* 

f7cf32405bc6553c92fec8364bf58d56b153324ad58ad6cb7aace1037d5d3e41

```
The decoded certificate:
```

```
Subject: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
Signature Algorithm: SHAlwithRSA, OID = 1.2.840.113549.1.1.5
Key: Sun RSA public key, 2048 bits
modulus:
ublic exponent: 65537
Validity: [From: Wed Feb 19 14:38:04 CET 2014,
       To: Wed Jun 11 15:38:04 CEST 2025]
Issuer: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
SerialNumber: [
         ebfb155e aad0eaff]
Certificate Extensions: 4
[1]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
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 [
0010: AA D7 90 51
Algorithm: [SHA1withRSA]
Signature:
0000: 94 2D D7 B2 33 29 EA A7
                              C5 A9 1D 83 2B 13 D4 59 .-..3).....+..Y
0010: 72 9A 87 19 51 41 C6 85
                              F6 D0 01 FA F8 38 49 B8 r...QA......8I.
0020: F0 B3 28 37 83 39 65 E7
                              91 31 52 30 93 88 CE 0D
                                                       ..(7.9e..1R0....
                              45 D1 81 FB 34 F3 20 C2 Dn..-(..E...4. .
0030: 44 6E 85 AC 2D 28 9D E1
0040: F1 78 F9 80 18 64 43 50
                              DA C3 C1 CB 69 9F C1 BF
                                                       .x...dCP....i...
0050: 46 A1 05 8E 58 1C E7 28
                               B5 20 21 C1 64 9A EF CA F...X..(. !.d...
0060: E7 7B 70 FC 33 F0 0C 0C
                               B5 5F 8A D6 21 66 6C 45
                                                      ..p.3...._.!flE
0070: AA BO 60 12 67 DE 89 E6
                               E8 A5 24 9F 91 90 F7 15 ....g.....$.....
                               4E C4 77 E1 9A AD 0F 09 ..p....N.w....
0080: DC E9 70 B6 08 B7 F8 8C
                              75 3F 77 E5 9F 12 7C 58
0090: D4 64 D6 4F 3E 73 B7 EB
                                                       .d.0>s..u?w....X
                                                       'h..DX6x.o.j...w
'_^?.J.gUU.8.0wP
00A0: 27 68 FC R8 44 58 36 78
                               A7 6F 0B 6A AC BE C1 77
00B0: 27 5F 5E 3F F0 4A 94 67
                               55 55 EE 38 C9 30 77 50
                              33 F2 57 21 03 79 54 4F !7)"..+.3.W!.yT0
00C0: 21 37 29 22 E2 C9 2B E0
                              C5 B9 13 BD 48 75 41 22 ....D..^...HuA"
C4 6A 2A D9 2B 2C E1 80 .C.wF..8.j*.+,...
00D0: A5 18 F7 94 44 A9 F8 5F
00E0: DF 43 ED 77 46 01 C5 38
```

#### The certificate in PEM format:

----BEGIN CERTIFICATE--

MIID3zCCAsegAwIBAgIJAOv7FV6q00r/MA0GCSqGSIb3DQEBBQUAMIGHMS0wKwYD VQQDEyRCZWxnaWFuIFRydXN0ZWQgTGlzdCBTY2hlbWUgT3BlcmF0b3IxSTBHBgNV BAoTQEZQUyBFY29ub215LCBTTUVzLCBTZWxmLWVtcGxveWVkIGFuZCBFbmVyZ3kg LSBRdWFsaXR5IGFuZCBTYWZldHkxCzAJBqNVBAYTAkJFMB4XDTE0MDIx0TEzMzqw NFoXDTI1MDYxMTEzMzgwNFowgYcxLTArBgNVBAMTJEJlbGdpYW4gVHJ1c3RlZCBM  ${\tt aXN0IFNjaGVtZSBPcGVyYXRvcjFJMEcGA1UEChNARlBTIEVjb25vbXksIFNNRXMs}$ IFNlbGYtZW1wbG95ZWQgYW5kIEVuZXJneSAtIFF1YWxpdHkgYW5kIFNhZmV0eTEL MAKGA1UEBhMCQkUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAgEFk oDPTYDvGk+/IPnGSPm58NRE7mpzLHk8lxpYnTAtbMhn7FWru9GlNi+blYYN0EmzN 2F5K09+7AAAMmx2x8zmFMwc3oII07F0WN5G1+Y+7n6N+X50D/4Shw4TiVvvwRRru8 Coj5vq5Hz3JKTgft8teEpwb5vSFZh6+o9irdX342RJU4AtG78sxZvzIqpa3WsddM f5XDyjnGK3dRgkDu0aBxWEexuUiN4Lv0+MacwoaxEqLhEZ6TALGWS2WmNEW30lUd f7nc0Tz/lnyQsuFn01c4pg56hjyxLtpjyHwNwbTDx+cjBpBve0T9Nb6UfKFHknC5AfrIOWnFLXUmyKD/AgMBAAGjTDBKMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgbAMB0G AludDgQWBBRf745pXfv0l1rxBwg0UhlQqteQUTARBgNVHSUECjAIBgYEAJE3AwAw  ${\tt DQYJKoZIhvcNAQEFBQADggEBAJQt17IzKeqnxakdgysT1FlymocZUUHGhfbQAfr4}$ OEm48LMoN4M5ZeeRMVIwk4jODURuhawtKJ3hRdGB+zTzIMLheOmAGGRDUNrDwctp n8G+RqEFjlgc5yi1ICHBZJrvyud7cPwz8AwMtV+K1iFmbEWqsGASZ96J9uilJJ+R kPcV30lwtgi3+Ix0xHfhmq0PCdRk1k8+c7frdT935Z8SfFgnaPy4RFg2eKdvC2qs vsF3J19eP/BKlGdVVe44yTB3UCE3KSLiySvgM/JXIQN5VE+lGPeURKnoXsW5E71I dUEi30Ptd0YBxTjEairZKyzhgGbZEnBUWSkn6n9uZ5Ai2lo= ----END CERTIFICATE-

#### The public key in PEM format:

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQBAMIIBCgKCAQEAwIBBZKAz02A7xpPvyD5x kj5ufDUROSqcyx5PJcaWJ0wLWzIZ+xVq7vRpTYvm5W6DThJszdhO5jvfuwAADJsd sfM5hDMHNGFEOxNFjeRpfmPu5+jbV+dA/+Em8OCIIb8MEUa7vAqI+b6uR89ySk4H 7fLXhKcG+b6hWYevqPYq3V9-NkSV0ALRu/LMWbByKqWt1rHXTH+VW8O5xit3UYJA 7jmgcVhHsblIjeC7zvjGnMKGSRKi4RGekwCxlktlpjRFtzpVHX+53NE8/5Z8kLLh Z9NXOKYOeoY8s57aY8h8DcG0w8fnIwaQb3jk/TW+LHyhRSJwuQH6yDlpxS1lJsig

----END PUBLIC KEY----