

Belgique/België (Belgium): Trusted List

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 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 2014-08-14T00:00:00.000Z

Next update 2014-12-28T00:00:00.000Z

Historical information period 65535 days

Sequence number 18

Scheme information URIs <http://tsl.belgium.be/>

Scheme Operator

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

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
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 locality Brussels

Service provider state Brussels

Service provider country BE

CN=Belgium Root CA, C=BE

Type CA/QC

Status undersupervision

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

Service digital identity (X509)

Version 3

Serial number 117029288888937864350596520176844645968

Signature algorithm SHA1withRSA

Issuer CN=Belgium Root CA, C=BE

Valid from Mon Jan 27 00:00:00 CET 2003

Valid to Mon Jan 27 00:00:00 CET 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

Scheme Service Definition URI

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

Qualifications

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:

```
[
[
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
4444513897535102557574950367954722638103130021380872795033349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
7741754485069632411877604954193498318303560891627721798430948172071644141969017225065301229219951
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
SerialNumber: [ 580b056c 5324dbb2 5057185f f9e5a650]

Certificate Extensions: 6
[1]: ObjectID: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[2]: 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 ....
]
]

[3]: 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 ....
]
]

[4]: 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
]
] ]

[5]: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSign
```

Crl_Sign
]
[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:
CA:true
PathLen:2147483647
]
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 49j.k*.YH.LI
0020: 37 D7 73 A1 6A 01 65 5E 32 BD E7 97 D3 D0 2E 3C 7.s.j.e^2.....<
0030: 73 D3 8C 7B 83 EF D6 42 C1 3F A8 A9 5D 0F 37 BA s.....B.?.].7.
0040: 76 D2 40 BD CC 2D 3F D3 44 41 49 9C FD 5B 29 F4 v.@...?.DAI..[]).
0050: 02 23 22 5B 71 1B BF 58 D9 28 4E 2D 45 F4 DA E7 .#[q..X.(N-E...
0060: B5 63 45 44 11 0D 2A 7F 33 7F 36 49 B4 CE 6E A9 .cED...*.3.6I...n.
0070: 02 31 AE 5C FD C8 89 BF 42 7B D7 F1 60 F2 D7 87 .1.\....B....
0080: F6 57 2E 7A 7E 6A 13 80 1D DC E3 D0 63 1E 3D 71 .W.z.j.....c.=q
0090: 31 B1 60 D4 9E 08 CA AB F0 94 C7 48 75 54 81 F3 1.'.....HuT...
00A0: 1B AD 77 9C E8 B2 8F DB 83 AC 8F 34 6B E8 BF C3 .w.....4k...
00B0: D9 F5 43 C3 64 55 EB 1A BD 36 86 36 BA 21 8C 97 ..C.dU...6.6.!..
00C0: 1A 21 D4 EA 2D 3B AC BA EC A7 1D AB BE B9 4A 9B .!...;.....J.
00D0: 35 2F 1C 5C 1D 51 A7 1F 54 ED 12 97 FF F2 6E 87 5/.\.Q..T.....n.
00E0: 7D 46 C9 74 D6 EF EB 3D 7D E6 59 6E 06 94 04 E4 .F.t...=.Yn....
00F0: A2 55 87 38 28 6A 22 5E E2 BE 74 12 B0 04 43 2A .U.8(j"^\...t...C*

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MID1DCCAnygAwIBAgIQWAsFbFMk27JQVxf+eWmUDANBgkqhkiG9w0BAQUFADAn
MQswCQYDVQGEwJCRTEYMBYGA1UEAxMPQmVsZ211bSBSb290IENBMB4XDTAzMDUy
NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowJzELMAkGA1UEBhMCQkxGDAWBgNVBAMT
D0JlbGdpdW0gUm9vdCBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMihcekCRk35eHFvna6pqKsot03HIOswkVp19eLSz8hMFJhCwK3HEcVAQGpa+X0S
J4fPn0VxTiIs0RIYqjBeoiG52bv/9nTrMQHn035YD5EWTXaJqAFPrSjmcPpLHZXB
MFjqvNL2Jq0i0tJRLLf0LMVdsuXRLJ3sW9q09P9vMI7EU/CT9YvzvU7wCMgTVy
v/cY6pZifSsofxVsY9LKyn0FmhtB20yvmi4BUCUvJhWpmbxMOjvxKuTXgfeMo8S
dKpbkCNuW0pszv42kqgJf+qhLc9s44Qd3ocuMws8d0IHUdiVLzlg5cYx+dtA+mqh
pIqTm6chBocdJ9EocLMSG8CAwEAa0BuzCBuDA0BgNVHQBBAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAE0zA5MDCGBWA4AQEBMCAwLAYIKwYBBQUHAgEW
IGh0dHA6Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlLmB0GA1UdDgQWBQ8A8XW
m2HqVzq2Nzdt925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth6lc6tjWxbZ/duRS02+YwD0YJKoZIhvcNAQEFBQADggEBAMhtILGKYfgP
lm7VILKB+Mbc0xYA2s1q52sq+LlIp0xJN9dzoWoBZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0A1m1W3Ebv1jZKE4trfTa57vjRUQRD5p/
M382SbT0bqkCMA5c/ciJv0J71/Fg8teH9lCuen5qE4A30PQY49cTGxYNSeCMqr
8JTHSHVUgfMbrXec6LKP240sJzRr6L/D2fVDw2RV6xq9NoY2uIGMLxoh10ot0y66
7Kcdq7655ps1LxxcHVGNH1TtEpf/8m6HFubJdNbv62195LluBp0E5KJvhzgoaiJe
4r50ErAEQyo=
-----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
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

Scheme Service Definition URI

en <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

RootCA-QC

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:
25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533471883040702374115053713546900035236027965047482684369657400131555243639532965596057682937264627486838678079794762230469369210950088797578757728341339292333654654510981797643030670179357915156526215843512360635833423071049762443221776521812652705725352885936886683614903840430636240528870143824637588105680040795881448654643858460532713400822409146679502714797245542101554942867836639308049158535662204430622722091644041294798682626345622247703196611536459503012648921426461410998536799349
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: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
SSL CA
S/MIME CA
Object Signing CA]

[2]: 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
]
]
```

Belgique/België (Belgium): Trusted List

```
]
[3]: 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
]
]
[4]: 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
]] ]
]
[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSign
CrL_Sign
]
[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
]
Algorithm: [SHA1withRSA]
Signature:
0000: 51 D8 85 DD BB 57 6F CC A0 6C B5 A3 20 9C 53 09 0....Wo..l...S.
0010: F3 4A 01 0C 74 BF 2B B3 9A 9A BA 18 F2 0B 88 AC ..J..t.+.....
0020: 1C B3 33 AF CE E5 13 01 27 92 84 58 9A 10 B9 F7 ..3.....'..X....
0030: CC 14 92 6B 74 16 8A 96 E8 51 EF BF FA 4A 25 A7 ...kt....Q...J%.
0040: 89 B6 63 2B 5D 94 58 D1 CF 11 72 B6 1E B9 39 41 ..c+].X...r...9A
0050: 16 4D 29 BC 35 53 0B DA DE 8E 0E CD A9 95 77 25 .M).5S.....w%
0060: CA 94 5A E9 B2 69 AE D8 C0 13 BE 98 FC 96 9C 84 ..Z..i.....
0070: 7F 55 13 E6 3C 87 E3 BC 20 A4 A4 36 68 6B 4D 60 .U..<... ..6hkM`
0080: 66 1C F9 BF AC 80 94 66 2E B9 41 8A D3 65 D3 84 f.....f..A..e..
0090: 80 02 EF 50 1D 5E 46 DC F7 C9 BA B5 34 7C 2A F3 ...P.^f....4.*.
00A0: C6 D8 5F 5F 54 9D DB 4D CD 11 E7 FD 14 02 83 66 ...T..M.....f
00B0: 5E C8 A6 00 12 A0 5F BE CE 14 FE BB 1F A7 61 F7 ^....._.....a.
00C0: AB 4A F1 06 14 9F CA 49 42 C2 A9 BC ED 85 B1 AB .J.....IB.....
00D0: 81 41 E6 0D C5 42 69 53 87 39 9D 4C 1F 00 0E 3E .A...BiS.9.L...>
00E0: 07 0D 75 57 44 A8 53 B4 36 76 64 99 DC 6E EB 3D ...uW.D.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-----
MIIDjjCCAnagAwIBAgIIVk++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMkA1UE
BHMCMQKUXGTAxBGNVBAMTEEJLbGdpdW0gUm9vdCB0QTIwHhcNMDcxMDA0MTAwMDAw
WhcNMjE1MDgwMDAwMjA0M0swCQYDVQQGEWJCRTEZMBCGAIUEAxMQQmVsZ211
bS5Bb290IENBmJjCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi790hqc/7bIYL52X+an7mEoj39WN4IzGMhwLQdC1122b1+n9fzGhYJdld61
IgdMqFNAn68KNaJ6x+HK92AQZw6nUHMxU5wfIp8MXW+2QbyM69odRr2nLL/zGsvU
+400HjPILtfsjFPeKx40HopQcSZYtF3CiInaYnkJIT/eIwEYnm7hLHADBGXvMAYr
XR5i3FVr/mZKIV/4L+HXmymvB82fqgXG0YjFnaKvN6w/Fa7yYd/vw2uaItgscf1Y
HewApDggLVrHITdjuK+bqv5WR15j2Qsj1Yr6tSPwiRuhFA0m2kHw0I8w7QUmecFL
TqG4fLV50mLGHUcAwEAa0BuzCBuDA0BgNVHQ8BA8EBAAMCAQYwDwYDVR0TAQH/
BAUwAWEb/zBCBgNVHSAE0zA5MDcGBWA4CQEBMC4wLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlM0B0GA1UdDgQWBBSFiu0xbu+dLkd
LN7WgAEV4xCc0TARBgLghkgBhvCAQEEBAMCAAcwHwYDVR0jBBgwFoAUHyr9MM7
vg5A5Te1oABFeMQNDkwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyC
UwnzSgEMdL8rs5qauhjyC4iSHLMzr87LEwEnkoRymhC598WUkmt0FoqW6FHvV/pK
JaeJtmMrXZRY0c8RcrYeuTLBFk0pvDVTc9rejj7NqZV3JcUWumyaa7YwB0+mPyW
nIR/VRPmPIfjvCCKpdZoa0Igz5v6yALGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9fVJ3btCR5/0UAoNmXsimABKgX770FP67H6dh96tK8QYUn8pJQsKpv02F
sauB0eYXUjpu4c5nUwFAA4+Bw1LV0SoU7QdmS23G7rPUZuFF1eR10NeE3gJ7u0
hXY=
-----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
Issuer CN=Belgium Root CA3, 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 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

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
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
4022292897790187651429542062848723560572075471815465553654740672119937451228803489479389781589873374361336080842299846657331444909264877243429847318212868757946477943923944
62687490398028495494344463316509704441880805330280656748039731016531817357098402749506393119772983757645685092450758730479725560212981580096389424844703793712327092036866308
0351919425068313464980278629369152701697759736384202776541620591588545291932466321499552953337563259732378154805928106136809503809799800229292061750390447533216339381404779
4956959421382197572947310250836645472304794333937457964148701121644586439773493445613256431505451689600807046471898622121897269823517896969688074733205559734650561444823679
2925190609006356545814179709805522858179027890695147721585965047687358534340606348654270524459674087994714793894190325164983453802445244240129496186620178930087479418923182
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: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
SSL CA
S/MIME CA
Object Signing CA]

[2]: 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+
]
]

[3]: 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+
]
]

[4]: 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
]] ]

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

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

Algorithm: [SHA1withRSA]
Signature:
0000: 45 62 3B FF 98 A5 FE 55 CC B1 11 A7 1C 92 0C 78 Eb;...U.....x
0010: 2F C5 EF 16 42 05 3D 7C E3 12 70 E7 02 D0 82 91 /...B.=...p....
0020: 13 94 FE 4E 67 D6 38 D5 2B E3 83 3A 7F 90 E2 42 ...Ng.8.+...B
0030: 60 E8 D7 7B 2B 8E FE CD 35 DC AD 27 B5 B4 1D A0 `...+...5...!....
0040: 54 CB 32 68 23 7D B1 CC B8 A6 12 D7 D6 A4 F8 F2 T.2h#.....
0050: C4 E1 0A 35 2D A2 8C 5F 22 84 72 72 97 65 7F 5E ...5-...rr.e.^
0060: 07 71 43 C2 62 50 12 4C 26 A9 65 4D 0C 9C 06 F3 .qC.bp.L&.eM....
0070: 7E 9C F1 9B 8F 48 93 F0 36 25 6C 40 87 15 D5 44 .....H..6%l@..D
0080: 7C 0E BB 74 CC 1A 24 38 58 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 C5 9C 34 0B EF 90 9.....VE.\.4....
```


0110: 35 44 2E F5 DF 26 94 71 C1 C4 5F 4B 92 AC E6 86 5D...&.q...K....
0120: 9F 39 F8 FC D5 1C C6 51 B9 A9 C2 5D AE B0 E7 82 .9.....Q...].
0130: 47 07 56 13 C8 0F BD B7 D6 35 04 02 F0 C2 6A B8 G.V.....5....j.
0140: 39 79 1D D7 AE CD 47 AC 4D 75 2A 5D E1 24 C8 03 9y.....G.Mu*].\$.
0150: A8 E9 89 C5 DE 0D 2A 19 C2 C8 F4 D5 EE B2 38 B5*.....8.
0160: 7A 04 54 67 B0 78 5C 2B C6 E7 69 53 07 B5 A0 77 z.Tg.x\+.iS...w
0170: FC 15 17 34 B7 7F 89 80 99 84 C6 25 71 FE 37 F9 ...4.....%q.7.
0180: 6B 04 11 8A B9 32 79 5E 77 09 6A 58 85 50 AC 46 k.....2y~w.jX.P.F
0190: 3F A5 66 37 26 9A 2D 41 79 22 54 EA 0B D0 86 1C ?.f&.-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.?....

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFjCCA3agAwIBAgII0yEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMkA1UE
BHMCCQkxGTAXBgNVBAMTEEJlbgdwdW0gUm9vdCBDQ0TmHhcnMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwWjAOMQswC0YDVoQ0QGEwJCRTEZMBCA1UEAxMQMmVsZ211
bSB5b290IENBMzCCAlIwDQYJKoZIhvcNAQEBBQADAgEPADCCAgQCGgIBAKjyAZ2L
g8kHoIX7JLc3BeZlTzy9MEv7Bnr59xcJezc/xJJ04V3bwMLtKfFNvqsQ5H/GQAD
FJ0GmTLPLDl5AoeUjBubRZ9hwrUuQ11+vhToVhuEuZuXofEIU2yJtiS00Nwpo/G
Ib9C4YZ5h+7ltDpC3MvsFyyordpZgwgShvFwTcmLs5SpU05Ubf7ZVPcfVf24A5I
HLpZTgQfAvnzPlm++eJY+sNoNZTBoe6iZphmPbxuPncJ6sLV8MQQk50/g+KmoPp
HX4AvoTr4/7TMTvuk8jS1dEn+fdVKdx9qo9ZRRHFw/TXEn5SrNUU99xhzLE/WBurr
VvFokCWCjm00CnekJlW0MT3HBTG5D4AidjNFUYaIcGJk/ha9rzHzY+HpdGoFZx
hbP83ZGeoqkgBr8UzF0FCY8cyUN2db6hpIaK6Nuho06QWnn+TSNh5HjuismiqpGx
S73gYLT2Qww16h8gFTJQ49fiS+QHLwRw5cqFuqfFLE3nFFF9KIam54TSe7T4dNGY
2VbHzpaGVT4wy+fL7gWsfauKvvhM4b00DzgdI9BHhKyTnlMzoa3SneiJ/CKur0dJ
50dMiAqUp5d0e8pdIbmQm1oP5cjkI0jxx7+vSxWtaccGovWk8+7oEsYc+7fLt3
GD6q/05Xi440Pd/sFJmfqRf3C1PPMdBqXcwjAgMBAAGjgbswgBgdgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAF8wQYDVR0gBDswOTA3BgVg0AoBATAuMCG
CCsGAUQFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS51aWw0YmVsZ211bS5iZTAuZG9u
VH04EFgQUuLxsA19bGYWdJ0Gc8BncQI700CswEQYJYIZIAyB4QgEBBAQDAHMB8G
A1UdIwYMBaAFLi8bACpWxmFmSUbNPAZ3EC00DgrMA0GCSqSIsb3DQEBBQUAA4IC
AQBFjYv/mKX+VcyxYaaccKgx4L8XvFKIFPXzjEnDnAtCCkR0U/k5n1jJVk+0D0n+Q
4Kjg6Nd7K47+zTXcrSe1tB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpd1
f14HcLUPCYIASTCapZU0MnAbzfpzxm49Ik/A2JWxAhxVVRHw0u3TMgiQ4W/VyVawx
jwQM08TneBDombmkXsI9bI00xwUuH2A5dKlqu0sYVE0dz8xDxr9ZkmZqYcPIkiZCZ
laP1zS5L1C5531gn3EUP+fd21q6ZxgU+50/gqoh/0UuaHRpedP0BES/FYc2IQZ2X
jhmeTm+9Lk7tnzHeHp3dgCo0fCeyPUaVkwIXMwCNAvkvDVELvXfJpRxcRfS5Ks
5oaF0fj81RzGUBmpwL2us0eCRwdWE8gPvbFWNQC8MjquD15HdeuzUesTXUqXeEk
yA0o6YnF3g0qGcLI9NXusji1egRUZ7B4XCvG52LTB7Wgd/wVFz53f4mAmYTGJXH+
N/LrBBGkuTJ5XncJaLiFUKxGP6VmYaaLUF5IITqC9CGHPLSX0gDoktZG9pNwFm2
t7AcpwAmegkMNPgcgTd+qk2yLjEaT8wf953jUAFedbpN3tX/3i+uvH00mWjQ0xJg
2LVKkC+bbkWaZFrTBDdrLEWLaRy+M+xeIctrc0WmP7u4xg==
-----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
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 cd4186bcd938ca5c19610f74c762b23acf07a564

SHA256 Thumbprint c3fbf37259af0954eeea4282dd1c7226a54e7150f7c29a2c495ba34dbfe09ca0

Scheme Service Definition URI

en <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:

```
[
[
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:
62241159068241220314333934144677342557957496612426970419727969713589761663492552027516102528196645068474513261170454526640944182035424569860936689008684747674264316825012182352256880531189580132728458568307660729363286780295993398641607575820781797829334771277758427264740541256591774911244974410560636250890042978670882365536958960066499635916926974922484072536312589852319267013024030944819956639752564879885995940797513756491247223155583989584598625577661561495707877863985269083424382019627610669355576767590328743708696354187918592365002904651508327891796764752123759700977230597799879313143129461389580095293270697956397428505408544811668100588053087190204290004659595000540204476361567140374287384555757238779613682983523763657215705693034188731739504172407715327381234065663116928590961408814859757143559001530346841514598904885138299612865991395755715162815883415449288903178308408884400931018214236597980739606621031947075945003910750853619537707761075688418384343286045715157573426989301124463242723093299927147162988283928766947013625480426811137103293454625262051881732832104879637264017398565292090224855096446539393723135313244013015486792504471132824903136816339047745407340214082204078193963133511429055306278731837
public exponent: 65537
```

Belgique/België (Belgium): Trusted List

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
SerialNumber: [4f33208c c594bf38]

Certificate Extensions: 6

[1]: ObjectID: 2.16.840.1.113730.1.1 Criticality=false

NetscapeCertType [
SSL CA
S/MIME CA
Object Signing CA]

[2]: 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..N0....o.....z
0010: D9 5B E7 49 .[.I
]
]

[3]: 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..N0....o.....z
0010: D9 5B E7 49 .[.I
]
]

[4]: 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
]]]
]

[5]: ObjectID: 2.5.29.15 Criticality=true

KeyUsage [
Key_CertSign
CrL_Sign
]

[6]: ObjectID: 2.5.29.19 Criticality=true

BasicConstraints:[
CA:true
PathLen:2147483647
]

Algorithm: [SHA256withRSA]

Signature:

```
0000: 25 89 3C AB 51 CB A6 8F D8 75 21 12 99 34 82 A5 %<.Q...u!...4..
0010: B7 68 40 C8 D5 B5 8D D9 18 CF E7 C9 E7 B3 C3 3A .h@.....:
0020: AB 69 B2 F9 9F A1 99 AE 3F EE AB 49 B8 43 8B 52 .i.....?.I.C.R
0030: 7D A5 F8 BB 61 CF 5F 20 3C 31 1B 07 E4 88 F2 40 ....a_<1....@
0040: 89 10 65 D5 AC 5D B6 99 E4 A0 03 04 73 14 28 9C ..e..].....s.(.
0050: B9 F1 32 24 BA FE 7E A7 42 A2 17 A5 BD 0E DF 86 ..2$...B.....
0060: 00 60 03 49 9F 92 EE 8D DE 55 F4 8F A2 BF 9A EB `^I.....U.....
0070: CD 78 EF 71 93 CD C6 01 01 DF 1E 9F 25 DA 55 6A .x.q.....%Uj
0080: 96 E8 92 18 2B 0E B8 35 83 B5 EA 11 8F 89 62 22 ....+.5.....b"
0090: 4F 9A FE DD 5C 8C E1 67 A9 4D DB D7 E8 07 3A 22 0..\^g.M....:"
00A0: 93 5A 3A 5A 9E 14 9C 2E 14 B0 54 E0 C7 F8 4D E7 .Z:Z.....T...M.
00B0: A7 23 91 D5 CC 09 1F 49 1D 03 16 99 C0 B3 92 4D .#.....I.....M
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.;;
00E0: E7 5E D5 40 89 07 F1 04 D2 5F 4C F0 74 1A A5 55 .^@.....L.t..U
00F0: C8 52 14 A6 A8 ED 51 F8 0D D1 0F C7 2F 8C FF 4F .R....Q...../..0
0100: E4 50 E8 C4 29 9E 19 3A EA 71 72 88 8F 5A 96 B3 .P...).:qr..Z..
0110: B8 2C AD 76 74 C8 30 AC EC 7C 92 4F 9F E8 33 E1 .,vt.0....0..3.
0120: 90 F4 E2 E1 53 DC 2B 1F 87 0C C1 6F 00 B0 E4 72 ....S+.....o.r
0130: 0A A6 6A 7A 08 52 6D DE 61 13 E0 25 9A 3E 12 9B .jz.Rm.a.%.>..
0140: 18 CF 86 DE E4 AE D4 17 44 67 9B 7F 9A 3A AB E4 .....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.....).
0170: 85 0C C4 EA F0 3D 1C 1B 8E A7 E5 D1 45 12 E8 8B .....=.....E...
0180: CA 66 10 0B 78 C0 5E E8 6B D7 A4 C8 93 AA 69 6D .f..x.^k.....im
0190: 6B B7 03 D7 7C 8A 25 00 40 BF 38 84 DD 02 4C 3D k.....%@;...L=
01A0: 8D 17 02 2B 3A 09 60 37 CD 45 5B CE 7B 90 D9 5B .+...:'.7.E[....[
01B0: 64 D0 C0 6D 95 01 1B FB 0D CE B1 48 78 78 88 3F d..m.....Hxx.?
01C0: 02 43 8D 27 8F F6 E0 01 5F 3B 39 25 98 1E E4 F7 .C.'.....;9%....
01D0: 7B 7B 5D AF D8 B9 55 9B F2 0A 37 EF 0B 6A FC 0F ..]...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 86 A8 CB 4C 59 >b.....>Y...LY
```

]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFjCCA3agAwIBAgIITzMgJmWUvzgwD0YJKoZIhvcNAQELBQAKDELMAKGAIUE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCB0DQwHhctNMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwAwJwAQM0swCOYDVQ0GEWJCRTEZMBCGAIUEAxMQmVsZ211
bSB5b290IENBNDBCA1IwDQYJKoZIhvcNAQEBBQADgIPADCCAgQCGgIBAJiQrvrH
Hm+04AU6sYn4TNHWL911PFsY6E9euwVmLSNAWTdw9p2mcmE0YGx424jFLpSQVNxx
xoh3LsIpdUMRQfuidQzVzX/4dCBaeKL/AMRJuL1d6wU73XKSkdDR5uH6H2Yf19z
SiU0m2x4k3aNLyT+Vryf11b1Prp67CBk630BmG0WUaB+ExtBHOkfPaHRHA04Mig
oVft3gLRQGH1V+H1rm1hydTzd6zppoJhp3ujWD4r4kLcRxVfV0QZ44usvAPLhKoe
cF0feiKtegS1ps+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7Mmpf8MEyGx
WmB+WrynTetWnIV6jTzZA1RmaZuqmIMDVWTA7JNkiDJ0QJBWQ3Ehp+Vn7Li1MCIj
XLEDYJ2wRmcRZQ0bsUzaM/V3p+Q+j8S3osma3Pc6+dDzxl+Og/LnRnLldapXx28X
B9urUR5H030zm77B9/mYgIeM8Y1XntLCCELBeuJeEYJUqc0FsGxWnwjsBtRoZ4dv
a1rvzKxmJJuNIR4YILg8G4kLhr9JDrtyCkVl9Xm86DjQI1J2KpQIJHBLJA0gKxL
Yem8CS0/an3A0xqTNZjWbQx6E320PB/rsU281dadi9c8yeRyXLWpUF4Ghjyoc40d
rAkXmLjnkzLMC459xGL8ggj6Lynb6UzX0eY9A9AgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVg0AwBATAuMCwG
CsGAQUFBwIBFiBodHRwOi8vcmlvdWV3NpdG9yeS5LaWQ0YmVsZ211b55iZTAAdBgNV
H04EFgQUZ+XjTK+ztfMHbwiCDIPZetlb50kwEQYJYZIAyB4qgEBBAQDAgAHMB8G
A1UdIwQYMBaAFGfo8U5Ps7XzB28InAyD2XrZw+dJMA0GCSqGSIb3DQEBCwUAA4IC
AQA1iTyrcumj9h1IRKZNIK1t2hAyNW1jdkYz+fJ57PD0qtpsvmfoZmuP+6rSbhd
i1J9pfi7Yc9fIDwxGwfkfPJAiRB1laxdtpnkoAMEcxQonLnxMiS6/n6nQqIXpb00
34YAYANJn5Lujd5V9I+iv5rrzXjvcZPNxgEB3x6fJdpVapbokhgrDrg1g7XqEY+J
Y1Pmv7dXiZhZ6LN29foBzo1k1o6Wp4UnC4UsFTgx/hN56cjkdxMCR9JHQMMwmc
kk2ZUN2SPYL14xK3dCHAdPcLmjVoUSZoyXEOHM14FTv10deIUCJB/EE0L9M8H0a
pVXIUHsmq01R+A3RD8cvjP9P5FDoxCmeGTqcxKIj1qW57gsrXZ0yDCs7Hy5T5/o
M+G090Lhu9wrH4cMwW8Ns0RyCqZqeghSbd5hE+ALmj4SmxjPht7krQXRGeBf5o6
q+RLHXnFCzBtqJea6U6Apr1SrSvEpk0XLIVs2nt8o/YpAoUMx0rwPRwbjqfL0UUS
6iVKhZALeMBe6gvXpMiTqmlta7cd13yKQBavzuE3QJMPY0XAis6CWA3zUVbznUQ
2Vtk0MBtLQEb+w30sU4eIg/Ak0NJ4/24AFf0zklmB7k93t7Xa/YuVwb8go37wtq
/A9HvfiEImuusfghZ6EU9pvUPmL62NPY54g+nFm2qMtMwQ==
-----END CERTIFICATE-----

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

Type CA/QC
Status undersupervision
Status starting time 2012-01-11T19:45:06.000Z

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 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
6654074619687706565029583663340264770269856720101489447350341548
9667917131633966990337885540161539197154038478640639231113106791
3663589486493118066042504737642498346914368670309047269922309076
6138772412256664686136790625895780242652401177074998149327839849
23682396679386042809154363424543342942381
public exponent: 65537
Subject key identifier 0e3733c7286ebfce5fe62ae698908bacc1e62844
CRL distribution points http://cdp1.public-trust.com/CRL/Omnirroot2034.crl
Authority key identifier 4c3811b898005b5a2b703eaa78e4d5676767a77e

Key usage

keyCertSign

cRLSign

Basic constraints

CA=true; PathLen=0

SHA1 Thumbprint

05e88c57c47c3b510aed61a8c9d427ffe2925c01

SHA256 Thumbprint

4671a19c0fb1e221aeda10c7d745b7e5bf4faaffafc63fc2e2f8add187adab69

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 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: [ 0388]

Certificate Extensions: 6
[1]: 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
]
]

[2]: 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..
]
]

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

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

[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 24 68 74 74 70 73 3A 2F 2F 77 77 77 2E 63 65 .https://www.ce
0010: 72 74 69 70 6F 73 74 2E 63 6F 6D 2F 73 68 6F 77 rtipost.com/show
0020: 70 6F 6C 69 63 79 policy
]] ]

[6]: ObjectID: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:0
]

]
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 07 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...V(
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.....+'...'f
00F0: 28 A9 09 73 9B 93 A7 3F E0 48 8F 9E B5 98 8A F8 (. ? . H

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIELTCCAwGwAwIBAgICA4gWdQYJKoZIhvcNAQELBQAwXDELMakGA1UEBhMCVVMx
GTAXBgNVBAoMEFZLcm16b24gQnVzaW5lc3MxETAPBgNVBAsMCE9tbnR0b290MR8w
HOYDVQDDDBWZWNpem9uIEEdsb2JhbCBSc290IENBMB4XDTEyMDExMTE5NDQzNFowYj
ELMakGA1UEBhMCQkUjHDAaBgNVBAoTE0NlcnRpcG9z
dCBuLnUuL3MuY54xNTAzBgNVBAMTLENlcnRpcG9zdCB0dWJsaWNgO0EgZm9yIFFl
YwpxZm1lZCBTaWduYXR1cmVzMIIBIjANBgkqhkiG9w0BAQEFAAQCAQ8AMIIBCGKC
AQEAow3rmuZKZMnGhQRGeEzZK4THeq59CIqK6BseSxLmZ3sh8znY0FBNK40XmFEj
0Y990nIYAJxnU5bcvS5BFQKpwtD5cFcmP7BR0i6/MyJCE6BMD8wcS61CJfLm
8/p/vRF9KsDfa6fMd/Wlghbq780wa22+UgXpFr27eqBCsUzEiZya5cILWXM0hmP+
ZE30i7pLZ/Dh+50tn/R+P0IVBBIypicnx/ u4Q/1oEqMyy+DF1iuMfCbCpE2Pbw
0R+ScqLFNeR09dLfMj5Xlp5r5K7dKXJP8DgoMw8Cu5fGLU8z2qwx+3ZvOXdxDNF
e2g8HHX4WdMymhSzbmnljGVYrQIDAQABo4HyMIHVMBIGAUdEwEB/wQIMAYBAf8C
AQAwRQYDVRR8gBD4wPDA6BgRVHSAAMDImAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3
LmNlcnRpcG9zdC5jb20vc2hvd3BvbGljeTA0BgNVHQ8BAf8EBAMCAQYwHwYDVR0j
BBgwFoAUTCgRuJgAWLorcd6qe0TVZ2dnp34wQgYDVR0fBDswOTA3oDwgM4YxaHR0
cDovL2NkcDEucHVibG1jLXRydXN0LmNvbS5DUkwvT2luaXV3b3QyMDM0LmNybDAd
BgNVHQ4EFQQUjczxyhuv85f51rmmJCLRMhmKEQnDQYJKoZIhvcNAQELBQADggEB
AHPwWcH8zTefMepGqIMwdsVUnSdYVUkvKAGRYGxdF0EDUYMaw1+I1LD21m5vXm
KJESedvEs0JlqERGoHcM9jigquuNQhgQ4SGsWyyWxLatIMfp2D7FsiNrTcry3y
h2v5fxZ3CyV7o2ZS5+pEvFhvufqZULgZ64/RhPcqlZV74asJUNBRZ756IF3PxxzA
KDN9Ytp8vJw1cs1RoS/0CJ/6aJS8HjBc863Rj39Ssc/LzW+KanvLvvdafCCJ/FN
uaA80VYjHwHsnk1ZjFwBwLp1bJNzIVr2UoSk5cBl60eYCRpeIreXknt5opr6Mn
ciipCX0bk6c/4EiPnrYivg=
-----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

The decoded certificate:

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

Key: Sun RSA public key, 2048 bits
modulus:
21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524
10138907899996057327037799082855868763511239453871155320357733059447691386874174245635141852555021482829759158432322784701980502938218351647645607213503509849133047234960429
39229874921930931967750335049019790482801757213056181588775191965365093248162094887390232254090353829320174804654449299032182277693346689585304048115718426896010472819175682
81756655319850133808983099704728097119747491723603914973200214236187812432050305807187505398614653
public exponent: 65537
Validity: [From: Tue Jul 26 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
SerialNumber: [ 04000000 00010552 64c425]

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

[2]: 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..
]
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [0.3.2062.7.1.0.1.2.0]
[PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.1
qualifier: 0000: 16 22 68 74 74 70 3A 2F 2F 77 77 77 2E 65 2D 74 ."http://www.e-t
0010: 72 75 73 74 2E 62 65 2F 43 50 53 2F 51 4E 63 65 rust.be/CPS/QNce
0020: 72 74 73 20 rts
]] ]
]

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

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
]
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...*.wo...o
0030: F4 EE 22 FC 9D 18 21 72 60 BB 18 80 82 95 FB F9 .."!r'.....
0040: F7 95 24 81 66 C1 B5 C3 B5 D2 B6 76 8B 3B 81 5C ..$.f.....v.;\
0050: B8 A1 0E 2B 01 14 8B 80 09 40 EE F8 60 4C 19 E4 ...+.....@..`L..
0060: 17 CD 27 01 B3 63 12 05 A4 08 C9 B4 BF 9E 50 4E ...'...c.....PN
```


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 cfa61bf3895cfe4244f8e684aedc88feadd14d6aa3c73f5688f2c1e52c9a604

Qualifications

Qualifier: QCForLegalPerson
Assert: atLeastOne
Policy OID: 1.3.21.6.3.10.200.3

The decoded certificate:

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

  Key: Sun RSA public key, 2048 bits
  modulus:
27134891449536663670091338916364605667193647212683610465365919934994474903020635584331677653228200210928489182501819079634477925849223359099983741305164508178246344443502931
30726196783245033886132455060944963076820096698396937698650371176940421592482842807501189962663935196363326061722619537358439485207288895730417811753135105697111634576689466
03482121013634442930239281415342850090702638641852043642713489930032407340925370177326311743127984228484805776174599366828375666985899520987211055858487771113785348435966527
64240089811159449759859139013698249064619618572718739685639915967136410239131574955455289383883587
  public exponent: 65537
  Validity: [From: Sat Jun 15 13:51:47 CEST 2002,
             To: Wed Jun 15 14:21:47 CEST 2022]
  Issuer: O=SWIFT
  SerialNumber: [ 3c09327d]

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

[2]: ObjectID: 2.5.29.14 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 ....
]
]

[3]: ObjectID: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[4]: 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 ....
]
]
```

[5]: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[CN=CRL1, 0=SWIFT]
]]
[6]: ObjectID: 2.5.29.15 Criticality=false
KeyUsage [
Key_CertSign
Crl_Sign
]
[7]: ObjectID: 2.5.29.16 Criticality=false
PrivateKeyUsage: [
From: Sat Jun 15 13:51:47 CEST 2002, To: Wed Jun 15 14:21:47 CEST 2022]
[8]: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
]
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 88 62 A7 9B ...B.....B..b..
0030: A3 D1 34 D6 C3 92 5F 03 1C 1D 39 5C FB 00 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 4Fq.....7..0
0080: 42 A2 DE D6 16 DD FF 81 03 17 6C 5C 7E F5 C2 C6 B.....l\.....
0090: 86 57 8E C7 D7 44 91 BA 09 5D 05 5D 87 1E F3 86 .W...D...].]....
00A0: BB F3 E7 3E 9C 55 53 B9 4A 18 49 01 2B 21 3D 55 ...>.US.J.I.+!+U
00B0: E3 31 DA B3 B5 62 42 00 2B 1D 55 0A CE 8B 28 83 ...l...bB.+U...+.
00C0: D9 46 A0 B5 17 BA 4E 66 88 33 07 0D E2 31 CD BA .F....Nf.3...1..
00D0: 7B AD ED 45 C1 DA C1 A8 FE 86 7E BC 82 40 E4 D4 ...E.....@..
00E0: 2E AC 78 80 91 FE C3 28 ED 42 F6 47 7C 6B 7C E0 ..x....(.B.G.k..
00F0: CA 50 B5 C3 7E 4B 39 AF 70 97 86 79 CB 0C 9E 09 ...P...K9.p..y....
]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIKDCCAAnigAwIBAgIEPAkyFTANBgkqhkiG9w0BAQUFADAQM04wDAYDVQQKEwVt
V0lGVDAeFw0wMjA2MTUxMTUxNDdaFw0yMjA2MTUxMjIxNDdaMBAxDjAMBGNVBAOT
BVNXS0ZUMiIjIjANBgkqhkiG9w0BAQEFAAQCAQ8AMiIBKgKCAQEA1vM1e2UrDY0Y
2yk3+hjUqqg5c8br8qtqzXhsB7Zt99Pen0dTFAsAnFyshdMVIgwwyJb8X3QpFEJ
nh6is3o+JrHfKDPs07ISroFc9LAD7TEGQEnfiCMNjJRH80ce0bLkmbFqv/Gwrsp
/SZRzFUlJjU+PILZaZ3uwVuxQ1ZLkKWLQVGSQJudNhh2qeWUJ3D3SsusRBNS37d4h5
zg3ZV3nmDwuQb0866KRj1YRRY7rau/amjUYegKJe3bhK18yRlYprz25A53XWl7a
z0pKv9obTQINRgg/wNwNdaqwSF2rZLtbZg8UnLomKwq7MTQfn/cHniG00bfntINL
MmbLH5aTQwIDAQABo4HxMIHMBEGCWCAGG+EIBAQQEAWIABzAyBgNVHR8EKzAp
MCegJaJpCewHzE0MAwGA1UECHMfUjdlJRLQxDALBgNVBAMTBENSTEdwKwYDVR0Q
BCQwIoAPMjAwMjA2MTUxMTUxNDdaG08yMDIyMDYxNTEyMjE0N0wCwYDVR0PBAQD
AgEGMB8GA1UdIwQYMBaAFD4wszs1l1f/8UDbG0UB0C4Vp56yMB0GA1UdDgQWBBO+
MLM7NzdX//FA2xtFATguFaeesjAMBGNVHRMEBTADAQH/MB0GCSqGSIb2FQDAAQ0
MA4bCFY1LjA6NC4wAwIEkDANBgkqhkiG9w0BAQUFAAQCAQEA1vM1e2UrDY0Y2yk3
+9A0U8+TwjZtFdSL0g7L9rI/lwIa2jkSSUCbzFtRkjM4pVR0wwYJTndw4IizkzKs
waSK8tnXx/erD3G4167LATfW5E9Cot7WFt3/gQMXbFx+9cLGHLe0x9dEkboJXQVd
hx7zhvz5z6cV05ShhJASshPVXjMdzqzWJcACsdV0r0iyu2UagtRe6TmaIMwcn
4jHNunut7UXB2sGo/oz+v1JA5NQurH1AkF7DK01C9kd8a3zgyLC1w35L0a9wL4Z5
ywyecQ==
-----END CERTIFICATE-----

Quo Vadis Trustlink BVBA

Service provider trade name VATBE-0537698318
Quo Vadis

Information URI https://www.quovadisglobal.com/en-GB/QVRepository.aspx

Service provider street address Steenberg 8

Service provider postal code 3583

Service provider locality Beringen

Service provider state Limburg
Service provider country BE

Quo Vadis BE PKI Certification Authority

Type uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC
Status undersupervision
Status starting time 2014-01-28T13:31:54.000Z

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
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

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
6478935536215699720906056393460135609950257208816552320585654567621525989833435792412071673530213110438235461609950233494658197320013934260142370525768530730648174392038504
89307475026119919108600127180985930937572274379190999324023048980609635572348358816072484994067170269394212885704794032888031826978293616900979564841015208237311036093100150
8185122324633173258785905907612479870628855689431012390109729200781940753684416562294413315647188319356591771633913545892011373776362193636814506011844368620196727006732532
80529883042295074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669
38102871794508560465821983194059528341619175314034894163206925073632423415715700412910266907296199739275914809783683066318757293297556425091860552963585268849419030407270774
1879985054593570602546547329191019290607044365007087591103957060761678635733849781722519130799704308014716559948849072838313070703058851956878669387044135295698957856629370
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 c4f15a9b]
```

Certificate Extensions: 7

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

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

```
[3]: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[URIName: http://crl.quovadisglobal.com/qvrca.crl]
]]
```

```
[4]: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSign
CrL_Sign
]
```

```
[5]: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [2.5.29.32.0]
[ ] ]
]
```

```
[6]: 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]
]
```

```
[7]: ObjectID: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:0
]
```

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

The certificate in PEM format:

```
MIIFFzCCBHEgAwIBAgIUAsr1yU... 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 14:37:52 CET 2014

Not after Tue Feb 11 14:37:52 CET 2025

Serial number 12597032158223217295

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...
  public exponent: 65537
  Validity: [From: Wed Feb 19 14:37:52 CET 2014, To: Tue Feb 11 14:37:52 CET 2025]
  Issuer: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
  SerialNumber: [ aed1a601 8711328f]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 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
]
[2]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
0.4.0.2231.3.0
]
```

Belgique/België (Belgium): Trusted List

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

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

Algorithm: [SHA1withRSA]
Signature:
0000: 16 9B 23 CA D4 FE 95 B8 BA 24 C7 93 8E D7 F3 7F ..#.....$......
0010: 2A 9E DC 7A 14 9E 62 0C 2B 3E 89 A1 03 D7 8D BE *....b.+>.....
0020: CA 3B BF C1 05 54 E0 9F 2B 8D 2E 14 AA C7 4E F3 ;...T...+.....N.
0030: 03 8C E2 C7 F2 2E 33 0B 45 1B 0A EB 4B 1A 67 9A .....3.E...K.g.
0040: 36 BB EB 4B 22 3D 10 AC 54 72 B5 30 F5 58 8B 8F 6..K"...Tr.0.X..
0050: 67 1A 41 8D 05 3C 66 3F FE 68 B9 2B E1 B4 26 CA g.A..<f?.h.+..&.
0060: A8 09 E1 7C C9 67 D0 4C BE 2D 08 BF 5F 23 43 12 .....g.L...#C.
0070: 52 8E F1 A9 5D A5 A9 50 D2 CD 9E 11 0D 4E EC CA R...].P.....N..
0080: BF C7 FF D2 F0 67 D8 89 E6 A6 0E DC C2 08 F6 AB .....g.....
0090: CA A1 67 FD EB D5 99 87 11 34 83 98 47 63 57 8A ..g.....4..GcW.
00A0: 2F 62 BB 80 29 7E 7C 8F 0C 27 45 D8 1A 71 3B 60 (/b...)...'E...q;`
00B0: 42 90 7C F3 EC D9 0E D0 29 DC 55 49 C5 1F 67 79 B.....).UI..gy
00C0: F0 9D BE 35 76 9E E3 7E F9 48 00 DA FF 1D DA EF ...5v....H.....
00D0: 5C F1 CE CE 6C 67 7B 74 BE 8E F6 B4 02 7E F0 56 \...lg.t.....V
00E0: 6F 0E BF 87 D9 E4 5D 22 52 02 32 97 4B 5B AF 9C o.....]"R.2.K[...
00F0: 00 6D AB 77 D0 69 B1 F0 C4 D7 3C AC 84 0F 90 B9 .m.w.i....<.....
]
]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIID3zCCAsagAwIBAgIJAK7RpgGHETKPA0GCsqGSib3DQEBBQAMIGHMS0wKwYD
VQDQEyRCZWxnaWfUIFRydxN0ZWN0qTGLzdCBTY2h1bWUgT3B1cmF0b3IxBTBBHbG
BAO0TQEZQUyBfY29ub215L3BTUUVzL2ZmZWxlLWVtcDxveWVrIGFuZCBFbVYzZ3k
LSBRdWfsaXR5IGFuZCBTYWZldHkxZzAJBgNVBAYTAkRlbnR1eXZlbnVlc290IHR1
Ml0xODI1M0I0MTE5MTE0Y2x1MjIwYjIwMTA0MDEyMDEzMDU2ODI1MDE0MDE5
aXN0IFNjaGVTZSBPcGVyYXRvcjFjMEcGA1UECHNARlBTEiEVjB25vbXksIFNFR
XMsIFNlbgYtZW1wbG95ZW0gYW5kIEVudXNjeSA0IFF1YXpHkgYw5kIFNhZmV0eTEL
MAKGA1UEBHMCKQlwggeEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAIBAQDAgEFk
oDPTyDvGk+/lPnGSPm58NRE7mpzLHK8lXpYnTAtbMhn7FWru9G1Ni+bLYNOEmzN
2E5K09+7AAAMmx2x8zmEMwC3oUQ7E0WN5G1+Y+7n6ntX50D/45bw4IjVvwRRru8
Coj5vq5Hz3JKTgtf8tEpbw5vSFZh6+o91rdX342RJU4AtG78sxZvzIqpa3WsdDM
f5XDyjnGk3dRgkDuo0aBxwEexuUjN4LVO+MacwoaxEqLhEZ6TALGWS2WmNEW30lUD
f7nc0Tz/lnyQsuFn0lC4pg56hjyXltpjyHwNwbTDx+cjBpBve0T9N6UfKfHknC5
AfrIOhnlFXUmYKD/AgMBAAGjTDBKMAKGA1UEdEwCMAAwCwYDVDR0PBAQDAgBAMB0G
A1UdDgQWBRRf745pxfv011rxBwgOUHLQqteQUTARBgNVHSUECjAIBgYEAJE3AwAw
DQYJKoZIhvcNAQEFBQADggEBABabI8RUPw4uiThk47X838qntx6FJ5iDCs+iaED
142+yju/wQVU4J8rjs4Uqsd08w0M4sfyLjMLRRSK60saZ5o2u+tLiJ00rFRytTD1
WiuPzxpBjQU8Zj/+aLkr4b0myqgJ4XzJZ9BMvi3Yv18jQxJ5jvGpXaWpUUNLnhEN
TuzKv8f/0vBn2Inmpg7cwgj2q8qHz/3r1ZmHETSDmEdjV4ovYruAKX58jwvnrDga
cTtGqPB88+zZdTAp3FVjXR9nefCdvjV2nu++UgA2v8d2u9c8c70bGd7dL609rQC
fvBmbw6/h9nkXSJSAjKX5IuvnABtq3fQabHwxNc8rIQPKLk=
-----END CERTIFICATE-----
```

The public key in PEM format:

```
-----BEGIN PUBLIC KEY-----
MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCCKGCAQEAwIBBZKAz02A7xpPvyD5x
kj5ufDUR05qcyx5PJcawJ0wLWzIZ+XvQ7vRptYvm5WGDThJszdh05jvfuwAADJsd
sfm5HDMHN6FE0XNFjeRpfmPu5+jbV+dA/+Em80CI1b8MEUa7vAqI+b6uR89ySk4H
7fLXhkCg+b0HwYevqPYq3V9+NK5V0ALRu/LMwbyKqWt1rHXTH+Vw8o5xit3UYJA
7jmgcVhHsblIjEc7zvjGmMKGsRK14RgekCxLktLpJRFtzpVXh+53NE8/5Z8kLLH
Z9NXOKY0eoY8s57aY8h8DcG0w8fnIwaQb3jk/TW+LHyhR5JwuQH6yDlpx511Jsig
/wIDAQAB
-----END PUBLIC KEY-----
```