

# Belgique/België (Belgium): Trusted List

## *Scheme name*

BE:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

## *Legal Notice*

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

*Scheme territory* BE

*Scheme status determination approach* EUappropriate

*Scheme type*

*community rules* <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

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

*Issue date* 2017-02-16T01:00:00.000Z

*Next update* 2017-08-13T00:00:00.000Z

*Historical information period* 65535 days

*Sequence number* 30

*Scheme information URIs* <https://tsl.belgium.be/>

## ***Scheme Operator***

*Scheme operator name* FOD Economie, KMO, Middenstand en Energie - Kwaliteit en Veiligheid

*Scheme operator street address* NG III - Koning Albert II-laan 16

*Scheme operator postal code* 1000

*Scheme operator locality* Brussels

*Scheme operator state* Brussels

*Scheme operator country* BE

*Scheme operator contact* <http://economie.fgov.be>  
<mailto:be.sign@economie.fgov.be>

## ***Trust Service Providers***

### ***Certipost n.v./s.a.***

*Service provider trade name* VATBE-0475396406

*Information URI* <http://repository.eid.belgium.be>  
<http://www.certipost.be/dpsolutions/en/e-certificates-legal-info.html>

*Service provider street address* Muntcentrum

*Service provider postal code* 1000

*Service provider locality* Brussels

*Service provider state* Brussels

*Service provider country* BE

### ***CN=Belgium Root CA, C=BE***

*Type* CA/QC

*Status* withdrawn

*Status starting time* 2016-09-06T00:00:00.000Z

### ***Service digital identity (X509)***

*Version* 3

*Serial number* 117029288888937864350596520176844645968

*Signature algorithm* SHA1withRSA

*Issuer* CN=Belgium Root CA, C=BE

*Valid from* Sun Jan 26 23:00:00 UTC 2003

*Valid to* Sun Jan 26 23:00:00 UTC 2014

*Subject* CN=Belgium Root CA, C=BE

*Public key* Sun RSA public key, 2048 bits  
modulus:  
2532727247174242475310876111302551541350771290487408393990707355  
3139389403581555633427000903307438065008396155423372038139338001  
1292283973874375661691461475691011321537351475763725785500152445  
9884908283374968661826239871065222401938973133495715806769163244  
2561241462450868417538609485432931629806056877222374520561111218  
9904505418533484099385023144445138975351025575749503679547226381  
0313002138087279503333496722494200200493483881237347138441152657  
9026650775354589375802255665011941485467556333747329602589496041  
6159860774175448506963241118776049541934983183035608916277217984  
30948172071644141969017225065301229219951  
public exponent: 65537

*Subject key identifier* 10f00c569b61ea573ab635976d9fddb9148edbe6

*Authority key identifier* 10f00c569b61ea573ab635976d9fddb9148edbe6

*Key usage* keyCertSign  
cRLSign

*Basic constraints* CA=true; PathLen=unlimited

*SHA1 Thumbprint* dfdfac8947bdf75264a9233ac10ee3d12833dacc

*SHA256 Thumbprint* 7c7ed4240bb253bb35c376e12e00b027f1659df9d8267422a93eed75edc7adfb

*Extension (critical: true)*

**Additional service information**

RootCA-QC

*Extension (critical: true)*

**Qualifications**

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.1.1.1.2.1

Policy OID: 2.16.56.1.1.1.7.1

*Extension (critical: true)*

**Additional service information**

ForeSignatures

*The decoded certificate:*

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

Key: Sun RSA public key, 2048 bits
modulus:
25327272471742424753108761113025515413507712904874083939907073553139389403581555633427000903307438065008396155423372038139338001129228397387437566169146147569101132153735147
57637257855001524459884908283374968661826239871065222401938973133495715806769163244256124146245086841753860948543293162980605687722237452056111121899045054185334840993850231
444451389753510255757495036795472263810313002138008727950333349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
774175448506963241118776049541934983183035608916277217984309481720716444141969017225065301229219951
public exponent: 65537
Validity: [From: Sun Jan 26 23:00:00 UTC 2003,
To: Sun Jan 26 23:00:00 UTC 2014]
Issuer: CN=Belgium Root CA, C=BE
SerialNumber: [ 580b056c 5324dbb2 5057185f f9e5a650]

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

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

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

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

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

---

## Belgique/België (Belgium): Trusted List

---

```
[6]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 10 F0 0C 56 9B 61 EA 57 3A B6 35 97 6D 9F DD B9 ...V.a.W:.5.m...
0010: 14 8E DB E6 .....
]
]
]
Algorithm: [SHA1withRSA]
Signature:
0000: C8 6D 22 51 8A 61 F8 0F 96 6E D5 20 B2 81 F8 C6 .m"Q.a...n. ....
0010: DC A3 16 00 DA CD 6A E7 6B 2A FA 59 48 A7 4C 49 .....j.k*.YH.LI
0020: 37 D7 73 A1 6A 01 65 5E 32 BD E7 97 D3 D0 2E 3C 7.s.j.e^2.....<
0030: 73 D3 8C 7B 83 EF D6 42 C1 3F A8 A9 5D 0F 37 BA s.....B.?.].7.
0040: 76 D2 40 BD CC 2D 3F D3 44 41 49 9C FD 5B 29 F4 v.@...?.DAI...[]).
0050: 02 23 22 5B 71 1B BF 58 D9 28 4E 2D 45 F4 DA E7 .#[q...X.(N-E...
0060: B5 63 45 44 11 0D 2A 7F 33 7F 36 49 B4 CE 6E A9 .cED...*.3.6I..n.
0070: 02 31 AE 5C FD C8 89 BF 42 7B D7 F1 60 F2 D7 87 .l.\....B.?.]`...
0080: F6 57 2E 7A 7E 6A 13 80 1D DC E3 D0 63 1E 3D 71 .w.z.j.....c.=q
0090: 31 B1 60 D4 9E 08 CA AB F0 94 C7 48 75 54 81 F3 l.`.....HuT...
00A0: 1B AD 77 9C E8 B2 8F DB 83 AC 8F 34 68 E8 BF C3 ..w.....4k...
00B0: D9 F5 43 C3 64 55 EB 1A BD 36 86 36 BA 21 8C 97 ..C.dU...6.6!..
00C0: 1A 21 D4 EA 2D 3B AC BA EC A7 1D AB BE B9 4A 9B .!...;.....J.
00D0: 35 2F 1C 5C 1D 51 A7 1F 54 ED 12 97 FF F2 6E 87 5/\..Q..T.....n.
00E0: 7D 46 C9 74 D6 EF EB 3D 7D E6 59 6E 06 94 04 E4 .F.t...=.Yn....
00F0: A2 55 87 38 28 6A 22 5E E2 BE 74 12 B0 04 43 2A .U.8(j"^..t...C*
```

]

### *The certificate in PEM format:*

```
-----BEGIN CERTIFICATE-----
MIIDLDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBqkqhkiG9w0BAQFADAN
M0swCQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ211bSB5b290IENBMB4XDTAzMDUy
NjIzMDAwMFoXDTE0MDEyMjIzMDAwMFowZjZELMkGA1UEBHMCAwGDAWBgNVBAMT
D0JlbGdwdW0gUm9vdCBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMiHcckCRKJ5eHFvna6pKsot03HIOswkVp19eLSz8hMFJhCWK3HEcVAQGa+X0S
J4fpn0VxTiIIs0RIYqjBeoiG52bv/9nTrMQHn035Y5EWTXaJqAFPrSjmcPpLHZXB
MFjqvNl12Jq0i0tJRLlf01MVDssUXRlJsw9q09P9vMI7EU/CT9YvzvU7wCMgTVy
v/cY6pZ1f5sofxVsY9LKyn0FmMtB20yvmi4BUCuJhWpmbxM0jvxKuTXgfeMo8S
dKpbNCNuwOpszv42kqgJF+qhLc9s44Qd3ocuMws8d0IhUDiVL1z95cYx+dtA+mqh
pIqTm6chBocdJ9PEoc1msG8CAwEAa0BuzCBuDA0BgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAEOzA5MDcGBW4A4QEBMCAwLAYIKwYBBQUHAgEw
IGh0dHA6Ly9yZXBvc210b3J3J5LmVpZC51ZWxnaXVtLmJlMB0GA1UdDgQWBQ8Axw
m2HqVzq2Nzdt925F17b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth61c6tjWxbZ/duRS02+YwDQYJKoZIhvcNAQEFBQADggEBAMhtILGKYfgP
lm7VILKB+MbcxYA2s1q52sq+llIp0xJN9dzoWbZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0A1M1w3Ebv1jZKE4tRfTa57VjRU0RD5p/
M3825bT0bqkCMA5c/ciJv0J71/Fg8teH9Lcuen5qE4Ad30PQYx49cTGxYNSeCMqr
8JTHSHVUgFmbrXec6lKP240sjzRr6L/D2fVDw2RV6x9NoY2u1GMLxoh10ot06y6
7Kcdq765Sp1LxxCHVGNHITtEpf/8m6HFubJdNbv6z1951luBpQE5KJVhzgoaiJe
4r50ErAE0yo=
-----END CERTIFICATE-----
```

## **CN=Belgium Root CA2, C=BE**

Type	CA/QC
Status	granted
Status starting time	2016-07-01T00:00:00.000Z

### *Service digital identity (X509)*

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

*Public key* Sun RSA public key, 2048 bits  
modulus:  
2505202035897286929802442931365977782136110157856742564234839581  
6436795380283967224876983130034020316820575216355360416605004533  
4718830407023741150537135469000352360279650474826843696574001315  
5524363953296559605768293726462748683867807979476223046936921095  
0088797578757728341339292333654654510981797643030670179357915156  
5262158435123606358334230710497624432217765218126527057253528859  
3688668361490384043063624052887014382463758810568004079588144865  
4643858460532713400822409146679502714797245542101554942867836639  
3080491585356622044306227220916440412947986826263456222477031966  
11536459503012648921426461410998536799349  
public exponent: 65537

*Subject key identifier* 858aebf4c5bbbe0e590394ded6800115e3109c39

*Authority key identifier* 858aebf4c5bbbe0e590394ded6800115e3109c39

*Key usage* keyCertSign  
cRLSign

*Basic constraints* CA=true; PathLen=unlimited

*SHA1 Thumbprint* 51cca0710af7733d34acdc1945099f435c7fc59f

*SHA256 Thumbprint* 9f9744463be13714754e1a3becf98c08cc205e4ab32028f4e2830c4a1b2775b8

*Extension (critical: true)*

*Additional service information*

RootCA-QC

*Extension (critical: true)*

*Qualifications*

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.9.1.1.2.1

Policy OID: 2.16.56.9.1.1.7.1

*Extension (critical: true)*

*Additional service information*

ForeSignatures

*The decoded certificate:*

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

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

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

## Belgique/België (Belgium): Trusted List

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

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

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

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

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

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

### The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIIVKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMakGA1UE
BHMCCkUxGTAXBgNVBAMTEEJlbgDpdW0gUm9vV2V3ZjYyYzY3ZjYyYzY3ZjYyYzY3
WhcNMjExMDgwMDAwMjE0MDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQw
bSB5b290IENBMjCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi790hqC/7bIYLS2X+an7mEoj39WN4IzGMhwLQdC1i22bi+n9fzGhYJdld61
IgdMqFNA68KNaJ6x+HK92AQZw6nUHMxU5wfIp8MXW+2QbyM69odRr2nLL/zGsvU
+400HjPIlTfsjFPekx40Hop0cSZYtF3CiInaYnkJIT/e1wEYnm7hLHADBGXvmAYr
XR5i3FVr/mZkIV/4L+HXmymvb82fqqxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y
HewApDggLVrH1Tdjuk+bqv5WR15j2Qsj1Yr6tSPwiRuhFA0m2khw0I8w7QUmecFL
TqG4f1V50mLGHUCAWEAa0BuzCBuDA0BgNVHQ8BAF8EBAMCAQYwDwYDR0TAQH/
BAUwAwEB/zBCBgNVHSAE0zA5MdcGBWA4COEBMCAwLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3JlMlVpZC5lZWxnaXVtLmJlM0GA1UdDgQWBBSFiuovxbu+dLk0
lN7WgAEV4xc0TARBg1ghkgBhvCAQEEBAMCAAcwHwYDR0jBBgwFoAUHyr9MMW7
vg5ZA5Te1oABFeM0NdKwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyCc
UwnzSgEMdL8rs5qauhjyC4isHLMzr87LEwEnkoRYmhCS98wUkmt0F0qW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTLBFk0pvDVTc9rejj7NqZV3JcqUWumyaa7YwB0+mPyW
nIR/VRPmPIfjvCCKpDZoa01gZhz5v6yALGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9F7J3bTc0R5/0UA0NmXsImABKgX770FP67H6d96tK8QYUn8pJQsKpv02F
sauB0eYxUjU4c5nUwFAA4+Bw11V0S0U7Q2dmS23G7rPUZUFF1eR10NeE3gJ7u0
hXY=
-----END CERTIFICATE-----
```

**CN=Belgium Root CA3, C=BE**

*Type* CA/QC  
*Status* granted  
*Status starting time* 2016-07-01T00:00:00.000Z

***Service digital identity (X509)***

*Version* 3  
*Serial number* 4260689877497748905  
*Signature algorithm* SHA1withRSA  
*Issuer* CN=Belgium Root CA3, C=BE  
*Valid from* Wed Jun 26 12:00:00 UTC 2013  
*Valid to* Fri Jan 28 12:00:00 UTC 2028  
*Subject* CN=Belgium Root CA3, C=BE  
*Public key* Sun RSA public key, 4096 bits  
modulus:  
6892368425204007372930073294443554123229459767731895868437789352  
7489331012499470148015728120971091408928778599011263917331397388  
7322735841404218927092481342245128960306942910996978037963366658  
7487677438166762048712847334427499268969797276699412687279269161  
8545497053924331052069875135564437218371995289927129772075947532  
4004770387044092331280439040222928977901876514295420628487235605  
7207547181546555365474067211993745122880348947938978158987337436  
1336080842299846657331444909264877243429847318212868757946477794  
3923944626874903980284954943444633165097044418808053302806567480  
3973101653181735709840274950639311977298375764568509245075873047  
9725560212981580096389424844703793712327092036866308035191942506  
8313464980278629369152701697759736384202776541620591588545291932  
4663214995529533375563259732378154805928106136809503809799800229  
2920617503904475332163393814047794956959421382197572947310250836  
6454723047943333937457964148701121644586439773493445613256431505  
4516896008070464718986221218972698235178969696880747332055597346  
5056144482367929251906090063565458141797098055228581790278906951  
4772158596504768735853434600634865427052445967408799471479389419  
0325164983453802445254424012949618662017893008747941892318218022  
78084190173776931  
public exponent: 65537

*Subject key identifier* b8bc6c008f5b19859d25019cf019dc408ed0382b

*Authority key identifier* b8bc6c008f5b19859d25019cf019dc408ed0382b

*Key usage* keyCertSign  
cRLSign

*Basic constraints* CA=true; PathLen=unlimited

*SHA1 Thumbprint* fd6b835c99b99e6ff84fcd0e6266a3610786a717

*SHA256 Thumbprint* a8d14e945e3e5156bcae5e39737cf6a1b1f51028bbbf982f50ce5f4c05568b4d

***Extension (critical: true)***

***Additional service information***

RootCA-QC

***Extension (critical: true)***

***Qualifications***

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.10.1.1.2.1

Policy OID: 2.16.56.10.1.1.7.1

### *Extension (critical: true)*

#### **Additional service information**

#### ForeSignatures

#### *The decoded certificate:*

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

Key: Sun RSA public key, 4096 bits
modulus:
68923684252040073729300732944435541232294597677318958684377893527489331012499470148015728120971091408928778599011263917331397388732273584140421892709248134224512896030694291
09969780379633666587487677438166762048712847334427499268969797276699412687279269161854549705392433105206987513556443721837199528992712977207594753240047703870440923312804390
40222928977901876514295420628487235605720754718154655536547406721199374512288034894793897815898733743613360808422998466573314449092648772434298473182128687579464777943923944
62687490398028495494344463316509704441880805330280656748039731016531817357098402749506393119772983757645685092450758730479725560212981580096389424844703793712327092036866308
0351919425068313464980278629369152701697759736384202776541620591588545291932466321499552953375563259732378154805928106136809503809799800229292061750390447533216339381404779
4956959421382197572947310250836645472304794333937457964148701121644586439773493445613256431505451689600807046471898622121897269823517896969688074733205559734650561444823679
2925190609006356545814179709805522858179027890695147721585965047687358534346006348654270524459674087994714793894190325164983453802445244240129496186620178930087479418923182
1802278084190173776931
public exponent: 65537
Validity: [From: Wed Jun 26 12:00:00 UTC 2013,
To: Fri Jan 28 12:00:00 UTC 2028]
Issuer: CN=Belgium Root CA3, C=BE
SerialNumber: [ 3b2102de 965b1da9]

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

]

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

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

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

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

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

]

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



0070: 7E 9C F1 9B 8F 48 93 F0 36 25 6C 40 87 15 D5 44 .....H..6%l@...D
0080: 7C 0E BB 74 CC 1A 24 38 5B F5 72 55 AC 31 8F 04 ...t..\$8[rU.1..
0090: 0C 3B C4 E7 78 10 E8 99 B9 A4 5E C2 3D 6C 8D 0E ;.x.....^.=L..
00A0: C5 65 21 D8 0E 5D 2A 5A AE D2 C6 2F 13 47 73 F3 .e!..]\*Z.../..Gs..
00B0: 10 F1 AF D6 64 99 9A 98 70 F2 0A 8B 30 99 95 A3 .....d...p...0...
00C0: F5 66 C4 A5 0A 2E 52 DF 58 27 DC 45 0F F9 F7 76 .f....R.X'.E...v
00D0: D6 AE 99 5E 05 3E E7 4F EA 82 88 7F D1 45 1A 1D ...>..0....E..
00E0: 1A 5E 74 F4 01 11 2F C5 61 CD 88 41 9D 97 8E 19 ^t.../..a..A...
00F0: 9E 4F 03 3E F4 B9 3B B6 7C C7 78 7A 77 76 00 A8 .0>...;...xzwv...
0100: 39 F7 1E C8 F5 1A 56 45 A2 5C 5E 9C 34 0B EF 90 9.....\..4...
0110: 35 44 2E F5 DF 26 94 71 C1 C4 5F 4B 92 AC E6 86 5D...&.q...K....
0120: 9F 39 F8 FC D5 1C C6 51 B9 A9 C2 5D AE B0 E7 82 .9.....Q...]....
0130: 47 07 56 13 C8 0F BD B7 D6 35 04 02 F0 C2 6A B8 G.V.....5...].
0140: 39 79 1D 07 AE CD 47 AC 4D 75 2A 5D E1 24 C8 03 9y.....G.Mu\*].\$.
0150: A8 E9 89 C5 DE 0D 2A 19 C2 C8 F4 D5 EE B2 38 B5 .....\*......8..
0160: 7A 04 54 67 B0 78 5C 2B C6 E7 69 53 07 B5 A0 77 z.Tg.x\+..iS...w
0170: FC 15 17 34 B7 7F 89 80 99 84 C6 25 71 FE 37 F9 ...4.....%q.7..
0180: 6B 04 11 8A B9 32 79 5E 77 09 6A 58 85 50 AC 46 k.....2y^w.jX.P.F
0190: 3F A5 66 37 26 9A 2D 41 79 22 54 EA 08 D0 86 1C ?.f7&.-AY"t.....
01A0: F2 D2 5C E8 03 A2 4B 76 1B DA 4D C0 59 B6 B7 B0 ..\...Kv..M.Y...
01B0: 1C A7 00 26 7A 09 0C 36 98 1C 81 37 7E AA 4D B2 ...&z..6...7..M..
01C0: 96 31 1A 4F CC 1F F7 9D E3 50 01 5E 75 BA 4D DE .1.0.....P.^u.M..
01D0: D5 FF DE 2F AE BC 73 8E 99 68 D0 3B 12 60 DA 55 .../..s...h.;`..U
01E0: 4A 90 2F 9B 91 66 B6 16 B4 C1 0D DA E5 11 65 5A J./..f.....eZ
01F0: 2E B6 3E 33 EC 5E 21 CB 6B 0B 45 A7 3F BB B8 C6 ..>3^!..k.E.?....

]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFjjCCA3agAwIBAgII0yEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BHMCCkxkGTAxGjBnVBAWMTeeJLbGpdwQ0Um9vdCBDQTMwHhcNMTMwNjI2MTIzMDAw
WhcNMjgwMTI4MTIwMDAwMjA0MQswCQYDVQQGEWJCRTEZMBCGAIUEAxMQQmVzZ211
bSB5b290IENBMzCCAIwDQYJKoZIhvcNAQEBBQADAgIPADCCAgCggIBAKjyAZ2L
g8kHoIX7JLc3BeZ1Tzy9MEv7Bnr59xcJezc/xJJd04V3bwM1tKfFVnqsQ5H/GQAD
FJ0GmTLPLD15AoeUjBubRZ9hwrUuQ11+vhtoVhuEuZuxofEIU2yJti500Nwpo/G
Ib9C4YZSh+71tDpC3MvsFyyordpZgwgShvFWtCmL55SpU05Ubf7ZVPcfVf24A5IG
HLpZTgQfAvnzPlm++eJY+sNoNzTBoe6iZphmPbxuPncJ6sLV8hMQQk50/g+KmoPp
HX4AvoTr4/7TMTvuK8j51dEn+fdvKdx9qo9ZZRHFW/TXEn55rNUu99xhzLE/wBur
rVwFoKWCjcm00CnekJLw0NTr3HBTG5D4A1DjNFUYaIcGJK/ha9rzHzY+WpGdoFZx
hbP83ZGeoqkgBr8Uzf0FCY8cyUN2db6hpIak6Nuoho60Wnn+TSNh5Hjuis5mqGx
S73gYLTQww16h8gFTJ049fiS+QHLwRw5cqFuqfLE3nFFF9KIam54TSe7T4dNGY
2VbHzpaGVT4wy+fL7gWsfauKvM4b00DzgdIj9BHiKytNLMzoa3Snejj/Ckur0dJ
50dMiAqUpSd00e8pdIbmQm1oP5cjk1Qjxx7+vSxWtaccpGowWK8+7oEsYc+7fL7t3
GD6q/05xi440Pd/sFjmfqRf3C1PPMdBqXcwjAgMBAAGjgbswgbwDgYDR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDR0gBDSw0TA3BgVg0AoBATAuMcWg
CCsGAQUFBwIBFIBodHRwOi8vcmlvb3NpdG9yeS51aWQumVzZ211bSB5b290IENBMz
H04EFgQUuLxsA19bGYWdJQgC8BncQ1700CsweQYJYIZIAyB40gEBBAQDAgAHMB8G
A1UdIwQYBAAFLi8bACPWxmFnsUBnPAZ3EC00DgrMA0GCSqGSIb3DQEBBQUAA4IC
AQBFIjv/mKX+VcyxEacckgx4L8XvFKIFPXzjEnDnAtCCKR0U/k5n1jjVK+0D0n+Q
4kJg6Nd7K47+zTXcrSe1tB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpdl
f14HcUPCYLA5TCapZU0MnAbzfpzxm49Ik/A2JWxhXVRHw0u3TMG1Q4W/VyVawx
jwQM08TneBDombmkXsI9bI00xWUj2A5dKlqu0sYvE0dz8xDr9ZkmZqYcPIKiZCZ
laP1zS5Lc15531gn3EUP+fd21q6ZxgU+50/qgoH/0UuaHRpedPQ8ES/FYc2IQZ2X
jhmeTmW+9Lk7tnzHeHp3dgCo0fceyPUaVkwjWmWcNvkvDVELvXfJpRxcRf55Ks
5oaF0fj81RzGUbmpwL2us0eCRwdWE8gPvbFWNQC8MjqudL5HdeuzUesTXUqXeEk
yAO06YnF3g0qGcL19NXusjilegRUZ7B4XCvG52LTB7Wgd/wVFzS3f4mAmYTGJXH+
N/LrBBGkuTJ5XncJa1iFUKxGP6VmYaaLUF5ILTqC9CGHPLSX0gDokt2G9pNwFm2
t7AcPwAmegkMnpgcgTd+qk2yljEaT8wF953jUAFedpbN3tX/3i+uvH00mWj00xJg
2LVKkC+bkWaZFrTBDdrLEWValrY+M+xeIctrc0WnP7u4xg==
-----END CERTIFICATE-----

CN=Belgium Root CA4, C=BE

Type CA/QC
Status granted
Status starting time 2016-07-01T00:00:00.000Z

Service digital identity (X509)

Version 3
Serial number 5706940941790920504
Signature algorithm SHA256withRSA
Issuer CN=Belgium Root CA4, C=BE
Valid from Wed Jun 26 12:00:00 UTC 2013
Valid to Fri Jan 28 12:00:00 UTC 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* c3fbf37259af0954eeee4282dd1c7226a54e7150f7c29a2c495ba34dbfe09ca0

### *Extension (critical: true)*

#### **Additional service information**

RootCA-QC

### *Extension (critical: true)*

#### **Qualifications**

Qualifier: QCQSCDStatusAsInCert

Assert: atLeastOne

Policy OID: 2.16.56.12.1.1.2.1

Policy OID: 2.16.56.12.1.1.7.1

### *Extension (critical: true)*

#### **Additional service information**

ForeSignatures

#### *The decoded certificate:*

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

    Key: Sun RSA public key, 4096 bits
    modulus:
    6224115906824122031433393414467734255795749661242697041972796971
    35225688053118958013272845856830766072936328678029599339864160757582078179782933477127775842726474054125659177491124497441056063625089004297867088236553695896006649963591692
    69749224840725363125898523192670130240309448199566397525648798859959407975137564912472231555839895845986255776615614957078778639852690834243820196276106693555767675903287437086963541879185923650029046515083278917967647521237597009772305977998793131431294613895800952932706979563974285054085448116681005880530871902042900046595950005402044763615671403742873845557572387796136829835237636572157056930341887317395041724077153273812340656631169285909614088148597571435590015303468415145989048851382996128659913957557151628158834154492889031783084088844009310182142365979807396066210319470759450039107508536195377707761075688418384343286045715157573426989301124463242723093299927147162988283928766947013625480426811137103293454625262051881732832104879637264017398565292090224855096446539393723135313244013015486792504471132824903136816339047745407340214082204078193963133511429055306278731837
```

# Belgique/België (Belgium): Trusted List

```
08696354187918592365002904651508327891796764752123759700977230597799879313143129461389580095293270697956397428505408544811668100588053087190204290004659595000540204476361567
1403742873845557572387796136829835237636572157056930341887317395041724077153273812340656631169285909614088148597571435590015303468415145989048851382996128659913957551516281
5883415449288903178308408884400931018214236597980739606621031947075945003910750853619537707761075688418384343286045715157573426989301124463242723093299927147162988283928766
9470136254804268113710329345462526205188173283210487963726401739856529209022485509644653939372313531324401301548679250447113282490313681633904774540734021408220407819396313
3511429055306278731837
public exponent: 65537
Validity: [From: Wed Jun 26 12:00:00 UTC 2013,
           To: Fri Jan 28 12:00:00 UTC 2028]
Issuer: CN=Belgium Root CA4, C=BE
SerialNumber: [ 4f33208c c594bf38]

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

]

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

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

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

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

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

]

Algorithm: [SHA256withRSA]
Signature:
0000: 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(...;...
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 0D 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 3B 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 B6 A8 CB 4C 59 >b.....>.Y...LY
```

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFjjCC3agAwIBAgIITzGjMjMwUvzgwDQYJKoZIhvcNAQELBQAwKDELMAkGA1UE
BHMCMQkxGTAXBgNVBAMTEEJlbgdwdW0gUm9vdCBDQ0QwHhcNMTMwNjE2MTIwMDAw
WhcNMjg1MTI4MTIwMDAwWjAoMQswCQYDVQ0GQwEJCRTZMBG81UEAxAQoMVsZ2L1
bSBSb290IENBNDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgCggIBAJiQrvrH
Hm+04AU6syN4TNHwL91PFsY6E9euwVmL5NAWtdw9p2mcnEOYgX424jFLpSQVnxx
xoh3LsIpdWUMRQfuiDqzvZx/4dCBaeKl/AMRJuL1d6wU73XKSkdR5uH6H2Yf19z
SiU0m2x4k3aNLyT+VryF11b1Prp67CBk630BmG0WUaB+ExtBHOkfPaHRHFA04Mig
oVft3gLQRgh1V+H1rm1hydTz6d6zpoJHp3ujWD4r4kLCrxVfV0QZ44usvAPLhKoe
cF0feikteqS1p5+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7Mmpf8MEyG
WMB+WrynTetWnIV6jTzZA1RmaZuqmIMDvMTA7JNkiDJQ0JBWQ3Ehp+Vn7Li1MCij
XLEDYJ2wRmcRZQ0bsUzaM/V3p+Q+j853osma3Pc6+dDzXL+Og/LnRnLdDapXx28X
B9urUR5H030zm77B9/mYgIeM8Y1XntLCCLEBeuJeEYJUqc0FsGxWnWjsBtRoZ4dv
a1rvzKXmjJuNIR4YILg8G4kLhr9JDrtYckvI9Xm8GDjQIJJ2KpQiJHBLJA0gKxL
Yem8CS0/an3A0xqTNzjWbQx6E320PB/rsu28Ldadi9c8yeRyXLWpUF4Ghjyoc40d
rAkXmLjnkzLMC459xGL8gj6Lynb6UzX0eYA9AgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEMAG8A1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVgOwBATAUwMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmlvb3NpdG9yeS51aWQwYmVsZ2L1bS5iZTAuZG9u
VH04EFGQUZ+jxTk+ztfMhwiCdIPZetLb50kwEQYJYIZIAyb40gEBBAQDAgAHMB8G
A1UdIwQYBAAFGfo8U5Ps7XzB28InAyD2XrZw+dJMA0GCsG5Ib3DQEBGUAA4IC
AQA1iTyrcumj9h1IRKZNIKL2hAyNW1jdkYz+fJ57PD0qtpsvmfoZmuP+6rSbhd
i1J9pfi7Yc9fIDwxGwfkIPJAiRBL1axdtpnkoAMEcxQonLnxMiS6/n6nQIXpb00
34YAYANJn5Lujd5V9I+iv5r rzXjvcZPNxgEB3x6fJdpVapbokhgrDrg1g7XqEY+J
Y1JpMv7dXiZh26LN29foBzoiKlo6Wp4UnC4UsFTgx/hN56cjkdXMC9JHQMMmcCz
kk2ZUN2SPYL14xK3dCHAdPcLmjVoUsZoyXEOHM14FTvV10deIUCJB/EE0L9M8H0a
pVLIUhsMq01R+A3RD8cvjP9P5FDoxCmeGTrcXKIj1qW57srxZ0yDCs7HyST5/o
M+GQ90Lhu9wrH4cMw8Ns0RyCqZqeghSbd5hE+ALmj45mxjPh7krTQXRgeb5o6
q+RLHXnFCzBtqJea6U6Apr15rSvEpk0XLIVs2nt8o/YpAoUMx0rwrPRwbjql0UUS
6IvKZHALeMB66vXpMiTqmlta7cd13yKJQBavzuE3QJMPY0XAis6CWA3zUVbznuQ
2Vtk0MBTlQEb+w30sU4eTg/AkONJ4/24AF0zkLm87k93t7Xa/YuVwB8go37wtq
/A9HvFieImuusfghZ6EU9pvUPmL62NPY54g+nFm2qMtMwQ=
-----END CERTIFICATE-----

CN=Certipost Public CA for Qualified Signatures, O=Certipost

n.v./s.a., C=BE

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

Service digital identity (X509)

Version 3
Serial number 904
Signature algorithm SHA256withRSA
Issuer CN=Verizon Global Root CA, OU=OmniRoot, O=Verizon Business, C=US
Valid from Wed Jan 11 19:45:06 UTC 2012
Valid to Tue Jan 11 19:44:34 UTC 2022
Subject CN=Certipost Public CA for Qualified Signatures, O=Certipost n.v./s.a., C=BE
Public key Sun RSA public key, 2048 bits
modulus:
2058370808117806886719567856147320061945292190592796129179327367
1328005822028265845465542836756717140506081882114668638826442932
4840744781703307017746497136667158332106505285154357277431791645
6871430942741492265542773700746837231916763966290548158739950199
2029174676515494584699514099891322542890739713299134792579834056
6654074619687706565029583663340264770269856720101489447350341548
9667917131633966990337885540161539197154038478640639231113106791
3663589486493118066042504737642498346914368670309047269922309076
6138772412256664686136790625895780242652401177074998149327839849
23682396679386042809154363424543342942381
public exponent: 65537
Subject key identifier 0e3733c7286ebfce5fe62ae698908bacc1e62844
CRL distribution points http://cdp1.public-trust.com/CRL/Omniroot2034.crl

*Authority key identifier* 4c3811b898005b5a2b703eaa78e4d5676767a77e

*Key usage* keyCertSign  
cRLSign

*Basic constraints* CA=true; PathLen=0

*SHA1 Thumbprint* 05e88c57c47c3b510aed61a8c9d427ffe2925c01

*SHA256 Thumbprint* 4671a19c0fb1e221aeda10c7d745b7e5bf4faaffafc63fc2e2f8add187adab69

*Extension (critical: true)*

*Additional service information*

ForeSignatures

*The decoded certificate:*

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

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

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

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

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

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

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

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

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

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

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIELTCCAxiGwAwIBAgICA4gwDQYKoZIHvcNAQELBQAwXDELMAKGA1UEBHMCMVVMx
GTAXBgNVBAoMEFZlcm16b24gQnVzaW5lc3MxETAPBgNVBAsMCE9tbnlSb290MR8h
HQYDVQODDBZWXZjcm9uIEEdsb2JhbCB5b290IENBM4XDTEyMDE5NDUwNlloX
DTIyMDE5NDUwNlloXZlcm16b24gQnVzaW5lc3MxETAPBgNVBAsMCE9tbnlSb290MR8h
dCBLNlYUL3MuYS4xNTAzBgNVBAMTElcnRpcG9zdCB0dWJsaWMyMDE5NDUwNlloX
YkxpZm1lZCBTaWduYXR1cmVzMIIBIjANBgkqhkiG9w0BAQFAAQCAQ8AMIIBCgKC
AQEAow3rmuZKZMnGhQRGeEzK4Theq59CIqK6BseSxLmZ3sh8znY0FBNK40XmFEj
0Y99QnIYAjxnU5bcvS5BFQKpwtD5cFcmP7BR0i6/MyJCE6BMD8wcS61CJfLlM
8/p/VRf9KsdFaf6fMd/Wlghbq780wa22+UgXpFr27eqBCsUzEiZya5cILWXM0hmP+
ZE30i7pLZ/Dh+50tn/R+P0IVBBIypicycnx/u4Q/loEqMyy+DFliuMfCbCpE2Pbwz
0R+SCqLfnER09d1fmJ5XlpSr5K7dKXJP8Dg0Mw8Cu5fGLU8z2qqqx+3Zv0XdDNF
e2g8HX4wdMymhSzbmLjGVYrQIDAQABo4HyMIHvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwRQYDVRR0gBD4wPDA6BgRVHSAAMDImAYIKwYBBQUHAgEwJGh0dHBz0i8vd3d3
LmNlcnRpcG9zdC5jb29vc2hvvd3BvbGljeTA0BgNVHQ8BAf8EBAMCAQYwHwYDVR0j
BBgwFoAUTDgRuJgAw1orrcD6qe0TVZ2dnp34w0gYDVR0fBDswOTA3oDWgM4YxaHR0
cDovL2NkcDEucHVi1bG1jLXRydXN0LmNvbS59DUkwvT21uaXJvb3QyMDM0LmNybDAD
BgnVH04EFgQUUDjczxyhu85f51rmmJCLrMhmKEQwDQYKoZIHvcNAQELBQADggEY
AHPwVwcH8zTeSFMePggIMwdsVUnSdYVUkvKAGRYGxdF0EDUyMawL+I1LD21mSxVM
KJSEdVes0JlqERGoHcM9jigquuN0hg04SGsWyyWxwLatIMfp2D7FsiNrTcr3y3
h2v5fxZ3Cyv7o2ZSS+pEvFhvuFqdZULgZ64/RhPcqLZV74asJuNBRZ756IF3PxxzA
KDN9Ytp8vJwLcs1RoS/0CJ/6aJ58HjBc863Rj39SscL/zZW+KanvLvDafCCJ/FN
uaA80VYjHMHsnk1ZjFWBwLpibJNzIvR2UoSkR5c8ln60eYCRpeIreXknt5opr6Mn
ciipCX0bk6c/4EiPnrWYivg=
-----END CERTIFICATE-----

CN=Certipost E-Trust Primary Qualified CA, O=Certipost

s.a./n.v., C=BE

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

Service digital identity (X509)

Version 3
Serial number 4835703278459639067624485
Signature algorithm SHA1withRSA
Issuer CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
Valid from Tue Jul 26 10:00:00 UTC 2005
Valid to Sun Jul 26 10:00:00 UTC 2020
Subject CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE

*Public key* Sun RSA public key, 2048 bits  
modulus:  
2198165027276639742335246370299919491834299685174947076499863829  
7101984511083629850948734739259892644517804066934196324549964291  
3192950780187748886826305662589231481198165241013890789999605732  
7037799082855868763511239453871155320357733059447691386874174245  
6351418525550214828297591584323227847019805029382183516476456072  
1350350984913304723496042939229874921930931967750335049019790482  
8017572130561815887751919653650932481620948873902322540903538293  
2017480465444929903218227769334668958530404811571842689601047281  
9175682817566553198501338089830997047280971197474917236039149732  
00214236187812432050305807187505398614653  
public exponent: 65537

*Subject key identifier* f078f9077710bbdc1ea1ae79fb3010dbc634f817

*Key usage* keyCertSign  
cRLSign

*Basic constraints* CA=true; PathLen=unlimited

*SHA1 Thumbprint* 742cdf1594049cbf17a2046cc639bb3888e02e33

*SHA256 Thumbprint* 058a40323ec8c46262c3052a5d357b91ac24d3da26351b3ff4407e99f7a4e9b4

*Extension (critical: true)*

*Additional service information*

RootCA-QC

*Extension (critical: true)*

*Qualifications*

Qualifier: NotQualified

Assert: atLeastOne

Policy OID: 0.3.2062.7.1.1.112.1

Policy OID: 0.3.2062.7.1.1.140.1

Policy OID: 0.3.2062.7.1.1.111.1

*Extension (critical: true)*

*Additional service information*

ForeSignatures

*The decoded certificate:*

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

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

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

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





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

## ***SWIFTNet PKI Certification Authority***

*Type* CA/QC  
*Status* granted  
*Status starting time* 2016-07-01T00:00:00.000Z

### ***Service digital identity (X509)***

*Version* 3  
*Serial number* 1007235709  
*Signature algorithm* SHA1withRSA  
*Issuer* O=SWIFT  
*Valid from* Sat Jun 15 11:51:47 UTC 2002  
*Valid to* Wed Jun 15 12:21:47 UTC 2022  
*Subject* O=SWIFT  
*Public key* Sun RSA public key, 2048 bits  
modulus:  
2713489144953666367009133891636460566719364721268361046536591993  
4994474903020635584331677653228200210928489182501819079634477925  
8492233590999837413051645081782463444435029313072619678324503388  
6132455060944963076820096698396937698650371176940421592482842807  
5011899626639351963633260617226195373584394852072888957304178117  
5313510569711163457668946603482121013634442930239281415342850090  
7026386418520436427134899300324073409253701773263117431279842284  
8480577617459936682837566698589952098721105585848777111378534843  
5966527642400898111594497598591390136982490646196185727187396856  
39915967136410239131574955455289383883587  
public exponent: 65537  
*Subject key identifier* 3e30b33b359757fff140db1b4501382e15a79eb2  
*Authority key identifier* 3e30b33b359757fff140db1b4501382e15a79eb2  
*Key usage* keyCertSign

cRLSign  
*Basic constraints* CA=true; PathLen=unlimited  
*SHA1 Thumbprint* d9a235c88c875b171174d1076b596af9e0a0363d  
*SHA256 Thumbprint* cfa61bf3895cfe4244fbe684aedc88feadd14d6aa3c73f5688f2c1e52c9a604

### ***Extension (critical: true)***

#### ***Qualifications***

Qualifier: NotQualified  
Assert: atLeastOne  
Policy OID: 1.3.21.6.3.10.200.3

*Extension (critical: true)*

**Additional service information**

ForeSignatures

*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:
2713489144953666367009133891636460566719364721268361046536591993499447490302063584331677653228200210928489182501819079634477925849223350099983741305164508178246344443502931
30726196783245033886132455060944963076820096698396937698650371176940421592482842807501189962663935196363326061722619537358439485207288895730417811753135105697111634576689466
03482121013634442930239281415342850090702638641852043642713489930032407340925370177326311743127984228484805776174599366828375666985899520987211055858487771113785348435966527
64240089811159449759859139013698249064619618572718739685639915967136410239131574955455289383883587
public exponent: 65537
Validity: [From: Sat Jun 15 11:51:47 UTC 2002,
To: Wed Jun 15 12:21:47 UTC 2022]
Issuer: O=SWIFT
SerialNumber: [ 3c09327d]

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

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

]

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

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

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

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

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

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

]

]
Algorithm: [SHA1withRSA]
Signature:
0000: BE CD 22 54 79 F9 BF D6 7E E7 EC 99 A5 E3 63 18 .."Ty.....c.
0010: 80 CB 07 4E 87 4E A5 CD AD F3 D7 9E ED CB B3 78 ...N.N.....x
0020: CE FD 20 2C C3 D5 F1 F3 1B 1A 42 CB 8B 62 A7 9B ..,.....B..b..
0030: A3 D1 34 D6 C3 92 5F 03 1C 1D 39 5C FB D0 34 53 ..4.....9\..45
0040: CF 93 5A 36 6D 15 D4 8B 3A 0E CB F6 B2 3F 97 02 ..Z6m.....?..
0050: 1A DA 39 12 49 40 9B CC 5B 51 92 33 38 A5 54 4E ..9.I@[Q.38.TN
0060: C3 06 09 4E 77 70 E0 88 B3 93 32 AC C1 A4 8A F2 ...Nwp....2....
0070: D9 D7 C7 F7 AB 0F 71 B8 D7 AE E5 01 37 D6 E4 4F .....q.....7..0
0080: 42 A2 DE D6 16 DD FF 81 03 17 6C 5C 7E F5 C2 C6 B.....\....
0090: 86 57 8E C7 D7 44 91 BA 09 5D 05 5D 87 1E F3 86 .W...D...].]....
00A0: BB F3 E7 3E 9C 55 53 B9 4A 18 49 01 2B 21 3D 55 ...>.US.J.I.+=U
```

00B0: E3 31 DA B3 B5 62 42 00 2B 1D 55 0A CE 8B 2B 83 .1...bB.+U...+.  
00C0: D9 46 A0 B5 17 BA 4E 66 88 33 07 0D E2 31 CD BA .F...Nf.3...1..  
00D0: 7B AD ED 45 C1 DA C1 A8 FE 86 7E BC 82 40 E4 D4 ...E.....@..  
00E0: 2E AC 78 80 91 FE C3 28 ED 42 F6 47 7C 6B 7C E0 ..X....(.B.G.k..  
00F0: CA 50 B5 C3 7E 4B 39 AF 70 97 86 79 CB 0C 9E 09 ...K9.p.y....

]

*The certificate in PEM format:*

-----BEGIN CERTIFICATE-----  
MIIDkDCCAnigAwIBAgIEPakyFTANBgkqhkiG9w0BAQUFADAQMq4wDAYDVQQKEwVTV0lGVDAeFw0wMjA2MTUxMTUxNDdaFw0yMjA2MTUxMjIxNDdaMBAXDjAMBGNVBAOTBVNXSUZUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIvMie2UrDYQy2yk3+hjuqq5c8br8qtzXHsB7Zt99PenOdTFAsAnFyshdMVIgwmYJb8X3QpFEJnh6is3o+JrHfKdPs07ISroF9c9LAD7TEGQEnfiCMNjnJRH80ce0bLkmbfQv/Gwrsp/SZRzFULJu+PILZaZ3uwVuxQ1ZLkKWLQVGSQJudNhh2qeWU3D3S5sRBNS37d4h5zg3ZV3nmdWuQb0K866KRjiYRRY7rau/amjUYegKJe3bhK18yRlYprz25A53XWL7az0pKv9obTQINRgg/wNwNdwqSF2rZLt/bZg8UnLomKwq7MTQfN/cHniG00bfNtINLMBw1H5aTQwIDAQABo4HxMIHUMBEGCWCsAGG+EIbAQEAWIABzAyBgNVHR8EKzApMcegJaAjpCEwHzEOMAwGA1UEChMFU1dJRlQxDALBgNVBAMTBENSTDEwKwYDVR0QBCQwIoAPMjAwMjA2MTUxMTUxNDdaQ08yMDIyMDYxNTEyMjE0N1owCwYDVR0PBAQDAgEGMB8GA1UdIwQYMBaAFD4wszsl1f/8UDbG0UBOC4Vp56yMB0GA1UdDgQWBQ+MLM7NzdX//FA2xtFATguFaeesjAMBGNVHRMEBTADAQH/MB0GCSqGSIs2fQdBAAQQMA4bCFY1LJA6NC4wAwIEKdANBgkqhkiG9w0BAQUFAAOCQAEAvs0iVhN5v9Z+5+ypeNjGIDLBO6HTqXnrFPXnu3Ls3j0/SAsw9Xx8xsaQsulYqeb09E01s05XwMcHTLc+9A0U8+TmjZtFdSl0g7L9rI/wIa2jkSSUCbzFtrKjM4pVR0wYJTndw4IizkzKswaSK8tnXx/erD3G4167LATfW5E9Cot7Wft3/gQMx6F+9cLGHle0x9dEkboJXQVd hx7zhrvz5z6cVV055hhJASshPVXjMdzqzTWJCAcsdVQr0Iyud2UagtRe6TmaIMwcn4jHnunun7UXB2sGo/aZ+vIA5NQRHIAkf7DK01C9kd8a3zgyLC1w35L0a9wL4Z5ywyecQ==  
-----END CERTIFICATE-----

**QuoVadis Trustlink BVBA**

Service provider VATBE-0537698318  
trade name

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

Service provider Schaliënhoeverdreef 20 boxT  
street address

Service provider 2800  
postal code

Service provider Mechelen  
locality

Service provider state Antwerpen

Service provider BE  
country

**QuoVadis BE PKI Certification Authority**

Type CA/QC

Status granted

Status starting time 2016-07-01T00:00:00.000Z

**Service digital identity (X509)**

Version 3  
Serial number 609679183321230578642917563116990405939188292251

Signature algorithm SHA256withRSA

Issuer CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM

Valid from Tue Jan 28 13:31:54 UTC 2014

Valid to Wed Mar 17 18:33:33 UTC 2021

Subject CN=QuoVadis Belgium Issuing CA G1, O=QuoVadis Trustlink BVBA, C=BE

**Public key** Sun RSA public key, 4096 bits  
modulus:  
9783964049937508596233198438506646025473388060525664736390216073  
2102443656154852856590692595277855257563778420931571542568909508  
0978631883136821438467859677425505518925295946478935536215699720  
9060563934601356099502572088165523220585654567621525989833435792  
4120716735302131104382354616099502334946581973200139342601423705  
2576853073064817439203850489307475026119919108600127180985930937  
5722743791909993240230489806096355723483588160724849940671702693  
9421288570479403288803182697829361690097956484101520823731103609  
3100150818512233246331732587859059076124798706288556894310123901  
0972920078194075368441656229441331564718831935659177163391354589  
2011373776362193636814506011844368620196727006732532805298830422  
9507472040779971787788316999945970815156831404655445754634094522  
5619263559926007219454491737036392400734256628057595967019737484  
9640740113884793702843399591566693810287179450856046582198319405  
9528341619175314034894163206925073632423415715700412910266907296  
1997392759148097836830663187572932975564250918605529635852688494  
1903040727077418799850545935706025465473291910192906070443650070  
8759110395706076167863573384978712251913079970430814716559994884  
9072838313070703058851956878669387044135529569895785662937077766  
97029462522370343  
public exponent: 65537

**Subject key identifier** f80f651c7a6319aabf446fa6491221f37a5de30d

**CRL distribution points** <http://crl.quovadisglobal.com/qvrca.crl>

**Authority key identifier** 8b4b6dedd329b90619ec3939a9f097846acbefdf

**Key usage** keyCertSign  
cRLSign

**Basic constraints** CA=true; PathLen=0

**SHA1 Thumbprint** 89c89b25fa25bafa839fbd9fc1d29caf6481bf28

**SHA256 Thumbprint** 27ebacd86dd3bf86143da4342861031a57cf3fa414d40a86e669c3f4f1d8cf24

**Extension (critical: true)**

**Additional service information**

**ForeSignatures**

**The decoded certificate:**

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

Key: Sun RSA public key, 4096 bits
modulus:
97839640499375085962331984385066460254733880605256647363902160732102443656154852856590692595277855257563778420931571542568909508097863188313682143846785967742550551892529594
64789355362156997209060563934601356099502572088165523220585654567621525989833435792412071673530213110438235461609950233494658197320013934260142370525768530730648174392038504
89307475026119919108600127180985930937572274379190999324023048980609635572348358816072484994067170269394212885704794032888031826978293616900979564841015208237311036093100150
81851223324633173258785905907612479870628855689431012390109729200781940753684416562294413315647188319356591771633913545892011373776362193636814506011844368620196727006732532
80529883042295074720407799717877883169999459708151568314046554457546340945225619263559926007219454491737036392400734256628057595967019737484964074011388479370284339959156669
38102871794508560465821983194059528341619175314034894163206925073632423415715700412910266907296199739275914809783683066318757293297556425091860552963585268849419030407270774
18799850545935706025465473291910192906070443650070875911039570607616786357338497871225191307997043081471655999488490728383130707030588519568786693870441355295698957856629370
7776697029462522370343
public exponent: 65537
Validity: [From: Tue Jan 28 13:31:54 UTC 2014,
To: Wed Mar 17 18:33:33 UTC 2021]
Issuer: CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
SerialNumber: [ 6acaf5c9 85274c50 27ba2928 3006d6e4 c4f15a9b]

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



6aj i2cYeetYh+QkGqCI0iYKLLXUx9ofM24Jq3mWqBP4QDgsWgoQ7L LLA+PwN0v9  
Zov90NaYD6D0IMn/dV1E7EshLK9VZiW9W+DuPSKaCAucSSK7dU21nH5UtB30EGs6  
0yy6hNG3J/VFc0uvu3uDJqI2TT5HD6hbN8JMK+z1s5edHE4=  
-----END CERTIFICATE-----

## QuoVadis BE PKI Certification Authority G2

Type CA/QC  
Status granted  
Status starting time 2016-07-01T00:00:00.000Z

### Service digital identity (X509)

Version 3  
Serial number 370861943658773060475449278572584178262799314517  
Signature algorithm SHA256withRSA  
Issuer CN=QuoVadis Enterprise Trust CA 1 G3, O=QuoVadis Limited, C=BM  
Valid from Mon Jun 13 12:22:05 UTC 2016  
Valid to Sat Jun 13 12:22:05 UTC 2026  
Subject CN=QuoVadis Belgium Issuing CA G2, O=QuoVadis Trustlink BVBA,  
OID.2.5.4.97=NTRBE-0537698318, C=BE  
Public key Sun RSA public key, 4096 bits  
modulus:  
6230883699587823739890387754379070477215155351948503696284928928  
6762659096876001348714059503980469058847658322816356034228132540  
6918046605165432002116706169653521048417532557931231131550972290  
0031197228268363040268982941023187957861042676034834020333070620  
7190772580042983034615584070613386365952220836153439341384692657  
8696826895714227903391959565967406530088771729767950440929656043  
2163014585345898816172521920376840236723120805789115312645387870  
9451857348024900006487730553140606594803912885436651803225622760  
4949718044388445919353619902272978753999638960838408864058539228  
3888884791066054654593043703817378828038101637553182828958483889  
7693248294658177178000733919714925449994792299096725660826469141  
5787505237699654446749444700012886783577363368972858974990045545  
5319090699985484921038680916093288098301753746986699829404622404  
8680718777040625727586310877882003632895696490807225717851431255  
6578194457426406147650960292115572503249495434740454018843282749  
6460397682941622995610157763156443595757370452444868333800151563  
7063821029431865926779220502562502734300590316041110043579026517  
8970118108782414636034722304625519061147374704385231750371749725  
0927026791542693181089165688800622906042384672374815917738285418  
78395623639261113  
public exponent: 65537

Subject key identifier 87c9bc3197127a73bb7ec03d4551b401259551ab

CRL distribution points <http://crl.quovadisglobal.com/qventca1g3.crl>

Authority key identifier 6c26bd605529294e663207a0ff638b835a4b34c6

Key usage keyCertSign  
cRLSign

Basic constraints CA=true; PathLen=0

SHA1 Thumbprint a8884570c16ec0337170e5058f960d74aaf67a78

SHA256 Thumbprint d90b40132306d1094608b1b9a2f6a9e23b45fe121fef514a1c9df70a815ad95c

Extension (critical: true)

## Additional service information

### ForeSignatures

#### The decoded certificate:

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

Key: Sun RSA public key, 4096 bits
modulus:
62308836995878237398903877543790704772151553519485036962849289286762659096876001348714059503980469058847658322816356034228132540691804660516543200211670616965352104841753255
79312311315509722900031197228268363040268982941023187957861042676034834020330706207190772580042983034615584070611338636595222083615343934138469265786968268957142279033919595
65967406530088771729767950440929656043216301458534589881617252192037684023672312080578911531264538787094518573480249000064877305531406065948039128854366518032256227604949718
0443884459193536199022729787539996389608384088640585392283888847910660546545930437038173788280381016375531828289584838897693248294658177178000733919714925449994792299096725
6608264691415787505237699654467494447000128867835773633689728589749900455455319090699985484921038680916093288098361753746986699829404622404868071877704062572758631087788200
36328956964908072257178514312556578194457426406147650960292115572503249495434740454018843282749646039768294162299561015776315644359575737045244486833380015156370638210294318
65926779220502562502734300590316041110043579026517897011810878241463603472230462551906114737470438523175037174972509270267915426931810891656888006229060423846723748159177382
8541878395623639261113
public exponent: 65537
Validity: [From: Mon Jun 13 12:22:05 UTC 2016,
To: Sat Jun 13 12:22:05 UTC 2026]
Issuer: CN=QuoVadis Enterprise Trust CA 1 G3, O=QuoVadis Limited, C=BM
SerialNumber: [ 40f60653 43c04cb6 71e9c825 0e90ebd5 8dd86e55]

Certificate Extensions: 7
[1]: ObjectID: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
accessMethod: 1.3.6.1.5.5.7.48.2
accessLocation: URIName: http://trust.quovadisglobal.com/qvntcalg3.crt,
accessMethod: 1.3.6.1.5.5.7.48.1
accessLocation: URIName: http://ocsp.quovadisglobal.com]
]

[2]: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 6C 26 BD 60 55 29 29 4E 66 32 07 A0 FF 63 8B 83 1&.U)Nf2...c..
0010: 5A 4B 34 C6 ZK4.
]
]

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

[4]: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
DistributionPoint:
[URIName: http://crl.quovadisglobal.com/qvntcalg3.crl]
]]

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

[6]: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSign
CrL_Sign
]

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

Algorithm: [SHA256withRSA]
Signature:
0000: A7 67 CB E3 94 A6 46 5B 5D 0E 02 E9 B3 7E 64 CC .g....F[]....d.
0010: 5C EB A6 75 7C 27 5C 3E 8A 26 E9 9C 77 24 F3 C3 \..u.'\>.&.w$.
0020: E4 4D 3F 9C C6 30 C2 77 02 86 06 DB 5E 1E 28 82 .M?...0.w....^.(.
0030: 38 09 6F 65 27 C5 89 BA 58 5F 5A 9F 16 0C 5F 50 8.oe'...X_Z...P
0040: 13 A7 B1 19 61 C7 EE F7 44 92 68 A4 95 E7 66 80 ....a...D.k...f.
0050: 95 95 83 41 96 96 20 50 45 4B 09 83 52 3B EC C1 ...A.. PEK.:R;..
0060: BE 41 0A B1 3F 0A 80 DF 89 12 3E 17 3E 16 E9 DC .A..?.....>.>...
0070: 99 9A CF 26 0E 0E E6 AD C4 80 FB 79 71 B1 D2 14 ...&.....yq...
0080: 8F 4F C5 DF 17 C2 F4 2F 77 04 7A 9B 18 C3 56 43 .0...../w.z...VC
0090: B6 84 CD FA 32 1C 73 5C 6A 50 AB 10 BA 06 0E E7 ....2.s\jP.....
00A0: 9F 41 AB 7B 26 C0 0E 8E 20 BE 9A E2 18 91 18 1E .A..&.....
```





## **Zetes TSP PKI certification authority**

*Type* CA/QC  
*Status* granted  
*Status starting time* 2016-07-01T00:00:00.000Z

### **Service digital identity (X509)**

*Version* 3  
*Serial number* 4044494821122691399  
*Signature algorithm* SHA256withRSA  
*Issuer* CN=ZETES TSP ROOT CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE  
*Valid from* Fri May 20 17:20:29 UTC 2016  
*Valid to* Wed May 20 17:20:29 UTC 2026  
*Subject* CN=ZETES TSP QUALIFIED CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE  
*Public key* Sun RSA public key, 4096 bits  
modulus:  
7966709637074040714320658184938038917028092405904624202903753477  
4799458811320809970072905178541448482348252543587667311043751542  
0735604726572971351905453910263879782247724079533201420434980906  
1259652247308046066627990399768704035009312298881553170826145735  
9470451717937201719785652613017682391030700889549269989627026410  
5325707292486709403261729124934205264059173193364705541586249507  
6834153593271925365257093421209559284118721797907404731583231496  
2682519430355956122549300816146144079913741952460191615207765565  
9687136786182992996855987043403957104672173646950330802423343213  
5080733069825853601849667775813367604127913317656392038062824337  
3652327925984793105172907246847023677094414821455351393962051121  
8083182177840750610896383923573133536872261434818526596231169060  
6550103273744647470280502580512087702608652531928666461230253981  
6061426252073514311729869399272487087371248545460690134508722398  
5476499537104029642559990594063568574302420354537223370647609793  
5914070469296940194774706386473904559200906938983111873090308121  
8392153063148362630958830429958529036243703457859882500465304738  
4241045855121661319645975335646628176987427562630329145631982930  
3457355499263101837014704295197539666915727491296546803494944852  
83853717680609119  
public exponent: 65537  
*Subject key identifier* e2b4db5f6a0f025054d51defd27672722195462b  
*CRL distribution points* <http://crl.tsp.zetes.com/ZETESTSPROOTCA001.crl>  
*Authority key identifier* 38bc5c3054dce2bb20efee6f41a0316e5cfd8b75  
*Key usage* keyCertSign  
cRLSign  
*Basic constraints* CA=true; PathLen=0  
*SHA1 Thumbprint* 1698dc47f4f5ff956c560324e1965aa7ed38e29d  
*SHA256 Thumbprint* d628417a992140d3bd98b310d6de33d04a91c49221841dbf0f52c81fd2fafab5

### **Extension (critical: true)**

#### **Additional service information**

ForeSignatures

The decoded certificate:

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

Key: Sun RSA public key, 4096 bits
modulus:
79667096370740407143206581849380389170280924059046242029037534774799458811320809970072905178541448482348252543587667311043751542073560472657297135190545391026387978224772407
95332014204349809061259652247308046066627990399768704035009312298881553170826145735947045171793720171978565261301768239103070088954926998962702641053257072924867094032617291
24934205264059173193364705541586249507683415359327192536525709342120955928411872179790740473158323149626825194303559561225493008161461440799137419524601916152077655659687136
78618299299685598704340395710467217364695033080242334321350807330698258536018496677758133676041279133176563920380628243373652327925984793105172907246847023677094414821455351
39396205112180831821778407506108963839235731335368722614348185265962311690606550103273744647470280502580512087702608652531928666461230253981606142625207351431172986939927248
70873712485454606901345087223985476499537104029642559990594063568574302420354537223370647609793591407046929694019477470638647390455920090693898311187309030812183921530631483
62630958830429958529036243703457859882500465304738424104585512166131964597533564662817698742756263832914563198293034573554992631018370147042951975396669157274912965468034949
4485283853717680609119
public exponent: 65537
Validity: [From: Fri May 20 17:20:29 UTC 2016,
To: Wed May 20 17:20:29 UTC 2026]
Issuer: CN=ZETES TSP ROOT CA 001, SERIALNUMBER=001, O=ZETES SA (VATBE-0408425626), C=BE
SerialNumber: [ 3820ee9c 74ecd147]

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

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

]

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

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

[5]: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.1
qualifier: 0000: 16 20 68 74 74 70 73 3A 2F 2F 72 65 70 6F 73 69 . https://reposit
0010: 74 6F 72 79 2E 74 73 70 2E 7A 65 74 65 73 2E 63 tory.tsp.zetes.c
0020: 6F 6D om
], PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.2
qualifier: 0000: 30 2E 0C 2C 5A 45 54 45 53 20 54 53 50 20 43 50 0...ZETES TSP CP
0010: 53 20 66 6F 72 20 4E 43 50 2B 20 61 6E 64 20 51 S for NCP+ and Q
0020: 43 50 2B 20 63 65 72 74 69 66 69 63 61 74 65 73 CP+ certificates
]] ]
]

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

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

]

Algorithm: [SHA256withRSA]
Signature:
0000: A8 7C 4D 53 16 D5 F8 35 E4 4F F2 02 A7 B6 1C BC ..MS...5.0.....
0010: DF 47 85 B2 54 AC 53 8B 9A D1 2D 35 F3 70 56 75 ..G..T.S....-pVu
0020: 2F 8B CE EB 40 9B 34 00 EF ED A9 62 95 90 9A C5 /...@.4...b....
0030: 90 A3 1A 5C 04 7A 3C 53 6C 9E 87 E4 70 2B 36 64 ...\.z<Sl...+p6d
```



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:
243009966895227133693003009371465176655969091190326193281992404510245187371320819543733804448624693522397655805338290368738930744837629562942067296575129066040125015273157
93517280217865321819160740775732194727930458919922521995692540951807923171115060769731590712346286509664439160107000534884146909041751636242027382031023466107500619524409877
27283427021323280307639992049788147229043339760080834570290066311843665221921835557433177168179986865374356704032605187207885089432302544936253416592529324143468606089203473
2092130460766588017750127431309112075130836326103436887414640755084886631307165625943996664160511
public exponent: 65537
Validity: [From: Wed Feb 19 13:37:52 UTC 2014,
To: Tue Feb 11 13:37:52 UTC 2025]
Issuer: C=BE, O="FPS Economy, SMEs, Self-employed and Energy - Quality and Safety", CN=Belgian Trusted List Scheme Operator
SerialNumber: [ aed1a601 8711328f]

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

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

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

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

Algorithm: [SHA1withRSA]
Signature:
0000: 16 9B 23 CA D4 FE 95 B8 BA 24 C7 93 8E D7 F3 7F ..#.....$......
0010: 2A 9E DC 7A 14 9E 62 0C 2B 3E 89 A1 03 D7 8D BE *....z.b.+>.....
0020: CA 3B BF C1 05 54 E0 9F 2B 8D 2E 14 AA C7 4E F3 ;...T.+.....N.
0030: 03 8C E2 C7 F2 2E 33 0B 45 1B 0A EB 4B 1A 67 9A .....3.E...K.g.
0040: 36 BB EB 4B 22 3D 10 AC 54 72 B5 30 F5 58 8B 8F 6..K"=...Tr.O.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 9C 67 D0 4C BE 2D D8 BF 5F 23 43 12 .....g.L..._#C.
0070: 52 8E F1 A9 5D A5 A9 50 D2 CD 9E 11 00 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.;`
00B0: 42 90 7C F3 EC D9 0E D0 29 DC 55 49 C5 1F 67 79 B.....)U.I..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 F0 9B 89 .m.w.i....<.....
]
]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID3zCCAsEgAwIBAgIJAK7RpgGHETKPMa0GCSqGSIb3DQEBBQUAMIGHM50wKwYD
VQ0QEYRCZmXnaWFrYFRyXN0ZWQGLzIzdCByT2h1bWUgT3B1cmF0b3IuSTBHBGNV
BAoTQEZQUyBFY29ub215LDBTUVzLDBTZWxMLVWtcGxveWVKGIFuZCBFbmlVYzNk
LSBRdWZsaXR5IGFuZCBTYWZldHkxZzJlbnVBAWYTAkFMB4XDT0MDIx0TEzMzc1
Ml0xMDI1MDI1MTEzMzc1Ml0wYXc1LTAuBgNVBAMTJEU1bGdpYW4gVHJlc3RlZCBM
aXN0IFNjaGVtZS5BPCGVyYXRvcjFJMEcGA1UEChNARlBTEVj25vbXksIFNRRXMs
IFNlbnV0eTEuZmV5bG95ZWQgYW5kIEVudXJneSAuIHR5YXp0dHkgYW5kIFNlbnV0eTEu
MAKGA1UEBHMCKQUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQA0AgEFk
oDPTYDvGk+/IPnGSPm58NRE7mpzLHk8LxpYnTAtbMhn7FWru9GLNi+bLYNOEmzN
2E5K09+7AAAMmx2x8zmEMvc3oUQ7E0WNS5G1+Y+7n6NtX50D/4Sbw4IjVvwRRru8
Coj5vqH5z3JKTgft8teEpbw5vSFZhg6+091rdX342RJU4AtG78sxZvzIqpa3WsdmH
f5XDyjnGK3dRgkDu0aBxwEexuU1N4Lv0+MacwoaxEqLhE26TALGWS2WmNEW30LUd
f7nc0Tz/\lNyQsuFn01c4pg56hjyxLtpjyHwNwbTDx+cjBpBve0T9Nb6UfKfHknC5
Afr10WnFLXUmykD/AqMBAAGjTDBKMAKGA1UdEQCMAAwCwDVDR0PBAQDQAgAMB0G
A1UdDgQWBRFR745pXfv011rxBwg0UhLQqteOUTARBgNVHSUECjAIBgYEAJEA3AwAw
DQYJKoZIhvcNAQEFBQADggEBABabI8ru/pW4uiThk47X838qntx6FJ5iDCs+iaED
142+yju/w0VU4J8rjS4UqsD08w0M4sfyLjMLRRsK60saZ5o2u+tLIj0QrFRyTD1
WUwPZxpBj0U8Zj/+aLkr4bQmyqgJ4XzJZ9BMvi3Yv18j0xJSjvGpXaWpUNLNhEN
TuzKv8f/0vBn2Inmpg7cwgj2q8qhz/3r1ZmHETSdMEdjV4ovYruAKX58jwnRdga
cTtg0pB88+zZdtAp3FvXr9nefCdvjV2nuN++UgA2v8d2u9c8c70bGd7dL609rQC
```

fvBw6/h9nkXSJSAjKXS1uvnABtq3fQabHwxNc8rIQPkLk=  
-----END CERTIFICATE-----

*The public key in PEM format:*

-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwIBBZKAz02A7xpPvyD5x  
kj5ufDUR05qcy5PJcaWJ0wLWzIZ+xVq7vRpTYvm5WGDThJszdh0SjvfuwAADJsd  
sfM5hDMHN6FE0xNFjeRpfmPu5+jbV+dA/+Em80CI1b8MEUa7vAqI+b6uR89ySk4H  
7FLXhKcG+b0hWYevqPYq3V9+nkSVOALRu/LMwb8yKqWt1rHXTH+Vw8o5xit3UYJA  
7jmgcVhHsb1IjeC7zvjGnMKGsRK14RGeKwCxLktLpjRFtzpVHX+53NE8/5Z8kLLh  
Z9NXOKY0eoY8sS7aY8h8DcG0w8fnIwaQb3jk/Tw+LHyhR5JwuQH6yDlpxS11Jsig  
/wIDAQAB  
-----END PUBLIC KEY-----