

# 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 Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.

## *Legal Notice*

The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for Belgium is the 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* appropriate

*Scheme type community rules* <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common>  
<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/BE>

*Issue date* 2012-05-01T00:00:00.000Z

*Next update* 2012-09-15T00:00:00.000Z

*Historical information period* 10959 days

*Sequence number* 8

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

## ***Scheme Operator***

*Scheme operator name* FPS Economy, SMEs, Self-employed and Energy - Quality and Security - Information Management

*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 NV/SA***

*Service provider trade name* Certipost NV/SA  
*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

*Extension (critical: true)*

**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

**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
4445138975351025575749503679547226381031300213808727950333349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
774175448506963241118776049541934983183035608916277217984309481720716444141969017225065301229219951
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:[
```

---

## Belgique/België (Belgium): Trusted List

---

```
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 49 .....j.k*.YH.LI
0020: 37 D7 73 A1 6A 01 65 5E 32 BD E7 97 D3 D0 2E 3C 7.s.j.e^2.....<
0030: 73 D3 8C 7B 83 EF D6 42 C1 3F A8 A9 5D 0F 37 BA s.....B.?..].7.
0040: 76 D2 40 BD CC 2D 3F D3 44 41 49 9C FD 5B 29 F4 v.@...?.DAI...].
0050: 02 23 22 5B 71 1B BF 58 D9 28 4E 2D 45 F4 DA E7 .#[q..X.(N-E...
0060: B5 63 45 44 11 0D 2A 7F 33 7F 36 49 B4 CE 6E A9 .cED..*.3.6I..n.
0070: 02 31 AE 5C FD C8 89 BF 42 7B D7 F1 60 F2 D7 87 .1.\.....B...].
0080: F6 57 2E 7A 7E 6A 13 80 1D DC E3 D0 63 1E 3D 71 .W.z.j.....c.=q
0090: 31 B1 60 D4 9E 08 CA AB F0 94 C7 48 75 54 81 F3 1.^.....HuT..
00A0: 1B AD 77 9C E8 B2 8F DB 83 AC 8F 34 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+eWmUDANBgkqhkiG9w0BAQUFADAn
M0swCQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ21lbSBzSb290IENBMB4XDzA0MDEy
NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowZELMAKGA1UEBHMCAxGDAWBgNVBAMT
D0JlbGdwdW0gUm9vdCBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMihceKCRKJ5eHFvna6ppKsot03HIOswkVp19eLSz8hMFJhCWK3HECVAQGa+X0S
J4fpn0VxTiIj0RiYqjBeoiG52bv/9nTrMQHn035YD5EWtXaJqAFPrSjmcPpLHZXB
MFjqvNlL2Jq0i0tJRLf0LMVdssUXRLJsw9q09P9vMI7EU/CT9YvzvU7wCMgTVy
v/cY6pZifSsofxVs9LkYn0FrMhtB20yvmi4BUCuVjHWPmbxM0jvxKuTXgfeMo8S
dKpbNCNUw0pszv42kqgJF+qhLc9s44Qd3ocuMws80IhUDiVLlg5cYx+dtA+mqh
pIqTm6chBocdJ9PEoc1MsG8CAwEAa0BuzCBuDA0BgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAE0zA5MDCGBWA4AQEBMCA4wLAYIKwYBBQUHAgEW
IGH0dHA6Ly9yZXBvc2l0b3J35LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBQ08Axw
m2HqVzq2Nzdtn925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth61c6tjWxbZ/duRS02+YwDQYJKoZIhvcNAQEFBQADggEBAMhtILGKYfgP
lm7VILKb+Mbc0xYA2s1q52sq+llIp0xJN9dz0w0BzV4yveeX09AuPHPTjHuD79ZC
wt+oqV0PN7p20kC9zC0/00RBSZz9Wyn0A1M1w3Ebv1jZKE4trfTa57vjRU0RD5p/
M3825bT0bqkCMA5c/ciJv0J71/Fg8teH9Lcuen5qE4Ad30PQYx49cTGxYNSeCMqr
8JTHSHVUgfmBrXec6LKP240sjzRr6L/D2FVDw2RV6xq9NoY2uiGMLxoh10ot06y6
7Kcdq765Sps1LxxCHVGnHITtEpF/8m6HFubJdNbv6z1951luBpQE5KJVhzgoaiJe
4r50ErAE0yo=
-----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

Extension (critical: true)

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

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:
25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533471883040702374115053713546900035236027965047
48268436965740013155524363953296559605768293726462748683867807979476223046936921095008879757875772834133929233365465451098179764303067017935791515652621584351236063583342307
10497624432217765218126527057253528859368866836149038404306362405288701438246375881056800407958814486546438584605327134008224091466795027147972455421015549428678366393080491
58535662204430622722091644041294798682626345622247703196611536459503012648921426461410998536799349
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
]

[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.....

---

## Belgique/België (Belgium): Trusted List

---

```
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 Q...Wo...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
BhMCQKXjGTAxBgNVBAMTEEJlbgdpdW0gUm9vdCBDQTIwHhcNMDCxMDA0MTAwMDAw
WhcNMjE1MDgwMDAwMjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQMVsZ211
bSB5b290IENBMjCCASIAwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZz0h6S
/3UPi790hqC/7bIYLS2X+an7mEoj39WN4IzGMhwLQdC1i22bi+n9fzGHYjd1d61
IgdMqFNAn68KNaJ6x+HK92AQZw6nUHMxU5wfIp8MXW+2QbyM69odRr2nLL/zGsvU
+400HjPlltfsjFPekx40HopQcSZYtF3CiInaYnkJIT/eIwEYnm7hLHADBGXvmAYr
XR5i3Fvr/mZkIV/4L+HXmymvb82fqqxG0YjFnaKvN6w/Fa7yYd/vw2uaItgscf1Y
HewApDggLVrH1Tdjuk+bqv5WR15j2Qsj1Yr6tSPwiRuhFA0m2kHw0I8w7QUmecFL
TqG4f1V50mlGhHUCaWEAAa0BuzCBuDAOBgNVHQ8BA8FEBAMCAQYwDwYDR0TAQH/
BAUwAwEB/zBCBgNVHSAE0zA5MDcGBW44CQEBMCAwLAYIKwYBBQUHAgEWIgH0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBSFiuuv0xbu+DlkD
lN7WgAEV4xCcOTARBg1ghkgBhvCAQEEBAMCAAcwHwYDR0jBBgwFoAUHyr9Mm7
vgZ5A5Te1oABFeMQndkwdQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyCc
Uwnz5gEmdL8rs5qauhjyC4isHLmZr87LEwEnkoRYmhC598wUkmt0F0qW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTLBFk0pvDVTc9rejjg7NqZV3JcqUwumyaa7YwB0+mPyW
nIR/VRPmPIfjvCCKpDZoa01gZhz5v6yALGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9fVJ3btC0R5/0UAoNmXsimABKx770FP67H6dh96tK8QYUn8pJ0sKpv02F
sauB0eYXUjpu4c5nUwFAA4+Bw11V0S0U7Q2dmS23G7rPUZuFF1eR10NeE3gJ7u0
hXY=
-----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

## Extension (critical: true)

### 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

### 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 [
```





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/Omniroot2034.crl  
Authority key identifier 4c3811b898005b5a2b703eea78e4d5676767a77e  
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 [
```

## Belgique/België (Belgium): Trusted List

```
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 D7 F4 lUI.u.T.....]..
0020: 10 35 18 31 AC 35 F8 8D 4B 0F 6D 66 48 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#.#..MY.U.ZZ
00D0: 62 6C 93 73 21 5A F6 52 84 8A AF 97 01 96 7E B4 bl.s!Z.R.....
00E0: 79 80 91 A5 E2 2B 7B 19 27 B7 9A 29 AF A3 27 72 y....+...'..)'r
00F0: 28 A9 09 73 9B 93 A7 3F E0 48 8F 9E B5 98 8A F8 (.s...?.H.....
]

]
```

### The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIELTCCAwgAwIBAgICA4gwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAoMEFZlcm16b24gQnVnVzAw5Lc3MxETAPBgNVBAsMCE9tbnRlSb290MR8w
HQYDVQODDBZWZKJpem9uIEdsb2JhbCB5b290IENBMB4XDTEyMDEyMDE1MDUwNl0x
DTIyMDEyMDE1MDUwNl0xELMAkGA1UEBhMCVVMxGTAXBgNVBAoMEFZlcm16b24gQnVn
dCBuLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYy
YwpxZml1LmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNl
AQEAow3rmuZKZMnGhQRGeEzZK4Theq59CiqK6BseSxLmZ3sh8znY0FBNK40XmFEj
0Y990nIYAjXnU5bcvS5BFQKpwtD5cFcmP7BR0i6/MyJCE6BMD8wc561CJfLlm
8/p/vRF9KSDfa6fMd/WJghbq780wa22+UgXpFr27eqBCsUzEiZya5cILWXM0hmp+
ZE30i7pLZ/Dh+50tn/R+P0IVBBIypicnx/u4Q/1oEqMyy+DF1iuMfCbCpE2Pbwz
0R+SCqLFNeR09dLfmJ5Xlp5r5K7dKXJP8DgoMw8Cu5fGLU8z2qwx+3zV0XdxDNF
e2g8HHX4WdMymhSzbmnljGVYrQIDAQABo4HyIHvMBIGAIUdEwEB/w0IMAYBAf8C
AQAwRQYDVDR0gBD4wPDA6BgRVHSAAMDImMAYIKwYBBQUHAgEwJGh0dHBz0i8vd3d3
LmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNl
BBGwFoAUTDgRuJgAWlorcd6qe0TVZ2dnp34w0gYDVR0fBDsw0TA3oDwgM4YxaHR0
cDovL2NkcDEucHViG1jLXRydXN0LmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNlLnYyLmNl
BgNVH04EFgQUUDjczxyhuv85f51rmmJCLrMhMKEQwDQYJKoZIhvcNAQELBQADggEB
AHPwVwH8zTeSFMePqgIMwdsVUnSdYVUkVAGRyGxdF0EDUYmaw1+I1LD21mSxVM
KJESedvEs0JlqER6GohCM9jigquuNQhg04S6sWyyWxw1atIMfp2D7F5iNrTcry3y
h2v5fxZ3CyV7oZSS5+pevFhvfqdZULgZ64/RhPcqlZV74asJunBRZ756IF3PxA
KDN9Ytp8vJw1cs1RoS/0CJ/6aJ58HjBc863Rj395ScL/zW+KanvLvvdafCCJ/FN
uaA80VYjHhHsnk1ZjFWBwlpjBzIvR2UoSkR5c8ln60eYCRpeIrexknt5opr6Mn
ciipCX0bk6c/4EiPnrWYivg=
-----END CERTIFICATE-----
```

**Trusted List Signer**

Subject OU=Ministry of Economic Affairs, O=Belgian Federal Government, C=BE, CN=Belgian Trust List Scheme Operator
Issuer OU=Ministry of Economic Affairs, O=Belgian Federal Government, C=BE, CN=Belgian Trust List Scheme Operator
Not before Fri Feb 26 11:42:04 CET 2010
Not after Mon Feb 24 11:42:04 CET 2020
Serial number 15681248625855287085
Version 3
Public key SHA1 0e2b1b3ce368b11ae8b9221982ce69740e3dceb9
Thumbprint
Public key SHA256 2efdccb9b768ea9654152816c48a53857f658c50462c12f66f5d56c0961616d
Thumbprint

The decoded certificate:

[
[
Version: V3
Subject: OU=Ministry of Economic Affairs, O=Belgian Federal Government, C=BE, CN=Belgian Trust List Scheme Operator
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5
Key: Sun RSA public key, 2048 bits
modulus:
2400675172998773746328503045299390237462905052654201613003175032293743139213202784813213482709335152611031406391633037540032036565000829743608508868431427838960727335586132
72260024738022754521550978668073613848886314527876619695170205142182992106517625874476574000109694632025016183163606961399776610711940089307587500742164497411652253547139771
69334557334399558495891953127385660029376236782791146443818739080758252054642538448809693082368758428714040768299077110739227256650318169746736582053355188697019790131215442
97724080223514852080052393728286375475080791685309752463786509412302789223792002372173162207444189
public exponent: 65537
Validity: [From: Fri Feb 26 11:42:04 CET 2010,
To: Mon Feb 24 11:42:04 CET 2020]
Issuer: OU=Ministry of Economic Affairs, O=Belgian Federal Government, C=BE, CN=Belgian Trust List Scheme Operator
SerialNumber: [ d99efc8a daafc2d]

Certificate Extensions: 4

[1]: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 95 B3 07 E5 F3 52 B0 CB 0F E9 6B 00 1F D0 B4 65 .....R....k....e
0010: 75 CC 6E 6C u.nl
]

[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
]

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

Algorithm: [SHA1withRSA]
Signature:
0000: A6 25 D0 FC 3F B8 08 E8 D5 9F E5 E2 BF DD FA E7 .%.?......
0010: A9 C1 F0 5F 2E 7B FC 54 B8 1A 69 D0 2B 4F 2B BE ...\_.T..i.+0+
0020: 52 F0 D2 53 FF 11 C5 BD 1E 6B B5 A7 CD 58 B2 1B R..S.....k...X..
0030: 1C 49 23 70 0C ED ED 1C 33 32 5F 2E 01 6D 43 CC .I#p....32...mC.
0040: D1 BF F2 A0 8C BC 6D 1A 59 77 11 4F 2B 01 22 9C .....m.Yw.O+."
0050: 48 57 D5 E2 74 07 1F 51 9A C7 26 6C 1C 40 FC 41 HW..t..Q..&l.@.A
0060: 57 1E 9E F8 E4 41 03 7F DF 7E E1 58 BB 68 6D 00 W...A....X.hm.
0070: 1B E4 B0 D7 03 9C 6B DC 17 EA 1E 49 93 16 23 B5 .....k...I.#.
0080: 82 0F 66 D2 F6 D6 BF 8D 1A 28 3B 4A 5A DB DF 9C .f.....(;JZ...
0090: 86 61 95 86 25 97 BD 40 09 70 9F B6 D7 C5 30 4D .a.%..@p....0M
00A0: 24 CE F8 E4 12 30 EE 6C 1D 5D 47 DA 91 81 63 99 \$....0.l.]G...c.
00B0: 88 4F B7 8B 8D CF 9D 69 7D 74 B4 56 37 5B 58 DF .0.....i.t.V7[X.
00C0: CC 26 B5 11 CC 1A 20 A0 AF 19 00 D7 04 33 0F 8C .&....3...
00D0: 96 FC 16 6C BC B2 BC 64 EB 95 53 C4 07 13 FE 01 ...l...d..S....
00E0: E7 AF 6E BA 99 50 5B 0C 75 D5 DB FC 69 22 9F 61 ...n.P[u...i" a
00F0: 92 43 1B 65 1D 49 51 D5 51 1B 2C E1 36 BC D5 42 .C.e.IQ.Q.,.6..B

The certificate in PEM format:

---

## Belgique/België (Belgium): Trusted List

---

```
-----BEGIN CERTIFICATE-----
MIID3TCCAsWgAwIBAgIJANme/Irar88tMA0GCSqGSIb3DQEBBQUAMIGMSswKQYD
VQ0DEyJCZWNnaWUFRydXN0IEp3c3QgU2NoZW11IE9wZXJhdG9yMQswCQYDVQ0G
EwJCRTEjMCEGA1UEChMaQmVsZ2Lhb1BGZWRlcmFzIEVudmVybmlLbnQxJTAjBgNV
BAsTHE1pbmLzdHJ5IG9mIEVjb25vbWljIEFmZmFpcnMwHhcNMTAwMjI2MjA0MjA0
WhcNMjAwMjI0MjA0MjA0WjCBhjErcmVhZG9wZXJhdG9wZXJhdG9wZXJhdG9wZXJhdG9w
IFNjaGVtZSBPcGVyYXRvcjELMakGA1UEBHMCKUxIzAhBgNVBAoTGk1LbGdpYW4g
RmVzZXJhbCBhb3Zlcm5tZW50MSUwIiwvDQ0LExxNaw5pc3RyeSBvZiBFY29ub21p
YyBBZmZhaXJzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviMAu242B
g3jI1V+lKm1FNaAgBzjDDXtP9+ZqI+0f0jzBacWXR67a5hUuPggpEgPt8yGe83
d0kjmS8hpUwZbs7WcbDgOC6ewI7+LSEx4wq2sEU/9mXMBdTqyhmXu5p0eM8fGV
ubzQWMLj2ZsmRbeGEfZxpb37tT3X5ok289YbUp5ngyMrYzjLh75nCHT495JgaIVq
V+y03zwJvTDHBLZdvMucvPJX68Lu7PbFdw0pCrF/b04AzLAMARVsw0LmVHUlF
Fxh0enzVTEkduqtBzTicZNomw5qIdK0Lb6gWEcRbvBJzgcNauLn30GgXuA1WMDVd
3S0fAWQKvRb83QIDAQABo0wSjAJBgNVHRMEAjAAMAASGA1UdDwQEAwIHGDAdbGNV
HQ4EFgQUl6MH5fNSsMsP6wsAH9C0ZXXMbmwEQYDVR0LBAowCAYGBACRNwMAMA0G
CSqGSIb3DQEBBQUAA4IBAQCmJdD8P7gI6Nwf5eK/3frnqcHwXy57/FS4GmnQK08r
vLLw0LP/Ecw9Hmu1p81YshscSSNwD03tHDMYxy48bUPM0b/yoIy8BRpZdxFPKwEi
nEhX1eJ0Bx9RmscmbBxA/EFXHp745EEDf99+4Vi7aG0AG+Sv1w0ca9wX6h5JkxYj
tYIPZtL21r+NG1g75Lrb35yGYZW6JZe9QA1wn7bXxTBNJH745B1w7mwdXUfakYfj
mYhPt4uNz51pfxS0VjdbwN/MJrURzBogoK8ZANcEMw+MLvWbLyyvGT rLVPEBxP+
AeevbrqZUfsMddXb/GkiN2GSQxtLHU1R1VEbLOE2vNVC
-----END CERTIFICATE-----
```

### *The public key in PEM format:*

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviMAu242B3jI1V+lKm
1FNaAgBzjDDXtP9+ZqI+0f0jzBacWXR67a5hUuPggpEgPt8yGe83d0kjmS8hpUw
Zbs7WcbDgOC6ewI7+LSEx4wq2sEU/9mXMBdTqyhmXu5p0eM8fGVubzQWMLj2Zsm
RbeGEfZxpb37tT3X5ok289YbUp5ngyMrYzjLh75nCHT495JgaIVqV+y03zwJvTDH
eBLZdvMucvPJX68Lu7PbFdw0pCrF/b04AzLAMARVsw0LmVHUlFfxh0enzVTEkdu
qtBzTicZNomw5qIdK0Lb6gWEcRbvBJzgcNauLn30GgXuA1WMDVd3S0fAWQKvRb8
3QIDAQABo
-----END PUBLIC KEY-----
```