Belgique/België (Belgium): Trusted List

Scheme name

BE:Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures 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	2010-05-01T00:00:00.000Z
Next update	2010-09-15T00:00:00.000Z
Historical information period	10959 days
Sequence number	2
Scheme information URIs	http://tsl.belgium.be/
	http://tsl.belgium.be/nl/
	http://tsl.belgium.be/fr/

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/EN/Index.htm
	http://www.certipost.be/dpsolutions/en/e-certificates-legal-info.html
Service provider street address	Centre Monnaie
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	117029288889378643505965201768446445968
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:
	25327272471742424753108761113025515413507712904874083939907073553139389403581555633427000903307438065008396155423372038139338001129228397387437566169146147569101132153735147576372578550015244598849082833749686618262398710652224019389731334957158067691632442561241462450868417538609485432931629806056877222374520561111218990450541853348409938502314444513897535102557574950367954722638103130021380872795033334967224942002004934838812373471384411526579026650775354589375802255665011941485467556333747329602589496041615986077417544850696324111877604954193498318303560891627721798430948172071644141969017225065301229219951
	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
57637257855001524459884908283374968661826239871065222401938973133495715806769163244256124146245086841753860948543293162980606568772223745205611121899045054185334840993850231
44445138975351025575749503679547226381031300213808727950333349672249420020049348388123734713844115265790266507753545893758022556650119414854675563337473296025894960416159860
7741754485069632411187760495419349831830356089162772179843094817207164414196901722506530122921921951
 public exponent: 65537
 Validity: [From: Mon Jan 27 00:00:00 CET 2003,
            To: Mon Jan 27 00:00:00 CET 2014]
 Issuer: CN=Belgium Root CA, C=BE
 SerialNumber: [    580b056c 5324dbb2 5057185f f9e5a650]

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

[2]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 10 F0 0C 56 9B 61 EA 57   3A B6 35 97 6D 9F DD B9  ...V.a.W:.5.m...
0010: 14 8E DB E6                                        ....
]
]

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

]

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

]]  ]
]

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

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

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: C8 6D 22 51 8A 61 F8 0F   96 6E D5 20 B2 81 F8 C6   .m"Q.a...n. ....
0010: DC A3 16 00 DA CD 6A E7   6B 2A FA 59 48 A7 4C 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 6B E8 BF C3   ..w........4k...
00B0: D9 F5 43 C3 64 55 EB 1A   BD 36 86 36 BA 21 8C 97   ..C.dU...6.6.!..
00C0: 1A 21 D4 EA 2D 3B AC BA   EC A7 1D AB BE B9 4A 9B   .!..-;.......J.
00D0: 35 2F 1C 5C 1D 51 A7 1F   54 ED 12 97 FF F2 6E 87   5/.\.Q..T.....n.
00E0: 7D 46 C9 74 D6 EF EB 3D   7D E6 59 6E 06 94 04 E4   .F.t...=..Yn....
00F0: A2 55 87 38 28 6A 22 5E   E2 BE 74 12 B0 04 43 2A   .U.8(j"^..t...C*

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDlDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBgkqhkiG9w0BAQUFADAn
MQswCQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ2l1bSBSb290IENBMB4XDTAzMDEy
NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowJzELMAkGA1UEBhMCQkUxUxGDAWBgNVBAMT
D0JlbGdpdW0gUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMihcekcRkJ5eHFvna6pqKsot03HIOswkVp19eLSz8hMFJhCWK3HEcVAQGpa+XQS
J4fpnOVxTiIs0RIYqjBeoiG52bv/9nTrMQHnO35YD5EWTXaJqAFPrSJmcPpLHZXB
MFjqvNll2Jq0iOtJRlLf0lMVdssUXRlJsW9q09P9vMIt7EU/CT9YvvzU7wCMgTVy
v/cY6pZifSsofxVsY9LKyn0FrMhtB20yvmi4BUCuVJhWPmbxMOjvxKuTXgfeMo8S
dKpbNCNUwOpszv42kqgJF+qhLc9s44Qd3ocuMws8dOIhUDiVLlzg5cYx+dtA+mqh
pIqTm6chBocdJ9PEoclMsG8CAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4AQEBMC4wLAYIKwYBBQUHAgEW
IGh0dHA6Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBQQ8AxW
m2HqVzq2NZdtn925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth6lc6tjWXbZ/duRSO2+YwDQYJKoZIhvcNAQEFBQADggEBAMhtIlGKYfgP
lm7VILKB+MbcoxYA2s1q52sq+llIp0xJN9dzoWoBZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0AiMiW3Ebv1jZKE4tRfTa57VjRUQRDSp/
M382SbTObqkCMa5c/ciJv0J71/Fg8teH9lcuen5qE4Ad3OPQYx49cTGxYNSeCMqr
8JTHSHVUgfMbrXec6LKP24OsjzRr6L/D2fVDw2RV6xq9NoY2uiGMlxoh1OotO6y6
7Kcdq765Sps1LxxcHVGnH1TtEpf/8m6HfUbJdNbv6z195lluBpQE5KJVhzgoaiJe
4r50ErAEQyo=
-----END CERTIFICATE-----
```

CN=Belgium Root CA2, C=BE

Type   CA/QC
Status   undersupervision
Status starting time   2007-10-04T10:00:00.000Z

Service digital identity (X509)

Version   3
Serial number   3098404661496965511
Signature algorithm SHA1withRSA
Issuer   CN=Belgium Root CA2, C=BE
Valid from   Thu Oct 04 12:00:00 CEST 2007
Valid to   Wed Dec 15 09:00:00 CET 2021
Subject   CN=Belgium Root CA2, C=BE

Public key	Sun RSA public key, 2048 bits

  modulus:
25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533471883040702374115053713546900035236027965047482684369657400131555243639532965596057682937264627486838678079794762230469369210950088797578757728341339292333654654510981797643030670179357915156526215843512360635833423071049762443221776521812652705725352885939368866836149038404306362405288701438246375881056800407958814486546438584605327134008224091466795027147972455421015549428678366393080491585356622044306227220916440412947986826263456222477031966115364595030126489214264614109985367993493

  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:
25052020358972869298024429313659777821361101578567425642348395816436795380283967224876983130034020316820575216355360416605004533471883040702374115053713546900035236027965047482684369657400131555243639532965596057682937264627486838678079794762230469369210950088797578757728341339292333654654510981797643030670179357915156526215843512360635833423071049762443221776521812652705725352885939368866836149038404306362405288701438246375881056800407958814486546438584605327134008224091466795027147972455421015549428678366393080491585356622044306227220916440412947986826263456222477031966115364595030126489214264614109985367993493
 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.......
```

```
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..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-----
MIIDjjCCAnagAwIBAgIIKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTIwHhcNMDcxMDA0MTAwMDAw
WhcNMjExMjE1MDgwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi79Qhqc/7bIYLS2X+an7mEoj39WN4IzGMhwWLQdC1i22bi+n9fzGhYJdld61
IgDMqFNAn68KNaJ6x+HK92AQZw6nUHMXU5WfIp8MXW+2QbyM69odRr2nlL/zGsvU
+40OHjPIltfsjFPekx40HopQcSZYtF3CiInaYNKJIT/e1wEYNm7hLHADBGXvmAYr
XR5i3FVr/mZkIV/4L+HXmymvb82fqgxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y
HewApDgglVrH1Tdjuk+bqv5WRi5j2Qsj1Yr6tSPwiRuhFA0m2kHwOI8w7QUmecFL
TqG4flVSOmlGhHUCAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4CQEBMC4wLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBSFiuv0xbu+DlkD
lN7WgAEV4xCcOTARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAUhYrr9MW7
vg5ZA5Te1oABFeMQnDkwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGy1oyCc
UwnzSgEMdL8rs5qauhjyC4isHLMzr87lEwEnkoRYmhC598wUkmt0FoqW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTlBFk0pvDVTC9rejg7NqZV3JcqUWumyaa7YwBO+mPyW
nIR/VRPmPIfjvCCkpDZoa01gZhz5v6yAlGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9fVJ3bTc0R5/0UAoNmXsimABKgX77OFP67H6dh96tK8QYUn8pJQsKpvO2F
sauBQeYNxUJpU4c5nUwfAA4+Bw11V0SoU7Q2dmSZ3G7rPUZuFF1eR1ONeE3gJ7uO
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:
21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524101389078999960573270377990828558687635112394538711553203577330594476913868741742456351418525550214828297591584323227847019805029382183516476456072135035098491330472349604293922987492193093196775033504901979048280175721305618158877519196536509324816209488739023225409035382932017480465444929903218227769334668958530404811571842689601047281917568281756655319850133808983099704728097119747491723603914973200214236187812432050305807187505398614653
  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:
21981650272766397423352463702999194918342996851749470764998638297101984511083629850948734739259892644517804066934196324549964291319295078018774888682630566258923148119816524101389078999960573270377990828558687635112394538711553203577330594476913868741742456351418525550214828297591584323227847019805029382183516476456072135035098491330472349604293922987492193093196775033504901979048280175721305618158877519196536509324816209488739023225409035382932017480465444929903218227769334668958530404811571842689601047281917568281756655319850133808983099704728097119747491723603914973200214236187812432050305807187505398614653
  public exponent: 65537
  Validity: [From: Tue Jul 26 12:00:00 CEST 2005,
               To: Sun Jul 26 12:00:00 CEST 2020]
  Issuer: CN=Certipost E-Trust Primary Qualified CA, O=Certipost s.a./n.v., C=BE
  SerialNumber: [    04000000 00010552 64c425]

Certificate Extensions: 5
[1]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
```

```
  SSL CA
  S/MIME CA
  Object Signing CA]

[2]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F0 78 F9 07 77 10 BB DC   1E A1 AE 79 FB 30 10 DB  .x..w......y.0..
0010: C6 34 F8 17                                        .4..
]
]


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

]]  ]
]


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


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


]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 6C E1 D8 5F 74 58 E9 70   49 D6 CA 0D 2C 58 DA CA  l.._tX.pI...,X..
0010: 64 B6 51 4F C3 06 64 01   E9 8A 73 1D 9E CF 46 78  d.QO..d..s...Fx
0020: BF 3B 85 86 E2 3D 4A 18   94 2A 81 77 6F 82 F8 6F  .;...=J..*.wo..o
0030: F4 EE 22 FC 9D 18 21 72   60 BB 18 80 82 95 FB F9  .."...!r`.......
0040: F7 95 24 81 66 C1 B5 C3   B5 D2 B6 76 8B 3B 81 5C  ..$.f......v.;.\
0050: B8 A1 0E 2B 01 14 8B 80   09 40 EE F8 60 4C 19 E4  ...+.....@..`L..
0060: 17 CD 27 01 B3 63 12 05   A4 08 C9 B4 BF 9E 50 4E  ..'..c........PN
0070: B5 DE 0F 92 33 66 75 D0   3D E7 23 7C EA 25 71 7C  ....3fu.=.#..%q.
0080: FE 3E 2E 36 79 A1 E5 29   50 23 35 05 95 78 BB 9F  .>.6y..)P#5..x..
0090: 79 64 DC 57 48 27 2C E2   5C 33 CD C2 BB 7E 68 77  yd.WH',.\3....hw
00A0: A7 2F A3 49 17 72 E1 00   84 6B 7D 7A AF 39 0B 2C  ./.I.r...k.z.9.,
00B0: D5 D8 57 64 32 6C 84 0A   6A 76 3A D3 AC CD 9D B1  ..Wd2l..jv:.....
00C0: E7 37 DC EC 0C 2F C5 57   60 DF 88 F5 43 B1 01 64  .7.../.W`...C..d
00D0: 26 B4 27 82 10 B2 A3 50   EF 97 E6 7F BF 91 87 B3  &.'....P........
00E0: DB 90 A9 2A E2 7A 34 6C   73 49 F4 E8 8D 2E 6B 8A  ...*.z4lsI....k.
00F0: DD A1 8A 7F 63 D0 BF 58   1E AF CC 3F 92 50 2D D1  ....c..X...?.P-.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID3jCCAsagAwIBAgILBAAAAAABBVJkxCUwDQYJKoZIhvcNAQEFBQAwXDELMAkG
A1UEBhMCQkUxHDAaBgNVBAoTE0NlcnRpcG9zdCBzLmEuL24udi4xLzAtBgNVBAMT
JkNlcnRpcG9zdCBFLVRydXN0IFByaW1hcnkgUXVhbGlmaWVkIENBMB4XDTA1MDcy
NjEwMDAwMFoXDTIwMDcyNjEwMDAwMFowXDELMAkGA1UEBhMCQkUxHDAaBgNVBAoT
E0NlcnRpcG9zdCBzLmEuL24udi4xLzAtBgNVBAMTJkNlcnRpcG9zdCBFLVRydXN0
IFByaW1hcnkgUXVhbGlmaWVkIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAriDSeNuaoHKcBFIlLG1S2NcniTOg4bLV+zB1ay1/HGeODucfEt8XeRi7
tBtv+D11G55nN/Dx+g917YadAwShKHAtPLJroHNR4zWpdKUIPpSFJzYqqnJk/Hfu
dpQccuu/Msd3A2olggkFr19gPH+sG7yS6Dx0Wc7xfFQtOK6W8KxvoTMMIVoBuiMg
W6CGAtvVT3EkfqDKzrztGO7bvnzmzOAvneor2KPmnblApyHlYi0nSpdiFflbxaRV4
RBE116VUPqtmJdLb4xjxLivicSMJN2RDQnQylnfel6LploacJUQJ1AGdUX4ztwlE
5YCXDWRbdxiXpUupnhCdh/pWp88KfQIDAQABo4GgMIGdMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTwePkHdxC73B6hrnn7MBDbxjT4
FzBIBgNVHSAEQTA/MD0GCQOQDgcBAAECADAwMC4GCCsGAQUFBwIBFiJodHRwOi8v
d3d3LmUtdHJ1c3QuYmUvQ1BTL1FOY2VydHMHMgMBEGCWCGSAGG+EIBAQQEAwIABzAN
BgkqhkiG9w0BAQUFAAOCAQEAb0HYX3RY6XBJ1soNLFjaymS2UU/DBmQB6YpzHZ7P
Rni/O4WG4j1KGJQqgXdvgvhv9O4i/J0YIXJguxiAgpX7+feVJIFmwbXDtdK2dos7
gVy4oQ4rARSLgAlA7vhgTBnkF80nAbNjEgWkCMm0v55QTrXeD5IzZnXQPecjfOol
cXz+Pi42eaHlKVAjNQWVeLufeWTcV0gnLOJcM83Cu35od6cvo0kXcuEAhGt9eq85
CyzV2FdkMmyECmp2OtOszZ2x5zfc7AwvxVdg34j1Q7EBZCa0J4IQsqNQ75fmf7+R
h7PbkKkq4no0bHNJ90iNLmuK3aGKf2PQv1ger8w/klAt0Q==
-----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 Thumbprint	0e2b1b3ce368b11ae8b9221982ce69740e3dceb9
Public key SHA256 Thumbprint	2efdccbd9b768ea9654152816c48a53857f658c50462c12f66f5d56c0961616d

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:
24006751729987737463285030452993902374629050526542016130031750322293743139213202784813213482709335152611031406391633037540032036565000829743608508868431427838960727335586132
72260024738022754521550978668073613848886314527876619695170205142182992106517625874476574000109694632025016183163606961399776610711940089307587500742164497411652253547139771
69334557334399558495891953127385660029376236782791146443818739080758252054642538448809693082368758428714040768299077110739227256650318169746736582053355188697019790131215442
977240802235148520800523937282863754750807916853097524637865094123027892237920023721731622207444189
 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 daafcf2d]

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.+O+.
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  .O.....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:

```
-----BEGIN CERTIFICATE-----
MIID3TCCAsWgAwIBAgIJANme/Irar88tMA0GCSqGSIb3DQEBBQUAMIGGMSswKQYD
VQQDEyJCZWxnaWFuIFRydXN0IExpc3QgU2NoZW1lIE9wZXJhdG9yMQswCQYDVQQG
EwJCRTEjMCEGA1UEChMaQmVsZ2lhbiBGZWRlcmFsIEdvdmVybm1lbnQxJTAjBgNV
BAsTHE1pbmlzdHJ5IG9mIEVjb25vbWljIEFmZmFpcnMwHhcNMTAwMjI2MTA0MjA0
WhcNMjAwMjI0MTA0MjA0WjCBhjErMCkGA1UEAxMiQmVsZ2lhbiBUcnVzdCBMaXN0
IFNjaGVtZSBPcGVyYXRvcjELMAkGA1UEBhMCQkUxIzAhBgNVBAoTGkJlbGdpYW4g
RmVkZXJhbCBHb3Zlcm5tZW50MSUwIwYDVQQLExxNaW5pc3RyeSBvZiBFY29ub21p
YyBBZmZhaXJzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviuMAu24
2Bg3jIlV+lKm1FNaAgBzjDDXtP9+zqI+0fOjzBacWXR67a5hUuPggpEgPt8yGe83
dQkjmhS8hpUwZbs7WcbDgOC6ewI7+LSEx4wq2sEU/9mXMbDTqyhmnxu5pOeM8fGV
uBzQWWLj2ZsmRbeGEfZXbp37tT3X5ok289YbUp5ngyMrYZjlh75ncHT495JgaIVq
V+yO3zwJvTDHeBLZDvMucvPJX68lu7Pbfdw0pCrF/b04AzLAMARVsWv0olMvHUlF
```

FxhOenzVTEkduqtBzTicZNomw5qIdK0Lb6gWEcRbvBJzgcNauln3OGgXuA1WMdVd
3SOfAWQKvRb83QIDAQABo0wwSjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIHgDAdBgNV
HQ4EFgQUlbMH5fNSsMsP6WsAH9C0ZXXMbmwwEQYDVR0lBAowCAYGBACRNwMAMA0G
CSqGSIb3DQEBBQUAA4IBAQCmJdD8P7gI6NWf5eK/3frnqcHwXy57/FS4GmnQK08r
vlLw0lP/EcW9Hmu1p81YshscSSNwDO3tHDMyXy4BbUPM0b/yoIy8bRpZdxFPKwEi
nEhX1eJ0Bx9RmscmbBxA/EFXHp745EEDf99+4Vi7aG0AG+Sw1wOca9wX6h5JkxYj
tYIPZtL21r+NGig7Slrb35yGYZWGJZe9QAlwn7bXxTBNJM745BIw7mwdXUfakYFj
mYhPt4uNz51pfXS0VjdbWN/MJrURzBogoK8ZANcEMw+MlvwWbLyyvGTrlVPEBxP+
AeevbrqZUFsMddXb/Gkin2GSQxtlHUlR1VEbLOE2vNVC
-----END CERTIFICATE-----

The public key in PEM format:

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviuMAu242Bg3jIlV+lKm
1FNaAgBzjDDXtP9+zqI+0fOjzBacWXR67a5hUuPggpEgPt8yGe83dQkjmhS8hpUw
Zbs7WcbDgOC6ewI7+LSEx4wq2sEU/9mXMbDTqyhmnxu5pOeM8fGVuBzQWWLj2Zsm
RbeGEfZXbp37tT3X5ok289YbUp5ngyMrYZjlh75ncHT495JgaIVqV+yO3zwJvTDH
eBLZDvMucvPJX68lu7Pbfdw0pCrF/b04AzLAMARVsWv0olMvHUlFFxhOenzVTEkd
uqtBzTicZNomw5qIdK0Lb6gWEcRbvBJzgcNauln3OGgXuA1WMdVd3SOfAWQKvRb8
3QIDAQAB
-----END PUBLIC KEY-----