EESTI (ESTONIA) : Trusted List

Tsl Id: EE0001

Valid until nextUpdate value: 2025-12-12T12:57:48Z

TSL signed on: 2025-06-12T12:16:26Z

PDF generated on: Thu Jun 12 14:20:58 CEST 2025

TSL Scheme Information

TSL Id	*EE0001*
TSLTag	*http://uri.etsi.org/19612/TSLTag*
TSL Version Identifier	*5*
TSL Sequence Number	*68*
TSL Type	*http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric*

Scheme Operator Name

Name	*[en]*	*Estonian Information System Authority*
Name	*[et]*	*Riigi Infosüsteemi Amet*

PostalAddress

Street Address	*[en]*	*139A Pärnu mnt*
Locality	*[en]*	*Tallinn*
Postal Code	*[en]*	*15169*
Country Name	*[en]*	*EE*

ElectronicAddress

URI	*[en]*	*mailto:ria@ria.ee*
URI	*[en]*	*https://sr.riik.ee/en.html*

Scheme Name

Name	*[en]*	*EE: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.*

Scheme Information URI

URI	*[en]*	*https://sr.riik.ee/en/tl.html*
URI	*[en]*	*http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN*
URI	*[et]*	*https://sr.riik.ee/et/tl.html*

URI	[et]	http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014R0910&from=EN

Status Determination Approach http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate

Scheme Type Community Rules

URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon
URI	[en]	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EE

Scheme Territory EE

Policy Or Legal Notice

TSL Legal Notice	[en]	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.
TSL Legal Notice	[et]	Käesoleva usaldusnimekirja suhtes kohaldatav õigusraamistik on Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

Historical Information Period 65535

Pointer to other TSL - EUROPEAN UNION

1.EU TSL - MimeType: application/vnd.etsi.tsl+xml

TSL Location https://ec.europa.eu/tools/lotl/eu-lotl.xml

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: 3

Serial Number: 660862747298009142807362633871991440505734410485

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIoDCCBoigAwIBAgIUc8lcSUtvEKAMMvHm9QWU05kXsPUwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZnlpYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gUVVBTEIgSUVEIENBIEcxMB4XDTIzMTExNzEwMTE0NloXDTI3MTEx
NzEwMTE0NlowggEVMQswCQYDVQQGEwJMVTFDMEEGA1UECww6Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZ2FuaXphdGlvbjE5MDcGA1UECwwwRGlyZWN0b3Jh
dGUtR2VuZXJhbCBmb3IgRGlnaXRhbCBTZXJ2aWNlcyAoREIHSVQpM5MwIQYDVQRhDBpMRUlYRyOy
NTQ5MDBaTlBMUZMVVE5VTM5MzEcMBoGA1UECgwTRVVST1BFQU4gQ09NTUlTU0lPTjElMCMGCSqG
Slb3DQEJARYWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTEcMBoGA1UEAwwTRVVST1BFQU4gQ09NTUlT
U0lPTjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKWYeBA9kYAREIGnHojRNpbby44G
+TSJcgHl9QtyXlYjB234hSAYyJvW+gKvoownskrogfUP6GOmOgEFZX335Y0sBwfppVemEoe9H9Aj
/cpT14Iqd805V4a88ASRfR0Va1xmOJrDsBZWqZHx0EEHBctIF5BjyTMAcQybha+4AOlotp3dfr/7Z
A3Cu4GYbN9BuQyyqfqrjMduDzzDjVwKC17aEsLev60C1FnIj/FVEda3JSGIlDSJyUceTaRcot1r
w6gjKrOVhwP/UHfevJ3jCsQsuAzkf7ivzHzYuPPPR9Ussecwr7O95Fr4wbPYlyX2AOTIieAC7GMV
XHN1/+4LH74ndvqlYEScXwmN9Skib3+G6TquOCQxvNXzHPZb95btCoSnVprCn14O3CXUTZMEKkhP
uKW8dl6pR2JSGbtT+xBkcc1wYl/UnzE3d+YK5SevUT2COwJM+AcjSoUaRTBINsD/ezDDvv7vtbF
1XccajjoCNkurzayTsMszGDvAF171LY69INY6yK0uzrS+3c/hEhctXa5KIC3PpWrBGQ5mw73KerR
vnAhzDZemVquPk1D59aJNfHoHXmy1bS52rHWYOwHH+2qbODdh8GkHwHXBzSpFit1Kg2brpavhztN
aGlj6GsLFAbr8okCUJlIOQLO8Tfy9Vnn5Rq0+7VTdd8dAxg9AgMBAAGjggKaMIICjAMBgNVHRMB
Af8EAjAAMB8GA1UdIwQYMBaAFHNJ8lUAcFAR8nhJ+i/NXGcjGOKUMIGGBggrBgEFBQcBAQR6MHgw
RgYIKwYBBQUHMAKGOmh0dHBzOi8vcWNhLWcxLmRpZ2lOYWxzaWduLnB0L0RjR0lUQUxTSUdOUVVB
TEIGSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGGImh0dHBzOi8vcWNhLWcxLmRpZ2lOYWxzaWduLnB0
L29jc3AwIQYDVR0RBBowGIEWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTBfBgNVHSAEWDBWMDcGCysG
AQQBgcdBAEBMCgwIgYIKwYBBQUHAgEWGmh0dHBzOi8vcGtpLmRpZ2lOYWxzaWduLnB0MBAGDisG
AQQBgcdBBAIBAQEGMAkGBwQAi+xAAQMwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMIGB
BggrBgEFBQcBAwSBrzCBrDAVBggrBgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYBATAIBgYEAI5G
AQQwEwYGBACORgEGMAkGBwQAjkYBBgIwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGln
aXRhbHNpZ24ucHQvUERTX2VuLnBkZhMCZlW4wLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24u
cHQvUERTX380Ln8kZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRh
bHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZJRURDQUcxLmNybDAdBgNVHQ4EFgQUlO5hwcl9/63i
ssm59r+TIHeJSZwwDgYDVR0PAQH/BAQDAgZAMA0GCSqGSIb3DQEBDQUAA4ICAQCn8qjJhTe3SsD7
cB85BkDzt+CBnJJm7bOFc9t9IU6iKntVtjPU4T+cYiPk8Tn7+/w7dBphRzjZCL1sDfSJGQ5JPBw+
hBPuvzGqP4xVi5j4jhg/GpYSaa2+dkFXlKe65d+Ij/RnwB5nfqVfNZtasj7yX+ou9au5LSUPlKQ
xDrMie8KjsNtlkFjQDoIoGAx8b0u6WyhAuqwEacCznft20Dim3sC7XJw8GHumrnW52rUzI4sbXoT
BAt8F1zPCbEbjU0oc85bFNPIChh+9sHUorEmHIlcg30LBHihkDCx4mK8J60Jybk57D4U2RO29VsJ
fDmnvNxfJZxfLHEJ2tkh+AMgIJXPDlvXQ+rZ1NmLHrbXkcHOlqR3F8BakTi2Mi5AZZfkfjZjkigE
StN6Enaq6gwF7EssIqEKmhSQ8XlhxWSRqJKcnEUw+NhrvR4WuKlvYrmxlCLOj6q89Hh121aUGUh
L2L2WCVBjVXqux7s4mvECDzrucl5ilaVT32HO3g8qNLGD5lum53U5v/Nv68ltyHH96unztwBebmg
ox8giVRdzPhmPrpSfbmeNNDKj1p95CeOvd3P9jCUvChVvH2P2ZUjc24tWe+tzclsCji7GbKr6kjH
c1jFudjehfIAbm1lZAYdDNrhXamnsRVsz7iSH20eygCArlwSQ//WIQZPFrRffg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *EUROPEAN COMMISSION*

Subject E: *digit-dmo@ec.europa.eu*

Subject O: *EUROPEAN COMMISSION*

Subject 2.5.4.97: *LEIXG-254900ZNYA1FLUQ9U393*

Subject OU: *Directorate-General for Digital Services (DIGIT)*

Subject OU: *Certificate Profile - Qualified Certificate - Organization*

Subject C: *LU*

Valid from: *Fri Nov 17 11:11:46 CET 2023*

Valid to: *Wed Nov 17 11:11:46 CET 2027*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A5:98:78:10:3D:91:80:11:12:51:A7:1E:82:51:36:96:DB:CB:8E:06:F9:34:89:
72:01:C8:F5:0B:72:5E:56:23:07:6D:F8:85:20:18:C8:9B:D6:FA:02:AF:A2:8C:27:B2:4A:E8:81:F5:0F:E8:63:A6:42:01:05:65:7D:F7:E5:8D:2C:07:07:E9:A5:57:A6:12:87:BD:1F:D0:23:FD:CA
:53:D7:82:2A:74:1D:39:57:86:BC:F0:04:91:7D:1D:15:6B:5C:66:40:9A:C3:B0:16:56:A9:91:F1:D0:41:07:05:CB:48:17:90:63:C9:33:00:71:0C:98:85:AF:B8:00:E2:28:B6:9D:DD:17:FE:D9:
03:70:AE:E0:66:1B:37:D0:6E:43:2C:AA:7E:AA:E3:31:DB:83:C7:30:E3:57:02:82:D7:B6:84:80:B7:AF:EB:40:85:16:72:09:FC:55:44:75:AD:E5:25:21:A2:94:3E:49:C9:47:1E:4D:A4:5C:A2:D
D:6B:C3:AB:23:2A:B3:95:87:03:FF:50:77:DE:BC:9D:C9:0A:C4:2C:B8:0C:E4:7F:B8:AF:CC:7C:D8:B8:F3:CF:47:D5:2C:B1:E7:30:AF:B3:BD:E4:5A:F8:C1:B3:D8:23:25:F6:00:E4:E5:89:E0:02
:EC:63:15:5C:73:75:FF:EE:0B:1F:BE:27:76:FA:09:60:44:9C:5F:09:8D:F5:29:22:6F:7F:86:E9:3A:AE:38:24:31:BC:D5:F3:1C:F6:5B:F7:96:ED:0A:84:A7:56:9A:C2:9F:5E:0E:DC:25:D4:4D:93
:04:2A:48:4F:B8:A5:BC:74:8E:A9:47:62:52:19:BB:53:FB:10:64:71:CD:70:61:59:54:9F:31:37:77:E6:0A:E5:24:9E:BD:44:F6:08:EC:09:33:E0:1C:8D:2A:14:69:14:C1:20:DB:03:FD:EC:C3:0
E:FB:FB:BE:D6:C5:D5:77:1C:68:98:E8:08:D9:2E:AF:36:82:4E:C3:2C:CC:60:EF:00:5D:78:D4:B6:3A:F6:53:58:EB:22:B4:BB:3A:D2:FB:77:3F:B4:41:DC:B5:76:B9:28:80:B7:3E:95:AB:D4:64
:39:9B:0E:F7:29:EA:D1:BE:70:21:CC:36:5E:99:5A:AE:3E:4D:43:E7:D6:B9:35:F1:E8:1D:79:B2:D5:B4:B9:DA:B1:D6:60:EC:07:1F:ED:AA:6C:E0:DD:87:C1:A4:1F:01:D7:07:34:A9:16:2B:75:
2A:0D:9B:AE:96:AF:87:3B:4D:68:69:63:E8:6B:0B:14:06:EB:F2:89:02:50:99:65:38:E2:D0:F1:37:F2:F5:59:E7:E5:1A:B4:FB:B5:53:75:DF:1D:03:18:3D:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

Authority Info Access *https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b*

https://qca-g1.digitalsign.pt/ocsp

Subject Alternative Name	*digit-dmo@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*94:EE:61:C1:C9:7D:FF:AD:E2:B2:C9:B9:F6:BF:93:20:77:89:49:9C*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*E0:A6:20:FB:B6:74:73:62:BB:93:3A:C4:41:69:D6:76:A5:53:44:47:16:CF:5F:31:60:5F:12:A2:2B:83:96:B1*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*231199879490522356566716403815664415819903446597*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----

MIIIBDCCBeygAwIBAgIUKH9cdKE3vD5rBCmH3Krsppm6rkUwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdlaENlcnRpZmlpYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTIzMDIyMjE1MzYyOVoXDTI2MDIy
MTE1MzYyOVowggFWMQswCQYDVQQGEwJHUjE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWlJcjEjMCEGA1UEYQwaTEVlWEctMjU0OTAwWk5Z
QTFGTVROVUtOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMTEwLwYJKoZIhvcNAQkBFiJpb2FubmEua2Fsb2dl
cm9wb3Vsb3VAZWMuZXVyb3BhLmV1MRcwFQYDVQQEDA5LQUxPR0VST1BPVUxPVTEPMA0GA1UEKgwG
SU9BTk5BMR0wGwYDVQQLDBRSZW1vdGVRU0NETWFuYWdlbWVudDEeMBwGA1UEAwwVSU9BTk5BIEtB
TE9HRVJPUE9VTE9VMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnIDj3MSrgRjPj4E7
hP7f2nf47K9P3KIWa9HBd77uD0bOvQ/U4d5GBJx6ildYnX0pIhj1uq+fMafM1BIvGAgPFg7NiWYj
dz1t5jcdx3iWrao6ElkzNP/a+3s/wPfHmvOitmgnBBAVOurgz7tT7WX1pUrATL5VxbrY8ETxD2Qg
frBajpwgSYeho+U2FmVV9UULw0rAQVbFqUEgg9Nb88GMXNt2sXPveO7GtXYbi0WClSdej1jVAr69
RuyDbrI7fCr4Q6yzXWpOWF7Vr2z2S3hhqnPPl21qVfhaHGg6mBu6wRqOK0ct+zp42OEEC246NYIO
JAoCftcj8zewo4zBlRjwjOIDAQABo4ICvTCCArkwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRz
SfFAHBQEfJoSf/ovzVxnlxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRklFRENBRzEucDdiMC4GCCsG
AQUFBzABhjodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMC0GA1UdEQQmMCSBImlv
YW5uYS5rYWxvZ2Vyb3BwdWxvdUlBIly5ldXJvcGEuZXUwXwYDVR0gBFgwVjA3BgsrBgEEAYHHfAQB
ATAoMCYGCCsGAQUFBwIBFhpodHRwczovL3Bra55kaWdpdGFsc2lnbi5wdDAQBg4rBgEEAYHHfAQC
AQEBBDAJBgcEAIvsQAECMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBLBgNVHR8ERDBC
MECgPqA8hjpodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRklF
RENBRzEuY3jsMB0GA1UdDgQWBBRkfGQMVVIxB/mVo0L3Zjs2nTpaRjAOBgNVHQ8BAf8EBAMCBkAw
gdMGCCsGAQUFBwEDBIHGMIHDMAgGBgQAjkYBATAIBgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYB
BgEwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX3B0LnBk
ZhMCcHQwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX2VuLnBkZhMCZW4wFQYI
KwYBBQUHCwIwCQYHBACL7EkBATAVBggrBgEFBQcLAjAjBgcEAIvs5QECMA0GCSqGSib3DQEBDQUA
A4ICAQBfvXM2+mTPDHZGA7BLQ+04SJ1rObRmuKy9w5xLRp9bBanBS90nRljixOMIATTgZFF6pT4H
6q3XFYDvbrm/SUNkVKnSovDucXB/bEhqEN+DYmLxxLFxbsGoBZosbFloFHgoct+OP/ttxe9e8hIL
5+j5TXwGB/+u3wbOWfA8XdwvKl1UVJHrEejjPTsneBBKJXLpnnQYrPM3guEayVRkNdYd9dsaVJKu
6bnw+yVjaBavX9Mspu4b5leUHA+lRR5kgSm+RjAJfymGtgy9/heE/MAX+ANL8tb4PqC3XEGfP/XM
4ZU597CeL5r+OwNnN+6yToYQh3LoQrtJvkvj2uNLoWX15WMt37KRVgiAdOkVFFlsQRvTJM9OYBl/4
Rmc1g3TD4O0TBlqzjoMnLGD8d3nhtKsfb29gW7Pj9lGZLI4OblzeBZwQZKK5U8LAh38mzlUJ2UGY
C1FHByNKLn9L6bVn0F7OdelRiNrnby9TiKwl8gwZUAC5bxOv/5dfswUFN1kQ2LTiRMM+8G/1lDe1
CAuN4H2W+0hAvkBy2KlAzcxa6nCOilHzu1BikfV7x4gojYoFAXl+tKe8JtlujlFR+gWb7T3ymRFG
sZMDoabXlRvnvrks/KRqhi8/6YmCDpx4jDTkQf3GOVC2AXULtNtV1i28md5isoH3GHgqPeKYdNxO
MJN7tg==

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA512withRSA*
Issuer CN:	*DIGITALSIGN QUALIFIED CA G1*
Issuer O:	*DigitalSign Certificadora Digital*

Issuer C:	*PT*
Subject CN:	*IOANNA KALOGEROPOULOU*
Subject OU:	*RemoteQSCDManagement*
Subject GIVEN NAME:	*IOANNA*
Subject SURNAME:	*KALOGEROPOULOU*
Subject E:	*ioanna.kalogeropoulou@ec.europa.eu*
Subject OU:	*Entitlement - EC STATUTORY STAFF*
Subject O:	*EUROPEAN COMMISSION*
Subject 2.5.4.97:	*LEIXG-254900ZNYA1FLUQ9U393*
Subject OU:	*Certificate Profile - Qualified Certificate - Member*
Subject C:	*GR*
Valid from:	*Wed Feb 22 16:36:29 CET 2023*
Valid to:	*Sat Feb 21 16:36:29 CET 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:80:E3:DC:C4:AB:81:18:CF:8F:81:3B:84:FE:DF:DA:73:F8:EC:AF:4F:DC:A2:16:6B:D1:C1:77:BE:EE:0F:46:CE:BC:EF:D4:E1:DE:46:04:9C:7A:8A:57:58:9D:7D:29:22:18:F5:BA:AF:9F:31:A7:CC:D4:19:6F:18:08:0F:16:AE:CD:89:66:23:77:3D:6D:E4:97:1D:C7:78:96:AD:AA:3A:12:59:33:34:FF:DA:FB:7B:3F:C0:F7:C7:9A:F3:A2:B6:68:27:04:10:15:3A:EA:E0:CF:BB:53:ED:65:F5:A5:4A:C0:4C:BE:55:C5:BA:D8:F0:44:F1:0F:64:20:7E:B0:5A:22:9C:2A:49:87:A1:A3:E5:36:16:65:55:F5:45:0B:C3:4A:C0:41:56:C5:A9:41:2A:83:D3:5B:F3:C1:8C:5C:DB:76:B1:73:EF:78:EE:C6:B5:76:1B:8B:45:82:21:27:5E:8F:52:55:02:BE:BD:46:EC:83:0E:B9:7B:7C:2A:F8:43:AC:B3:5D:6A:4E:58:5E:D5:AF:6C:F6:4B:78:61:AA:73:CF:97:6D:6A:55:F8:5A:1C:6A:BA:98:1B:BA:C1:1A:8E:2B:47:2D:FB:3A:78:65:01:04:0B:6E:3A:35:82:0E:24:0A:02:FE:D7:23:F3:37:B0:A3:8C:C1:95:12:70:25:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*ioanna.kalogeropoulou@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*64:7C:64:0C:55:59:71:04:99:95:A3:42:F7:66:3B:36:9D:3A:5A:46*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_QcSSCD

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *87:90:5C:2C:90:51:CE:2D:45:DD:BE:38:22:83:8F:A7:05:BF:3A:3A:60:73:64:93:3B:8D:1F:7A:70:15:53:DE*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *566117616430214055757992355472683005220982589151*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIH9DCCBdygAwIBAgIUYymXhglnqt2gl4PHVh4juzinht8wDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWdulENlcnRpZmlJYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIhSVRBTFNJR04gUVVBTEIGSUVEIENBIEcxMB4XDTI0MDQyNjEyNDkyMloXDTI3MDQy
NjEyNDkyMlowggFKMQswCQYDVQQGEwJHUjE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWljcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50OCDgRUMgU1RBVFVUT1JZIFNUQUZGMS0wKwYJKoZIhvcNAQkBFh5hcG9zdG9sb3MuYXBs
YWRhc0BlYy5ldXJvcGEuZXUxEDAOBgNVBAQMB0FQTEFEQVMxEjAQBgNVBCoMCUFQT1NUT0xPUzEd
MBsGA1UECwwUUmVtb3RlUVNDRE1hbmFnZW1lbnQxGjAYBgNVBAMMEUFQT1NUT0xPUyBBUExBREFT
MIIBIjANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsILa9o3bgz0l/dR1R01MhItrd6BLkxak
Jxlgpnlc1fhTbR3uYGvSVwfsmjQei/YkbjMoNzakjo4voPhUJlBa9077TjLGwZSghfkp0+vcg4yeC
LodAQatG7iEsh5Fr5uZgwPpLXExiI0234QRcw7kJsl4k7wd7YvXAj1kv5zLTFo6sOr8ZF9km2rU1
7gbdZislH3/uR+jHkkhbljm+MspETNN+Nva7duhkz14llh/EJryTEPQLAdsgz+cRkBkyLQ1YYS6i
R3pifrsMvXzHYiwjY9AzPNd3cOBS2Ov0SkB6tRyOka+6MREWY9aU22K/Q0anyrNCns5N/UXs589T
wrWp0QIDAQABo4ICuTCCArUwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRzSfFAHBQEfJoS6ov
zVxnIxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRwczovL3FjYS1nMS5kaWdp
dGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRkIFRENBRzEucDdiMC4GCCsGAQUFBzABhIJodHRw
czovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMCkGA1UdEQQiMCCBHmFwb3N0b2xvcy5hcGxh
2GFzQGVjLmV1cm9wYS5ldTBfBgNVHSAEWDBWMDcGCysGAQQBgcd8BAEBMCgwJgYIKwYBBQUHAgEW
Gmh0dHBzOi8vcGtpLmRpZ2l0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEEMAKGBwQAi+xAAQIw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEsGA1UdHwREMElwQKA+oDyGOmh0dHBzOi8v
cWNhLWcxLmRpZ2l0YWxzaWduLnB0L0RjR0lUQUxTSUdOUVVBTEIGSUVEQ0FHMS5jcmwwHQYDVR0O
BBYEFHG/mw4edY/tTzrYu+8+Up7LgWyGMA4GA1UdDwEB/wQEAwIGODCB0wYIKwYBBQUHAQMEgcYw
gcMwCAYGBACORkEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATBqBgYEAI5GAQUwYDAu
FihodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfcHQucGRmEwJwdDAuFihodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfZW4ucGRmEwJlbjAVBggrBgEFBQcLAjAJBgcEAlvs
SQEBMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwDQYJKoZIhvcNAQENBQADggIBALUt37pV7w5ZwRxB
B5PdTGTC+KcWytkuyuRlJlVu+hVD5yVC2E+4+EPB2mRUzkjeEZM/3lMtpzdwaNHe2YU9lCkoUFtD7V
LIEdiIfGO0MnXde2BAQN1VAt0s8xLwr3DNATsrtYPbtkQ73WCNqQwuNlg4LCFXHHpzvsKzYmYz+h
YgkA8daRZRJdnZx/eX05iYFtShbbz8VamNb+A1L/KmqSrt5iG8d95LSSq95bNrntxSLaYDjfOlTj
hW5KOwlXBJPA+sQDYPngHur1nLWUJg6QB8fo/YwMOTmylciurp8Qzktxfjlu1wSZEpd/xZKoDWVDN
jIa8p0RFbQs/l7DpP/s57p8PKcntDOvQkYCajpRf1KJ/69gKdVkB6nOKHFQCTmAeCDapWsl9+jPC
nriywN60ep+MMqedZ/lV8LecbJ/1E+kw6PhC6Rs4MlwmHHCe6BB/9oTK7SWW/CtlZh8ygtl0+5jI
DS/83b0F0jdnZUV2qhlZJIVOROcQIjcWs7kYS8vWAqBbcCAhYNpaaUh1rnKGqo2jpOo5HXhgSVHN
RrC+CylNNDUGAhpgPsAD93ui6JQCjdISzDkraWZA/GtmdpId0b7IR6HfRBs/QzeA4Rj7ChMMOFxD
ZPp2t6kEyPb1UOshC79fmoNRkBxmGKqMCPakQiiUolg/BkLIUVYCIloQ8zsk

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *APOSTOLOS APLADAS*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *APOSTOLOS*

Subject SURNAME: *APLADAS*

Subject E: *apostolos.apladas@ec.europa.eu*

Subject OU: *Entitlement - EC STATUTORY STAFF*

Subject O:	*EUROPEAN COMMISSION*
Subject 2.5.4.97:	*LEIXG-254900ZNYA1FLUQ9U393*
Subject OU:	*Certificate Profile - Qualified Certificate - Member*
Subject C:	*GR*
Valid from:	*Fri Apr 26 14:49:22 CEST 2024*
Valid to:	*Mon Apr 26 14:49:22 CEST 2027*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:82:DA:F6:8D:DB:83:3D:25:FD:D4:75:47:4D:4C:84:8B:6B:77:A0:4B:93:16:A4:27:19:6A:A6:79:5C:D6:18:53:F1:1D:EE:60:6B:D2:57:07:EC:9A:34:1E:8B:F6:24:6E:33:28:37:36:A4:8E:8E:2F:A0:F8:54:20:90:5A:F7:4E:D3:24:B1:B0:65:28:21:7E:4A:74:FA:F7:20:E3:27:82:2E:87:40:41:AB:46:EE:21:2C:87:91:6B:E6:E6:60:C0:FA:4B:5C:4C:62:97:4D:B7:E1:04:5C:C3:B9:09:B0:8E:24:EF:07:7B:62:F5:C0:8F:59:2F:E7:32:D3:16:8E:AC:3A:BF:19:17:D9:26:DA:B5:35:EE:06:DD:66:2B:08:1F:7F:EE:47:E2:47:92:48:5B:96:39:BE:32:CA:44:4C:D3:7E:36:F6:BB:76:E8:64:CF:5E:25:96:1F:C4:26:BC:93:10:F4:0B:01:DB:20:CF:E7:11:90:19:32:2D:0D:58:61:2E:A2:47:7A:62:7E:BB:0C:BD:7C:C7:62:5C:09:63:D0:33:3C:D7:77:73:40:52:D8:EB:F4:E6:40:7A:B5:1C:8E:91:AF:BA:31:11:16:63:D6:94:DB:62:BF:43:46:A7:CA:B3:42:9E:CE:4D:FD:45:EC:E7:CF:53:C2:B5:A9:D1:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*apostolos.apladas@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*71:BF:9B:0E:1E:75:8F:ED:4F:3A:D8:BB:EF:3E:52:9E:CB:81:6C:86*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B6:3D:41:67:44:E7:09:8B:F9:EC:2C:AA:59:6A:93:BC:24:68:E3:7F:82:84:BA:65:EC:C0:61:71:1B:CB:AA:18*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*

Serial Number: *165751212142046865099794733233293184155782588036*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIIAjCCBeggAwIBAgIUHQiKmcmM7NMyG25PRlC8Qs9VpoQwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZZl0YWxTaWdulENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTIzMTAwMjEzMjk1MFoXDTI2MTAw
MTEzMjk1MFowggFaMQswCQYDVQQGEwJSTzE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJlvZmlsZSAt
IFE1YWypZmlZCBDZXJ0aWZpY2FlZSAtIE1lbWllcjEjMCEGA1UEYQwaTE1YIWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMSswKQYJKoZIhvcNAQkBFhxhZHJpYW4uY3JvaXRv
cnVAZWMuZXVyb3BhLmV1MREwDwYDVQQEDAhDUk9VE9VTEaMBgGA1UEKgwRO09OU1RBTlRjTiBB
RfJQU4xHTAbBgNVBAsMFFJlbW90ZVFTQ0RMYW5hZ2VlZW50MSMwIQYDVQQDDBpDTG5TVEFQVEIO
IEFEUklBTiBDUk9JVE9SVTCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAOoCggEBAMEPfdAKKFfK
pCzoMFhBvEv5Ol0t9wQ1Ua5JzVpENOOKKJS9Cm/lwzyTLsWuLJDgaUvml6oTOZ4TYo7WaFyyi2YY
q4TSVXo9G8t8RykHMu13vwrCyoMJ/GucZ9ypgkRnEEWUdvUGN26ROmCsryBlfvCpC/Pe9tF6Oh6d
Bi2CmX8HIE43zNYOkVuikxa5ymB13W1yYsNKV920My/ZCfpFoEyW34H3+6ZNR7lwh6h6T4QkIMkj
cRTTaeMTYD/kaQV+IFntXIfP2of6XdqaIf39rnJeuthCpgL8cIWAE3mbOvuJlRXAcrHRhj2gDT3kX
Jvpo8S+qmkvMlRdabzeYbVzo+3kCAwEAAaOCArcwggKzMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUc0nxQBwUBHyaEn/6L81cZyMY6RQwgYYGCCsGAQUFBwEBBHoweDBGBggrBgEFBQcwAoY6aHR0
cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZjRURDQUcxLnA3YjAu
BggrBgEFBQcwAYYiaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvb2NzcDAnBgNVHREEIDAe
gRxhZHJpYW4uY3JvaXRvcnVAZWMuZXVyb3BhLmV1MF8GA1UdIARYMFYwNwYLKwYBBAGBx3wEAQEw
KDAmBggrBgEFBQcCARYaaHR0cHM6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwEAYOKwYBBAGBx3wEAgEB
AQQwCQYHBACL7EABAjAdBgNVHSUEFjAUBggrBgEFBQcDAgYlKwYBBQUHAwQwSwYDVR0fBEQwQjBA
oD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFMSUZjRURD
QUcxLmNybDAdBgNVHQ4EFgQUInlF6CI5HKvUE35Ifm8y7cfQvvAwDgYDVR0PAQH/BAQDAgZAMIHT
BggrBgEFBQcBAwSBxjCBwzAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcEAI5GAQYB
MGoGBgQAjkYBBTBgMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2lOYWxzaWduLnB0L1BEU19wdC5wZGYT
An8DMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2lOYWxzaWduLnB0L1BEU19lbi5wZGYTAmVuMBUGCCsG
AQUFBwsCMAkGBwQAi+xJAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjANBgkqhkiG9w0BAQ0FAAOC
AgEACH5DHJNDzsMXTu+ph7fXEEbFK6xgbg68tRcvwr7xgmaAwfM2pGjq62O637y5yVfYT6Aa7oiC
4sshT7Tu/c/UHpjTn4/tDghkwlhSkUc9FREmOu9doRLWNJ6QE31UBW94w9s0EjpvFJLpkODv0F2M
4iqTLMtV7H0M+ggNA+cMa2NnyRZCCNVKoP8CxgQySjgv7DhSXTSahhaKJUQgE5yXvrjBZvrlyE5I
TCtoLFa0mWIjWlW4aVf4P+m1lLjCpqzpLc5B9m1gXxwzjzUT0DcQgLdTka/QBFKTvD0F8+6qUqaz
M6+26ddFOQegX8Kc8xzvyXss1bu8JqXkwjzEwHd6ywAWgqji7v1+KIT0DvX0Y4X8kSh9X5Xuz5tj
Znby0hvP7qQSXhHsYUOrxU3Dkj8V9kJvDKhnCuTdjcEaCrcdWbimNib4YIicCQOoE79XL5/KQ5gY
geCGkudcLkteOfvDBM/G8HbqSbv4x8+HEdnjgoCL4Iv4iaD4qtpfvkU6bRXlMtT2Q4Q7pg/Mo02j
h66+59HoXtoBUeUZMWER2OkjUG1CbOOwcllw6GuiCZTBR5u0tG3C54f0jBdDqj2Unvh9geRjBiRN
q0pksCD9GOj4yQc0iYxEbu2RCum8suLlkeQZL2oVYvRdjYFiT5kcWAYuGaZH3YGoR+MT3b7ABaho
lIY=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *CONSTANTIN ADRIAN CROITORU*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *CONSTANTIN ADRIAN*

Subject SURNAME: *CROITORU*

Subject E: *adrian.croitoru@ec.europa.eu*

Subject OU: *Entitlement - EC STATUTORY STAFF*

Subject O: *EUROPEAN COMMISSION*

Subject 2.5.4.97: *LEIXG-254900ZNYA1FLUQ9U393*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject C: *RO*

Valid from: *Mon Oct 02 15:29:50 CEST 2023*

Valid to: *Thu Oct 01 15:29:50 CEST 2026*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:0F:7D:D0:0A:28:57:CA:A4:2C:E8:30:58:41:BC:4B:F9:38:8D:2D:F7:04:35
:51:AE:49:CD:5A:44:34:E3:8A:2A:34:BD:0A:6F:C8:C3:3C:93:2E:C5:AE:2C:90:EA:69:4B:E6:23:AA:13:39:9E:13:62:8E:D6:68:5C:B2:8B:66:15:AB:84:D2:55:7A:3D:1B:CB:7C:47:29:07:32:
ED:77:BF:0A:C2:CA:83:09:FC:6B:9C:67:DC:A9:82:44:67:10:45:94:76:F5:06:37:6E:91:3A:60:AC:AF:20:48:7E:F0:A9:0B:F3:DE:F6:D1:7A:3A:1E:9D:06:2D:82:99:7F:07:94:4E:37:CC:D6:0
E:91:5B:A2:93:16:B9:CA:60:75:DD:6D:72:62:C3:4A:57:DD:B4:33:2F:D9:09:FA:45:A0:4C:96:DF:81:F7:FB:A6:4D:47:B2:30:87:AB:7A:4F:84:24:20:C9:23:71:14:D3:69:E3:13:60:3F:E4:69:
05:7E:94:59:ED:5E:57:CF:DA:87:FA:5D:DA:9A:89:FD:FD:9C:97:AE:B6:10:A9:80:BF:1C:89:60:04:DE:66:F4:BE:E2:48:45:70:1C:AC:74:61:8F:6A:83:4F:79:17:26:FA:68:F1:2F:AA:9A:4B:C
C:21:17:5A:6F:37:98:6D:5C:E8:FB:79:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*adrian.croitoru@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*22:79:45:E8:29:79:1C:AB:D4:13:7E:48:7E:6F:32:ED:C7:D0:BE:F0*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*9C:01:27:83:96:92:47:AD:30:2F:05:84:79:7E:17:43:ED:23:05:EF:76:BD:B7:A8:31:1C:5F:EF:63:87:A0:ED*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*620818890745556847869731431413617216995310914687*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----

MIIH9DCCBdygAwIBAgIUbL57W2NNkznemb+sNTEfKSmLTH8wDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2I0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbREIHSVRBTFNJR04gUVVBTEIGSUVEIENBIEcxMB4XDTIzMDQyMTE1NTk0M1oXDTI2MDQy
MDE1NTk0M1owggFPMQswCQYDVQQGEwJCRTE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWljcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
QTFGTVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JUU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMSgwJgYJKoZIhvcNAQkBFhlqZXJvZW4ucmF0aGVA
ZWMuZXVyb3BhLmV1MQ8wDQYDVQQEDAZSQVRIw4kxGDAWBgNVBCoMD0pFUk9FTiBBUk5PTEQgTDEd
MBsGA1UECwwUUmVtb3RlUVNDRE1hbmFnZW1lbnQxHzAdBgNVBAMMFkpFUk9FTiBBUk5PTEQgTCBS
QVRlw4kwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDgC3u493b8aZgWC+wdf0+1/ILG
/e+XYcHOiNxCL0kCVEo+sRt9z55sX2wHmon/aXsi54twfqk9AQxlWpLyXuZa3jRrBil55Bdqtmh+
2+rrV0AuOhHhupwAKO52bP+yI5U8G4r+g+NzYUMwNCDM9nvj0A5xFiVqRV+ogU5tWmaRJ7sazSXa
G9sjs531SZilsyjvMH72jtbeQiYEmdfc0GKa2Cnj9vcxS/+1ht9yMCiH/OzTZXOPht9v8dVXx2TV
1pZaDB/1Bl8qPGew2YRL7WPKgn2GnNm1dm7H5vL3l5pz5An9mQR4iu1uj2WALi+9BzauxLyQnhCCM
WawlofaNrrudAgMBAAGjggK0MIICsDAMBgNVHRMBAfBEAjAAMB8GA1UdIwQYMBaAFHNJ8UAcFAR8
mhJ/+i/NXGcjGÖkUMIGGBggrBgEFBQcBAQR6MHgwRgYIKwYBBQUHMAKGOmh0dHBzOi8vcWNhLWcx
LmRpZ2I0YWxzaWduLnB0L0RjR0lUQUxTSUdOUVVBTElGSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGG
Imh0dHBzOi8vcWNhLWcxLmRpZ2I0YWxzaWduLnB0L29jc3AwJAYDVR0RBB0wG4EZamVyb2VuLnJh
dGhlQGVLmV1cm9wYS5idTBfBgNVHSAEWDBWMDcGCysGAQQBgcd8BAEBMCgwJgYIKwYBBQUHAgEW
Gmh0dHBzOi8vcGtpLmRpZ2I0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEEMAkGBwQAi+xAAQIw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEsGA1UdHwREMEIwQKA+oDyGOmh0dHBzOi8v
cWNhLWcxLmRpZ2I0YWxzaWduLnB0L0RjR0lUQUxTSUdOUVVBTElGSUVEQ0FHMS5jcmwwHQYDVR0O
BB1YEFBvvbgFnORNt1DwbohrG8iqrqWC5MA4GA1UdDwEB/wQEAwIGQDCB0wYIKwYBBQUHAQMEgcYw
gcMwCAYGBACORgEBMAgGBgQÄjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATBqBgYEAI5GAQUwYDAu
FihodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfcHQucGRmEwJwdDAuFihodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNfZW4ucGRmEwJlbjAVBggrBgEFBQcLAjAJBgcEAIvs
SQEBMBUGCCSGAQUFBwsCMAKGBwQAi+xjAQIwDQYJKoZIhvcNAQENBQADggIBACHUG1CXS1SNDV6Z
YlzoVoxk3LaOLrGoS12X33snN8eaHQ78UyjMlmul6xBfC9qte0T0wS5apug3UGpg2Xir983tPHea
weu43sx1fkdpPnltDm/KcwwGxb0/LvrArl4FTlvGRmHD2dmwBs2G7Qgxyvh38nsCzuKEA4ySuMPL
6XOCuoXxAfeM9S1kVikHzCUcwamLC9k4+2+KdusJDXvRMlWcpgHjkfCZqb+ELpLOkVQ7hdRPPJn
5isQFbU6/Gbc/01THQvaNPRS948ITi6IMSwOHHI8BXvSF0k/XBodJXv/C3VhZoxivMtvX1e4jyhO
E9y7G8kSjJd5ztv6JIG+Tr9YP04bOH13C0yYvgr8Wrpx26o+9N5sS54OQ3/VHw6+yU67cBAU/JUk
FbFe3FqU+i6s5oXnRxnrMQPNKAx7+Vuwe9V5c6iM7LiHMbCkgBeQq67YYiuQJ73+Pc/1OJOR/r3/
GtoS+q3xJYKSMHyLqwUFO4gJhLPm8DYSXrWymqEzQ1extyCMO73v1o/UVsKabFAG1XHgqULXsiK
XoidcAC6H4zkQ95NmVy6BI2ws3UVH6/Nz9r2pH9VXtiRLr1CjCq+k8CuGFS6COQWtqdylb0FwmtA
s81cd88W7I1IXWyF8mrxu55zf0qHxsTwFxyB57kCk4km92MalqzuOQYZ0LzW

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA512withRSA*

Issuer CN:	*DIGITALSIGN QUALIFIED CA G1*
Issuer O:	*DigitalSign Certificadora Digital*
Issuer C:	*PT*
Subject CN:	*JEROEN ARNOLD L RATHÉ*
Subject OU:	*RemoteQSCDManagement*
Subject GIVEN NAME:	*JEROEN ARNOLD L*
Subject SURNAME:	*RATHÉ*
Subject E:	*jeroen.rathe@ec.europa.eu*
Subject OU:	*Entitlement - EC STATUTORY STAFF*
Subject O:	*EUROPEAN COMMISSION*
Subject 2.5.4.97:	*LEIXG-254900ZNYA1FLUQ9U393*
Subject OU:	*Certificate Profile - Qualified Certificate - Member*
Subject C:	*BE*
Valid from:	*Fri Apr 21 17:59:43 CEST 2023*
Valid to:	*Mon Apr 20 17:59:43 CEST 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E0:0B:7B:B8:F7:76:FC:69:9A:96:0B:EC:1D:7F:4F:B5:FC:82:C6:FD:EF:97:61:C1:D0:88:DC:42:2F:49:02:54:4A:3E:B1:1B:7D:CF:9E:6C:5F:6C:07:9A:89:FF:69:7B:22:4B:8B:70:7E:A9:3D:01:0C:65:5A:92:F2:5E:E6:5A:DE:34:6B:06:22:39:E4:17:6A:B6:68:7E:DB:EA:E8:57:40:2E:3A:11:E1:BA:9C:00:28:EE:76:6C:FF:B2:21:25:3C:1B:8A:FE:83:E3:73:61:43:30:34:20:CC:F6:7B:E3:D0:04:B1:16:25:6A:45:5F:A8:81:4E:6D:5A:66:91:27:BB:1A:CD:25:DA:1B:DB:23:B1:2D:F5:49:98:A5:B3:28:EF:30:7E:F6:8E:D6:DE:42:26:04:99:D7:DC:D0:62:9A:D8:29:C9:F6:F7:31:4B:FF:B5:86:DF:72:30:28:87:FC:EC:D3:65:73:8F:86:DF:6F:F1:D5:57:C7:64:D5:D6:96:5A:0C:1F:F5:04:8F:2A:3C:67:B0:D9:84:4B:ED:63:C6:9F:61:A7:36:6D:5D:9B:B1:F9:BC:BD:E5:E6:9C:F9:02:7F:66:41:1E:22:BB:5B:A3:D9:60:0B:8B:EF:41:CD:AB:B1:2F:24:27:84:20:8C:59:AC:08:A1:F6:8D:AE:BB:9D:02:03:01:00:01*
Basic Constraints	*IsCA: false*
Authority Key Identifier	*73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*
Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*jeroen.rathe@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*

CRL Distribution Points *https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*

Subject Key Identifier *1B:EF:6E:01:67:39:13:6D:D4:3C:1B:A2:1A:C6:F2:28:2B:A9:60:B9*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_QcSSCD

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D3:23:8E:D2:84:DC:47:8F:86:2C:28:5B:00:5F:72:E9:BE:61:E0:76:D0:77:AE:C5:13:DA:C9:A2:BF:B6:93:41*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *212676479325594043390357602242635120 27*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG7zCCBNegAwIBAgIQEAAAAAAAnuXHXttK9Tyf2zANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQG
EwJCRTERMA8GA1UEBxMIQnJ1c3NlbHMxHDAaBgNVBAoTE0NlcnRpcG9zdCBOLlYuL1MuQS4xEzAR
BgNVBAMTCkNpdGl6ZW4gQ0ExDzANBgNVBAUTBjIwMTgwMzAeFw0xODA2MDEyMjA0MTlaFw0yODA1
MzAyMzU5NTlaMHAxCzAJBgNVBAYTAkJFMSMwIQYDVQQDExpQYXRyaWNrIEtyZW1lciAoU2lnbmF0
dXJlKTEPMA0GA1UEBBMGS3JlbWVyMRUwEwYDVQQqEwxQYXRyaWNrIEplYW4xFDA5BgNVBAUTCzcy
MDIwMzI5OTcwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr7g7VriDY4as3R4LPOg7
uPH5inHzaVMOwFb/8YOW+9lVMHz/V5djAzeTKvhLG554Pk6Kd2E+h18FIRonp70Gv2+ijtkPk7ZQ
kfezOycuAbLXiNx257fc5GG9LGJafDJg8gTQuQm1aDVLDQ653mqR5tAO+gEf6vs4zRESL3MkYXAU
q+S/WocEaGplheNVAF3iP5kvEe3LvUJF/xXHWf4aMvqGK6kXGseaTcn9hgTbceuW2PAiEr+eDTNc
zkwGBDFXwzmnGFPMRez3ONk/jIKhha8TylDSfl/MX3ODt0dU3jvJEKPIfUJixBPehxMJMwWxTjFb
Nu/CK7tJ8qT2i1S4VQIDAQABo4ICjzCCAoswHwYDVR0jBBgwFoAU2TQhPjpCJW3hu7++R0z4Aq3j
L1OwcwYIKwYBBQUHAQEEZzBlMDkGCCsGAQUFBzAChi1odHRwOi8vY2VydHMuZWlkLmJlbGdpdW0u
YmUvY2l0aXplbjlwMTgwMy5jcnQwKAYIKwYBBQUHMAGGHGh0dHA6Ly9vY3NwLmVpZC5iZWxnaXVt
LmJlLzlwggEjBgNVHSAEggEaMIIBFjCCAQcGB2A4DAEBAgEwgfswLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMlHKBggrBgEFBQcCAjCBvQyBukdlYnj1aWsgb25k
ZXJ3b3JwZW4gYWFuIGFhbnNwcmFrZWxpamtoZWlkc2JlcGVya2luZ2VuLCB6aWUgQ1BTIC0gVXNh
Z2Ugc291bWlzIMOgIGRlcyBsaW1pdGF0aW9ucyBkZSByZXNwb25zYWJpbGl0eiBlZvaXIgQ1BT
IC0gVmVyd2VuZHVuZyB1bnRlcmxpZWd0IEhhZnR1bmdzYmV2Y2hyw6Rua3VuZ2VuLCBnZW3DpHNz
IENQUzAJBgcEAIvsQAECMDkGA1UdHwQyMDAwLqAsoCqGKGh0dHA6Ly9jcmwuZWlkLmJlbGdpdW0u
YmUvZWlkY2lwMTgwMy5jcmwwDgYDVR0PAQH/BAQDAgZAMBMGA1UdJQQMMAoGCCsGAQUFBwMEMGwG
CCsGAQUFBwEDBGAwXjAIBgYEAI5GAQEwCAYGBACORgEEMDMGBgQAjkYBBTApMCcWIWh0dHBzOi8v
cmVwb3NpdG9yeS5laWQuYmVsZ2l1b55lZRMCZW4wEwYGBACORgEGMAkGBwQAjkYBBgEwDQYJKoZI
hvcNAQELBQADggIBACBY+OLhM7BryzXWkIDUh9UK1+cDVboPg+lN1Et1lAEoxV4y9zuXUWLco9t8
M5WfDcWFfDxyhatLedku2GurSJ1t8O/knDwLLyojE1r2Db9VrdG+jtST+j/TmJHAX3yNWjn/9dsj
iGQQuTJcce8ólzbGdUqjFTt5mGMm4zy4l/wKy6XiDKiZT8cFcOTevsl+l/vxiLiDnghOwTztVZh
mWExeHG9ypqMF1mIucHQ05fZre8mv3c7DF+VhqVsY9xLERK3Ffk4l6B5qRPyglmXqGzN5WiDISd
YeUf4XoZLXJBEP7/36r4mlnP2NWQ+c1ORjesuDAZ8tD/yhMvR4DVG95ESCjpTYv1wOmVB2lQrWnE
tygZli60HXfozo8uOekBnqWyDc1kuizZsYRfVNlwhCu7RsOq4zN8gkaeI0fejU5NtBf2/9A+rc9L
Qeu6AcdPauWmbxtJV93H46pFptsR8zXo+Jjn5m2P9QPZ3mvDkzldNTGLG+ukhN7/F2CCcagt/WoV
ZLg3qKC35WVcqeoSMEE/XeSrf3/mI/1OyfQm+tsfhTceOFDXuUgl3E86bR/f8Ur/bapwXpWpFxGl
pXLGaJXbzQGSTtyNEYrdENlh71I3OeYdw3xmzU2B3tbaWREOXtj2xjyW2tlv+vvHG6sloR1QklkG
MFfzsT7W5U6lLetv

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer SERIAL NUMBER: *201803*

Issuer CN: *Citizen CA*

Issuer O: *Certipost N.V./S.A.*

Issuer L: *Brussels*

Issuer C: *BE*

Subject SERIAL NUMBER: *72020329970*

Subject GIVEN NAME: *Patrick Jean*

Subject SURNAME: *Kremer*

Subject CN:	*Patrick Kremer (Signature)*
Subject C:	*BE*
Valid from:	*Sat Jun 02 00:04:19 CEST 2018*
Valid to:	*Wed May 31 01:59:59 CEST 2028*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AF:B8:3B:56:B8:83:63:86:AC:DD:1E:0B:3C:E8:3B:B8:F1:F9:8A:71:F3:69:53:0E:C0:56:FF:F1:83:96:FB:D2:15:30:7C:FF:57:97:49:03:37:93:2A:F8:4B:1B:94:B8:3E:4E:8A:77:61:3E:87:5F:05:95:1A:27:A7:BD:06:BF:6F:A2:8E:D9:0F:93:B6:50:91:F7:B3:D3:27:2E:01:B2:D7:88:DC:76:4B:B7:DC:E4:61:BD:2C:62:5A:7C:32:60:06:04:D0:B9:09:B5:68:35:4B:0D:0E:B9:DE:6A:91:E6:D0:0E:FA:01:1F:EA:FB:3B:CD:11:12:2F:73:24:61:70:14:AB:E4:BF:5A:87:04:68:6A:48:85:E3:55:00:5D:E2:3D:29:2F:11:ED:CB:BD:48:C5:FF:15:C7:58:5E:1A:32:FA:B6:2B:A9:17:1A:C7:9A:4D:C9:FD:86:04:DB:71:EB:96:DB:F0:22:12:BF:9E:0D:33:5C:CE:4C:06:04:31:57:C3:39:A7:18:53:CC:45:EC:F7:38:D9:3F:8C:82:A1:85:AF:13:CA:50:D2:7C:8F:CC:5F:73:83:B7:47:54:DE:3B:C9:10:A3:C8:7D:42:62:C4:13:DE:87:13:09:33:05:B1:4E:31:5B:36:EF:C2:2B:BB:49:F2:A4:F6:8B:54:B8:55:02:03:01:00:01*
Authority Key Identifier	*D9:34:21:3E:3A:42:25:6D:E1:BB:BF:BE:47:4C:F8:02:AD:E3:2F:54*
Authority Info Access	*http://certs.eid.belgium.be/citizen201803.crt* *http://ocsp.eid.belgium.be/2*
Certificate Policies	*Policy OID: 2.16.56.12.1.1.2.1* *CPS pointer: http://repository.eid.belgium.be* *CPS text: [Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage soumis à des limitations de responsabilité, voir CPS - Verwendung unterliegt Haftungsbeschränkungen, gemäss CPS]* *Policy OID: 0.4.0.194112.1.2*
CRL Distribution Points	*http://crl.eid.belgium.be/eidc201803.crl*
Extended Key Usage	*id_kp_emailProtection*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*D2:06:4F:DD:70:F6:98:2D:CC:51:6B:86:D9:D5:C5:6A:EA:93:94:17:C6:24:B2:E4:78:C0:B2:9D:E5:4F:84:74*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*416260670660158992857603279521251626757860879766*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIICDCCBfCgAwIBAgIUSOnGJxOHWc5N+Nk12eZPPCwr7ZYwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQwKAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmlyYWRvcmEgRtGlnaXRhbDEkMCIG
A1UEAwwbRElhSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTI0MDUwNjEyNDUxNloXDTI3MDUw
NjEyNDUxNlowggFZMQswCQYDVQQGEwJFUzE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWlcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
QTFGTVRQVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NjT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMTIwMAYJKoZIhvcNAQkBFiN2aWNlbnRlLmFuZHll
dS1uYXZhcnJvQGVjLmV1cm9wYS5ldTEXMBUGA1UEBAwOQU5EUkVVIE5BVkFSUk8xEDAOBgNVBCoM
B1ZJQ0VOVEUxHTAbBgNVBAsMFFJlbW90ZVFTQ0RNYW5hZ2VtZW50MR8wHQYDVQQDDBZWSUNFTlRF
IEFORFJFVSBOQVZBUjlPMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAveJV7goW3mvq
Jq2kMT0cnrkFAnT/lyzbgaHVxd5jEMHy6Ryol1Af4JTIOW5jC+6fsNzApFR1Tv3w8/WuSqjHTWfD
npqs20ijh979A5WwvfXuzcuUqeFFptdR/tjm/08TSTAD+CeA+rQo6K23B1xMYRwX/BNt/EL03Q/T
OQj5V4uV3Kyf0945yu5gOhmrMs/RZCZ8M+iahwTaVktf+ZvhocSsPt+a2OuPl8lpTU+xlWAXWuQ+
27Q7zzD0d6sqBdruDr16clFtZXWNRikm9g6pCOAOKG/myszeUuy++TPtQnI3+OQlTuyDXsz9lNKb
oQCF25NmfRoe8xcx02t5/2UgPwlDAQAB o4ICyjCCArowDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW
gBRz5fFAHBQEfjoSf/ovzVxnlxjpFDCBhgYIKwYBBQUHAQEEejB4MEYGCCsGAQUFBzAChjpodHRw
czovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdlVEFMU0lHTIFVQUxjRkIFRENBRzEucDdiMC4G
CCsGAQUFBzABhjodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMC4GA1UdEQQnMCWB
I3ZpY2VudGUuYW5kcnV1LWShdmFycm9AZWMuZXVyb3BhLmV1MFBGA1UdIARYMFYwNwYLKwYBBAGB
x3wEAQEwKDAmBggrBgEFBQcCARYaaHR0cHM6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwEAYOKwYBBAGB
x3wEAgEBAQQwCQYHBACL7EABAjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwSwYDVR0f
BEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFM
5UZjRURQUcxLmNybDAdBgNVHQ4EFgQUjueweY4Pl0KGjetMh84vTaEnxQcwDgYQVR0PAQH/BAQD
AgZAMIHTBggrBgEFBQcBAw5BxjCBwzAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcE
AI5GAQYBMGoGBgQAjkYBBTBgMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19w
dC5wZGYTAnB0MC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19lbi5wZGYTAmVu
MBUGCCsGAQUFBwsCMAkGBwQAi+xJAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjAN8gkqhkiG9w0B
AQ0FAAOCAgEAHBjW4N8NKNCJot414m/L76pB/15LKiGDi1/2V7MHe8u2GcpIR1ijESrSEhhwUAW
1hwDIK9xJcj/hdDUMIQcKScSjlCqTCb0Yk39yj/gfOYaN/3fgw8Pjh9k++3Ox7KnvY3R/foFvGjl
yiuqaai/JgBmc4qDBHSlDyo5gRw6v70osRPDR5sJs4Xh3FOjn9Y0JZPLF/skYtLrNVysL/4A4DbA
xB2Dcj5MpoIegh/fnJ5s2BOVq2Xq8ADpejoLFYbtlbP7NwsGgew2wKiDW963MlJL/Xa2AqcPVE/U
nXFkIBCwZH+covxSEQH2iVcF8cEDHBiYHGERaSmL/uHK/F8soDQ9VQwtKNxsIKAWsQHTYcKfEgV
uweyLj7TsCmh6T4pIHqaNDqWvrgEIo0ZwuBmfXVEd+JMSzSgIcJ2bPR2KNoJ14MO4FFYdAAnVIfd
hipErsK6R23hlto7b3XKiMRUt9xrvPUjuEJdGI5hPm9CqGK1GxlRoKLewyX7A+OIcPMPu1KfuuUT
Un+3hLJjZO5H9k4uVMJ/fOhwzc2VhRpyvNjfmFZksFvseFGvMI5EWIqp3JCo0ltkOBG59uIBwg/9
9YOpT6LW9cviTzKIwDtHmQrIgYLa+lCYwWdGhIidXynvLpWiVRZjvYrPIGpzQCRcw9Vzi8zT7nks
j7QF9v88kto=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer CN: *DIGITALSIGN QUALIFIED CA G1*

Issuer O: *DigitalSign Certificadora Digital*

Issuer C: *PT*

Subject CN: *VICENTE ANDREU NAVARRO*

Subject OU: *RemoteQSCDManagement*

Subject GIVEN NAME: *VICENTE*

Subject SURNAME: *ANDREU NAVARRO*

Subject E: *vicente.andreu-navarro@ec.europa.eu*

Subject OU: *Entitlement - EC STATUTORY STAFF*

Subject O: *EUROPEAN COMMISSION*

Subject 2.5.4.97: *LEIXG-254900ZNYA1FLUQ9U393*

Subject OU: *Certificate Profile - Qualified Certificate - Member*

Subject C: *ES*

Valid from: *Mon May 06 14:45:16 CEST 2024*

Valid to: *Thu May 06 14:45:16 CEST 2027*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BD:E2:55:EE:0A:16:DE:6B:EA:26:AD:A4:31:3D:1C:9E:B9:05:02:74:FF:97:2C
:DB:81:A1:D5:BD:DE:63:10:C1:F2:E9:1C:A8:23:50:1F:E0:94:E5:39:64:A3:0B:EE:9F:B0:DC:C0:A4:54:75:4E:FD:F0:F3:F5:AE:4A:08:C7:4D:67:C3:9E:9A:AC:DB:48:B9:87:DE:FD:03:95:B0:
BD:F5:EE:CD:CB:94:A9:E1:45:A6:D7:51:FE:D2:66:FF:4F:13:B1:30:03:F8:27:80:FA:B4:28:E8:AD:B7:07:5C:4C:61:1C:17:FC:13:6D:FC:42:F4:DD:0F:D3:39:08:F9:57:8B:95:DC:AC:9F:D3:D
E:39:CA:EE:60:3A:19:AB:32:CF:D1:64:26:7C:33:E8:9A:87:04:DA:56:4B:5F:F9:9B:E1:A1:C4:AC:3E:DF:9A:DB:EB:8F:23:C2:29:4D:4F:B1:21:60:17:5A:E4:3E:DB:B4:3B:CF:30:F4:77:AB:2A:
05:DA:EE:0E:BD:7A:72:51:6D:65:75:8D:46:29:26:F6:AE:A9:08:E0:0E:28:6F:E6:CA:CC:DE:52:EC:BE:F9:33:ED:42:72:37:F8:E4:25:4E:EC:83:5E:CC:FD:50:D2:9B:A1:00:85:D9:23:66:7D:1
A:1E:07:17:31:D3:6B:52:FF:35:20:3F:02:03:01:00:01
```


Basic Constraints *IsCA: false*

Authority Key Identifier *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

Authority Info Access	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b* *https://qca-g1.digitalsign.pt/ocsp*
Subject Alternative Name	*vicente.andreu-navarro@ec.europa.eu*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.25596.4.1.1* *CPS pointer: https://pki.digitalsign.pt* *Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4* *Policy OID: 0.4.0.194112.1.2*
Extended Key Usage	*id_kp_clientAuth*
CRL Distribution Points	*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*
Subject Key Identifier	*8E:E7:B0:79:8E:0F:23:42:86:8D:EB:4C:87:CE:2F:4E:C1:27:C5:07*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*DF:7E:29:36:0C:34:B2:B8:D6:D5:F4:03:25:C1:D4:D1:2C:99:22:CE:CD:33:B7:40:76:74:A7:4B:2B:3C:A1:E5*
TSL Type	*http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists*
Scheme Territory	*EU*
Mime Type	*application/vnd.etsi.tsl+xml*

Scheme Operator Name

Name	*[en]*	*European Commission*

Scheme Type Community Rules

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists*

List Issue Date Time

2025-06-12T11:57:48Z

Next Update

date Time *2025-12-12T12:57:48Z*

Distribution Points

URI *https://sr.riik.ee/tsl/estonian-tsl.xml*

1 - TSP: SK ID Solutions AS

TSP Name

Name	*[en]*	*SK ID Solutions AS*

TSP Trade Name

Name	*[en]*	*VATEE-100687640*
Name	*[en]*	*SK ID Solutions AS*
Name	*[en]*	*AS Sertifitseerimiskeskus*
Name	*[en]*	*ESTEID*
Name	*[en]*	*SK*

PostalAddress

Street Address	*[en]*	*Pärnu mnt 141*
Locality	*[en]*	*Tallinn*
Postal Code	*[en]*	*11314*
Country Name	*[en]*	*EE*

ElectronicAddress

URI	*[en]*	*mailto:info@sk.ee*
URI	*[en]*	*https://www.sk.ee/en*

TSP Information URI

URI	*[en]*	*https://www.sk.ee/en/repository/*
URI	*[et]*	*https://www.sk.ee/repositoorium/*

1.1 - Service (withdrawn): ESTEID-SK

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *ESTEID-SK*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1011113090*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFAjCCA+ggAwIBAgIEPERcgjANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxC2AJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWla2Vza3V2MRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTAyMDExNTE2NDQ1MFoXDTEyMDExMzE2NDQ1MFowfDEYMBYGCSqG
SIb3DQEJARYJcGtpQHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVy
aW1pc2tlc2t1czEPMA0GA1UECxMGRVNURUlEMQ0wCAYDVQQEEwExMRIwEAYDVQQDEwlFU1RFSUQt
U0swggEiMA0GCSqGSIb3DQEBAQUAA4IBDwA4wggEKAoIBAQC1eZO5NVo3zbwA8eFVCrrbe2QKvPDB
7LUDPvzCqw7U2sC+IwEOdjjpJRF4lxFs+f8yC1bP+rgtWzrKhhJ2owfSAlZMbly/OFjfLqOcyyi
7qdfA/66u+69u/DY9tW5fqW93D73v5WNcNolemCTydh9IFkQvMihWKH7LblBzCHa4W6qUcBZ7QsB
gYpQS9n9fGjt5D2wCDeq0pF1Zy72G3CQFrpuR/aPG28tv9r+C7oqncapbj7xlOa77Fm3o07M/9a
arq/m1oHEp9CxYrH9nmD3kyMe8yxw5v02MTMmAcxOm83z504oXSDTALG5qDFZNPjlaNPno7j8FuG
rI3vV8z3AgMBAAGjggGpMIIBpTAMBgNVHRMEBTADAQH/MA4GA1UdDwEB/wQEAwIB5jCCARYGA1Ud
IASCAQ0wggEJMIIBBQYKKwYBBAHOHwEBATCB9jCB0AYIKwYBBQUHAgIwgcMegcAAUwBlAGUAIABz
AGUAcgB0AGkAZgBpAGsAYQBhAHQAIABvAG4AIAB2AOQAbABqAGEAcwB0AGEAdAB1AGQAIABBAFMA
LQBpAHMAIABTAGUAcgB0AGkAZgBpAHQAcwBlAGUAcgBpAG0AaQBzAGsAZQBzAGsAdQBzACAAYQBs
AGEAbQAtAFMASwAgAHMAZQByAHQAaQBmAGkAawBhAGEAdABpAGQAZQAgAGsAaQBuAG4AaQB0AGEA
bQBpAHMAZQBrAHMwIQYIKwYBBQUHAgEWFWh0dHA6Ly93d3cuc2suZWUvY3BzLzArBgNVHR8EJDAi
MCCgHgAchhpodHRwOi8vd3d3LnNrLmVlL2p1dXIvY3JsL2AfBgNVHSMEGDAWgBQEqnpHo+5JrxrP
CkCnGD9v7+I9vjAdBgNVHQ4EFgQUeBe1BfmzWM1ZjN5nXkQGTHWGaV0wDOYJKoZIhvcNAQEFBQAD
ggEBAFisMHag4Fkrxmzw38rHYh5Ia5JGxjtWfPpag9pBtQNZHzY8j97xfPl15haE9Ah3u1WC+bs
U2SndVSUGaZ0gKafMxDOy2DUw3B84ymbNRiAFSWty+aKrMCjtdlPktbSQmxNSJAX9vVtM4Y2ory+
dtAQ7g11GKHJ+l8BDUpOJA+l8hvS2l4K5whWDHCSqlplMiHPIKgBVArFRNzAq6dquMY+kS3e2PL+
PM4GdDW5lRHR/6KUy0BHP2gX/BO4mYQ3BH2BHlmUcINras0HISnV/pt6hlkgd1PsFt3rtEoIAWP4
DWBmc4zAYQJ50cEwFM3292CXSGIQIm3a1cMugF5Q/k=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Juur-SK*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject CN: *ESTEID-SK*

Subject SURNAME: *1*

Subject OU: *ESTEID*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

Valid from: *Tue Jan 15 17:44:50 CET 2002*

Valid to: *Fri Jan 13 17:44:50 CET 2012*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8B:79:93:B9:35:5A:37:CD:BC:00:F1:E1:55:0A:BA:DB:79:94:0A:BC:F0:C1:EC
:85:03:3E:FC:C2:AB:0E:D4:DA:C0:BE:23:01:0E:76:38:E9:25:11:78:97:11:6C:F9:FF:32:0B:56:CF:FA:BA:AD:5B:3A:CA:86:12:76:A3:07:D2:02:52:19:31:B9:72:FC:E1:63:7C:BA:8E:73:2C:A
2:EE:A7:5F:03:FE:BA:BB:EE:BD:BB:F0:D8:F6:D5:B9:7E:A5:BD:DC:3E:F7:BF:95:8D:70:DA:08:7A:60:93:C9:D8:7D:20:59:10:BC:C8:A1:58:A1:FB:2D:B9:41:CC:21:DA:E1:6E:AA:51:C0:59:E
D:0B:01:81:8A:50:4B:D9:FD:7C:62:6D:E4:3D:B0:08:37:AA:D2:91:75:67:2E:F6:1B:70:90:16:BA:6E:47:F6:8F:1B:6F:2D:BF:DA:FE:0B:BA:2A:9D:C6:A9:6E:22:7B:C4:83:9A:EF:B1:66:DE:8
D:3B:33:FF:5A:6A:BA:BF:9B:5A:07:12:9F:42:C5:88:87:F6:79:83:DE:4C:8C:7B:CC:B1:C3:9B:F4:D8:C4:CC:98:07:31:3A:6F:37:CF:93:B8:A1:74:83:4C:02:C6:E6:00:DF:64:D3:E3:25:A3:4F:
9E:8E:C9:F0:5B:86:AC:8D:EF:57:CC:F7:02:03:01:00:01
```


Basic Constraints *IsCA: true*

Certificate Policies	*Policy OID: 1.3.6.1.4.1.10015.1.1.1* *CPS text: [See sertifikaat on väljastatud AS-is Sertifitseerimiskeskus alam-SK sertifikaatide kinnitamiseks]* *CPS pointer: http://www.sk.ee/cps/*
CRL Distribution Points	*http://www.sk.ee/juur/crl/*
Authority Key Identifier	*04:AA:7A:47:A3:E4:89:AF:1A:CF:0A:40:A7:18:3F:6F:EF:E9:7D:BE*
Subject Key Identifier	*78:17:B5:05:F9:B3:58:CD:59:8C:DE:67:5E:44:06:4C:75:86:69:5D*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*0B:7A:9D:B6:0D:95:B0:6A:8F:4C:FC:0A:9C:1D:7D:92:EC:8D:45:55:1C:56:B6:79:58:79:29:C9:9B:20:C5:73*

X509SubjectName

Subject CN:	*ESTEID-SK*
Subject SURNAME:	*1*
Subject OU:	*ESTEID*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Subject E:	*pki@sk.ee*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*

Status Starting Time

2017-06-30T22:00:00Z

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.1.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.1.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.1.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK*

Service digital identities

X509SubjectName

Subject CN:	*ESTEID-SK*
Subject SURNAME:	*1*
Subject OU:	*ESTEID*

Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Subject E:	*pki@sk.ee*

X509SKI

X509 SK I	*eBe1BfmzWM1ZjN5nXkQGTHWGaV0=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

1.1.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.1.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name [en] *ESTEID-SK: Qualified certificates for Estonian ID-card*

Service digital identities

X509SubjectName

Subject CN: *ESTEID-SK*

Subject SURNAME: *1*

Subject OU: *ESTEID*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *eBe1BfmzWM1ZjN5nXkQGTHWGaV0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2002-01-15T17:44:50Z*

1.1.5.4 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage [digitalSignature] *true*

Key Usage [nonRepudiation] *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.1.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.2 - Service (withdrawn): ESTEID-SK 2007

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *ESTEID-SK 2007*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1167826957*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIERZugDTANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Va3VzMRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTA3MDEwMzEyMjIzN1oXDTE2MDgyNjE0MjMwMVowWzELMAkGA1UE
BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZmI0c2VlcmltaXNrZXNrdXMxDzANBgNVBAsTBkVTVEVJ
RDEXMBUGA1UEAxMORVNURUlELVNLIDIwMDcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDtWp2jLCsA7K9AxoPDOL0geM1GoR0Q6wSUlCCJYyFkUMboEMxp5zFB6tlb0ySlHEU6Fs+tiA4Q
r5qwaw0uNk4BXv1IkoOr6DUc+2O+AQd5jB6AOafrfZ1KG5IvDEep3DjPykkk2MPxIz7dZx7XUEr
/kdUWI9cDIkFWic7y9oTBY9JaV6Ixm08kweZ/qTw5PU8/bTvZCE0ygvBXU4TDS2FpUJ/+JTzM2oc
Wa3QjFQv2Sir6LBvgNY3du/m+WLABq0dgN18R4nhFtmaVepqAeUuEi8eRBI6yLTSmMwYCY46LsK5
CdjTCZSZv934FtNuyY6Ph9nCXjAgNAY+GfNJfdMXAgMBAAGjgZwwgZkwEgYDVR0TAQH/BAgwBgEB
/wIBADAOBgNVHQ8BAf8EBAMCAf4wMwYDVR0fBCwwKjAooCagIlYiaHR0cDovL3d3dy5zay5lZS9j
cmxzL2p1dXIvY3JsLmNybDAfBgNVHSMEGDAWgBQEqnpHo+SjrxrPCkCnGD9v7+l9vjAdBgNVHQ4E
FgQUSAbevoyHV5WAeGP6nCMrK6A6GHUwDQYJKoZIhvcNAQEFBQADggEBACO6SJrjN5WZuiLSMy/t
SmT/w3dd/KPErSAdUIJYkC7hOIauW7jZ3VNgNUMHSIkUoP8AviEMjGA4IkT61YScpJAdmgI8Y80H
FdZV5CsThhddoIdZ3cZjSI4NZm1VkSduTjpy5ALxKL3ZElPrepQDvNEaV1WSpI5+u/vMakUWJSPc
8BK9O2av1e9ResKyPjidqrlksHFjN5+Yt8Ouw7F10MHaPPzMiwoa0DYTVsIKJncPTQmvdJG8M0DD
ToiiNPQuUly5d1CA75Wtjs+ylLGZXpOfbdoQhE7G4pbZaF1s69jKp+zc0ZT4g2OoKfI2TilX9qeGJ
MxkOENcd1DDqYVfePmo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Juur-SK*

Issuer O:	*AS Sertifitseerimiskeskus*
Issuer C:	*EE*
Issuer E:	*pki@sk.ee*
Subject CN:	*ESTEID-SK 2007*
Subject OU:	*ESTEID*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Wed Jan 03 13:22:37 CET 2007*
Valid to:	*Fri Aug 26 16:23:01 CEST 2016*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:ED:5A:9D:A3:2C:2B:00:EC:AF:40:C6:83:C3:38:BD:20:78:CD:46:A1:1D:10:EB:04:94:20:20:89:63:21:64:50:C6:EB:10:CC:69:4B:31:41:EA:D9:5B:D3:24:A5:1C:45:3A:16:CF:AD:8C:0E:10:AD:2A:B0:6B:0D:2E:36:4E:01:5E:FD:65:92:83:AB:E8:35:1C:FB:6D:3E:01:07:79:8C:1E:80:D1:AB:6B:96:D6:75:5C:6E:48:BC:31:1E:A7:70:C9:3F:29:24:93:63:0F:C5:4C:FB:75:9C:7B:5D:41:2B:FE:47:54:58:8F:5C:0C:89:05:5A:27:3B:CB:DA:13:05:8F:49:69:5E:A5:C6:6D:3C:93:07:99:FE:A4:F0:E4:F5:3C:FD:B4:EF:64:21:34:CA:0B:C1:5D:4E:13:0D:2D:B5:A5:42:7F:FA:34:F3:33:6A:1C:59:AD:D0:8C:54:2F:D9:28:AB:E8:B0:6F:80:D6:37:76:EF:E6:F9:62:C0:06:AD:1D:80:DD:7C:47:89:E1:16:D9:9A:55:6A:6A:01:E5:2E:12:2F:1E:44:19:7A:C8:B4:D2:98:CC:18:09:8E:3A:2E:C2:B9:09:D8:D3:09:94:99:BF:DD:F8:16:D3:6E:C9:8E:8F:87:D9:C2:5C:90:20:34:06:3E:19:F3:49:7D:D3:17:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://www.sk.ee/crls/juur/crl.crl*
Authority Key Identifier	*04:AA:7A:47:A3:E4:89:AF:1A:CF:0A:40:A7:18:3F:6F:EF:E9:7D:BE*
Subject Key Identifier	*48:06:DE:BE:8C:87:57:95:80:78:63:FA:9C:23:2B:2B:A0:3A:18:75*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment - keyAgreement - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B1:14:C6:A2:F2:10:F8:B4:39:76:28:9C:AF:FD:70:F6:48:4F:BC:C6:1F:18:93:E5:D1:26:76:F4:C2:E5:80:5B*

X509SubjectName

Subject CN:	*ESTEID-SK 2007*
Subject OU:	*ESTEID*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2017-06-30T22:00:00Z

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.2.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.2.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK 2007*

Service digital identities

X509SubjectName

Subject CN: *ESTEID-SK 2007*

Subject OU: *ESTEID*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *SAbevoyHV5WAeGP6nCMrK6A6GHU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.2.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.2.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK 2007: Qualified certificates for Estonian ID-card, the residence permit card, the digital identity card, the digital identity card in form of the Mobile-ID*

Service digital identities

X509SubjectName

Subject CN: *ESTEID-SK 2007*

Subject OU: *ESTEID*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *SAbevoyHV5WAeGP6nCMrK6A6GHU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-01-03T13:22:37Z*

1.2.5.4 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.2.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.3 - Service (withdrawn): ESTEID qualified certificates for electronic signatures (ESTEID-SK 2011)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name	*[en]*	*ESTEID qualified certificates for electronic signatures (ESTEID-SK 2011)*
Name	*[et]*	*ESTEID kvalifitseeritud e-allkirjastamise sertifikaatide väljastamise teenus (ESTEID-SK 2011)*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*549271112310506669194903650496752069 25*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFBTCCA+2gAwIBAgIQKVKTqv2MxtRNgzCjwmRRDTANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUlgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMTQ1OVoXDTI0MDMxODEwMTQ1OVowZDELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxFzAVBgNVBAMMDkVTVEVlRC1TSyAyMDExMRgwFgYJKoZIhvcN
AQkBFglwa2lAc2suZWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCz6XksZh6r/aXc
Ne3kSpNMOqmQoAXUpzzcr4ZSaGZh/7JHlplvNl6tbW/lK7sAiRsb65KzMWROEauld66qbDPqa6
kU97C+AXGu7+DROXstjUOv6VlrHZVAnLmlOkycpWaxjM+EfQPZuDxEbkw96B3/fG69Zbp3s9y6WE
hwU5Y9IiQl8YTkGnNUxiQbON1BGQm+HVEsgTf22J6r6G3FsE07rnMNskNC3DjuLSCUKF4kH0rVG
VK9BdiCdFaZjHEykjwjlGzqnyxyRKe4Ybj6B9ABm95eSFgMBHtZEYU+q0VUlQGhAGAurOTXjWi1T
ssA4ZmnLGQZEI5GXMXtabp51AgMBAAGjggGqMIIBnDASBgNVHRMBAf8EBDADAQH/ApEAMA4GA1Ud
DwEB/wQEAwIBBjCB9gYDVR0gBIHuMIHrMIHoBgsrBgEEAc4fZAEBATCB2DCBsgYIKwYBBQUHAgIw
gaUegaIASwBhAHMAdQB0AGEAdABhAGsAcwBlACAAaQBzAGkAawB1AHQAdAD1AGUAbgBkAGEAdgBh
AGwAZQAgAGQAbwBrAHUAbQBlAG4AZABpAGwAZQAgAGsAYQBuAHQAYQB2AGEAdABlACAAcwBlAHIA
dABpAGYAaQBrAGEAYQB0AGkAZABlACAAdgDkAGwAagBhAHMAdABhAG0AaQBzAGUAawBzAC4wIQY1
KwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL0NQUzAdBgNVHQ4EFgQUe2ryVVBcuNl6CldBrvqi
Kz1bV3YwHwYDVR0jBBgwFoAUEvjaPupWHL/NBqzx8SXJqUvUFjkwPQYDVR0fBDYwNDAyoDCgLoYs
aHR0cDovL3d3dy5zay5lZS9yZXBvc2l0b3J5L2NybHMvZWVjY3JlYS5jcmwwDQYJKoZIhvcNAQEF
BQADggEBAKC4lN3FCZqVDlH05TNMgFrQOCGSnKhzojclRLoQ81BCOXTZI4qn7N74FHEnrAy6uNG7
SS5qANqSaPlL8dp63jg/L4qn4iWaB5q5GGJOV07SnTH57gUrqChGClnUeHxiZbL13PkP37Lnc+TK
I1SKfgtn5FbH5cqrhvbA/VF3Yzlimu+L7EVohW9HKxZ//z8kDn6ieiPFfZdTOov/0eXVLlxqklyb
UuS6LYRRDiqOupgBKQBTwNbC8x0UHX00HokW+dCVcQvsUbv4xLhRq/MvyTthE+RdbkrV0JuzbfZv
ADfj75nA3+ZAzFY55ZpMOjZ9p4rQVKpzQTkIrF0m6mkdcEo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Fri Mar 18 11:14:59 CET 2011*

Valid to: *Mon Mar 18 11:14:59 CET 2024*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:E9:7C:6C:66:1E:AB:FD:A5:DC:35:ED:E4:4A:93:4C:3A:A9:90:A0:05:D4:A7
:3C:DC:AF:86:52:68:66:61:FF:B2:47:22:2A:65:BC:D8:BA:B5:B5:BF:94:AE:EC:02:24:6C:6F:AE:4A:CC:C5:91:38:46:AE:95:DE:BA:82:06:C3:3E:06:BA:91:4F:7B:0B:E0:17:1A:EE:FE:0D:13:9
7:B2:D8:D4:3A:FE:95:96:B1:D9:54:09:CB:98:83:A4:C9:CA:56:6B:18:CC:F8:47:D0:3D:9B:83:C4:46:E4:C3:DE:81:DF:F7:C6:EB:D6:5B:A7:7B:3D:CB:A5:84:87:05:39:63:D2:22:42:5F:18:4
E:41:A7:35:4C:62:75:06:CE:37:50:46:42:6F:87:54:4B:20:4D:FD:B6:27:AA:FA:18:71:6C:13:4E:EB:9C:C3:6C:90:D0:B7:0E:3B:8B:48:25:0A:17:89:07:D2:B5:46:54:AF:41:76:20:9D:15:A6:
63:1C:4C:A4:8F:08:C8:18:3A:A7:CB:1C:91:29:EE:18:6C:9E:81:F4:00:66:F7:97:92:16:03:01:1E:D6:44:61:4F:AA:D1:55:08:40:68:40:18:0B:AB:39:35:E3:5A:2D:53:B2:C0:38:DA:69:CB:1
9:06:44:23:91:97:31:7B:5A:6E:9E:75:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.100.1.1.1

CPS text: [Kasutatakse isikuttõendavale dokumendile kantavate sertifikaatide väljastamiseks.]

CPS pointer: https://www.sk.ee/CPS

Subject Key Identifier *7B:6A:F2:55:50:5C:B8:D9:7A:08:87:41:AE:FA:A2:2B:3D:5B:57:76*

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

CRL Distribution Points *http://www.sk.ee/repository/crls/eeccrca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:EC:80:8E:33:CC:A8:65:9E:AE:A8:16:70:D6:C7:DC:01:44:66:36:E1:F2:27:56:1B:63:07:B8:0B:A6:38:62*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2021-05-21T10:00:00Z

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.3.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.1*

Description *Certificate Policy for ID card and Digi-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.3*

Description *Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.3.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.1*

Description *Certificate Policy for ID card and Digi-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.3*

Description *Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.3.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*ESTEID qualified certificates for electronic signatures (ESTEID-SK 2011)*
Name	*[et]*	*ESTEID kvalifitseeritud e-allkirjastamise sertifikaatide väljastamise teenus (ESTEID-SK 2011)*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*ESTEID-SK 2011*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*e2ryVVBcuNl6CIdBrvqiKz1bV3Y=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2018-11-02T14:00:00Z*

1.3.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*

Policy Identifier:

Identifier	*1.3.6.1.4.1.10015.1.1*
Description	*Certificate Policy for ID card and Digi-ID*
Documentation Reference	*https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier	*1.3.6.1.4.1.10015.1.3*
Description	*Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.3.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.1*

Description *Certificate Policy for ID card and Digi-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.3*

Description *Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.3.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.3.5 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK 2011 qualified certificates for electronic signatures*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *e2ryVVBcuNl6CIdBrvqiKz1bV3Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.3.5.4 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.3.5.5 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.3.5.6 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.3.6 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK 2011: Qualified certificates for Estonian ID-card, the residence permit card, the digital identity card, the digital identity card in form of the Mobile-ID*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *e2ryVVBcuNl6CIdBrvqiKz1bV3Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-03-18T11:14:59Z*

1.3.6.7 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.3.6.8 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.4 - Service (granted): ESTEID qualified certificates for electronic signatures (ESTEID-SK 2015)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name	*[en]*	*ESTEID qualified certificates for electronic signatures (ESTEID-SK 2015)*
Name	*[et]*	*ESTEID kvalifitseeritud e-allkirjastamise sertifikaatide väljastamise teenus (ESTEID-SK 2015)*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*92090760538140121355861069916590054235*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIGcDCCBVigAwIBAgIQRUgJC4ec7yFWcqzT3mwbWzANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMCAXDTE1
MTIxNzEyMzg0M1oYDzIwMzAxMjE3MjM1OTU5WjBjMQswCQYDVQQGEwJFRTEiMCAGA1UECgwZQVMg
U2VydGlmaXRzZWVyaW1pc2tlc2t1czEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMM
DkVTVEVJRC1TSyAyMDE1MlCjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAOoH61NDxbdW9
k8nLA1qGaL4B7vydod2EwpSTBZB3wEtJCLdkpEs58pXfFiRqwDVsgGGbu+Q99trIb5LI7yi7rI
kRov5NftBdSNPSU5rAhYPQhvZZOgOwRaHa5Ey+BaLJHmLgYQS9hQvQsCYyws+xVvNFUpK0pGD64i
ycqdMuBl/nWq3fLuZppwBh0VFltm4nhr/1S0R9TRJpqFUGbGr4OK/DwebQ5PjhdS40gCUNwmC7fP
Q4vIH+x+TCk2aG+u3MoAz0lrpVWqiwzG/vxreuPPAkgXeFCeYf6fXLsGz4WivsZFbph2pMjELu6s
ItIBXfAG3fGvI43t91VXicyzR/6T5dsB+zFsW1sHV+1QNPr+qzqDxCH2cmuqoqZNfIlq+buob3eA8e
e+XpJKJQr+1qGrmhggjvAhc7m6cU4x/QfxwRYhIVNhjF+sKVThkQhbJ9XxUkk3c18wymwL1mpDD0
PIGJqlssMeiuJ4IzagFBgESGNDUd4icm0hQT8CmQeUm1GbWeBYsegPhMQX97QFBLXJLVy2SCyoAz
7Bq1qA43++EcibN+yBc1nQs2Zoq8ck9MK0bCxDMeUkQUz6VeQGp69ImOQrsw46qTz0mtdQrMSbnk
XCuLan5dPm284J9HmaqIYi6j6KLcZ2NkUnDQFesBVIMEm+fHa2iR6lnAFY206UECAwEAAaOCAgow
ggIGMB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fElyalL1BSZMB0GA1UdDgQWBBSzq4i8mdVipIUq
CM20HXI7g3jHUTAOBgNVHQ8BAf8EBAMCAQYwdwYDVR0gBHAwbjAIBgYEAI96AQIwCQYHBACL7EAB
AjAwBgkrBgEEAc4fAQEwIzAhBggrBgEFBQcCARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMAsGCSsG
AQQBzhBBAjALBgkrBgEEAc4fAQMwCwYJKwYBBAHOHwEEMBIGA1UdEwEB/wQIMAYBAfBCAQAwQQYD
VR0eBDowOKE2MASCAiiIMAqHCAAAAAAAAAAAMCKHIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAMCcGA1UdJQQgMB4GCCsGAQUFBwMJBggrBgEFBQcDAgYIKwYBBQUHAwQwfAYIKwYBBQUH
AQEEcDBuMCAGCCsGAQUFBzABhhRodHRwOi8vbzNzcC5zay5lZS9DQTBKBggrBgEFBQcwAoY+aHR0
cDovL3d3dy5zay5lZS9lZXI0cy9FRV9DZXI0aWZpY2F0aW9uX0NlbnRyZV95b290X0NBLmRlci5j
cnQwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovL3d3dy5zay5lZS9yZXBvc2l0b3l5L2NybHMvZWVj
Y3JjYS5jcmwwDQYJKoZIhvcNAQEMBQADggEBAHRWDGI3P00r2sOnlvLHKk9eE7X93eT+4e5TeaQs
OpE5zQRUTtshxN8Bnx2ToQ9rgi18q+MwXm2f0mrGakYYG0bix7ZgDQvCMD/kuRYmwLGdfsTXwh8K
uL6uSHF+UZTss6qG7mxCHG9YvebkN5Yj/rYRvZ9/uJ9rieByxw4wo7b19p22PXkAkXP5y3+qK/O
et98lqwI97kjhiS2zxFYRk+dXbazmoVHnozYKmsZaSUvoYNNh19tpS7BLdsgi9KpbvQLb5ywlMq9
ut3+b2Xvzq8yzmHMFtLlJ6Afu1jjpqD82BUAFcvi5vhnP8M7b974R18WCOpgNQvXDl+2/8ZINeU=

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject CN: *ESTEID-SK 2015*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Thu Dec 17 13:38:43 CET 2015*

Valid to: *Wed Dec 18 00:59:59 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:81:FA:D4:D0:F1:6D:D5:BD:93:C9:CB:03:5A:86:68:BE:01:EE:FC:9D:A1:D
D:84:C2:9F:D2:4C:16:41:DF:01:2D:20:90:8B:76:4A:44:B1:2F:29:5D:F1:62:46:AC:03:56:C8:06:19:BB:BE:43:DF:6D:AE:56:F9:2C:8E:F2:8B:BA:C8:91:1A:2F:E4:D7:ED:05:D4:8D:3D:25:3
9:AC:08:58:3D:08:6F:65:94:20:3B:04:5A:1D:AE:44:CB:E0:5A:2C:91:E6:2E:A6:10:4B:D8:50:BD:0B:02:63:2C:2C:FB:15:6F:34:55:29:2B:4A:46:0F:AE:22:C9:CA:9D:32:E0:65:FE:75:AA:DD
:F2:EE:66:9A:70:06:1D:15:16:5B:66:E2:78:6B:FF:54:B4:47:D4:D1:26:9A:85:50:66:C6:AF:83:8A:FC:3C:1E:6D:0E:4F:8E:17:52:E3:48:02:50:DC:26:0B:B7:CF:43:BB:C8:1F:EC:7E:4C:29:3
6:68:6F:AE:DC:CA:00:CF:42:2B:A5:55:AA:8B:0C:C6:FE:FC:6B:7A:E3:CF:02:48:17:78:50:9E:61:FE:9F:5C:BB:06:CF:85:A2:BE:C6:45:6E:98:76:A4:C8:C4:2E:EE:AC:96:D9:41:5D:F0:06:DD:
F1:AF:E3:7B:7D:D5:55:E2:73:2C:D1:FD:E4:F9:76:C0:7E:CC:5B:16:D6:C1:D5:FB:53:8D:3E:BF:AA:CE:00:F1:08:7D:9C:9A:EA:A8:64:D7:C8:22:AF:9B:BA:86:F7:78:0F:1E:7B:E5:E9:24:A2:5
0:AF:ED:6A:1A:B9:A1:82:08:EF:02:17:3B:9B:A7:14:E3:1F:D0:7F:1C:11:62:12:15:36:12:5F:FA:C2:95:4E:19:10:85:B2:7D:5F:1B:BA:93:77:35:F3:0C:A6:C0:BD:66:A4:30:F4:3C:81:89:AA:
5B:2C:31:E8:AE:27:82:33:6A:01:5B:80:44:86:34:35:1D:E2:27:26:D2:14:13:F0:29:90:79:49:85:19:B5:9E:05:BB:1E:A8:F8:4C:41:7F:7B:40:50:4B:5C:92:D5:CB:64:82:CA:80:33:EC:1A:B5
:A8:0E:37:FB:E1:1C:89:B3:7E:C8:17:35:9D:0B:36:66:8A:BC:72:4F:4C:2B:46:C2:C4:33:1E:52:44:14:CF:A5:5E:40:6A:7A:F4:89:8E:42:BB:30:E3:AA:93:CF:49:AD:75:0A:CC:49:B9:E4:5C:2
B:8B:6A:7E:5D:3E:6D:BC:E0:9F:47:99:AA:A2:62:2E:A3:E8:A2:DC:67:63:64:52:70:D0:15:EB:01:56:53:04:9B:E7:C7:6B:68:91:EA:59:C0:15:86:74:E9:41:02:03:01:00:01

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

Subject Key Identifier *B3:AB:88:BC:99:D5:62:A4:85:2A:08:CD:B4:1D:72:3B:83:72:47:51*

Certificate Policies

Policy OID: 0.4.0.2042.1.2

Policy OID: 0.4.0.194112.1.2

Policy OID: 1.3.6.1.4.1.10015.1.1

CPS pointer: https://www.sk.ee/CPS

Policy OID: 1.3.6.1.4.1.10015.1.2

Policy OID: 1.3.6.1.4.1.10015.1.3

Policy OID: 1.3.6.1.4.1.10015.1.4

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage	*id_kp_clientAuth - id_kp_OCSPSigning*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*74:D9:92:D3:91:0B:CF:7E:34:B8:B5:CD:28:F9:1E:AE:B4:F4:1F:3D:A6:39:4D:78:B8:C4:36:72:D4:3F:4F:0F*

X509SubjectName

Subject CN:	*ESTEID-SK 2015*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2018-11-02T14:00:00Z

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*

Policy Identifier:

Identifier	*1.3.6.1.4.1.10015.1.1*
Description	*Certificate Policy for ID card and Digi-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.3*

Description *Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.1*

Description *Certificate Policy for ID card and Digi-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Policy Identifier:

Identifier *1.3.6.1.4.1.10015.1.3*

Description *Certificate Policy for the digital identity card in form of the Mobile-ID*

Documentation Reference *https://sk.ee/en/repository/CP/*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.4.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*ESTEID-SK 2015 qualified certificates for electronic signatures*

Service digital identities

X509SubjectName

Subject CN:	*ESTEID-SK 2015*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*s6uIvJnVYqSFKgjNtB1yO4NyR1E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.4.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.4.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.4.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.4.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ESTEID-SK 2015: Qualified certificates for Estonian ID-card, the residence permit card, the digital identity card, the digital identity card in form of the Mobile-ID*

Service digital identities

X509SubjectName

Subject CN: *ESTEID-SK 2015*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *s6uIvJnVYqSFKgjNtB1yO4NyR1E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2015-12-17T12:38:00Z*

1.4.5.4 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.4.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.5 - Service (granted): ESTEID qualified certificates for electronic signatures (ESTEID2018)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *ESTEID qualified certificates for electronic signatures (ESTEID2018)*

Name *[et]* *ESTEID kvalifitseeritud e-allkirjastamise sertifikaatide väljastamise teenus (ESTEID2018)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *155893412819766287602132218565978641901*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFVzCCBLigAwIBAgIQdUf6rBR054tbo2bU/mZV7TAKBggqhkjOPQQDBDBaMQswCQYDVQQGEwJF
RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEV
MBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkyMDA5MjIyOFoXDTMzMDkwNTA5MTEwM1owWDEL
MAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIEIEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTlRSRUUt
MTA3NDcwMTMxEzARBgNVBAMMCkVTVEVJRDIwMTgwgZswEAYHKoZIzj0CAQYFK4EEACMDgYYABAHH
OBlv7UrRPYP1yHhOb7RAiYBDbtqynSVMqYdxnFrKHUXh6fKghvHuA1k2DSom1hE5kqhB5VspDem
bwWDJBOQWQGOI/0t3EtccLYjeM7F9xOPdzUbZalbpNRHpQgVBpFX0xpLTgW27MpIMhU8DHBWFpeA
aNX3eUpD4gC5cvhsK0RFEqOCAx0wggMZMB8GA1UdIwQYMBaAFH4pVuc0knhOd+FvLjMqmHHB/T5f
MB0GA1UdDgQWBBTZrHDbX36+lPig5L5HotA0rZoqEjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/
BAowBgEB/wIBADCCAc0GA1UdIASCAcQwggHAMAqGBgQAj3oBAjAJBgcEAIvsQAECMDIGCysGAQQB
g5EhAQEBMCMwIQYIKwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL0NQUzANBgsrBgEEAYORIQEB
AjANBgsrBgEEAYORIwEBATANBgsrBgEEAYORIQEBBTANBgsrBgEEAYORIQEBBjANBgsrBgEEAYOR
IQEBBzANBgsrBgEEAYORIQEBAzANBgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEBCDANBgsrBgEE
AYORIQEBCTANBgsrBgEEAYORIQEBCjANBgsrBgEEAYORIQEBC2ANBgsrBgEEAYORIQEBDDANBgsr
BgEEAYORIQEBDTANBgsrBgEEAYORIQEBDjANBgsrBgEEAYORIQEBDzANBgsrBgEEAYORIQEBEDAN
BgsrBgEEAYORIQEBETANBgsrBgEEAYORIQEBEjANBgsrBgEEAYORIQEBEzANBgsrBgEEAYORIQEB
FDANBgsrBgEEAYORfwEBAjANBgsrBgEEAYORfwEBAzANBgsrBgEEAYORfwEBBDANBgsrBgEEAYOR
fwEBBTANBgsrBgEEAYORfwEBBjAqBgNVHSUBAf8EIDAeBggrBgEFBQcDCQYIKwYBBQUHAwIGCCsG
AQUFBwMEMGoGCCsGAQUFBwEBBF4wXDApBggrBgEFBQcwAYYdaHR0cDovL2FpYS5zay5lZS9lZS1n
b3ZjYTlwMTgwLwYIKwYBBQUHMAKGI2h0dHA6Ly9jLnNrLmVlL0VFLUdvdkNBMjAxOC5kZXluY3J0
MBgGCCsGAQUFBwEDBAwwCjAIBgYEAI5GAQEwMAYDVR0fBCkwJzAloCOgIYYfaHR0cDovL2Muc2su
Zlk0UUtR292Q0EyMDE4LmNybDAKBggqhkjOPQQDBAOBjAAwgYgCQgDeuUY4HczUbFKS002HZ88g
cIgYdztHqgIENyTMtXE6dMBRnCbgUmhBCAA0mJSHbyFI8W9jkLISyurmkJM0hDE9KgICASOqA405
Ia5nKjTJPNsHQlMi7KZsIcTHOoBccx+54N8ZX1MgBozjmT59rZY2/OeE163BAwD0UdUQAnMPP6+
W3Vd

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withECDSA*

Issuer CN: *EE-GovCA2018*

Issuer 2.5.4.97: *NTREE-10747013*

Issuer O: *SK ID Solutions AS*

Issuer C: *EE*

Subject CN: *ESTEID2018*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

Valid from: *Thu Sep 20 11:22:28 CEST 2018*

Valid to: *Mon Sep 05 11:11:03 CEST 2033*

Public Key:


```
30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:01:C7:38:19:6F:ED:4A:D1:3D:83:F5:C8:78:4E:6F:B4:40:FD:80:43:6E:D8:32:9D:25:4C:A9:87:71:9C
:5A:CA:1D:45:E1:EA:D1:64:82:18:C7:B8:0D:64:D8:34:A8:9B:58:44:E6:4A:A1:07:95:6C:A4:37:A6:6F:05:83:24:13:90:59:01:8E:23:FD:2D:DC:4B:5C:70:B6:23:78:CE:C5:F7:13:8F:77:35:
1B:65:A2:1B:A4:D4:47:A5:08:15:06:91:57:D3:1A:4B:4E:05:B6:EC:CA:48:32:15:3C:0C:70:56:16:97:80:68:D5:F7:79:4A:43:E2:00:B9:72:F8:6C:2B:44:45:12
```


Authority Key Identifier *7E:29:56:E7:34:92:78:4E:77:E1:6F:2E:33:2A:98:71:C1:FD:34:9F*

Subject Key Identifier *D9:AC:70:DB:5F:7E:BE:94:F8:A0:E4:BE:47:A2:D0:34:AD:9A:2A:12*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies	*Policy OID: 0.4.0.2042.1.2* *Policy OID: 0.4.0.194112.1.2* *Policy OID: 1.3.6.1.4.1.51361.1.1.1* *CPS pointer: https://www.sk.ee/CPS* *Policy OID: 1.3.6.1.4.1.51361.1.1.2* *Policy OID: 1.3.6.1.4.1.51455.1.1.1* *Policy OID: 1.3.6.1.4.1.51361.1.1.5* *Policy OID: 1.3.6.1.4.1.51361.1.1.6* *Policy OID: 1.3.6.1.4.1.51361.1.1.7* *Policy OID: 1.3.6.1.4.1.51361.1.1.3* *Policy OID: 1.3.6.1.4.1.51361.1.1.4* *Policy OID: 1.3.6.1.4.1.51361.1.1.8* *Policy OID: 1.3.6.1.4.1.51361.1.1.9* *Policy OID: 1.3.6.1.4.1.51361.1.1.10* *Policy OID: 1.3.6.1.4.1.51361.1.1.11* *Policy OID: 1.3.6.1.4.1.51361.1.1.12* *Policy OID: 1.3.6.1.4.1.51361.1.1.13* *Policy OID: 1.3.6.1.4.1.51361.1.1.14* *Policy OID: 1.3.6.1.4.1.51361.1.1.15* *Policy OID: 1.3.6.1.4.1.51361.1.1.16* *Policy OID: 1.3.6.1.4.1.51361.1.1.17* *Policy OID: 1.3.6.1.4.1.51361.1.1.18* *Policy OID: 1.3.6.1.4.1.51361.1.1.19* *Policy OID: 1.3.6.1.4.1.51361.1.1.20* *Policy OID: 1.3.6.1.4.1.51455.1.1.2* *Policy OID: 1.3.6.1.4.1.51455.1.1.3* *Policy OID: 1.3.6.1.4.1.51455.1.1.4* *Policy OID: 1.3.6.1.4.1.51455.1.1.5* *Policy OID: 1.3.6.1.4.1.51455.1.1.6*
Extended Key Usage	*id_kp_clientAuth - id_kp_OCSPSigning*
Authority Info Access	*http://aia.sk.ee/ee-govca2018* *http://c.sk.ee/EE-GovCA2018.der.crt*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
CRL Distribution Points	*http://c.sk.ee/EE-GovCA2018.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *C4:5A:E8:1A:C8:B5:ED:5D:80:65:21:3F:D3:DC:25:0C:7B:32:77:36:8A:3E:97:BD:82:99:EF:FA:F8:B6:5E:31*

X509SubjectName

Subject CN: *ESTEID2018*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *2axw219+vpT4oOS+R6LQNK2aKhI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2018-11-02T14:00:00Z

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.5.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.51361.1*

Description *Certificate Policy for ID-card, Digi-ID, RP-card and Diplomatic-ID*

Documentation Reference *https://www.id.ee/?id=30500*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.5.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *1.3.6.1.4.1.51361.1*

Description *Certificate Policy for ID-card, Digi-ID, RP-card and Diplomatic-ID*

Documentation Reference *https://www.id.ee/?id=30500*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.5.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.6 - Service (withdrawn): EID-SK 2007

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK 2007*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1167992746*
X509 Certificate	*-----BEGIN CERTIFICATE-----* *MIID4jCCAsqgAwIBAgIERZ4nqjANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA* *c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAw* *DgYDVQQDEwdKdXVyLVNLMB4XDTA3MDEwNTEwMjU0NloXDTE2MDgyNjE0MjMwMVowajELMAkGA1UE* *BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZmlt0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRp* *Zml0c2VlcmltaXN0ZWVudXNlZDEUMBIGA1UEAxMLRUlELVNLIDIwMDcwggEiMA0GCSqGSIb3DQEB* *AQUAA4IBDwAwggEKAoIBAQDifhEdyvuhk/3TjEGMJ1tEZOskE81yMqPGGXaPHXACJ7fncn1D1uQF* *t+RG8/ckh7zDquHV1m4HQk7dchaP00rvgsvRlYC9GPcFt6TW8w3t+BkxY1RNbmONgH3qzikjk7m* *6Nb8UGtL9hOmZdw5k5t9HtBfgHTnoBkFrxYgsv9d4CCkBTSprNUK+vyNTak4dAYinWtK6RHHlb1* *fxRsLUXiDLSO42Kz+rehhslANX+9Y5/h0wlh3pcmxLB1JWAP0O9fV6N1LUQ3Ym7wMpIBXuPvl52* *yJuSZDWUF7GkIp+vUifOSefF6CeGh8K9BXDvuOqg+5c/6gkfEQxpRgdu+q5FAgMBAAGjgZwwgZkw* *EgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAf4wMwYDVR0fBCwwKjAoocCagJIYiaHR0* *cDovL3d3dy5zay5lZS9jcmxzL2p1dXlvY3JsLnNybDAfBgNVHSMEGDAWgBQEqnpHo+SjrxPCkCn* *GD9v7+I9viAdBgNVHQ4EFgQUHAf0nL+kjWyztJ4iHx+U5BtYeo0wDQYJKoZIhvcNAQEFBQADggEB* *ABaiEXv415Oh7AgHODwKRyNFqPcSSOgpLCy1XJB3hl3fi21fsIccWuBhfzqHQCiQi0fewh109Ij* *Hq8n1PeKoHBCUVq6NFpxkVsUlUPBr0Osya1O3SQjuOsBLzUWBvY25dtBuAkBMCo0V1Erf7iTeOzu* *L4LLbCoeOfeQT3HPmEf5qP5f8V10ST8erbiTVPJwzr66vXaT9YKxy8NyAQc2iaOHuYmGKxs8dgDQ* *RkG6b2af5q21YEQKDhvz7VvM6tH+F+rohA2wAvVz4tcPtyw5WEYcavr1KHgz4eZVWsqh2OsHUK9* *qMas5m/44O1/hXrjpMy5IQsiB4ASXDuXvdOTVbU=* *-----END CERTIFICATE-----*
Signature algorithm:	*SHA1withRSA*
Issuer CN:	*Juur-SK*
Issuer O:	*AS Sertifitseerimiskeskus*
Issuer C:	*EE*
Issuer E:	*pki@sk.ee*
Subject CN:	*EID-SK 2007*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Fri Jan 05 11:25:46 CET 2007*
Valid to:	*Fri Aug 26 16:23:01 CEST 2016*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E2:7E:11:1D:CA:FB:A1:93:FD:D3:24:41:8C:27:5B:44:64:EB:24:13:CD:72:32:A3:C6:19:76:8F:1D:70:02:27:B7:E7:72:7D:43:D6:E4:05:B7:E4:46:F3:F7:24:87:BC:C3:AA:E1:D5:D6:6E:07:42:4E:DD:72:16:8F:D3:4A:EF:82:CB:D1:95:80:BD:18:F7:05:B7:A4:D6:F3:0D:ED:F8:19:31:63:54:4D:6E:63:8D:80:7D:EA:CE:29:25:8E:4E:E6:E8:D6:FC:50:6B:4B:F6:13:A6:65:DC:39:93:9B:7D:1E:DF:1F:80:74:E7:A0:19:05:AF:16:20:B2:FF:5D:E0:20:A4:05:34:A9:AC:D5:0A:FA:FC:BF:35:36:A4:E2:20:18:8A:75:AD:2B:AB:51:1C:76:F5:7F:14:6C:2D:45:E2:0C:B4:8E:E3:62:B3:FA:B7:A1:86:C9:40:35:7F:BD:63:9F:E1:D3:09:61:DE:97:26:C4:B0:75:25:60:0F:D0:EF:5F:57:A3:75:2D:44:37:62:6E:F0:32:9F:E5:05:7B:8F:BE:5E:76:C8:9B:92:64:35:94:17:B1:A4:22:9F:AF:52:27:CE:49:E7:C5:E8:27:86:87:C2:BD:05:70:EF:B8:EA:A0:FB:97:3F:EA:09:1F:11:0C:69:46:07:6E:FA:AE:45:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://www.sk.ee/crls/juur/crl.crl*
Authority Key Identifier	*04:AA:7A:47:A3:E4:89:AF:1A:CF:0A:40:A7:18:3F:6F:EF:E9:7D:BE*
Subject Key Identifier	*1C:07:F4:9C:BF:A4:25:6C:B3:B4:9E:22:1F:1F:94:48:1B:58:7A:8D*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment - keyAgreement - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*5D:05:51:6D:8D:31:D0:86:6A:67:9D:9B:5A:CF:9F:CA:56:6F:58:1A:00:98:31:7D:45:E4:04:BE:FF:15:97:03*

X509SubjectName

Subject CN: *EID-SK 2007*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2017-06-30T22:00:00Z

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.6.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.6.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.6.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.6.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK 2007*

Service digital identities

X509SubjectName

Subject CN: *EID-SK 2007*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *HAf0nL+kJWyztJ4iHx+USBtYeo0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.6.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.6.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.6.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.6.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK 2007: Qualified certificates for Mobile-ID*

Service digital identities

X509SubjectName

Subject CN: *EID-SK 2007*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *HAf0nL+kJWyztJ4iHx+USBtYeo0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-01-05T11:25:46Z*

1.6.5.4 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.6.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.7 - Service (withdrawn): EID-SK 2011 qualified certificates for electronic signatures

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK 2011 qualified certificates for electronic signatures*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *89285850563550046921807203058435567450*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIFADCCA+igAwIBAgIQQyvUTmJDa0ZNgy+/fS0vWjANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUlgQ2Vy
dGlnaWNhdGlvbiBDZW5cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMTExMVoXDTI0MDMxODEwMTExMVowYTELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNl
cnRpZml0c2VlcmItaXNrZXNrdXMxFDASBgNVBAMMC0VjRC1TSyAyMDExMRgwFgYJKoZIhvcNAQkB
Fglwa2lAc2suZWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2Q1zKMt7DytbntSLo
YAAVkEwV+5djSr0v5lGiZm9seKyx+2PYBsVzXRoUD1CMIYnstDhBSKMjn2/+HpA7pOipAlAMrk6u
KnpST7dFbQ+0fzJVPokBgsdsQ6R5TZFPB1nu5zgRRIQmWIFxOpDiNHTt0LObUhWLXzUb31vc1Wma
o2IYcDx1TCs/1E9+camiCI2B5lXrPEU3wBq4waD54izS20DK05+6+hHRg+TqoIg5YSmwbjStEyd/
8AQeokwVloyyH49bnpeluADcZlgxxE9ZUvVWHoxYfmg1eRU72jHTcIjNf1cQN2+9/FtHOMnGzDB
gmAPpgIwW9r3ltW0JWvMXAgMBAAGjggGeMIIBmjA5BgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB
/wQEAwIBBjCB9AYDVR0gBIHsMIHpMIHmBgsrBgEEAc4fZAEBATCB1jCBsAYIKwYBBQUHAgIwgaMe
gaAASwBhAHMAdQB0AGEAdABhAGsAcwBlACAAZgD8APwAcwBpAGwAaQBzAHQAZQBsAGUAIABpAHMA
aQBrAHUAdABlAGwAZQAgAHMAZQByAHQAaQBmAGkAawBhAGEAdABpAGQAZQAgAHYA5ABsAGoAYQBz
AHQAYQBtAGkAcwBlAGsAcwAgAGsAbwBtAG0AZQByAHQAcwBhAGwAdQBzAGUAbAAuMCEGCCsGAQUF
BwIBFhVodHRwczovL3d3dy5zay5lZS9DUFMwHQYDVR0OBBYEFLEQIwL63YbGeEGkwzKl+/4f5BAF
MB8GA1UdIwQYMBaAFBLyWj7qVhyfzQas8fElyalL1BSZMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6
Ly93d3cuc2suZWUvcmVwb3NpdG9yeS9jcmxzL2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBBQUAA4IB
AQAxau3ohdFkpvaiVUR7arNovQUZRCG9Ge3udqHYemovyU7N60Hgomc/ZG+uunScATTUhBcv9a5z
kQxb1dQ1LYDRfNr9Cql0QvSEE4t95fu3fOhydLrlmb3s8xhhYLIBj325uDvtO/qFeXUcRXMF5nU8
FE2IyaZP1CHYKVh5QNPPQiGZGSox5oOkCvmt4IUI4IZUwVie75us/WtrD6DJeREBTEDHORIfg8E9
RA1y/7t2gT9vrU8tabeSZlD03qwXe0nJ9RscI/P0HT8vuo1PGzCfbH9xFqfoZ2jdJ0HzxrFM8VsL
/AtCw0dmrxRHLiZzqSw0G7b0W40mwOQauO2gbMfn
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Fri Mar 18 11:11:11 CET 2011*

Valid to: *Mon Mar 18 11:11:11 CET 2024*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B6:43:5C:CA:32:DE:C3:CA:D6:E7:B5:22:E8:60:00:15:90:4C:15:FB:97:63:4A:
BD:2F:48:81:BF:66:6F:6C:78:AC:B1:FB:63:D8:F2:C5:73:5D:1A:14:0F:50:8C:21:89:EC:B4:38:41:48:A3:23:9F:6F:FE:1E:90:3B:A4:E8:A9:00:B0:0C:AE:4E:AE:2A:7A:52:4D:37:45:6D:0F:B4
:7F:32:55:3E:89:01:82:C7:6C:43:A4:79:4D:91:4F:07:59:EE:E7:38:11:46:54:26:58:81:71:3A:90:E2:34:74:ED:D0:B3:9B:52:15:8B:5F:35:1B:DF:5B:DC:D5:69:9A:A3:62:18:70:3C:75:4C:2
B:3F:D4:4F:7E:71:A9:A2:0A:5D:81:E6:55:EB:3C:45:37:C0:1A:B8:C1:A0:F9:E2:2C:D2:DB:40:CA:D3:9F:BA:FA:11:D1:83:E4:EA:A0:88:39:61:29:B0:6E:34:AD:13:27:7F:F0:04:1E:A2:4C:15
:96:8C:B2:1F:8F:5B:9E:97:A5:B8:00:DC:64:98:31:C4:4F:59:52:F5:56:1E:8C:58:7E:68:35:21:E4:54:EF:68:C7:4D:C2:23:35:FD:5C:40:DD:BE:F7:F1:6D:1D:03:27:1B:30:C1:82:60:0F:A6:0
8:70:5A:BD:C9:B5:6D:09:5A:F3:17:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.100.1.1.1

CPS text: [Kasutatakse füüsilistele isikutele sertifikaatide väljastamiseks kommertsalusel.]

CPS pointer: https://www.sk.ee/CPS

Subject Key Identifier *B1:10:97:02:FA:DD:86:C6:78:41:A4:C3:32:88:FB:FE:1F:E7:C0:05*

Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*7B:16:66:A7:99:1C:FC:28:B6:4D:A3:71:F1:71:41:DB:D6:F5:32:1F:21:B8:3A:1A:65:8D:6A:41:0D:37:4E:05*

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*EID-SK 2011*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*

Status Starting Time

2020-12-05T09:14:31Z

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.7.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*

Criteria list assert=atLeastOne

Key Usage	*[digitalSignature]*	*true*
Key Usage	*[nonRepudiation]*	*true*
Description		*This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.7.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.7.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.7.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK 2011 qualified certificates for electronic signatures*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *sRCXAvrdhsZ4QaTDMoj7/h/nwAU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.7.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an QSCD*

1.7.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.7.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.7.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK 2011: Qualified certificates for Mobile-ID, organisation cards for natural persons*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2011*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *sRCXAvrdhsZ4QaTDMoj7/h/nwAU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-03-18T11:11:11Z*

1.7.5.4 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=atLeastOne

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Description *This service issues qualified certificates for e-signing and e-authentication within the same process. The Relying Party shall make distinction by inspection of keyUsage field contents - e-signature certificates have nonRepudation bit set exclusively. Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) and that has either its nR or its dS bit set is to be considered as supported by an SSCD*

1.7.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.8 - Service (granted): EID-SK 2016 qualified certificates for electronic signatures

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK 2016 qualified certificates for electronic signatures*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *79090250639102344903633087262654973146*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG4jCCBcggAwIBAgIQO4A6a2nBKoxXxVAFMRvE2jANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSib3DQEJARYJcGtpQHNrLmVlMCAXDTE2
MDgzMDA5MjEwOVoYDzIwMzAxMjE3MjM1OTU5WjBgMQswCQYDVQQGEwJFRTEiMCAGA1UECgwZQVMg
U2VydGlmaXRzZWVyaW1pc2tlc2t1czEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFDASBgNVBAMM
C0VjRC1TSyAyMDE2MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAr7XWFN0j1CFoGluV
e9xRezEnA0Tk3vmvIpvURX+y7Z5DJsfub2mtpSLtbhXjAeyng9QV78zjgQ73pNVGh+GQ6oPG7HF8
KlIZuIYsf1+gBxPxNiLa0+sCWxa6p4HQbgdgYRYGod4lQbib9KbOki3WjCG5W0Wh15P9qcu7ZVY+
9zawkSMf65Px/Y4ChjtNFtY66MEvsPChlHHfsBNiUbtZ68jJNYCECjtkm0vxz2iiSXB2WRIv3/hT
rRgMJ2CNMyFjRQoGQlpH010+fcisObKeyPwA8kI22Oto9MzLw7kSY524OD3B1L5MExYxHD916XIE
HT/9gBP2Zn8qZu/BlIKdSlapOlJW9ZEw+3w5UOU6LT3tTSbAzeQAnD3eCABPiYwHYC0lmKsPpQJ
qtx0Q3Jbm3BGReYiZ9KuK36nF/G78YjhM+yioERr2BcKT3Ij0W/GuGvyHakbokwy7nsbL30sTuR
LR70Oqi5UBMy4e8J2CduR3R3NJw5UqpScJlchngsLAx+WsyC0w38AmMewMBcnlp/QbakKo52HrsY
RR1m+NhCVDBy45Lzl8I0/OGd9Ikdg1h7T7SIguZVpyzys8E0yfrcS5YMEd9hMqVPr7rszXCzbxyw
0tVIk8QLMwIl+XE1Oi7SkgzA2i5Vpa6i2K0ard6GPHzRgGPTkjc5Z4DzZMCAwEAAaOCAn8wggJ7
MB8GA1UdIwQYMBaAFBLyWj7qVhyzQas8fElyaIL1B5ZMB0GA1UdDgQWBBScCagHhww9rC6H/KCu
0vtlSYgo+zAOBgNVHQ8BAf8EBAMCAQYwgcQGA1UdIASBvDCBuTA8BgcEAIvsQAECMDEwLwYIKwYB
BQUHAgEWI2h0dHBzOi8vd3d3LnNrLmVlL3JlcG9zaXRvb3JpdW0vQ1BTMDwGBwQAi+xAAQAwMTAv
BggrBgEFBQcCARYjaHR0cHM6Ly93d3cuc2suZWUvcmVwb3NpdG9vcml1bS9DUFMwOwYGBACPegEC
MDEwLwYIKwYBBQUHAgEWI2h0dHBzOi8vd3d3LnNrLmVlL3JlcG9zaXRvb3JpdW0vQ1BTMBIGA1UdE
EwEB/wQIMAYBAf8CAQAwJwYDVR0lBCAwHgYIKwYBBQUHAwkGCCsGAQUFBwMCBggrBgEFBQcDBDB8
BggrBgEFBQcBAQRwMG4wIAYIKwYBBQUHMAGGFGh0dHA6Ly9vY3NwLnNrLmVlL0NBMEoGCCsGAQUF
BzAChj5odHRwOi8vd3d3LnNrLmVlL2NlcnRzL0VFX0NlcnRpZmljYXRpb25fQ2VudHJlX1Jvb3Rf
Q0EuZGVyLmNydDBBBgNVHR4EOjA4oTYwBIICliwCocIAAAAAAAAAAwlocgAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAwJQYIKwYBBQUHAQMEGTAXMBUGCCsGAQUFBwsCMAkGBwQAi+xJ
AQEwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovL3d3dy5zay5lZS9yZXBvc2l0b3J5L2NybHMvZWVj
Y3JjY55jcmwwDQYJKoZIhvcNAQEMBQADggEBAKSloud5DSfhDU6yp+VrXYL40wi5zFTt19ha/kO/
zzLxZ1hf45VJmSyukMWaWXEqhaLWBZuw5kP78mQ0HyaRUennN0hom/pEiBz6cuz9oc+xlmPAZM25
ZoaLqa4upR2/+NCWoRTzYktdc9MEECs5RMBUmyT1G4s8J6n8L2M2yYadBMvPGj5JyXxYdc/b3a2f
oiw3kKa/q1tXAHXZCsuxFVYxXdZt3AwInYHemCVKjZg8BaRpvIEXd3AgJwt+9bpV/x0/MouRPNRv
0jjWIx1sAlL94hO74WZDMFbZVaV6gpG77X2P3dPHKFlRWzjtSQJX4C5n1uvQBxO4ABoMswq0Iq0=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject CN: *EID-SK 2016*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Tue Aug 30 11:21:09 CEST 2016*

Valid to: *Wed Dec 18 00:59:59 CET 2030*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:B5:D6:14:DD:23:D4:21:68:18:8B:95:7B:DC:51:7B:31:27:03:44:E4:DE:F9:AF:22:9B:D4:45:7F:B2:ED:9E:43:26:C7:EE:6F:69:AD:A5:22:ED:6E:15:E3:01:EC:A7:AB:D4:15:EF:CC:E3:81:0E:F7:A4:D5:46:87:E1:90:EA:83:C6:EC:71:7C:28:89:59:B8:86:2C:7F:5F:A0:07:13:F1:36:22:DA:D3:EB:02:5B:16:BA:A7:81:D0:6E:07:60:61:15:46:A1:DE:08:41:B8:9B:F4:A6:CE:92:2D:F0:8C:21:B9:5A:25:A1:D5:23:FD:A9:CB:93:65:56:3E:F7:36:B0:91:23:1F:EB:93:F1:FD:8E:02:86:3B:4D:16:D6:3A:E8:C1:2F:B0:F0:A1:94:71:DF:B0:13:62:51:BB:59:EB:CB:C9:35:80:84:0A:3B:64:9B:48:F1:CF:68:A2:49:70:76:59:12:2F:DF:F8:53:AD:18:0C:27:60:BD:33:21:63:45:0A:06:42:5A:47:D3:5D:3E:7D:C8:AC:39:B2:9E:C8:FC:00:F2:42:36:D8:EB:68:F4:CC:CB:C3:B2:AC:63:9D:B8:38:3D:C1:D4:BE:4C:13:16:31:1C:3F:75:E9:72:04:1D:3F:FD:80:13:F6:66:7F:2A:66:EF:C1:96:52:9D:48:86:A9:38:82:56:F5:91:30:FB:7C:39:50:E5:3A:2D:3D:ED:4D:26:C0:CD:E4:00:9C:3D:DE:08:00:4F:89:F6:30:1D:80:B4:96:62:AC:3E:94:09:AA:DC:74:43:72:5B:9B:70:46:45:E6:22:67:D2:AF:2B:7E:A7:17:F1:BB:F1:88:E1:33:EC:A2:A0:44:6B:D8:1F:DC:29:FD:F5:8F:45:BF:1A:E1:AF:C8:76:A4:6E:89:30:CB:B9:EC:6C:BD:F4:B1:3B:91:2D:1E:F4:3A:A8:B9:50:13:32:E1:EF:09:D8:27:6E:47:74:77:34:9C:39:52:AA:52:70:92:1C:86:78:2C:2C:0C:7E:5A:CC:82:D3:0D:FC:02:63:1E:C0:C0:5C:9E:5A:7F:41:B6:A4:2A:8E:76:1E:BB:18:45:1D:66:F8:D8:42:54:30:72:E3:92:F3:97:C2:34:FC:E1:9D:F4:89:1D:B3:58:7B:4F:B4:88:82:E6:55:A7:2C:F2:B3:C1:34:C9:FA:DC:4B:96:0C:11:DF:61:32:A5:4F:AF:BA:EC:CD:70:B3:6F:1C:B0:D2:D5:48:93:C4:0B:33:0F:E5:23:E5:C4:D4:E8:BB:4A:48:33:03:68:B9:56:96:BA:8B:62:B4:6A:B7:7A:18:F1:F3:46:A1:8F:4E:48:DC:E5:9E:03:CD:93:02:03:01:00:01

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

Subject Key Identifier *9C:09:A8:07:87:0C:3D:AC:2E:87:FC:A0:AE:D2:FB:65:49:88:28:FB*

Certificate Policies

Policy OID: 0.4.0.194112.1.2

CPS pointer: https://www.sk.ee/repositoorium/CPS

Policy OID: 0.4.0.194112.1.0

CPS pointer: https://www.sk.ee/repositoorium/CPS

Policy OID: 0.4.0.2042.1.2

CPS pointer: https://www.sk.ee/repositoorium/CPS

Basic Constraints *IsCA: true - Path length: 0*

Extended Key Usage *id_kp_clientAuth - id_kp_OCSPSigning*

Authority Info Access

http://ocsp.sk.ee/CA

http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt

CRL Distribution Points *http://www.sk.ee/repository/crls/eeccrca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E7:3F:1F:19:A4:45:9A:60:67:A4:5E:84:DB:58:5D:6C:1D:F8:F1:2A:73:9D:73:3F:5B:28:99:65:46:F1:87:5A*

X509SubjectName

Subject CN: *EID-SK 2016*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *nAmoB4cMPawuh/ygrtL7ZUmIKPs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2016-12-21T10:00:00Z*

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.8.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Policy Identifier:		
Identifier		*1.3.6.1.4.1.10015.17.2*
Description		*Certificate Policy for Qualified Smart-ID*
Documentation Reference		*https://sk.ee/en/repository/CP/*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.9 - Service (withdrawn): KLASS3-SK

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name	*[en]*	*KLASS3-SK*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*1020859637*
X509 Certificate	*-----BEGIN CERTIFICATE----- MIIEBDCCAuygAwIBAgIEPNkU9TANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFgIwa2lA c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAw DgYDVQQDEwdKdXVyLVNLMB4XDTAyMDUwODEyMDcxN1oXDTEyMDUwNTExMDcxN1owgY4xGDAWBgkq hkiG9w0BCQEWCXBraUBzaysiZTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZmlt0c2Vl cmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEKMAgGA1UEBRMB MTESMBAGA1UEAxMJS0xBU1MzLVNLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvIIe K3GJxoPCXVwan+HjJwYGaH3nb/rTPEgg5v9e1c7dnTDBdD2Yteg+IUdHBZDHLj1Tz+j/W9Foc0dz Er9658+6nMXoonK2x0B54JNH2UVb5/+YOGUM6iIW5xkHw525tyn5tFalQoaeh46aQFp9Dngcnv4Ga td0/7NCkLggIFrKmnNTPINpLAG9VoCpVyIMvcVCyTNv5Q+n33ToPO5vtULNYOtCF9MDVND+uNRE2 o0tWIG0l84owYPA47tJOLgCpAxLNFR5Ys0nB/ofBYcO+YiCri0yc6t7ZPs/vcfbR6czIwW0GMjyH mVPLB+/WHS3P1sk29DdgIC42RTMthJS6ZOIDAQABo4GZMIGWMA8GA1UdEwQIMAYBAf8CAQAwDgYD VR0PAQH/BAQDAgHmMDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly93d3cuc2suZWUvY3jscy9qdXVy L2NybC5jcmwwHwYDVR0jBBgwFoAUBKp6R6PKia8azwpApxg/b+/pfb4wHQYDVR0OBBYEFOU/DJ1x PW+8Gb+a9G6/Cf5A652WMA0GCSqGSIb3DQEBBQUAA4IBAQASvWB+YrgN23EMLW7C5/XUwQLNN1RM Dhr6UzOo5XHZ3pxUXq2Erk5ggiS+UJIxkQaSg4OHRru8KTchojDvS2neeYHOz05zJcAIwoy2GGkH g1iVN+QZaprDaDNYR5GGKgIb3FZrMtyX4dNwnrZzMFzd6t5YibCW+BDPAmqGjvNHzJ5YYdA7I3WT 9Baan1ncKd4FtUVb54fpqd19NkbCKK5Ud7qRYDduNYqVs1CJCDqqLq4Trxoxqx5o+WNLlD01896s IRiPly8qDOAXJU67382J5XXETe9wZO6o7+NaG0CrpzVY1OaaD2O6Wv/vSpxE2ugqaf0WsP35+coF CWdM2uHZ -----END CERTIFICATE-----
Signature algorithm:	*SHA1withRSA*
Issuer CN:	*Juur-SK*
Issuer O:	*AS Sertifitseerimiskeskus*
Issuer C:	*EE*
Issuer E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK*
Subject SERIAL NUMBER:	*1*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Subject E:	*pki@sk.ee*
Valid from:	*Wed May 08 14:07:17 CEST 2002*
Valid to:	*Sat May 05 13:07:17 CEST 2012*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:82:1E:2B:71:89:C6:83:C2:5D:5C:1A:9F:E1:E3:27:06:06:68:7D:E7:6F:FA: D3:3C:4A:A0:E6:FF:5E:D5:CE:DD:9D:30:C1:74:3D:98:B5:E8:3E:95:47:47:05:90:C7:2E:3D:53:CF:E2:7F:5B:D1:68:73:47:73:12:BF:7A:4B:CF:BA:9C:C5:E8:A2:72:B6:C7:4F:39:E0:93:47:D 9:45:5B:4B:FF:98:38:65:0C:EA:25:92:C6:41:F0:E7:6E:6D:BE:7E:6D:15:A2:10:A1:A7:A1:E3:A6:90:16:9F:43:9E:07:27:BF:81:9A:B5:DD:3F:EC:D0:A4:2E:08:23:16:B2:A6:9C:D4:CF:20:DA: 4B:00:6F:55:A0:2A:55:C8:83:2F:71:50:B2:4C:DB:D2:43:E9:F7:DD:3A:0F:3B:9B:ED:50:B3:58:3A:D0:B5:F4:C0:D5:34:3F:AE:35:11:36:A3:4B:56:20:6D:25:F3:8A:30:60:F0:38:EE:D2:4E:2 E:D0:A9:03:12:CD:15:1E:58:B3:49:C1:FE:B7:C1:61:C3:BE:62:20:AB:8B:4C:9C:EA:DE:D9:3E:CF:EF:71:F6:D1:E9:CC:C8:C1:6D:06:32:3C:B7:99:53:CB:07:EF:D6:1D:2D:CF:D6:C9:36:F4:3 7:60:20:2E:36:45:33:2D:84:94:BA:65:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://www.sk.ee/crls/juur/crl.crl*
Authority Key Identifier	*04:AA:7A:47:A3:E4:89:AF:1A:CF:0A:40:A7:18:3F:6F:EF:E9:7D:BE*
Subject Key Identifier	*E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*
Key Usage:	*digitalSignature - nonRepudiation - keyEncipherment - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A8:32:B7:A7:9B:0E:E1:62:A2:DA:04:7F:83:8C:83:A0:7E:03:2F:85:64:66:AD:08:2B:DC:B9:DF:C7:59:0F:FA*

X509SubjectName

Subject CN: *KLASS3-SK*

Subject SERIAL NUMBER: *1*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:01Z

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.9.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its non-repudation bit set exclusively, is to be considered as supported by an SSCD. They are issued for digital stamping according to Estonian Digital Signature Act*

1.9.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.9.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.9.4 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KLASS3-SK*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK*

Subject SERIAL NUMBER: *1*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *5T8MnXE9b7wZv5r0br8J/kDrnZY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.9.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its non-repudation bit set exclusively, is to be considered as supported by an SSCD. They are issued for digital stamping according to Estonian Digital Signature Act*

1.9.4.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.9.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.9.5 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KLASS3-SK: Qualified electronic seals*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK*

Subject SERIAL NUMBER: *1*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *5T8MnXE9b7wZv5r0br8J/kDrnZY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2002-05-08T12:07:17Z*

1.9.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.9.5.5 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its non-repudation bit set exclusively, is to be considered as supported by an SSCD. They are issued for digital stamping according to Estonian Digital Signature Act*

1.9.5.6 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.10 - Service (withdrawn): Klass3-SK 2010 qualified certificate for electronic seal

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *Klass3-SK 2010 qualified certificate for electronic seal*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1270027048*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIID5TCCAs2gAwIBAgIES7MTKDANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFgIwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTEwMDMzMTA5MTcyOFoXDTE2MDgyNjE0MjMwMVowbTELMAkGA1UE
BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZmI0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRp
Zmi0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEAxMOSOxBU1MzLVNLUDIwMTAwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCrIaYRX2v89k8Hd0ADaOfntUcIn7iM6aOXkAR+jp5827ZhDqDyN
ddF9ZUoBgPghGNlrkHbH7qwex39Ynl0ka24ICjcwEMvQMPbyPnX/a4RyJ+wEZttmjßl++FfrZK54
L+vD7Dyy4YYB0Og9ktB4qptsDBj+giiv/MGPeGeNs3TacJdNb7+3spITPtPKIDfrufvq4H6jNOv9
S9bC+j2VVY9uCFXUro8AA3hoOEKJdSJlpYCa51N8KGLVJYRuc/K81xqI054Jz+Cy/HY/AcXkk2Ik
xIpJoEXmcuTkxJO/QE/Xbd+mRjHnq6+HurOiKcxKw2CPAa+d+dvRPkbyg9ohMXH9AgMBAAGjgZww
gZkwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAcYwMwYDVR0fBCwwKjAooCagIIYi
aHR0cDovL3d3dy5zay5lZS9jcmxzL2p1dXIvY3JsLmNybDAfBgNVHSMEGDAWgBQEqnpHo+SJrxrP
CkCnGD9v7+I9vjAdBgNVHQ4EFgQUXXUUEYz0pY5Cj3uyQESj7tZ6O3IwDQYJKoZIhvcNAQEFBQAD
ggEBADFuAGt5oQ8PsWRw/QxFzc5EZtbq2KXC9yZ8YQPWBLY4Mh3OVLFjqWyKC+8jHy9D5tJTG49F
5UHyDjPufD/XvC2rjRlkqvS/W7sy3MgGh7e+6bg+aD4mo+98OaInqi12UD+ki+N8JKPXjHNJ31Av
H6E/xDsCsvtzubyIxl+FU8R0XODiUFbBqRtatRI1/zVaKRhD6LNGPt3rz/3ijKmuEv6b29mzL+p4
oNULqpPr6aTmheZme8ZHuElh3Zp5kdoX3i2D4hsmgClpevZifo196zeKRLk0Qs6nmRjoMxyk6jYl
ric3/VnV81oyhXSBY1GZnbM4qP1w255kSA2bb1pkwFo=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *Juur-SK*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject CN: *KLASS3-SK 2010*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Wed Mar 31 11:17:28 CEST 2010*

Valid to: *Fri Aug 26 16:23:01 CEST 2016*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:95:A6:11:5F:6B:FC:F6:4F:07:77:40:03:68:E7:E7:51:C2:27:EE:23:3A:68:E5:E4:01:1F:A3:A7:9F:36:ED:98:43:A8:3C:8D:75:D1:7D:65:4A:01:80:F8:21:18:D2:2B:90:76:C7:EE:AC:1E:C7:7F:58:9C:8D:24:6B:6E:25:0A:37:30:10:CB:D0:30:F6:F2:3E:75:FF:6B:84:72:27:EC:04:66:DB:66:8C:19:7E:F8:57:EB:64:AE:78:2F:EB:C3:EC:3C:B2:E1:86:01:D0:E8:3D:92:D0:78:AA:98:6C:0C:18:FE:82:28:AF:FC:C1:8F:78:67:8D:B3:74:DA:70:97:4D:6F:BF:B7:B2:99:53:3E:D3:CA:94:37:EB:89:FB:EA:E0:7E:A3:34:EB:FD:4B:D6:C2:FA:3D:95:55:8F:6E:08:55:D4:AE:8F:00:03:78:68:38:42:89:75:28:E5:A5:80:9A:E7:53:7C:28:62:D5:25:84:6E:73:F2:BC:D7:1A:A2:D3:9E:09:CF:E0:B2:FC:76:3F:01:C5:E4:93:62:64:C6:5A:49:A0:45:E6:72:E4:E4:C6:33:BF:40:4F:D7:6D:DF:A6:44:91:E7:AB:AF:87:BA:B3:A2:29:CC:4A:C1:90:8F:01:AF:9D:F9:DB:D1:3E:46:F2:AB:DA:21:31:71:FD:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://www.sk.ee/crls/juur/crl.crl*

Authority Key Identifier *04:AA:7A:47:A3:E4:89:AF:1A:CF:0A:40:A7:18:3F:6F:EF:E9:7D:BE*

Subject Key Identifier *5D:75:14:11:8C:F4:A5:8E:42:8F:7B:B2:40:44:A3:EE:D6:7A:3B:72*

Key Usage: *digitalSignature - nonRepudiation - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DC:62:4A:71:15:DD:C4:1B:4A:84:06:6F:FC:0D:BC:38:F7:1A:A8:7D:54:FE:62:F0:C8:20:40:D8:36:F6:13:BD*

Certificate fields details

Version: *3*

Serial Number: *42879783182822194711502757635696878 74*

X509 Certificate

-----BEGIN CERTIFICATE-----

*MIIErDCCA55gAwIBAgIQAznVp1LayatNgy6bN8f9QjANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUIgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVIMB4XDTEx
MDMxODEwMDYxOFoXDTI0MDMxODEwMDYxOFowbTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNl
cnRpZmlOc2VlcmItaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZmlOc2VlcmItaXN0ZWVudXNlZDEX
MBUGA1UEAxMOS0xBU1MtLVNLIDIwMTAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCr
IaYRX2v89k8Hd0ADaOfnUcIn7iM6aOXkAR+jp5B27ZhDqDyNddF9ZUoBgPghGNlrkHbH7qwex39Y
nI0ka24lCjcwEMvQMPbyPnX/a4Ryj+wEZttmjBl++FfrZK54L+vD7Dyy4YYB0Og9ktB4qptsDBj+
giiv/MGPeGeNs3TacJdNb7+3spITPtPKIDfrufvq4H6jNOv9S9bC+j2VVY9uCFXUro8AA3hoOEKJ
dSjlpYCa51N8KGLVlYRuc/K81xqi054Jz+Cy/HY/AcXkk2JkxJpJoEXmcuTkxjOj/QE/Xbd+mRjHn
q6+HurOiKcxKwZCPAa+d+dvRPkbyg9ohMXH9AgMBAAGjggE+MIIBOjA5BgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBxjCBlAYDVR0gBIGMMIGJMIGGBgsrBgEEAc4fZAEBATB3MCEGCCsG
AQUFBwIBFhVodHRwczovL3d3dy5zay5lZS9jcHMwUgYIKwYBBQUHAgIwRh5EAEEAcwB1AHQAdQBz
AGUAIABzAGUAcgB0AGkAZgBpAGsAYQBhAHQALgAgAEMAbwByAHAAbwByAGEAdABlACAASQBEAC4w
HQYDVR0OBBYEFF11FBGM9KWOQo97skBEo+7WejtyMB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fEI
yalL1BSZMD0GA1UdHwQ2MDQwMgAwoC6GLGh0dHA6Ly93d3cuc2suZWUvcmVwb3NpdG9yes9jcmxz
L2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQC3qNBgY2I9Wqm4LZYKAjCYkc2Nltm1RS9f
rMvQJ4aEE4Y4TtW2LPcQp2lenOf9aYdEB8G/E9CytZSPlFuvDdsdknj6fg1XCeu6lTR2wlkxJeAe
LQvrFEfb1mcAa5tU9RNalZhYc7MFMFQTjQP+GBNxz+KjjNDVASFdv7TCe7GBjsW8Dfes9IQGHaWs
BRkHCyuPGlHfH+cmMuhLtWqa4Qlg4f54kcsGO7s4buKtk6XqEj8CJ2ITdfk/aUs9QoxxkYWGwSUl
CueTamzufXEJo9yz5Jp6lFdGjotmjb/EBUCf2sFfI83a4Cm1D3L3/KYb5g3cYlDEpPWNqbNuA1Xo
slqK*

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject CN: *KLASS3-SK 2010*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Fri Mar 18 11:06:18 CET 2011*

Valid to: *Mon Mar 18 11:06:18 CET 2024*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:95:A6:11:5F:6B:FC:F6:4F:07:77:40:03:68:E7:E7:51:C2:27:EE:23:3A:68:E
5:E4:01:1F:A3:A7:9F:36:ED:98:43:A8:3C:8D:75:D1:7D:65:4A:01:80:F8:21:18:D2:2B:90:76:C7:EE:AC:1E:C7:7F:58:9C:8D:24:6B:6E:25:0A:37:30:10:CB:D0:30:F6:F2:3E:75:FF:6B:84:72:
27:EC:04:66:DB:66:8C:19:7E:F8:57:EB:64:AE:78:2F:EB:C3:EC:3C:B2:E1:86:01:D0:E8:3D:92:D0:78:AA:9B:6C:0C:18:FE:82:28:AF:FC:C1:8F:78:67:8D:B3:74:DA:70:97:4D:6F:BF:B7:B2:9
9:53:3E:D3:CA:94:37:EB:B9:FB:EA:E0:7E:A3:34:EB:FD:4B:D6:C2:FA:3D:95:55:8F:6E:08:55:D4:AE:8F:00:03:78:68:38:42:89:75:28:E5:A5:80:9A:E7:53:7C:28:62:D5:25:84:6E:73:F2:BC:
D7:1A:A2:D3:9E:09:CF:E0:B2:FC:76:3F:01:C5:E4:93:62:64:C6:5A:49:A0:45:E6:72:E4:E4:C6:33:BF:40:4F:D7:6D:DF:A6:44:91:E7:AB:AF:87:BA:B3:A2:29:CC:4A:C1:90:8F:01:AF:9D:F9:D
B:D1:3E:46:F2:AB:DA:21:31:71:FD:02:03:01:00:01
```


Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.100.1.1.1

CPS pointer: https://www.sk.ee/cps

CPS text: [Asutuse sertifikaat. Corporate ID.]

Subject Key Identifier *5D:75:14:11:8C:F4:A5:8E:42:8F:7B:B2:40:44:A3:EE:D6:7A:3B:72*

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

CRL Distribution Points *http://www.sk.ee/repository/crls/eeccrca.crl*

Key Usage: *digitalSignature - nonRepudiation - keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *17:F3:02:21:9F:CF:CE:8F:D1:8C:AC:17:2F:8B:0D:44:96:BA:5D:A8:E4:9F:87:1A:BC:1F:9D:0C:AA:A3:60:E5*

Certificate fields details

Version: *3*

Serial Number: *134258170546889953808822672640472260 74*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFKjCCBBKgAwIBAgIQChm34x8ah3BVcFedls2c2jANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUlgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE1
MDYwNDEzNTAyMVoXDTI0MDMxNzIyMDAwMFowbTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEX
MBUGA1UEAxMO50xBU1MtLVNLIDIwMTAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCr
iaYRX2v89k8Hd0ADaOfnUcIn7iM6aOXkAR+jp5827ZhDqDyNddF9ZUoBgPghGNlrkHbH7qwex39Y
nI0ka24lCjcwEMvQMPbyPnX/a4Ryl+wEZttmjBl++FfrZK54L+vD7Dyy4YYB0Og9ktB4qptsDBj+
giiv/MGPeGeNs3TacJdNb7+3spIT PtPKIDfrufvq4H6jNOv9S9bC+j2VVY9uCFXUro8AA3hoOEKJ
dSjlpYCa5 1N8KGLVjYRuc/K81xqi054Jz+Cy/HY/AcXkk2JkxJpJoEXmcuTkxjO/QE/Xbd+mRjHn
q6+HurOiKcxKwZCPAa+d+dvRPkbyg9ohMXH9AgMBAAGjqqG8MIIBuDA5BgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBxjCBlAYDVR0gBIGMMIGJMIGGBgsrBgEEAc4fZAEBATB3MCEGCCsG
AQUFBwIBFhVodHRwczovL3d3dy5zay5lZS9jcHMwUgYIKwYBBQUHAgIwRh5EAEEAcwB1AHQAdQBz
AGUAIABzAGUAcgB0AGkAZgBpAGsAYQBhAHQALgAgAEMAbwByAHAAbwByAGEAdABlACAASQBEAC4w
HQYDVR0OBBYEFF11FBGM9KWOOo97skBEo+7WejfyMBBGA1UdIwQYMBaAFBLyWj7qVHy/zQas8fE/
yaIL1BSZMHwGCCsGAQUFBwEBBHAwbjAgBggrBgEFBQcwAYYUaHR0cDovL29jc3Auc2suZWUvQ0Ew
SgYIKwYBBQUHMAKGPmh0dHA6Ly93d3cuc2suZWUvY2VydHMvRUVfQ2VydGlmaWNhdGlvbl9DZW50
cmVfUm9vdF9DQS5kZXIuY3j0MD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly93d3cuc2suZWUvcmVw
b3NpdG9yeS9jcmxzL2VlY2NyY2EuY3jsMA0GCSqGSIb3DQEBDAUAA4IBAQB4/0TLXatMTnzl8Z81
0lR3pESCq6ueQRvGPPl2isGe3ldA9PhKZ7j6323ifI2ldOdMeU12gd4pzuHXieFC1YhswqXCR1hu
LNu1KA8PRhgxdOBQ1etRSkZTIftMhBgpxot2Tu4G2xKQ7wfetdqnrUQ/u++BuAhuHA2xsma236eQ
7z3izoxCOSc+FMpQT/SY9NvKtZlmFEPycxZxu0uWCQtBbx+b/MAYKgq2/vMvLO4IyRqkeSRuLMZT
4AA4ZHggGIwL7NWiwedyEqvwq05g3e92F2wBff+Xah/WeZBioxuI1TRtzFcge6BTfF250RdbaaOW
eXsbNaA/azZ4WrNj1CTv

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer E:	*pki@sk.ee*
Issuer CN:	*EE Certification Centre Root CA*
Issuer O:	*AS Sertifitseerimiskeskus*
Issuer C:	*EE*
Subject CN:	*KLASS3-SK 2010*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Thu Jun 04 15:50:21 CEST 2015*
Valid to:	*Sun Mar 17 23:00:00 CET 2024*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:95:A6:11:5F:6B:FC:F6:4F:07:77:40:03:68:E7:E7:51:C2:27:EE:23:3A:68:E5:E4:01:1F:A3:A7:9F:36:ED:98:43:A8:3C:8D:75:D1:7D:65:4A:01:80:F8:21:18:D2:2B:90:76:C7:EE:AC:1E:C7:7F:58:9C:8D:24:6B:6E:25:0A:37:30:10:CB:D0:30:F6:F2:3E:75:FF:6B:84:72:27:EC:04:66:DB:66:8C:19:7E:F8:57:EB:64:AE:78:2F:EB:C3:EC:3C:B2:E1:86:01:D0:E8:3D:92:D0:78:AA:9B:6C:0C:18:FE:82:28:AF:FC:C1:8F:78:67:8D:B3:74:DA:70:97:4D:6F:BF:B7:B2:99:53:3E:D3:CA:94:37:EB:B9:FB:EA:E0:7E:A3:34:EB:FD:4B:D6:C2:FA:3D:95:55:8F:6E:08:55:D4:AE:8F:00:03:78:68:38:42:89:75:28:E5:A5:80:9A:E7:53:7C:28:62:D5:25:84:6E:73:F2:BC:D7:1A:A2:D3:9E:09:CF:E0:B2:FC:76:3F:01:C5:E4:93:62:64:C6:5A:49:A0:45:E6:72:E4:E4:C6:33:BF:40:4F:D7:6D:DF:A6:44:91:E7:AB:AF:87:BA:B3:A2:29:CC:4A:C1:90:8F:01:AF:9D:F9:DB:D1:3E:46:F2:AB:DA:21:31:71:FD:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.10015.100.1.1.1* *CPS pointer: https://www.sk.ee/cps* *CPS text: [Asutuse sertifikaat. Corporate ID.]*
Subject Key Identifier	*5D:75:14:11:8C:F4:A5:8E:42:8F:7B:B2:40:44:A3:EE:D6:7A:3B:72*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Key Usage:	*digitalSignature - nonRepudiation - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*00:DB:86:A7:08:7A:75:0C:E0:7B:32:55:D0:D3:12:9E:88:8C:A9:E0:EE:CA:CF:9E:72:BD:B2:76:B1:71:47:EF*

X509SubjectName

Subject CN:	*KLASS3-SK 2010*
Subject OU:	*Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2023-05-09T21:00:00Z

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.10.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.10.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.10.3 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.10.4 - Extension (critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description

1.10.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.10.6 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Klass3-SK 2010 qualified certificate for electronic seal*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK 2010*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *XXUUEYz0pY5Cj3uyQESj7tZ6O3I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.10.6.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.10.6.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.10.6.3 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.10.6.4 - Extension (critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		

1.10.6.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.10.7 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name	*[en]*	*KLASS3-SK 2010*

Service digital identities

X509SubjectName

Subject CN:	*KLASS3-SK 2010*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*XXUUEYz0pY5Cj3uyQESj7tZ6O3I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.10.7.6 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.10.7.7 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description *[en]* *undefined.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.10.7.8 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.10.8 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KLASS3-SK 2010: Qualified electronic seals*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK 2010*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *XXUUEYz0pY5Cj3uyQESj7tZ6O3I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-03-31T09:17:28Z*

1.10.8.9 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.10.8.10 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its non-repudation bit set exclusively, is to be considered as supported by an SSCD. They are issued for digital stamping according to Estonian Digital Signature Act*

1.10.8.11 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.11 - Service (granted): Klass3-SK 2016 qualified certificate for electronic seal

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *Klass3-SK 2016 qualified certificate for electronic seal*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *125379590422109434570404910176131905756*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGgTCCBWmgAwIBAgIQXIM7EyVgNCtYSVcwizB43DANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMCAXDTE2
MTIwODEyNTA1NloYDzIwMzAxMjE3MjM1OTU5WjCBhjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFT
IFNlcnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNl
ZDEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAIkOLeKQPKK1U8VK7z2Dzt2SX2KbIGqrBmOXfzIlm
zXHxGVopSeji24MdR5Ok6NjqXxanbyufXXRTeuE5nQ8Olzr5+9U21DPmVUADFNWnDLy6NWyqE3C
vrYp7tVOHbfTb9Mf3ECvQNt8YM0HGwd5fc8KGXuX8d4oixxeG4AD+wrj1+LI0ioaQFIS6Tbcwq3x
EO0WVv1hMrJOoMmPpaqrvRLcoikpmjnPm/Gtfx64FcyXiMmNxFDnROVMgr1OQKbxAdlX3lu32fcX
jXesCTcACLINRMi5Sb1wowjGEpqL2H53+JDIrdE7hM0uUqX4aaT5etaUh0o2hxOBHg3m6WRAZmBP
qO1BgIBN6PRMWYgab7B8tjMUKXE+FUaNy9Lb8jraX85t3IwN/hbbMx3wUAqZvoQVIajlu2tsP8eTG
lUd6jE59q9rH788LNf2w9o16blr1cM0AkzfbPf1ktCIERcQd+iEhAPluSjKwMHlehRQGwGGuo7db
4QXKhXDXPGK5YRw6Q56mp+BpSqJJqpdlQCieEXbHm9sHsoP5yaQygZl8nJpd0nlpdcTq91aEjrWu
uksQTNDG9++8NSAql2G/BVCesWx/zR0KtcWecMPUVfe7qEEFurWsewpLqZFsk5RLtNGwyTEgHHBf
JqAJC8I2VMfbbsEW+tcjdMqb6BHgT6hNCx8CAwEAAaOCAfcwggHzMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgHGMIHTBgNVH5AEgcswgcgwgYQGCSsGAQQBzh8HAzB3MCEGCCsGAQUF
BwIBFhVodHRwczovL3d3dy5zay5lZS9jcHMwUgYIKwYBBQUHAgIwRh5EAEEAcwB1AHQAdQBzAGUA
IABzAGUAcgB0AGkAZgBpAGsAYQBhAHQALgAgAEMAbwByAHAAbwByAGEAdABlACAASQBEAC4wCAYG
Z4EMAQICMAsGCSsGAQQBzh8HAjAIBgYEAI96AQEwCQYHBACL7EABATAIBgYEAI96AQcwCQYHBACL
7EABAzAdBgNVHQ4EFgQUri5Y9fLy2cGQ2e9OB9t1yIDihwAwHwYDVR0jBBgwFoAUEvJaPupWtHL/N
Bqzx8SXJqUvUFJkweAYIKwYBBQUHAQEEbDBqMCAGCCsGAQUFBzABhhRodHRwOi8vb2N2cC5zay5l
ZS9DQTBGBggrBgEFBQcwAoY6aHR0cDovL3NrLmVlL2NlcnRzL0VFX0NlcnRpZmljYXRpb25fQ2Vu
dHJlX1jvb3RfQ0EuZGVyLmNydDA9BgNVHR8ENjA0MDKgMKAuhixodHRwOi8vd3d3LnNrLmVlL3Jl
cG9zaXRvcnkv Y3Jscy9lZWNjcmNhLmNybDANBgkqhkiG9w0BAQwFAAOCAQEAah2vGoj+Re5+Cpta
rh0vCQWOm233nI5Y9qL+/JqG5PccowQ41kzf4qknmP6BHfisYGQsRc75K07A+/BdlFrLMbP3fFsuT
i7+HAmAjXYEq35G49GAQg52+HvZiBe+RtbR8yOOar5fAKnzS1yNy9M1z7g7yMcEouk3TUebe2aan
Mvzabc7qgV3HGDfZkzhL9PlcjmFI0LQEfIef/6sdMhy6C0HiditdLSUZYfSySJpb6lvJBGdN4Vrb
o2fNtL3qlc+vX1jvh/qLFIFmFXuC6IljFJFtplbCIQMtHoMXdI1A5JzzkmrTLPTSYDAQXXn9RPnz
sRz2GnlYRV4xGayDGbUyow==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C:	*EE*
Subject CN:	*KLASS3-SK 2016*
Subject 2.5.4.97:	*NTREE-10747013*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Thu Dec 08 13:50:56 CET 2016*
Valid to:	*Wed Dec 18 00:59:59 CET 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:96:43:8B:78:A4:0F:28:AD:54:F1:52:BB:CF:60:F3:B7:64:97:D8:A6:E5:1A:AA:C1:98:E5:DF:CE:52:26:CD:71:F1:19:5A:29:49:E8:E2:DB:FE:0C:75:1E:4E:93:A3:49:A9:7C:5A:9D:BC:AE:7D:75:D1:4D:EB:84:E6:74:3C:3A:5C:EB:E7:EF:54:DB:50:CF:99:55:00:0C:53:56:9C:32:F2:E8:D5:B2:A8:4D:C2:BE:B6:29:EE:D5:4E:1D:B7:D3:6F:D3:1F:DC:40:AF:40:DB:7C:60:CD:07:1B:07:52:7D:CF:24:19:7B:97:F1:DE:28:8B:1C:5E:18:80:03:FB:0A:E3:D7:E2:C9:D2:2A:1A:40:59:52:E9:36:DC:C2:AD:F1:10:ED:16:56:FD:61:32:B2:4E:A0:C9:8F:A5:AA:AB:BD:12:DC:A2:29:29:9A:39:CF:9B:F1:AD:7F:1E:B8:15:CC:97:88:C9:8D:C4:50:E7:44:E5:4C:82:BD:4E:40:A6:F1:01:D9:57:DC:8B:B7:D9:F7:17:8D:77:AC:09:37:00:08:B9:4D:44:C8:B9:49:BD:70:A3:08:C6:12:9A:8B:D8:7E:77:F8:90:C8:AD:D1:3B:84:CD:2E:52:A5:F8:69:A4:F9:7A:D6:94:87:4A:36:87:13:81:1E:0D:E6:E9:64:40:66:60:4F:A8:ED:41:AB:80:4D:E8:F4:4C:59:88:1A:6F:B0:41:B4:93:14:29:71:3E:15:46:8D:CB:D2:DB:F2:3A:DA:5F:CE:6D:DC:8C:0D:FE:16:DB:33:1D:F0:50:0A:99:BE:84:15:21:A2:6E:DA:DB:0F:F1:E4:C6:25:47:7A:8C:44:BD:AB:DA:C7:EF:CF:0B:35:FD:80:F6:8D:7A:6E:5A:F5:70:CD:00:93:37:DB:3D:FD:64:B4:29:44:45:C4:1D:FA:21:21:00:F9:6E:4A:32:B0:30:72:1E:85:14:06:C0:61:AE:A3:B7:5B:E1:05:CA:B5:70:D7:3C:62:B9:61:1C:3A:43:9E:A6:A7:E0:69:4A:A2:49:AA:97:65:40:28:9E:11:76:C7:9B:DB:07:B2:83:F9:C9:A4:32:81:92:3C:9C:9A:5D:D2:79:69:75:C4:EA:F7:56:84:8E:B5:AE:BA:4B:10:4C:D0:C6:F7:EF:BC:35:20:2A:97:61:BF:05:50:9E:B1:6C:7F:CD:1D:0A:B5:C5:9E:70:C3:D4:55:F7:BB:A8:41:05:BA:B5:AC:7B:0A:4B:81:91:6C:93:94:4B:B4:D1:B0:C9:31:20:1C:70:5F:26:A0:09:0B:C9:76:54:C7:DB:6E:C1:16:FA:D7:23:74:CA:9B:E8:11:E0:4F:A8:4D:0B:1F:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.10015.7.3* *CPS pointer: https://www.sk.ee/cps* *CPS text: [Asutuse sertifikaat. Corporate ID.]* *Policy OID: 2.23.140.1.2.2* *Policy OID: 1.3.6.1.4.1.10015.7.2* *Policy OID: 0.4.0.2042.1.1* *Policy OID: 0.4.0.194112.1.1* *Policy OID: 0.4.0.2042.1.7* *Policy OID: 0.4.0.194112.1.3*
Subject Key Identifier	*AE:5E:58:F5:F2:F2:D9:C1:8E:D9:EF:4E:07:DB:75:CA:50:E2:87:00*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Key Usage:	*digitalSignature - nonRepudiation - keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A5:A8:59:CE:03:10:A8:5F:42:A5:41:1D:A6:3F:83:B4:14:4E:B9:4B:C8:A6:5A:99:75:AC:86:82:F6:67:DB:77*

X509SubjectName

Subject CN:	*KLASS3-SK 2016*
Subject 2.5.4.97:	*NTREE-10747013*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*rl5Y9fLy2cGO2e9OB9t1ylDihwA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2017-06-03T06:00:00Z

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.11.1 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Policy Identifier:		
Identifier		*0.4.0.194112.1.3*
Description		*Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.11.2 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage	*[nonRepudiation]*	*true*
Key Usage	*[nonRepudiation]*	*false*
Description		*Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.11.3 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.11.4 - Extension (critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Description		

1.11.5 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.12 - Service (withdrawn): ESTEID-SK OCSP RESPONDER 2005

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *ESTEID-SK OCSP RESPONDER 2005*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1110287041*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDPDCCAiSgAwIBAgIEQi2iwTANBgkqhkiG9w0BAQUFADB8MRgwFgYJKoZIhvcNAQkBFgIwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWIza2Vza3VzMQ8w
DQYDVQQLEwZFU1RFSUQxCjAIBgNVBAQTATExEjAQBgNVBAMTCUVTVEVjRC1TSzAeFw0wNTAzMDgx
MzA0MDFaFw0xMjAxMTIxMzA0MDFaMG8xCzAJBgNVBAYTAkVFMQ8wDQYDVQQKEwZFU1RFSUQxDTAL
BgNVBAsTBE9DU1AxJjAkBgNVBAMTHUVTVEVjRC1TSyBPQ1NQIFJFU1BPTkRFUiAyMDA1MRgwFgYJ
KoZIhvcNAQkBFgIwa2lAc2suZWUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAI8mLeLkRHLx
MNCB5Pz8R5DnvPdVxBS91PoHboLnbhjlp1ecByVosjwGpXCGu8tUPuv81Azgqg97AsSugM1J7Pu0
gj4bg0Mf6O/9XyoT7Ri7H0BuEn4KJOlFcw7tXizI5KUWFFZ4Og8kfg0xwrDrLIjusBtRbeRARG3D
hH8dgZBpAgMBAAGjVzBVMBMGA1UdJQQMMAoGCCsGAQUFBwMJMB8GA1UdIwQYMBaAFHgXtQX5s1jN
WYzeZ15EBlx1hmIcIMB0GA1UdDgQWBBRM+GJhIoJeOPpJDqvA0clxOXdnVTANBgkqhkiG9w0BAQUF
AAOCAQEAfD8dP+swtSeigLxL3uUXV/tmQkjre7Ww39Uey71LdtxQ6zC7MDjcsLW13JaU0pRuu/p/
eGe6h4/w46tSMsBx/U+D1WnHeCj1ED9SFWwfNQFVz9FkM5JEkPDm7lw5hHoxIghRHAC3NMbR3sCr
VQA2YELf2WypslROoz8XlRT1LN4pwVehpBeWO7xbOPUtoaxKrSCGumtxtxA3KRj7POHPTAH4cvip
xaZhS1ZcXbKtxsesGW+7KLZirpTBT17lCXEA1CFXDWnj8MHRhbeNWK3G1PERgTiGtBQV7Z00CzmJ
PHmb1yfcT27+WZ1W9tRQsjhGEWyMVkNnZooWHIjLpNucQA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ESTEID-SK*

Issuer SURNAME: *1*

Issuer OU: *ESTEID*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER 2005*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

Valid from: *Tue Mar 08 14:04:01 CET 2005*

Valid to: *Thu Jan 12 14:04:01 CET 2012*

Public Key:


```
30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:8F:26:2D:E2:E4:44:72:F1:30:D0:81:E4:FC:FC:47:90:E7:BC:F7:55:C4:14:BD:D4:FA:07:6E:
82:E7:6E:18:E5:A7:57:9C:07:25:68:B2:3C:06:A5:70:86:BB:CB:54:3E:EB:FC:D4:0C:E0:AA:AF:7B:02:C4:AE:80:CD:49:EC:FB:B4:82:3E:1B:83:43:1F:E8:EF:FD:5F:2A:13:ED:12:3B:1F:40:6E
:12:7E:0A:25:09:45:73:0E:ED:5E:2C:C8:E4:A5:16:14:56:78:42:0F:24:7E:0D:31:C2:B0:EB:2C:88:EE:B0:1B:51:6D:E4:40:44:6D:C3:84:7F:1D:81:90:69:02:03:01:00:01
```


Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *78:17:B5:05:F9:B3:58:CD:59:8C:DE:67:5E:44:06:4C:75:86:69:5D*

Subject Key Identifier *4C:F8:62:61:96:82:5E:38:FA:49:0E:0B:C0:D1:C9:71:41:77:67:55*

Thumbprint algorithm: *SHA-256*

Thumbprint: *46:C5:54:6F:E6:AE:3D:F8:07:01:11:6A:68:06:F1:BF:13:EC:FE:78:B5:D9:C4:FB:EB:52:E2:A8:41:2B:A5:E7*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER 2005*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.12.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *ESTEID-SK OCSP RESPONDER 2005*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER 2005*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *TPhiYZaCXjj6SQ4LwNHJcUF3Z1U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.12.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, ESTEID-SK OCSP RESPONDER 2005*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER 2005*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *TPhiYZaCXjj6SQ4LwNHJcUF3Z1U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2005-03-08T14:04:01Z*

1.13 - Service (withdrawn): ESTEID-SK 2007 OCSP RESPONDER

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *ESTEID-SK 2007 OCSP RESPONDER*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1167923826*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDnDCCAoSgAwIBAgIERZ0acjANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwlFRTEiMCAGA1UE
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEPMA0GA1UECxMGRVNURUlEMRcwFQYDVQQDEw5F
U1RFSUQtU0sgMjAwNzAeFw0wNzAxMDQxNTE3MDZaFw0xMDAxMDgxNTE3MDZaMG8xCzAJBgNVBAYT
AkVFMO8wDQYDVQQKEwZFU1RFSUQxDTALBgNVBAsTBE9DU1AxJjAkBgNVBAMTHUVTVEVjRC1TSyAy
MDA3IE9DU1AgUkVTUE9OREVSMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUxCzAJBgNVBAYTAkVF
AQEBBQADgY0AMIGJAoGBAJmoB3SjCpPzcoHNqK1J0tRNQjgr5iuB27uE1VacIbITjD/Nc1AefKz5
ydNPlaBNehm4yKxBYGxEeWOSjHVXyhJMg53EAUOw/45c46gvznXupHuj6TEiGjh1pxaXTeLSnTqz
NDZDAGQsOTglbwGLa5U5ad8rXYu2YkJKSAfo6jT5AgMBAAGJgdcwgdQwEwYDVR0lBAwwCgYIKwYB
BQUHAwkwEgYJKwYEBQUHMAEFBAUwAwQBMDCBiQYDVR0jBIGBMH+AFEgG3r6Mh1eVgHhj+pwjKyug
Ohh1oWGkXzBdMRqwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQK
ExlBUyBTZXJ0aWZpdHNlZXJpbWIza2Vza3VzMRAwDgYDVQQDEwdKdXVyLVNLggRFm6ANMB0GA1Ud
DgQWBBRJ/snw1GDL3fUH9n9Cpn8yhXiC7DANBgkqhkiG9w0BAQUFAAOCAQEAYzGkZD/uaXIWPeye
1z5IIl83nmAjIjyvoj/r3BB9ZFWMX+ZY4Fz6/V/fzD0xXoeDpWbBKxcuctPXzXYxEH17n0/3yGOz
8jhdINBUCwRmd+96oHtsU9aW5f+D2tig1JPw6HVCIUYOhC/OWjg/+JpFIWsBV4gTWB/2P5Gig85Xl
EsWLK7i7tle60nnw/rWnfbCckMRcbrAF1L/JlInUYUdkGOGQ9KPVqwR/MyWrwFlcSy2QIbcIaWMu
iUc1nt8bmIXKoFZxbLzXYC00zba9cY7ISC4WPuhBtrQJ9JWb4OeoXd5j6O45UaH6XbarfrhER1GH
L06cTyksT18p2L2GrMuEJg==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ESTEID-SK 2007*

Issuer OU: *ESTEID*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

Valid from: *Thu Jan 04 16:17:06 CET 2007*

Valid to: *Fri Jan 08 16:17:06 CET 2010*

Public Key: *30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:99:A8:07:74:89:0A:93:F3:72:81:CD:A8:AD:49:D2:D4:4D:42:38:2B:E6:2B:81:DB:BB:84:D5:56:9C:21:B2:13:8C:3F:CD:73:50:1E:7C:AC:F9:C9:D3:4F:21:A0:4D:7A:19:B8:C8:AC:41:60:6C:44:79:63:92:24:75:57:CA:12:4C:83:9D:C4:01:43:B0:FF:8E:5C:E3:A8:2F:CE:75:EE:A4:7B:89:E9:31:22:1A:38:75:A7:16:97:4D:E2:D2:9D:3A:B3:34:36:43:00:64:2C:39:38:08:6F:01:8B:6B:95:39:69:DF:2B:5D:8B:B6:62:42:4A:B0:07:E8:EA:34:F9:02:03:01:00:01*

Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *48:06:DE:BE:8C:87:57:95:80:78:63:FA:9C:23:2B:2B:A0:3A:18:75*

Subject Key Identifier *49:FE:C9:F0:D4:60:CB:DD:F5:07:F6:7F:42:A6:7F:32:85:78:82:EC*

Thumbprint algorithm: *SHA-256*

Thumbprint: *94:95:8D:5A:11:E2:07:6E:1D:5A:BF:7C:02:D6:11:4C:BC:D1:B5:5A:44:B9:7D:0B:4F:4E:E7:A4:DD:97:80:1B*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.13.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *ESTEID-SK 2007 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *Sf7J8NRgy931B/Z/QqZ/MoV4guw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.13.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.13.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *OCSP, ESTEID-SK 2007 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *Sf7J8NRgy931B/Z/QqZ/MoV4guw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-01-04T16:17:06Z*

1.14 - Service (withdrawn): ESTEID-SK 2007 OCSP RESPONDER 2010

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *ESTEID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1259671449*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIESxUPmTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJFRTEiMCAGA1UE
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEPMA0GA1UECxMGRVNURUIEMRcwFQYDVQQDEw5F
U1RFSUQtU0sgMjAwNzAeFw0wOTEyMDExMjQ1MDBaFw0xNjA4MjYxMzIzMDBaMIGHMQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECwwET0NTUDEr
MCkGA1UEAwwiRVNURUIELVNLIDIwMDcgT0NTUCBSRVNQT05ERVIgMjAxMDEYMBYGCSqGSIb3DQEJ
ARYfcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA48byM/QfeIU1Kbu4
AdcAUKXBiwbYbBl4gCltZHC5fZ77fKj2mqfPX2/XW1EqzbVvG0PYIkapkQzBr3R1S6Uaxh1DLC2C
c8BRnqmhXoE03o8En7N9xpN9dGGDBHp2aElBcVVZnAvF4jgbPDCNFAeo3cvpjlx18n0URiVOZFEd
xDvF8PFo/exKXtjRM+jk3K6+9doHYvSXn9klFbT8Wge87Qdll3gQzZE3L8QMXF0z4xbBH1IyTmVL
t5yZ0fxoE0jNlZFvn2w2EDnU4CKfld8w6Zjd5kdxomcwDzGuuLzdjIlPt05USjcY4FHn9YAVKWm
ofYY/o6xOUzU8fAz6yA1tQIDAQABo4IBLzCCASswEwYDVR0lBAwwCgYIKwYBBQUHAwkwaQYDVR0g
BGIwYDBeBgorBgEEAc4fBAECMFAwJQYIKwYBBQUHAgIwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xp
Y3kwJwYIKwYBBQUHAgEWG2h0dHA6Ly93d3cuc2suZWUvYWphdGVtcGVsLzCBiQYDVR0jBIGBMH+A
FEgC3r6Mh1eVgHhj+pwjKyugOhh1oWGkXz8dMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUxCzAJ
BgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlzaZVza3VzMRAwDgYDVQQDEwdK
dXVyLVNLggRFm6ANMB0GA1UdDgQWBBQ4AhAwumZ6EXROIl5wZQXedXpOFDANBgkqhkiG9w0BAQUF
AAOCAQEAJ/LvPUevNRcBp+J78fZRofhk/ifKNLxCUoh8T3MjtU9u5R0KojRlye+1NU8MgH/zrKhr
6TPxuXD0cRrFQ9Hy60lI7lzzaegrQVNgq7UgQlNvCuNxWZcGtEa3ba9M7tBpQeFxqp3CpBytGeVu
Xn65hqOBKdp2YEIMUUkYNAT5A6SSPYLAQgARCI/ydBx+cw0l0fwYvw72FKZa2MIt5DmXBccCtrQ
4I/sb95xfANCNe5n5sBvBhY4F+sIWZUVJ8fTVh7iGaVPSayQfeAAei0m/4/ksiXBwfx6qhzyB3yq
cnSk489oBrrCegua/t+3LizfHpNZvDphKMPuAZ4uheLfQA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ESTEID-SK 2007*

Issuer OU: *ESTEID*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E:	*pki@sk.ee*
Subject CN:	*ESTEID-SK 2007 OCSP RESPONDER 2010*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Tue Dec 01 13:45:00 CET 2009*
Valid to:	*Fri Aug 26 15:23:00 CEST 2016*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E3:CA:72:33:F4:1F:7A:25:35:29:BB:B8:01:D7:00:50:A5:C1:8B:06:D8:6C:19:78:80:29:6D:64:70:B9:7D:9E:FB:7C:A8:F6:9A:A7:CF:5F:6F:D7:5B:51:2A:CD:B5:6F:1B:43:D8:22:46:A9:91:0C:C1:AF:74:75:4B:A5:1A:C6:1D:43:2C:2D:82:73:C0:51:9E:A9:A1:5E:81:34:DE:8F:04:9F:B3:7D:C6:93:7D:74:61:83:04:7A:76:68:49:41:71:55:59:9C:0B:C5:E2:38:1B:3C:30:8D:14:07:A8:DD:CB:E9:8C:8C:75:F2:7D:14:46:25:4E:64:51:1D:C4:3B:C5:F0:F1:68:FD:EC:4A:5E:D8:D1:33:E8:E4:DC:AE:BE:F5:DA:07:62:F4:97:9F:D9:25:15:B4:FC:5A:07:BC:ED:07:65:97:78:10:CD:91:37:2F:C4:0C:5C:5D:33:E3:16:C1:1F:59:72:4E:65:4B:B7:9C:99:D1:FC:68:13:48:CD:95:91:6F:9F:6C:36:10:39:D4:E0:22:9F:21:DF:30:E9:98:DD:E6:47:71:A2:67:30:0F:31:AE:B8:BC:DD:B8:99:65:3E:DD:39:51:22:5C:63:81:47:9F:D6:00:54:A5:A6:A1:F6:18:FE:8E:B1:39:4C:D4:F1:F0:33:EB:20:35:B5:02:03:01:00:01*
Extended Key Usage	*id_kp_OCSPSigning*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.10015.4.1.2* *CPS text: [SK time stamping policy]* *CPS pointer: http://www.sk.ee/ajatempel/*
Authority Key Identifier	*48:06:DE:BE:8C:87:57:95:80:78:63:FA:9C:23:2B:2B:A0:3A:18:75*
Subject Key Identifier	*38:02:10:30:BA:66:7A:11:74:4E:22:5E:70:65:05:DE:75:7A:4E:14*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*09:CD:0B:7E:88:7E:FE:7C:DE:E4:89:F5:6A:F0:63:69:98:4A:33:A1:AA:DE:D7:1B:69:FD:0B:DE:3D:26:8A:94*

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*ESTEID-SK 2007 OCSP RESPONDER 2010*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2018-03-20T07:00:00Z

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.14.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *ESTEID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER 2010*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *OAIQMLpmehF0TiJecGUF3nV6ThQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.14.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.14.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, ESTEID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK 2007 OCSP RESPONDER 2010*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *OAIQMLpmehF0TiJecGUF3nV6ThQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-12-01T13:45:00Z*

1.15 - Service (withdrawn): EID-SK 2007 OCSP RESPONDER

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *EID-SK 2007 OCSP RESPONDER*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1176459405*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDOjCCAiKgAwIBAgIERh9YjTANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJFRTEiMCAGA1UE
ChMZQVMgIi2VydGlmaXRzZWVyaW1pc2tlc2t1czEhMB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3Rl
ZW51c2VkMRQwEgYDVQQDEwtFSUQtU0sgMjAwNzAeFw0wNzA0MTMxMDE2NDVaFw0xMDA0MTcwOTE2
NDVaMH8xCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMQ0w
CwYDVQQLEwRPQ1NQMSMwIQYDVQQDExpFSUQtU0sgMjAwNyBPQ1NQIFJFU1BPTkRFUjEYMBYGCSqG
SIb3DQEJARYJcGtpOHNrLmVlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD+Z0LZ6TjBzx4x
+UshExea1nlMsS86xAN6u/amLV8XQE+vodEld8iqtRsrvFiQ74isYOys1JKqiq+1ryic6j2FnMDZ
ueLiXZI51QWyuhWu+aT4BwEaA8rUxMgKJ94zWksrgSf9cjoaap+9DIDhEsrDa+/89CPl2rlZIB5I
qeHLQQIDAQABo1cwVTATBgNVHSUEDDAKBggrBgEFBQcDCTAfBgNVHSMEGDAWgBQcB/Scv6OlbLO0
nilfH5RIG1h6jTAdBgNVHQ4EFgQUMsMzikmZqG6CcdgnD5VAXfQeCrgwDQYJKoZIhvcNAQEFBQAD
ggEBAH0eUFQ7LznD4R8XWj/6rsNhe0fme3Qs7cyZGNkx1EWenkqdMHCV/qN35yIfrjW7sEjM62sS
1X+8Ke2J+6b5YH0TcSmSDgYICn6zVbsq5MLtHW5wmwKucBJ5xFgoC3NNCEp8wVrzuQmm6xCvFWQV
Q6uNhjuxCQxcDKgLwpL7iEcBEMmTTKkvqEtqrvu/LZ/a2OHytkEoXGheN8KlEclv7AJBPVL8OCv4
UpgyUOrVnmleX2F/KG3wmo4U3kVupuF9kaPrOeOGYG3ZzK2HNwfRNkZ/Ej7AuPazkumAHdsJBbpT
dBYq8d8er8XZkal24Ka/e5eEmcMye+O8IpxAA4ExY+I=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *EID-SK 2007*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Fri Apr 13 12:16:45 CEST 2007*

Valid to: *Sat Apr 17 11:16:45 CEST 2010*

Public Key:

```
30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:FE:67:42:D9:E9:38:C1:CF:1E:31:F9:4B:21:13:17:9A:D6:72:0C:B1:2F:3A:C4:03:7A:BB:F6:
A6:2D:5F:17:40:4F:AF:A1:D1:25:77:C8:AA:B5:1B:2B:BC:58:90:EF:88:AC:60:EC:AC:D4:92:AA:8A:AF:B5:AF:28:9C:EA:3D:85:9C:C0:D9:B9:E2:E2:5D:99:79:D5:05:B2:BA:15:AE:F9:A4:F8:
07:01:1A:03:CA:D4:C4:C8:0A:27:DE:33:5A:4B:2B:A9:27:FD:72:3A:1A:6A:9F:BD:0E:50:E1:12:CA:C3:6B:EF:FC:F4:23:E5:DA:B9:59:20:1E:65:A9:E1:CB:41:02:03:01:00:01
```

Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *1C:07:F4:9C:BF:A4:25:6C:B3:B4:9E:22:1F:1F:94:48:1B:58:7A:8D*

Subject Key Identifier *32:C3:33:8A:49:99:A8:6E:82:71:D8:27:0F:95:40:5D:F4:1E:0A:B8*

Thumbprint algorithm: *SHA-256*

Thumbprint: *78:8C:A8:29:DC:BE:F9:AE:45:47:D8:89:7F:3E:91:C8:9E:56:4C:A1:DA:02:2F:91:2A:12:3D:EF:66:C7:BF:CA*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.15.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *EID-SK 2007 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *MsMzikmZqG6CcdgnD5VAXfQeCrg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.15.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.15.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *OCSP, EID-SK 2007 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *MsMzikmZqG6CcdgnD5VAXfQeCrg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2007-04-13T10:16:45Z*

1.16 - Service (withdrawn): EID-SK 2007 OCSP RESPONDER 2010

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description [en] *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name [en] *EID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

.

Certificate fields details

Version: *3*

Serial Number: *1259667697*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEMTCCAxmgAwIBAgIESxUA8TANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJFRTEiMCAGA1UE
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEhMB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3Rl
ZW51c2VkMRQwEgYDVQQDEwtfSUQtU0sgMjAwNz4eFw0wOTEyMDExMTQxMzBaFw0xNjA4MjYxMzIz
MDBaMIGEMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEN
MAsGA1UECxMET0NTUDEoMCYGA1UEAxMfRUIELVNLIDIwMDcgT0NTUCBSRVNQT05ERVlgMjAxMDEY
MBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
so91KG7EHsjAxMairaCKUHSOyXp5rzxRq5Y9L fDyglVbhffh34fb87M5G+wnu5CZgJsfj7DF3MjpA
7nlAHd5aIAynlUl/CNXejf+XnJ/vyF1eQvAoWvnjBPVIS0mbaABgF54ybAGE2E7UKeZVOAj7RoQV
AMHQcYVjxZW5OWz3yjX9KdaDZPOzqlGtRYKUASHiwAFwExKcqfaHOj0qO8+KdSvEBaVIpe5kunEV
Evn+kgNKBtzdH2XFMjVFa4im31KW+iq7mNQwUiZDSe9ho6T6UrWu7g8yTOowx3SYLTqVxR0YVgcY
NCx7nn1AVGNxK3oeonrHHqc8p6q5AIYXeQNfiIQIDAQABo4HDMIHAMBMGA1UdJQQMMAoGCCsGAQUF
BwMJMGkGA1UdIARiMGAwXgYKKwYBBAHOHwQBAjBQMCUGCCsGAQUFBwICMBkaF1NLIHRpbWUgc3Rh
bXBpbmcgcG9saWN5MCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LnNrLmVlL2FqYXRlbXBlbC8wHwYD
VR0jBBgwFoAUHAf0nL+kJWyztj4iHx+USBtYeo0wHQYDVR0OBBYEFPBOCDPMR+kfp7Ozk5U68E68
/AseMA0GCSqGSIb3DQEBBQUAA4IBAQCRaqmxZgJj+MLamb/P4vy56azr6/tj8dZCK++V/3GnecR
m7CiZpR47EnW0NyDzCecGyTW5kVlnZPnNvXRx700Nn0M4Inia5pNhSuVmW53p5eV70vCbsfRD26+
6CZhkHWnLJ2xpqeacULtgPPz9gBTyC2ybQr17dv7W5Qc+3UFywmE5N8ozQuEJroGz7P+yCbBEss
WcmlUNDNdOOxs6aQZ1f+DV4FUB0lajuILYFz4xM+81akYFVqaGPCVwbQgFSWRKmamj8FxfWjA4DC
rgkHVR1rA3tZyirfCBK9cfWpTCLr8zq9Ur0jTAeGrHRzHIUrB9mYZwyr0kNOyI9293xh

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *EID-SK 2007*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER 2010*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Tue Dec 01 12:41:30 CET 2009*

Valid to: *Fri Aug 26 15:23:00 CEST 2016*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:8F:75:28:6E:C4:1E:C8:C0:C4:C6:A2:AD:A0:8A:50:74:8E:C9:7A:79:AF:3C:
51:AB:96:3D:2D:F0:F2:A6:55:5B:1D:F8:77:E1:F6:C1:EC:CE:46:FB:09:EE:E4:26:60:26:C7:C9:EC:31:77:32:3A:40:EE:79:40:1D:DE:5A:94:0C:A7:21:49:7F:08:D5:DE:8D:FF:97:9C:9F:EF:C8
:5D:5E:42:F0:28:5A:F9:E3:04:F5:48:4B:49:9B:68:00:60:17:9E:32:6C:01:84:D8:4E:D4:29:E6:55:38:08:FB:46:84:15:00:C1:D0:71:85:63:C5:95:B9:39:6C:F7:C8:95:FD:29:D6:83:64:F3:B3
:AA:51:AD:45:82:94:01:21:E2:C0:01:70:13:12:9C:A9:F6:87:3A:3D:2A:3B:CF:8A:75:2B:C4:05:A5:65:A5:EE:64:8A:71:15:12:F9:FE:92:03:4A:06:DC:DD:1F:65:C5:32:35:45:68:88:A6:DF:5
2:96:FA:2A:B8:98:D4:30:52:26:43:49:EF:61:A3:A4:FA:52:B5:AE:EE:0F:32:4D:0A:30:C7:74:98:2D:3A:95:C5:1D:18:56:07:18:34:2C:7B:9E:7D:40:54:63:71:2B:7A:1E:A2:7A:C7:1E:A7:01:
A7:AA:92:00:86:17:79:03:5F:89:02:03:01:00:01
```


Extended Key Usage *id_kp_OCSPSigning*

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.4.1.2

CPS text: [SK time stamping policy]

CPS pointer: http://www.sk.ee/ajatempel/

Authority Key Identifier *1C:07:F4:9C:BF:A4:25:6C:B3:B4:9E:22:1F:1F:94:48:1B:58:7A:8D*

Subject Key Identifier *F0:4E:08:33:CC:47:E9:1F:A7:B3:B3:93:95:3A:F0:4E:BC:FC:0B:1E*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AC:6C:A5:87:4F:5F:13:8F:AD:E1:74:40:1F:A4:1D:8D:EF:1B:67:D7:47:E3:29:9C:83:CC:F4:76:4C:01:4C:57*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *EID-SK 2007 OCSP RESPONDER 2010*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.16.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.16.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *EID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN:	*EID-SK 2007 OCSP RESPONDER 2010*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*8E4IM8xH6R+ns7OTlTrwTrz8Cx4=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

1.16.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.16.3 - History instance n.2 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name	*[en]*	*OCSP, EID-SK 2007 OCSP RESPONDER 2010*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*EID-SK 2007 OCSP RESPONDER 2010*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*8E4IM8xH6R+ns7OTlTrwTrz8Cx4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-12-01T12:41:30Z*

1.17 - Service (withdrawn): KLASS3-SK OCSP RESPONDER 2009

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *KLASS3-SK OCSP RESPONDER 2009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1238049866*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIDzzCCAregAwIBAgIE5cskSjANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDkwMzI2MDY0NDI2WhcNMTIwNTA0MDU0NDI2WjCBgjELMAkGA1UEBhMCRUUx
IjAgBgNVBAoTGUFTIFNlcnRpZmlkc2VlcmltaXNrZXNrdXMxDTALBgNVBAsTBE9DU1AxjjAkBgNV
BAMTHUtMQVNTMy1TSyBPQ1NQIFJFU1BPTkRFUiAyMDA5MRgwFgYJKoZIhvcNAQkBFglwaZlAc2su
ZWUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKi6weNl7Wj7sL6JD4YUNtJXQ79KL53x5m4
QGRsijGJaV5YggE5rJyVZGIsX4FSd9jFiV597ypAUGDbLPf0nDdlSIGtePTzamyETI3Gl6bKfkeU
uIE7D7r7uC+8Fre9iHOOL20+pi7WFzwnyXT9yuWsDeCoKdjQvLpMiq0MBIm9AgMBAAGjgcIwgb8w
EwYDVR0lBAwwCgYIKwYBBQUHAwkwaAYDVR0gBGEwXzBdBgorBgEEAc4tBAECME8wIQYIKwYBBQUH
AgIwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xpY3kwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuc2su
ZWUvYWphdGVtcGVsMB8GA1UdIwQYMBaAFOU/DJ1xPW+8Gb+a9G6/Cf5A652WMB0GA1UdDgQWBBT5
9PTkSlzYXNBxQOnAhgH3BtEDOTANBgkqhkiG9w0BAQUFAAOCAQEAhyI3H6fo1bz3mD0JcD4eY1sI
cwec92Qqkn6i9TsO5TlDQCJkiC/80zlh+H5dgIMcN06gNbr1cWsUw7xAanv2hGIg20IWq7uCyy5L
DghFpO2BWDzTJjmiVTXzyVEvqST0W6efDiwi1tA8H7b+aAzc9ltWm7pYlucGvneKJq07t/UvU9ON
SDUfVLPNMr8sIwCMOexVDZ+eiBIvrLL3N7NouPs7UpFh/+m5JsERmeLbbrNYimHUUn2PJ/trj3kB
EVFToO+nFdBEIfzC3bjSlbPXFxSOL+Aq5gvRlaB4CEWUxa33wzoZNaVpCh5AupxQOGdr4u7ajw5h
kV8Y9VZ7OFejGA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *KLASS3-SK*

Issuer SERIAL NUMBER: *1*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *KLASS3-SK OCSP RESPONDER 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Thu Mar 26 07:44:26 CET 2009*

Valid to: *Fri May 04 07:44:26 CEST 2012*

Public Key: *30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:A8:BA:C1:E3:65:ED:68:FB:B0:BE:89:0F:86:14:36:DF:C9:5D:0E:FD:28:BE:77:C7:99:B8:40:64:6C:8A:31:89:69:5E:58:82:01:39:AC:9C:95:64:69:6C:5F:81:52:77:D2:45:21:5E:7D:EF:2A:40:50:60:DB:2C:F7:F4:9C:37:65:48:81:AD:78:FE:F3:6A:6C:84:4C:8D:C6:23:A6:CA:7E:47:94:B8:81:3B:D3:BA:FB:B8:2F:BC:14:57:BD:88:73:8E:2F:6D:3E:A6:2E:D6:17:3C:27:C9:74:FD:CA:E5:AC:D1:E0:A8:29:D8:D0:BC:BA:4C:8A:AD:0C:04:89:BD:02:03:01:00:01*

Extended Key Usage *id_kp_OCSPSigning*

Certificate Policies *Policy OID: 1.3.6.1.4.1.10015.4.1.2*

CPS text: [SK time stamping policy]

CPS pointer: http://www.sk.ee/ajatempel

Authority Key Identifier *E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*

Subject Key Identifier *F9:F4:F4:E4:48:8C:D8:5C:D0:71:41:09:C0:86:A1:F7:06:D1:03:D1*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6C:66:57:EE:A0:6D:49:46:B4:2A:33:87:F2:AE:CA:02:39:7D:38:84:DE:43:0A:B1:2F:34:39:A6:7D:45:FF:71*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *KLASS3-SK OCSP RESPONDER 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

1.17.2 - History instance n.1 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service Name

Name [en] KLASS3-SK OCSP RESPONDER 2009

Service digital identities

X509SubjectName

Subject E: pki@sk.ee

Subject CN: KLASS3-SK OCSP RESPONDER 2009

Subject OU: OCSP

Subject O: AS Sertifitseerimiskeskus

Subject C: EE

X509SKI

X509 SK I +fT05EiM2FzQcUEJwIah9wbRA9E=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2016-06-30T22:00:00Z

1.17.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

1.17.3 - History instance n.2 - Status: granted

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service Name

Name [en] KLASS3-SK OCSP RESPONDER 2009

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER 2009*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*+fT05EiM2FzQcUEJwIah9wbRA9E=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

1.17.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.17.4 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name	*[en]*	*OCSP, KLASS3-SK OCSP RESPONDER 2009*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER 2009*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *+fT05EiM2FzQcUEJwIah9wbRA9E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-03-26T07:44:26Z*

1.18 - Service (withdrawn): KLASS3-SK 2010 OCSP RESPONDER

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *KLASS3-SK 2010 OCSP RESPONDER*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *203*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIELzCCAxegAwIBAgICAMswDQYJKoZIhvcNAQEFBQAwbTELMAkGA1UEBhMCRUUxljAgBgNVBAoT
GUFTIFNlcnRpZmI0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZmI0c2VlcmltaXNOZWVu
dXNlZDEXMBUGA1UEAxMOS0xBU1MzLVNLIDIwMTAwHhcNMTAwNDA4MDgwMTMxWhcNMTYwODI1MjIw
MDAwWjCBgEYMBYGCSqGSIb3DQE6JARYJcGtpOHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZ
QVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEmMCQGA1UEAxMdS0xBU1Mz
LVNLIDIwMTAgT0NTUCBSRVNQT05ERVlwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDh
WwGpngF0sdGCgOgiyT12A/Vdm9sMPr/cUwZhU7DA5C8rU1yJhbrh28fMpv0eas6/+IC1oDxl24zj
fWKfHwpBmhUTFsmvmKRIu4a1F6VwNw1YEdoAZrQOpzZSve6H6R/+0Uy0BAolebdhPUK22pKd8V1C
BY3de886Ray8uUJu09MAU8J+xsoUNOzyxiWdAVp1YTXRhhUt+EQVYJ2RBZ6++b9fPQvgb9aWgE/W
wqUh7OrgTnrGZVzgO46prfE7zkALG0FYZCzQTCMH8aIqqte0E3HwSVlKh9qwbRPB9WTDCtCqajh4
qgGRTXvWT4vATIHvx8GpJ3roZkp5AlOno3hTAgMBAAGjgcIwgb8waAYDVR0gBGEwXzBdBgorBgEE
Ac4fBAECME8wIQYIKwYBBQUHAgIwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xpY3kwIgYIKwYBBQUH
AgEWGmh0dHA6Ly93d3cuc2suZWUvYWphdGVtcGVsMBMGA1UdIQQMMAoGCCsGAQUFBwMJMB8GA1Ud
IwQYMBaAFF11FBGM9KWOQo97skBEo+7WejtyMB0GA1UdDgQWBBQ3MJkXG2Go/6j4bem465aue3P5
gjANBgkqhkiG9w0BAQUFAAOCAQEAKhoVTIl1ECecFkyt9Ogr0XW3WEFprrqTDE4IycMlx+LNjWk3
0aknMldEtzIC5nCDX27NCWkpbN1o/3ddBvOcKMa05ZK8sHQxU6A5Oev8DCp72/LFEChq5IDqggW2
BiHhyfPfr93JluV03b/Wgq3fpRy8d21VE9254W4A90xeNxDvdpqxIrD2Lonzm/V/oomzEHsp4kKx
XkPmRU4vGtTnxxAnxYp9OuLkvpUCLNoAWMbYqb4cbYzaZ9tQlkBy3nJ352Rs5obYDb3R/ZVWuYLL
SocWL7b2QwIDP7LA8VNDqmQvioHt8GcyKXQ5/eWMvj2ePt58waVhwfSdd4nANKtq1g==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *KLASS3-SK 2010*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject CN: *KLASS3-SK 2010 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

Valid from: *Thu Apr 08 10:01:31 CEST 2010*

Valid to: *Fri Aug 26 00:00:00 CEST 2016*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E1:5B:01:A9:9E:01:74:B1:D1:82:80:E8:22:C9:3D:76:03:F5:5D:9B:DB:0C:3E:BF:DC:53:06:61:53:B0:C0:E4:2F:2B:53:5C:89:85:BA:E1:DB:C7:CC:A6:FD:1E:6A:CE:BF:F8:80:B5:A0:3C:48:DB:8C:E3:7D:62:0A:7C:7C:29:06:68:54:4C:5B:26:BE:62:91:22:EE:1A:D4:5E:95:C0:DC:18:11:DA:00:66:B4:03:A7:36:52:BD:EE:87:E9:1F:FE:D1:4C:B4:04:0A:25:79:B7:61:3D:42:B6:DA:92:9D:F1:5D:42:05:8D:DD:7B:CF:3A:45:AC:BC:B9:42:6E:D3:D3:00:53:C8:FE:C6:CA:14:34:EC:F2:C6:25:9D:01:5A:75:61:35:D1:86:15:2D:F8:44:15:60:9D:B6:44:16:7A:F9:BF:5F:3D:0B:E0:6F:D6:96:80:4F:D6:C2:A5:21:EC:EA:E0:4E:7A:C6:65:5C:E0:3B:8E:A9:AD:F1:3B:CE:40:0B:1B:41:58:64:2C:D0:4C:23:07:F1:A2:2A:AA:D7:B4:13:71:F0:49:59:4A:87:DA:B0:6D:13:C1:F5:64:C3:0A:D0:AA:6A:38:78:AA:01:91:4D:7B:D6:4F:8B:C0:4E:51:EF:C7:C1:A9:27:7A:E8:66:4A:79:02:54:27:A3:78:53:02:03:01:00:01

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.4.1.2

CPS text: [SK time stamping policy]

CPS pointer: http://www.sk.ee/ajatempel

Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *5D:75:14:11:8C:F4:A5:8E:42:8F:7B:B2:40:44:A3:EE:D6:7A:3B:72*

Subject Key Identifier *37:30:99:17:1B:61:A8:FF:A8:F8:6D:E9:B8:EB:96:AE:7B:73:F9:AA*

Thumbprint algorithm: *SHA-256*

Thumbprint: *81:D9:1B:3B:A7:12:F3:3B:83:71:00:52:1E:D8:DF:F8:FB:EE:30:20:B6:85:38:A3:EE:49:9F:B5:5D:1F:62:E9*

X509SubjectName

Subject CN: *KLASS3-SK 2010 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2018-03-20T07:00:00Z

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.18.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *KLASS3-SK 2010 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK 2010 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *NzCZFxthqP+o+G3puOuWrntz+ao=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.18.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.18.3 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *KLASS3-SK 2010 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK 2010 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *NzCZFxthqP+o+G3puOuWrntz+ao=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.18.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.18.4 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *OCSP, KLASS3-SK 2010 OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject CN: *KLASS3-SK 2010 OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Subject E: *pki@sk.ee*

X509SKI

X509 SK I *NzCZFxthqP+o+G3puOuWrntz+ao=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-04-08T08:01:31Z*

1.19 - Service (granted): SK OCSP RESPONDER 2011

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *SK OCSP RESPONDER 2011*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *152345024098107435434516224939977300289*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEvDCCA6SgAwIBAgIQcpyVmdruRVxNgzl3N/NZQTANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMjE0M1oXDTI0MDMxODEwMjE0M1owgZ0xCzAJBgNVBAYTAkVFMQ4wDAYDVQQIEwVlYXJq
dTEQMA4GA1UEBxMHVGFsbGlubjEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEN
MAsGA1UECxMET0NTUDEfMB0GA1UEAxMWUDsgT0NTUCBSRVNQT05ERVIgMjAxMTEYMBYGCSqGSIb3
DQEJARYJcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAihvGyhMVrgRe
HluKln1za6gvCE/mlSREmWjJFpL9lIvuEUZoPFlypYA8g5u1VfgkeW5gDq25jAOq4FyXeDGla+pj
n2h0o2Wc2aeppVG/emfGm/jA8jjeyMrwH8fAJrqVQ7c9X2xSwJEch/P2d8CfMZt5YF6gqLtPvG1b
+n6otBZA5wjlFfJ/nJ8MUvqHSz3+PLfxO2/T3Wyk/c8M9HlMqTelgyiMGRgWehUJ1O6L9armv3d
QrHs1wm6vHaxfpfWB9YAFpeo9aYqhPCxVt/zo2NQB6vxyZS0hsOrXL7SxRToOJaqsnvlbf0erPPF
tRHUvbojYYgl+fzlz0Jt6QJoNwIDAQABo4IBHTCCARkwEwYDVR0lBAwwCgYIKwYBBQUHAwkwHQYD
VR0OBBYEFKWhSGft537Nmj50nCm7vYrecgxZMIGCBgNVHSAEezB5MFcGCisGAQQBzh8EAQIwATA+
BggrBgEFBQcCAjAyHjAUIwBLACAAdABpAG0AZQAgAHMAdABhAG0AcABpAG4AZwAgAHAAbwBsAGkA
YwB5AC4wIwYIKwYBBQUHAgEWG2h0dHBzOi8vd3d3LnNrLmVlL2FqYXRlbXBlbDAfBgNVHSMEGDAW
gBQS8Io+6lYcv80GrPHxJcmpS9QUmTA9BgNVHR8ENjA0MDKgMKAuhixodHRwOi8vd3d3LnNrLmVl
L3JlcG9zaXRvcnkvY3Jscy9lZWNjcmNhLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAw2sKwvThtYGt
D8Jw9mNUuj/mWiBSBEBeY2LhW8V6tjBPAPp3s6iWOh0FbVR2LUyrqRwgT3fyWiGsIDm/6clqM+Ib
ILp/8ztfRQjquhW6XCD9SK02OQ9ZSdBwcmoAApZLGXQC34wdgmV/hLTTNxONnDACBKz9U+Dy9a4Z
T4tpNkbH8jq/BMne8FzbvRt1bjpXBP7gjLX+zdx8/hp0Wq4tD+f9NVX0+vm9ahEKuzx4QzPnSB7h
hWM9OnLZT7noRQa+KWk5c+e5VoR5R2t7MjVl8Cd+2lIxiSxqMSbU5/23BzAKgN+NQdrBZAzpZ7lf
aAuLFaICP+bAm6uW2JUrM6abOw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C:	*EE*
Subject E:	*pki@sk.ee*
Subject CN:	*SK OCSP RESPONDER 2011*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject L:	*Tallinn*
Subject ST:	*Harju*
Subject C:	*EE*
Valid from:	*Fri Mar 18 11:21:43 CET 2011*
Valid to:	*Mon Mar 18 11:21:43 CET 2024*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:8A:1B:C6:CA:13:15:AE:04:5E:1E:5B:8A:96:7D:73:6B:A8:2F:08:4F:E6:95:24:44:99:68:C9:16:92:FD:96:5B:EE:11:46:68:3C:52:32:A5:80:3C:83:9B:B5:55:F8:24:79:6E:60:0E:AD:B9:8C:03:AA:E0:5C:97:78:31:88:6B:EA:49:9F:68:74:A3:65:9C:D9:A7:A9:A5:51:BF:7A:67:C6:9B:F8:C0:F2:38:DE:C8:CA:F0:1F:C7:C0:26:BA:95:43:B7:3D:5F:6C:52:C0:91:1C:87:F3:F6:77:C0:9F:31:9B:79:60:5E:A0:A8:BB:4F:BC:6D:5B:FA:7E:A8:B4:16:40:E7:08:C8:15:F2:7F:8A:72:41:31:4B:EA:1D:2C:F7:F8:F2:DF:C4:ED:BF:4F:75:B2:93:F7:3C:33:D1:C8:32:A4:DE:96:AC:A2:30:64:60:59:E8:62:53:53:AC:2F:D6:AB:9A:FD:DD:42:B1:EC:D7:09:BA:BC:76:B1:7E:97:D6:07:D6:00:16:97:A8:F5:A6:2A:84:F0:B1:56:DF:F3:A3:63:50:07:AB:F1:C9:94:B4:86:C3:AB:5C:BE:D2:C5:14:E8:38:96:AA:B2:7B:E5:6D:FD:1E:AC:F3:C5:B5:11:D4:BD:BA:23:61:88:25:F9:FC:E5:CF:42:6D:E9:02:68:37:02:03:01:00:01*
Extended Key Usage	*id_kp_OCSPSigning*
Subject Key Identifier	*A5:A1:48:61:6D:E7:7E:CD:98:9E:74:9C:29:BB:BD:8A:DE:72:0C:59*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.10015.4.1.2* *CPS text: [SK time stamping policy.]* *CPS pointer: https://www.sk.ee/ajatempel*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*50:D6:2F:37:37:42:28:7B:5F:18:31:9E:51:3C:7B:CA:89:BD:78:78:8B:23:DA:35:61:24:CB:90:F9:A6:36:AF*

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*SK OCSP RESPONDER 2011*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*

Subject L: *Tallinn*

Subject ST: *Harju*

Subject C: *EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.19.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.19.2 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, SK OCSP RESPONDER 2011*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *SK OCSP RESPONDER 2011*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject L: *Tallinn*

Subject ST: *Harju*

Subject C: *EE*

X509SKI

X509 SK I *paFIYW3nfs2YnnScKbu9it5yDFk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-03-18T11:21:43Z*

1.20 - Service (withdrawn): SK Proxy OCSP Responder 2009

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *SK Proxy OCSP Responder 2009*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1242385909*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIEUjCCAzqgAwIBAgIESg1N9TANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDkwNTE1MTExMTQ5WhcNMTIwNTA1MTEwNzE3WjCBgTELMAkGA1UEBhMCRUUx
IjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmltaXNrZXNrdXMxDTALBgNVBAsTBE9DU1AxJTAjBgNV
BAMTHFNLIFByb3h5IE9DU1AgUmVzcG9uZGVyIDIwMDkxGDAWBgkqhkiG9w0BCQEWCXBraUBzay5l
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ6rr1AZFPunWKMJAse70wx9Utc57qgb
rJdk8iiOrcUN2fApNal2wFnRIw9rsF8u9KPu3g47ZSuKX7kpdVVupTwt6gK+brQczfQ5hO3xOGj7
cubcl5+6jDPXSh47zma10hh4tJ5VECOiCDBhIRfA/UjfMYj6BYgEhFuRQxEBgAF5yyEjX1X8Sco/
GQcha4Er5SyEhHvXu/vvg0OVfLRqH/7gGBBRLPMOsDImmXf+C0UYKs7ywFBf+M0VnWH9u0p7E8Xz
A8s3m2ivTdUJYIU5Zy7NFeV9NJgZw3iaLCO1dbV2gBIWpgGvqIwQ3coKHMs3tMBT25+WWmKVMsH
Fi2S4ysCAwEAAaOBwjCBuzATBgNVHSUEDDAKBggrBgEFBQcDCTBoBgNVHSAEYTBfMF0GCisGAQQB
zhBEAQIwTzAlBggrBgEFBQcCAjAZGhdTSyB0aWIlIHN0YW1waW5nIHBvbGlieTAmBggrBgEFBQcC
ARYaaHR0cDovL3d3dy5zay5lZS9hamF0ZW1wZWwwHwYDVR0jBBgwFoAU5T8MnXE9b7wZv5r0br8J
/kDrnZYwHQYDVR0OBBYEFCRXW4FmpJ/GGw3/AXu5czpgogbJMA0GCSqGSIb3DQEBBQUAA4IBAQB9
U7sG/M/w7eXBQh5tDOZ7XLCRmhrmGk9+1RdAP54SmMzc1nngImfgI13ncaizPleu0p8541a51XCY
qOMJbry47YkEnq48ImiAjEpkbaCZsZhX06uUpA9DIstEW/wBZzSCUoGskIb8oIwTWAP97B7trizP
e102hNvD5IMaXrMqaH9hQcoYmKyJHBQnxW2bXxYjeXvIDcAQvevLP8IIOLqdib029GFcM7U889Fa
BcO4cPxx4kITXC2hAvdiZwGuDVAz15Byl8RAfNWrImv+IBRSQpAecnLYozJYyRNcFPrYLd9aXbej
6p6sRCHgC452czoM0VbMmisrK8pm6yZ0j1r+

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *KLASS3-SK*

Issuer SERIAL NUMBER: *1*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *SK Proxy OCSP Responder 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Fri May 15 13:11:49 CEST 2009*

Valid to: *Sat May 05 13:07:17 CEST 2012*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9E:AB:AF:50:19:14:FB:A7:58:A3:09:02:C7:BB:D3:0C:7D:52:D7:39:EE:A8:18:AC:97:64:F2:28:8E:AD:C5:0D:D8:50:29:35:A9:76:C0:59:D1:23:0F:6B:B0:5F:2E:F4:A3:EE:DE:0E:3B:65:2B:8A:29:89:29:75:55:6E:A5:3C:2D:EA:02:BE:6E:B4:1C:CD:F4:12:84:ED:F1:38:28:FB:72:E6:DC:97:9F:BA:8C:33:D7:4A:1E:3B:CE:66:B5:D2:18:78:B4:9E:55:10:23:A2:08:30:61:21:17:C0:FD:42:5F:31:88:FA:05:88:04:84:5B:91:43:11:01:80:01:79:CB:21:09:5F:55:FC:49:CA:3F:19:07:21:6B:81:2B:E5:2C:84:84:7B:D7:BB:FB:EF:83:43:95:7C:B4:6A:1F:FE:E0:18:10:51:2C:F3:0E:B0:32:26:99:77:FE:0B:45:18:2A:CE:F2:C0:50:5F:F8:CD:15:9D:61:FD:BB:4A:7B:13:C5:F3:03:CB:37:9B:68:AF:4D:D5:3F:25:82:14:E5:9C:BB:34:57:95:F4:D2:60:67:0D:E2:68:B0:8E:D5:D6:D5:DA:00:48:5A:98:06:BE:A9:70:43:77:28:28:73:2C:DE:D3:01:4F:6E:7E:59:69:8A:54:CB:07:16:2D:B9:E3:2B:02:03:01:00:01

Extended Key Usage *id_kp_OCSPSigning*

Certificate Policies

Policy OID: 1.3.6.1.4.1.10015.4.1.2

CPS text: [SK time stamping policy]

CPS pointer: http://www.sk.ee/ajatempel

Authority Key Identifier *E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*

Subject Key Identifier *24:57:5B:81:66:A4:9F:C6:1B:0D:FF:01:7B:B9:73:3A:60:A2:06:C9*

Thumbprint algorithm: *SHA-256*

Thumbprint: *87:52:E3:32:39:B3:FE:58:D1:A2:82:70:E4:97:44:40:95:02:F9:AC:23:A8:93:04:C3:90:78:9C:FF:EC:B8:A8*

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *SK Proxy OCSP Responder 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2018-03-20T07:00:00Z

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.20.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.20.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name [en] *SK Proxy OCSP Responder 2009*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *SK Proxy OCSP Responder 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *JFdbgWakn8YbDf8Be7lzOmCiBsk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.20.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.20.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, SK Proxy OCSP Responder 2009*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *SK Proxy OCSP Responder 2009*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *JFdbgWakn8YbDf8Be7lzOmCiBsk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2009-05-15T11:11:49Z*

1.21 - Service (withdrawn): ESTEID-SK OCSP RESPONDER

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*

Service Name

Name *[en]* *ESTEID-SK OCSP RESPONDER*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1016636872*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDuDCCAqCgAwIBAgIEPjilyDANBgkqhkiG9w0BAQUFADB8MRgwFgYJKoZIhvcNAQkBFgIwa2lA
c2suZWUxCzAJBgNVBAYTAkVFM5IwIAYDVQQKExlBUyBTZXI0aWZpdHNlZXIjbWlza2Vca3VzMQ8w
DQYDVQQLEwZFU1RFSUQxCjAIBgNVBAQTATExEjAQBgNVBAMTCUVTVEVJRC1TS2AeFw0wMjAzMjAx
NTA3NTJaFw0wNTAzMjQxNTA3NTJaMGoxCzAJBgNVBAYTAkVFMQ8wDQYDVQQKEwZFU1RFSUQxDTAL
BgNVBAsTBE9DU1AxITAfBgNVBAMTGEVTVEVjRC1TSyBPQ1NOIFJFU1BPTkRFUjEYMBYGCSqGSIb3
DQEJARYjcGtpQHNrLmVlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC10BeCObXZZWcDX298
Wqfd16hpi9tuSbT4L+kowTj+aWz7PDsFpKQWqhxCdlicu67xCT0zAAjaK6x9cwasildre++lkscR
i00w20G5nTPocxpwGTHqwHx4ED7cceK4t4pbj/zB8FluVNVii8ouG9ZEhH76j/lcx0X27Sq5A50C
wwIDAQABo4HXMIHUMBMGA1UdJQQMMAoGCCsGAQUFBwMJMBIGCSsGBAUFBzABBQQFMAMEATAwgYkG
A1UdIwSBgTB/gBR4F7UF+bNY2VmM3mdeRAZMdY2pXaFhpF8wXTEYMBYGCSqGSIb3DQEJARYjcGtp
QHNrLmVlMQswCQYDVQQGEwlFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEQ
MA4GA1UEAxMHSnV1ci1TS4IEPERcgjAdBgNVHQ4EFgQUzpYj2gwIDYK9ahyGyKa0AkK5ys0wDQYJ
KoZIhvcNAQEFBQADggEBADrq0tGkwsrddEqUbsOpXi75Xs4GVkOyseysNqZZCvLqCF7qTSMiC+fz
RxQbXQDhuOT7QQvi3JAoA5zTlm2RvIO1fmrVnJ6CsObjxxvXtcSLI+bICG4uQYgEA+duDRgICpmt
CCjtmxb+2/cSjLGioaKiwm0YwgeEowOgIDMh2o4otm6Fity71GZsZm56U7WkFa7t5wkHKw427iZU
WVrED6W9AfATY14rNnAk8Jqz06w4rPnGE4kYjO+UqMLmFU2KImdrTp1O7h4YLCVIxH/e/He8r7F5
gzXSG4EqID/TMEdCLu7DSWR3SEgJPvKWCpNWzv2DRIdHp+kQO3k+R/f2c80=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *ESTEID-SK*

Issuer SURNAME: *1*

Issuer OU: *ESTEID*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

Valid from: *Wed Mar 20 16:07:52 CET 2002*

Valid to: *Thu Mar 24 16:07:52 CET 2005*

Public Key:


```
30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:B5:D0:17:82:39:B5:D9:65:67:03:5F:6F:7C:5A:A7:DD:D7:A8:69:8B:DB:6E:49:B4:F8:2F:E9
:28:C1:38:FE:69:6C:FB:3C:3B:05:A4:A4:16:AA:1C:42:76:58:9C:BB:AE:F1:09:3D:33:00:08:DA:2B:AC:7D:73:06:AC:88:87:6B:7B:EF:88:92:C7:11:8B:4D:30:DB:41:B9:9D:33:E8:73:1A:70:
19:31:EA:C0:7C:78:10:3E:DC:71:E2:B8:B7:8A:5B:8F:FC:C1:F0:59:6E:54:D5:62:8B:CA:2E:1B:D6:44:84:7E:FA:8F:F2:1C:C7:45:F6:ED:2A:B9:01:2D:02:C3:02:03:01:00:01
```


Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *78:17:B5:05:F9:B3:58:CD:59:8C:DE:67:5E:44:06:4C:75:86:69:5D*

Subject Key Identifier *CE:96:23:DA:0C:25:0D:82:BD:6A:1C:86:C8:A6:B4:02:42:B9:CA:CD*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EA:3D:54:19:15:2B:3F:8A:92:8A:F8:23:EE:BC:CB:D6:3A:68:81:B0:D8:38:CB:05:6F:D9:CD:5C:A4:85:7D:AB*

X509SubjectName

Subject E: *pki@sk.ee*

Subject C: *EE*

Subject O: *ESTEID*

Subject OU: *OCSP*

Subject CN: *ESTEID-SK OCSP RESPONDER*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.21.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.21.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *ESTEID-SK OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *zpYj2gwlDYK9ahyGyKa0AkK5ys0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.21.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.21.3 - History instance n.2 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, ESTEID-SK OCSP RESPONDER*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *ESTEID-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *ESTEID*

Subject C: *EE*

X509SKI

X509 SK I *zpYj2gwlDYK9ahyGyKa0AkK5ys0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2002-03-20T16:07:52Z*

1.22 - Service (deprecatedatnationallevel): KLASS3-SK OCSP RESPONDER (2003)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP*

Service type description	*[en]*	*A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses.*

Service Name

Name	*[en]*	*KLASS3-SK OCSP RESPONDER (2003)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1049195451*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIEPolzuzANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSlb3DQEJARYJcGtp
QHNrLmViMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDMwNDAxMTExMDUxWhcNMDYwNDA1MTAxMDUxWjB9MQswCQYDVQQGEwJFRTEi
MCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEhMB8GA1UE
AxMYS0xBU1MzLVNLIE9DU1AgUkVTUE9OREVSMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALXQF4I5tdlI2wNfb3xap93XqGmL225JtPgv6SjBOP5p
bPs8OwWkpBaqHEj2WJy7rvEjPTMACNorrH1zBgvIh2t774iSxxGLTTDbQbmdM+hzGnAZMerAfHgQ
Ptxx4ri3iluP/MHwWW5U1WKLy4b1k5EfvqP8hzHRfbtKrkBLQLDAgMBAAGjVzBVMBMGA1UdJQOM
MAoGCCsGAQUFBwMJMB8GA1UdIwQYMBaAFOU/DJ1xPW+8Gb+a9G6/Cf5A652WMB0GA1UdDgQWBBTO
liPaDCUNgr1qHlblprQCQrnKzTAN8gkqhkiG9w0BAQUFAAOCAQEAd/8FCyPC9zXxcAZN67KCNU4+
XNJBe+LmG602lBe+lS7Pw4pOgMKebgULKh1fEBHQ2K7F5UWMZdPWkDHaKVRh646yVbFZbfEmKNq4
LhRT13hoUdrG5uRVmCsV03WStgfUVfb1cZf8tD0MIwCmsNXu22k9wykeHaIlpUmGUfbVZyqqfKE2
NVQpm2FULiKWBFKXqbMtW5R3xmDS3bjrAIAdUdYhxhfdCHCphsQf/FJlxb8UFOUa8SeRNr5eL7s8
znLnrC5pKPpWGbUNSlrhLJZHIeXfwbOamae6UVvjto6bMqRe2sxCsMA0dGz+tMigIfmTVInxpEKB
kyvF/on/2qwtVw==
-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *KLASS3-SK*

Issuer SERIAL NUMBER: *1*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *KLASS3-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Tue Apr 01 13:10:51 CEST 2003*

Valid to: *Wed Apr 05 12:10:51 CEST 2006*

Public Key:


```
30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:B5:D0:17:82:39:B5:D9:65:67:03:5F:6F:7C:5A:A7:DD:D7:A8:69:8B:DB:6E:49:B4:F8:2F:E9
:28:C1:38:FE:69:6C:F8:3C:38:05:A4:A4:16:AA:1C:42:76:58:9C:BB:AE:F1:09:3D:33:00:08:DA:2B:AC:7D:73:06:AC:B8:87:6B:7B:EF:B8:92:C7:11:BB:4D:30:DB:41:B9:9D:33:E8:73:1A:70:
19:31:EA:C0:7C:78:10:3E:DC:71:E2:B8:B7:8A:5B:8F:FC:C1:F0:59:6E:54:D5:62:8B:CA:2E:1B:D6:44:84:7E:FA:8F:F2:1C:C7:45:F6:ED:2A:B9:01:2D:02:C3:02:03:01:00:01
```

Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*

Subject Key Identifier *CE:96:23:DA:0C:25:0D:82:BD:6A:1C:86:C8:A6:B4:02:42:B9:CA:CD*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:96:EA:C9:51:18:CC:85:57:43:F3:5D:FB:69:BD:6A:72:E4:3D:33:D1:77:EE:E1:00:E6:3A:5E:29:63:E7:25*

X509SubjectName

Subject E: *pki@sk.ee*

Subject C: *EE*

Subject O: *AS Sertifitseerimiskeskus*

Subject OU: *OCSP*

Subject CN: *KLASS3-SK OCSP RESPONDER*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.22.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.22.2 - History instance n.1 - Status: recognisedatnationallevel

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP*

Service Name

Name *[en]* *KLASS3-SK OCSP RESPONDER (2003)*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*zpYj2gwlDYK9ahyGyKa0AkK5ys0=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*
Status Starting Time	*2016-06-30T22:00:00Z*

1.22.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.22.3 - History instance n.2 - Status: recognisedatnationallevel

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP*

Service Name

Name	*[en]*	*KLASS3-SK OCSP RESPONDER (2003)*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I *zpYj2gwlDYK9ahyGyKa0AkK5ys0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Status Starting Time *2016-06-30T22:00:00Z*

1.22.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.22.4 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP*

Service Name

Name *[en]* *OCSP, KLASS3-SK OCSP RESPONDER (2003)*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *KLASS3-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *zpYj2gwlDYK9ahyGyKa0AkK5ys0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2003-04-01T11:10:51Z*

1.23 - Service (withdrawn): KLASS3-SK OCSP RESPONDER (2006)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

Service type description *[en]*

A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.

Service Name

Name *[en]*

KLASS3-SK OCSP RESPONDER (2006)

Service digital identities

Certificate fields details

Version:

3

Serial Number:

1143114520

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIDXTCCAkWgAwIBAgIERCKLGDANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDYwMzIzMTE0ODQwWhcNMDkwMzI3MTE0ODQwWjB9MQswCQYDVQQGEwJFRTEi
MCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEhMB8GA1UE
AxMYS0xBU1MzLVNLIE9DU1AgUkVTUE9OREVSMRgwFgYJKoZIhvcNAQkBFgIwa2lAc2suZWUwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKKTI8Aex0Gva9eeeBkM3fGTiNOEvjj2McN3tOJBMAEv
G/G7Npu0/2fAEKFFUv4NnPyH3MiC7s6R8PtPMhV5GBG6kWVztL/gQnIJjAbo1l654+jApIQjT3vd
VZDIYy56lKlYoAdG40CgLIVtRihargQ77aziKORkyRfhKZcS0e8tAgMBAAGjVzBVMBMGA1UdJQQM
MAoGCCsGAQUFBwMJMB8GA1UdIwQYMBaAFOU/DJ1xPW+8Gb+a9G6/Cf5A652WMB0GA1UdDgQWBBQU
QsudE6pYaIJSuWuryIGltfy52DANBgkqhkiG9w0BAQUFAAOCAQEAV+Vu+qzrHe7HDjMHq9DdOQTz
833QcMRY0hu5gphMOggNjqjPqTNpHPgNvE6HKGdQ0+VWr8IyRWcxnPMZNihmaCGMpFMpYuH0fx9n
sjXDbjat8MfGuX2m1EADbGOlwjbMuoYTEGEUe3MBeFkmPFDIYpeuS+I4Qv34tOsGvFOpsDkobSATq
4EFw/5hI9WfWaEMYkmBXdeokoVjbNpt+gtdGKNBU42AIxLrcc+Y2AE1hj5qH99/hI0X6r63pTjUb
1ZMRjGQg7ELwmddms7wB5LKKi5kbfmag5hBtDKGs2s0xW1be4yINOrT9lqUYuPn9lwcHNg1I542m
YVChV97Tlt/5vw==

-----END CERTIFICATE-----
```


Signature algorithm:

SHA1withRSA

Issuer CN:

KLASS3-SK

Issuer SERIAL NUMBER:

1

Issuer OU:

Sertifitseerimisteenused

Issuer O:

AS Sertifitseerimiskeskus

Issuer C:

EE

Issuer E:

pki@sk.ee

Subject E:

pki@sk.ee

Subject CN:

KLASS3-SK OCSP RESPONDER

Subject OU:

OCSP

Subject O:

AS Sertifitseerimiskeskus

Subject C:

EE

Valid from:

Thu Mar 23 12:48:40 CET 2006

Valid to:

Fri Mar 27 12:48:40 CET 2009

Public Key: *30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:A2:93:23:C0:1E:C7:41:AF:6B:D7:9E:78:19:0C:DD:F1:93:88:D3:84:BE:38:F6:31:C3:77:B4:E2:41:30:01:2F:1B:F1:BB:36:9B:B4:FF:67:C0:10:A1:45:52:FE:0D:9C:FC:87:DC:C8:82:EE:CE:91:F0:FB:4F:32:15:79:18:11:BA:91:65:73:B4:BF:E0:42:79:48:8C:06:E8:D6:5E:B9:E3:E8:C0:A4:84:23:4F:7B:DD:55:90:C8:63:24:BA:94:A9:58:A0:07:46:E3:40:A0:2E:55:6D:46:28:5A:AE:04:3B:ED:AC:E5:7C:E4:64:C9:17:E1:29:97:12:41:EF:2D:02:03:01:00:01*

Extended Key Usage *id_kp_OCSPSigning*

Authority Key Identifier *E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*

Subject Key Identifier *14:42:CB:9D:13:AA:58:68:82:52:B9:6B:AB:CA:51:88:B5:FC:B9:D8*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CB:16:7D:E2:F0:5B:38:93:1A:BD:F2:96:91:1F:69:51:23:9D:0A:3B:23:62:59:76:62:F2:25:70:EC:3E:9B:0B*

X509SubjectName

Subject E: *pki@sk.ee*

Subject C: *EE*

Subject O: *AS Sertifitseerimiskeskus*

Subject OU: *OCSP*

Subject CN: *KLASS3-SK OCSP RESPONDER*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2018-03-20T07:00:00Z*

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.23.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.23.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *KLASS3-SK OCSP RESPONDER (2006)*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*FELLnROqWGiCUrlrq8pRiLX8udg=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2016-06-30T22:00:00Z*

1.23.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.23.3 - History instance n.2 - Status: granted

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name	*[en]*	*KLASS3-SK OCSP RESPONDER (2006)*

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*KLASS3-SK OCSP RESPONDER*
Subject OU:	*OCSP*
Subject O:	*AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *FELLnROqWGiCUrlrq8pRiLX8udg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.23.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.23.4 - History instance n.3 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC*

Service Name

Name *[en]* *OCSP, KLASS3-SK OCSP RESPONDER (2006)*

Service digital identities

X509SubjectName

Subject E: *pki@sk.ee*

Subject CN: *KLASS3-SK OCSP RESPONDER*

Subject OU: *OCSP*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *FELLnROqWGiCUrlrq8pRiLX8udg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2006-03-23T12:48:40Z*

1.24 - Service (deprecatedatnationallevel): SK Proxy OCSP Responder 2008

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

Service type description *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses.*

Service Name

Name *[en]* *SK Proxy OCSP Responder 2008*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1225186383*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEgTCCA2mgAwIBAgIESQbcTzANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVlMQswCQYDVQQGEwlFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tic2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDgxMDI4MDkzMzAzWhcNMTExMTAyMDgzMzAzWjCBITELMAkGA1UEBhMCRUUx
IjAgBgNVBAoTGUFTIFNlcnRpZmI0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZmI0c2Vl
cmltaXN0ZWVudXNlZDEIMCMGA1UEAxMcU0sgUHJveHkgT0NTUCBSZXNwb25kZXIgMjAwODEYMBYG
CSqGSIb3DQEJARYJcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnguv
UBkU+6dYowkCx7vTDH1S1znuqBusI2TyKI6txQ3YUCk1qXbAWdEjD2uwXy70o+7eDjtlK4opiSI1
VW6IPC3gAr5utBzN9BKE7fE4KPty5tyXn7qMM9dKHjvOZrXSGHi0nlUQI6IIMGEhF8D9Ql8xiPoF
iASEW5FDEQGAAXnLIQfVfxJyj8ZByFrgSvILISEe9e7++++DQSV8tGof/uAYEFEs8w6wMiaZd/4L
RRqqzvLAUF/4zRWdYf275nsTxfMDyzebak9N1T8lgh7InLs0V5X00mBnDejosI7V1tXaAEhamAa+
qXBDdygocyze0wFPbn5ZaYpUywcWLbnjKwIDAQABo4HdMIHaMA4GA1UdDwEB/wQEAwIHgDATBgNV
HSUEDDAKBggrBgEFBQcDCTBoBgNVHSAEYTBfMF0GCisGAQQBzh8EAQIwTzAlBggrBgEFBQcCAjAZ
Ghd7SyB0aW1lIHN0YW1waW5nIHBvbGljeTAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5zay5lZS9h
amFD2lW1wz1WwwHwYDVR0jBBgwFoAU5T8MnXE9b7wZv5r0brBJkDrnZYwHQYDVR0OBBYEFCRXW4Fm
pJ/GGw3/AXu5czpgogbJMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQEFBQADggEBALnuqrbcM13+ISq6
lzlbwaHr6Om2zAiaIZcAAU0i++Iqs1lLTSA/cXoRuUIcjJ54Csh9pVPt3tj76193H57ICkeKE+Yh
pHKFTdD3tPtgAU0prOlwiVq7Gh5MR+sMNX2TKaWTj0qdBVgeui4MB5uWSUWYCNIKnmgoZbV+Zt0A
yBHQVG9oRBqcEK1iPUJwsjkDUdghUHNUTcXpXfiPWCEvhQz+BX3TRMkR4NREvAw7/tfHVtweJi+
mr7RPrbtvdYBjdTppFwZVZDpGC34AM6KtL+mpVeGkK73h5V/pDvQ1rmLQn2L2GJe6n9ztghE/BB5
zYJ1hWACaoJh5IEm+6xNPyU=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer CN: *KLASS3-SK*

Issuer SERIAL NUMBER: *1*

Issuer OU: *Sertifitseerimisteenused*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Issuer E: *pki@sk.ee*

Subject E: *pki@sk.ee*

Subject CN: *SK Proxy OCSP Responder 2008*

Subject OU: *Sertifitseerimisteenused*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

Valid from: *Tue Oct 28 10:33:03 CET 2008*

Valid to: *Wed Nov 02 09:33:03 CET 2011*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9E:AB:AF:50:19:14:FB:A7:58:A3:09:02:C7:BB:D3:0C:7D:52:D7:39:EE:A8:18:AC:97:64:F2:28:8E:AD:C5:0D:D8:50:29:35:A9:76:C0:59:D1:23:0F:6B:B0:5F:2E:F4:A3:EE:DE:0E:3B:65:2B:8A:29:89:29:75:55:6E:A5:3C:2D:EA:02:BE:6E:B4:1C:CD:F4:12:84:ED:F1:38:28:FB:72:E6:DC:97:9F:BA:8C:33:D7:4A:1E:3B:CE:66:B5:D2:18:78:B4:9E:55:10:23:A2:08:30:61:21:17:C0:FD:42:5F:31:88:FA:05:88:04:84:5B:91:43:11:01:80:01:79:CB:21:09:5F:55:FC:49:CA:3F:19:07:21:6B:81:2B:E5:2C:84:84:7B:D7:BB:FB:EF:83:43:95:7C:B4:6A:1F:FE:E0:18:10:51:2C:F3:0E:B0:32:26:99:77:FE:0B:45:18:2A:CE:F2:C0:50:5F:F8:CD:15:9D:61:FD:BB:4A:7B:13:C5:F3:03:CB:37:9B:68:AF:4D:D5:3F:25:82:14:E5:9C:BB:34:57:95:F4:D2:60:67:0D:E2:68:B0:8E:D5:D6:D5:DA:00:48:5A:98:06:BE:A9:70:43:77:28:28:73:2C:DE:D3:01:4F:6E:7E:59:69:8A:54:CB:07:16:2D:B9:E3:2B:02:03:01:00:01

Extended Key Usage *id_kp_OCSPSigning*

Certificate Policies *Policy OID: 1.3.6.1.4.1.10015.4.1.2*

CPS text: [SK time stamping policy]

CPS pointer: http://www.sk.ee/ajatempel

Authority Key Identifier *E5:3F:0C:9D:71:3D:6F:BC:19:BF:9A:F4:6E:BF:09:FE:40:EB:9D:96*

Subject Key Identifier *24:57:5B:81:66:A4:9F:C6:1B:0D:FF:01:7B:B9:73:3A:60:A2:06:C9*

Basic Constraints *IsCA: false*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *98:C5:A4:76:60:44:DC:5C:A4:59:B4:E3:26:C4:9C:54:24:FE:F0:EA:1C:49:BD:4C:D3:12:8B:E9:54:05:01:0C*

X509SubjectName

Subject E: *pki@sk.ee*

Subject C: *EE*

Subject O: *AS Sertifitseerimiskeskus*

Subject OU: *Sertifitseerimisteenused*

Subject CN: *SK Proxy OCSP Responder 2008*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel

Service status description *[en]* *undefined.*

Status Starting Time

2018-03-20T07:00:00Z

Service Supply Points

Service Supply Point *http://ocsp.sk.ee*

1.24.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

1.24.2 - History instance n.1 - Status: recognisedatnationallevel

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

Service Name

Name [en] SK Proxy OCSP Responder 2008

Service digital identities

X509SubjectName

Subject E: pki@sk.ee

Subject CN: SK Proxy OCSP Responder 2008

Subject OU: Sertifitseerimisteenused

Subject O: AS Sertifitseerimiskeskus

Subject C: EE

X509SKI

X509 SK I JFdbgWakn8YbDf8Be7lzOmCiBsk=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel

Status Starting Time 2016-06-30T22:00:00Z

1.24.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

1.24.3 - History instance n.2 - Status: undersupervision

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

Service Name

Name [en] OCSP, SK Proxy OCSP Responder 2008

Service digital identities

X509SubjectName

Subject E:	*pki@sk.ee*
Subject CN:	*SK Proxy OCSP Responder 2008*
Subject OU:	*Sertifitseerimisteenused*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*JFdbgWakn8YbDf8Be7lzOmCiBsk=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2008-10-28T10:33:03Z*

1.25 - Service (withdrawn): SK Time-Stamping Authority for qualified electronic time stamps

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*48765665071482659663074918749208248665*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIQJK/s6xJo0AJUF/eG7W8BWTANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE0
MDkxNjA4NDAzOFoXDTE5MDkxNjA4NDAzOFowYzELMAkGA1UEBhMCRUUxIjAgBgNV BAoMGUFTIFNl
cnRpZml0c2VlcmlteXNrZXNrdXMxDDAKBgNVBAsMA1RTQTEiMCAGA1UEAww2U0sgVElNRVNUQU1Q
SU5HIEFVVEhPUkIUWTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJPa/dQKemSKCNSw
lMUp9YKQY6zQOfs9vgUnbzTRHCRBRdsabZYknxTl4DqQ5+JPgw8MTkDvb6nfDZGd15t4oY4tHXXo
CfRtbMjl9+DV+M7bd+vrBI8vi7DBCM59/VAjx8AuZ9P7Tsg8a88rVqdB9c0ezlSCtFg8X0x2ET3Z
BtZ49UArh/XP07I7eRk/DtSLYauxJDPzXVEZmSJClybcIox93u8F5/o8GvSbD5GYMhfFOJgXmul/
Vz7eR0d5SxCMvJlRrP7WfjlYaUjLYgL2wjFQe/nUltcGCn2KtqGCyH7vl+Xzefea6Xjc8ebTgan2
Fj0UH0mHv98IWADKu1I2fXcCAwEAAaOBgjCBpzAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwHQYDVR0OBBYEFLGwvffmoGkWbCDlUftc9DBic1cnMB8GA1UdIwQYMBaAFBLy
Wj7qVhyzQas8fElyalL1BSZMDOGA1UdHwO2MDQwMqAwoC6GLGh0dHA6Ly93d3cuc2su ZWUvcmVw
b3NpdG9ye59jcmxzL2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQCopcU932wVPD6eed+s
DBht4zt+kMPPFXv1plX0RgbizaKvHWU4oHpRH8zcgo/gpotRLlLhZbHtu94pLFN6enpiyHNwevkm
UyvrBWylONR1Yhwb4dLS8pBGGFR6eRdhGzoKAUF4B4dloXOj4p26q1yYULF5ZkZHxhQFNi5uxak9
tgCFIGtzXumjL5j8mtWeDTGE4YSa34pzDXjz8VAjPJ9sVuOmK2E0gyWxUTLXF9YevrWzRLzVfqw+
qewBVZl4of/6miZOOT2wIA/meL7zr3hnfo7KSJQmMNUjZ6Ih6RBIVvYI0t+A/fpTKiZfviz/Xn2e
4PC6i57wmH5EgOOav0UK

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA256withRSA*

Issuer E:	*pki@sk.ee*
Issuer CN:	*EE Certification Centre Root CA*
Issuer O:	*AS Sertifitseerimiskeskus*
Issuer C:	*EE*
Subject CN:	*SK TIMESTAMPING AUTHORITY*
Subject OU:	*TSA*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*
Valid from:	*Tue Sep 16 10:40:38 CEST 2014*
Valid to:	*Mon Sep 16 10:40:38 CEST 2019*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:93:DA:FD:D4:0A:7A:64:8A:08:D4:B0:94:C5:29:F5:82:90:63:AC:D0:39:FB:3D:BE:05:27:6F:34:D1:1C:24:41:45:DB:1A:6D:96:24:9F:14:C8:E0:3A:90:E7:E2:4F:AB:0F:0C:4E:40:EF:6F:A9:DF:0D:91:9D:D7:9B:78:A1:8E:2D:1D:75:E8:09:F4:6B:6C:C8:C9:F7:E0:D5:F8:CE:DB:77:EB:EB:04:8F:2F:8B:B0:C1:08:CE:7D:FD:50:23:C4:10:2E:67:D3:FB:4E:C8:3C:A3:C0:6B:56:AA:81:F5:CD:1E:CE:54:82:B4:58:3C:5F:4C:76:11:3D:D9:06:D6:78:F5:40:11:87:F5:CF:D3:B2:3B:79:19:3F:0E:D4:8B:61:AB:B1:24:33:F3:5D:51:19:99:22:42:23:26:DC:96:8C:7D:DE:EF:05:E7:FA:3C:1B:24:9B:0F:91:98:32:17:DF:38:98:17:9A:E9:7F:57:3E:DE:47:47:79:4B:10:8C:BC:92:11:AC:FE:D6:7E:22:58:69:48:CB:62:A2:F6:C2:31:50:7B:F9:D4:96:D7:06:0A:7D:8A:B6:A1:82:C8:7E:EF:97:E5:F3:79:F7:9A:E9:78:DC:F1:E6:D3:81:A9:F6:14:9D:14:1F:49:87:BF:DF:25:58:00:CA:B9:32:36:7D:77:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*B1:B0:BD:F7:E6:A0:69:16:6C:20:E5:51:FB:5C:F4:30:62:73:57:27*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
CRL Distribution Points	*http://www.sk.ee/repository/crls/eeccrca.crl*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1E:49:F4:97:D8:9D:43:0A:AD:53:4B:62:2D:82:BD:9B:9D:0D:4A:FD:B7:B7:D3:69:86:C5:DF:09:81:D9:06:7D*

X509SubjectName

Subject C:	*EE*
Subject O:	*AS Sertifitseerimiskeskus*
Subject OU:	*TSA*
Subject CN:	*SK TIMESTAMPING AUTHORITY*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time *2020-09-28T22:01:00Z*

Service Supply Points

Service Supply Point *http://tsa.sk.ee*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.25.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps*

Service digital identities

X509SubjectName

Subject CN: *SK TIMESTAMPING AUTHORITY*

Subject OU: *TSA*

Subject O: *AS Sertifitseerimiskeskus*

Subject C: *EE*

X509SKI

X509 SK I *sbC99+agaRZsIOVR+1z0MGJzVyc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:01:00Z*

1.25.2 - History instance n.2 - Status: withdrawn

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *SK TIMESTAMPING AUTHORITY*

Service digital identities

X509SubjectName

Subject CN:	*SK TIMESTAMPING AUTHORITY*
Subject OU:	*TSA*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*sbC99+agaRZsIOVR+1z0MGJzVyc=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*
Status Starting Time	*2016-06-30T22:00:00Z*

1.25.3 - History instance n.3 - Status: undersupervision

Service Type Identifier	*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name	*[en]*	*SK TIMESTAMPING AUTHORITY*

Service digital identities

X509SubjectName

Subject CN:	*SK TIMESTAMPING AUTHORITY*
Subject OU:	*TSA*
Subject O:	*AS Sertifitseerimiskeskus*
Subject C:	*EE*

X509SKI

X509 SK I	*sbC99+agaRZsIOVR+1z0MGJzVyc=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*
Status Starting Time	*2014-09-16T08:40:38Z*

1.26 - Service (withdrawn): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2019)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2019)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *168600497314008997544586035080465486444*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEFjCCAv6gAwIBAgIQftdGTujTD01cG10EjrASbDANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE5
MDEwMTIxMDAwMFoXDTI0MDEwMTIxMDAwMFowejEnMCUGA1UEAwweU0sgVElNRVNUQU1QSUSHIEFV
VEhPUkIUWSAyMDE5MRcwFQYDVQRhDA5OWFjfFRS0xMDc0N2AxMzEMMAoGA1UECwwDVFNBMRswGQYD
VQQKDBJTSyBjRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAqff9D1IK8LveyTb3tIOjZfc0j+W3uG7czOZuQKigwkxq2jXrqndigVtSZWzN
noO+somaNgXqw0lpu+8P0NdUw+y1a4znJntvf7HK4WNrHO94DcrcxJlRdRkxRH/e3/05E1FpX8B9
6igyieQj9Y3tgHYAf5Mo05j2ANYc/NpF59NWf0nBzJ5QvXD80N1ybiVVu4NALKFxTOEHPRmdFdpt
NNEaipwHyLwaSDpXCtnXxBz6zV/jlsMYCxNl0cXlx+mkD97scmLhGB27rmI8gEPM6Tue0iGp1Tb6
hIFdEQF2gZ8VPOsyJl3cpQd5GRkT63bOtHUm54TYCfw/P7NhO7pFLwlDAQABo4GcMIGZMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUnUvt/uXDNtWuqmMv
TS8vDyrTJxYwHwYDVR0jBBgwFoAUEvJaPupWHL/NBgzx8SXJqUvUFjkwLwYIKwYBBQUHAQEEIzAh
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMA0GCSqGSIb3DQEBCwUAA4IBAQApC2BN
nwqlgm3KsBMbp0lWw2uGVzUXiu4Cfsol6290Jzn6UftA3HjOG33vg5Dl3SV9Z97AfqgbE4A9Czms
8veHwtNRLIaAHuRVm6C/GWa4+nuzNFoAK1pjBGoPWvfYhud/bAlbYY1qF6nHA50/tFT0GGixrnm
I9YsZ0tuXM9pOaoOOYnoCvw8cvMIt68lWqIE5T+OoCZipqdQRZ5IEJTmvE+LLBDuE87orGfxxsws y
+jnOfHX8MLBOhWglrj7RrXLNdKXOlbvhcU3vXl89gKtWWfr+OdVGdJc+/A3wdtTFhNdy7Ce0VlzZ
vmEx/UtUmfF41g/y+3lXOb3h6ipk037x
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject OU: *TSA*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2019*

Valid from: *Tue Jan 01 22:00:00 CET 2019*

Valid to: *Mon Jan 01 22:00:00 CET 2024*

Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A9:F9:7D:0F:59:4A:F0:BB:DE:C9:36:F7:B6:53:89:65:F7:34:27:E5:B7:B8:6E:DC:CC:E6:6E:40:A8:A0:C2:4C:6A:D8:95:EB:AA:77:62:81:5B:52:65:6C:CD:9E:83:BE:B2:89:9A:36:05:EA:C3:49:69:BB:EF:0F:D0:D7:54:C3:EC:B5:6B:8C:E7:26:7B:6F:7F:B1:CA:E1:63:6B:1C:EF:78:0D:CA:DC:C4:82:51:75:19:31:44:7F:DE:DF:FD:12:13:51:69:5F:C0:7D:E8:88:32:8D:E4:23:F5:8D:ED:80:76:00:7D:23:28:D1:28:F6:00:D6:1C:FC:DA:45:E7:D3:56:7F:49:C1:CC:9E:50:BD:70:FC:D0:DD:72:6E:25:55:BB:B3:40:2C:A1:71:4C:E1:07:3D:19:9D:15:DA:6D:34:D1:1A:8A:9C:07:C8:BC:1A:48:3A:57:0A:D9:D7:C4:1C:FA:CD:5F:E3:22:C3:18:0B:13:65:D1:C5:E5:C7:E9:A4:0F:DE:EC:72:62:E1:18:1D:BB:AE:62:3C:A8:43:CC:E9:3B:9E:D2:21:A9:D5:36:FA:84:81:5D:11:01:76:81:9F:15:3C:EB:32:26:5D:DC:A5:07:79:19:19:13:EB:76:CE:B4:75:26:E7:84:D8:09:FC:3F:3F:B3:61:3B:BA:45:2F:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*9D:4B:ED:FE:E5:C3:36:D5:AE:AA:63:2F:4D:20:6F:0F:2A:D3:27:16*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
Authority Info Access	*http://aia.sk.ee/CA*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*25:D4:5A:83:4C:1E:A0:E6:69:A8:A5:88:2D:74:1C:96:18:9F:EF:C0:8F:8C:AE:9A:CC:AB:F7:77:58:33:07:54*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2019*

X509SKI

X509 SK I	*nUvt/uXDNtWuqmMvTSBvDyrTJxY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*

Status Starting Time

2024-02-08T05:00:01Z

Service Supply Points

Service Supply Point	*http://tsa.sk.ee*

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.26.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2019)*

Service digital identities

X509SubjectName

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject OU: *TSA*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2019*

X509SKI

X509 SK I *nUvt/uXDNtWuqmMvTSBvDyrTJxY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-03-10T22:00:00Z*

1.27 - Service (withdrawn): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2020)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2020)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *130547272137066251696452519452253092462*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEFjCCAv6gAwIBAgIQYjZ9dFrZQ6tdpFC5Xj/6bjANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE5
MTIzMTIyMDAwMFoXDTI0MTIzMTIyMDAwMFowejEnMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV
VEhPUklUWSAyMDIwMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD
VQQKDBJTSyBlRCBTb2x1dGlvbnMgQVMxC2AJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAxdOHoD/xEAXVYd6m64QhKHoNZhT5L+wEkO59DH4K8IW1r/kEJusfY60zDY8
o9s96HYACcQOR9Yltg3T3neqRZJ5GEPt5uFzCWzuSdyxIWMacxu/sSYaIn4bqbCd97ML4qVdvwPG
LNGRu8Utuy0JyhyuoBlCHUcgyw1O2ATlc+95zdhGvKq15gazGXTpVUYgLpInkChp1ojZCvWFdKN
3dNGB5tqn3xsdfUfGDWxe4gLFFLeXjxo0pT2Y+5hjF1++r+PlZRnu1LKXEcrHxeyyZ+KL6wSLUyv
fxZ++5hd0wR1pCnVqZ+hfYaGZ+YGRJXtIIA8DFqeKZ6gAhABa6v99QIDAQABo4GcMIGZMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUqD4KKP6RKqGdYfXN
IT35pc1GkjEwHwYDVR0jBBgwFoAUEvjaPupWHL/NBqzx8SXJqUvUFjkwLwYIKwYBBQUHAQEEIzAh
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMA0GCSqGSIb3DQEBCwUAA4IBAQAJ06Qp
/kiOhcNbEsDUVGfLuVycKjEbrGGMWnAj18508aWx7jXtDD9mY5CxtRUI9IbjBJeyI/RtBRDVURt
IioiNckkxC/bOHxiCj2WNCvRxo8GT/qn4M1vV/Sy8vwx/ZlYsZrIRnuo7/dqPsQyxIgRGbUp12bV
KO4KQb4DNOcA6KDwcPd2zv4nBT/4XW7qD07spW9LPVKEvsOU1MV1tznjD0lC5ZL67FdB8kKEjCbb
NfqVLVBOYjBopct5qzTLLPB5LTmV8I281X2TEqeFxbFy+wo7VOT6K36OYSd+9CnPn2M/l6VfrSCl
3OvaWcq+IggGR1kQzDsS4lN1JoyZqd39
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject OU: *TSA*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2020*

Valid from: *Tue Dec 31 23:00:00 CET 2019*

Valid to: *Tue Dec 31 23:00:00 CET 2024*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:D3:87:A0:EF:F1:10:05:D5:61:DE:A6:EB:84:21:28:7A:0D:66:14:F9:2F:EC:
04:90:EE:7D:0C:7E:0A:F2:55:B5:AF:FF:E4:10:9B:AC:7D:8E:B4:CC:36:3C:A3:DB:3D:E8:76:00:09:C4:0E:47:D6:25:B6:0D:D3:DE:77:AA:45:92:79:18:43:ED:E6:E1:73:09:6C:EE:49:DC:B1:
21:63:1A:73:1B:BF:B1:26:1A:96:7E:1B:A9:B0:9D:F7:B3:0B:E2:A5:5D:BF:03:C6:2C:D1:91:BB:C5:2D:BB:2D:09:CA:1C:AE:A0:12:02:1D:47:20:CB:0D:4E:D8:04:E5:73:EF:79:CD:D8:46:BC:
AA:B5:E6:06:B3:19:74:E9:55:46:20:2E:92:27:90:28:69:D6:88:D9:0A:FF:D6:15:D2:8D:DD:D3:46:07:98:6A:9F:7C:6C:75:F5:1F:18:35:B1:7B:88:08:14:52:DE:5E:3C:68:D2:94:F6:63:EE:6
1:24:5D:7E:AF:E3:E5:95:94:67:BB:52:CA:5C:47:2B:1F:17:B2:C9:9F:8A:2F:AC:12:2D:4C:AF:7F:16:7E:FB:98:5D:D3:04:75:A4:29:D5:81:9F:A1:7D:86:86:67:E6:06:44:95:ED:88:80:3C:0C:
5A:9E:29:9E:AA:02:10:3C:6B:AB:FD:F5:02:03:01:00:01
```


Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *A8:3E:0A:28:FE:91:2A:A1:9D:61:F5:CD:95:3D:F9:A5:CD:46:92:31*

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

Authority Info Access *http://aia.sk.ee/CA*

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FD:04:12:2A:D6:30:AA:00:99:87:85:50:D8:38:EB:FA:EC:5D:0F:33:DA:03:5D:0D:09:76:FA:96:70:B1:72:D9*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2020*

X509SKI

X509 SK I	*qD4KKP6RKqGdYfXNlT35pc1GkjE=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*

Status Starting Time

2025-02-14T03:00:00Z

Service Supply Points

Service Supply Point	*http://tsa.sk.ee*

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*
URI	*[et]*	*https://sk.ee/repositoorium/*

1.27.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name	*[en]*	*SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2020)*

Service digital identities

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2020*

X509SKI

X509 SK I *qD4KKP6RKqGdYfXNlT35pc1GkjE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2019-12-03T22:00:00Z*

1.28 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2021)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2021)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *142168993972586756930521877712410666 75*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIEWjCCA0KgAwIBAgIQCrlTQgwdM4hfdZRtSgVwszANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTIw
MTIzMTIyMDAwMVoXDTI1MTIzMTIyMDAwMVowejEnMCUGA1UEAwweU0sgVEIlNRVNUQU1QSU5HIEFV
VEhRUkIlIW5AyMDIxMRcwFQYDVQRhDA5QVFjFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNlBMRswGQYD
VQQKDBJTSyBjRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAwmZuFcXZ3UGPjIEX0mldGSTiUxMcfG8Fh0f4VlAg6aN/buuRVaEpwrS7UfTD
/HFJ0jcJdFf7wTBd+B52oqYhya7rTJd11exeDtwIZpymksqC+F8bWolej3HkSByyGfuGcGGSno
waCJcZgTT2YCT40PdfjfPlaUgobjNC9idFPJFOzgHWu8hUlOAixZ+X22rdCVgTnNW0/xiaRPq/Pg
pgDAsxlYDABonFKiCEfHyK5T1rjV585lfwWBcPo5jnI9tlyT3fSB06QZ0i4rmFcPli/0XvyHrGNN
pJNPJ9Ib9q0VhcPwktoDr2nBFgBzpjRufwVPjQCBuDVidkuMEjLOTwIDAQABo4HgMIHdMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUEDIBfAAH5r+iCV+i
rQKE3Tk2/h8wHwYDVR0jBBgwFoAUIEvjaPupWFHL/NBqzx8SXJqUvUfjkwcwYIKwYBBQUHAQEEZzBl
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMEIGCCsGAQUFBzAChjZodHRwOi8vYy5z
ay5lZS9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlci5jcnQwDQYJKoZIhvcNAQEL
BQADggEBACnGDxtyt0EmeLyGhwW01/rg6q9KStXW65qwNnTdW7QpY+3Q8Oc64zJAAOAkfcaSa1Bq
IJmO7QMkSnpeEa5AH//48bdfZ0RYRGnEpoqg6L5Qi6iCHBduRDxrea0bR7s/UaIB9PMR6jNU7Y4h
SIAZCTxZvsuOwgbYzU1kJipc5mh4nSDU3gyL7vPefgQAgLMQhMI7BZFSHGxGJf+BNOaHzD4IYBRd
81Facnr5+hfD2gNFPcuf9DPFVinKUG9c4XuKj6V30fGBBZoSfju53Jk6/aGfKwKWLpN13Sh4RMb+
KL2S/mDIMKRVCst901nPorgq58Bjd/zm6CptMqABrIpGRl8=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject OU: *TSA*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2021*

Valid from: *Thu Dec 31 23:00:01 CET 2020*

Valid to: *Wed Dec 31 23:00:01 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C2:66:6E:15:C5:D9:DD:41:8F:8C:81:17:D2:69:5D:19:24:E2:53:13:1C:7C:6F:05:87:47:F8:56:50:20:E9:A3:7F:6E:EB:91:55:A1:29:C2:B4:BB:51:F4:C3:FC:71:7B:26:88:DC:26:27:45:7F:BC:13:05:DF:81:E7:6A:2A:62:1C:9A:EE:B4:FF:77:5D:5E:C5:E0:ED:C0:86:69:CA:69:2C:A8:2F:85:F1:B5:A8:95:E2:77:1E:44:81:CB:21:9F:B8:67:06:19:29:E8:C1:A0:A3:71:9A:93:4F:66:02:4F:8D:0F:75:F2:5F:3C:86:94:AA:86:E3:34:2F:62:74:53:FF:14:EC:E0:1D:6B:BC:85:48:8E:02:2C:59:F9:7D:B6:AF:40:95:81:39:CD:5B:4F:F1:89:A4:4F:AB:F3:E0:A6:00:C0:B3:19:58:0C:00:68:9C:52:A2:08:47:C7:C8:AE:53:D6:B8:D5:E7:CE:65:7F:05:81:70:FA:39:8E:72:3D:B4:8C:93:DD:F4:81:D3:A4:19:D2:2E:2B:98:57:0F:96:2F:F4:5E:FC:87:AC:63:4D:A4:93:4F:27:D9:5B:F5:DD:15:85:C3:F0:92:DA:03:AF:69:C1:16:00:73:A6:34:6E:7F:05:4F:8D:00:81:B8:35:62:76:4B:8C:12:32:CE:4F:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Subject Key Identifier *10:32:01:7C:00:07:E6:BF:A2:09:5F:A2:AD:02:84:DD:39:36:FE:1F*

Authority Key Identifier *12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*

Authority Info Access *http://aia.sk.ee/CA*

http://c.sk.ee/EE_Certification_Centre_Root_CA.der.crt

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *57:2B:6C:07:B0:CD:48:48:66:1F:09:97:84:98:A7:AA:96:AC:43:AA:88:D0:C8:2B:77:60:D4:04:6A:70:2B:66*

X509SubjectName

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject OU: *TSA*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING AUTHORITY 2021*

X509SKI

X509 SK I *EDIBfAAH5r+iCV+irQKE3Tk2/h8=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time *2020-11-13T22:00:00Z*

Service Supply Points

Service Supply Point *http://tsa.sk.ee*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.29 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2022)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2022)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *93411973411781417825221539674059615 74*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIEWjCCA0KgAwIBAgIQBwcMIj8ecuJheR6jfOMRZjANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVIMB4XDTIx
MTIzMTIyMDAwMVoXDTI3MTIzMTIyMDAwMVowejEnMCUGA1UEAwweU0sgVEINRVNUQU1QSU5HIEFV
VEhPUkIUWSAyMDIyMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEMMAgGA1UECwwDVFNBMRswGQYD
VQQKDBJTSyBjRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAIgz0fx7rjs9QC/aFmkHHiuLWTxxJCBGzK/SB9tEYp5fK0++TnO0by6de2cDf
nmin3Yk3F840xLM4gms8M4Fu/MOVG17Alv0vua4ygRmhH7O2dWM8lTyi+8sRuyeQC4o9+LS9aCzE
SZUKyYlf/KsM4DYqIE254mzU8YodMqoHPwsp4gAev+1zP2hdzQfQBbO9+cviCpzBjcEtHJquQH6W
7waIBOMhrXMQBlOuj6qVkKUbvDN1spOcmLWGY1NooF2JlOyCPyzLSxa1tivhHNb3edLCRuklZwo
1yco67/yJHxIwH36hX6Al/s1btXYg+GRL602Rk7VBzTc30dhPLZIPwIDAQABo4HgMIHdMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUsnUQr3QDlUM34ksg
HzFY59QFNQcwHwYDVR0jBBgwFoAUEvjaPupWHL/NBqzx8SXJqUvUFJkwcwYIKwYBBQUHAQEEZzBl
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMElGCCsGAQUFBzAChjZodHRwOi8vYy5z
ay5lZS9FRV9DZXI0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlc5jcnQwDQYJKoZIhvcNAQEL
BQADggEBABlnW9utp6qGo1QB57aGQ3tKST+f9aFmceDMZ+w0XGuQ+W/m4YKnVDmb0O8a+TykHaQn
wD7obf6hA8zV3NXFAW6JmLiy4wycnJwKPS3qmZ42dPANtlq3upvgPzMhbCzGaXxRZZrfb4ikZGSP
Jreer6Sgymv4wZku21Com1xFY52sQQdB2C43/cQwur9XqxXWoiS+ZSrNrU0RUu0h4YN5pM6WcGx
gcNOqul7vtkWS060QgmWss0I2n9rgfd+RVziKAr/364DCR++VCWcUj0uiCgmpo5a/NHUcy0BTX6
dTgOOcFAxLwQR4uOmAPEFPpKhX6PRfZL5o1yBW8cO3EemxU=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C: *EE*

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2022*
Valid from:	*Fri Dec 31 23:00:01 CET 2021*
Valid to:	*Fri Dec 31 23:00:01 CET 2027*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:96:0C:F4:7F:1E:EB:8E:CF:50:0B:F6:85:9A:41:C7:22:E2:D6:4F:1C:49:08:11:B3:2B:F4:81:F6:D1:18:A5:27:CA:D3:EF:93:9C:E3:9B:CB:A7:5E:D9:C0:DF:9E:68:A7:DD:89:37:17:CE:34:C4:B3:38:82:6B:3C:33:81:6E:FC:C3:95:1B:5E:C0:96:FD:2F:B9:AE:32:81:19:A1:1F:B3:B6:75:63:3C:95:3C:A2:FB:CB:11:BB:27:90:0B:8A:3D:F8:B4:BD:68:2C:C4:49:95:0A:C9:89:5F:FC:AB:0C:E0:36:2A:20:4D:B9:E2:6C:D4:F1:8A:1D:32:AA:07:3F:0B:29:E2:00:1E:BF:ED:73:3F:68:5D:CD:07:D0:05:B3:BD:F9:CB:E2:0A:9C:C1:8D:C1:2D:1C:9A:AE:40:7E:96:EF:06:88:04:E3:21:AD:73:10:04:83:AE:BF:AA:95:90:A5:1B:BC:33:75:B2:94:1C:98:B5:86:63:53:68:A0:5D:A5:25:0C:82:3F:2C:CB:4B:16:B5:B4:88:AF:84:73:5B:DD:E7:4B:09:1B:A4:95:9C:28:D7:27:28:E9:3F:F2:24:7C:48:C0:7D:FA:85:7E:80:27:FB:35:6E:D5:D8:83:E1:91:2F:AD:36:46:4E:D5:07:34:DC:DF:47:61:3C:B6:48:3F:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*B2:75:10:AF:74:03:21:43:37:E2:4B:20:1F:31:58:E7:D4:05:35:07*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
Authority Info Access	*http://aia.sk.ee/CA* *http://c.sk.ee/EE_Certification_Centre_Root_CA.der.crt*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*27:B3:CD:A7:A2:1E:D1:09:CE:56:A0:A0:D9:95:12:CE:D5:63:64:5B:D8:C0:51:51:71:95:7B:6C:90:B0:C2:1A*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2022*

X509SKI

X509 SK I	*snUQr3QDIUM34ksgHzFY59QFNQc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time

2021-12-27T22:00:24Z

Service Supply Points

Service Supply Point *http://tsa.sk.ee*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.30 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2023)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2023)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *67205934710543798222704146034089873665*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgIQMo9kZ98gZ1djdKF45mVRATANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VyqGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTIy
MTIzMTIyMDAwMVoXDTI4MTIzMTIyMDAwMVowejEnMCUGA1UEAwweU0sgVEIlNRVNUQU1QSU5HIEFV
VEhPUklUWSAyMDIzMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD
VQOKDBJTSyBjRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVfMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAnefs1HxAHAVoc7labGuHXp4IrX1cC9hDa/lidDrodPiFF6y+8EAQEzP22Lkr
rxPVybrep3kodxFj4aVw4i6Q3c8EYyLE1gbbtrB4vTxeQIB2f2HGZ56Hr3uNj8JD+/iFvCe/5iAE
so8dRVSX48kRRe8viAw6fnlrXb+8iyff8y0VlcfSveNLiQXkYNB+TxQ0f/5+PCTIFez4plzw8p0Z
SIddUzIdx2beyspNhAiju1cgy/bMULscvBj7YbFKZ4TmsUZHZuQc59MjaIJderIwtV/tLBrg3OqR
5nDq1Ol+aukjMNQX3fS76yXIPnwte2I3+0GrEGYst9yfpQk8c0xdcwIDAQABo4HgMIHdMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUuTR73sWfYH5L+mH3
/RD0UAIC7egwHwYDVR0jBBgwFoAUEvJaPupWHL/NBqzx8SXJqUvUFjkwcwYIKwYBBQUHAQEEZzBl
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMElGCCsGAQUFBzAChjZodHRwOi8vYy5z
ay5lZS9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV95Sb290X0NBLmRlc5jcnQwDQYJKoZIhvcNAQEL
BQADggEBACQXxeUVbmIeij5NIN3f7Iv426xyTHXIxaxTh3T6MrLnVOBtCxa99jqKTG6Ljz1N6m/w
E3GSnLVDL5Q77FqhJRasiyl3JlUjz82n0GL4L+C1jiW+n5dy6nUJUnSDHZhhD3LfnHxWLLfyRyWm
DltXVHhU6Sgn2syAUrZ/alzufY++iX0yoWYaMKhgfyz848r+nh+sK2pVp5rVT57D7x5+xFWDeyLQ
jhe9tHmXyGCyyjlSChg+3cV+oQUY6VeMWS40+8E+rAHtxgvhN3YiSDGvOdNct6whea+daYyuJqu4
emGCDHKa63iPSXhuD2c/AhiqSesCuRsRCEVNr/iLC5Il37Q=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer E: *pki@sk.ee*

Issuer CN: *EE Certification Centre Root CA*

Issuer O: *AS Sertifitseerimiskeskus*

Issuer C:	*EE*
Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2023*
Valid from:	*Sat Dec 31 23:00:01 CET 2022*
Valid to:	*Sun Dec 31 23:00:01 CET 2028*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9D:E7:EC:D4:7C:40:1C:05:68:73:B2:1A:6C:6B:87:5E:9E:08:AD:7D:5C:0B:D8:43:6B:F9:62:74:3A:E8:74:F8:85:17:AC:BE:F0:40:10:13:33:F6:D8:B9:2B:AF:13:D5:C9:BA:DE:A7:79:28:77:11:63:E1:A5:70:E2:2E:90:DD:CF:04:63:22:C4:D6:06:DB:B6:B0:78:BD:3C:5E:40:80:76:7F:61:C6:67:9E:87:AF:7B:BD:8F:C2:43:FB:F8:85:BC:27:BF:E6:20:04:B2:8F:1D:45:54:97:E3:C9:11:45:EF:2F:88:0C:3A:7E:78:9F:5D:BF:BC:BB:27:DF:F3:2D:15:21:C7:D2:BD:E3:4B:89:05:E4:60:D0:7E:4F:14:34:7F:FE:7E:3C:24:C8:15:EC:F8:A4:8C:F0:F2:9D:19:48:87:5D:53:39:5D:C7:66:DE:CA:CA:4D:84:08:A3:BB:57:20:CB:F6:CC:50:BB:1C:BF:C8:FB:61:B1:4A:67:84:E6:B1:46:47:66:E4:1C:E7:D3:23:6A:58:DD:7A:B9:70:B5:5F:ED:2C:1A:E0:DC:EA:91:E6:70:EA:D4:E8:BE:6A:E9:23:30:D4:17:DC:54:BB:EB:25:E5:3E:7C:2D:7B:69:77:FB:41:AB:10:66:2C:B7:DC:9F:A5:09:3C:73:4C:5D:73:02:03:01:00:01*
Extended Key Usage	*id_kp_timeStamping*
Subject Key Identifier	*B9:34:7B:DE:C5:9F:60:7E:4B:FA:61:F7:FD:10:F4:50:09:42:ED:E8*
Authority Key Identifier	*12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99*
Authority Info Access	*http://aia.sk.ee/CA* *http://c.sk.ee/EE_Certification_Centre_Root_CA.der.crt*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*AF:1F:E6:65:62:A3:A7:CE:B9:9A:41:E5:B0:9B:6D:C4:67:49:03:6F:64:1B:2D:ED:17:FE:44:75:F2:2B:E6:C0*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject OU:	*TSA*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING AUTHORITY 2023*

X509SKI

X509 SK I	*uTR73sWfYH5L+mH3/RD0UAlC7eg=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2022-12-31T22:00:00Z

Service Supply Points

Service Supply Point *http://tsa.sk.ee*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

1.31 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2024E)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2024E)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *168860431470254928716508813509924923249*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDjzCCAxWgAwIBAgIQfwIWDTXOBgXEqiABoa6ncTAKBggghkjOPQQDAjBdMRgwFgYDVQQDDA9T
SyBUU0EgQ0EgMjAyM0UxFzAVBgNVBGEMDk5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBjRCBT
b2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTIzMTAwMTExMzE1OFoXDTMwMDQwMTExMzE1N1ow
aDEjMCEGA1UEAwwaU0sgVEINRVNUQU1QSU5HIFVOSVQgMjAyNEUxFzAVBgNVBGEMDk5UUkVFLTEw
NzQ3MDEzMRswGQYDVQQKDBJTSyBjRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAE6ie8TjQ1MsNdMX7X2fCAkHYLZZH24Jt4pSa4rxsKEvobnpZ1r6kk
Z8idEAS2+06sr6eRvDKAPbCEs0ZStuBf6KOCAaowgqGrmMB8GA1UdIwQYMBaAFFoYwDTO17eZ3wiQ
wAR9GPNzlr3PMGYGCCsGAQUFBwEBBFowWDAzBggrBgEFBQcwAoYnaHR0cHM6Ly9jLnNrLmVlL1NL
X1RTQV9DQV8yMDIzRS5kZXluY3J0MCEGCCsGAQUFBzABhhVodHRwOi8vb2NzcC5zay5lZS90c2Ew
gZ4GA1UdIASBljCBkzCBkAYGBACPegECMIGFMDsGCCsGAQUFBwIBFi9odHRwczovL3d3dy5za2lk
c29sdXRpb25zLmV1L2VuL3JlcG9zaXRvcnkvdHNhLzBGBggrBgEFBQcCAjA6DDhUU1Ugr2VydGim
aWNhdGUgaGFzIGllZW4gaXNzdWVkIGFjY29yZGluZyB0byBOQ1ArlHBvbGljeTAWBgNVHSUBAf8E
DDAKBggrBgEFBQcDCDAzBgNVHR8ELDAqMCigJqAkhjodHRwOi8vYy5zay5lZS9za190c2FfY2Ff
MjAyM2UuY3JsMB0GA1UdDgQWBBT05pTRiTTkkODyNnyZ/S6xX8UKUzAOBgNVHQ8BAf8EBAMCBsAw
CgYIKoZIzj0EAwIDaAAwZQIwGO/wcHlvgTdwZcargDFjnao48XZI6QpoTrPQzFhpOXuB4TFweq0/
knkExnTAPUE/AjEA+5Rae12eOciDTXgkq95jRyTMoKx7Gvg8OievvYOJLVpFHGKlnEC2aliFtc8O
fldS

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withECDSA*

Issuer C: *EE*

Issuer O: *SK ID Solutions AS*

Issuer 2.5.4.97: *NTREE-10747013*

Issuer CN: *SK TSA CA 2023E*

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2024E*
Valid from:	*Sun Oct 01 13:31:58 CEST 2023*
Valid to:	*Mon Apr 01 13:31:57 CEST 2030*
Public Key:	*30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:EA:27:BC:4E:34:35:32:C3:5D:31:7E:D7:D9:F0:80:90:76:0B:65:91:F6:E0:9B:78:A5:26:B8:AF:1B:0A:12:FA:1B:9E:96:75:AF:A9:24:67:C8:9D:10:04:B6:FB:4E:AC:AF:A7:91:BC:32:80:15:B0:84:B3:46:52:B6:E0:5F:E8*
Authority Key Identifier	*5A:18:C0:34:CE:D7:B7:99:DF:08:90:C0:04:7D:18:F3:73:96:BD:CF*
Authority Info Access	*https://c.sk.ee/SK_TSA_CA_2023E.der.crt* *http://ocsp.sk.ee/tsa*
Certificate Policies	*Policy OID: 0.4.0.2042.1.2* *CPS pointer: https://www.skidsolutions.eu/en/repository/tsa/* *CPS text: [TSU certificate has been issued according to NCP+ policy]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://c.sk.ee/sk_tsa_ca_2023e.crl*
Subject Key Identifier	*F4:E6:94:D1:89:34:E4:90:E0:F2:36:7C:99:FF:9E:B1:5F:C5:0A:53*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*84:E0:29:3A:C6:DE:1C:3C:D1:B4:20:A3:C8:45:3D:27:9D:29:27:50:3C:32:64:59:58:35:17:D3:5D:9A:A6:45*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2024E*

X509SKI

X509 SK I	*9OaU0Yk05JDg8jZ8mf+esV/FClM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2023-11-07T22:00:18Z

Service Supply Points

Service Supply Point *http://tsa.sk.ee/ecc*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.32 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2024R)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2024R)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *72101065433466638175204307345381995791*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIG+zCCBOOgAwIBAgIQNj4o++yE3RYvac/itJs1DzANBgkqhkiG9w0BAQwFADBdMRgwFgYDVQQD
DA9TSyBUUO0EgQ0EgMjAyM1IxFzAVBgNVBGEMDk5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJ
RCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTIzMTAwMTExMzMwMloXDTMwMDQwMTExMzMw
MVowADEjMCEGA1UEAwwaU0sgVEINRVNUQU1QSU5HIFVOSVQgMjAyNFIxFzAVBgNVBGEMDk5UUkVF
LTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAoon1w0AzSATQU8rFn8Fn+2Bt+I6YjyW7KmHGRVMN
hIAA2A3w4Xr7XAfpMRIGiCQZaENUJO22ENN5YwJufcnMB8Bgh5Gigm6n4UbjgW4XAFjuzuD33mRY
t7U2FS28YtibgJVXM8oeIXFISdTYm2WnkNhKAwMgG+QPyiM2RiAgOj/lmKGUNXDBIzmWc8oAPu+f
7YHwIWCmg+dikH3OaxNNLCMIdMAy1oJBK0ZfqnbOFZ4eqPSht2LvMmmIW7AixHWI+/iG/L9RGXju
niIHcHvBUYGR7L9pzl2GLWFw9b9HV4QEZXf7HWVPsTu6xb733x/+5JlbkyjLUO2TQ2/JscmF9lZp
RqCNoX+gNgRkVE+qlbbc16xSVA+W8Zc+LAG5PyxjDfDWLusShB3CNuRECUCcIeM/r/42ueDN58YS
jOVGzhoAk0oiYSngnqtbgJYWwQb5NcYcB56EioXusMxn0SFHyTsRudpJ2lmM9PREW52LGTLm0/Vw
WMsB+FPgN/HXLOmYmdJA5zEfU3oEzxnkPsdazb53PARxgCZKpoRPNBHqLJ1oMTakZvDuT/ubGqsR
jJLwNqOxfZ2bguPb9d9dwsYyxYWc85La0mRdH/VHrduGYfA/fTMrPGCn+XXnJUx1ZBgyh5AK7p1N
KnJnJyhEBuaEDmFI0RyJh5jY5P/+ID+A9sUCAwEAAaOCAaowggGmMB8GA1UdIwQYMBaAFP25tFTt
uXdg0bHtjiWEEhVKeplZMGYGCCsGAQUFBwEBBFowWDA2BggrBgEFBQcwAoYnaHR0cHM6Ly9jLnNr
LmVlL1NLX1RTQV9DQV8yMDIzUi5kZXIuY3J0MCEGCCsGAQUFBzABhhVodHRwOi8vb2NzcC5zay5l
ZS90c2Ewg24GA1UdIASBjjCBkzCBkAYGBACPegECMIGFMDsGCCsGAQUFBwIBFi9odHRwczovL3d3
dy5za2lkc29sdXRpb25zLmV1L2VuL3JlcG9zaXRvcnkvdHNhLzBGBggrBgEFBQcCAjA6DDhUU1Ug
Y2VydGlmaWNhdGUgaGFzIGlZW4gaXNzdWVkIGFjY29yZGluZyBO6yBOQ1ArIHBvbGljeTAWBgNV
HSUBAf8EDDAKBggrBgEFBQcDCDAzBgNVHR8ELDAqMCigJqAkhjodHRwOi8vYy5zay5lZS9za190
c2FfY2FfMjAyM3IuY3JsMB0GA1UdDgQWBBSuR4OucOcshpn/hL1pLtS7TB+ONTAOBgNVHQ8BAf8E
BAMCBsAwDQYJKoZIhvcNAQEMBQADggIBAKGSNmtz7gwfeQwxMe2tSd2g1PhL6IOf8n33igry2NA8
F51kaRjAd+0wENvmoNROSHEpZ6+YlFYurj8bfpgl30LopxlI1/0X+Hqk3shrDpz7/bXij+nh7S1h
UKTLH1J6cS869RP7XZhzGiIlgvWUuOF77ODum+tePuggBPrvfGf9HwgdVbPKEm0tRZL/BiL5md6/
tJWB0BeZnOA4075dK4+DTGJdEeu4CVji9bF5ndNkwXK+EVX8GVTf4xSMTcScB7Ha13lbGmlWQj
YdTG5dTteAolpkeuuCcu+1DMpQxTkKfEEpmztOWgAxQ7zr9HK1oqPNgf9eJVTuLcwBK6IpqOPB0
JCVOmUPBC3lY5TcDOxnt3xrbsn58VHfIhkFsqwFmrwvnHcjVPtDMuX/iIWDu3/rp3j5imMGGi3KR
Up8r8FOy3S1Yg7tF4nFCx5eFIrIbGmATekFRgxgHv/YNu2b+Ft+yWvygrdY1Fj+G4BnWBi5W30BG
nY5fsTbEU9JSXj/O3W5FnJKHiBWnpu2iwk1HI3KEk8nH8ekcEgI1M4gfY6L6xMp6JOYYmZnhYAtV
ruUM55IjmKu2/rhDCI0Y9a8eq8XKB/qEmBTJUx3L2FBD150kUvvhg2hYBF7nuDk1Q8AxGiYVs9XT
mI3e4klnJM/vgZy1IdWG1IDytKzOuCOm

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer C: *EE*

Issuer O:	*SK ID Solutions AS*
Issuer 2.5.4.97:	*NTREE-10747013*
Issuer CN:	*SK TSA CA 2023R*
Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2024R*
Valid from:	*Sun Oct 01 13:33:02 CEST 2023*
Valid to:	*Mon Apr 01 13:33:01 CEST 2030*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A2:89:F5:C1:00:33:48:04:D0:53:CA:C5:9F:C1:67:FB:60:6D:F8:8E:98:27:25:BB:2A:61:C6:45:53:0D:84:80:00:D8:0D:F0:E1:7A:FB:5C:07:E9:31:19:46:8B:24:19:68:43:54:24:EC:F6:10:D3:79:63:02:6E:7D:C9:CC:07:C0:60:87:91:A2:82:6E:A7:E1:46:E3:81:6E:17:00:52:6E:CE:E0:F7:DE:64:58:B7:B5:36:15:2D:BC:62:D8:9B:80:95:57:33:CA:1E:95:71:48:49:D4:D8:9B:65:A7:90:D8:4A:03:03:20:1B:E4:0F:CA:23:36:46:20:20:42:3F:CB:98:A1:94:35:70:C1:23:39:96:73:CA:00:3E:EF:9F:ED:81:F0:21:60:A6:83:E7:62:90:7D:CE:6B:13:4D:2C:23:25:74:C0:32:D6:82:41:2B:46:5F:AA:76:CE:15:9E:1E:A8:F4:A1:B7:62:EF:32:69:88:5B:B0:22:C4:75:A5:FB:F8:86:FC:BF:51:19:78:EE:9C:88:87:70:7B:C1:51:81:91:EC:BF:69:CC:8D:86:2D:61:70:F1:BF:47:57:84:04:65:77:FB:1D:65:4F:B1:3B:BA:C5:BE:F7:DF:1F:FE:E4:92:5B:93:28:CB:50:ED:93:43:6F:C9:B1:C9:85:F6:56:69:46:A0:8D:A1:7F:A0:36:04:64:54:4F:AA:95:B6:DC:D7:AC:52:54:0F:96:F1:97:3E:2C:01:92:3F:2C:63:0D:F0:D6:2E:EB:12:84:1D:C2:36:E4:44:09:40:9C:95:E3:3F:AF:FE:36:B9:E0:CD:E7:C6:12:8C:E5:46:CE:1A:00:93:4A:22:61:29:E0:9E:AB:5B:80:96:16:C1:06:F9:35:C6:1C:07:9E:84:8A:85:EE:B0:CC:67:D1:21:47:C9:3B:11:B9:DA:49:DA:59:8C:F4:F4:44:5B:9D:8B:19:32:E6:D3:F5:70:58:CB:01:F8:53:EA:37:F1:D7:2C:E9:98:99:D2:40:E7:31:1F:53:7A:04:CF:19:E4:3E:C7:5A:CD:BE:77:3C:04:71:80:26:4A:A6:84:4F:34:11:EA:2C:9D:68:31:36:A4:66:F0:EE:4F:FB:9B:1A:0B:11:8C:92:F0:36:A4:31:7D:9D:9B:82:E3:DB:F5:DF:5D:C2:C6:32:C5:85:9C:F3:92:DA:D2:64:5D:1F:F5:47:AD:DB:86:61:F0:3F:7D:33:2B:3C:60:A7:F9:75:E7:25:4C:75:67:C8:32:87:90:0A:EE:9D:4D:2A:72:67:27:28:44:06:E6:84:0E:61:65:D1:1C:89:87:98:D8:E4:FF:FE:94:3F:80:F6:C5:02:03:01:00:01*
Authority Key Identifier	*FD:B9:B4:54:ED:B9:77:60:D1:B1:ED:26:25:84:12:15:4A:7A:92:19*
Authority Info Access	*https://c.sk.ee/SK_TSA_CA_2023R.der.crt* *http://ocsp.sk.ee/tsa*
Certificate Policies	*Policy OID: 0.4.0.2042.1.2* *CPS pointer: https://www.skidsolutions.eu/en/repository/tsa/* *CPS text: [TSU certificate has been issued according to NCP+ policy]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://c.sk.ee/sk_tsa_ca_2023r.crl*
Subject Key Identifier	*AE:47:83:AE:70:E7:2C:86:99:FF:84:BD:69:2E:D4:BB:4F:CF:8E:35*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*63:B3:7B:65:60:C9:AA:F7:23:75:5C:CE:A7:C4:EA:94:32:DD:B7:A5:06:F3:4D:C6:14:43:45:3B:B2:92:D8:4A*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING UNIT 2024R*

X509SKI

X509 SK I *rkeDrnDnLIaZ/4S9aS7Uu0/PjjU=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2023-11-07T22:00:00Z

Service Supply Points

Service Supply Point *http://tsa.sk.ee/rsa*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

URI *[et]* *https://sk.ee/repositoorium/*

1.33 - Service (granted): KLASS3-SK ORG 2021E qualified certificate for electronic seal

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *KLASS3-SK ORG 2021E qualified certificate for electronic seal*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *420108968431287616103734969243263365 00*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDiDCCAuggAwIBAgIQH5sBIc4ZTj1hWvEFaRQX9DAKBggqhkjOPQQDAzBmMQswCQYDVQQGEwJF
RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEh
MB8GA1UEAwwY0sgSUQgU29sdXRpb25zIFJPT1QgRzFFMB4XDTlxMTAwNDEyMTgxMloXDTM2MTAw
NDEyMTgxMlowZzELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIElEIFNvbHV0aW9ucyBBUzEXMBUG
A1UEYQwOTlRSRUUtMTA3NDcwMTMxIjAgBgNVBAMMGVNLIEIEIFNvbHV0aW9ucyBPUkcgMjAyMUUw
djAQBgcqhkjOPQIBBgUrgQQAIgNiAAT5UvjTY26GyX5dkIOsjGOvy4W1MFXjWgXW3q9aqT1yuEOU
yuPnHtm/fTUiIXY5PCVviBhdqubUdP/U9bxOs6M6oTptGU95JgQ7JY9tK4HbpJPk+J3Iz1JHMqq3
JCktyUWjggFaMIIBVjAfBgNVHSMEGDAWgBSGdE866zjysKfu7bmFm52DCUUxazAdBgNVHQ4EFgQU
/Inn/EN4/+wsw4Sod4DJf0ga1CgwDgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAfBCAQAw
bQYIKwYBBQUHAQEEYTBfMCAGCCsGAQUFBzABhhRodHRwOi8vb2NzcC5zay5lZS9DQTA7BggrBgEF
BQcwAoYvaHR0cDovL2Muc2suZWUvU0tfSURfU29sdXRpb25zX1JPT1RfRzFFLmRlci5jcnQwLwYD
VR0fBCgwjjAkoCKgIIYeaHR0cDovL2Muc2suZWUvU0tfUk9PVF9HMUUuY3JsMFAGA1UdIARJMEcw
RQYEVR0gADA9MDsGCCsGAQUFBwIBFi9odHRwczovL3d3dy5za2lkc29sdXRpb25zLmV1L2VuL3Jl
cG9zaXRvcnkvQ1BTLzAKBggqhkjOPQQDAwOBiwAwgYcCQXOIw72bQj2lOzbDp3xy5TIFrgBPQBlN0
YbWV+TSenzGfqT6aOjHTZ9migRQeEXw97kXLSD3wN/g9LQ9Ok1dZVDQ3AklAt+bOVtVzJr+43e8I
Fl4Cot5wPywcml042EtuAT1SJ7lOkIUoaQZ6ZPj3pnl+5wX+z6s753MznY97AdwpGvEADkE=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN:	*SK ID Solutions ROOT G1E*
Issuer 2.5.4.97:	*NTREE-10747013*
Issuer O:	*SK ID Solutions AS*
Issuer C:	*EE*
Subject CN:	*SK ID Solutions ORG 2021E*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*
Subject C:	*EE*
Valid from:	*Mon Oct 04 14:18:12 CEST 2021*
Valid to:	*Sat Oct 04 14:18:12 CEST 2036*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:F9:52:F2:53:63:6E:86:C9:7E:5D:90:83:AC:8C:63:AF:CB:85:B5:30:55:E3:5A:05:D6:DE:AF:5A:A9:3D:72:B8:43:94:CA:E3:E7:1E:D9:BF:7D:35:22:21:76:39:3C:25:6F:88:18:5D:AA:E6:D4:74:FF:D4:F5:BC:4E:B3:A3:3A:A1:3A:6D:19:4F:52:26:04:3B:25:8F:6D:2B:81:DB:A4:93:E4:F8:9D:C8:CF:52:47:32:AA:B7:24:29:2D:C9:45*
Authority Key Identifier	*86:74:4F:3A:EB:38:F2:B0:A7:EE:ED:B9:85:9B:9D:83:09:45:31:6B*
Subject Key Identifier	*FC:89:E7:FC:43:78:FF:EC:2C:C3:84:A8:A3:80:E3:23:48:1A:D4:28*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://c.sk.ee/SK_ID_Solutions_ROOT_G1E.der.crt*
CRL Distribution Points	*http://c.sk.ee/SK_ROOT_G1E.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.skidsolutions.eu/en/repository/CPS/*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*EC:57:02:F3:9E:83:5E:12:DA:BE:D3:F3:19:E3:41:1E:78:37:74:98:C2:11:A7:E1:DC:5C:37:6E:F1:74:C3:81*

X509SubjectName

Subject CN:	*SK ID Solutions ORG 2021E*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I */Inn/EN4/+wsw4Soo4DjI0ga1Cg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2024-10-17T01:00:00Z*

1.33.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.33.2 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.33.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.33.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.33.5 - Extension (critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description

1.33.6 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KLASS3-SK ORG 2021E*

Service digital identities

X509SubjectName

Subject CN: *SK ID Solutions ORG 2021E*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *lnn/EN4/+wsw4Soo4DjI0ga1Cg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-02-08T05:00:41Z*

1.33.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.33.6.2 - Extension (critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.33.6.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.33.6.4 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.33.6.5 - Extension (critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description

1.34 - Service (granted): KLASS3-SK ORG 2021R qualified certificate for electronic seal

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *KLASS3-SK ORG 2021R qualified certificate for electronic seal*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *104631294886120067599766131374780892342*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGszCCBJugAwIBAgIQTrdBH/kVRQFhWvLs8/TEtjANBgkqhkiG9w0BAQwFADBmMQswCQYDVQQG
EwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAx
MzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzF5MB4XDTIxMTAwNDEyMjYyMFoXDTM2
MTAwNDEyMjYyMFowZzELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIEIEIFNvbHV0aW9ucyBBUzEX
MBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxIjAgBgNVBAMMGVNLIEIEIFNvbHV0aW9ucyBPUkcgMjAy
MVIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCv5cBZz+xsh2xEQ3R4grPzjzzjuRk
HXs0xfNVhNhJG8WZh6NldtL8HJPVT1PD8au9ism51NJMirstdbuYVBuoGXIBF+I/lg0M4KaLEDb1w
gz/BXhBgRDMXjGdqIv24MnPx5Il0qTb2G7pBauksvTlOKWncM1CvcBA46zWjXHRGNv87BJcACaaU
9/DA4hZZ1/my0Z+d+Fdh2YNCgfXWEJ8Sz3UVO16QMas2g8mL5vsp/0Viy4HAX5Gw+XwUmU+HKqdt
Hf0iW0zjTdUafOPdrbt0fr1ivIi9FtZ9CpBXxUPdgC798VnK3jsaUwGwIKhXf7coT+6uIGSvERGCe
WQ9yLfoswAieqDZ7Zp7iDG6CTMvMfn+dTdfHqmklWG2jYcFW9QVoCyQKTjvZfxtO1xAcVavvgXa+v
aXX8EsyQqnYF7Zkp5PzB5/x9jmX70HBHEPc1CLarxYpMLLPc3FqtMiX2wVqv5HtfKuE8Q6xqmcQW
Mbjl51xHBrMOD51ahOs3W9bq6NT/BsHvzZ+fSFcjRjh4Jq7OFN/ymA0hD4+rbrixgpkj3w1iA2mL
yPT5BfwL2fEGMxtWxFj7y2ET2XN/mW34+CqyJcQHRYeXs9/Bvg1iXiRyTCZA0MkwBZ8E56PyXbNn
hH6AOMg7S1YQ7yXFXzES5Eja7mBZI5jPq4t/FThzPHnwwwIDAOAB0dIBWj/CCAVYwHwYDVR0jBBgw
FoAUlQ23ZBjCpptmdti8/JpajLwo1s0wHQYDVR0OBBYEFOLGphjgoLJ8oWgse1E8b2HyKY2MA4G
A1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMG0GCCsGAQUFBwEBBGEwXzAgBggrBgEF
BQcwAYUaHR0cDovL29jc3Auc2suZWUvQ0EwOwYIKwYBBQUHMAKGL2h0dHA6Ly9jLnNrLmVlL1NL
XDIEX1NvbHV0aW9uc195T09UX0cxUi5kZXIuY3J0MC8GA1UdHwQoMCYwJKAioCCGHmh0dHA6Ly9j
LnNrLmVlL1NLX1JPT1RfRzFSLmNybDBQBgNVHSAESTBHMEUGBFUdIAAwPTA7BggrBgEFBQcCARYv
aHR0cHM6Ly93d3cuc2tpZHNvbHV0aW9ucy5ld59lbi9yZXBvc2I0b3J5L0NQUy8wDQYJKoZIhvcN
AQEMBQADggIBAC/df7QO74rBXo+wQnChGnbtpWZSdISgqMKtBhO3hAvy7s27odXThZi9fLPEpqw9
Cl5NSeGz6e5HGc258o4kYzhymMLF7Hyne255OVvfj25XMtXOR23MGC4Yn1ogZXNPlaZULvty/1Uz
SLbjdGDnkfdHWTEPJPskXH51CM70ZM2wGtfAjPRW90wThSZAh6CS/KNlJTTOJYMDYknQPTESiUV3
3YiB7xL5wV/9ymoM03lvZ0ew0ktY1YNsfr4eb3FfcFmCiXMRmPYbdncxBvyzLXxHoZtZJq2y3SHp
Pb1fqWv+LQC6+c3YeEYYyzNVwCgpdOpvr3QU6imr2H8elcKCe5unD+glFZC4+ITcF56RLQ/uzddw
ez+QYjWylg9ZEwfvZZOqoWzvhxNlgr2yUs8cPV6rK3l+STVvS4BgwsGQlvrbddwIlNHDVHbO3h6z
SkjqUhYcAHWCHzptbjtI5GOVs/55m2/knIrxl8MuDXPl5h2PosaVqO7dI+2SI/rpDTwyPlfnwdV8
vKS6m81yc7H2pn29EspMBTE6/dRoaq2q0B17lt9jutkEus8QCbuFWs0avUnmDALgZq2qBg878WF
SEIxS87EJ6X/zFm9kf/u+4aCN9hul2YzqQ/saFpWsvg083GHz1gNiikXYeUwygZmqqOj8tbX+thc
E+XU/HSLWlHR

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA384withRSA*
Issuer CN:	*SK ID Solutions ROOT G1R*
Issuer 2.5.4.97:	*NTREE-10747013*
Issuer O:	*SK ID Solutions AS*
Issuer C:	*EE*
Subject CN:	*SK ID Solutions ORG 2021R*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*
Subject C:	*EE*
Valid from:	*Mon Oct 04 14:26:20 CEST 2021*
Valid to:	*Sat Oct 04 14:26:20 CEST 2036*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AF:E5:CF:19:CF:EC:6C:87:6C:44:43:74:78:82:B1:69:66:3C:F3:26:E4:64:1D:7B:34:C6:15:47:36:12:46:F1:66:61:E8:D9:5D:B4:B0:47:24:F5:53:D4:F0:FC:6A:EF:62:B2:6E:75:34:93:22:AE:CB:5D:6E:E6:15:06:EA:06:5C:80:5F:FB:5F:E5:83:43:38:29:A2:C4:39:BD:70:83:3F:C1:5E:10:60:44:33:17:8C:67:6A:96:FD:B8:32:73:F1:E4:89:74:A9:36:F6:1B:BA:41:6A:E9:2C:BD:32:0E:29:69:DC:33:50:AF:70:10:38:EB:35:A3:5C:74:46:36:FF:3B:04:97:00:09:A6:94:F7:F0:C0:E2:16:59:D7:F9:B2:D1:9F:9D:F8:57:61:D9:83:42:A9:F5:D6:10:9F:12:CF:75:15:38:5E:90:31:AB:36:83:C9:8B:E6:FB:29:FF:45:62:CB:81:C0:5F:91:B0:F9:7C:14:99:4F:87:2A:A7:6D:1D:FD:22:5B:4C:E3:4D:D5:1A:7C:E3:DD:AD:BB:74:7F:58:AF:22:2F:45:B5:9F:42:A4:15:F1:50:F7:60:0B:BF:7C:56:72:B7:8E:C6:94:C0:6C:25:2A:15:DF:ED:CA:13:FB:AB:A5:19:2B:C4:44:60:9E:59:0F:72:2D:FA:2C:C0:08:9E:A8:36:7B:66:9E:E2:0C:6E:82:4C:CB:CC:7E:7F:9D:4D:D1:EA:9A:42:16:1B:62:58:70:55:BD:41:5A:02:C9:02:93:8E:F6:5F:C6:D3:B5:C4:07:15:6A:FB:E0:5D:AF:AF:69:75:FC:12:CC:90:AA:76:05:ED:99:29:E4:FC:C1:E7:FC:7D:8E:65:FB:D0:70:47:10:F7:35:08:B6:AB:C5:8A:4C:2C:B3:DC:DC:5A:AD:32:25:F6:C1:5A:AF:E4:7B:5F:2A:E1:3C:43:AC:6A:99:C4:16:31:B8:E5:E7:5C:47:06:B3:0E:0F:9D:5A:84:EB:37:5B:D6:EA:E8:D4:FF:06:C1:EF:CD:9F:9F:48:57:23:46:38:78:26:AE:CE:14:DF:F2:98:0D:21:0F:8F:AB:6E:B8:B1:82:99:09:DF:0D:62:03:69:8B:C8:F4:F9:05:FC:0B:D9:F1:06:33:1B:56:C4:58:FB:CB:61:13:CD:73:7F:99:6D:F8:F8:2A:B2:25:C4:07:45:87:97:B3:DF:DB:BE:0D:62:5E:24:72:4C:26:40:D0:C9:30:F1:9F:04:E7:A3:F2:5D:B3:67:84:7E:80:38:C8:3B:4B:56:10:EF:25:C5:5F:31:12:10:96:89:EE:60:59:97:98:CF:83:8B:7F:15:38:73:3C:79:F0:C3:02:03:01:00:01*
Authority Key Identifier	*95:0D:B7:64:18:C2:A6:9B:66:76:D8:FC:FC:9A:5A:24:BC:28:D6:CD*
Subject Key Identifier	*E2:C6:A6:18:E0:A0:B2:49:F2:85:A0:B1:ED:44:F1:BD:87:C8:A6:36*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://c.sk.ee/SK_ID_Solutions_ROOT_G1R.der.crt*
CRL Distribution Points	*http://c.sk.ee/SK_ROOT_G1R.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.skidsolutions.eu/en/repository/CPS/*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*B6:82:82:50:C1:9C:96:10:4A:AA:F3:09:28:C4:0C:CE:D2:61:8F:B5:55:C5:E9:B5:14:A1:7C:13:7C:8F:56:BA*

X509SubjectName

Subject CN:	*SK ID Solutions ORG 2021R*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *4samGOCgsknyhaCx7UTxvYfIpjY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2024-10-17T01:00:00Z

1.34.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.34.2 - Extension (not critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.34.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.34.4 - Extension (not critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.34.5 - Extension (not critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

1.34.6 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KLASS3-SK ORG 2021R*

Service digital identities

X509SubjectName

Subject CN: *SK ID Solutions ORG 2021R*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *4samGOCgsknyhaCx7UTxvYfIpjY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-02-08T05:00:37Z*

1.34.6.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

1.34.6.2 - Extension (not critical): Qualifiers [QCQSCDStatusAsInCert]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:0.4.0.194112.1.3*

Description *Any certificate that is issued under the CA/QC Sdi certificate and that is issued as a QC (i.e. containing a QcCompliance statement) and having its Certificate Policy PolicyIdentifier OID set as 0.4.0.194112.1.3, is to be considered as supported by a QSCD. They are issued for digital stamping according to eIDAS regulation*

1.34.6.3 - Extension (not critical): Qualifiers [QCForLegalPerson]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

Criteria list assert=atLeastOne

Key Usage *[nonRepudiation]* *true*

Key Usage *[nonRepudiation]* *false*

Description *Any certificate issued under the CA/QC Sdi certificate and is issued as a QC (i.e. containing a QcCompliance statement) is to be considered as issued to a Legal Person*

1.34.6.4 - Extension (not critical): Qualifiers [QCStatement]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.34.6.5 - Extension (not critical): Qualifiers [QCForESeal]

Qualifier type description *[en]* *undefined.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

1.35 - Service (granted): EID-SK-Q 2021E qualified certificates for electronic signatures

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK-Q 2021E qualified certificates for electronic signatures*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *161893725775996041986690601031977427171*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDizCCAuygAwIBAgIQecuY8QtlSqphWu7gI1Bg4zAKBggqhkjOPQQDAzBmMQswCQYDVQQGEwJF
RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFjFRS0xMDc0NzAxMzEh
MB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzFFMB4XDTIxMTAwNDEyMDkwNFoXDTM2MTAw
NDEyMDkwNFowaTELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIEIiEIFNvbHVOaW9ucyBBUzEXMBUG
A1UEYQwOTlRSRUUtMTA3NDcwMTMxJDAiBgNVBAMMG1NLIElEIFNvbHV0aW9ucyBFSUQtUSAyMDIx
RTB2MBAGByqGSM49AgEGBSuBBAAiA2IABARd6setRXHlBuFzkZJwxhF6JYTAU79CeQhtlCvctME5
AaGKUGbIox+ssIrWmh5mCkbpyWjmsiqYhn3gyKmfmCdmjB09rOdKwz522D1m+UWFDQnwKVD/LBFi
fq2WMjQDj6OCAVowggFWMBBGA1UdIwQYMBaAFIZ0TzrrOPKwp+7tuYWbnYMjRTFrMB0GA1UdDgQW
BBTolOaPYRI99x/BLk/8FI8tC4LYHDAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIB
ADBtBggrBgEFBQcBAQRhMF8wIAYIKwYBBQUHMAGGFGh0dHA6Ly9vY3NwLnNrLmVlL0NBMDsGCCsG
AQUFBzAChi9odHRwOi8vYy5zay5lZS9TS19JRF9Tb2x1dGlvbnNfUk9PVF9HMUUuZGVyLmNydDAv
BgNVHR8EKDAmMCSgIqAghh5odHRwOi8vYy5zay5lZS9TS195T09UX0cxRS5jcmwwUAYDVR0gBEkw
R2BFBgRVHSAAMD0wOwYIKwYBBQUHAgEWL2h0dHBzOi8vd3d3LnNraWRzb2x1dGlvbnMuZXUvZW4v
cmVwb3NpdG9yeS9DUFMvMAoGCCqGSM49BAMDA4GMADCBiAJCANcDgGx2tAky5vu1LoyXKPqe7DlW
o/kDv6GR30OSYxB4FOm9xslclKUSObuyTs5vNY8yqk8souAMMShajbW8G49BAkIA6+WMbJjw3Wly
7ezIxciQkKV4ODVK+fUxIP6a3CJ35bhsGOnUQ/Dand5syDuxAYzXJQD3XqzO+QpYFu9fDuXej6k=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *SK ID Solutions ROOT G1E*

Issuer 2.5.4.97: *NTREE-10747013*

Issuer O:	*SK ID Solutions AS*
Issuer C:	*EE*
Subject CN:	*SK ID Solutions EID-Q 2021E*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*
Subject C:	*EE*
Valid from:	*Mon Oct 04 14:09:04 CEST 2021*
Valid to:	*Sat Oct 04 14:09:04 CEST 2036*
Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:04:5D:EA:C7:AD:45:71:E5:06:E1:73:91:92:70:C6:11:7A:25:84:C0:53:BF:42:79:08:6D:94:2B:DC:B4:C1:39:01:A1:8A:50:66:E5:A3:1F:AC:B0:8A:D6:9A:1E:66:0A:46:E9:C9:62:66:B2:2A:98:86:7D:EA:C8:A9:9F:98:27:66:8C:1D:3D:AC:E7:4A:C3:3E:76:D8:3D:66:F9:45:85:0D:09:F0:29:50:FF:2C:11:62:7E:AD:96:30:94:0E:8F*
Authority Key Identifier	*86:74:4F:3A:EB:38:F2:B0:A7:EE:ED:B9:85:9B:9D:83:09:45:31:6B*
Subject Key Identifier	*E8:94:E6:8F:61:12:3D:F7:1F:C1:2E:4F:FC:14:8F:2D:0B:82:D8:1C*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Info Access	*http://ocsp.sk.ee/CA* *http://c.sk.ee/SK_ID_Solutions_ROOT_G1E.der.crt*
CRL Distribution Points	*http://c.sk.ee/SK_ROOT_G1E.crl*
Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: https://www.skidsolutions.eu/en/repository/CPS/*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*3B:35:5E:9B:66:4D:F0:FA:3F:CC:92:22:72:5A:94:11:D7:22:07:E3:18:AC:9E:F1:02:8B:21:1F:E0:3A:10:52*

X509SubjectName

Subject CN:	*SK ID Solutions EID-Q 2021E*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*
Subject C:	*EE*

X509SKI

X509 SK I *6JTmj2ESPfcfwS5P/BSPLQuC2Bw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2024-10-17T01:00:00Z*

1.35.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.35.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.18.1*

Description *Certificate Policy for Qualified Mobile-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.35.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK-Q 2021E qualified certificates for electronic signatures*

Service digital identities

X509SubjectName

Subject CN: *SK ID Solutions EID-Q 2021E*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *6JTmj2ESPfcfwS5P/BSPLQuC2Bw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-10-17T01:00:00Z*

1.35.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.35.3.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.17.2*

Description *Certificate Policy for Qualified Smart-ID*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.18.1*

Description *Certificate Policy for Qualified Mobile-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.35.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK-Q 2021E*

Service digital identities

X509SubjectName

Subject CN: *SK ID Solutions EID-Q 2021E*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *6JTmj2ESPfcfwS5P/BSPLQuC2Bw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-02-08T05:00:01Z*

1.35.4.3 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.35.4.4 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.17.2*

Description *Certificate Policy for Qualified Smart-ID*

Policy Identifier:

Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.10015.18.1*
Description		*Certificate Policy for Qualified Mobile-ID*
Description		*All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.36 - Service (granted): EID-SK-Q 2021R qualified certificates for electronic signatures

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]*

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

Service Name

Name *[en]*

EID-SK-Q 2021R qualified certificates for electronic signatures

Service digital identities

Certificate fields details

Version:

3

Serial Number:

746484452877302363572926908628739753 17

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIGtTCCBJ2gAwIBAgIQOCjEgffj3n9hWvHCGo8aFTANBgkqhkiG9w0BAQwFADBmMQswCQYDVQQG
EwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAx
MzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzFSMB4XDTIxMTAwNDEyMjEyMloXDTM2
MTAwNDEyMjEyMlowaTELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEiNLIEIEIFNvbHVoaW9ucyB8UzEX
MBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxJDAiBgNVBAMMG1NLIEIEIFNvbHVOaW9ucyBFSUQtUSAy
MDIxIjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMw6wtLCsUzKKXHy7e1T/8tzpQzc
EDt8lhIfj53+KELujxXOhdVk5SoPvv3YOb5vXjhvGpaaOOMRxwQCBxFv5qQ3ZGtvc8Uyd8pxpKi/
VHI3CUAXmPIt7/Cx7cH7+zT0YyE41RT2bRpsxzU2LMfIckJloSO+CeBStcaSZJ23LW/MXbegtmOo
orU68fg82HIJOuFxv5NZNIQdsh03ZedRveEBkATyp4WjCTZtlyUKSIeKxzRDAtvuZhAui6w84bt
VtUic6K/BuN6hHxwMR8uvInIZ76a/9n2N2t7JgYx8qoaq5dte8oqpSOucr1Y8imr+3T4byRZlL3E
HK4I33q0+4lCZSjy7UbMRfpz8DcuFGFX59tnDlaOD2UlsgP/dU28i6jruQOol6X6Z+LQ/8OGgxXT
/nbJzgROs/KrrCUI20d4jOe79PT532wVeOhWc8+ethQd0sjLEV/1tRd55SqLGlBmv/+IPRVPdlk86
kS1TQP/PwKVU2kH5loaYmhzlqLTp/ir0yFj5+0T5OcfBUuBFazomdhPHNcy6PmaOQnV7rE92OFiV
FiZLPfcSBmnCW9Zeeq05kvljbDmJnjmYihyQwcOQr4iIn458bPPFm18gxlVVn8mJAi/8Z37wNtAD
GS2Hj4xd+L5dQTHijDOKwlnzVGc/8HI5Cy3tixi7U8vmSMN3AgMBAAGjggFaMIIBVjAfBgNVHSME
GDAWgBSVDbdkGMKmm2Z22Pz8mlokvCjWzTAdBgNVHQ4EFgQUpW/ifkyViDntwvVH12J+c6YD1YYw
DgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwbQYIKwYBBQUHAQEEYTBfMCAGCCsG
AQUFBzABhhRodHRwOi8vb2Nzcc5zay5lZS9DQTA7BggrBgEFBQcwAoYvaHR0cDovL2Muc2suZWUv
U0tfSURfU29sdXRpb25zX1JPT1RfRzFSLmRIci5jcnQwLwYDVR0fBCgwJjAkoCKgIlYeaHR0cDov
L2Muc2suZWUvU0tfUk9PVF9HMVluY3JsMFAGA1UdIARJMEcwRQYEVR0gADA9MDsGCCsGAQUFBwIB
Fi9odHRwczovL3d3dy5zaZlkc29sdXRpb25zLmV1L2VuL3JlcG9zaXRvcnkvQ1BTLzANBgkqhkiG
9w0BAQwFAAOCAgEAoLWe39b3tLZlKYJEIR55D9hP2VyRQ6v9bhKKNa+DiVxvlvpgRKEu1L0Obys+
Bu3h04HtzxS+smrLKVTCK7cQn4tdMkoVEU70KXjCknza1pgl5Z4R24T2R/iakhGt6Go38m5kfGMZ
7iv3N7ooFcWrptk/PjhGNxjcC/tBkNsGgrJoJpa5uHUsT8dB1PHNTod2oLZhrRGKQl63Ahwa4NCx
Rlu9972Kuxgph+ARbkIUR9GzF5e75D5XA8nGxOILN/YbDQpN+PKvyumI4eKfQEDyu2w1/+Gkqz/k
RDlrE57/Hvpr5VSkmunw8BpCSDxfEst9JrEhpkO2RHcVxh6LKMW9PXrvi1phNqLctFs2jDiQCexP
f8FWW4OhIHvFqAnz4Yb4ShWKN6ATe45qJoQ7ee+rz25jhhWwMQ0yLTe2kx+nPLo5Tqj1vnwXRYLe
ynKDAEn4brXP0KzenSGU5Ywkg0TVfM4L7mSxYrsDyr+4PYw9+RrThtGbUXHI65lKFOxVBFdcdCnc
qn/O9TXedtzxUsxMbDrgkNz9B3TF3+o0SbN/xoPR/TYvIpmXxuANPylBShFvQcCTX5UrzBEzp7vd
0YM+Lexde+ZuCnlihOwDezT08TnOlWA/Tq8+YrBVyc6KgrQbKZ+0KhIMTLiqnua5QVW7oMEFqdFU
ILImHvppaa+1Aks=

-----END CERTIFICATE-----
```


Signature algorithm:

SHA384withRSA

Issuer CN:

SK ID Solutions ROOT G1R

Issuer 2.5.4.97:

NTREE-10747013

Issuer O:

SK ID Solutions AS

Issuer C:

EE

Subject CN:

SK ID Solutions EID-Q 2021R

Subject 2.5.4.97:

NTREE-10747013

Subject O: *SK ID Solutions AS*

Subject C: *EE*

Valid from: *Mon Oct 04 14:21:22 CEST 2021*

Valid to: *Sat Oct 04 14:21:22 CEST 2036*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CC:3A:C2:D2:C2:B1:4C:CA:29:71:F2:ED:ED:53:FF:CB:73:A5:0C:DC:10:3B:7C:22:12:1F:27:9D:FE:28:42:EE:8F:15:CE:85:D5:64:E5:2A:0F:BE:FD:D8:39:B4:AF:5E:38:6F:1A:96:9A:38:E3:11:C7:04:02:07:11:6F:E6:A4:37:64:6B:6F:73:C5:32:74:1A:71:A4:A8:BF:54:72:37:09:40:17:98:F8:ED:8F:BF:C2:C7:B7:07:EF:EC:D3:D1:8C:84:E3:54:53:D9:B4:69:B3:1C:D4:D8:B3:1F:21:C9:09:A1:23:BE:09:E0:52:B5:C6:92:64:9D:B7:2D:6F:CC:5D:B7:A0:B6:63:A8:A2:B5:3A:F1:FA:BC:D8:79:49:3A:E1:71:BF:93:59:36:24:1D:B2:1D:37:65:E0:D1:BD:E1:01:90:04:F2:A7:B5:A3:09:36:6D:97:25:0A:4A:57:8A:C7:37:D1:0C:0B:6F:B9:98:40:B8:8E:B0:F3:86:ED:56:D5:22:73:A2:BF:06:E3:7A:84:7C:70:31:1F:2E:BC:89:C8:67:BE:9A:FF:D9:F6:37:6B:7B:26:06:31:F2:AA:1A:AB:97:6D:7B:CA:2A:A5:23:AE:72:BD:58:F2:29:AB:FB:74:F8:6F:24:59:20:BD:C4:1C:AE:25:DF:7A:B4:FB:89:42:65:28:F2:ED:46:CC:45:FA:73:F0:37:2E:14:61:57:E7:DB:67:0E:56:8E:0F:65:25:B2:03:FF:75:4D:BC:8B:A8:EB:B9:03:A8:97:A5:FA:67:E2:D0:FF:C3:86:B3:15:D3:FE:76:C9:CE:04:4E:B3:F2:AB:AC:25:22:DB:47:78:8C:E7:BB:F4:F4:F9:DF:6C:15:79:08:56:73:CF:9E:B6:14:1D:D2:C8:CB:11:5F:F5:B5:17:79:4A:A2:C6:94:19:AF:FF:E9:4F:45:53:DD:22:4F:3A:91:2D:75:38:FF:CF:C0:A5:54:DA:41:F9:96:86:98:9A:1C:E5:A8:B4:E9:FE:2A:F4:C8:58:D2:FB:44:F9:39:C7:FC:52:E0:45:6B:3A:26:76:13:C7:35:CC:BA:3E:66:8E:42:75:7B:AC:4F:59:38:58:95:16:26:4B:3D:F7:12:06:69:C2:5B:D6:5E:7A:AD:39:92:F9:63:6C:39:89:9E:39:98:8A:1C:90:C1:C3:90:AF:88:88:9F:8E:7C:6C:F3:C5:9B:5F:20:C6:55:55:9F:C9:89:02:2F:FC:67:7E:F0:36:D0:03:19:2D:87:8F:8C:5D:F8:B4:9D:41:31:E2:24:33:8A:C2:59:F3:54:67:3F:F0:72:39:0B:2D:ED:8B:18:BB:53:CB:E6:48:C3:77:02:03:01:00:01

Authority Key Identifier *95:0D:B7:64:18:C2:A6:9B:66:76:D8:FC:FC:9A:5A:24:BC:28:D6:CD*

Subject Key Identifier *A5:6F:E2:7E:4C:95:88:39:ED:C2:F5:47:D7:62:7E:73:A6:03:D5:86*

Basic Constraints *IsCA: true - Path length: 0*

Authority Info Access

http://ocsp.sk.ee/CA

http://c.sk.ee/SK_ID_Solutions_ROOT_G1R.der.crt

CRL Distribution Points *http://c.sk.ee/SK_ROOT_G1R.crl*

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.skidsolutions.eu/en/repository/CPS/

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *08:9D:D3:35:25:CC:B9:96:C5:F1:DE:BE:DD:C1:7F:1B:3C:0C:4D:F1:7C:9A:99:3A:32:CA:05:57:01:47:BF:03*

X509SubjectName

Subject CN: *SK ID Solutions EID-Q 2021R*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *pW/ifkyViDntwvVH12J+c6YD1YY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2024-10-17T01:00:00Z*

1.36.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.36.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.18.1*

Description *Certificate Policy for Qualified Mobile-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.36.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK-Q 2021R qualified certificates for electronic signatures*

Service digital identities

X509SubjectName

Subject CN: *SK ID Solutions EID-Q 2021R*

Subject 2.5.4.97: *NTREE-10747013*

Subject O: *SK ID Solutions AS*

Subject C: *EE*

X509SKI

X509 SK I *pW/ifkyViDntwvVH12J+c6YD1YY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2024-10-17T01:00:00Z*

1.36.3.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.36.3.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.17.2*

Description *Certificate Policy for Qualified Smart-ID*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.18.1*

Description *Certificate Policy for Qualified Mobile-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.36.4 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *EID-SK-Q 2021R*

Service digital identities

X509SubjectName

Subject CN:	*SK ID Solutions EID-Q 2021R*
Subject 2.5.4.97:	*NTREE-10747013*
Subject O:	*SK ID Solutions AS*
Subject C:	*EE*

X509SKI

X509 SK I	*pW/ifkyViDntwvVH12J+c6YD1YY=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2024-02-08T05:00:20Z*

1.36.4.3 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.36.4.4 - Extension (not critical): Qualifiers [QCStatement, QCForESig]

Qualifier type description	*[en]*	*it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.10015.17.2*
Description		*Certificate Policy for Qualified Smart-ID*
Policy Identifier:		
Identifier	*[OIDAsURN]*	*urn:oid:1.3.6.1.4.1.10015.18.1*
Description		*Certificate Policy for Qualified Mobile-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.37 - Service (granted): EID-SK-Q 2024E qualified certificates for electronic signatures

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK-Q 2024E qualified certificates for electronic signatures*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *207522722449406181056781318964182753780734497934*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDrzCCAxCgAwIBAgIUJFmkBcQvQ0QOhvceUs8st3JaFI4wCgYIKoZIzj0EAwMwZjELMAkGA1UE
BhMCRUUxGzAZBgNVBAoMEINLIElEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTIRSRUUtMTA3NDcw
MTMxITAfBgNVBAMMGFNLIElEIFNvbHV0aW9ucyBST09UIEcxRTAeFw0yNDA3MDIwODM0NThaFw0z
OTA2MjkwODM0NTdaMGkxJDAiBgNVBAMMG1NLIElEIFNvbHV0aW9ucyBFSUQtUSAyMDI0RTEXMBUG
A1UEYQwOTIRSRUUtMTA3NDcwMTMxGzAZBgNVBAoMEINLIElEIFNvbHV0aW9ucyBBUzELMAkGA1UE
BhMCRUUwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAS50qdCTcqwsTWm/TSe1ZTHV8+92muF2Lr8s8og
8kF8lVAk/b9BEIch05lB99gWbjZcXEGVY5pn3TnxbOlB4gAfbcrkToAGHZ6CnQHy0Cu1yGx265qx
GiIT7G6aWKgVjRyjggF6MIIBdjASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFIZOTzrr
OPKwp+7tuYWbnYMjRTrrMG0GCCsGAQUFBwEBBGEwXzA7BggrBgEFBQcwAoYvaHR0cDovL2Muc2su
ZWUvU0tfSURfU29sdXRpb25zX1JPT1RfRzFFLmRIci5jcnQwIAYIKwYBBQUHMAGGFGh0dHA6Ly9v
Y3NwLnNrLmVlL0NBMHAGA1UdIARpMGcwBgYEVR0gADBdBgNVHSAwVjBUBggrBgEFBQcCARZIaHR0
cHM6Ly93d3cuc2tpZHNvbHV0aW9ucy5ldS9yZXNvdXJjZXMvY2VydGlmaWNhdGlvbi1wcmFjdGIj
ZS1zdGF0ZW1IbnQvMC8GA1UdHwQoMCYwJKAioCCGHmh0dHA6Ly9jLnNrLmVIL1NLX1JPT1RfR2FF
LmNvbDAdBgNVHQ4EFgQUdkUHZ+4If+4gTZwsqVexnp+H1TkwDgYDVR0PAQH/BAQDAgEGMAoGCCqG
SM49BAMDA4GMADCBiAJCAIBxMPYdVnp1WBtpFerhIPritsebecWtmgE59KIirv/bsIPBIFecs6Ty
vLY00l0XVD0KoEuPO+OxjPbNX5e2GmWoAkIBjZTfQqK4XPWV0QIBMr2GIFCTWOVs4MY/jMMBmGnZ
283eQ+PTJhyz2kA+rEdlhlMGwz1RGluh2gbUwvB11yoHhnc=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withECDSA*

Issuer CN: *SK ID Solutions ROOT G1E*

Issuer 2.5.4.97: *NTREE-10747013*

Issuer O: *SK ID Solutions AS*

Issuer C: *EE*

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK ID Solutions EID-Q 2024E*

Valid from: *Tue Jul 02 10:34:58 CEST 2024*

Valid to: *Wed Jun 29 10:34:57 CEST 2039*

Public Key:	*30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:92:D2:A7:42:4D:CA:B0:B1:35:A6:FD:34:9E:D5:94:C7:57:CF:BD:DA:6B:85:D8:BA:FC:B3:CA:20:F2:41:7C:95:50:24:FD:BF:41:10:87:21:D1:29:41:F7:D8:16:6E:36:5C:5C:41:95:63:9A:67:DD:39:F1:6C:E2:01:E2:00:1F:6D:CA:E4:4E:80:06:1D:9E:82:9D:01:F2:D0:2B:B5:C8:6C:76:E9:28:31:1A:22:13:EC:6E:9A:58:A8:15:8D:1C*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*86:74:4F:3A:EB:38:F2:B0:A7:EE:ED:B9:85:9B:9D:83:09:45:31:6B*
Authority Info Access	*http://c.sk.ee/SK_ID_Solutions_ROOT_G1E.der.crt* *http://ocsp.sk.ee/CA*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 2.5.29.32* *CPS pointer: https://www.skidsolutions.eu/resources/certification-practice-statement/*
CRL Distribution Points	*http://c.sk.ee/SK_ROOT_G1E.crl*
Subject Key Identifier	*76:45:07:67:EE:25:7F:EE:20:4D:9C:2C:A9:57:B1:9E:9F:87:D5:39*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*95:C4:E7:E2:B5:C2:61:7E:87:74:42:F4:27:61:46:F8:89:5C:EE:8B:AA:33:34:0E:FA:03:E4:5A:66:D6:2D:25*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK ID Solutions EID-Q 2024E*

X509SKI

X509 SK I	*dkUHZ+4lf+4gTZwsqVexnp+H1Tk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2024-10-17T01:00:00Z

1.37.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.37.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig, QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.17.2*

Description *Certificate Policy for Qualified Smart-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.38 - Service (granted): EID-SK-Q 2024R qualified certificates for electronic signatures

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

Service Name

Name *[en]* *EID-SK-Q 2024R qualified certificates for electronic signatures*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *529793211993959716961095331453823380568895105180*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIG2TCCBMGgAwIBAgIUXMy/z4HaMHlhVHiAuftKBIfHqJwwDQYJKoZIhvcNAQEMBQAwZjELMAkG
A1UEBhMCRUUxGzAZBgNVBAoMEINLIEIElFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTlRSRUUtMTA3
NDcwMTMxITAfBgNVBAMMGFNLIElFNvbHV0aW9ucyBST09UIEcxUjAeFw0yNDA3MDIwODQwMjRa
Fw0zOTA2MjkwODQwMjNaMGkxJDAiBgNVBAMMG1NLIEIElFNvbHV0aW9ucyBFSUQtUSAyMDI0UjEX
MBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxGzAZBgNVBAoMEINLIEIElFNvbHV0aW9ucyBBUzELMAkG
A1UEBhMCRUUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDakmc2loLVmkcKO+Cc2ntz
5axekiTqL10C416W2uNeBVax+LUWvf1Yw9tFhygUXlMsgLOy6G7gQb5C6SOmKjulFd0WeicY7QS
baTI+MjUH2qsEz4syipPcnLj2S6jFvZgWmtSlehAvFacyoOvKCOAMdw1v/LxiaqJLl8gN/RTZ3Ju
ihQsz19TqICPA8yharQOffCPoj/keHCiy7hjLGAnaL7KWGZy4y+PH5q5TCNNB0HcpTNst7GzlfB6
xriXyeqcNFAuQ/5697YpSQ2H8zae9kBLAjcpAUzzhY75C5Fe0Xpo51VlrGdly8hgHqh+9Tw2ZlSlB
bO1o/PzxqrjHUlTp+p4LAYl/SN3U1sRu4msi3y0vLb4AFwpzyjTlI7BGqwy1JgvEO/ojdgBoSVsd
zrzrhS/hXSc3aBrqfndr/tg+Ylj3e5N8xPD8d8jAjplz+crrZFlJh/YBMtN+/xck5xrgcQoly2Tx
5qqq6i1mq70m9Dj4X6Rz7Wl9wVRYkVc0TExtkdYHh/wMmAKxR7/LnM7b9rCg9aIu4xy+9Lp4Jsf
ZiR33a6+VrVoDsaSgpmNRPve17qfWHlGj8LGdz0lvWPiOBXJzbmgt3lmCGUuxnwlI0HeK/T1KWuC
sVNCOROYg7zayi9+odukfoaIF24SbApJbUF/spXlfNwFkF/FqylGOwIDAQABo4IBejCCAXYwEgYD
VR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBSVDbdkGMKmm2Z22Pz8mlokvCjWzTBtBggrBgEF
BQcBAQRhMF8wOwYIKwYBBQUHMAKGL2h0dHA6Ly9jLnNrLmVlL1NLXDlEX1NvbHV0aW9uc19ST09U
X0cxUi5kZXluY3J0MCAGCCsGAQUFBzABhhRodHRwOi8vb2Nzcc5zay5lZS9DQTBwBgNVHSAEaTBn
MAYGBFUdIAAwXQYDVR0gMFYwVAYIKwYBBQUHAgEWSGh0dHBzOi8vd3d3LnNraWRzb2x1dGlvbnMu
ZXUvcmVzb3VyY2VzL2NlcnRpZmlj YXRpb24tcHJlbY3Rp Y2Utc3RhdGVtZW50LzAvBgNVHR8EKDAm
MCSgIqAghh5odHRwOi8vY5zay5lZS9TS19UXQcxUi5jcmwwHQYDVR0OBBYEFFRw5zS5YAJC
y5pf1c9JKx8cDZ9XMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQwFAAOCAgEACNJHFWFKDPGm
/PKZJVY+ZN1R2IgRqCxxCx2A+2rLbZJV0YtL0OBFgt0Vy2WA7AiEF4dqfugIO73c4Nq6wCzB3dUC
g6XD6eKqUdJ+/GpuebbALe4ntk7ka6cISjNpNroBpHONCZGucZVBbKeWNqx/W1dh/De5Lx0u+Jbk
A1UXf4ne9ZKjZBrCH5PznDIXdx7ta7xggSulzlRfa6SN2cjvxczuS4ExTM1JH9jiT3qHoehovJ8A
e80kaceLB6OGh3nMp0rpbY4ra0iZiUZpMxEjruDpq5c4kIY76YJ0 9AkU7PztiW44zL5PWsMDKxf
Bz5XEwdB6kZ3pSP5QdRJ55/ZMJ23dH/SXVrGGo+zKI6MaDIeYRvejfyR9Jq7CP4UnrcQ4TiyKssL
xWHa4ah/AUn0dXRxVHs+87zAUWx1nA5VdJCU+/pektlUjFCf21i5el6zo3w7dBob803T0cg1MZ2I
XkJmjfpzcBSh8/ewT2lQR/M2SzBDMjwE9SzN/bR8CCfQuG67UwIXrRz/IvfzHXUkG+uexK83bqeL
hdqGoUp77T7H5VtQ9HYYYDJN/wiMaCpVdEuTUYnNxRZs36kZlqI20ZTBLELxOmCj1Oc1yIQJ3CnP
Os1OXoeoHCm9c6YlV9o4AHGcOy4HKnqjncdBkQ3RNde0zgG4jMeSLgVHxCm1eTI=

-----END CERTIFICATE-----
```

Signature algorithm:	*SHA384withRSA*
Issuer CN:	*SK ID Solutions ROOT G1R*
Issuer 2.5.4.97:	*NTREE-10747013*
Issuer O:	*SK ID Solutions AS*
Issuer C:	*EE*
Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK ID Solutions EID-Q 2024R*
Valid from:	*Tue Jul 02 10:40:24 CEST 2024*
Valid to:	*Wed Jun 29 10:40:23 CEST 2039*
Public Key:	*30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DA:92:67:36:96:82:D5:9A:47:0A:3B:E0:9C:DA:7B:73:E5:AC:5E:90:84:EA:2F:5D:02:E3:5E:96:DA:E3:5E:05:56:B1:F8:BF:D4:5A:F7:F5:63:0F:6D:16:1C:A0:51:79:4C:B2:02:E8:CB:A1:BB:81:06:F9:0B:A4:8E:98:A8:EE:94:57:74:59:E8:9C:63:B4:12:6D:A4:C8:F8:C8:D4:1F:6A:AC:13:3E:2C:CA:2A:4F:72:72:E3:D9:2E:89:17:FB:D9:81:69:AD:4A:57:A1:02:F1:5A:73:2A:0E:BC:A0:8E:00:C7:70:D6:FF:CB:C6:26:AA:24:BF:20:37:F4:53:67:72:6E:8A:14:2C:CF:5F:53:A8:80:8F:00:1C:A1:6A:B4:0E:7D:F0:8F:A0:9F:E4:78:70:A2:CB:B8:63:2C:60:27:68:BE:CA:58:66:72:E3:2F:8F:1F:9A:92:4C:23:4D:07:41:DC:A5:33:6C:B7:B1:B3:95:F0:7A:C6:B8:97:C9:EA:9C:34:50:2E:43:FE:7A:F7:B6:29:49:0D:87:F3:36:9E:F6:40:4B:02:37:29:01:4C:F3:85:8E:F9:0B:91:5E:D1:7A:52:D5:52:2B:19:D2:32:F2:18:07:AA:1F:BD:4F:0D:99:95:29:41:6C:ED:68:FC:FC:F1:AA:B8:C7:50:84:E9:FA:9E:0B:01:82:3F:48:DD:D4:D6:C4:6E:E2:6B:22:DF:2D:2F:2D:BE:00:17:0A:73:C8:94:E2:23:B0:46:AB:0C:B5:26:0B:C4:3B:FA:23:76:00:68:49:5B:1D:CE:BC:EB:85:2F:E1:5D:27:37:68:1A:EA:7E:77:6B:FE:D8:3E:62:58:F7:7B:93:7C:C4:F0:FC:77:C8:C0:8E:99:73:F9:CA:EB:64:59:49:87:F6:01:32:D3:7E:FF:17:24:E7:1A:E0:71:0A:25:CB:64:F1:E6:AA:AA:EA:2D:66:AB:BD:26:F7:42:78:5F:A1:F3:ED:69:7D:C1:54:58:91:57:34:4C:4C:6D:91:D6:07:87:FC:0C:98:02:B1:47:BF:D4:9C:CE:DB:F6:B0:AA:F5:A9:62:B8:8C:72:FB:D2:E9:E0:9B:1F:66:24:77:DD:AE:BE:56:B5:68:0E:C6:92:82:99:BD:44:FB:DE:D7:BA:9F:58:79:46:8F:C2:C6:77:3D:25:BD:63:E2:38:15:C9:CD:B9:A0:B7:72:26:08:65:2E:C6:7C:25:23:41:DE:2B:F4:F5:29:6B:82:B1:53:42:39:13:98:AB:BC:DA:CA:2F:7E:A1:DB:A4:7E:86:88:17:6E:12:6C:0A:49:6D:41:7F:B2:95:C8:7C:DC:05:90:5F:C5:AB:29:46:3B:02:03:01:00:01*
Basic Constraints	*IsCA: true - Path length: 0*
Authority Key Identifier	*95:0D:B7:64:18:C2:A6:9B:66:76:D8:FC:FC:9A:5A:24:BC:28:D6:CD*
Authority Info Access	*http://c.sk.ee/SK_ID_Solutions_ROOT_G1R.der.crt* *http://ocsp.sk.ee/CA*
Certificate Policies	*Policy OID: 2.5.29.32.0* *Policy OID: 2.5.29.32* *CPS pointer: https://www.skidsolutions.eu/resources/certification-practice-statement/*
CRL Distribution Points	*http://c.sk.ee/SK_ROOT_G1R.crl*
Subject Key Identifier	*53:F0:E7:34:B9:60:02:42:CB:9A:5F:D5:CF:49:93:1F:1C:0D:9F:57*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*C6:62:44:D2:9C:F8:03:3B:1D:4A:6F:16:D8:B0:F9:DB:7B:27:CD:AB:CE:5A:D0:C0:5E:FF:70:ED:A1:25:72:35*

X509SubjectName

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK ID Solutions EID-Q 2024R*

X509SKI

X509 SK I *U/DnNLlgAkLLml/Vz0mTHxwNn1c=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

Status Starting Time *2024-10-17T01:00:00Z*

1.38.1 - Extension (not critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.38.2 - Extension (not critical): Qualifiers [QCStatement, QCForESig, QCQSCDManagedOnBehalf]

Qualifier type description *[en]* *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier:

Identifier *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.10015.17.2*

Description *Certificate Policy for Qualified Smart-ID*

Description *All certificates issued under this CA/QC service that have nonRepudiation bit set exclusively are issued as qualified certificates*

1.39 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2025E)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name	*[en]*	*SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2025E)*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*106776098361613790529366293050818207 8*
X509 Certificate	


```
-----BEGIN CERTIFICATE-----
MIIDjDCCAxOgAwIBAgIQAM2krlZn0f8oqXSmRMfyPjAKBggqhkjOPQQDAjBdMRgwFgYDVQQDDA9T
SyBUU0EgQOEgMjAyM0UxFzAVBgNVBGEMDk5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBT
b2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTI1MDIyODIyMDAwMFoXDTMxMDMyOTIxNTk1OVow
aDEjMCEGA1UEAwwaU0sgVEINRVNUQU1QSU5HIFVOSVQgMjAyNUUxFzAVBgNVBGEMDk5UUkVFLTEw
NzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAEziAkd0sCAdrr2jwUEtFKSXDPuBBWi1Tk89PvvPGOhOt9tYkwy58X
Sd2I2BiLK2tq/8eE30PYAt32Injdy8FC/KOCAagwggGkMB8GA1UdIwQYMBaAFFoYwDTO17eZ3wiQ
wAR9GPNzlr3PMGQGCCsGAQUFBwEBBFgwVjAyBggrBgEFBQcwAoYmaHR0cDovL2Muc2suZWUvU0tf
VFNBX0NBX2IwMjNFLmRlci5jcnQwIAYIKwYBBQUHMAGGFGh0dHA6Ly9haWEuc2suZWUvdHNhMIGe
BgNVHSAEgZYwgZMwgZAGBgQAj3oBAjCBhTA7BggrBgEFBQcCARYvaHR0cHM6Ly93d3cuc2tpZHNv
bHlVdaW9ucy5ld5lbi9yZXBvcZ0b3j5L3RzYS8wRgYIKwYBBQUHAgIwOgw4VFNVIGNlcnRpZmlj
YXRlIGhhcyBiZWVuIGlzc3VlZCBhY2NvcmRpbmcgdG8gTkNQKyBwb2xpY3kwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwMwYDVR0fBCwwKjAoOCagJIYiaHR0cDovL2Muc2suZWUvc2tfdHNhX2NhXzIw
MjNlLmNybDAdBgNVHQ4EFgQUean8IWa8bFRphkphpMAC/QDT6p4wDgYDVR0PAQH/BAQDAgbAMAoG
CCqGSM49BAMCA2cAMGQCMDKgkQS/KTNjn8yqXrvnfW83T4GKf/NhIEDaI7NiLnYz+Z1nV58NnEWP
f9QHFODq7AIwIZXcVbx1lxcKm1LH+DyF1Te3NhcpkWuPC8hymZej2WXGL2FWzChUkwma5z1C2JG

-----END CERTIFICATE-----
```


Signature algorithm:	*SHA256withECDSA*
Issuer C:	*EE*
Issuer O:	*SK ID Solutions AS*
Issuer 2.5.4.97:	*NTREE-10747013*
Issuer CN:	*SK TSA CA 2023E*
Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2025E*
Valid from:	*Fri Feb 28 23:00:00 CET 2025*
Valid to:	*Sat Mar 29 22:59:59 CET 2031*
Public Key:	*30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:CE:20:24:D2:C0:80:76:BA:F6:8F:05:04:B4:52:92:5C:33:EE:F0:15:A2:D4:84:E4:F3:D3:EF:BC:F1:8E:84:EB:7D:B5:89:30:C9:2F:17:49:DD:A5:D8:18:8B:2B:6B:6A:FF:C7:84:DF:43:D8:02:DD:F6:22:78:DD:CB:C1:42:FC*
Authority Key Identifier	*5A:18:C0:34:CE:D7:B7:99:DF:08:90:C0:04:7D:18:F3:73:96:BD:CF*
Authority Info Access	*http://c.sk.ee/SK_TSA_CA_2023E.der.crt* *http://aia.sk.ee/tsa*

Certificate Policies	*Policy OID: 0.4.0.2042.1.2* *CPS pointer: https://www.skidsolutions.eu/en/repository/tsa/* *CPS text: [TSU certificate has been issued according to NCP+ policy]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://c.sk.ee/sk_tsa_ca_2023e.crl*
Subject Key Identifier	*79:A9:FC:89:66:BC:6C:54:69:86:4A:61:A4:C0:02:FD:00:D3:EA:9E*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A5:8C:1C:6E:68:39:01:13:AB:CA:60:69:B6:BC:F2:96:56:20:FF:40:D7:71:41:7F:9D:90:98:84:26:75:09:09*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2025E*

X509SKI

X509 SK I	*ean8iWa8bFRphkphpMAC/QDT6p4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description	*[en]*	*undefined.*

Status Starting Time

2025-02-14T03:00:00Z

Service Supply Points

Service Supply Point	*http://tsa.sk.ee/ecc*

TSP Service Definition URI

URI	*[en]*	*https://sk.ee/en/repository/*

1.40 - Service (granted): SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2025R)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name	*[en]*	*SK Time-Stamping Authority for qualified electronic time stamps (SK-TSA 2025R)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *805743310001091602087162696529378698 54*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIG+TCCBOGgAwIBAgIQPJ4NOwuQs78n+nWRxQEKHjANBgkqhkiG9w0BAQwFADBdMRgwFgYDVQQD
DA9TSyBUUU0EgQO0EgMjAyM1IxFzAVBgNVBGEMDk5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJ
RCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTI1MDIyODIyMDAwMFoXDTMxMDMyOTIxNTk1
OVowADEjMCEGA1UEAwwaU0sgVEINRVNUQU1QSU5HIFVOSVOgMjAyNVIxFzAVBgNVBGEMDk5UUkVF
LTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAiPA5MPUvPVko Y4zKJDlaZsQA8LCoEY5OkCkQBbN
AGfXRwFdQPDiPtBBhiAcU3MnjILWSGQgOMilPkRkxE1whCvszOHOTca5yPiUGzeHybeyOppXMdXW
2qfO432H25lkhsUUml1+EV3dNdYQjZ59rRmSRxyGT1r0MtAaezwpgKZoT6wQTGQEJO/T/x8Z/Q8
tsuldZ5i+d39qBg2w67CEN+lXzlkQ/REJ2iZmN8Al9U2HDjlzYgGm9X9C/V8LWEKEhbHqX/TcLE2
n4+a4nlQaLfqu2xWKhVsDAemGupFS6rUxrqStaCxemTlfOuhpGs5O0e2wPlC2NgDAXd+HuAe9bLO
Cl5w1WgCNPv0cauuOCINGFdXLoZ6yUgAyFiQgft4L12HfGi0f6hhfXC4FWukua+FfRL9/av17m5Q
T1PEzTK7IQFgO4/7+1xZlnkW0VoudKSYcOCF7a5WTnxI3zXgaphrJfHhl+OR3GGLuqHElp3c0OPV
qR0tO1fEOw1TZupFWkWfts/j293pmlcLNpzIhWVzo/fvdHVAbZskwLyr8sz5PDNNWwKGyMQdleWm
VWup+cZWGKDP+HTC2RissStp+34Hy2b+nn+n0mlH31dTN3Fa08/LTCrSuAIEbW5LGOiU7oRyFXNv4
7n1/1ld1yKoQKy+KOYCGTaDHjbdN94pTXtMCAwEAAaOCAagwggGkMB8GA1UdIwQYMBaAFP25tFTt
uXdg0bHtjiWEEhVKeplZMGQGCCsGAQUFBwEBBFgwVjAyBggrBgEFBQcwAoYmaHR0cDovL2Muc2su
ZWUvU0tfVFNBX0NBXzIwMjNSLmRlci5jcnQwIAYIKwYBBQUHMAGGFGh0dHA6Ly9haWEuc2suZWUv
dHNhMIGeBgNVHSAEgZYwgZMwgZAGBgQAj3oBAjCBhTA7BggrBgEFBQcCARYvaHR0cHM6Ly93d3cu
c2tpZHNvbHV0aW9ucy5lb59lbi9yZXBvc2l0b3J5L3RzYS8wRgYIKwYBBQUHAgIwOgw4VFNVIGNl
cnRpZmljYXRlIGhhcyBlZWVuIGlzc3VlZCBhY2NvcmRpbmcgdG8gTkNQKyBwb2xp Y3kwFgYDVR0l
AQH/BAwwCgYIKwYBBQUHAwgwMwYDVR0fBCwwKjAoocCagJlYiaHR0cDovL2Muc2suZWUvc2tfdHNh
X2NhXzIwMjNyLmNybDAdBgNVHQ4EFgQUzYZVolgDU5EOivFLS4RCMlzCwaIwDgYDVR0PAQH/BAQD
AgbAMA0GCSqGSIb3DQEBDAUAA4ICAQB/aNYfFgW5FImhkY20vxa34r3Ypyj0PLMf8wML8eL4RK+y
hD4T+rqcBvmnPvVEcB5kI9+ESPJ/ASVXXKRbe1nM81XBQiuRxr/9ON5B8+pTq3zyfUlhChx/ujXW
Q83tFxC5W5Fu3lLB190ESVeBCR1+aOkJ/fB9b5XtRXqhqHA+O7BXx4bh6int8za88cJQDQVoRWb
myMlwIU+Ex5LVgyDhexKWoCZXW/gCstNYtWFp0V79UlO4PnUl87xl99YrUdbNDp4b5/tnKL8Bwk
pwk/C9iocKVNn2/020f39bhgkbYvGMRzdEoYaoyXfzKCChM2bKwVrYMFshwCrYF7PxG8/8wbY/CLX
Qsr5sQHQZv1d18SAS7ot+H5ByS6XJaoei1/n2h80QgjhDUs9d1KGCKSYGcAk3ya1Gphkm782MRz
Y6SmwiNMt7AceZ9xEFNW8h7Ddcs9rXqyjLaTwvNvt4/E8dM1vqU3klvjdx3EukbD9WZ3RndnayzP
zdl35csgN/d4AP5ohf5IV9mGF6e7rROYZHMehnFlde4tQPOggjV0r+cu318naC0g/tznlM7wLpTe
VFXVqLAPNvpha1MU/W/6TucK5oaEXQfoQusmUMFGb4orgpq7YQhR90wvh7g9onpuWZlS4dxV7K8
zu8bL3zM0Gcdmt3kvGAGEzrsyJGNRA==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA384withRSA*

Issuer C: *EE*

Issuer O: *SK ID Solutions AS*

Issuer 2.5.4.97: *NTREE-10747013*

Issuer CN: *SK TSA CA 2023R*

Subject C: *EE*

Subject O: *SK ID Solutions AS*

Subject 2.5.4.97: *NTREE-10747013*

Subject CN: *SK TIMESTAMPING UNIT 2025R*

Valid from: *Fri Feb 28 23:00:00 CET 2025*

Valid to: *Sat Mar 29 22:59:59 CET 2031*

Public Key:


```
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:FE:23:C0:E4:C3:D4:BC:F5:64:A1:8E:33:2A:30:C8:69:9B:10:03:C2:C2:A0:46:
12:D2:40:A4:40:16:CD:00:67:D7:47:01:5D:40:F0:E2:3E:D0:41:86:20:1C:53:73:27:26:52:D6:48:64:2A:38:C8:88:3E:44:64:C4:4D:70:84:2B:EC:CD:01:CE:4D:C6:92:C8:F8:94:1B:37:87:C
9:B7:B2:3A:9A:57:31:D5:D6:DA:A7:CE:E3:7D:87:DB:99:64:86:C5:14:98:8D:7E:11:5D:DD:35:D6:3F:42:36:79:F6:B4:66:49:1C:72:19:3D:6B:D0:CB:40:69:EC:F0:A6:02:99:A1:3E:B0:41:3
1:90:10:93:BF:4F:FC:7C:67:F4:3C:B6:CB:A5:75:9E:62:F9:DD:FD:AB:18:36:C3:AE:C2:10:DF:A5:5F:39:64:43:F4:44:27:68:99:98:DF:00:23:D5:36:1C:38:C8:CD:88:06:98:D5:FD:D8:F5:7C:
2D:61:0A:12:16:C7:A9:7F:D3:70:B1:36:9F:8F:9A:E2:79:50:68:B7:EA:BB:6C:56:2A:15:6C:0C:07:A6:1A:EA:45:4B:AA:D4:C6:B7:52:B5:A0:B1:7A:64:E5:7C:EB:A1:A4:6B:39:3B:47:B6:C0:F
9:42:D8:DA:83:01:77:7E:1E:E0:1E:F5:B2:CE:0A:5E:70:D5:68:02:34:FB:F4:71:AB:AE:38:22:0D:18:57:57:2E:86:7A:C9:48:00:C8:58:90:81:FB:78:2F:5D:87:7C:68:B4:7F:A8:61:7D:70:B8:
15:6B:A4:89:AF:85:7D:12:FD:FD:AB:F5:EE:6E:50:4F:53:C4:CD:32:BB:21:01:60:3B:8F:FB:FB:5C:59:96:79:16:D1:5A:2E:74:A4:98:70:E0:85:ED:AE:56:4E:7C:65:DF:35:E0:6A:98:6B:25:F1
:E1:23:E3:91:DC:61:BB:BA:A1:C4:96:9D:DC:D0:E3:D5:A9:1D:2D:3B:57:C4:3B:0D:53:66:EA:45:5A:45:9F:B6:CF:FF:DB:DD:E9:98:87:0B:36:9C:C8:85:65:73:A3:F7:EF:74:75:40:6D:98:24
:C0:BC:AB:F2:CC:F9:3C:33:4D:5B:02:86:C8:C4:1D:95:E5:A6:55:6B:A9:F9:C6:56:18:A0:CF:F8:74:C2:D9:18:AC:4A:DA:7E:DF:81:F2:D9:BF:A7:9F:E9:F4:98:81:F7:D5:D4:CD:DC:56:B4:F0:
92:D3:0A:B4:AE:00:81:1B:5B:92:C6:3A:25:3B:A1:1C:85:5C:DB:F8:EE:7D:7F:D6:57:75:C8:AA:10:2B:2F:8A:39:80:86:4D:A0:C7:8D:B7:4D:F7:8A:53:5E:D3:02:03:01:00:01
```

Authority Key Identifier	*FD:B9:B4:54:ED:B9:77:60:D1:B1:ED:26:25:84:12:15:4A:7A:92:19*
Authority Info Access	*http://c.sk.ee/SK_TSA_CA_2023R.der.crt* *http://aia.sk.ee/tsa*
Certificate Policies	*Policy OID: 0.4.0.2042.1.2* *CPS pointer: https://www.skidsolutions.eu/en/repository/tsa/* *CPS text: [TSU certificate has been issued according to NCP+ policy]*
Extended Key Usage	*id_kp_timeStamping*
CRL Distribution Points	*http://c.sk.ee/sk_tsa_ca_2023r.crl*
Subject Key Identifier	*CD:86:55:A0:88:03:53:91:0E:8A:F1:4B:4B:84:42:30:8C:C2:C1:A2*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*BB:CE:70:37:AB:2D:A3:EA:1D:7A:2D:95:4A:E1:CA:DE:A1:27:DB:11:40:06:27:ED:67:1B:89:FC:30:E4:BB:42*

X509SubjectName

Subject C:	*EE*
Subject O:	*SK ID Solutions AS*
Subject 2.5.4.97:	*NTREE-10747013*
Subject CN:	*SK TIMESTAMPING UNIT 2025R*

X509SKI

X509 SK I	*zYZVoIgDU5EOivFLS4RCMIzCwaI=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

Status Starting Time

2025-02-14T03:00:00Z

Service Supply Points

Service Supply Point *http://tsa.sk.ee/rsa*

TSP Service Definition URI

URI *[en]* *https://sk.ee/en/repository/*

2 - TSP: GuardTime OÜ

.

TSP Name

Name	*[en]*	*GuardTime OÜ*

TSP Trade Name

Name	*[en]*	*VATEE-101114112*
Name	*[en]*	*GuardTime AS*
Name	*[en]*	*Guardtime*
Name	*[en]*	*Guardtime OÜ*
Name	*[en]*	*VATEE-11313216*

PostalAddress

Street Address	*[en]*	*Tammsaare tee 60*
Locality	*[en]*	*Tallinn*
Postal Code	*[en]*	*11316*
Country Name	*[en]*	*EE*

ElectronicAddress

URI	*[en]*	*mailto:info@guardtime.com*
URI	*[en]*	*https://www.guardtime.com*

TSP Information URI

URI	*[en]*	*https://guardtime.com/library/tsp*

2.1 - Service (withdrawn): TSA0

.

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name	*[en]*	*TSA0*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwJjENMAsGA1UEAxMEVFNBMDEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTExMDQyOTA5MTUxNVoXDTEyMDUyOTA5MTUxNVowJjENMAsGA1UEAxMEVFNB
MDEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2WKqpwAceqQ1DNnslvmj7AsSFgFR4g0U3ot8aLmIVT3Cj0rVN8PaQ4zuClGf0xTM6mp1nQRqvtES
cYkijZ9ISW44KDs4P71rC/8MYuX0NL/AwDIevmjCEkvHvqCQw7SAJ5gFkObc6FGjMcOzzVDTLc/0
g9txSaFy6A2kTQYWY2a7DhgRDVBJphGhW8Ir28DmH+AGRxj5I3vs6V8W/x1xy90yWunh8b/DNbS+
29YKQ04phwPl0Ks59qvsgm1wPpplx0xf/mp9HGC574qQzq2Ee7v4PAhu2FwYZt6HJ887KTWeVDUa
RsVtwKqqDWJdmJBG/Pa96H/k9v1t5Ln8NIxHQIDAMm9MA0GCSqGSIb3DQEBCwUAA4IBAQBit30l
5IzoldRcKYbWRLPrii5nNcmdLFfOVbjjfh/BcQV4G9cIaNtimuaw75Kq0eVuMaD1GBzn3gNSA7UF
pCURt5xtEt/TNdO4ht+5LkVuFeW7AgRSlsJ/M1LiNrQei7qkPRTYrjwT4TGFbycy6oQVkfsFx0WS
ntG1TECDxNfutS4oKJOVp9pCwt99CVpt2M1sniRFlsCqeYgwP6Eqf80fwHpAZGzeX42VMmvLUFdk
uijBqW8phGP5yxDWGWHkYJ+XDTZB2SlBbYcgDpQuS1k0lhGRZScIDSUr4g2ig1LBrbPlMakNXg/
EWh74KkDeDDE8NSZFnh/cr2azvcXqt1G

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA0*

Subject O: *GuardTime AS*

Subject CN: *TSA0*

Valid from: *Fri Apr 29 11:15:15 CEST 2011*

Valid to: *Tue May 29 11:15:15 CEST 2012*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D9:62:AA:A7:00:1C:7A:A4:35:0C:D9:EC:22:F9:A3:EC:0B:12:16:01:51:E2:0D
:14:DE:8B:7C:68:B9:88:55:3D:DC:27:4A:D5:37:C3:DA:43:8C:EE:08:81:9F:D3:14:CC:EA:6A:75:9D:04:6A:BE:D1:12:71:89:22:8D:9F:65:49:6E:38:28:3B:38:3F:BD:6B:0B:FF:0C:62:E5:F4:
34:BF:C0:C0:39:5E:BE:68:C2:12:4B:C7:BE:A0:90:C3:B4:80:27:98:05:90:E6:DC:E8:51:A3:31:C3:B3:CD:50:D3:2D:CF:F4:83:DB:71:49:A1:72:E8:0D:A4:4D:06:16:63:66:BB:0E:1A:91:0D:
50:49:A6:11:A1:5B:C8:AB:DB:C0:E6:1F:E0:06:47:18:F9:23:7B:EC:E9:5F:16:FF:1D:71:CB:DD:32:5A:E9:E1:F1:BF:C3:35:B4:BE:DB:D6:0A:43:4E:29:87:03:E5:D0:AB:39:F6:AB:EC:82:6D:7
0:3E:9A:62:C7:4C:5F:FE:6A:7D:1C:60:B9:EF:8A:B4:CE:AD:84:7B:BB:F8:3C:08:6E:D8:5C:18:DA:DE:87:8F:CF:3B:29:35:9E:54:35:1A:46:C5:6D:C0:AA:AA:0D:62:5D:98:90:46:FC:F6:BD:E
8:7F:E4:F6:FD:6D:E4:B9:67:F0:D9:71:1D:02:03:00:C9:BD
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *0A:AC:8E:BE:46:47:50:B0:AE:71:48:38:C5:5D:8B:E9:C6:6D:E3:89:78:FA:75:D7:FC:EB:AD:66:9F:FB:0C:E1*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA0*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.1.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA0*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA0*

X509SKI

X509 SK I *FYIbyUnpkQO13KX4X2hiUVTAjj8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2011-04-29T12:15:15Z*

2.2 - Service (withdrawn): TSA1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMTEVMBMGA1UEChMMR3Vh
cmRuaW1lIEFTMB4XDTExMDQyOTExMDMzOFoXDTEyMDUyOTExMDMzOFowjjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRuaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
3leYUjkf9LPKTkMUrjeOofT57NjJd+5WUmrsTRDGJsW6CWN/rM405B4EbXdrxeKR5TXqvTc8uKB8
vb7QdQTBYAEiy8y49jL0wApQ40B2wnAj7kpyeWHwvMLwqeVyAxFxcR+gytsUxdRXl601g7GvwIXp
Cgi8Alj4vKykx99SBgsrya0CnR63v+Rgwv+0tc3A24b5SiE395Dzh1R9N1pgXWYNOPqn98A1cYWG
A0bwayHzpcqw+e4YcR6gQ1gykULsPNlnIGCkakiOshblezzB1WrSziTGlNAjNSev+M7Uo4j6bCB3
sFRrv1NXJWM7AqLxn+zC1xVqihB+N9m0YmNkjOIDAPHnMA0GCSqGSIb3DQEBCwUAA4IBAQDUXshm
A1Kx+fPyMrbQkOim5FrSoTuLw4Jaxhhcw5wQLTnI0H25IwciqGisi7ou4fYffaQlSbLfbXEpGG2a
aZ9DPGGeG//5NPvtLoxLYw3igmaCYi4QEO+O8Q5bH/YgxJWlZha8qtDXYjBVq7giX+1Kkb4O87Bc
Bm9yGWXnDbu/Cbjvv+lnbhLff3N9AGlhEVZW4y/WNgd4RjRANYuKHLsNdBBT2jnxTirGzHRbcQ3Q
wxjUcTO+z8f/WUJfq6b/VayReUnWrrmYG6btzU2iwUUusb+eZ2uvNNAjuIJ5+ngc8g9FLity5ZcT
R+SadzU1H36mdCE1uGHVDl3L07SlHNja

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA1*

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Valid from: *Fri Apr 29 13:03:38 CEST 2011*

Valid to: *Tue May 29 13:03:38 CEST 2012*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DC:87:98:52:39:1F:F4:B3:CA:4E:43:14:AE:37:8E:A1:F4:F9:EC:D8:C9:77:EE:56:52:6A:EC:4D:10:C6:26:C5:BA:09:63:7F:AC:CE:34:E4:1E:04:6D:77:6B:C5:E2:91:E5:35:EA:BD:37:3C:B8:A0:7C:BD:BE:D0:75:04:C1:60:01:22:CB:CC:B8:F6:32:F4:C0:0A:50:E3:40:76:C2:70:23:EE:4A:72:79:61:F0:BC:C2:F0:A9:E5:72:03:11:71:71:1F:A0:CA:DB:14:C5:D4:57:97:AD:35:83:B1:AF:C2:55:E9:0A:A8:BC:02:58:F8:BC:AC:A4:C7:DF:52:06:0B:2B:C9:AD:02:9D:1E:B7:BF:E4:60:C2:FF:B4:B5:CD:C0:DB:86:F9:4A:21:37:F7:90:F3:B7:54:7D:37:5A:60:5D:66:0D:38:FA:A7:F7:C0:35:71:85:86:03:46:F0:6B:21:F3:A5:CA:B0:F9:EE:18:71:1E:AA:43:58:32:91:42:EC:3C:D9:67:20:60:A4:6A:48:8E:B2:16:E5:7B:3C:C1:D5:6A:D2:CE:24:FA:94:D0:23:35:27:AF:F8:CE:D4:A3:88:FA:6C:20:77:B0:54:6B:BF:53:57:25:63:3B:02:A2:F1:9F:EC:C2:D7:15:6A:8A:10:7E:37:D9:B4:62:63:64:8D:02:03:00:F1:E7*

Thumbprint algorithm: *SHA-256*

Thumbprint: *63:19:72:50:FC:E3:63:CC:39:28:15:3E:76:4C:F2:39:AE:85:1D:2E:00:8C:F8:FA:68:6A:4C:60:2A:6F:13:0B*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.2.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA1*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

X509SKI

X509 SK I *45sv4BLKD1el+RtP/81SVdyGgmc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2011-04-29T14:03:38Z

2.3 - Service (withdrawn): TSA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMTEVMBMGA1UEChMMR3Vh
cmRUaW1IEFTMB4XDTEwMDQwOTA5MzMzNFoXDTExMDUwOTA5MzMzNFowjjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRUaW1IEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
x77CtLsrKHF3SswUv5uBEiIPF3hJS6j+W54dKIFj4fE0xkxI7/yMIDMf3Gk2tunTpZoIsOKDPCb
sl/95sV8dY7y+yCT7bRT467yfiZcqTrFybHjXduYGSlvagNpYVw260he6qVH27D/ldpQv2eWQOSc
GAWcBOZTr6pZxEuX7b24luq7sSci8hv4ARpJamWBTLQX6sdxfiPhjnyMIacEGOQuEQgUjPKxAxo4
5ApwSHWESD7lAm2PQNacSZJg8+pkxrOq0s/7FrsgfjzQxIDhyF9BA7u28ilsCL60WdVbxqshmQBp
91yyuX3ZHAkJ8Wp0kT8EwVfVnLutFWxzXp/4gwIDAOHjMA0GCSqGSIb3DQEBCwUAA4IBAQAYwPU
IEPlzB88xdz9WTaC8/QNF/DbfYOYKOD5439rG9PhWj/0YBe6SIiohQf3IK0tfBrnaCj+Nw8Ewzj7f
UD6+9xJ4FLSSQP5sH3pxZlIAdiLXKWXUNou6jiPTh9gSDBkkjHvWCMhHj7GNDdlEABbwfqSlejz
NsQZGUVu9Z7vP0+fITGvqC3qJlqschhpQWZqaD4YR73K06H+JEFn6vnGQ6UVsWM/KDaktvLStQui
/OwlqK8kyEm2cpCQOdkVPJZ7vTcGDgonWvbwaxf78xPJUqHSNkuWIHveV6dFlS949v1eJYEwvcsv
6DyVD6UlBA2efjnQmjA4KbXucmWzm0KY
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA1*

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Valid from: *Fri Apr 09 11:33:34 CEST 2010*

Valid to: *Mon May 09 11:33:34 CEST 2011*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:BE:C2:B4:BB:2B:28:71:77:4A:CC:14:BF:9B:81:12:29:4F:17:78:49:4B:A2:
7E:5B:9E:1D:28:81:63:E1:F1:34:C6:4C:65:EC:9E:F2:32:50:CC:7F:71:A4:DA:DB:A7:4E:96:68:96:C3:8A:0C:F0:9B:B2:5F:FD:4A:C5:7C:75:8E:F2:FB:20:93:ED:B4:53:E3:AE:F2:7E:2D:B3:A
9:3A:C5:C9:B1:E3:5D:DB:98:19:29:6F:6A:03:69:61:5C:36:EB:48:5E:EA:05:47:DB:B0:FF:21:DA:50:BF:67:96:38:E4:9C:18:05:9C:04:E6:53:AF:AA:59:C4:4B:97:ED:BD:B8:96:EA:BB:B1:27
:22:F2:1B:F8:01:1A:49:6A:65:81:4C:B4:17:EA:C7:71:7E:23:E1:8E:7C:8C:21:A7:04:18:E4:2E:11:08:14:8C:F2:B1:03:1A:38:E4:0A:70:48:75:84:48:3E:E5:02:6D:8F:40:D6:9C:49:92:60:F3
:EA:64:C6:B3:AA:D2:CF:FB:16:BB:20:7C:9C:D0:C6:50:E1:C8:5F:41:03:BB:B6:F2:29:6C:08:BE:B4:59:D5:5B:C6:AB:21:99:00:69:F7:5C:B2:B9:7D:D9:1C:09:09:F1:6A:74:91:3F:04:C1:57:
D5:9C:BB:AD:15:6C:73:5E:9F:F8:83:02:03:00:E1:E3
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *9B:36:C8:D5:0E:48:1F:3E:B7:91:54:0A:0A:9E:B2:C5:A0:24:46:1E:AA:FB:99:01:E4:53:2F:52:0D:E8:92:78*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

2.3.1 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *TSA1*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

X509SKI

X509 SK I *nsIInN9NggJuait7/oodYeuYG8E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2010-04-09T12:33:34Z*

2.4 - Service (withdrawn): TSA2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA2*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMjEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTEwMDQxMjA3NTIyOVoXDTExMDUxMjA3NTIyOVowjjENMAsGA1UEAxMEVFNB
MjEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
p430lCKJvdyzzdK95iX4IlSE3MyVDkiPcQWKdvM/O0K/skXMKxK9308G01VVPz4Q0Fe/zm9Hd/b0
tF6INehGpi+CUfS13eg32JZvfyI7UsGNZCiU0nnkuGUUfLCXqIEMVsgfxXu9RAhwaJE3Zw0GZLc4
jSF9xJy1HRS5ryUkgp09pO/PP5l0lgBeUES M0U3ALPvS5xjgMpYJAOshZCI5+rsyQ1Cp83ymVNy
GAw2lUCgjHGHu/l+wbTwBb6C2pUnqcUacaemjctKhtf6hNs+5+uTPBW2q9oA8k2c0SQii7+V04H8
L8rvSdLaeVuNDgjEjzqPIJV7oS62APrWIWOf3wIDAKlzMA0GCSqGSIb3DQEBCwUAA4IBAQCCHTCm
S6YOLlnhSEMpOq6F6ZUPq7B4BIEVJPlZOkrPuGRnwXY3CP1CM01mM2FcNc7OMYwEVyJNt11Aj12k
B2yoCGCqABdYij78P2n4MzQykakymH/lQhTiP6rZ1gIB1stye5ybo Avezm5Cor9lbdGSf9QEv7DP
GYqgyEwDAgCIhIgyKWBDTxccKkRFIP7hvDWCzYaDaC2axcxN0Cjv0KTMoTDzK97IZJ2+qrBcgPr/9
AEsZlfPOlvzObbrRpnmwowwgNvYT3p3il7irrlwHryQh8H1kU4AwxmHtuMDcVKvQQrxpCQuEITPl
BleIY2MdXKRoCcu4q//X5Iq9YYP1XIjH

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA2*

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Valid from: *Mon Apr 12 09:52:29 CEST 2010*

Valid to: *Thu May 12 09:52:29 CEST 2011*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A7:8D:F4:94:22:89:BD:DC:B3:CD:D2:BD:E6:25:F8:22:54:84:DC:CC:95:0E:4
8:8F:71:05:8A:76:F3:3F:3B:42:BF:B2:45:CC:2B:12:BD:DF:4F:06:D3:55:55:3F:3E:10:D0:57:BF:CE:6F:47:77:F6:F4:B4:5E:A5:35:E8:46:A6:2F:82:51:F4:B5:DD:EA:B7:D8:96:6F:7F:22:3B:5
2:C1:8D:64:28:94:D2:79:E4:B8:65:14:7C:B0:97:AA:51:0C:56:CA:9F:C5:78:BD:44:08:70:68:91:37:67:0D:D6:64:B7:38:8D:21:7D:C4:9C:B5:1D:14:92:AF:25:24:82:9D:3D:A4:E9:7F:3C:FE
:65:D0:88:01:79:41:12:33:45:37:00:B3:EF:4B:9C:63:80:CA:58:24:03:AC:85:90:88:4B:EA:EC:C8:ED:42:A7:CD:F2:99:53:72:18:0C:36:BD:40:A0:8C:71:87:BB:F9:7E:C1:B4:F0:F1:BE:82:D
A:95:27:A9:C5:1A:71:A7:A6:8D:CB:4A:86:D7:FA:84:DB:3E:E7:EB:93:3C:15:B6:AB:DA:00:F2:4D:9C:D1:24:22:8B:BF:95:D3:81:FC:2F:CA:EF:49:D2:DA:79:5B:8D:0E:08:C4:8F:3A:8F:20:9
5:7B:A1:2E:B6:00:FA:D6:95:63:9F:DF:02:03:00:A9:73
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *47:F6:61:FF:2B:CF:97:2B:BC:69:A3:17:C8:C1:13:D1:A2:62:21:19:2B:CA:8F:62:EC:6E:08:76:D8:3B:DD:1F*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.4.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA2*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

X509SKI

X509 SK I *aj+TWPM7OpTB+vFnEQk4DETK8Hk=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2010-04-12T10:52:29Z

2.5 - Service (withdrawn): TSA1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMTEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTEyMDUwMzA4NDEwM10XDTEzMDYwMzA4NDEwM1owjjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0AjnC81sjs87Vv9e8XDGWcKaj7kjTxuaeWpC+WULgIfyU2YSawqwb1PZbM9AT0Oi4Dz44tCG1o0K
caeik+vWFe7AU3GSSC9K4Y3+jrhKZEOhySn1yI1DMdnI+Iv844R/Iq5+XEKvP0c2LLnT0Bnmz6l8
GIUh2c9MlWXtXfNyfgymIdyT3sswRabL/lksTdqMsa9B7ar81vtmEG2rzsUjCI6l8U6N7Etv3hs
eALX/mcdWplpWn8uxAGUl8KqskF1itQ04BOU3P6Qk0WsLFBNCeQ2Rj+HcHPEdxtkT1eM0lbmOT71
Fu57YZjCSfqza+CoiSPKBMJioU+28KG1qOFC1QIDAOwjMA0GCSqGSIb3DQEBCwUAA4IBAQBftgbU
f5jzWS5EwcLmi7OgQ4ejPme6ZO5M+SX4OJh8cTViXOpqrF6jmIaFI7auqTKa4KNtgWmeGzjaqD3U
9WamJ2aU3xmtf+t9rHWrns9dBE+jRVdwNljvOyEt+foSCENaFxtPRDqpaphx/fYC+jdCdNh+jHuKx
qf1tW9ktBFNxG7qxmSeBa4eC+RosAXtt0gbmHBVMOQJOApGKlIQzruj3c5YrCRzza/+D9j5kyp19
6VO+aYmt2epLMTK5CvJlgljvF/vyuJuEXAnqd1Si6qUbfLxchWHgJ/dxUf7DxeqpPzJ8s+V0CD0f
XYTiHa3p9Kz7/gLqpZMcuY8OH0nVnYOn

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA1*

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Valid from: *Thu May 03 10:41:03 CEST 2012*

Valid to: *Mon Jun 03 10:41:03 CEST 2013*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:08:E7:0B:CD:6C:8E:CF:3B:56:FF:5E:F1:70:C6:59:C2:9A:8F:B9:09:4F:1B:9A:79:6A:42:F9:65:0B:82:57:F2:53:66:12:6B:0A:B0:6F:53:D9:6C:CF:40:4F:43:A2:E0:3C:F8:E2:D0:86:D6:8D:0A:71:A7:A2:93:EB:D6:15:EE:C0:53:71:92:48:2F:4A:E1:8D:FE:8E:B8:4A:64:43:A1:C9:29:F5:C8:8D:43:31:D9:E5:F8:88:FC:E3:84:7F:22:A4:BE:5C:42:AF:3F:47:36:2C:B9:D3:D0:19:E6:CF:A9:7C:18:85:21:D9:CF:4C:25:65:C8:5D:F3:72:7E:0C:A6:95:DC:93:DE:CB:30:FD:16:9B:2F:F2:24:B1:37:6A:32:C6:BD:07:B6:AB:F3:5B:ED:98:41:B6:AF:3B:14:8C:29:7A:23:C5:3A:37:B1:2D:BF:78:6C:78:02:D7:FE:67:1D:5A:99:69:5A:7F:2E:C4:01:94:97:C2:AA:B2:41:75:8A:D4:34:E0:13:94:DC:FE:90:93:45:AC:2C:50:4D:09:E4:36:46:3F:87:70:73:C4:77:1B:64:4F:57:8C:D0:86:E6:39:3E:F5:16:E4:BB:61:98:C2:E5:FA:B3:6B:E0:A8:89:23:CA:04:C2:62:A1:4F:B6:F0:A1:B5:A8:E1:42:D5:02:03:00:EC:23

Thumbprint algorithm: *SHA-256*

Thumbprint: *29:BB:E7:D4:C4:C7:FE:60:F0:78:49:63:FE:50:B8:E6:6F:D1:34:4D:E3:FC:79:5A:3C:BD:35:92:4D:9C:BD:1A*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.5.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA1*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

X509SKI

X509 SK I *QdnoWaDRXvOdBJZ4GSjbfUW5bjs=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2012-05-28T07:45:00Z

2.6 - Service (withdrawn): TSA2

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA2*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMjEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTEyMDUwMjEyMTM1M1oXDTEzMDYwMjEyMTM1M1owjjENMAsGA1UEAxMEVFNB
MjEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uWgbOYOThEhCRi61lnP3GSdD+V4sjuQCehCt9MJ+yyFvrEcJewvGhMaCBq7mUjuI0yV5pCNoSH7g
LDaO8XByJ4acmV8DxKAH1KILSH/tashAjxQLMbReolA9c/qKiwO1oK12z5OCN7rA9C7PBO8gk/sC
LFacOwgYtDCz7faY5l94AEanilA62hT3PZ7Sd0IkcL5Gp9goJ2tZdQ+G58GBZawF+pfS2dzWSkKx
WiV/IMzZahRdaXUf7vCGsXDsVHqS3AhL7ZbIGCRVX0Thg+RCyRBqE1ZiPea8HWcVMxSjFHLhvSvK
HTpi3iA6WVIOCjGUlhcz7h373WCKtqwGx7U+tQIDAMRFMA0GCSqGSIb3DQEBCwUAA4IBAQC4F/Sn
Pubk6gaCyw5/7+sMTMIlLecuEGZ3W3ScAWLY4KP04pS7ViqIJxCvH3brl52dc9gUG0h602hRlEhdc
Xpk96tcd108er0mv666mGp97CT92vIL2E46mnz6QUG8uWyNfs+7K5SCgfkAfIU7+lypM0NjOLXfD
gCDRK2x357EAJh1mIqYSRHL9mst1sBLxjUMzi2xzOEGh55aijIb0xelm2bp2J3jZrCvyjvGGA+95
XRwHrGL9sMFzksrY6u66pG9zea8qurk52RYBv0OGNUHwQWpw95QfZ47lITq9IpqC+J67FIEZheHT
UtgPfvx1ch19lS8GiSM72M6rAeS8Kq19

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA2*

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Valid from: *Wed May 02 14:13:53 CEST 2012*

Valid to: *Sun Jun 02 14:13:53 CEST 2013*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:68:1B:39:83:93:84:48:42:46:2E:B5:96:73:F7:19:27:43:F9:5E:2C:8E:E4:0
2:7A:10:AD:F4:C2:7E:CB:21:6F:AC:47:09:7B:0B:C6:84:C6:82:06:AE:E6:50:9B:A5:D3:25:79:A4:23:68:48:7E:E0:2C:36:8E:F1:70:72:27:86:9C:99:5F:03:C4:A0:07:D4:A9:4B:48:7F:ED:6A:
CB:40:8F:14:0B:31:B4:5E:A2:50:3D:73:FA:8A:8B:03:B5:A0:AD:76:CF:93:82:37:BA:C0:F4:2E:CF:04:EF:20:93:FB:02:2C:56:9C:3B:08:18:B4:30:B3:ED:F6:98:E6:5F:78:00:46:A7:88:80:3A:
DA:14:F7:3D:9E:D2:77:42:24:70:8E:46:A7:D8:28:27:6B:59:75:0F:86:E7:C1:81:65:AC:05:FA:97:D2:D9:DC:D6:4A:42:B1:5A:25:7F:94:CC:D9:6A:14:5D:69:75:05:EE:F0:B6:B1:70:EC:54:7
A:92:DC:08:4B:ED:96:E5:18:24:55:5F:44:E1:83:E4:42:C9:10:6A:13:5D:A2:3D:E6:BC:1D:67:15:33:14:89:14:72:E1:BD:2B:CA:1D:3A:63:DE:20:3A:59:52:0E:08:91:94:96:17:33:EE:1D:FB
:DD:60:8A:B6:0C:06:C7:B5:3E:B5:02:03:00:C4:45
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *2E:5A:DB:83:B7:70:57:A6:3F:15:02:DC:83:F8:11:3C:08:F7:B1:15:77:13:77:22:2B:BE:33:C2:35:82:E9:F5*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

2.6.1 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *TSA2*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

X509SKI

X509 SK I *wDEee81dyoI53eLTZ4ElUd6o/QE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-05-28T07:45:00Z*

2.7 - Service (withdrawn): TSA1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwjjENMAsGA1UEAxMEVFNBMTEVMBMGA1UEChMMR3Vh
cmRuaW1lIEFTMB4XDTEyMTAxOTE3MzE0M1oXDTEzMTAxOTE3MzE0M1owjjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRuaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+OA6jsb8QE/mLd3RPZFW4D+I9RiGhpIVWtaPSNgjAu1emrld4SFmLpOWM5BPsK6tVj2waLNUcmEuR
tG3r6H91E7EEgjsiBDxJaaREHYtXMgpatMkt26X6Cg73Eb0pvD+5eBIh6VpksIWHtRrtq6ahde2w
pb9CUmF8nb9IjfjqEsd3L9+EfsF4/EppRzOs4GDzKG+NGmBz95IEMGIlf0yh9Ot05b0Wj4xdOT7s
JONbF0IC5qpQiPoXMKeLzsWWj6RfctjjhJZ9s2xEyLfwM89Yb4/vdwVVaa9Rk36ZkCvuojeP1e+F
KDXAJmNRGp2knEC1IQ8ZvXLG027BKmDdU0+WGwIDAKKPMA0GCSqGSib3DQEBCwUAA4IBAQCR63M7
Z45TV0MW2eA1bYO1vmRSryLbBK7fC4+2T8BqCXC8PYVxRtdMrQMdLUvXolibDY8bUDIC3Gl4LMD
u1ivVcAcRjOCO4ii5KHxmK+mImInif8v7YTZIIXAqPxbxJlYmpRNaEHFcDS7fciYzvohPzpbxRCK
b4Nu9rfA0YqJv2s0vZmkZPTQ7W1vwHQw/+7KeRL3v/oY6/ANP0eKcNURwdhV3es2kya3RyEXH6sJ
uv3iUGOIPTAp5h8T7RV0xjlDxnz6BcRMSxxpFhyaUJHaA8ELKQXqHx1jjz0Ycri/AdIM21F3wc5U
q6855rm1STGythhxYFkrgx/dgLU7JeXc

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA1*

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Valid from: *Fri Oct 19 19:31:43 CEST 2012*

Valid to: *Sat Oct 19 19:31:43 CEST 2013*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:F8:E0:3A:8E:C6:FC:40:4F:E6:2D:DD:D1:3D:91:56:E3:4F:A5:F5:18:86:86:95:56:B5:A3:D2:36:02:40:BB:57:A6:AE:57:78:48:59:8B:A4:E5:8C:E4:13:EC:2B:AB:55:8F:6C:1A:2C:DB:9C:98:4B:91:B4:6D:EB:E8:7F:75:13:B1:04:82:3B:22:04:3C:49:69:A4:44:1F:2B:57:32:0A:5A:B4:C9:2D:DB:A5:FA:0A:0E:F7:11:BD:29:BC:3F:B9:78:12:21:E9:5A:64:B0:85:87:B5:1A:ED:AB:A6:A1:75:ED:B0:A5:BF:42:52:61:7C:9D:BF:48:8D:F2:6A:12:C7:77:2F:DF:84:7E:C1:78:FC:4A:69:47:33:AC:E0:60:F3:28:6F:8D:1A:60:73:F7:92:04:30:68:88:7F:4C:A1:F4:EB:74:E5:BD:16:8F:8C:5D:39:3E:EC:24:E3:5B:17:49:42:E6:AA:50:88:FA:17:30:A7:8B:CE:C5:96:8F:A4:5F:72:DB:E3:84:96:7D:B3:6C:44:C8:B7:F0:33:CF:58:6F:8F:EF:77:05:55:69:AF:51:93:7E:99:90:2B:EE:A0:97:8F:D5:EF:85:28:35:C0:26:63:51:1A:9D:A4:9C:40:B5:95:00:59:BD:72:C6:D3:6E:DB:2A:60:DD:53:4F:96:1B:02:03:00:A2:8F

Thumbprint algorithm: *SHA-256*

Thumbprint: *DF:73:40:56:91:11:B0:FD:56:E6:06:09:21:AD:E0:1D:CE:4C:B6:61:46:12:2C:BB:6F:1F:0D:73:7A:CE:6A:B3*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.7.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA1*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA1*

X509SKI

X509 SK I *u4+kp6DnUM0luSdwJVgTsm7g84Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-10-19T16:31:00Z*

2.8 - Service (withdrawn): TSA2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *TSA2*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQEFBQAwJjENMAsGA1UEAxMEVFNBMjEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTE2MDUxNTEyNDA1MVcsXDTE0MDUxNTEyNDA1MVowJjENMAsGA1UEAxMEVFNB
MjEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mbkBqCyj5DTDvCRFqy9AubKiWtz1NczYGFG4Uu1YrtNpY7hOrutp2SxjBZGMwcXDXdzIceE28FCv
uPjhTF1MsSm1WA3wRqEFfdoKtwj3hYM4N8NKB8GHgDKRYKw5nY++1anjt+KoxhpZsRbaAvPZSkbON
r6trgSe9DUXE1Wj632LAvC0PGdd4LnUExnernnhs5N/mQwv4BJmMPHcZ2IpiMfBCgJ2/v7r9Ubo
dVRRGr/EHMzp9RdehneT3IQpMDV+7oL1niOyXi6KVdlbqaLzmLBQTpQuopfhaA6uKaAegWkkEaYO
o50BK3xYKZjCUHwL+yH6Sw7ddgGNtBld7vtdpwIDALyRMA0GCSqGSIb3DQEBBQUAA4IBAQAjIFih
75+4WvKgcTr7CHVgftiGLaSCa93uq57kmebap1raFgigOkCYpgg3Jx5DDhdGcx93VjdqTt6qC8lA
vx2VjAywQXOisTtlrfiXK5hXUjMWiKzqT6q6Kv1q3Ac86O3Qy5f5mVg5vehW504bg2UnjjL2oY0
+X9e/D8nQRpel8zVNAYYk2elAr3nNDrcR/kRtEfughvIK2F4f5SR4UrNO2P7xTaiNdQwRuq3CJZE
kA2HjPRXE3kjloL80p7aWU6DKOOHZr6VQjcOHjIK5T/ZUHeOT10tM3BCPHzmmHAs1ziMkFFfItOm
AXooOXBsw8L3cOX5BiopaTnMzMw7Pwfo

-----END CERTIFICATE-----
```


Signature algorithm: *SHA1withRSA*

Issuer O: *GuardTime AS*

Issuer CN: *TSA2*

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Valid from: *Wed May 15 14:40:51 CEST 2013*

Valid to: *Thu May 15 14:40:51 CEST 2014*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:99:B9:01:A8:2C:A3:E4:34:C3:BC:24:45:AB:2F:40:B9:B2:A2:5A:DC:F5:35:CC
:D8:18:51:B8:52:ED:58:AE:D3:69:63:B8:4E:AE:EB:69:D9:2C:63:05:91:8C:C1:C5:C3:5D:DC:C8:71:E1:36:F0:50:AF:B8:F8:E1:4C:5D:4C:B1:29:96:03:7C:11:A8:41:5F:76:82:AD:C0:9D:E1:
60:CE:0D:F0:D2:81:F0:61:E0:0C:A4:58:2B:0E:67:63:EF:B5:6A:78:ED:FB:AA:31:86:96:6C:45:B6:80:BC:F6:52:91:B3:8D:AF:AB:6B:81:27:BD:0D:45:C4:D5:62:7A:DF:62:C0:BC:2D:0F:19:
D7:78:2E:75:04:47:19:DE:AE:79:E1:83:93:7F:99:0C:2F:E0:12:66:30:F1:DC:67:69:69:88:C7:C1:0A:02:76:FE:FE:EB:F5:46:E8:75:54:64:1A:BF:C4:1C:CC:E9:F5:17:5E:86:77:93:DC:84:29:
30:35:7E:EE:82:F5:9E:23:B2:5E:2E:8A:55:D9:5B:A9:A2:F3:98:BF:10:4E:94:2E:A2:97:E1:68:0E:AE:29:A0:1E:81:69:24:11:A6:0E:A3:9D:01:2B:7C:58:29:98:C2:50:7C:0B:FB:21:FA:4B:0E:
DD:76:01:8D:B4:12:1D:EE:FB:5D:A7:02:03:00:BC:91
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *42:F3:F8:41:86:22:BE:86:BB:19:8F:13:91:33:02:B7:11:DD:39:1D:2E:34:E5:10:38:AE:D3:7C:C6:01:B5:AB*

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.8.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *TSA2*

Service digital identities

X509SubjectName

Subject O: *GuardTime AS*

Subject CN: *TSA2*

X509SKI

X509 SK I *D3QyCl0LQEFZ0QcjGfxJDWFGZyY=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2013-05-15T11:40:51Z

2.9 - Service (withdrawn): H1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate

-----BEGIN CERTIFICATE-----

MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwlTELMAkGA1UEAxMCSDExEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMjI1MDhaFw0xNDEyMjYxMjI1MDhaMCExCzAJBgNVBAMTAkgxMRIwEAYD
VOQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6jdPpv5oA0BNH
cFTVZpB8CEjGZvWix4KWgbAVbjI0aiLx2TgmRrimtAi7ogQ2qWPpJlbxgnKQUvpL/913tMH1bIL2
PXYk2fR6xU/jF3DoBvQBA7TrX39OlcTn+GO/noh9/hz3/a5ebyp452AyFow/g7lzvECf/kT8G+Oc
Ij4aWK/M7qbmrj98eBj/j6t5kuBF26llyLzExJr4iJOTSuCaR7BT3yWuLC3rAUtXJaG0XiQxkmTd6
Ibt5GK8pSBtsQfKeJv9/TUS6I093rqZ8dSiP9/k2satrk9/hy464niGyXiKWfiEwWBeEe6okg7Fw
tZZ7ZHL42lATqLBRmbl9qvbXAgMBc7MwDQYJKoZIhvcNAQELBQADggEBAEbHvn6BZArTuTDE+opw
N0NZ6FdtQ102tR1qWMcNGgKKICc1dvQpTCsUD5X4RL26pE0aNy9IBbHFa2vNlS4ZOz7LAbxKWn9D
wSTHZVCBmDz7cThAop6YaVd+f2cYk6aP4FnIWr0dfSTTqxIWyFURip5TLC4vgu2FvjRuQU3LTBcp
dbi5WwVSxxgS5VCzpEc5qUC7kZFGBV/aze6CAxUoE2nWrK3udj/8RUOSpUyaeF+f4oEAkR/xMKvd
1xuWjl09rRyOD71h7WhfmNAjDHY2VRVthl6XBJbv+DMOkjpltfeFUHyvZm9eXEZnUh+KS8Vpj4O6
2VA+rNwV6e2QgaaVu7M=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H1*

Subject O: *Guardtime*

Subject CN: *H1*

Valid from: *Mon Nov 26 13:25:08 CET 2012*

Valid to: *Fri Dec 26 13:25:08 CET 2014*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:8D:D3:E9:BF:9A:00:D0:13:47:70:54:D5:66:90:7C:08:48:C6:66:F5:A2:C7:82:96:81:B0:15:6C:98:90:6A:22:F1:D9:38:26:46:B8:A6:B4:08:BB:A2:04:36:A9:63:E9:24:96:F1:82:72:90:52:FA:4B:FF:DD:77:B4:C1:F5:6E:52:F6:3D:76:24:D9:F4:7A:C5:4F:E3:17:70:E8:06:F4:01:03:B4:EB:5F:7F:4E:95:C4:E7:F8:63:BF:9E:88:7D:FE:1C:F7:FD:AE:5E:6F:2A:78:E7:60:32:16:8C:3F:83:B2:33:BC:40:9F:FE:44:FC:1B:E3:9C:22:3E:1A:58:AF:CC:EE:A6:E6:AE:3F:7C:78:1F:E3:EA:DE:64:BB:11:76:EA:59:72:2F:31:31:26:BE:22:24:E4:D2:B8:26:91:EC:14:F7:C9:6B:8B:0B:7A:C0:52:D5:C9:68:6D:17:89:0C:64:99:37:7A:21:BB:79:18:AF:29:48:1B:6C:41:F2:9E:26:FF:62:4D:44:BA:23:4F:77:AE:A6:7C:75:28:8F:F7:F9:36:B1:AB:6B:93:DF:E1:CB:8E:B8:9E:21:B2:5E:22:96:7E:21:30:58:17:84:7B:AA:24:83:B1:70:B5:96:7B:64:72:F8:D8:80:13:A8:B0:51:99:B2:3D:AA:F6:D7:02:03:01:73:B3

Thumbprint algorithm: *SHA-256*

Thumbprint: *15:9A:F6:4E:07:C8:5A:08:E4:01:79:87:1C:BA:36:2B:48:16:23:02:83:3C:C8:94:DE:A1:F5:23:CA:51:D8:86*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H1*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.9.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H1*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H1*

X509SKI

X509 SK I *zQ97Xa7ocnzmMZDaA9ZAuQVArp0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-11-26T12:25:08Z*

2.10 - Service (withdrawn): H2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H2*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDIxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMjQwNDZaFw0xNDEyMjYxMjQwNDZaMCExCzAJBgNVBAMTAkgyMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDGUFzXDI8KWQj8
/UcZLf1BecHHG3+YYoA3FwfZfdNjlbRepRdwypQx8p0RNbvcZC5eP7TnOLz8tCA95jBcILXOOMEK
LeldbcEuERrVNNZ6MplCsLBfxf0rSZzPcgjUA8vnREZj+rLqYkUwt6P2qt3uwCT/Ymm6D25UG373
TX/058+7+8YlftspEowUPZt1E23ZzpTr0bervZSigvy4V1++ef0PQZq0B/h71hkmw0+/zuWj9vjTU
hS3sde86AqDf8s3q6G1FbVEH9ilnJ8XZipam95fZx+kRCeBQ/Yitw+lYeLcGFQKOJ0uZuqMo3HnF
cJfNkd27uA1Ymi938SVOCypfAgMBbiswDQYJKoZIhvcNAQELBQADggEBAHR1TVGVluBLeTtrfIzX
P4bnsczEudLu36D0dTKcwTvBeGB4YEnaBp69vKT2/boNbdeZ0Pm6ft7PQYRzOg5v8NVlqmYwq8pA
xNhrywGOICOynoW7mnRboaDKVQ25Ct4vdJwdfjpcrJ0l9F1WX3MZ5rNgKTPW6sXrMReXojfFf/2Y
wAvdwPhATjtRvnXYhkkN0aeXvkgPiPMctEP0lEiZeIwWm+DjVFHOy8l1d4+38rvh25tuChxxcl/p
45/H7xpAndHO1qpKEu9Dly6q5eWBcNgvHVf7UTXSDtluRCOcS6g0Q2yz72sdW1Z/m1W/67ToYjof
Qwvhc14CrhQkD05pRAA=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H2*

Subject O: *Guardtime*

Subject CN: *H2*

Valid from: *Mon Nov 26 13:40:46 CET 2012*

Valid to: *Fri Dec 26 13:40:46 CET 2014*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C6:50:5C:D7:0C:8F:0A:59:08:FC:FD:47:19:2D:FD:41:79:C1:C7:1B:7F:98:62:80:37:17:07:D9:7D:D3:63:95:B4:5E:A5:17:70:CA:94:31:F2:9D:11:35:BB:DC:64:2E:5E:3F:B4:E7:38:BC:FC:B4:20:3D:E6:30:5C:94:B5:CE:38:C1:0A:2D:E2:1D:6D:C1:2E:11:1A:D5:34:D6:7A:32:99:42:B0:B0:5F:C5:FD:2B:49:9C:CF:72:08:D4:03:CB:E7:44:46:63:FA:B2:EA:62:45:30:B7:A3:F6:AA:DD:EE:C0:24:FF:62:69:BA:0F:6E:54:1B:7E:F7:4D:7F:F4:E7:CF:BB:FB:C6:25:7E:DB:29:12:8C:14:3D:9B:75:13:6D:D9:CE:94:EB:39:B7:AB:BD:94:A2:AA:FC:B8:57:5F:9E:7C:E3:D0:66:AD:01:FE:1E:F5:86:49:B0:D3:EF:F3:B9:62:7D:BE:34:D4:85:2D:EC:75:EF:3A:02:A0:DF:F2:CD:EA:EB:6D:45:6D:51:07:F6:29:67:27:C5:D9:8A:96:A6:F7:97:D9:C7:E9:11:09:E0:50:FD:88:AD:C3:E9:58:7B:B7:06:15:02:8E:27:4B:99:BA:A3:28:DC:79:C5:70:97:CD:91:DD:BB:B8:0D:58:9A:2F:77:F1:25:4E:0B:2A:5F:02:03:01:6E:2B

Thumbprint algorithm: *SHA-256*

Thumbprint: *70:B4:CF:67:63:7A:00:BF:D2:D1:B5:F2:21:ED:99:65:1E:51:4E:BA:6E:7B:5E:68:95:90:F3:4A:08:5D:AF:CA*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.10.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H2*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H2*

X509SKI

X509 SK I *4wZ8Qgdniap0mVcJ7mqsZKvwOjA=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2012-11-26T12:40:46Z

2.11 - Service (withdrawn): H3

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H3*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDMxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMzAwMTZaFw0xNDEyMjYxMzAwMTZaMCExCzAJBgNVBAMTAkgzMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkmSzH2Au23FO
AGkCMTdCZUoHCcOHV7EPqVxFmwea01gS0nDfAjzFUcudvgYRtaw6r6r4ZPLC+pqBI0W7FjeVpRQA
uKypYGhie2IEd2FAQLDB4grjI68Z7K9B+Njc8rvwKbrgix+N3ReqFz9IENbwtGrXj905MFBoCqfk
mUCe+fy5H/YYjhud7wnZUhYPw7DsYU+5eqAh9dNXNSD4gxOLDoZgID49G953fS2pkgdZKIWpZI+/
hftiTDLD92NB0HYwoqEjZZGSM+RUKMxPeRiHz6goGcqoXp/WjeXyd5uiP4TQX8KsvAQQDTBrBs8D
FbFIL7MOEzM+vvV2PdFdU0bRAgMBDskwDOYJKoZIhvcNAQELBQADggEBAL/lnvma9hUUj7tcZAKK
NlZm2bktd6jguW+eFUbf7m1zfSLw3sq85mwFkI8h5DIV/d4pasJJCd8KmGLki5T9BM/TAJvzf1g2
orBGMArhZKYNnYkuJThcxetLFqtyBxdMKGiObmhfTl1YNAckomnvsausj8ejsKKFxFTcWQ1TOeL3
v3N/sZ/c/pwVd80ZbTIo/k/dFwbRVkhuj3Q+DDi/8tlcGXSAppBVX+uFqDGudu3TZ8XQY7VX7ZSH
/2rIO5SZm0CbgAOFYQitDLKLIXEBS6R4W4n559L+dXIaStAR3U8Jmx8WXWMSsa1FJVynyiVLUMMw
07mVgQGUs2lK81ghXsY=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H3*

Subject O: *Guardtime*

Subject CN: *H3*

Valid from: *Mon Nov 26 14:00:16 CET 2012*

Valid to: *Fri Dec 26 14:00:16 CET 2014*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D5:92:64:B3:1F:60:2E:DB:71:4E:00:69:02:31:37:42:65:4A:07:09:C3:87:57:
B1:0F:A9:5C:45:98:07:9A:D3:58:12:D2:70:DF:02:3C:C5:51:CB:9D:BE:06:11:B5:AC:3A:AF:AA:F8:64:F2:C2:FA:9A:81:23:45:BB:16:37:95:A5:14:00:BB:AC:A9:60:68:62:7B:62:04:77:61:4
0:40:B0:C1:E2:09:C9:97:AF:19:EC:AF:41:F8:D8:DC:F2:BB:F0:29:BA:EA:8B:1F:8D:DD:17:AA:17:3F:48:10:D6:F0:B4:6A:D7:8F:DD:12:30:50:68:0A:87:E4:99:40:9E:F9:FC:B9:1F:F6:18:8E:
1B:9D:EF:09:D9:52:16:0F:C3:B0:EC:61:4F:B9:7A:A0:21:F5:D3:57:35:20:F8:83:13:8B:0E:86:60:20:3E:3D:1B:DE:77:7D:2D:A9:92:07:59:28:85:A9:66:5F:BF:85:FB:62:4C:32:C3:F7:63:41
:D0:76:30:A2:A1:09:65:91:92:33:E4:54:28:CC:4F:79:18:87:CF:A8:28:19:CA:A8:5E:9F:D6:8D:E5:F2:77:9B:A2:3F:84:D0:5F:C2:AC:BC:04:10:0D:30:6B:06:CF:03:15:B1:65:2F:B3:0E:13:3
3:3E:BE:F5:76:3D:D1:5D:53:46:D1:02:03:01:0E:C9
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:4B:AB:47:33:0A:3D:39:08:3B:B9:4D:30:43:A2:EC:79:63:B1:A6:06:2E:F9:75:7D:21:C9:61:9F:32:F7:70*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H3*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

2.11.1 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *H3*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H3*

X509SKI

X509 SK I *d8R/lqslVchhyESZTyjfFalKaYM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-11-26T13:00:16Z*

2.12 - Service (withdrawn): H4

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H4*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDQxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMzA3NDdaFw0xNDEyMjYxMzA3NDdaMCExCzAJBgNVBAMTAkg0MRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDNVtvh71sZgFYc
sv6a/zRU3/iby6KWNztiEjzuLI2oaqsUEVHq4kpAAj6/Hl+UPpIEwPEckB6rpGRgeN/+K+4bWJTr
xh/7S/k3sQiHozTAYIOf6TIC4xAK5rjkfRyJNWZMbKU55hXGC+DMh5sn5ZLtxOLshP4bVjCDrKUb
+bNjCxYE/UT4N3b5Rj3j45CgYnwqANWu2MFYcuuw5I6M+BiLWRA9HNLwHF3nVibCQtyo17gN4oa
236h61/+hehqICa9xeFBBRh9gao35dtFNOEUgEN+qjqXGkUBrcFst65G0nGh67AGjcQeku3QKU8Z
81qocY9NhUKeXordC1C/XPsfAgMBWGEwDQYJKoZIhvcNAQELBQADggEBAGAdaaN8Zy/BWVBH+hLT
+LXFJLKmFxaqRKRiyPtuerCRHmKjIHw8JgIVJB1UDUy4BN1LL04k6iwcpZX/ahuvIG0cwrdh2/I
d++ngyMQ8ecFEvjvI5u9kqiW5FxwDtA7fU5rsTm+Qni5hkIPA60VMQHKuyIx5oHejoyvPoBEft/
tQnQ3QL+re7Cs06in8hkBtWndYK9jyot7G99wWfR5TEY2YQkze1L0oTjmy5W/+EkrsT66XmRWHQu
YLgo5tL5D+oO6H2tfeiKQ5PO0+zDLwQJJYjvvITCVKudR7/sH1v6/B4nXuvch82gaAzIfHK3EP6T
Q7CBC3cw+uZ7qkggdIY=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H4*

Subject O: *Guardtime*

Subject CN: *H4*

Valid from: *Mon Nov 26 14:07:47 CET 2012*

Valid to: *Fri Dec 26 14:07:47 CET 2014*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:56:DB:E1:EF:5B:19:80:56:1C:B2:FE:9A:FF:34:54:DF:F8:9B:CB:A2:96:37:
3B:62:12:3C:EE:2E:5D:A8:6A:AB:14:11:51:EA:E2:4A:40:02:3E:BF:1E:5F:94:3E:92:04:C0:F1:1C:90:1E:AB:A4:64:60:78:DF:FE:2B:EE:1B:58:94:EB:C6:1F:FB:4B:F9:37:B1:08:87:A3:34:C0:
60:83:9F:E9:32:02:E3:10:0A:E6:B8:E4:7D:1C:89:35:66:4C:6C:A5:39:4A:15:C6:0B:E0:CC:B7:9B:27:E5:92:ED:C4:E2:EC:84:FE:1B:56:30:83:AC:A5:1B:F9:B3:49:0B:16:04:FD:44:F8:37:76
:D2:3E:3D:E3:E3:90:A0:62:7C:2A:00:D5:AE:D8:C1:58:72:EB:B0:48:8E:8C:F8:18:8B:59:10:3D:1C:D2:F0:1C:5D:E7:56:26:C2:08:9B:72:A3:5E:E0:37:8A:1A:DB:7E:A1:EB:5F:FE:85:E8:6A:
20:26:BD:C5:E3:C1:05:18:7D:81:AA:37:E5:DB:45:34:E1:14:80:43:7E:AA:3A:97:1A:45:01:AD:C1:6C:B7:A4:86:D2:71:A1:EB:B0:06:25:C4:1E:92:ED:D0:29:4F:19:F3:5A:A8:71:8F:4D:85:4
2:9E:5E:8A:DD:0B:50:BF:5C:FB:1F:02:03:01:58:61
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *83:C6:70:99:FE:9A:31:4D:5F:D0:E9:42:BB:55:AF:C1:DA:90:A3:24:AD:86:90:86:69:96:C0:14:CE:F2:BA:22*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H4*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.12.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H4*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H4*

X509SKI

X509 SK I *g4Rp4hbka/wb/X12o1eSDeWB078=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2012-11-26T13:07:47Z*

2.13 - Service (withdrawn): H5

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H5*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDUxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMjUzMjJaFw0xNDEyMjYxMjUzMjJaMCExC2AJBgNVBAMTAkg1MRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzNmmpHjZG/rb8
xYUBH5TgSkSE9tkVl+JgtkeokY0BLZvrJhM9TZ/XX3AbN5aagJWnMgxPDBCyTYcA7XzsW6lRIQk7
gym+zbLI9bmLEcpQzEYdeQs4Bi39Hb4vtIHYOFQjdck5H0CCaiLojVjxX4b5y1dczJjXN5n7pkBl
/YXXult4h/41bdZKw25j/KxEGWU/CmlZdrrDPzYW85aYk++cdbO+uKspRkklQZV+imp5UpbwjOoN0
VjfrmbJ7s+iyvB94j6qvvSTI537uFY6TOK//W3O4OrtEd8ze3aiePC517yTM8IQaUOrNy/pojan7
FkhvLCVi1duQjLuAcDu7gaQjAgMBMMcwDQYJKoZIhvcNAQELBQADggEBADndrk/PCTqGVmbrtjFW
mYjLyFgbUihSoHHf2+kw66MzI77LFkDc+CYSz5M1pIjsXQe+a+Kkrvpc9YKkvxnT81ttiSduRuj
CNwZlSrYfFVP91Hzxh6hZmnR5F6LOLsNbZCaSjkHdjPuFdnY7wUiozKFrntt/6T/Sgu487osH5o+
sLuCJKcgk0fXgssx41JM+ZUWf5JhS/QUUaPiW18s4SOZmNmO5w1IYVVG70bUOXsoGsVmrBNuuQei
kPPdE30OAf+4ODB82rudUZok/ZrSW69p+eiAbkLKqIVfd1Lx05xeLf/EBglvlSXRUECHV2LDmTbw
Jq1wDjHh5NHN7Z8I22I=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H5*

Subject O: *Guardtime*

Subject CN: *H5*

Valid from: *Mon Nov 26 13:53:22 CET 2012*

Valid to: *Fri Dec 26 13:53:22 CET 2014*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:36:69:A9:1E:36:46:FE:B6:FC:C5:85:01:1F:94:E0:4A:44:84:F6:D9:15:97:E2:60:B6:47:A8:91:8D:01:2D:9B:EB:26:13:3D:4D:9F:D7:5F:70:1B:37:96:9A:80:95:A7:32:0C:4F:0C:10:B2:4D:87:00:ED:7C:EC:5B:A9:51:95:02:BB:83:29:BE:CD:B2:E2:F5:B9:B8:11:CA:50:CC:46:1D:79:0B:38:06:2D:FD:1D:BE:2F:B6:51:D8:38:54:23:75:C9:39:1F:40:82:6A:22:E8:25:52:71:5F:86:F9:CB:57:5C:CC:98:D7:37:99:FB:A6:40:65:FD:85:D7:B8:8B:78:87:FE:35:6D:D6:4A:C3:6E:63:FC:AC:44:19:65:3F:0A:69:59:76:BA:C3:3F:36:16:F3:96:98:93:EF:9D:6C:EF:AE:2A:CA:51:92:42:10:65:5F:A2:9A:94:94:A5:BC:23:3A:83:74:56:37:EB:99:B2:7B:B3:E8:B2:BC:1F:78:8F:AA:AF:BD:24:E5:E7:7E:EE:15:8E:93:38:AF:FF:5B:73:B8:3A:BB:44:77:CC:DE:DD:A8:9E:3C:2E:75:EF:24:CC:F0:84:1A:50:EA:CD:CB:FA:68:8D:A9:FB:16:48:6F:2D:C5:62:D5:DB:90:20:BB:80:70:3B:BB:81:A4:23:02:03:01:30:C7*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B7:4A:36:77:23:80:EF:97:B7:DB:1B:40:35:5B:9B:41:4F:B7:93:F6:D0:ED:9C:48:78:BE:E4:82:91:5C:6E:5F*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H5*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.13.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H5*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H5*

X509SKI

X509 SK I *1y2GEphAgI0iKD3RaFtEI/53Aoo=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2012-11-26T12:53:22Z

2.14 - Service (withdrawn): H1

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H1*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwlTELMAkGA1UEAxMCSDExEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDkwODQ1NDNaFw0xNzAxMDkwODQ1NDNaMCExCzAJBgNVBAMTAkgxMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqG5Ib3DQEBAQUAA4IBDwAwggEKAoIBAQDLkt35YJHx+Y0z
Qypj43j9k23BtR7VxLy+FDL54GkqmAiCmaknWz/nRy19FM+kDfciM92OySnneN+nOyykfoblJ0u
L2ClhN5vYlTV9QvHxNNsij0urOiWu5eXui6N6T+lZPOl938EmNeorJbgzG7FeDjid5W4kRBE9api
RBPp3YFehI0cryc8gLY6kHlvvoH33AgwsW9Zbp2B7jWU92GdH1D3aBw5JwhEh5l01sqjcI7Odbh7
PZaygsXpoVRyW1T5PzDDR1+qoWHoak/oN9J0NXMEAVyswpytQ0rckOlbnXhfA7va2WLQ8+Gulm7w
KwquS2wtqqBPbyvO7rP4LAfAgMB4EEwDQYJKoZIhvcNAQELBQADggEBAI52GHcEe75qB8Sps07G
3TVA+XXh+PGFZYSMrH5bsn1ujvaDNDb1fI1dQCK+YibtoxzVM0pdyBVlHFWsex1wTpdmstsmZYP8
Xaj9ezabN6nPSCz6pdzhFUKM2XG0kuny6jLAFuNjqsh13SxsATARL6yZv7L2PI5VclXHbcpRhNaq
iTeTKxLfXqfTgSX1f1RGNJl/r4SoiTBT+PFj2Tcjfc5GTuRunaTeGVle+QGlrv0WXAlZylGTFsz
qq2e2hh/1l9KFixD7gS1IFvSRrxHVWdTEjM9BH5jMd/y6L6jQ9Ti9qW+UYz2CRo8sOYgfB7axA1m
Vmv/W60TQr2pkCI7GDM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H1*

Subject O: *Guardtime*

Subject CN: *H1*

Valid from: *Tue Dec 09 09:45:43 CET 2014*

Valid to: *Mon Jan 09 09:45:43 CET 2017*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:2A:DD:D2:60:91:F1:F9:8D:33:43:2A:63:E3:7D:E3:F6:4D:B7:06:D4:7B:57
:12:F2:F8:50:CB:E7:81:A4:AA:60:22:0A:66:A4:9D:6C:FF:9D:1C:B5:F4:53:3E:90:37:DC:88:CF:76:3B:24:A7:9D:E3:7E:9C:EC:B2:91:FA:1B:94:9D:2E:2F:60:88:84:DE:6F:60:84:D5:F5:0B:C
7:C4:D3:6C:8A:3D:2E:AC:E8:96:BB:97:97:BA:2E:8D:E9:3F:A5:64:F3:A5:F7:7F:04:98:D7:A8:AC:96:E0:CC:6E:C5:78:32:62:77:95:B8:91:10:44:F5:AA:62:44:13:E9:DD:81:5E:86:5D:1C:AF
:27:01:80:B6:3A:90:79:6F:BE:81:F7:DC:08:30:B1:6F:59:6E:9D:81:EE:35:94:F7:61:9D:1F:50:F7:68:1C:39:27:08:44:85:22:34:D6:CA:A3:70:8E:CE:75:B8:78:3D:96:B2:82:C5:E9:A1:54:7
2:5B:54:F9:3F:30:C3:47:5F:AA:A1:61:E8:6A:4F:E8:37:D2:74:35:73:04:01:5C:AC:C2:9C:AD:43:4A:DC:90:E2:1B:9D:78:5F:03:BB:DA:D9:62:D0:F3:E1:AE:22:6E:F0:2B:0A:AE:4B:6C:2D:AA
:00:4F:6F:2B:CE:EE:B3:F8:2F:F0:1F:02:03:01:E0:41
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *13:E9:AE:D9:0A:7D:57:15:8B:3A:B9:74:FB:AF:2E:C6:0F:13:FE:45:62:7F:DA:B0:61:EE:0D:39:80:72:1A:C8*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H1*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

2.14.1 - History instance n.1 - Status: undersupervision

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *H1*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H1*

X509SKI

X509 SK I *Eh8iaw0jrxBJx9MGEmtlnpGmxyM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-12-09T09:45:43Z*

2.15 - Service (withdrawn): H2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H2*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDIxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDMxMjIwMDZaFw0xNzAxMDMxMjIwMDZaMCExCzAJBgNVBAMTAkgyMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSgGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8ojFnaqso7obL
f56sDn8Mj22sZcmY2NbwfGy12xX+1FpEjgwrwea8Ugj6YS55Mvux/oRcBh2UsgFxm0llz5LgrmR
x0t42PVuufygcXVGy+voYjxsOJUkP8uFgdv+QhLPUHYyV2MKHIYvVEa434dHKl5K2mwWkpFVqEQ2
hITU/uSv3ZAX64F+7iJullraefdZ0QC6ucdOsxAFwC3FEH+HfPpV2rb6nhsBu8hxIGWOqDHoCcd3
y0H2+7n/BE1pmOCkuT0j1tKU2NwUrEvWfRna2xyx+zNff9PmcNRrIT0yytr4ghCuQJbcGpA7+EGf
5jGKfGjL1xL6GXwnb3WZ3SPDAgMBHWMwDQYJKoZIhvcNAQELBQADggEBALxmxs0QzRhDlICmedBn
grnOGYIBd9sj3TtWXak+4cJemPttrKPetWIDnSHyWZleuO6neIUtvKSXVETrIqbX0Y2bn37qPseBu
3284qWLi2fAYhhOKfz2PEuUmck0+p3wKH6iDgsXgjmQuu6wO9m1+Y8qB/K+mSwi8gpxjBU38aPCg
QrPZnlAbBPpju2NBb241ep+aOlonKQRO+KcsPMwYzLt0xEmkjopq4dRI0i+Nl/m3EVcIJClslvSD
37tUBQlbEpvv7OrXbv37xvY9Cr4JRWrrjrRO6n1d2NSxdaghHjwobdBgPCQXGqroMxUNL0EprVmlb
RNvWkxmj4wd6PYKfnaQ=
-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H2*

Subject O: *Guardtime*

Subject CN: *H2*

Valid from: *Wed Dec 03 13:20:06 CET 2014*

Valid to: *Tue Jan 03 13:20:06 CET 2017*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:A2:31:67:6A:AB:2B:EE:86:CB:7D:2E:AC:0E:7F:0C:8F:6D:AC:FD:97:26:63:63:5B:C1:F1:B2:D7:6C:57:FB:51:69:12:38:30:AF:07:9A:F1:4A:BA:61:2E:79:32:FB:B1:FE:84:5C:06:1D:94:B2:01:71:9E:7D:08:97:34:8B:82:B9:91:C7:4B:78:D8:F5:6E:B9:FC:A0:71:75:46:CB:EB:E8:62:3C:6C:38:95:24:3F:CB:85:A9:DB:FE:42:12:CF:50:74:F2:57:33:0A:1C:86:2F:54:46:B8:DF:87:47:2A:24:8A:DA:7C:16:92:91:55:A8:44:36:84:84:D4:FE:E4:AF:DD:90:17:EB:81:7E:EE:22:6E:22:5A:DA:79:F7:59:D1:00:BA:B9:C7:4E:B3:10:05:C0:2D:C5:10:7F:87:7C:FA:55:DA:B6:FA:9E:1B:01:BB:C8:71:20:65:8E:A8:31:E8:09:C7:77:CB:41:F6:FB:B9:FF:04:4D:69:98:E0:A4:B9:3D:23:D6:D2:94:D8:DC:14:AC:4B:D6:7D:19:DA:DB:1C:B1:FB:33:5F:7F:D3:E6:70:D4:6B:95:3D:32:CA:DA:F8:82:10:AE:40:96:DC:1A:90:3B:F8:41:9F:E6:31:8A:7C:68:CB:D7:12:FA:19:7C:27:8F:75:B6:DD:23:C3:02:03:01:1D:63

Thumbprint algorithm: *SHA-256*

Thumbprint: *93:45:FE:3F:75:62:EE:16:26:44:FD:0C:F9:2C:32:78:5E:1C:7D:AF:EB:BE:91:87:12:0D:09:D9:99:78:F2:DC*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H2*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.15.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H2*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H2*

X509SKI

X509 SK I *EYQKyMAHRbdf0QdxvZ2qxd7XipQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-12-03T13:20:06Z*

2.16 - Service (withdrawn): H3

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H3*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDMxEjAQBgNVBAoTCUd1YXJk
dGlzTTAeFw0xNDEyMDQwOTI4MTFaFw0xNzAxMDQwOTI4MTFaMCExCzAJBgNV/BAMTAkgzMRIwEAYD
VOQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC15sVKLBcJ6NRM
FmMZxyBy/kKCcBr8zwozbZ+3cyuKeRk8s2+9IEH0xklpE9MxCmDaW65rpk24aX01A9LvYaM/Jn8b
zE9H955wuRTWZbUpW22ljLxjg3x6bM2mwMB/BRkWPK/0BZ8mO1XOXFGh6eRD5OqLXDen3AXno3L
gxpibK7jHekfX1a7ZG35c2zDcZmIf86bQiFSxPxl/xJXjcswX3XI1CoEdoyiOhyYIl1756QKzNL
/yzXy4W7Fczk5gjax+ke9snndPg/ZnPzKLHJowNyPzobhG0R7W7eG/S7BpxMTEG3aIA3BZvV2gmV
Dw8Bp8t6mNNtxgbWL6fqKQdrAgMBb5cwDQYJKoZIhvcNAQELBQADggEBACyCZSs4DiVR9FvRRUCe
XAU4zpvlO2+nlAqL/SnK657aHNbnnQKgtBdoW4N/Gf6Pxz27B7PB1c1p1qgmKzvVewKfwh+37XoC
lxqenoLzwALGN0wPne3dVB1Jf8DMEMtECB5ktZMd/Bl8fgc6VlY8DnDXa+gu13hbTHYuWV0dloks
eMOoNU9fwcABn14E0AsEwfaIZpXps9LQqlVx609pZwDFRQo3igzY4qKxpivUD0xyrjsh5UebIdL
j2K7gtFubrenuQuRerVFIJ82VmNsAdFFzyVsCXdUdULO+wxcnljCUIAY2I8CEM70z/UXmuCCqnoq
PmmXk/oEldqPLZQqR3c=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H3*

Subject O: *Guardtime*

Subject CN: *H3*

Valid from: *Thu Dec 04 10:28:11 CET 2014*

Valid to: *Wed Jan 04 10:28:11 CET 2017*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B5:E6:C5:4A:2C:17:09:E8:D4:4C:16:63:19:C7:20:72:FE:42:82:70:1A:FC:CF:
0A:33:6D:9F:B7:73:2B:8A:79:19:3C:B3:6F:BD:20:41:F4:C6:49:69:13:D3:31:0A:60:DA:5B:AE:6B:A6:4D:B8:69:7D:35:03:D2:EF:61:A3:3F:26:7F:1B:CC:4F:47:F7:9E:70:B9:14:D6:65:B5:2
9:5B:6D:A2:96:32:F1:8E:AD:F1:E9:B3:36:98:03:01:FC:14:64:58:F2:BF:D0:16:7C:98:ED:57:39:71:46:87:A7:91:0F:93:AA:2D:70:DE:9F:70:17:9E:8D:CB:B3:1A:62:6C:AE:E3:1D:E9:1F:5F:
56:93:D8:6D:F9:73:6C:C3:71:99:A2:7F:CE:9B:42:21:52:C4:FC:48:FF:12:57:88:97:2C:C1:7D:D7:97:50:A8:11:DA:32:88:E8:72:60:89:75:EF:9E:90:2B:33:4B:FF:2C:D7:CB:85:BB:15:CC:E
4:E6:08:DA:C7:E9:1E:F6:C9:E7:74:F8:3F:66:73:F3:28:B1:C9:A3:03:72:3F:3A:1B:84:6D:11:ED:6E:DE:1B:F4:BB:06:9C:4C:4C:41:B7:6A:50:37:05:9B:D5:DA:09:95:0F:0F:01:A7:CB:7A:98:
D3:6D:C6:06:D6:2F:A7:EA:29:07:6B:02:03:01:6F:97
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *4F:72:A3:3C:38:42:1F:78:82:A0:A9:97:83:72:2F:E9:BB:CD:68:09:0D:8E:4D:02:7E:C0:63:94:3B:FE:B8:33*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H3*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.16.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H3*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H3*

X509SKI

X509 SK I *QirOC5zp/hiyOrBnqKibCdrnyZ4=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2014-12-04T10:28:11Z

2.17 - Service (withdrawn): H4

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H4*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwlTELMAkGA1UEAxMCSDQxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDUwOTQwMzVaFw0xNzAxMDUwOTQwMzVaMCExCzAJBgNVBAMTAkg0MRIwEAYD
VOQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCgdoH5rbrx9r/C
kW7gdHjEGtjlVYP9/sF26W0yMVvyEApwXJk9ccM5FNejlnHO94DQ4jOJYGU8MnFu0Xs8FlrRt47v
Pikjsdl/HfGW8zQFvPq/CGR2JWtoTW/OS3TLlhuKsgZ4ynsIZs7VrU9H1bk/OyAgtvK3sbdyELF6
JYIy0t2mN5kXHPgFYs3PCifQteLEDsYLdxKKtwnEpR8Vyptw/9iNHPsvnqwpa/U5UL0Q/0dF4fxp
YNwVdgTKL5bpjal6I2NmYBdhl8L9aTdEXsP+kSA/+pB5iqNGZ9vlrfweRLsqb8fIILjgIheJwgOK
MMTzfIsxfN8nJPr6ICAjd37DAgMBrnHswDQYJKoZIhvcNAQELBQADggEBAHh80N8rHNlR29mMguKbY
l5b6EnhIs0VWx/F3oDe+gfZ3p+ASXHPqZG8+e0BwDZh0Qyk23g8etSBL4yOEUi5PEhiIECuny++N
qFItHheyUXFFjih5qCqP8w+qiseVignIRH/oumNXMt0HZUeWvh0G43Nc/6OdW2g2OtjUKjO3Wtb
NP9Znx+okruUAzOrWpYN0V5PgE5FXrrssIykYb6ou3xThvmkowHddyI3x/koUd1nfra5YUAY9hzf
FfUC8SdRg80SOSy+Ewl+dE006j91dR1EyNKZhqEg1Q5Wb2BGGRXbAYDOGeuX6NE9X+V2gKqD+kau
xfz+t2f6lzWEueaexo8=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H4*

Subject O: *Guardtime*

Subject CN: *H4*

Valid from: *Fri Dec 05 10:40:35 CET 2014*

Valid to: *Thu Jan 05 10:40:35 CET 2017*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A0:76:81:F9:AD:BA:F1:F6:BF:C2:91:6E:E0:74:78:C4:1A:D2:65:55:83:FD:FE:
C1:76:E9:6D:32:31:5B:F2:10:0A:70:5C:99:3D:71:C3:39:14:D7:89:96:71:CE:F7:80:D0:E2:34:08:60:65:3C:32:71:6E:D1:7B:3C:16:5A:D1:23:8E:EF:3E:29:23:B1:D2:3F:1D:F1:96:F3:34:05
:BC:FA:BF:08:64:76:25:6B:68:4D:6F:CE:4B:74:CB:96:1B:8A:B2:06:78:CA:7B:08:66:CE:D5:AD:4F:47:D5:B9:3F:3B:20:20:B6:F2:B7:B1:B7:72:10:B1:7A:25:82:32:D2:DD:A6:37:99:17:1C:
F8:05:62:CD:CF:0A:27:D0:B5:E2:C4:0E:C6:0B:77:12:8A:B7:09:C4:A5:1F:15:CA:9B:70:FF:D8:8D:1C:FB:2F:9E:AC:29:6B:F5:39:50:BD:10:FF:47:45:E1:FC:69:60:DC:15:76:04:CA:2F:96:E9
:8D:A2:3A:23:63:66:60:17:61:23:C2:FD:69:37:44:5E:C3:FE:91:20:3F:FA:90:79:8A:A3:46:67:DB:E5:AD:FC:1E:44:BB:2A:6F:C7:C8:20:B8:E0:22:17:89:C2:03:8A:30:C4:DD:7C:8B:31:7C:
DF:27:24:FA:FA:20:20:23:77:7E:C3:02:03:01:98:7B
```


Thumbprint algorithm: *SHA-256*

Thumbprint: *BE:7A:89:43:E1:6A:F9:37:C8:D3:C8:37:B8:60:E4:F7:65:9E:BD:D8:74:F3:B0:9E:F9:AB:A7:14:5D:7C:A1:FA*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H4*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.17.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H4*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H4*

X509SKI

X509 SK I *2zNKmjgO3GbRjbtLb/2gxC95Ydg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-12-05T10:40:35Z*

2.18 - Service (withdrawn): H5

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *H5*

Service digital identities

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDUxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDgwOTAzNDdaFw0xNzAxMDgwOTAzNDdaMCExCzAJBgNVBAMTAkg1MRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSib3DQEBAQUAA4IBDwAwggEKAoIBAQC60wohNDbrmyAL
/7WupGYRFg8sBizryJup1HDV/YjvhVAo7jt63nrzuxqnADeqlzeek2GuYugh5LbYRR8EeBtxE3ss
IabIc5TLKPZj1hzj+Tsw39BrbYebQUwusxU+BUcIQ9TpxgSAM6eXa5w2pi9o8eiHVMxzXQ5c5BE0
XGSSH4IRRoej/xmeaIXgxNIFvEm14sFvkAg04WQQw09ZTmWMY80WHeYDFr+v7N520r19GMyTc8Yo
R8DfWI0ILBYrcG1yDXu6gZlaLD+Xrb633Qn7WRgWD0ejCh9taWbEDBwoc6aM8yZDLfBsExYQSn8R
MCcVXZjDZv5k7+IQaozgj0q7AgMBarkwDQYJKoZIhvcNAQELBQADggEBALnzytGvxyDEf8fDaErx
IVaZpUcZrWSifiBc3jK3h3PvFTuaY98DT9keY2X1vM9mSeMBusRdMblkFROA6+uUUNEXIp7IQEoZ
9/N1HAvCGscvZW8Oua668qw2PrLCQoD5sp1SDH/0IpK4wX+Xk8bdl+Q6cHu2p606r4PBtjVv2oR5
y+LaghTC10pT+4+EQ8rDPmseiatvSa9dJdz3RM/blR+Ki9OO5nBYpPBQJuvDTJ1rfWSfr7JD0ejD
OVeG9OfN0J26L/sChV5uZxRMs/mvIlRibHqXU0+oeOGCCsZGb6YN27nLFh5TUdqtGRbJuu3f/8tY
NLa7Gb/il6afpO8nRXc=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer O: *Guardtime*

Issuer CN: *H5*

Subject O: *Guardtime*

Subject CN: *H5*

Valid from: *Mon Dec 08 10:03:47 CET 2014*

Valid to: *Sun Jan 08 10:03:47 CET 2017*

Public Key: *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:D3:0A:21:34:36:EB:9B:20:0B:FF:B5:AE:A4:66:11:16:0F:2C:06:2C:EB:C8:9B:A9:D4:70:D5:FD:82:6F:85:50:28:EE:3B:7A:DE:7A:F3:BB:1A:A7:00:37:AA:97:37:9E:93:61:AE:62:E8:21:E4:B6:D8:45:1F:04:78:1B:71:13:7B:2C:21:A6:E5:73:94:CB:28:F6:63:D6:1C:C9:F9:3B:30:DF:D0:6B:6D:87:9B:41:4C:2E:B3:15:3E:05:47:25:43:D4:E9:C6:04:80:33:A7:97:6B:9C:36:A6:2F:68:F1:E8:87:54:CC:73:5D:0E:5C:E4:11:34:5C:64:92:1F:82:11:46:87:A3:FF:19:DE:6A:55:E0:C4:D2:05:BC:49:B5:E2:C1:6F:90:08:34:E1:64:10:C0:3F:59:4E:65:8C:63:CD:16:1D:E6:03:16:BF:AF:EC:DE:76:D2:BD:7D:18:CC:93:73:C6:28:47:C0:DF:5B:8D:25:2C:16:2B:70:6D:72:0D:7B:BA:81:99:5A:2C:3F:97:AD:BE:B7:DD:09:FB:59:18:16:0F:47:A3:0A:1F:6D:69:66:C4:0C:1C:28:73:A6:8C:F3:26:43:2D:F0:6C:13:16:10:4A:7F:11:30:27:15:5D:98:C3:66:FE:64:EF:E2:10:6A:8C:E0:8F:4A:BB:02:03:01:6A:B9*

Thumbprint algorithm: *SHA-256*

Thumbprint: *03:8F:EA:97:61:37:87:0F:61:22:53:0B:37:2E:5D:14:28:18:3E:96:1E:BE:EE:3D:FA:CF:50:ED:A2:44:89:79*

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H5*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

2.18.1 - History instance n.1 - Status: undersupervision

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name *[en]* *H5*

Service digital identities

X509SubjectName

Subject O: *Guardtime*

Subject CN: *H5*

X509SKI

X509 SK I *i8kh3VDj6mI46TJ0BxYTItfimzM=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

Status Starting Time

2014-12-08T10:03:47Z

2.19 - Service (withdrawn): Guardtime KSI ajatempliteenus

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[et]* *Guardtime KSI ajatempliteenus*

Name *[en]* *Guardtime KSI timestamp service*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *133034341412651619539987101 16*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFeDCCBGCgAwIBAgIMKvxXwd+2ViRgXqVkMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlHbG9iYWxTaWduIFF1YWxpZmll
ZCBDQSAxMB4XDTE5MTAwMjEyMDIyM1oXDTIwMTAwMjEyMDIyM1owgaIxCzAJBgNVBAYTAkVFMQ4w
DAYDVQQIEwVlYXJqdTEQMA4GA1UEBxMHVGFsbGlubjEVMBMGA1UEChMMR3VhcmR0aW1lIEFTMRUw
EwYDVQQDEwxHdWFyZHRpbWUgQVMxKTAnBgkqhkiG9w0BCQEWGnB1YmxpY2F0aW9uc0BndWFyZHRp
bWUuY29tMRgwFgYDVQRhEw9WQVRFRS0xMDExMTQxMTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCt1f0R2cimqb2lM0/zVB00PfcY/w2zkpWSKuHlcyFMyxPaDsUFAxBlHpBn4bk9QEyp
WB/RpK15SPV1Veb5oL7o7A+62O75XdA4jEyajyFVvP+mK/cXsSQx7Bb7r9woPHZFmm1zExAkjrp
yW2H9jjBav2TSD5sLW1/ANfg0G9c1OgC0nizc2dKMCmXLvB5gVSa4PiZ1RGO+IcHVzfQhElrmywp
oe9MFfyB22eQfsKqXedopNLF8Ix3iHE9bp75yrhmuOrFG32vDbdgQTGwJBbRc8QDidyVQiuKwija
YPnhAryZXXgnrl7PldFib7aE3MQDHEmW4VPqKlfTX2r4HyFAgMBAAGjggIBMIIB/TAOBgNVHQ8B
Af8EBAMCBkAwgYUGCCsGAQUFBwEBBHkwdzBABggrBgEFBQcwAoY0aHR0cDovL3NlY3VyZS5nbG9i
YWxzaWduLmNvbS9jYWNlcnQvZ3NxY2Exc2hhMmc0LmNydDAzBggrBgEFBQcwAYYnaHR0cDovL29j
c3AuZ2xvYmFsc2lnbi5jb20vZ3NxY2Exc2hhMmc0MFkGA1UdIARSMFAwQwYLKwYBBAGgMgEoIwEw
NDAyBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5jb20vcmVwb3NpdG9yeS8wCQYH
BACL7EABAzAJBgNVHRMEAjAAMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwuZ2xvYmFsc2ln
bi5jb20vZ3NxY2Exc2hhMmc0LmNybDAlBgNVHREEHjAcqRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1l
LmNvbTA3BggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACO
RgEGAjAgBgNVHSUEGTAXBgkqhkiG9y9BAQUGCisGAQQBgjcKAwwwHwYDVR0jBBgwFoAUrDfbzzLJ
lRaqCxwGA4bwXcdpzRowHQYDVR00BBYEFPe+Zbcss+ahPvlOaNUGuBxgwHg1MA0GCSqGSIb3DQEB
CwUAA4IBAQALCkY2jkPjPdJV8N5+2gm3MDVurit5dp6AjRLIEoo2tmgQkos YnfyPXajH4iF9ik2E
B8K4piO+9ASijEewIfGaHABpfY9lXYM87RRbuw2Q1YScog4ev6NdvhJZjSTQzu5wj//djB5rE9jP
tN9eAY3ihQXB/lhSuX1M2p82wCBma51+jZnyQgOVwXXgX/+RqotnAznRt63NqfAQkAOp3NPW2EPk
eoFz1Lv5eBxGZapggF0I5alhYWhR/96McP3isQAtftLnakwAPgHvj9rxWnTAhOB6N0kWRiECIgnG
xOnZT1TQVVTDpXwBYsgiZ1cv82ag2sH75vCKnyFIxHHIgCo+

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *GlobalSign Qualified CA 1*

Issuer O: *GlobalSign nv-sa*

Issuer C: *BE*

Subject 2.5.4.97: *VATEE-101114112*

Subject E: *publications@guardtime.com*

Subject CN: *Guardtime AS*

Subject O: *Guardtime AS*

Subject L: *Tallinn*

Subject ST: *Harju*

Subject C: *EE*

Valid from:	*Wed Oct 02 14:02:23 CEST 2019*
Valid to:	*Fri Oct 02 14:02:23 CEST 2020*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AD:D5:FD:11:D9:C8:A6:A9:BD:A2:33:4F:F3:54:1D:34:3D:F7:18:FF:0D:B3:92:95:92:2A:E1:C8:73:21:4C:C8:13:DA:0E:C5:05:03:10:65:1E:90:67:E1:B9:3D:40:4C:A9:58:1F:D1:A4:AD:79:48:F5:75:55:E6:F9:A0:BE:E8:EC:0F:BA:D8:EE:D2:5D:D0:38:8C:4C:9A:9F:21:55:BC:FF:A6:2B:F7:17:B1:24:3F:C7:B0:5B:EE:BF:70:A0:F1:F6:16:69:B5:CC:4C:40:92:3A:E9:C9:6D:87:F6:38:C1:6A:FD:93:48:3E:6C:2D:6D:7F:00:D7:E0:D0:6F:5C:D5:08:02:D2:78:99:73:67:4A:30:29:97:2E:F0:79:81:54:9A:E0:F8:99:D5:11:90:F8:87:07:57:37:D0:84:42:2B:9B:2C:29:A1:EF:4C:15:FC:81:DB:67:90:7E:C2:AA:5D:E7:68:A4:D2:C5:F0:8C:77:88:71:3D:6E:9E:F9:CA:B8:66:B8:EA:C5:1B:7D:AF:0D:B7:60:41:31:B0:24:16:D1:73:C4:03:89:DC:95:42:2B:8A:C2:22:5A:60:F9:E1:02:BC:99:5D:78:27:AC:8E:CF:21:D7:45:89:BE:DA:13:73:10:0C:71:26:5B:85:4F:A8:A9:5F:4D:7D:AB:E0:7C:85:02:03:01:00:01*
Authority Info Access	*http://secure.globalsign.com/cacert/gsqca1sha2g4.crt* *http://ocsp.globalsign.com/gsqca1sha2g4*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.4146.1.40.35.1* *CPS pointer: https://www.globalsign.com/repository/* *Policy OID: 0.4.0.194112.1.3*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crl.globalsign.com/gsqca1sha2g4.crl*
Subject Alternative Name	*publications@guardtime.com*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
Authority Key Identifier	*AC:37:DB:CF:32:C9:21:16:AA:0B:1C:06:03:86:F0:5D:C7:69:CD:1A*
Subject Key Identifier	*F7:BE:65:B7:2C:B3:E6:87:3E:F9:4E:68:D5:06:B8:1C:60:C0:78:35*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*89:F3:BC:E2:8B:9C:E3:75:67:F0:C1:D0:0D:25:85:2E:14:E7:9A:C4:29:0C:95:47:70:91:7F:5A:1E:15:35:94*

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*Guardtime AS*
Subject O:	*Guardtime AS*
Subject L:	*Tallinn*
Subject ST:	*Harju*

Subject C: *EE*

X509SKI

X509 SK I *975ltyyz5oc++U5o1Qa4HGDAeDU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2021-02-13T22:00:00Z*

2.19.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[et]* *Guardtime KSI ajatempliteenus*

Name *[en]* *Guardtime KSI timestamp service*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATEE-101114112*

Subject E: *publications@guardtime.com*

Subject CN: *Guardtime AS*

Subject O: *Guardtime AS*

Subject L: *Tallinn*

Subject ST: *Harju*

Subject C: *EE*

X509SKI

X509 SK I *975ltyyz5oc++U5o1Qa4HGDAeDU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-04-07T21:00:00Z*

2.20 - Service (withdrawn): Guardtime KSI ajatempliteenus (2020)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[et]* *Guardtime KSI ajatempliteenus (2020)*

Name *[en]* *Guardtime KSI timestamp service (2020)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *100067200787907560827413108 92*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIFYDCCBEigAwIBAgIMIFVdZnGni6mwPnWsMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlHbG9iYWxTaWduIFF1YWxpZmll
ZCBDQSAxMB4XDTIwMDgyMDExMDY1NFoXDTIzMDgyMTExMDY1NFowgccxCzAJBgNVBAYTAkVFMRYw
FAYDVQQIEw1IYXIqdSBtYWFrb25kMRAwDgYDVQQHEwdUYWxsaW5uMRkwFwYDVQQLExBLU0kgUHVi
bGljYXRpb25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT8OcMRYwFAYDVQQDDA1HdWFyZFRpbWUgT8Oc
MSkwJwYJKoZIhvcNAQkBFhpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1LmNvbTEYMBYGA1UEYRMPVkFU
RUUtMTAxMTE0MTEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAntxxAxMzPwFmNY09
BYpYGUZeNQIwmUrbE3Msz+VäBapgIX5oapUjmWuXV0wOXcEMdlxbbhl4wArKuhjZICduZnvfe/T
JSuINrOeGl+FEf9Lc0BLrCPT4sX2XlVfoV6/fyN1uUbGD0ISF3StFynI4S68VgQSFCcNtlLvcIZm
5rMwdw3dh/w5FQQeVmH4/bgr3mc8OCRXkoFW6+LtwRJjg1I4RYR0unME0q+IXOKXV0H6GcJtK82L
lq50bor53qLlVDNfoBnEACD27TeKiyZsL9dwMtU+TcsMC6GEc/ldEkvfSKxu8QnA/i5/JtvGmCHr
2D6CxDGCDNrI7ro8++rXk8QIDAQABo4IBxDCCAcAwDgYDVR0PAQH/BAQDAgZAMIGFBggrBgEFBQcB
AQR5MHcwQAYIKwYBBQUHMAKGNGh0dHA6Ly9zZWN1cmUuZ2xvYmFsc2lnbi5jb20vY2FjZXJ0L2dz
cWNhMXNoYTJnNC5jcnQwMwYIKwYBBQUHMAGGJ2h0dHA6Ly9vY3NwLmdsb2JhbHNpZ24uY29tL2dz
cWNhMXNoYTJnNDBZBgNVHSAEUjBQMEMGCysGAQQBoDIBKCMBMDQwMgYIKwYBBQUHAgEWJmh0dHBz
Oi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkvMAkGBwQAi+xAAQMwCQYDVR0TBAIwADAI
BgNVHREEHjAcgRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1ILmNvbTA3BggrBgEFBQcBAwQrMCkwCAYG
BACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGAjAgBgNVHSUEGTAXBgkqhkiG9y8B
AQUGCisGAQQBgjcKAwwwHwYDVR0jBBgwFoAUrDfbzzLjlRaqCxwGA4bwXcdpzRowHQYDVR0OBBYE
FOM9BPC4T+QE2tBZskLYBs5DhC03MA0GCSqGSIb3DQEBCwUAA4IBAQCYULFVSQs6zmVrmYT5Rkex
oTFYkBD9Kxui4RhX35yz/FLv0QaGhIQmkD9oLc5CYNzL4WpbH4uhEH4npEXGj6Q+HMRvkU4g/HyP
NohgzojxZFe5QLYPvAI3EfED5RLUcI2/Co8bEqn0RYHs3yK+cnUvzd443JOXoR2WsX88sKC2HFxu
gOJlm9gtuQtmCX46Ws98cwsW4NnP2mp/s9y8Fh/lEcQlFQG3rpxIt3ROS7RfGJ06hP1wGCMEh4kp
az0eYf4SA0kpI5FqvF7JD/W+McQZS7o2VGaygXqo4a5g+jra99df1WOShiCb3fkDxfrCPHOZ/utG
2jSKmXlORlcOy/X7

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer CN: *GlobalSign Qualified CA 1*

Issuer O: *GlobalSign nv-sa*

Issuer C: *BE*

Subject 2.5.4.97: *VATEE-101114112*

Subject E: *publications@guardtime.com*

Subject CN: *GuardTime OÜ*

Subject O: *GuardTime OÜ*

Subject OU: *KSI Publications*

Subject L: *Tallinn*

Subject ST: *Harju maakond*

Subject C:	*EE*
Valid from:	*Thu Aug 20 13:06:54 CEST 2020*
Valid to:	*Mon Aug 21 13:06:54 CEST 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9E:DC:71:03:13:33:3F:01:66:35:8D:3D:05:8A:58:19:46:5E:35:09:70:99:4A:DB:13:73:2C:CF:E5:5A:05:AA:60:95:7E:68:6A:95:25:8E:65:AE:5D:5D:30:39:77:04:31:D9:71:6D:B8:48:E3:00:2B:2A:E8:63:64:80:9D:B9:99:EF:7D:EF:D3:25:2B:88:36:B3:9E:1A:5F:85:11:FF:4B:73:40:4B:AC:23:D3:E2:C5:F6:5C:85:5F:A1:5E:BF:7F:23:75:B9:46:C6:0F:42:12:17:74:AD:17:29:C8:E1:2E:BC:56:04:12:14:27:0D:B4:82:EF:70:86:66:E6:B3:30:77:0D:DD:87:FC:39:15:04:1E:56:61:F8:FD:B8:2B:DE:67:3C:38:24:57:92:81:56:EB:E2:ED:C1:12:63:83:52:38:45:84:74:BA:73:04:D2:AF:88:5C:E2:97:57:41:FA:19:C2:6D:2B:CD:8B:96:A4:B4:6E:8A:F9:DE:A2:E5:54:33:5F:A0:19:C4:00:20:F6:ED:37:8A:88:26:6C:2F:D7:70:32:D5:3E:4D:CB:0C:0B:A1:84:73:F9:5D:12:4B:DF:48:AC:6E:F1:09:C0:FE:2E:7F:26:DB:C6:98:21:EB:D8:3E:82:C4:31:82:0C:DA:C8:EE:BA:3C:FA:B5:E4:F1:02:03:01:00:01*
Authority Info Access	*http://secure.globalsign.com/cacert/gsqca1sha2g4.crt* *http://ocsp.globalsign.com/gsqca1sha2g4*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.4146.1.40.35.1* *CPS pointer: https://www.globalsign.com/repository/* *Policy OID: 0.4.0.194112.1.3*
Basic Constraints	*IsCA: false*
Subject Alternative Name	*publications@guardtime.com*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
Authority Key Identifier	*AC:37:DB:CF:32:C9:21:16:AA:0B:1C:06:03:86:F0:5D:C7:69:CD:1A*
Subject Key Identifier	*E3:3D:04:F0:B8:4F:E4:04:DA:D0:59:B2:42:D8:06:CE:43:84:2D:37*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*83:6B:53:11:DA:DB:18:C5:C9:57:8E:09:18:61:C5:59:3A:6B:E4:B5:B8:05:C5:EA:4A:26:B1:15:46:BF:2D:5B*

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*
Subject O:	*GuardTime OÜ*
Subject OU:	*KSI Publications*
Subject L:	*Tallinn*

Subject ST: *Harju maakond*

Subject C: *EE*

X509SKI

X509 SK I *4z0E8LhP5ATa0FmyQtgGzkOELTc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

Status Starting Time *2022-03-22T22:00:00Z*

2.20.1 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[et]* *Guardtime KSI ajatempliteenus (2020)*

Name *[en]* *Guardtime KSI timestamp service (2020)*

Service digital identities

X509SubjectName

Subject 2.5.4.97: *VATEE-101114112*

Subject E: *publications@guardtime.com*

Subject CN: *GuardTime OÜ*

Subject O: *GuardTime OÜ*

Subject OU: *KSI Publications*

Subject L: *Tallinn*

Subject ST: *Harju maakond*

Subject C: *EE*

X509SKI

X509 SK I *4z0E8LhP5ATa0FmyQtgGzkOELTc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2020-09-28T21:00:00Z*

2.21 - Service (withdrawn): Guardtime KSI ajatempliteenus (2021)

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[et]* *Guardtime KSI ajatempliteenus (2021)*

Name *[en]* *Guardtime KSI timestamp service (2021)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *118355836981318486421393061 92*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIGsTCCBJmgAwIBAgIMJj4qVehNPMq23LjQMA0GCSqGSIb3DQEBCwUAMH8xCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9lYWxTaWduIGS2LXNhMTowOAYDVQQDEzFHbG9lYWxTaWduIEdDQyBSNDUg
UXVhbGlmaWVkIFFTQ0QgU2lnbmluZyBDQSAyMDIwMRkwFwYDVQRhExBOVFJCRS0wNDU5MTM0MjU2
MB4XDTIxMDEwNjEyNDEyNFoXDTIzMDgyMTExMDY1NFowgccxCzAJBgNVBAYTAkVFMRYwFAYDVQQI
Ew1IYXJqdSBtYWFrb25kMRAwDg YDVQQHEwdUYWxsaW5uMRkwFwYDVQQLExBLU0kgUHVibGljYXRp
b25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT8OcMRYwFAYDVQQDDA1HdWFyZFRpbWUgT8OcMSkwJwYJ
KoZIhvcNAQkBFhpwdWfJsaWNhdGlvbnNAZ3VhcmR0aW1LmNvbTEYMBYGA1UEYRMPVkFURUUtMTAx
MTE0MTEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr0PRuQ/kZTcxbY+Khgtimytq
K7fwX6hOxnozDX5/YX1G6GQUVCCgLvDPO4u3oELiwW12eW8InJsdeUxhbnly1mqFs+J1asWM1Fdj
pgTEjwhayhURFEZ5VMTyL+CtB8Ue0nGRJZZmqtphh/GFk2hf0KZS24vGdTaERBO5LD8YFzZOLeTmF
PBSDqsdRz0267YtecGndLJ4ZCxq0Z7cA7UYoZvtkmwPo1RKzNX53vQ3p8fPbQq0mIxLIeC70vObd
I0gjLHzj5vipIAbd8oEa+jl0NfjjPQpwM0LyN9yeJZjo4jveaudNXfvGxrMpvfxmJQs6cFVQGfQZ
WVwVrB1z6LNzaQIDAQABo4IB4jCCAd4wDgYDVR0PAQH/BAQDAgZAMIGjBggrBgEFBQcBAQSBIjCB
kzBOBggrBgEFBQcwAoZCaHR0cDovL3NlY3VyZS5nbG9iYWxzaWduLmNvb59jYWNlcnQvZ3NnY2Ny
NDVxdWFscXNjZHNpZ25jYTIwMjAuY3J0MEEGCCsGAQUFBzABhjVodHRwOi8vb2NzcC5nbG9iYWxz
aWduLmNvb59nc2djY3J0NXF1YWxxc2Nkc2lnbmNhMjAyMDBZBgNVHSAEUjBQMEMGCysGAQQBoDIB
KCQCMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkv
MAkGBwQAi+xAAQMwCQYDVR0TBAIwADAlBgNVHREEHjAcgRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1I
LmNvbTA38ggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACO
RgEGAjAgBgNVH5UEGTAXBgkqhkiG9y8BAQUGCisGAQQBgicKAwwwHwYDVR0jBBgwFoAUBbpbOncU
LIeGRvxwFl9idZl0oRgwHQYDVR0OBBYEFAaesnAAlnefqQMdEfF2n4gsTHOXMA0GCSqGSIb3DQEB
CwUAA4ICAQAiR/0mlTxAqooHW7mPhxK0MromXCKtSJ0F6TadH1iU95WfuORXKWxO1BtX87ObZJ8h
pZzX1j6SD1e+5H47pmZC1TAMoEGjmnLjRo7y794FQYoYwlcfByZswLVtkoiy34U25+VDOLWrEds
O0KR7TeE5qO4ZwQ5D34Dvb3O9fgOqLNcqWCRYmvwPYSwNK5zm8pO864iyCvohXxoZF4zyxhK0qmq
ib016ADdXMb16OevELELA3sDjCV+yOU9004fvXdM3R/UFv15NLvB8G+7ehrP3XQuTxbBoaerzSJS
7uhy7Bcl1kOQO+M/59xvFX9GzBHto2SDPiGbgu5/uFJocQE9ntxGCZF5ypxaAamvaPffUQdtrhKA
KszBHjIPdHZ2L3iUl/8So/BA847Q5KhH1rwyOFV2e93Ow9oY+GcHW7fM35umXgYxNvQUk4ZGRK24O
ZsxbEyGVoCwHXj4jTkuXpPZcbE3Ik8Mp8ig/96RrQD3zBIvVfK7QZW9WPZ+8OUC9laX2oqbMLAaE
SWvG4Wrz08sHTIYLQZBnTCymjL/ud+8gFmeXuPoWxvqsGF+FZyGDZibERC0L0rgAQ4IqXEsFNI09
Esc6RQ1oJnmsTtcaOCVq81Vv/8FuD9SK8YExEliRlvNfd1ladNTr4vWMm/DjDGszdNXRzvBBr0ES
lQUBGJDNVw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *NTRBE-0459134256*

Issuer CN: *GlobalSign GCC R45 Qualified QSCD Signing CA 2020*

Issuer O: *GlobalSign nv-sa*

Issuer C: *BE*

Subject 2.5.4.97: *VATEE-101114112*

Subject E: *publications@guardtime.com*

Subject CN: *GuardTime OÜ*

Subject O: *GuardTime OÜ*

Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*
Valid from:	*Wed Jan 06 13:41:24 CET 2021*
Valid to:	*Mon Aug 21 13:06:54 CEST 2023*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AF:43:D1:B9:0F:E4:65:37:31:6D:8F:8A:86:0B:62:9B:2B:6A:2B:B7:F0:5F:A8:4E:C6:7A:33:0D:7E:7F:61:7D:46:E8:64:14:54:20:AA:2E:F0:CF:3B:8B:B7:A0:42:E2:C1:6D:76:79:6F:08:9C:9B:1D:79:4C:61:6E:72:32:D6:6A:85:B3:E2:75:6A:C5:8C:D4:57:63:A6:04:C4:8F:08:5A:CA:15:11:14:46:79:54:C4:F2:2F:E0:9F:05:47:B4:9C:64:49:D9:99:AA:B6:98:61:FC:61:64:DA:17:F4:29:94:B6:E2:F1:9D:4D:A1:11:04:EE:4B:0F:C6:05:CD:93:8B:79:39:85:3C:14:83:AA:C7:4F:CF:4D:BA:60:BB:5E:70:69:DD:2E:3E:19:08:1A:B4:67:B7:00:ED:46:28:66:FB:64:9B:03:E8:D5:12:B3:35:7E:77:BD:0D:E9:F1:F3:DB:42:AD:26:97:12:C8:78:2E:F4:BC:E6:DD:23:48:23:2C:7C:E3:E6:F8:A9:20:06:DD:F2:81:1A:FA:39:74:35:F2:63:3D:0A:70:33:42:F2:37:DC:9E:25:98:E8:E2:3B:DE:6A:E7:4D:5D:FB:C6:C6:B3:29:BD:FC:66:25:0B:3A:70:55:50:19:F4:19:5A:FC:15:AC:1D:73:E8:B3:73:69:02:03:01:00:01*
Authority Info Access	*http://secure.globalsign.com/cacert/gsgccr45qualqscdsignca2020.crt* *http://ocsp.globalsign.com/gsgccr45qualqscdsignca2020*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.4146.1.40.36.2* *CPS pointer: https://www.globalsign.com/repository/* *Policy OID: 0.4.0.194112.1.3*
Basic Constraints	*IsCA: false*
Subject Alternative Name	*publications@guardtime.com*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
Authority Key Identifier	*05:BA:5B:3A:77:14:2C:87:86:46:FC:70:16:5F:62:75:99:74:A1:18*
Subject Key Identifier	*06:9E:B2:70:00:96:77:9F:A9:03:1D:11:F1:76:9F:8A:AC:4C:74:17*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*96:DF:B9:E3:A5:3D:FB:C3:B6:4D:E5:FA:C4:5C:2E:29:57:95:3A:00:9C:1A:9D:71:1B:2A:98:BB:68:10:1F:96*

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*

Subject O:	*GuardTime OÜ*
Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*

X509SKI

X509 SK I	*Bp6ycACWd5+pAx0R8XafiqxMdBc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description	*[en]*	*undefined.*

Status Starting Time

2025-06-12T09:00:00Z

2.21.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name	*[et]*	*Guardtime KSI ajatempliteenus (2021)*
Name	*[en]*	*Guardtime KSI timestamp service (2021)*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*
Subject O:	*GuardTime OÜ*
Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*

X509SKI

X509 SK I *Bp6ycACWd5+pAx0R8XafiqxMdBc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-02-13T22:00:00Z*

2.22 - Service (withdrawn): Guardtime KSI Time-stamping service (2023)

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

Service Name

Name *[en]* *Guardtime KSI Time-stamping service (2023)*

Name *[et]* *Guardtime KSI ajatempliteenus (2023)*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *178134478399250258750962616 14*

X509 Certificate


```
-----BEGIN CERTIFICATE-----

MIIG/DCCBOSgAwIBAgIMOY7wTmAM4B7sRFPuMA0GCSqGSIb3DQEBCwUAMH8xCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMTowOAYDVQQDEzFHbG9iYWxTaWduIEdDQyB5NDUg
UXVhbGlmaWVkIFFTQ0QgU2lnbmluZyBDQ5AyMDIwMRkwFwYDVQRhExBOVFJCRS0wNDU5MTM0MjU2
MB4XDTIzMDgwMTE2NTUzM1oXDTI2MDcyODAwMDAwMFowgccxCzAJBgNVBAYTAkVFMRYwFAYDVQQI
Ew1IYXlqdSBtYWFrb25kMRAwDgYDVQOHEwdUYWxsaW5uMRkwFwYDVQOLExBLU0kgUHViBGlJYXRp
b25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT8OcMRYwFAYDVQQDDA1HdWFyZFRpbWUgT8OcMSkwJwYJ
KoZIhvcNAQkBFhpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1ILmNvbTEYMBYGA1UEYRMPVkFURUUtMTAx
MTE0MTEyMIIBIjANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqddlsZ9Nc5xsctW09zEjN3Hi
8Rj2gl5eLg1+AlqLp+ZpmCo+teFtEGGstanKW07nrcM9qlMsL30R/MlkeyI+ass6AbpQfE84XdkT
LBy92qAHqxYTYkvXGxK8zfcZh2vlZCfecCG8IDFxh0yozQBtHRi8BqsC9R5V2L5msu1X87rRner9
WKwJbUDpM8uAYTXc8dfK5/rhAPx06oxSls+kcvvqi9Hfv4NSZSUTIhdWyDvjutiYjhNa1vDwaorO
owPKL7dfQiTUUnqWRMxZP6ishhSuATr4rp27lZSorw3hTwHoQeQHzQ865UdQSe92abiPGHP8Hqju
335Com3MlMtoRQIDAQABo4ICLTCCAikwDgYDVR0PAQH/BAQDAgZAMIGjBggrBgEFBQcBAQSBljCB
kzB0BggrBgEFBQcwAoZCaHR0cDovL3NlY3Vyc2S5nbG9iYWxzaWduLmNvb59jYWNlcnQvZ3NnY2Ny
NDVxdWFscXNjZHNpZ25jYTlwMjAuY3J0MEEGCCsGAQUFBzABhjVodHRwOi8vb2NzcC5nbG9iYWxz
aWduLmNvbS9nc2djY3I0NXF1YWxxc2Nkc2InbmNhMjAyMDBZBgNVHSAEUjBQMEMGCysGAQQBoDIB
KCQCMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2lhbHNpZ24uY29tL3JlcG9zaXRvcnkv
MAkGBwQAi+xAAQMwCQYDVR0TBAIwADBjBgNVHR8EQjBAMD6gPKA6hjhodHRwOi8vY3JsLmdsb2lh
bHNpZ24uY29tL2dzZ2NjcjQ1cXVhbHFzY2RzaWduY2EyMDIwLmNybDAIBgNVHREEHjAcgRpwdWJs
aWNhdGlvbnNAZ3VhcmR0aW1ILmNvbTA3BggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYB
BDATBgYEAI5GAQYwCQYHBACORgEGAjAgBgNVH5UEGTAXBgkqhkiG9y8BAQUGCisGAQQBgjcKAwww
HwYDVR0jBBgwFoAUBppOncULleGRvxwFi9idZl0oRgwHQYDVR0OBBYEFI6z5c12tsdlDk3ha6m9
8I4/L13MA0GCSqGSIb3DQEBCwUAA4ICAQAnDWBUOJWUttYZgPzzh3E1vf6/jsWyr22VKemOOb2w
+HBGVmsjGVRogTTeNfmumWc+X44iESZ6BpLETali8F/ygMjhblE8Trth/3fduXhgUZQnM6AJlfNV
kiyT95kvZJaRwZTjFGIb1J9Wtv4dfGwkm3XyjTV0g/m+4jVg7nOhEWpXP1X4sqYZtqckiVOp0pNd
D52KHTPN5FvLpu35+iJxxIy1jFQUYUIAX99RBqbxk4D0GwdieT7T40zRWP5CrgPIFnCwyiGstslv
OeNLybhwTYrpQyxNx9nr6jZ8B5sNKhDRg91x2vaSI4JjIERQr4m6K/RB1WPM8NCQcqC94UG+/xT1
oFGMPY066pkKDQfg119txahIH/qcG7XbXRblm0DP6uSe3luQJz0UT+2k0WHNRleuUsCgshf4A82X
oRIBGbPeg7pOf1YCay6P4io/eBC09gc4l/fv6aa/MRPaW/ZmnSONMy446Wx0aAWQ8XQjV9wR/UDH
H9NM0GokpyYOlaLDHFCBQ0M463y7Pl9Bcap/d2WlG0/RG8LvqOl7qXMVvYDv6h2CeHTI2nHvaZx1
jeH+QBmxkHh/nAqvnogN3m3nLjFWfYhcgM2+7dhi/fDN5+5D+B9GbNdE8OyFgYxqp/AqCojh9Wvnaj
KhS75jBBUseNVYDBFmM3M2ELApdkvjXXJw==

-----END CERTIFICATE-----
```


Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *NTRBE-0459134256*

Issuer CN: *GlobalSign GCC R45 Qualified QSCD Signing CA 2020*

Issuer O: *GlobalSign nv-sa*

Issuer C: *BE*

Subject 2.5.4.97: *VATEE-101114112*

Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*
Subject O:	*GuardTime OÜ*
Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*
Valid from:	*Tue Aug 01 15:55:33 CEST 2023*
Valid to:	*Tue Jul 28 02:00:00 CEST 2026*
Public Key:	*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A9:D7:65:B1:9F:4D:73:9C:6C:72:D5:B4:F7:31:23:37:71:E2:F1:1F:E3:DA:09:79:78:88:35:F8:02:2A:2E:9F:99:A6:60:A8:FA:D7:85:B4:41:86:B2:D6:A7:29:6D:3B:9E:B7:0C:F6:A3:2C:2F:7D:11:FC:C2:24:7B:29:7E:6A:CB:3A:01:BA:50:7C:4F:38:5D:D9:13:2C:1C:BD:DA:A0:07:AB:16:13:62:4B:D7:1B:12:BC:CD:F7:19:87:6B:E5:64:27:DE:70:21:BC:88:31:71:87:4C:A8:CD:00:6D:1D:18:BC:06:AB:02:F5:1E:55:D8:B4:A6:B2:ED:57:F3:BA:D1:9D:EA:FD:58:AC:09:6D:40:E9:33:CB:80:61:35:DC:F1:D7:CA:E7:FA:E1:00:FC:74:EA:8C:52:22:CF:A4:72:FB:EA:8B:D1:DF:BF:83:52:65:25:13:22:17:56:C8:3B:E3:BA:D8:98:8E:13:5A:D6:F0:F0:6A:8A:CE:A3:03:CA:2F:B7:5F:42:24:D4:52:7A:96:44:CC:59:3F:A8:AC:86:14:AE:01:3A:F8:AE:9D:BB:95:94:A8:AF:0D:E1:4F:01:E8:41:E4:07:CD:0F:3A:E5:47:50:49:EF:76:69:B8:8F:18:73:FC:1E:A8:EE:DF:7E:42:A2:6D:CC:94:CB:68:45:02:03:01:00:01*
Authority Info Access	*http://secure.globalsign.com/cacert/gsgccr45qualqscdsignca2020.crt* *http://ocsp.globalsign.com/gsgccr45qualqscdsignca2020*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.4146.1.40.36.2* *CPS pointer: https://www.globalsign.com/repository/* *Policy OID: 0.4.0.194112.1.3*
Basic Constraints	*IsCA: false*
CRL Distribution Points	*http://crl.globalsign.com/gsgccr45qualqscdsignca2020.crl*
Subject Alternative Name	*publications@guardtime.com*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
Extended Key Usage	*Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
Authority Key Identifier	*05:BA:5B:3A:77:14:2C:87:86:46:FC:70:16:5F:62:75:99:74:A1:18*
Subject Key Identifier	*8E:B3:E5:CD:76:B6:C7:65:0E:4D:E1:6B:A9:BD:F0:8E:25:FC:BD:77*
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*81:CA:ED:E8:94:74:B3:C0:B8:97:91:EC:F5:DB:3C:3B:6E:5F:4E:56:24:5E:C5:60:A6:09:A9:B1:51:09:D6:09*

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*
Subject O:	*GuardTime OÜ*
Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*

X509SKI

X509 SK I	*jrPlzXa2x2UOTeFrqb3wjiX8vXc=*

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

Service status description *[en]* *undefined.*

Status Starting Time

2025-06-12T09:00:00Z

2.22.1 - History instance n.1 - Status: granted

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name	*[en]*	*Guardtime KSI Time-stamping service (2023)*
Name	*[et]*	*Guardtime KSI ajatempliteenus (2023)*

Service digital identities

X509SubjectName

Subject 2.5.4.97:	*VATEE-101114112*
Subject E:	*publications@guardtime.com*
Subject CN:	*GuardTime OÜ*
Subject O:	*GuardTime OÜ*

Subject OU:	*KSI Publications*
Subject L:	*Tallinn*
Subject ST:	*Harju maakond*
Subject C:	*EE*

X509SKI

X509 SK I	*jrPlzXa2x2UOTeFrqb3wjiX8vXc=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*
Status Starting Time	*2023-08-20T09:00:01Z*

3 - Signature node - Id: id-6fe6a8ce1c109d25015e2999c95b42ac

.

Signing Time

2025-06-12T12:16:26Z

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *11132080187539732902*

X509 Certificate


```
-----BEGIN CERTIFICATE-----
MIIDrDCCApSgAwIBAgIJAJp9F/NFeDmmMA0GCSqGSIb3DQEBDQUAMG0xLjAsBgNVBAMMJUVzdG9u
aWFuIFRydXN0ZWQgTGlzdCBTY2hlbWUgT3BlcmF0b3lxCzAJBgNVBAYTAkVFMS4wLAYDVQQKDCVF
c3RvbmlhbiBjbmZvcm1hdGlvbiBTeXN0ZW0gQXV0aG9yaXR5MB4XDTE5MDEyNTA5NDAwNloXDTI4
MDcyNDA5NDAwNlowbTEuMCwGA1UEAwwlRXN0b25pYW4gVHJ1c3RlZCBMaXN0IFNjaGVtZSBPcGVy
YXRvcjELMAkGA1UEBhMCRUUxLjAsBgNVBAoMJUVzdG9uaWFuIEluZm9ybWF0aW9uIFN5c3RlbSBB
dXRob3lpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBMux4ivfdIZy9W75NgMWf
D7ahajygYHCp8Tw9LxQ0vkmpuyaNNlXU+uj+yffWfekVgMoLaQrCpVlN0FF8ZMnnlsK600hpgnQN
I+snPxU1u9BK6P87ZpoQU2wvan2oqjWflm06ybLzvvJrPjVNoVelrUDTY65PngMbygqpsdXo+dW8
916ZoRUcEkTFWjOXVjhY1Lqsorbpaop1iv9BV2SXmsh4szRlqpu4dDSEIWViBn0+A1ptiSAt7JIN
r0DDJfswqE+dhvjf6xq+lEaqUoMtGPKqz7SDqKKyg/KBO1ZGunUZE+91HKUASt+sPy3O3wMZM1Sp
Ze1lNEXQ0EQ4gytdAgMBAAGjTzBNMAwGA1UdEwQFMAMCAQAwCwYDVR0PBAQDAgeAMB0GA1UdDgQW
BBScAndEhykw8vEHVFuQ7XPtHnqFajARBgNVHSUECjAIBgYEAJE3AwAwDQYJKoZIhvcNAQENBQAD
ggEBAHaLclDZmUA9Bcv7TjuQW2Q3cFWFSmKc8aT5HaRKBxRRy10j9czqT439w/sm T4De8JYyULXU
+SoUX6/5sjmcpYxczFIC6imH8XLTqOca3vRAhek5iM80+h6v8CvxQHrsqNiSrLlmE4LWfXWhQ/WP
cyQdNrHCFrynJ9Gf6Q1DzQBRstpj5l8WjE+ME+w+vDj+VHHjl4wd5NkJhwwaF5PFB6uRrdb95e1d
qLe4CTALe6+dh2QYhzSWZ+AZ2GaF+LIFreHhyV0sI+KwcNKSzSotStHL0zPTnq/yxPNaihhFmAIP
dZdwq7vTN+yn5PAqEcfhTn06Gf5yDZjrmf5JO5eMpzM=

-----END CERTIFICATE-----
```


Signature algorithm: *SHA512withRSA*

Issuer O: *Estonian Information System Authority*

Issuer C: *EE*

Issuer CN: *Estonian Trusted List Scheme Operator*

Subject O: *Estonian Information System Authority*

Subject C: *EE*

Subject CN: *Estonian Trusted List Scheme Operator*

Valid from: *Fri Jan 25 10:40:06 CET 2019*

Valid to: *Mon Jul 24 11:40:06 CEST 2028*

Public Key:


```
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:32:EC:78:8A:F7:DD:95:9C:BD:5B:BE:4D:80:C5:9F:0F:B6:A1:6A:3C:A0:60
:70:A9:F1:3C:3D:2F:14:34:BE:49:A9:BB:26:8D:36:55:D4:FA:E8:FE:C9:F7:D6:7D:E9:15:80:CA:0B:69:0A:C2:A5:52:0D:D0:51:7C:64:C9:E7:96:C2:BA:D3:48:69:82:74:0D:23:EB:27:3F:15:
35:BB:D0:4A:E8:FF:3B:66:9A:10:53:6C:2F:6A:7D:A8:AA:35:9F:96:6D:3A:C9:82:F3:BE:F2:6B:3C:95:4D:A1:57:A5:AD:40:D3:63:A4:8F:9E:03:1B:CA:AA:A9:B1:D5:E8:F9:D5:BC:F7:5E:99:A
1:15:1C:12:44:C5:5A:34:17:56:3B:58:D4:BA:AC:A2:86:E9:6A:8A:75:8A:FF:41:57:64:97:9A:C8:78:B3:34:65:AA:9B:B8:74:34:B4:95:65:62:D6:7D:3E:03:5A:6D:89:20:2D:EC:92:0D:AF:40:
C3:8D:FB:30:A8:4F:9D:86:F8:DF:EB:1A:BE:20:46:AA:52:83:2D:18:F2:A0:CF:B4:83:A8:A2:B2:83:F2:81:3B:56:46:BA:75:19:13:EF:75:1C:A5:00:4A:DF:AC:3F:2D:CE:DF:03:19:33:54:A9:6
5:ED:48:34:45:D0:D0:44:38:83:2B:5D:02:03:01:00:01
```


Basic Constraints *IsCA: false - Path length: 0*

Subject Key Identifier *9C:02:77:44:87:29:30:F2:F1:07:54:5B:90:ED:73:ED:1E:7A:85:6A*

Extended Key Usage *id-tsl-kp-tslSigning*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *51:F3:58:D9:0E:9F:C6:E1:3A:8D:04:83:44:E2:17:19:50:BD:AE:86:AA:7F:1E:13:A6:8B:A4:BC:3B:1B:94:A7*