EESTI (ESTONIA) : Trusted List

Tsl Id: EE0001

Valid until nextUpdate value: 2024-08-07T08:07:14Z

TSL signed on: 2024-02-07T10:29:55Z

PDF generated on: Wed Feb 07 11:32:04 CET 2024

TSL Scheme Information

TSL Id

EE0001

TSLTag

http://uri.etsi.org/19612/TSLTag

TSL Version Identifier

5

TSL Sequence Number

64

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: *620818890745556847869731431413617216995310914687*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIH9DCCBdygAwIBAgIUbL57W2NNkznemb+sNTEfKSmLTH8wDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIlURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTEIGSUVEIENBIExMB4XDTIzMDQyMTE1NTk0M1oXDTI2MDQy
MDE1NTk0M1owggFPMQswCQYDVQQGEwJCRTE9MDsGA1UECwww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
lFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWJlcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWkSZ
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGViZW50IC0gRUMgU1RBVFVVT1JZIFNUQUZGMSgwJgYJKoZIhvcNAQkBFhlqZXJvZW4ucmF0uGVA
ZWMuZXYyb3BhLmV1MQ8wDQYDVQQEDAZSQVRIw4kxGDAWBgNVBCoMD0pFUk9FTiBBU5PTEQgTDEd
MBsGA1UECwwUUmVtb3RlIUmV0DRE1hbmnFnZW1lbnQxHzAdBgNVBAMMFKpFUk9FTiBBU5PTEOgTCBS
QVRIw4kwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDgC5u493b8aZqWC+wdf0+1/ILG
/c+XYcHQiNxCL0kCVEo+sRt9z55sX2wHmon/aXsiS4twfqk9AQxIWpLyXuZa3jRrBil55Bdqtmh+
2+rV0AuOhHhupwAKO52bP+yISU8G4r+g+NzYUMwNCDM9myi0ASxFiVqRV+ogU5tWmaRJ7sazSXa
G9sjsS31SZilsyivMH72jtheQtYEmdfc0GKa2CnJ9vcxS/+1ht9yMCfH/OzTZXOPbt9v8dVXx2TV
1pZaDB/1Bl8qPGew2YRL7WPGn2GnNm1dm7H5vL3l5pz5An9mQR4iu1uj2WALi+9BzauxLyQnhCCM
WawIofaNrrudAgMBAAGjggK0MIICsDAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFHN8U/AcFAR8
mhJ/+i/NXGcjGOkUMIGGBggrBgEFBQcBAQR6MHgwRgYIKwYBBQUHMAKGOmh0dHBzOi8vcWNhbC5cx
LmRpZ2l0YWxzaWduLnB0L0RJR0lUQUxTSUdOUVVBTEIGSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGG
Imh0dHBzOi8vcWNhbL.WcxLmRpZ2l0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEEMAkGBwQAi+xAAQlw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEsGA1UdHwREMEIwQKA+oDyGOmh0dHBzOi8v
cWNhbLWcxLmRpZ2l0YWxzaWduLnB0L0RJR0lUQUxTSUdOUVVBTEIGSUVEQ0FHMS5jcmwwHQYDVR0O
BBYEFBvvbgFnORNt1Dwbohrc8igrqWC5MA4GA1UdDwEB/wQEAwIGQDCB0wYIKwYBBQUHAQMEgcYw
gcMwCAYGBACORgEBMAgGCBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATBqBgYEAI5GAQUwYDAu
FihodHRwczovL3F5S1nMS5kaWdpdGFsc2lnbi5wdC9QRFNNEhQucGRmEwJwdDAuFihodHRwczov
L3FjYYS1nMS5kaWdpdGFsc2lnbi5wdC9QRFNlZW4ueuJlbjAVBggrBgEFBQcLAjAJBgcEAIvs
SQEBMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQIwDQYJKoZIhvcNAQENBQADggIBACHUd1cXS1SNDV6Z
YIzoVoxk3LaOLrGoS12X33snN8eaHQ78UyjMlmul6xBfC9qt0T0wS5apuq3UGpg2Xir983dPHea
weu43sx1fkdpPnltDm/KcwwGxb0/LvrAr4F1lvGRmHD2dmwBs2G7Qqxyvh38nsCzuKEA4ySuMPL
6XOCuoXxAfeM9S1kVikHzCUcwamL9k4+2+KdusJDXvRMlWcpgHjkfCZgb+ELIpLOkVQ7bdRPPJn
9isSFoU6/Gbc/01THQvaNPRS948ITi6iMSwOfHI8BXvSF0k/XBodfXv/C3VhZoxivMtvX1e4jyhO
E9y7G8kSiJd5zty6JIG+Tr9YP04bOH13C0yYvgr8Wrpx26o+9N5sS54OQ3/VHw6+yU67cBAU//JUk
FbFz3FqU+r6s5oXnRxnrMQPNKAx7+VuvvE9Vc5c6iM7LiHMbCkgBeQq67YYiuQJ73+Pc/10lOR/3/
GtoS+g3xJYKSMfJyLqwUFO4gJhLPm8DYSXrWymqEzQ1extyCMO75v1o/UVsKabFAG1XHqgUlXsiK
XoidcAC6H4zkK95NmVy6Bl2ws3UVH6/Nz9r2pH9VXtiRLr1CjCq+k8CuGFS6COQWtqdylb0FwmtA
s81cd88W7l1lXWyF8mrxu55zf0qHxsTwFxyB57kCk4km92MalqzuOQYZ0LzW

-----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:EB: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:	*660862747298009142807362633871991440505734410485*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIIoDCCBoigAwIBAgIUc8IcSUtVEKAMMvHm9QWU05kXsPUwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTIzMTExNzEwMTE0NloXDTI3MTEx
NzEwMTE0NlowggEVMQswCQYDVQQGEwJMVTFDMEEGA1UECww6Q2VydGlmaWNhdGlvblHvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE9yZFuaXphdGlvbjE5MDcGA1UECwwwRGlyZW50b3Jh
dGUtR2VuZXJhbCBmb3IgRGlnaXRhbCBTZXJ2aWNlcyAoRElHSVQpMSMwIQYDVQRhDBpMRUlYRy0y
NTQ5MDBaTllBMUZMVVE5VTM5MzEcMBoGA1UECgwTRVVST1BFQU4gQ09NTUlTU0lPTjElMCMGCSqG
SIb3DQEJARYWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTEcMBoGA1UEAwwTRVVST1BFQU4gQ09NTUlT
U0lPTjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKWYeBA9kYAREIGnHoJRNpbby44G
+TSJcgHl9QtyXlYjB234hSAYyJvW+gKvoownskrogfUP6GOmQgEFZX335Y0sBwfppVemEoe9H9Aj
/cpT14IqdB05V4a88ASRfR0Va1xmQJrDsBZWqZHx0EEHBctIF5BtyTMAcQvbha+4AOlotp3dF/7Z
A3Cu4GYbN9BuQyyqfgrjMduDzzDjVwKC17aEsLev60C1FnIJ/FVEda3USGiID5JyUceTaRcot1r
w6gjKrOVhwP/UHfev13JCsQsuAzkf7ivzHzYuPPPR9Usecwr7O95Fr4wbPYIyX2AOTIieAC7GMV
XHN1/+4LH74ndvoJYEScXwmN95kib3+G6TquOCQxvNXzHPZb95btCoSnVprCn14O3CXUTZMEKkhP
uKW8dl6pR2JSGbtT+xBkcc1wYVIUnzE3d+YK5SSevUT2COwJM+AcjSoUaRTBINsD/ezDDvv7vtbF
1XccaJjoCNkurzayTsMszGDvAF17ILY69lNY6yK0uzrS+3c/hEHctXa5KIC3PpWrBGQ5mw73KerR
vnAhzDZemVquPk1D59aJNfHoHXmy1bS52rHWYOwHH+2qbODdb8GkHwHXBzSpFit1Kg2brpavhztN
aGlj6GsLFAbr8okCUJllOOLQ8Tfy9Vnn5Rq0+7VTdd8dAxg9AgMBAAGjggKaMIICljAMBgNVHRMB
Af8EAjAAMB8GA1UdIwQYMBaAFHNJ8UAcFAR8mhJ/+i/NXGcjGOkUMIGGBggrBgEFBQcBAQR6MHgw
RgYIKwYBBQUHMAKGOmh0dHB2Oi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L0RJR0lUQUxTSUdOUVVB
TElGSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGGImh0dHB2Oi8vcWNhLnB0L0RJR0lUQUxTSUdOUVVB
TElGSUVEQ0FHMS5wN2IwLgYIKwYBBQUHMAGGImh0dHB2Oi8vcWNhLnB0L0RJR0lUQUxTSUdOUVVB
L29jc3AwIQYDVR0RBBowGIEWZGlnaXQtZG1vQGVjLmV1cm9wYS5ldTBfBgNVHSAEWDBWMDcGCysG
AQQBgcd8BAEBMCgwJgYIKwYBBQUHAgEWGmh0dHB2Oi8vcGtpLmRpZ2l0YWxzaWdu.LnB0MBAGDisG
AQQBgcd8BAIBAQEGMAkGBwQAi+xAAQMwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMIIG8
BggrBgEFBQcBAwSBrzCBrDAVBggrBgEFBQcLAjAJBgcEAIvsSQECMCAgGBgQAjkYBATAIBgYEAI5G
AQQwEwYGBACORgEGMAkGBwQAjkYBBgIwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGln
aXRhbHNpZ24uxcHQvUERTX2VuLnBkZhMCZW4wLhYoaHR0cHM6Ly9xY2EtZzEuZGluaXRhbHNpZ24u
cHQvUERTX3B0LnBkZhMCcHQwSwYDVR0fBEQwQjBAoD6gPIY6aHR0cHM6Ly9xY2EtZzEuZGluaXRh
bHNpZ24uHQvRElHSVRBTFNJR05RVUFMSUZJRURDQUcxLmNybDAdBgNVHQ4EFgQUIO5hwcl9/63i
ssm59r+TIHeJSZwwDgYDVR0PAQH/BAQDAgZAMA0GCSqGSIb3DQEBDQUAA4ICAQCn8qjJbTc3SsD7
cB8S8kDzt+CBnJJm7bOFc9t9IU6iKntVtjPU4T+cYiPk8TnT+/w7dBphRzjZCL1sDfSJGQ5JPBw+
hBPuvzEqP4xVi5i4Jhg/GpYSaa2+dkFXlKe6Sd+ii/RnwBSnfqVfNZtasj7yX+oujGauSLSUPIkQ
xDrMie8KjsNtlkFjQDoioGAx8b0u6WyhAuqwEacCznfl20Dim3sC7XJw8GHumrnW52tUzl4sbXoT
BAt8F1zPCbEbjU0oc8SbFNPIChh+9sHUorErmHlkcg30LBHihkDCx4mK8J60Jybk57D4U2RO29VsJ
fDmnvNx0ZxfLHEJ2tkh+AMqlJXPDlvXQ+rZ1NmLHrbXkcHOlqR3F8Bak1i2Mi5AZZfkfjZjkigE
StN6Enaq6gwF7EsslqEKmhSQ8XlhxWSRqljK/cnEUw+NhrvR4WuKlvYmxlCLQj6q89Hh12IaUGUh
L2L2WCVBjVXqux7s4mvECDzrucl5ilaVT32HO3g8qNLGD5lum53U5v/Nv68ItyHH96unztwBebmg
ox8giVRdzPhmPrpSfbmeNNDKj1p9SCeOvd3P9jCUvChVvH2P2ZUjc24tWe+tzcIsCJi7GbKrt6kjH
c1jFudjehflAbm1lZAYdDNrhXamnsRVsz7iSH20eygCArlwSQ//WlQZPFrRflg==
-----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:F8:8 5:20:18: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:9B: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:CF:30:E3:57:02:82:D7:B6:84:B0:B7:AF:EB:40: B5:16:72:09:FC:55:44:75:AD:E5:25:21:A2:94:3E:49:C9:47:1E:4D:A4:5C:A2:DD:6B:C3:A8:23:2A: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:C3:0E:FB:FB:BE:D6: C5:D5:77:1C:68:98:E8:08:D9:2E:AF:36:B2:4E:C3:2C:CC:60:EF:00:5D:7B:D4:B6:3A:F6:53:58:EB:22:B4:BB:3A:D2:FB:77:3F:84:41:DC:B5:76:B9:28:80:B7:3E:95:AB:04:64:39:9B:0E:F7:29:EA:D1:BE:70:21:CC:36:5E:99: 5A:AE:3E:4D:43:E7:D6:89:35:F1:E8:1D:79:82: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:F2:89:02:50:99:6 5:38: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:8 3:96:B1*

EU TSL digital identities

.

TSL Scheme Operator certificate fields details

Version:	*3*

Serial Number:

1657512121420468650997947332332931841557825880036

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIIAjCCBeqgAwIBAgIUHQiKmcmM7NMyG25PRlC8Qs9VpoQwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGIUVEIENBIEcxMB4XDTIzMTAwMjEzMjk1MFoXDTI2MTAw
MTEzMjk1MFowggFaMQswCQYDVQQGEwJSTzE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWJlcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RBVFVUT1JZIFNUQUZGMSswKQYJKoZIhvcNAQkBFhxhZHJpYW4uY3JvaXRv
cnVAZWMuZXVyb3BhLmV1MREwDwYDVQQEDAhDUk9JVE9SVTEaMBgGA1UEKgwRQ09OU1RBTlRJTiBB
RFJJQU4xHTAbBgNVBAsMFFJlbW90ZVFTQ0RNYW5hZ2VtZW50MSMwIQYDVQQDDBpDT05TVEFOVElO
IEFEUklBTiBDUk9JVE9SVTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMEPfdAKKFfK
pCzoMFhBvEv5OI0t9wQ1Ua5JzVpENOOKKjS9Cm/lwzyTLsWuLJDqaUvmI6oTOZ4TYo7WaFyyi2YV
q4TSVXo9G8t8RykHMu13vwrCyoMJ/GucZ9ypgkRnEEWUdvUQN26ROmCsryBIfvCpC/Pe9tF6Oh6d
Bi2CmX8HlE43zNYOkVuikxa5ymB13W1ySNKV920My/ZCIpFoEyW34H3+6ZNR7Iwh6b6T4QkIMkj
cRTTaeMTYD/kaQV+IFntXlfP2of6Xdqaif39nJeuthCpgL8ciWAE3mb0vuJIRXAcrHRhj2qDT3kX
Jvpo8S+qmkvMIRdabzeYbVzo+3kCAwEAAaOCArcwggKzMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUc0nxQBwUBHyaEn/6L81cZyMY6RQwgYYGCCsGAQUFBwEBBHoweDBGBggrBgEFBQcwAoY6aHR0
cHM6Ly9Y2EzEuZzGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFMSUZIRURDQUcxLnA3YjAu
BggrBgEFBQcwAYYaHR0cHM6Ly9xY2EzEuZzGlnaXRhbHNpZ24ucHQvb2NzcDANBgNVHREEIDAe
gRxhZHJpYW4uY3JvaXRvcnVAZWMuZXVyb3BhLmV1MF8GA1UdIARYMFYwNwYLKwYBBAGBx3wEAQEw
KDAmBggrBgEFBQcCARYaaHR0cHM6Ly9wa2kuZGlnaXRhbHNpZ24ucHQwEAYOKwYBBAGBx3wEAgEB
AQQwCQYHBACL7EABAjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwQwSwYDVR0fBEQwQjBA
oD6gPIY6aHR0cHM6Ly9xY2EzEuZzGlnaXRhbHNpZ24ucHQvREIHSVRBTFNJR05RVUFMSUZIRURD
QUcxLmNybDAdBgNVHQ4EFgQUInlF6Cl5HKvUE35Ifm8y7cfQvvAwDgYDVR0PAQH/BAQDAgZAMIIHT
BggrBgEFBQcBAwSBxjCBwzAIBgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcEAI5GAQYB
MGoGBgQAjkYBBTBgMC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19zd2ZGYT
AnB0MC4WKGh0dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19lbi5wZGYTAmVuMBUGCCsG
AQUFBwsCMAkGBwQAi+xJAQEwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjANBgkqhkiG9w0BAQ0FAAOC
AgEACH5DHJNDzsMXTu+ph7fXEEbFK6xqbg68tRcvwr7xgmaAwfM2pGjq62O637y5yVfYT6Aa7oiC
4ssh77Tu/c/UHpjTn4/tDghkwlhSkUc9FREmOu9doRLWNJ6OE31UBW94w9s0EjpvFJLpkODv0F2M
4iq7LMtV7H0M+ggNA+cMa2NnyRZCCNVKoP8CxgQySigv7DhSX7SahhaKJUQqE5yXvrjBZvrIyESl
TCtoLFa0mWljWlW4aVf4P+m1lL/Cpqzpl.c5B9m1gXxwzJzU70lDcQgLdTka/QBFKTvD0F8+6qUqaz
M6+26ddFOQegX8Kc8xzvyXss1bu8JqXKwjzEwHd6ywAWggJi7v1+KlT0DvX0Y4X8kSh9X5Xuz5tj
Znby0hvP7qQSXhHsYUOrxU3Dkj8Vk/vDKhnCuTdJcEaCrcdWbimNib4YlicCQOoE79XL5/KQ5gY
geCGkudcLkteOfvDBM/G8HbqSbv4x8+HEdnjgoCL4lv4iaD4qtpfvkU6bRXlMrT2Q4Q7pg/Mo02j
h66+S9HoXtoBUeUZMWER2QkjUG1CbOOwcIIw6GuiCZ7BRSut0tG3C54f0jBdDqj2Unvh9geRjBiRN
q0pksCD9GQj4yQc0iYxEbu2RCum8suL.lkeQZL2oVYvRdjYFiT5kcWAYuGaZH3YGoR+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:C4:83:09: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:D6:0E: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:A8:7A: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:CC: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:	150088603496836965305860138666951323383672938340
X509 Certificate	

-----BEGIN CERTIFICATE-----
MIIH8DCCBdigAwIBAgIUAqEFRGliNgocV6sZ4jm3XSys6YowDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGSUVElENBIEcxMB4XDTIxMDkzMDE4NTYxN1oXDTI0MDUx
MDE4NTYxN1owggfKMQswCQYDVQQGEwJHUjE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSA1IElbWJlcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWkSZ
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NIT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC0gRUMgU1RVBVFVT1JZIFNUQUZGMS0wKwYJKoZIhvcNAQkBFh5hcG9zdG9sb3MuYXBs
YWRhc0BlYy5ldXXJvcGEuZXUxEDAOBgNVBAQMB0FQTEFEQVMxEjAQBgNVBCoMCUFQT1NUT0xPUzEd
MBsGA1UECwwUUmVtb3RlUVNDRElhbmFnZW1lbnQxGjAYBgNVBAMMEUFQT1NUT0xPUyBBUExBREFT
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsARkOHMiUr+4vsKLAoiP6X4tHeVs0Y59
wqRdYwAg+ebeb0ubiNmGzGDMxeunvk8BwJEWnu2Qi+yzTrcbpPhNPTJam1PyhlzxRnbETM27JjrC
5AyKHsQ29SbuBJA0cnh36HletOzLoo23PCfaOBKvSQw+HAJecw5XsEE+YWC+tuBDgRFTVnxobUpG
JMcvmmztLdo3SCjvuRTuCRNJEmBDY0WhmK9A98bUFgWir0KDVgP8h1plkZi33pL7Rv/104OQwE8Q
4cDq8TCZqZ6xYNlDx6eTZcwzVLniwvds+EhAIhqgkTL7m56r4qkfiFgozv8RdP0qheb8Ob/EyYNF
rVW/YQIDAQABo4ICrTCCAfEwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBRzSfFAHBQEIoSf/ov
zVxnIxjpFDCBhAYIKwYBBQUHAQEEeDB2MEUGCCsGAQUFBzAChjlodHRwOi8vcWNhLWcxLmRpZ2l0
YWxzaWduLnB0L0RJR0lUQUxTSUdOUVVBTEIGSUVEQ0FHMS5wN2IwLQYIKwYBBQUHMAGGIWh0dHA6
Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvb2NzcDAPBgNVHREEljAggR5hcG9zdG9sb3MuYXBsYWRh
c0BlYy5ldXXJvcGEuZXUwXgYDVR0gBFcwVTA2BgsrBgEEAYHHAQBATAnMCUGCCsGAQUFBwIBFhlo
dHRwOi8vcGtpLmRpZ2l0YWxzaWduLnB0MBAGDisGAQQBgcd8BAIBAQEEMAkGBwQAi+xAAQIwHQYD
VR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEoGA1UdHwRDMEEwP6A9oDuGOWh0dHA6Ly9xY2Et
ZzEuZGlnaXRhbHNpZ24ucHQvRElHSVRBTFNJR05RVUFMSUZJRURDQUcxLmNybDAdBgNVHQ4EFgQU
TK7kKcckq1yO29zWWVbTXsoQDNswDgYDVR0PAQH/BAQDAgZAMIIHTBggrBgEFBQcBAwSBxjCBwzAI
BgYEAI5GAQEwCAYGBACORgEEMBMGBgQAjkYBBjAJBgcEAI5GAQYBMGoGBgQAjkYBBTBgMC4WKGh0
dHBzOi8vcWNhLWcxLmRpZ2l0YWxzaWduLnB0L1BEU19wdC5wZGYTAmB0MC4WKGh0dHBzOi8vcWNh
LWcxLmRpZ2l0YWxzaWduLnB0L1BEU19wbc5wZGYTAmVuMBUGCCsGAQUFBwsCMAkGBwQAi+xJAQEw
FQYIKwYBBQUHCwIwCQYHBACL7EkBAjANBgkqhkiG9w0BAQ0FAAOCAgEAJu2ay08mPKn2pS/Mc96o
RLsQxEAIx7baADy3Fe9p1DBdmXXDkuTCLH4P2ALzrPRRlgrTnQ5w7ORxnZw6pNZyBj/d3yQutsL1
kJnjmxBhR76cqgGft/+l4eiwRUPyUi01KSCaLSf1mYocvgJgmjdQljpoeOeb6n7Ua8tY7aflWPgI
7o8tbTLyMSb4Lh2ZcYqTgV65ZxHD6lfWu1/m7GzKcTLE1+iNJxjjLRgkloQHUAe8bKyugMJW21i1
PELrNSp1LUie5Ykaq/F2lN7bl9AK+cAWDfxUQhtq3f3gkkn3Nd80sThaafcn9GNWpSJhd82/fiC
gHEoOl9LqWpRJ567RffnYrmvdY5HwzB4UmDWsFAVUKsBwpbl22S2zL9/+yDIYdW6Jw7jXCQqFenS
DD49PK1wb/Ciq6zRs3SsKYl/aXLD98m/My7s1E8+x35zwy3TxGU48HZCc4/hquYdml9LPahdGomy
xTHiKTAgGPAynB9Ym+Hx4DRSmUlNExRZWA9FEH/2F8B9BcagjyDNDB/+5HIhP59YU0tG0lgS5I
rEJ49ESIPov1NiUQlalNPQp 8xLyu+TmTlZ3n43bcdoJoth8AFawB2jkDCSdz8flikPlhdS336hWM
rm6G38RsKu/XpXyyK05+UeLpeYu2YOutn7bUVKlyWLZsaS59kwalibY=
-----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:	*Thu Sep 30 20:56:17 CEST 2021*
Valid to:	*Fri May 10 20:56:17 CEST 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:B0:04:64:38:73:22:52:BF:B8:BE:C2:8B:02:88:8F:E9:7E:2D:1D:E5:6C:D1:8E:7D:C2:A4:5D:63:00:20:F9:E6:DE:6F:4 B:9B:88:D9:86:CC:60:CC:C5:EB:A7:BE:4F:01:C0:91:16:9E:ED:90:8B:EC:B3:4E:B7:1B:A4:F8:4D:3D:32:5A:9B:53:F2:84:8C:F1:46:76:C4:4C:CD:BB:26:3A:C2:E4:0C:8A:1E:C4:36:F5:26:EE:04:90:34:72:78:77:E8:72:1E: B4:EC:CB:A2:8D:B7:3C:27:DA:38:12:AF:49:0C:3E:1C:02:5E:73:0E:57:B0:41:3E:61:60:BE:B6:E0:43:81:11:53:56:7C:68:6D:4A:46:24:C7:2F:9A:6C:ED:2D:DA:37:48:28:EF:B9:14:EE:09:13:49:12:60:43:63:45:A1:98:AF:40 :F7:C6:D4:16:05:A2:AF:42:83:56:03:FC:87:5A:65:91:98:B7:DE:92:FB:46:FF:F5:D3:83:90:C0:4F:10:E1:C0:EA:F1:30:99:A9:9E:B1:60:D9:43:C7:A7:93:65:CC:33:54:B9:E2:C2:F7:6C:F8:48:40:26:1A:A0:91:32:FB:9B:9E:A B:E2:A9:1F:88:58:28:CF:2F:11:74:FD:20:85:E6:FC:39:BF:C4:C9:83:45:7D:55:BF:61:02:03:01:00:01
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	*http://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b*
	http://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: http://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	*http://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*

Subject Key Identifier	*4C:AE:E4:29:C7:24:AB:5C:8E:DB:DC:D6:59:56:D3:5E:CA:10:0C:DB*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance*
	id_etsi_qcs_QcSSCD
Key Usage:	*nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*26:97:CD:0F:55:AE:D0:90:50:55:89:4E:E0:B6:3D:7C:31:C8:75:55:4C:C6:39:4B:5C:35:41:CA:CB: 4B:1E:F1*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*36267112580322024539771398225422705688170119 2273*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIHLjCCBRagAwIBAgIUP4a8WPhZN++7VkfYyuAcDGmTglEwDQYJKoZIhvcNAQELBQAwczELMAkG
A1UEBhMCQkUxGTAXBgNVBGEMEE5UUkJFLTA1Mzc2OTgzMTgxIDAeBgNVBAoMF1F1b1ZhZGlzIFRy
dXN0bGluayBCVkJBMScwJQYDVQQDDB5RdW9WYWRpcyBCZWxnaXVtIElzc3VpbmcgQ0EgRzIwHhcN
MjEwMTIxMDg0ODM4WhcNMjQwMTIxMDg1ODAwWjCBwDELMAkGA1UEBhMCQkUxLDAqBgNVBAsMMl0Rp
cmVjdG9yYXRlLUdlbmVyYWwgZm9yIEluZm9ybWF0aWNzMRkwFwYDVQRhDBBOVFJCRS0wOTQ5Mzgz
MzQyMUowSAYDVQQKDEFDT01NSVNTSU9OIERFIEwnVU5JT04gRVVST1BFRU5ORSAtIENPTU1JU1NJ
RSBWQU4gREUgRVVST1BFU0UgVU5JRTEcMBoGA1UEAwwTRXVyb3BlYW4gQ29tbWlzc2lvbjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMCq40SQWaqRkbc5nsdPjLKyxghYzBLJCmeN3/nd
D5mMzhy9tsP8WOpsfi8CnMDStasEEmS5Fj73DQ+sL9PIyImLzBJVhuCyzwKpDiFAhAa+ec/LTyVR
a6+oCh91KZUcPDVXpCtGA3t6WS0pCgrIJNkZequ2yIWUZxyVOACYmkxmWbWmGe7LRaLv80PCl0Q
ERL2BzV+mKb2tQylUphPPI8hd9LG9EwCvSSXv0tb4rK1C+llcxuYsui7dNyfw9UHDBnuI5452c3O
18N5+GSl9uiEmOI8s++tbubn61RskePhk3ISURPGIAeDKV9pCZezBGysq5IINkC1C4AtYS2eKFcC
AwEAAaOCAmowggJmMB8GA1UdIwQYMBaAFIDvDGXEinpzu37APUVRtAEllVGrMHcGCCsGAQUFBwEB
BGswaTA4BggrBgEFBQcwAoYsaHR0cDovL3RydXN0bGluFb3ZhZGlzZ2xvYmFsLmNvbNvbS9xdmJlY2Fn
Mi5jcnQwLQYIKwYBBQUHMAGGIWb0dHA6Ly9ldy5vY3N3LnF1b3Zhc9mXpZGlzZ2xvYmFsLmNvbYTBaBgNV
HSAEUzBRMEQGCisGAQQBvlgBgxAwNjA0BggrBgEFBQcCARYoaHR0cDovL3d3dy5xdW92YWRpc2ds
b2JhbC5jb20vcmVwb3NpdG9yeTAJBgcEAIvsQAEDMCkGA1UdDQQiMCAGCCsGAQUFBwMCBggrBgEF
BQcDBAYKKKwYBBAGCNwoDDDCBiwYJKwYBBQUHAQMEfzB9MBUGCCsGAQUFBwsCMAkGBwQAi+xJAQlw
CAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGAjA7BgYEAI5GAQUwMTAvFiln
dHRwczovL3d3dy5xdW92YWRpc2dsb2JhbC5jb20vcmVwb3NpdG9yeRMCZW4wOwYDVR0fBDQwMjAw
oC6gLIYqaHR0cDovL2NybC5xdW92YWRpc2dsb2JhbC5jb20vcXZiZWNhZ2luZzIuY3JsMB0GA1UdDgQW
BBQspnrB2Vq7SM99egtZxs2jZv1QOjAOBgNVHQ8BAf8EBAMCBsAwEwYKKoZIhvcvAQEJAgQFMAMC
AQEwNAYKKoZIhvcvAQEJAQQmMCQCAQGGH2h0dHA6Ly90cy5xdW92YWRpc2dsb2JhbC5jb20vYmU0w
DQYJKoZIhvcNAQELBQADggIBACGQDYsjrM3nsKSpiW1SqzBlZOkvuiphSLNhv5o5V1W+maYLtXYH
/iMadrP0+K2X5XB5e+8yMw4Sbrvxv4LRR/CQ2WX03KjYGcqdcIUAH+A/8phwA7eLyKd3ip8k8ukT
9kUKMJxbqVR5O8x2vOlAM9VFirOenOI+MuIFDSaNKlJKt+PDhcSxDyzjsZMRKHAJcTCs23T8IBf6+
Qvw3uKUgniVg4MTLFvWpL8bvMXX7QUyvsScskUCns918hHA4Ett7fxdWXJFFJuuculChIlf8jbXZ
Q/8SAoecPyADnJw0C4uGNl/zc9/DWqMSMMytFwGeOpQb0/pukdmNe3sai8SUQj4+vyhkCHKMD27c
ak9buDO7cu5yhKEuLCERTga2QvbGSeiFAa6KuyPGY1Ad9AOuz5KPyyfVG0h3lFvNL0MnAib1lpZr
7mPQgWOsEX9ipgQXoE2Rh11yydTiKwmyTTrp/uMOJp+6UD06ldgPkHmqnqaKkqzGu6RKiHLqYWX5
qhWXt0EatHQ0YY+92B03cDTLMgjPHKY+wN6qPfetz0oQNmort+G2HIXb9P+Q43sqMjXpQY/I3YmM
0VBmcYWUon11BOavnGGOCVVPBQFKU6Kt7r69li1CmIA7KgK7Jn2o/jb8BupWUPGej++MkkrFDS0T
6tmNH9ZDteyO3dSyOcl1IHcs

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

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*QuoVadis Belgium Issuing CA G2*
Issuer O:	*QuoVadis Trustlink BVBA*
Issuer 2.5.4.97:	*NTRBE-0537698318*
Issuer C:	*BE*
Subject CN:	*European Commission*
Subject O:	*COMMISSION DE L'UNION EUROPEENNE - COMMISSIE VAN DE EUROPESE UNIE*
Subject 2.5.4.97:	*NTRBE-0949383342*
Subject OU:	*Directorate-General for Informatics*
Subject C:	*BE*

Valid from:	*Thu Jan 21 09:48:38 CET 2021*
Valid to:	*Sun Jan 21 09:58:00 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:C0:AA:E3:44:90:59:AA:91:91:B7:39:9E:C7:4F:8C:B2:C6:08:58:CC:12:C9:0A:67:8D:DF:F9:DD:0F:99:8C:CE:1C:BD:B6:C3:FC:58:EA:6C:7E:2F:02:9C:C0:F9:B5:AB:04:12:64:B9:16:3E:F7:0D:0F:AC:2F:D3:C8:C9:F9:8B:CC:12:55:86:E0:B2:CF:02:A9:0E:21:40:84:06:BE:79:CF:CB:4F:25:51:6B:AF:A8:0A:1F:75:F1:95:1C:3C:35:57:A4:2B:46:03:7B:7A:59:2D:29:0A:0A:C8:24:D9:19:7A:AB:B6:C8:85:94:67:18:B2:54:E0:02:62:69:31:99:68:56:9C:67:BB:2D:16:8B:BF:CD:0F:08:8D:10:11:12:F6:07:35:7E:98:A6:F6:B5:0C:A5:52:98:4F:3C:8F:21:77:D2:C6:F4:4C:02:BD:24:97:BF:4B:5B:E2:B2:B5:0B:E9:48:73:1B:98:B2:E8:BB:74:DC:9F:C3:D5:07:0C:19:EE:23:9E:39:D9:CD:CE:D7:C3:79:F8:64:88:F6:E8:84:98:E2:3C:B3:EF:9F:6E:E6:E7:EB:54:6C:91:E3:E1:93:72:12:51:13:C6:2:0:07:83:29:5F:69:09:97:B3:04:6C:AC:AB:92:25:36:40:B5:0B:80:2D:61:2D:9E:28:57:02:03:01:00:01*
Authority Key Identifier	*87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB*
Authority Info Access	*http://trust.quovadisglobal.com/qvbecag2.crt* *http://uw.ocsp.quovadisglobal.com*
Certificate Policies	*Policy OID: 1.3.6.1.4.1.8024.1.400* *CPS pointer: http://www.quovadisglobal.com/repository* *Policy OID: 0.4.0.194112.1.3*
Extended Key Usage	*id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*
QCStatements - crit. = false	*id_etsi_qcs_QcCompliance* *id_etsi_qcs_QcSSCD*
CRL Distribution Points	*http://crl.quovadisglobal.com/qvbecag2.crl*
Subject Key Identifier	*2C:A6:7A:C1:D9:5A:BB:48:CF:7D:7A:0B:59:C6:CD:A3:66:FD:50:3A*
Key Usage:	*digitalSignature - nonRepudiation*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F7:E8:E4:E5:54:FB:7C:7A:8F:6F:36:0E:0C:A2:F5:9D:46:6C:8F:95:39:A2:59:63:F5:ED:37:E9:05:F0:C7:97*

EU TSL digital identities

.

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*212676479325594043390357602224263512027*
X509 Certificate	*-----BEGIN CERTIFICATE-----*

MIIG7zCCBNegAwIBAgIQEAAAAAAAnuXHXttK9Tyf2zANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQG
EwJCRTERMA8GA1UEBxMIQnJ1c3NlbHMxHDAaBgNVBAoTE0NlcnRpcG9zdCBOLlYuL1MuQS4xEzAR
BgNVBAMTCkNpdGl6ZW4gQ0ExDzANBgNVBAUTBjIwMTgwMzAeFw0xODA2MDEyMjA0MTIaFw0yODA1
MzAyMzU5NTlaMHAxCzAJBgNVBAYTAkJFMSMwIQYDVQQDExpQYXRyaWNrIEtlYZW1lciAoU2lnbmF0
dXJlKTEPMA0GA1UEBBMGS3JlbWVyMRUwEwYDVQQgEwxQYXRyaWNrIEplYW4xFDASBgNVBAUTCzcy
MDIwMzI5OTcwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr7g7VnDY4as3R4LPOg7
uPH5inHzaVMOwFb/8YOW+9IVMHIz/V5dJAzeTKvhLG5S4Pk6Kd2E+h18FlRonp70Gv2+ijtkPk7ZQ
kfez0ycuAbLXiNx2S7fc5GG9LGJatDJgBgTQuQm1aDVLDQ653mqR5tAO+gEf6vs4zRESL3MkYXAU
q+S/WocEaGpIheNVAF3iPSkvEc3LvUjF/xXHWF4aMvqGK6kXGseaTcn9hgTbceuW2PAiEr+eDTNc
zkwGBDFXwzmnGFPMRez3ONk/jKhha8TyJDSll/MX3ODt0dU3jvJEKPIfUJxBPehxMJMwWxTjFb
Nu/CK7t8gT2t1S4VQIDAQABo4ICpCCAoswHwYDVR0jBBgwFoAU2TQhPipCJW3hu7++R0z4Ag3j
L1QwcwYIKwYBBQUHAQEEZzBlMDkGCCsGAQUFBzAChi1odHRwOi8vY2VydHMuZWlkLmJlbGdpdW0u
YmUvY2l0aXplbnJhMTgwMy5jcnQwKAYIKwYBBQUHMAGGHGh0dHA6Ly9v3NwLmVpZC5iZWxnaXxVt
LmJlL2wggEjBgNVHSAEggEaMIIBFjCCAQcGB2A4DAEBAgEwgfswLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBv2l0b3J5LmVpZC5iZWxnaXVtLmJlMIIHIKBggrBgEFBQcCAjCBvQyBukdIYnJ1aWsgb25k
ZXJ3b3JwZW4gYWFulGFhbnNwcmmFrZWxwamantoZWlkc2J1cGVya2luZ2VlmVuL2Vlm1bsbBCb6aW1gO1BTIC0gVXNh
Z2Ugc291bWIzIMOgIGRIcyBsaW1pddGF0aW9ucyBkZSByZXNwb25zYWJpbGl0w6ksIHZvaXXlgQ1BT
IC0gVmVyd2VuZ3VuZ3VzIHJhdBRlcmxpZW0/ZW4l0IEhhZnR1bmdzZYmVzY2hyw6Rua3VuZ2VuLCBnZW3DpHNz
IENQUzAJBgcEAIvsQAECMDkGA1UdHwQyMDAwLqAsoCgGGKGh0dHA6Ly9jcmwuZWlkLmJlbGdpdW0u
YmUvZVlkYzIwMTgwMy5jcmwwDgYDVR0PAQH/BAQDAgZAMBMGA1UdJQQMMAoGCCsGAQUFBwMEMGwG
CCsGAQUFBwEDBGAwXjAIBgYEAI5GAQEwCAYGBACORgEEMDMGBgQAjkYBBTApMCcWIWh0dHBzOi8v
cmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5iZS9yZICMCZW4wEwYGBACORgEGMAkGBwQAjkYBBgEwDQYJKoZI
hvcNAQELBQADggIBAC8Y+0LbM7BryzXWkIDU/h9UK1+cDVboPg+lN1Et1lAEoxV4y9zuXUWLco9t8
M5WfDcWFfDxvhatLedku2GurSJ1t8O/knDwLLyoJE1r2Db9VrdG+jtST+j/TmJHAX3yNWjn9dsj
iGQQuTJcce86rlzbGdUqjFTt5mGMm4zy4I/wKy6XiDKiZT8cFcOTevsl+l/vxiLiDnghOwTztVZh
mWExcHG9ypqMFYmIucHQ0SFZre8mv3c7Df+VbqV/sY9xLERK3Flk4l6BSgRPygImNxjGzNSWiDISd
YeUf4XoZLXJBEP736r4mlnP2NWQ+c1ORjesuDAZRtDyhMvR4DVG95EScjpTYv1wOmVB2lQrWnE
tygZI60HXfozo8uOekBnqWyDc1kuizZsYRfVNlwhCu7RsOq4zN8gkael0fejuSNtBf2J9A+rc9L
Qeu6AcdPauWmbxtJV93H46pFpts8zXo+IJn5m2P9QPZ3mvDkzldNTGLG+ukhN7lF2CCcagt/WoV
ZLq3qKC35WVcqeoSMEE/XeSrf3/mIJ1OyFQm+tsfhTceOFDXuUgl3E86bR/l8Ur/bapwXpWpFxGI
pXLGaJXbzQGSTtyNEYrdENlh71I3OeYdw3xmzU2B3tbaWREOXtj2xjyW2tIv+vvHG6sloR1QkIkG
MFZsI7W5U6ILetv

-----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:38: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:86:2B:A9:17:1:A:C7:9A:4D:C9:FD:86:04:DB:71:EB:96:D8: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:42:6:2: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:	231199879490522356566716403815664415819903446597

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIIBDCCBevgAwIBAgIUKH9cdKE3vD5rBCmH3Krsppm6rkUwDQYJKoZIhvcNAQENBQAwXzELMAkG
A1UEBhMCUFQxKjAoBgNVBAoMIURpZ2l0YWxTaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbDEkMCIG
A1UEAwwbRElHSVRBTFNJR04gUVVBTElGSUVEIENBIEcxMB4XDTIzMDIyMjE1MzYyOVoXDTI2MDIy
MTE1MzYyOVowggFWMQswCQYDVQQGEwJHUjE9MDsGA1UECww0Q2VydGlmaWNhdGUgUHJvZmlsZSAt
IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSAtIE1lbWJlcjEjMCEGA1UEYQwaTEVJWEctMjU0OTAwWk5Z
QTFGTFVROVUzOTMxHDAaBgNVBAoME0VVUk9QRUFOIENPTU1JU1NJT04xKTAnBgNVBAsMIEVudGl0
bGVtZW50IC9gRUMgU1RBVFVUT1JZIFNUQUZGMTEwLwYJKoZIhvcNAQkBFiJpb2FubmEua2Fsb2dl
cm9wb3Vsb3VAZWMuZXVyb3BhLmV1MRcwFQYDVQQEDA5LQUxPR0VST1BPVUxPVTEPMA0GA1UEKgwG
SU9BTk5BMR0wGwYDVQQLDBRSZW1vdGVRU0NETWFuYWdlbWVudDEeMBwGA1UEAwwVSU9BTk5BIEtB
TE9HRVJPUE9VTE9VMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnIDj3MSrgRjPj4E7
hP7l2nP47K9P3KIWa9HBd77uD0bOvO/U4d5GBx6ildYnX0pIhj1uq+fMatM1BlvGAgPFq7NiWYj
dz1t5Icdx3iWrao6ElkzNP/a+3s/wPfHmvOitmgnBBAVOurgz7tT7WX1pUrA7L5VxbrY8E7xD2Qg
frBaIpwqSYeho+U2FmVV9UULw0rAQVbFqUEqg9Nb88GMXNt2sXPveO7GtXYbi0WClSdej1JVAr69
RuyDDrl7fCr4Q6yzXWpOWF7Vr2z2S3hhqnPPl2lqVfhaHGq6mBu6wRqOK0ct+zp4ZQEEC246NYIO
JAoC/tcj8zewo4zBIRJwJQIDAQABo4ICvTCCArkwDAYDVR0TAQH/BAIwADAIBgNVHSMEGDAWgBRz
StFAHBQEDoSf/ovzVxnlxipFDCBhgYIKwYBBQUHAQEFEcziB4MEYGCCsGAQUFBzAChjpodHRwczov
L3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRklFRENBRzEucDdiMC4GCCsG
AQUFBzABhiJodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9vY3NwMC0GA1UdEQQmMCSBImlv
YW5uYS5rYWxvZ2Vyb3BvdWxvdUBly5ldXJvcGEuZXUwXwYDVR0gBFgwVjA3BgsrBgEEAYHHAQB
ATAoMCYGCCsGAQUFBwIBFhpodHRwczovL3BraS5kaWdpdGFsc2lnbi5wdDAQBg4rBgEEAYHHAQC
AQEBBDAJBgcEAIvsQAECMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDBLBgNVHR8ERDBC
MECgPqA8hjpodHRwczovL3FjYS1nMS5kaWdpdGFsc2lnbi5wdC9ESUdJVEFMU0lHTlFVQUxJRklF
RENBRzEuY3JsMB0GA1UdDgQWBBRkfGQMVVlxBJmVo0L3Zjs2nTpaRjAOBgNVHQ8BAf8EBAMCBkAw
gdMGCCsGAQUFBwEDBIHGMIHDMAgGBgQAjkYBATABgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYB
BgEwagYGBACORgEFMGAwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX3B0LnBk
ZhMCcHQwLhYoaHR0cHM6Ly9xY2EtZzEuZGlnaXRhbHNpZ24ucHQvUERTX2VuLnBkZhMCZW4wFQYI
KwYBBQUHCwIwCQYHBACL7EkBATAVBggrBgEFBQcLAjAJBgcEAIvsSQECMA0GCSqGSIb3DQEBDQUA
A4ICAQBfvXM2+mTPDHZGA7BLQ+04S/1rObRmuKy9w5xLRp9bBanBS90nRJjixOMIATTgZFF6pT4H
6q3XFYDvbrm/SUNkVKnSovDucXB/bEhqEN+DYmLxxLFxbsGoBZosbFloFHgoct+OP/ttxe9e8hiL
5+J5TXwGB/+u3wbOWfA8XdwvKl1UVJHrEeJjPTsneBBKIXLpnnQYrPM3guEayVRkNdYd9dsaVJKu
6bnw+yVjaBAvX9Mspu4b5leUHA+lRR5kgSm+RjAJfymGtgy9/hcE/MAX+ANL8tb4PgC3XEGfP/XM
4ZUS97CeL5r+OwNnN+6yToYQh3LoQrUvkvj2uNLoWX15WMt37KRVgiAdOkVFFlsQRvTJM9OYBl/4
Rmc1g3TD4O0TBlqzjoMnLGD8d3nhtKsfb29gW7Pj9lGZLl4ObIzeBZwQZKK5U8LAh38mzlU2UGY
C1FHbyNKLn9L6bVn0F7OdelRiNrmby9TiKwl8gwZUAC5bxOv/5dfswUFN1kQ2LTiRMM+8G/1lDe1
CAuN4H2W+0hAvkBy2KIAzcxa6nCOilHzu1BtkfV7x4qojYoFAXl+tKe8ItluJlFR+gWb7T3ymRFG
sZMDoabXIRvnvrks/KRqhi8/6YmCDpx4jDTxQf3GOVC2AXULtNtV1i28md5isoH3GHgqPeKYdNxO
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:B6:6 8:27:04:10:15:3A: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:B 1:73: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:	*602137478369718753674691090226768309702106444486*

X509 Certificate	

-----BEGIN CERTIFICATE-----
MIIHQTCCBSmgAwIBAgIUCowT7Q98oPLpaLF0FnUX3eobcgYwDQYJKoZIhvcNAQELBQAwczELMAkG
A1UEBhMCQkUxGTAXBgNVBGEMEE5UUkJFLTA1Mzc2OTgzMTgxIDAeBgNVBAoMF1F1b1ZhZGlzIFRy
dXN0bGluayBCVkJBMScwJQYDVQQDDB5RdW9WYWRpcyBCZWxnaXVtIElzc3VpbmcgQ0EgRzIwHhcN
MjEwMTIxMDg0ODIzWhcNMjQwMTIxMDg1ODAwWjCB0zELMAkGA1UEBhMCQkUxPzA9BgNVBAsMNkRH
IGZvciBDb21tdW5pY2F0aW9ucyBOZXR3b3JrcywgQ29udGVudCBhbmQgVGVjaG5vbG9neTEZMBcG
A1UEYQwQTlRSQkUtMDk0OTM4MzM0MjFKMEgGA1UECgxBQ09NTU1TU0lPTiBERSBMJ1VOSU9OIEVV
Uk9QRUVOTkUgLSBDT01NSVNTSUUgVkFOIERFIEVVUk9QRVNFIFVOSUUxHDAaBgNVBAMME0V1cm9w
ZWFuIENvbW1pc3Npb24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDtD1bnPz0vyl0g
xH+Ye/UEyssxITWyXmT2SjX8T0oR36yu+FvEI1YB7q7CGA2JNUxKdOPgFi4MZxj9vOoMwqR1+cbP
DNzXsdzlNLZCDy3mrPt3hIqmijhmqmwwXSQnO2+uDee+BYGXL74oWngJTe+GT6SjYQMyeXvyfl1J
U4pC+QL53kpcNI7dO5EJzHAfLDp8HILebtafvWAQA9+Psf3BT/0lHQZ1nqnyMfjBntCBG6/Cj2m
tM44vldCKtRDdGno7MT5lxTvwolcEA5Lupbdu9sudHsJT4iOub8QshI3bjHqP7n7q+OsNSRX5/Cb
mlG033j7Yn+DfwCKwE4eKsZHAgMBAAGjggJqMllCZjAfBgNVHSMEGDAWgBSHybwxIxJ6c7t+wD1F
UbQBJZVRqzB3BggrBgEFBQcBAQRrMGkwOAYIKwYBBQUHMAKGLGh0dHA6Ly90cnVzdC5xdW92YWRp
c2dsb2JhbC5jb20vcXZiZWNhZzIuY3J0MC0GCCsGAQUFBzABhiFodHRwOi8vdXcub3VzcC5xdW92
YWRpc2dsb2JhbC5jb20wWgYDVR0gBFMwUTBEBgorBgEEAb5YAYMQMDYwNAYIKwYBBQUHAgEWKGh0
dHA6Ly93d3cucXVvdm4FkaXNnbG9iYWwuY29tL3JlcG9zaXRvcmnkwCQYHBACL7EABAzApBgNVHSUE
IjAgBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQBgicKAwwwgYsGCCsGAQUFBwEDBH8wfTAVBggr
BgEFBQcLAjAJBgcEAIvsSQECMAgGBgQAjkYBATAIBgYEAI5GAQQwEwYGBACORgEGMAkGBwQAjkYB
BgIwOwYGBACORgEFMDEwLxYpaHR0cHM6Ly93d3cuXVdmFkaXNnbG9iYWwuY29tL3JlcG9zaXRv
cnkTAmVuMDSGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwuXVvdmFkaXNnbG9iYWwuY29tL3F2
YmVjYWcyLmNybDAdBgNVHQ4EFgQUSiKJPwxZvfi51U75EfhdERrDf98wDgYDVR0PAQH/BAQDAgbA
MBMGCCqGSIb3LwEBCQIEBTADAgEBMDQGCiqGSIb3LwEBCQEEJAkAgEBhh9odHRwOi8vdHMucXVv
dmFkaXNnbG9iYWwuY29tL2JlMA0GCSqGSIb3DQEBCwUAA4ICAQCWLVCxzkKy/s+8kRvxCPvTlExl
WkNGsrhCO+PXsh1UgWMdJCpc33OzL1GegNMSL9f3Hw6gqjXV+mJqtTmvrP1ZvXCagv2LRLeyxSYA
jIVywYkaraddydS8Or86OyIA0OIs1UruPe0lClb6rBKwqqx7LvXotk7XvPYQo0HrP57pCqlp4Mli
NEpGeW3gRwFq8IBQceeO3k009ad+tuTSB51+o4t/7kEd//6voViy7d/EmlOgUZzXsJZ4NV4pFAmy
c2FlkEvYOqw8YvEsOV2hluvcG3wmkMEF/SY4X+kvpw+Ph7JQdWpWGlozzAFVppkIIrSM2Sxw2QXF
QZWwah210HiVY0Ax4VkQbRJQNYmFWVizixPONWtc3PfMz3/TvD9ZbExFfoQzVYXZPmtK2aQjG3C
H2bJcefvS18YdR169au8yNKs5PvlLaRa1k7Qv6Hv8iE3GtQmszzDwnQHIGrbxdft306gOFl8/U0cty
Il2YkG6J/uTnYiiibeDoHK6wBo3BfCJQ2X7/lab3971k1wSCwe39w4x3Xw72HL9E3czRkcfpg+uT
xt5jSJ7HL7BRdMD34ysjQ4gOV8h6NU4z+QQ3W4sZTQkFqHGHKZKt2dTrCjhE+11hULvo4274heBr
/5F0DBAXRi9lHBCBUV5iJDm90bxjHjKuvj893WLEFW3WPkWlRw==
-----END CERTIFICATE-----

Signature algorithm:	SHA256withRSA
Issuer CN:	QuoVadis Belgium Issuing CA G2
Issuer O:	QuoVadis Trustlink BVBA
Issuer 2.5.4.97:	NTRBE-0537698318
Issuer C:	BE
Subject CN:	European Commission
Subject O:	COMMISSION DE L'UNION EUROPEENNE - COMMISSIE VAN DE EUROPESE UNIE
Subject 2.5.4.97:	NTRBE-0949383342
Subject OU:	DG for Communications Networks, Content and Technology
Subject C:	BE
Valid from:	Thu Jan 21 09:48:23 CET 2021
Valid to:	Sun Jan 21 09:58:00 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:ED:0F:56:E7:3F:3D:2F:C8:8D:20:C4:7F:98:7B:F5:04:CA:CB:31:D5:35:B2:5E:64:F6:4A:35:FC:4F:4A:11:DF:AC:AE:F8:5B:C4:23:56:01:EE:AE:C2:18:0D:89:35:4C:4A:74:E3:E0:16:2E:0C:67:18:FD:BC:EA:0C:C2:A4:75:F9:C6:CF:0C:DC:D7:B1:DC:C8:34:B6:42:0F:2D:E6:AC:FB:77:85:FA:A6:8A:38:66:AA:6C:30:5D:24:27:3B:6F:AE:0D:C7:BE:05:81:97:2F:BE:28:5A:7A:89:4D:CF:86:4F:A4:A3:61:03:32:79:7B:F2:7D:FD:49:53:8A:42:F9:02:F9:DE:D7:29:70:D7:FB:74:EE:44:27:31:C0:7C:B0:E9:F0:72:0B:79:BB:5A:7E:F5:80:40:0F:7E:3E:C7:F7:05:3F:F4:94:74:19:D6:7A:A7:C8:C7:E3:06:7B:42:04:6E:BF:0A:3D:A6:B4:CE:38:BE:57:42:2A:D4:43:74:69:E8:EC:C4:F9:97:14:EF:C2:82:1C:10:0E:4B:BA:96:DD:BB:DB:2E:74:7B:09:4F:88:8E:B9:BF:10:B2:12:37:6E:31:EA:3F:B9:F:B:AB:E3:AC:37:94:57:E5:7F:DB:98:81:B4:DF:78:FB:62:7F:83:7F:00:8A:C0:4E:1E:2A:C6:47:02:03:01:00:01
Authority Key Identifier	87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB
Authority Info Access	http://trust.quovadisglobal.com/qvbecag2.crt
	http://uw.ocsp.quovadisglobal.com
Certificate Policies	Policy OID: 1.3.6.1.4.1.8024.1.400
	CPS pointer: http://www.quovadisglobal.com/repository
	Policy OID: 0.4.0.194112.1.3
Extended Key Usage	id_kp_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12

QCStatements - crit. = false			*id_etsi_qcs_QcCompliance*
			id_etsi_qcs_QcSSCD

CRL Distribution Points

http://crl.quovadisglobal.com/qvbecag2.crl

Subject Key Identifier

4A:22:89:3F:0C:59:BE:58:B9:D5:4E:F9:11:F8:5D:11:1A:C3:7F:DF

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

91:27:BC:BD:E1:58:6E:02:DB:9D:71:49:88:13:9E:A2:80:5F:21:DC:08:83:48:A7:E4:FE:62:69:89:51:38:BD

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

2024-02-07T09:07:14Z

Next Update

date Time

2024-08-07T08:07:14Z

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
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbX1za2za2VzMRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTAyMDExNTE2NDQ1MFoXDTEyMDExMzE2NDQ1MFowfDEYMBYGCSqG
SIb3DQEJARYJcGtpQHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVy
aW1pc2tlc2t1czEPMA0GA1UECxMGRVNURUlEMQowCAYDVQQEEwExMRIwEAYDVQQDEwlFU1RFSUQt
U0swggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCLeZO5NVo3zbwA8eFVCrrbeZQKvPDB
7LUDPvzCqw7U2sC+IwEOdjjpJRF4lxFs+f8yC1bP+rqtWzrKhhJ2owfSAlIZMbly/OFjfLqOcvyi
7qdfA/66u+69u/DY9tW5fqW93D73v5WNcNolemCTydh9IFkQvMihWKH7LblBzCHa4W6qUcBZ7QsB
gYpQS9n9IGJt5D2wCDeq0pF1Zy72G3CQFrpuRaPG28tv9r+C7oqncapbiJ7xIOa77Fm3o07M/9a
arq/m1oHEp9CxYiH9nmD3kyMe8yxw5v02MTMmAcxOm83z5O4oXSDTALG5gDfZNPjJaNPno7J8FuG
rI3vV8z3AgMBAAGjggGpMIIBpTAMBgNVHIRMEBTADAQH/MA4GA1UdDwEB/wQEAwIB5jCCARYGA1Ud
IASCAQ0wggEJMIIBBQYKKwYBBAHOHwEBATCB9jCB0AYIKwYBBQUHAgIwgcMagIwgcMegcAAUwBlAGUAIABz
AGUAcgB0AGkAZgBpAGsAYQBhHQAIABvAG4AIAB2AQABgAGAEAcwB0AEGADABIAGQAIABBAFMA
LQBpAHMAIABTAGUAcgB0AGkAZgBpAHQAcwBlAGUAcmlAGkAcABzAGsAZQBzAGsAdQBzACAAYQBs
AGEAbQQtAFMASwAgAHMAZQByAHQAaQBmAGkAawBhAGEABhpAGEAdABpAGkAQGAQZQAgAGsAaQBuaGEaQB0AGEA
bQBpAHMAZQBrAHMwlQYIKwYBBQUHAgEWFWh0dHA6Ly93d3cuc2suZWUvY3BzL3BzLzArBgNVHR8EJDAi
MCCgHgAchhpodHRwOi8vd3d3LmNrLmVlL2p1dXIvY3JsLzAfBgNVHSMEGDAWgBQEqnpHo+SlrxrP
CkCnGD9v7+I9vjAdBgNVHQ4EFgQUcBe1BtmzWM1ZjN5nXkQGTHWGaV0wDQYJKoZIhvcNAQEFBQAD
ggEBAFIsMHaq4Ffkrxmzw38rHYh5fa5JGxjtWfPpag9pBtQNZHzY8j97xfPi15haE9Ah3u1WC+bs
U2SndVSUGaZ0gKafMxDOy2DUw3B84ymbNRiAFSWty+aKrMCjidlPktbSQmxNSJAX9vVtM4Y2ory+
dtAQ7g11GKIJ+l8BDUpOJA+l8hvS2I4K5whWDHCSqlplMiHPlKgBVArFRNzAq6dquMY+kS3c2PL+
PM4GdDW5lRHR/6KUy0BHP2gX/BO4mYQ3BH2BHImUclNras0HISnV/pt6hIkgd1PsFt3rtEolAWP4
DWBmc4zAYQJ5t0cEwFM3z9zCXSGlQlm3a1cMugF5Qk=

-----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:B5:03:3E: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:A2:EE:A7:5F:03:FE:BA:BB:EE:8D: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:ED: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:B
A: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:8D: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:3
7: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:C9:9 B: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 nonRepudiation 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
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTA3MDEwMzEyMjIzN1oXDTE2MDgyNjE0MjMwMVowWzELMAkGA1UE
BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmltaXNrZXNrdXMxDzANBgNVBAsTBkVTVEVJ
RDEXMBUGA1UEAxMORVNURUlELVNLIDIwMDcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDtWp2jLCsA7K9AxoPDOL0geM1GoR0Q6wsSUlCCJYyFkUMboEMxpSzFB6tlb0ySlHEU6Fs+tjA4Q
rSqwaw0uNk4BXv1lkoOr6DUc+20+AQd5jB6A0atrltZ1XG5IvDEep3DJPykkk2MPxUz7dZx7XUEr
/kdUW9cDlkFWic7y9oTBY9JaV6lxm08kweZ/qTw5PU8/bTvZCE0ygvBXU4TDS2fpUJ/+jTzM2oc
Wa3QjFQv2Sir6LBvgNY3du/m+WLABq0dgN18R4nhFtmaVcpqAeUuEi8eRBl6yLTSmMwYCY46LsK5
CdjTCZSZv934FtNuyY6Ph9nCXJAgNAY+GtNJ8JMXAgMBAAGjgzZwwgZkwEgYDVR0TAQH/BAgwBgEB
/wIBADAOBgNVHQ8BAf8EBAMCAf4wMwYDVR0fBCwwKjAooCagJIYiaHR0cDovL3d3dy5zay5lZS9j
cmxzL2p1dXIuY3JsMNyLbDAtBgNVHSMEGDAWgBQEqnpHo+SJrxrPCkCnGD9v7+i9vjAdBgNVHQ4E
FgQUSAbevoyHV5WAeGP6nCMrK6A6GHUwDQYJKoZIhvcNAQEFBQADggEBACO6SJrjN5WZuiLSMy/t
SmT/w3dd/KPErSAdUlJYkC7bOIauW7jZ3VNgNUMHSIkUoP8Av1EMjGA4IkT61YScpJAdmgi8Y80H
FdZV5CsThhddoIdZ3cZjSI4NZmTVkSduTjoySALxKL3ZEIPrepQDvNEeV1WSpl5+u/vMekUWJSPc
8BK9O2av1e9ResKyPJidqrIksHFjNS+Yt8Ouw7F10MHaPPzMiwoa0DYTVsIKJncPTQmvdJG8M0DD
ToiiNPQuUy5d1CA75Wtjs+yILGZXpOtbdoQhE7G4pbZaF1s69jKp+zc0ZT4g2OoKIl2TiIX9qeGJ
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:04:94:20:89:63:21:64:50:C6:E8:1 0: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:85:A5:42:7F:FA:3 4: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:EA:6A:01:E5:2E:12:2F:1E:44:19:7A:C8:B4:D2:98:CC:18:09:8E:3A:2E:C2:B9:09:D8:D3:0 9:94:99: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:E 5:80:5B*

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) 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: *54927111231050666919490365049675206925*

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIFBTCCA+2gAwIBAgIQKVKTqv2MxtRNgzCjwmRRDTANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMTQ1OVoXDTI0MDMxODEwMTQ1OVowZDELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxFzAVBgNVBAMMDkVTVEVJRC1TSyAyMDExMDExMRgwFgYJKoZIhvcN
AQkBFgIwa2IAc2suZWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCz6XxsZh6r/aXc
Ne3kSpNMOqmQoAXUpzzcr4ZSaGZh/7JHliplvNi6tbW/lK7sAiRsb65KzMWROEauld6ggbDPga6
kU97C+AXGu7+DROXstjUOv6VlrHZVAnLmlOkycpWaxjM+EfQPZuDxEbkw96B3/fG69Zbp3s9y6WE
hwU5Y9liQI8YTkGnNUxidQbON1BGQm+HVEsgTf22J6r6G3FsE07mMNskNC3DjuLSCUKF4kH0tVG
VK9BdiCdFaZjHEykjwjIGzqnyxyRKc4YbJ6B9ABm95cSFgMBHtZEYU+q0VUIQGbAGAurOTXjWi1T
ssA42mnLGQZEI5GXMXtabp51AgMBAAGJjggGgMIIBnDASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1Ud
DwEB/wQEAwIBBjCB9gYDVR0gBIHuMIHrMIHoBgsrBgEEAc4fZAEBATCB2DCBsgYIKwYBBQUHAgIw
gaUegaIASwBAHHMAdQB0AGEdABhAGsAcwBlACAAqBzAGkAawB1AHQAdAD1AGUAbgBkAGEAdgBh
AGwAZQAgAGQAbwBrAHUAbQBlAG4AZABpbAGwAZQAgAsAYQBuAHQAYQB2AGEdABlACAAcwBlAHIA
dABpAGYYAaQBrAGEYYQB0AGkAZABlACAAdgDkAGwAaAgBthAHMAdABhHAG0AaQBzAGUAdgBzAC4wIQYI
KwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL2NwMVIL0NQUzAdBgNVHQ4EFgQUe2ryVVBcuNl6CIdBrvqi
Kz1bV3YwHwYDVR0jBBgwFoAUEvJaPupWHL/NBgzx8SXJqUvUFJkwPQYDVR0fBDYwNDAyoDCgLoYs
aHR0cDovL3d3dy5zay5lZS9yZXBvc2l0b3J5L2NybHMvZWVjY2EyMDExLmNybDANBgkqhkiG9w0BAQEF
BQADggEBAKC4IN3FC2gVDIH05TNMgFrQOCGSnXhzoJclRLoQ81BCOXTZl4qn7N74FHEnrAy6uNG7
SS5qANqSaPIL8dp63jg/L4qn4iWaB5q5GGJOV07SnTHS7gUrqChGClnUeHxiZbL13PkP37Lnc+TK
l1SKJgtn5FbH5cqrhvbA/VF3Yzlimu+L7EVohW9HKxZ//z8kDn6ieiPFfZdTOov/0cXVLlxqklyb
UuS6LYRRDiqQupgBKQBTwNbC8x0UHX00HokW+dCVcQvsUbv4xLhRq/MvyTIhE+RdbkrV0JuzbfZv
ADfj75nA3+ZAzFYS5ZpMOyZ9p4rQVKpzQTkIrF0m6mkdcEo=
-----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:B2:4
7:22:2A:65:BC:D8:BA: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:13:97:B2:D8:D4:3A:FE:95:96:B1:D9:54:09:CB:98:83:A4:C9:CA:56:6
B: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:18:4E:41:A7:35:4C:62:75:06:CE:37:50:46:42:6F:87:54:4B:20:4D:FD:B6:27:AA:FA:1B:71:6C:13:4E:E
B: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:C8:1B: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:D1:55:08:40:68:4
0:18:0B:AB:39:35:E3:5A:2D:53:B2:C0:38:DA:69:CB:19:06:44:23:91:97:31:7B: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 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
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMCAXDTE1
MTIxNzEyMzg0M1oYDzIwMzAxMjE3MjM1OTU5WjBjMQswCQYDVQQGEwJFRTEiMCAGA1UECgwZQVMg
U2VydGlmaXRzZWVyaW1pc2tlc2t1czEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMM
DkVTVEVJRC1TSyAyMDE1MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0oH61NDxbdW9
k8nLA1qGaL4B7vydod2Ewp/STBZB3wEtIJCLdkpEs58pXfFiRqwDVsgGGbu+Q99trlb5L17yi7rl
kRov5NfiBdSNPSU5rAhYPQhvZZQgOwRaHa5Ey+BaLJHmLqYQS9hQvQsCYyws+xVvNFUpK0pGD64i
ycqdMuBl/nWq3lLuZppwBh0VFltm4nhr/1S0R9TRJpqFUGbGr4OK/Dweb05PjhdS40gcUNwmC7fP
Q4vJH+x+TCk2aG+u3MoAz0frpVWqiwzG/vxreuPPAkgXeFCeYf6fXLsGz4Wivsf2Fbph2pMfjELu6s
ltlBXfAG3fGv43r91VXicyzR/eT5dsB+zFsW1sHV+1ONPr+qzgDxCH2cmuqoZNfIlq+buob3eA8e
e+XpJKJQr+1qGrmhgigvAhc7m6cU4x/QfxwRYhIVNhJf+sKVThkQhbJ9XxuKk3c18wymwL1mpDD0
PlGJqIssMeiuJ4IzagFbgESGNDU4icm0hQT8CmQeUm1GbWeBYseqPbMQX97QFBLXJLVy2SCyoAz
7Bq1qA43++EcibN+yBc1nQs2Zoq8ck9MK0bCxDMeUkQUz6VeQGp69ImOQrsw46qTz0tmdQrMSbnk
XCuLan5dPm284J9Hmaqi1i6j6KLcZ2NkUnDQFesBVlMEm+fHa2iR6lnAFYZ06UECAwEAAaOCAgow
ggIGMB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fElyalL1BSZMB0GA1UdDgQWBBSzq4i8mdViplUq
CM20HXI7g3JIjJtAOBgNVHQ8BAf8EBAMCAQYwdwYDVR0gBHAwbjAIBgYEAl96AQIwYCQYIBACL7EAB
AjAwBgkrBgEEAc4IAQEwIzAhBggrBgEFBQcCARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMASGCSsG
AQQBZh8BAjALBgkrBgEEAc4IAQMwCwYJKwYBBAHOHwEEMBlGA1UdEwEB/wQIMAYBAf8CAQAwQQYD
VR0eBDowOKE2MASCAiIiMAqHCAAAAAAAAAAMCKHIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAMCcGA1UdJQQgMB4GCCsGAQUFBwMJBggrBgEFBQcDAgYIKwYBBQUHAwQwfAYIKwYBBQUH
AQEEcDBuMCAGCCsGAQUFBzABhhRodHRwOi8vb2NzcC5zay5lZS9DQTBKBggrBgEFBQcwAoY+aHR0
cDovL3d3dy5zay5lZS9jYXMvRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlcg==
Y3JjYS5zay5jb20vv2RLe5z3l0cy9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlci5j
cnQwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovL3d3dy5zay5lZS9jZXVZXBvc2l0b3J5L2NybC9lZVVj
Y3JjYS5zjcmwwDQYJKoZIhvcNAQEMBQADggEBAHRWDGl3P00t2sOnlvLHKk9eE7X93cT+4e5TcaQs
OpE5zQRUTIshxN8Bnx2ToQ9rgi18q+MwXm2lRmrGakYYG0bix7ZgDQvCMD/kuRYmwLGdfsTXwh8K
uL6uSHF+U/ZTss6qG7mxCHG9YvebkN5YjrYRvZ9/uJ9rieByxw4wo7b19p22PXkAkXP5y3+qK/O
et98lqwI97tJhiS2zxFYRk+dXbazmoVHnozYKmsZaSUvoYNNH19tpS7BLdsgi9KpbvQLb5ywIMq9
ut3+b2Xvzq8yzmHMFtLIJ6Afu1jJpqD82BUAFcvi5vhnP8M7b974R18WCOpgNQvXDl+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:DD:84:C2:9F:D2:4C:16:41:DF:01:2D:2
0:90:3B:76:4A:44:D1:2F:29:5D:F1:62:46:AC:03:56:C8:06:19:BB:BE:43:DF:6D:AE:56:F9:2C:8E:F2:3B:BA:C8:91:1A:2F:E4:D7:ED:05:D4:8D:3D:25:39: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:43:8B:C8:1F:EC:7E:4C:29:36:68:6F: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:F7:7
8:0F:1E:7B:E5:E9:24:A2:50:AF:8D: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:8A: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:B5:19:B5:9E:05:8B: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:C8:17:35:9
D: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:2B:8B:6A:7E:5D:3E:6D:BC:E0:9F:47:99:AA:A2:62:2E:A3:E8:A2:DC:67:6
3:64:52:70: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 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 nonRepudiation 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-----
MIIFVzCCBL1gAwIBAgIQdUf6rBR0S4tbo2bU/mZV7TAKBggqhkjOPQQDBDBaMQswCQYDVQQGEwJF
RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEV
MBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkyMDA5MjIyOFoXDTMzMDkwNTA5MTEwM1owWDEL
MAkGA1UEBhMCRUUxGzAZBgNVBAoMEkNLIElEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTlRSRUUt
MTA3NDcwMTMxEzARBgNVBAMMCkVTVEVJRDIwMTgwgZswEAYHKoZIzj0CAQYFK4EEACMDgYYABAHH
OBlv7UtRPYP1yHhOb7RA/YBDbtgynSVMqYdxnFrKHUXh66FkghvHuA1k2DSom1hE5kqhB5VspDem
bwWDJBOQWQGOI/0t3EtccLYjeM7F9xOPdzUbZaIbpNRHpQgVBpFX0xpLTgW27MplMhU8DHBWFpeA
aNX3eUpD4gC5cvhsK0RFEqOCAx0wggMZMB8GA1UdIwQYMBaAFH4pVuc0knhOd+FvLjMqmHHB/TSf
MB0GA1UdDgQWBBTZHiDbX36+iPig5L5HotA0tZoqFjAOBgNVHQ8BAf8EBAMCAQYwFgEYDVR0TAQH/
BAgwBgEB/wIBADCCAc0GA1UdIASCAcQwggHAMAgGBgQAj3oBAjAJBgcEAIvsQAECMDlGCysGAQQB
g5EhAQEBMCMwIQYIKwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL0NQUzANBgsrBgEEAYORIQEB
AjANBgsrBgEEAYORIwEBATANBgsrBgEEAYORIQEBBTANBgsrBgEEAYORIQEBBjANBgsrBgEEAYOR
IQEBBzANBgsrBgEEAYORIQEBAzANBgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEBCDANBgsrBgEE
AYORIQEBCTANBgsrBgEEAYORIQEBCjANBgsrBgEEAYORIQEBCzANBgsrBgEEAYORIQEBDDANBgsr
BgEEAYORIQEBDTANBgsrBgEEAYORIQEBDjANBgsrBgEEAYORIQEBDzANBgsrBgEEAYORIQEBEDAN
BgsrBgEEAYORIQEBETANBgsrBgEEAYORIQEBEjANBgsrBgEEAYORIQEBEzANBgsrBgEEAYORIQEB
FDANBgsrBgEEAYORIwEBAjANBgsrBgEEAYORIwEBAzANBgsrBgEEAYORIwEBBDANBgsrBgEEAYOR
IwEBBTANBgsrBgEEAYORIwEBBjAqBgNVHSUBAf8EIDAeBggrBgEFBQcDCQYIKwYBBQUHAwIGCCsG
AQUFBwMEMEMGoGCCsGAQUFBwEBBF4wXDApBggrBgEFBQcwAYYdaHR0cDovL2FpYS5zay5lZS9lZS1n
b3ZjYTIwMTgwLwYIKwYBBQUHMAKGI2h0dHA6Ly9jLnNrLmVlL0VFLUdvdkNBMjAxOC5kZXIuY3J0J0
MBgGCCsGAQUFBwEDBAwwCjAIBgYEAI5GAQEwMAYDVR0fBCkwJzAloCOgIYYfaHR0cDovL2Muc2su
ZWUvRUUtR292Q0EyMDE4LmNybDAKBggqhkjOPQQDBAOBjAAwgYgCQgDeuUY4HclUbFKS002HZ88g
clgYdztHqgIENyTMtXE6dMBRnCbgUmhBCAA0mJSHbyFJ8W9ikLiSyurmkJM0hDE9KgJCASOqA405
la5nKjTJPNsHQlMi7KZslcTHOoBccx+54N8ZX1MgBozJmT59rZY/2/OcE163BAwD0UdUQAnMPP6+
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:D1:64:82:1B:C
7: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-----
MIID4jCCAsggAwIBAgIERZ4nqiANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAw
DgYDVQQDEwdKdXJVyL VNLMB4XDTA3MDEwNTEwMjU0NloXDTE2MDgyNjE0MjMwMVowajELMAkGA1UE
BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRp
Zml0c2VlcmltaXN0ZWVudWQxNlZDEUMBIGA1UEAxMLRUlELVNLIDIwMDcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDithEdyvuhk/3TJEGMJ1tEZOskE81yMqPGGXaPHXACJ7fncn1D1uQF
t+RG8/ckh7zDquHV1m4HQk7dchaP00rvgsvRlYC9GPcFt6TW8w3t+BkxY1RNbmONgH3qzikljk7m
6Nb8UGL9bOmZdw5k5t9Ht8fgHTnoBkFrxYgsv9d4CCkBTSprNUK+vy/NTak4iAYinWtK6tRHHb1
fxRsLUXiDLSO42Kz+rehhslANX+9Y5/h0wlh3pcmxLB1JWAP0O9fV6N1LUQ3Ym7wMp/lBXuPvl52
yJuSZDWUF7Gklp+vUifOSefF6CeGh8K9BXDvuOqg+5c/6gkfEQxpRgdu+q5FAgMBAAGjgZwwgZkw
EgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAf4wMwYDVR0fBCwwKjAooCagJIYiaHR0
cDovL3d3dy5zay5lZS9jcmxzL2p1dXIvY3JsLmNybDAdBgNVHSMEGDAWgBQEqnpHo+SJrxrPCkCn
GD9v7+i9vjAdBgNVHQ4EFgQUHAf0nL+kJWyztJ4iHx+USBtYeo0wDQYJKoZIhvcNAQEFBQADggEB
ABaiEXv4l5Oh7AgHODwKRyNFqPcSSOgpLCy1XJB3hl3fi21fslccWuBhfzqHQCiQt0fewh109Li
Hq8n1PeKoHBCUVq6NFpxkVsUlUPBr0QsyalO3SQjuOsBLzUWBvY25dtBuAkBMCo0V1Erf7iTeOzu
L4LLbCoeOfeQT3HPmEfSqP5f8V10ST8erbiTVPJwzr66vXaT9YKxy8NyAQc2iaOHuYmGKxs8dgDQ
RkG6b2a/f5q21YEQKDhvz7VvM6tH+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:01:01:05:00:03:82:01:0F: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:E7:7
2:7D: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 nonRepudiation 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 nonRepudiation 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+igAwIBAgIQyvUTmJDa0ZNgy+/fS0vWjANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMTExMVoXDTI0MDMxODEwMTExMVowYTELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxFDASBgNVBAMMC0VJRC1TSyAyMDExMRgwFgYJKoZIhvcNAQkB
Fglwa2lAc2suZWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2QlzKMr7DythntSLo
YAAVkEwV+5djSr0vSIG/Zm9seKyx+2PY8sVzXRoUDlCMlYnstDhBSKMjn2/+HpA7pOipAIAMrk6u
KnpSTTdFbQ+0fzJVPokBgsdsQ6R5TZFPB1nu5zgRRlQmWIFxOpDiNHTt0LObUhWLXzUb31vc1Wma
o2lYcDx1TCs/1E9+camiCl2B5IXrPEU3wBq4waD54izS20DK05+6+hHRg+Tqolg5YSmwbjStEyd/
8AQeokwVloyyH49bnpeluADcZJgxxE9ZUvVWHoxYfmg1IeRU72jHTcljNf1eQN2+9/FtHQMnGzDB
gmAPpghwWz3JtW0JWvMXAgMBAAGjggGeMIIBmjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB
/wQEAwIBBjCB9AYDVR0gBIHsMIHpMIHmBgsrBgEEAc4fZAEBATCB1jCBsAYIKwYBBQUHAgIwgaMe
gaAASwBhAHMAdQB0AGEAdABhAGsAcwBlACAAZgD8A8PwAcwBpAGwAaQBzAHQAZQBsAGUAIABpAHMA
aQBrAHUAdABlAGwAZQAgAHMAZQByAHQAaQBmAGkAawBhAGEAdABpAGQAZQAgAHYA5ABsAGoAYQBz
AHQAYQBtAGkAcwBlAGsAcwAgAGsAbwBtAG0AZQByAHQAcwBhAGwAdQBzAGUAbAAuACECgWQUF
BwIBFhVodHRwczovL3d3dy5zay5lZS9DUFMwHQYDVR0OBBYEFEQlwL63YbGzEGkwzK1+/4f58AF
MB8GA1UdIwQYMBaAFBLyWj7gVhy/zQas8fElyaIL1BSZMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6
Ly93d3cuc2suZWU/cmVwb3NpdG9yeS9jcmxzL2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBBQUAA4IB
AQA4xau3ohdFkpvaiVUR7arNovQUZRCG9Gc3udqHYemovyU7N60Hgomc/ZG+uunScATTUhBcv9a5z
kQxb1dQ1LYDRNr9VCql0QvSEE4t9Sfu3fOhyLrlmb3s8xhhYLJBJ325uDvtO/qFeXLkRXMF5nU8
FE2lyaZP1CHYKVh5QNPPQtGZGSox5oOkCvmt4lUl4lZUwVie75us/WtrD6DJeREBTEDHORlfg8E9
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:A9:00:80:0C: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:2B: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:A6:08:70:5A: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 nonRepudiation 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 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 nonRepudiation 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:

790902506391023449036330872626654973146

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIG4jCCBcqgAwIBAgIQO4A6a2nBKoxXxVAFMRvvE2jANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFR1TEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UEAwwtRUUtgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYfcGtpQHNrLmVVIMCAXDTE2
MDgzMDA5MjEwOVoYDzIwMzAxMjE3MjM1OVjBgMQswCQYDVQQGEwJFRTEiMCAGA1UECgwZQVMg
U2VydGlmaXRzZWVyaW1pc2tlc2t1czEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFDASBgNVBAMM
C0VJRC1TSyAyMDE2MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAr7XWFN0j1CFoGIuV
c9xRezEnA0Tk3vmvIpvURX+y7Z5DJsfub2mtpSLtbhXjAcynq9QV78zjgQ73pNVGh+GQ6oPG7HF8
KllZulYsf1+gBxPxNiLa0+sCWxa6p4HQbgdgYRVGod4IQbib9KbOki3wjCG5WiWh1SP9qcuTZVY+
9zawkSMf65Px/Y4ChjtNFtY66MEvsPChlHHsBNiUbtZ68jJNYCECjtkm0vxz2nSXB2WRlv3/hT
rRgMJ2CNMyFjRQoGQlpH010+fcisObKeyPwA8kI22Oto9MzLw7KsY524OD3B1L5MExYxHD916XIE
HT/9gBP2Zn8qZu/BilKdSlapOlW9ZEw+3w5UOU6LT3t5bAzeQAnD3eCABPifYwHYC0lmKsPpQJ
qtx0Q3Jbm3BGReYiZ9KuK36nF/G78YjhM+yaoERt2B/cKf31j0W/GaGvyHakbokwy7nsbL30sTuR
LR70Oqi5UBMy4e8J2CduR3R3NJw5UqpScJlchngsLAx+WsyC0w38AmMewMBcnlpQbakKo52HrsY
RR1m+NhCVDBy45Lzl8I0/OGd9Ikdg1h7T7SIguZVpyzys8E0yfrcS5YMEd9hMqVPr7rszXCzbxyw
0tVlk8QLMw/lI+XE1Oi7SkgzA2i5Vpa6i2K0ard6GPHzRqGPTkjc5Z4DzZMCAwEAAaOCAn8wggJ7
MB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fEIyaIL1BSZMB0GA1UdDgQWBBScCagHhww9rC6H/KCu
0vtISYgo+zAOBgNVHQ8BAf8EBAMCAQYwggcQGA1UdIASBvDCBuTA8BgcEAIvsQAECMDEwLwYIKwYB
BQUHAgEWI2h0dHBzOi8vd3d3LnNrLmVlL3JlcG9zaXRvcnkvBTMDwGBwQAi+xAAQAwMTAv
BggrBgEFBQcCARYjaHR0cHM6Ly93d3cuc2suZWUvcmVwb3NpdG9yeS9BQBACPegEC
MDEwLwYIKwYBBQUHAgEWI2h0dHBzOi8vd3d3LnNrLmVlL3JlcG9zaXRvcnkvBTMDwGBwQAi+xAAQ1Ud
EwEBwQIMAYBAf8CAQAwHwYDVR0lBCAwHgYIKwYBBQUHAwkGCCsGAQUFBwMCBggrBgEFBQcDBDB8
BggrBgEFBQcBAQRwMG4wJwIIKwYBBQUHMAGGGh0dHA6Ly9vY3NwLnNrLmVlL0NBMEoGCCsGAQUF
BzAChj5odHRwOi8vd3d3LnNrLmVlL2NlcnRzL0VFX0NlcnRpZmljYXRpb25fQ2VudHJlX1Jvb3Rf
Q0EuZGVyLmNydDBBBgNVHR4EOjA4oTYwBIIICIiIwCocIAAAAAAAAwIocqAAAAAAAAAAwI+xJ
AQEwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovL3d3dy5zay5lZS9yZXBvc2l0b3J5L3RzbHMvZWVj
Y3JjYS5jcmwwDQYJKoZIhvcNAQEMBQADggEBAKSIoudSDShDU6yp+VrXYL40wi5zFTfI9ha/kO/
zzLxZ1hf45VJmSyukMWaWXEqhaLWBZuw5kP78mQ0HyaRUennN0hom/pEiBz6cuz9oc+xlmPAZM25
ZoaLqa4upP2/+NCWoRTzYkIdc9MEECs5RMBUmyT1G4sJ6n8L2M2yYadBMvPGjS3yXxYdc/b3a2f
oiw3kKa/q1tXAHXZCsuxFVYxXdZt3AwInYHemCVKjZg8BaRpvIEXd3AgJwt+9bpVx0/MouRPNRv
0jjWIx1sAlL94hO74WZDMFbZVaV6gpG77X2P3dPHKFlRWzjtSQJX4C5n1uvQBxO4ABoMswq0lq0=

-----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:28:89:59:88:86:2C: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:C8:C9:35:80:
84:0A:3B:64:9B:4B:F1:CF:68:A2:49:70:76:59:12:2F:DF:F8:53:AD:18:0C:27:60:8D:33:21:63:45:0A:06:42:5A:47:D3:5D:3E:7D:C8:AC:39:B2:9E:C8:FC:00:F2:42:36:DB: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:AE: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:B
9:50:13:32:E1:F9:09:D8:27:6E:47:74:77:34:9C:39:52:AA:52:70:92:1C:46:78:2C: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:83:58:7B: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-----

MIIEBDCCAuygAwIBAgIEPNkU9TANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2VzdXMxMRAw
DgYDVQQDEwdKdXVyLVNLMB4XDTAyMDUwODEyMDcxN1oXDTEyMDUwNTExMDcxN1owgY4xGDAWBgkq
hkiG9w0BCQEWCXBraUBzay5lZTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZml0c2Vl
cmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEKMAgGA1UEBRMB
MTESMBAGA1UEAxMJS0xBU1MzLVNLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvIIe
K3GJxoPCXVwan+HjJwYGaH3nb/rTPEqg5v9e1c7dnTDBdD2Yteg+IUdHBZDHLj1Tz+JW9Foc0dz
Er96S8+6nMXoonK2x0854JNH2UVbS/+YOGUM6iWSxkHw525tvn5tFaIQoaeh46aQFp9Dngcnv4Ga
td0/7NCkLggjFrKmnNTPlNpLAG9VoCpVyIMvcVCyTNvsSQ+n33ToPO5vtULNYOtCF9MDVND+uNRE2
o0tWIG0Il84owYPA47tJOLgCpAxLNFR5Ys0nB/otBYcO+YiCri0yc6t7ZPs/vcfbR6czhwW0GMjyH
mVPLB+/WHS3P1sk29DdgIC42RTMthJS6ZQIDAQABo4GZMIGWMA8GA1UdEwQIMAYBAf8CAQAwDgYD
VR0PAQH/BAQDAgHmMDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly93d3cuc2suZWUvY3Jscy9qdXVy
L2NybC5jcmwwHwYDVR0jBBgwFoAUBKp6R6Pkia8azwpApxg/b+/pfb4wHQYDVR0OBBYEFOU/DJ1x
PW+8Gb+a9G6/Cf5A652WMA0GCSqGSIb3DQEBBQUAA4IBAQASvWB+YrgN23EMLW7C5/XUwQLNN1RM
Dhr6UzOo5XHZ3pxUXq2ErkSggrS+UJIxkQaSg4OHRru8KTchoJDvS2neeYHOt05zlcAIwoy2GGkH
q1iVN+QZaprDaDNYR5GGKgJb3FZrMtyX4dNwnrZzMFzd6t5YibCW+BDPAmqGJvNHzi5YYdA7l3WT
9Baan1ncKd4FtUVb54fppd19NkbCKKSUd7qRYDduNYqVs1C/C0qqLq4TrxoxoSo+WNLiD01896s
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:D9:45:5B:4B:FF:98:38:65:0C:EA:25:92:C6:41:F0:E7:6E:6D:BE:7E:6D:1
5: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
:85:F4:C0:D5:34:3F:AE:35:11:36:A3:4B:56:20:6D:25:F3:8A:30:60:F0:38:EE:D2:4E:2E:00:A9:03:12:CD:15:1E:58:B3:49:C1:FE:87: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:87:99:53:CB:07:EF:D6:1D:2D:CF:D6:C9:36:F4:37:60:20:2E: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:C 7:59:0F: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-repudiation 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-repudiation 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-----
MIID5TCCAs2gAwIBAgIES7MTKDANBgkqhkiG9w0BAQUFADBdMRgwFgYJKoZIhvcNAQkBFglwa2lA
c2uZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2VzMRAwDgYDVQQDEwdKdXVyLVNLMB4XDTEwMDMzMTA5MTcyOFoXDTE2MDgyNjE0MjMwMVowbTELMAkGA1UE
BhMCRUUxIjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmltaXNrZXNrMxcITAfBgNVBAsTGFNlcnRp
Zml0c2VlcmiltaXN0ZWVudXNlMRUwEwYDVQQDEwtLTEFTUzMtU0sgMjAxMzELMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCrIaYRX2v89k8Hd0ADaOfnUcIn7iM6aOXkAR+jp5827ZhDqDyN
ddF9ZUoBgPghGNIrkHbH7qwex39Yn10ka24lCjcwEMvQMPbyPnXa4RyJ+wEZttmjBl++FfiZK54
L+vD7Dyy4YYB0Og9ktB4qptsDBj+giiv/MGPeGeNs3TacIdNb7+3spITPtPKlDfrufvq4H6jNOv9
S9bC+j2VVY9uCFXUro8AA3hoOEKJdSjlpYCa51N8KGLVJYRuc/k81xqi054Jz+Cy/HY/AcXkk2Jk
xJpJoEXmcuTkxjO/QE/Xbd+mRJHnq6+HurOiKcxKwZCPAa+d+dvRPkbyq9ohMXH9AgMBAAGjgZww
gZkwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAcYwMwYDVR0tBCwwKjAooCagHo+SJrxrP
CkCnGD9v7+I9vjAdBgNVHQ4EFgQUXXUUEYz0pY5Cj3uyQESj7tZ6O3IwDQYJKoZIhvcNAQEFBQAD
ggEBADFuAGtSoO8PsWRw/QxFzcSEZtbq2KXC9yZ8YQPWBLY4Mh3OVLFJqWyKC+8JHy9D5tJTG49F
5UHyDJPuIDXvC2rjRlkqvS/W7sy3MqGh7e+6bg+aD4mo+98Oalnqi12UD+ki+N8JKPXjHNJ31Av
H6E/xDsCsvtzubyIxI+FU8R0XODIUFbBqRtatRI1/zVaKRhD6LNGPt3rz/3IKmuEv6b29mzL+p4
oNULqpPr6aTmheZme8ZHuEIh3Zp5kdoX3i2D4hsmgClpevZifo196zeKRLk0Qs6nmRjoMxyk6jY1
ric3/VnV81oyhXSBY1GZnbM4qPIw2S5kSA2bb1pkwFo=
-----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:01:01:05:00:03:82:01:0F: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:F6B: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:8
F: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:A
F: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:D8:3 6:F6:13:BD*

Certificate fields details

Version:	*3*
Serial Number:	*42879783182822194711502757635696878 74*
X509 Certificate	

-----BEGIN CERTIFICATE-----
MIIErDCCA5SgAwIBAgIQAznVp1LayatNgy6bN8f9QjANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMDYxOFoXDTI0MDMxODEwMDYxOFowbTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxJTAfBgNVBAsTGFNlcnRpZml0c2VlcmltaXN0ZXN1ZDEX
MBUGA1UEAxMOS0xBU1MzLVNLIDIwMTAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCr
laYRX2v89k8Hd0ADaOfnUcln7iM6aOXkAR+jp5827ZhDqDyNddF9ZUoBgPghGNIrkHbH7qwex39Y
nI0ka24lCjcwEMvQMPbyPnX/a4RyJ+wEZttmjBl++FfiZK54L+vD7Dyy4YYB0Og9ktB4qptsDBj+
giiv/MGPeGeNs3TacJdNb7+3spI1PtPKlDfrufvq4Hf6jNOv9S9bC+j2VVY9uCFXUro8AA3hoOEKJ
dSjlpYCa51N8KGLVJYRuc/K81xqi054Jz+Cy/HY/AcXkk2JkxIpJoEXmcuTkxjO/QE/Xbd+mRJHn
q6+HurOiKcxKwZCPAa+d+dvRPkbyq9ohMXH9AgMBAAGjggE+MIIBOjASBgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBxjCBlAYDVR0gBIGMMIGJMIGGBgsrBgEEAc4fZAEBATB3MCEGCCsG
AQUFBwIBFhVodHRwczovL3d3dy5zay51ZS9jcHMwUgYIKwYBBQUHAgIwRhpEAEEAcwB1AHQAdQBz
AGUAIABzAGUAcgB0AGkAZgBpAGsAYQB9hAHQALgAgAEMAbwByAGEdABIACAASQBEAC4w
HQYDVR0OBBYEFF11FBGM9KWOQo97skBEo+7WejtyMB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fEl
yalL1BSZMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly93d3cuc2suZWUvcmVzL3NpdG9yeS9jrmxz
L2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQC3qNBgY2I9Wqm4LZYKAjCYkc2Nltm1RS9f
rMvQJ4aEE4Y4TtW2LPcQp2lenOf9aYdEB8G/E9CytZSPlFuvDdsdknj6fg1XCeu6lTR2wIkxJcAe
LQvrFEfb1mcAa5tU9RNalZhYc7MFMFQTjQP+GBNxz+KIjNDVASFdv7TCe7GBjsW8Dfcs9lQGHaWs
BRkHCyuPGlHfH+cmMuhLtWqa4Qlg4f54kcsGO7s4buKtk6XqEj8Cj2ITdfk/aUs9QoxxkYWGwSUl
CueTamzutXEJo9yz5Jp6IFdGjotmjb/EBUCt2sFfl83a4Cm1D3L3/KYb5g3cYlDEpPWNqbNuA1Xo
sIqK

-----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: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:60:84:72:27: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:D6:A: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:8 F: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:A F: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*
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:A A:A3:60:E5*

Certificate fields details

Version:	*3*
Serial Number:	*134258170546889953808822267264047226074*
X509 Certificate	-----BEGIN CERTIFICATE----- MIIFKjCCBBKgAwIBAgIQChm34x8ah3BVcFcdIs2c2jANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE1 MDYwNDEzNTAyMVoXDTI0MDMxNzIyMDAwMFowbTELMAkGA1UEBhMCRUUxIjAgBgNVBAoTGUFTIFNl cnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEX MBUGA1UEAxMOS0xBU1MzLVNLIDIwMTAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCr laYRX2v89k8Hd0ADaOfnUcln7iM6aOXkAR+jp5827ZhDqDyNddF9ZUoBgPghGNIrkHbH7qwex39Y nI0ka24lCjcwEMvQMPbyPnX/a4RyJ+wEZttmjBl++FfiZK54L+vD7Dyy4YYB0Og9ktB4qptsDBj+ giiv/MGPtGeNs3TacJdNb7+3spl7PtPKlDfrufvq4H6jNOv9S9bC+j2VVY9uCFXUro8AA3boOEKJ dSjlpYCa51N8KGLVJYRuc/K81xqi054Jz+Cy/HY/AcXkk2JkxIpJoEXmcuTkxjO/QE/Xbd+mRJHn q6+HurOiKcxKwZCPAa+d+dvRPkbyq9ohMXH9AgMBAAGjggG8MIIBuDASBgNVHRMBAf8ECDAGAQH/ AgEAMA4GA1UdDwEB/wQEAwIBxjClBlAYDVR0gBIGMMIGJMIGGBgsrBgEEAc4fZAEBATB3MCEGCCsG AQUFBwIBFhVodlHRwczovL3d3dy5zay5lZS9jcHMwUgYIKwYBBQUHAgIwRh5EAEEAcwB1AHQAdQBz AGUAIABzAGUAcgB0AGkAZgBpAGsAYQBhAHQALgAgAEMAbwByAHAAbwByAGEAdABlACAASQBEAC4w HQYDVR0OBBYEFF11FBGM9KWOQo97skBEo+7WejtyMB8GA1UdIwQYMBaAFBLyWj7qVhy/zQas8fE1 yaIL1BSZMHwGCCsGAQUFBwEBBHAwbjAgBggrBgEFBQcwAYYUaHR0cDovL29jc3Auc2suZWUvQ0Ew SgYIKwYBBQUHMAKGPmh0dHA6Ly93d3cuc2suZWUvY2VydHMvRUVfQ2VydGlmaWNhdGlvbl9DZW50 cmVfUm9vdF9DQSSkZXluY3J0MD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly93d3cuc2suZWUvcmVw b3NpdG9yeS9jcmxzL2VIY2NyY2EuY3JsMA0GCSqGSIb3DQEBDAUAA4IBAQB4/0TLXdtMTnzl8Z81 0lR3pESCq6ueQRvGPPl2isGe3ldA9PhKZ7j6323ifl2ldOdMeU12gd4pzuHXieFClYhswqXCR1hu LNu1KA8PRhgxdOBQ1etRSkZTlf1MhBgpxot2Tu4G2xKQ7wfetdqnrUQ/u++BuAhuHA2xsma236eQ 7z3izoxCOSe+FMpQT/SY9NvKtZlmFEPycxZxu0uWCQtBbx+b/MAYKgq2/vMvLO4lyRqkeSRuLMZT 4AA42HgggUwL7hWiwedyEqvwq0Sg3e92F2wBtf+Xah/WeZBioxul1TRtzFcge6BTiF2S0RdbaaOW 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: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:A:F: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-repudiation 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:

12537959042210943457040491017613190 5756

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIGgTCCBWmgAwIBAgIQXlM7EyVgNCtYSVcwizB43DANBgkqhkiG9w0BAQwFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMCAXDTE2
MTIwODEyNTA1NloYDzIwMzAxMjE3MjM1OTU5WjCBhjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFT
IFNlcnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNl
ZDEXMBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MIICIjAN
Bgkqhkig9w0BAQEFAAOCAg8AMIICCgKCAgEAlkOLeKQPKK1U8VK7z2Dzt2SX2KbIGqrBmOXfzllm
zXHxGVopSeji24MdR5Ok6NqXxanbyufXXRTeuE5nQ80lzr5+9U21DPmVUADFNWnDLy6NWyqE3C
vrYp7tVOHbiTb9MI3ECvQNt8YM0HGwdSfc8kGXuX8d4oxxeG4AD+wrj1+LJ0ioaQfIS67bcwq3x
EO0WVv1hMrJOoMmPpaqrvRLcoikpmjnPm/Gtfx64FcyXiMmNxFDnROVMgr1OQKbxAdIX3fu32fcX
jXesCTcACLINRMi5Sb1wowjGEpqL2H53+JDIrdE7hM0uUqX4aaT5etaUh0o2hxOBHg3m6WRAZmBP
qO1BqIBN6PRMWYgab7BBtJMUKXE+FUaNy9Lb8jraX85t3IwN/hbbMx3wUAqZvoQVIaJu2tsP8eTG
JUd6jES9q9rH788LNf2w9o16blr1cM0AkzfbPf1ktClERcQd+iEhAPluSjKwMHlehRQGwGGuo7db
4QXKhXDXPGK5YRw6Q56mp+8pSqJJqpdIQCieEXbHm9sHsoP5yaQygZf8nJpd0nlpdcTq91aEjrWu
uksQTNDG9++8NSAql2G/BVCesWx/zR0KtcWecMPUVfe7qEEFurWsewpLgZFsk5RLtNGwyTEgHHBf
JqAJC8l2VMfbbsEW+tcjdMqb6BHgT6hNCx8CAwEAAaOCAfcwggHzMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgEGMIHTBgNVHSAEgceswgcgwgYQGCSsGAQQBzh8HAzB3MCCGCCsGAQUF
BwIBFhVodHRwczovL3d3dy5zay5lZS9DUHMwUgYIKwYBBQUIHAgIwRh5EAEEAcwB1AHQAdQBzAGUA
1ABzAGUAcgB0AGkAZgBpAGsAYQBhAHQALgAgAEMAbwByAHAAbwByAGEAdABIACAASOBEAC4wCAYG
Z4EMAQICMAsGCSsGAQQBzh8HAjAIBgYEA96AQEwCQYHBACL7EABATAIBgYEA96AQcwCQYHBACL
7EABAzAAdBgNVHQ4EFgQUrl5Y9fLy2cGO2e9OB9t1ylDihwAwHwYDVR0jBBgwFoAUEvJaPupWHL/N
Bgzx8SXJqUvUFJkweAYIKwYBBQUHAQEEbDBqMCAGCCsGAQUFBzABhhRodHRwOi8vb2NzcC5zay.51
ZS9DQTBGBggrBgEFBQcwAoYYaHR0cDovL3NrLmVlL2NlcnRzL0VFX0NlcnRpZmljYXRpb25fQ2Vu
dHJlX1Jvb3R3RjQt0EuZGVyLmNydDA9BgNVHR8ENjA0MDKgMKAuhhxodHRwOi8vd3d3LmNrLmVlL3Jl
cG9zaXRvcnkvY3Jscy9lZWNjcm9vdC5jcmwwDQYJKoZIhvcNAQEMBQADggIBAAah2vGqi+Pe5+CPta
rh0vCQWOm233nl5Y9qL+JgG5PccowQ41kzf4qknmP6BHfisYGQsRc75K07A+/BdlFrLMbP3fFsuT
i7+HAmAjXYEq35G49GiAQg52+HvZiBe+RtbR8yOOar5fAKnzS1yNy9M1z7g7yMcEouk3TUebc2aan
Mvzabc7qgV3HfGDfZkzbL9PIcjmFl0LQEfleef6sdMhy6C0HiditdLSUZYISySJpb6lvJBGdN4Vrb
o2fNtL3qlc+vX1Jvh/qLFIFmFXuC6lIjFJFtpIbCIQMtHoMXdl1A5lzzkmrTLPTSYDAQXXn9RPnz
sRz2GnIYRV4xGayDGbUyow==

-----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:A4:4D: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:DC:28:8B:1C:5E:1B: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:A8:80:4D: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:B0: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:85:70: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:C
4:EA:F7:56:84:8E:B5:AE:BA:4B:10:4C:D0:C6:F7:EF:BC:35:20:2A:97:61:BF:05:50:9F: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-----
MIIDPDCCAiSgAwIBAgIEQi2iwTANBgkqhkiG9w0BAQUFADB8MRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMQ8w
DQYDVQQLEwZFU1RFSUQxCjAIBgNVBAQTATExEjAQBgNVBAMTCUVTVEVJRC1TSzAeFw0wNTAzMDgx
MzA0MDFaFw0xMjAxMTIxMzA0MDFaMG8xCzAJBgNVBAYTAkVFMQ8wDQYDVQQKEwZFU1RFSUQxDTAL
BgNVBAsTBE9DU1AxAzJjAkBgNVBAMTHUVTVEVJRC1TSyBPQ1NQIFJFU1BPTkRFUiAyMDA1MRgwFgYJ
KoZIhvcNAQkBFglwa2lAc2suZWUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ8mLeLkRHLx
MNCB5Pz8R5DnvPdVxBS91PoHboLnbhjlp1ecByVosjwGpXCGu8ttUPuv81Azgqq97AsSugMIJ7Pu0
gj4bg0Mf6O/9XyoT7RI7H0BuEn4KJQlFcw7tXizI5KUWFFZ4Qg8kfg0xwrDrL1jusBtRbeRARG3D
hH8dgZBpAgMBAAGjVzBVMBMGA1UdJQQMMAoGCCsGAQUFBwMJMB8GA1UdIwQYMBaAFHgXtQX5s1jN
WYzeZ15EBkx1hmIdMB0GA1UdDgQWBBRM+GJhloJeOPpJDgvA0clxQXdnVTANBgkqhkiG9w0BAQUF
AAOCAQEAtD8dP+swtSeigLxL3uUXV/tmQkjre7Ww39Uev71Ldtx Q6zC7MDjcsLW13JaU0pRuu/p/
eGe6b4/w46tSMsBx/U+D1WnHeCj1ED9SFWwfNQFVz9FkM5JEkPDm7lw5hHoxIghRHAC3NMbR3sCr
VQA2YEL12WypslROoz8XlRT1LN4pwVchpBeWO7xbQPUtoaxKrSCGumtxtxA3KRJ7POHPTAH4cvip
xaZhS1ZcXbKtxsesGW+7KLZirpTBT17ICXEA1CFXDWmJ8MHRhbeNWK3G1PERgTiGtBQV7Z00CzmJ
PHmb1yfcT27+WZ1W9tRQsjhGEWyMVkNnZooWHljLpNucQA==
-----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:B 2:3C: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:2 4:7E: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-----
MIIDnDCCAoSgAwIBAgIERZ0acjANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJFRTEiMCAGA1UE
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEPMA0GA1UECxMGRVNURUlEMRcwFQYDVQQDEw5F
U1RFSUQtU0sgMjAwNzAeFw0wNzAxMDQxNTE3MDZaFw0xMDAxMDgxNTE3MDZaMG8xCzAJBgNVBAYT
AkVFMQ8wDQYDVQQKEwZFU1RFSUQxDTALBgNVBAsTBE9DU1AxJjAkBgNVBAMTHUVTVEVJRC1TSyAy
MDA3IE9DU1AgUkVTUE9ORVSMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAJmoB3SJCpPzcoHNqK1J0tRNQjgr5iuB27uE1VacIbITjD/Nc1AefKz5
ydNPIaBNehm4yKxBYGxEcWOSJHVXyhJMg53EAUOw/45c46gvznXupHuJ6TEiGjh1pxaXTeLSnTqz
NDZDAGQsOTgIbwGLa5U5ad8rXYu2YkJKsAfo6jT5AgMBAAGjgdcwgdQwEwYDVR0lBAwwCgYIKwYB
BQUHAwkwEgYJKwYEBQUHMAEFBAUwAwQBMDCBiQYDVR0jBIGBMH+AFEgG3r6Mh1eVgHhj+pwjKyug
Ohh1oWGkXzBdMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQK
ExIBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMQ8wDQYDVQQKEwdKdXVzdGVlcmltaXNlc3Qwgg
DgQWBBRJ/snw1GDL3fUlH9n9Cpn8yhXiC7DANBgkqhkiG9w0BAQUFAAOCAQEAYzGkZD/uaXlWPeye
1z5IiI83nmAjiJyvoj/z3BB9ZFWMX+ZY4Fz6/V/fzD0xXoeDpWbBKxcuctPXzXYxEH17n0/3yGOz
8jhdJNBUCwRmd+96oHsU9uWSf+D2tiq1jPw6HVCiUYObCOWig/+JpFIWsBV4gTW8/2PSGig85Xl
EsWLK7i7tIe60nnw/rWnfbCxkMRcbrAF1L/JIlmUYUdkGOGQ9KPVqwR/MyWrwFlcSy2QIbclaWMu
iUc1nt8bmIXKoFZxbLzXYC00zba9cY7lSC4WPuhBtrQJ9JWb4OeoXd5j6O45UaH6XbarfrhER1GH
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:B3:34:36:43:00:64:2
C: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:D D: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
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2tlczEPMA0GA1UECxMGRVNURUlEMRcwFQYDVQQDEw5F
U1RFSUQtU0sgMjAwNzAeFw0wOTEyMDExMjQ1MDBaFw0xNjA4MjYxMzIzMDBaMIGHMQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2tlczENMAsGA1UECwwETONTUDEr
MCkGA1UEAwwiRVNURUlELVNLIDIwMDcgT0NTUCBSRVNQT05ERVIgMjAxMDEYMBYGCSqGSIb3DQEJ
ARYcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA48pyM/QfeiU1Kbu4
AdcAUKXBiwbYbBl4gCltZHC5tZ77fKj2mqfPX2/XW1EqzbVvG0PYIkapkQzBr3R1S6Uaxh1DLC2C
c8BRnqmhXoE03o8En7N9xpN9dGGDBHp2aElBcVVZnAvF4jgbPDCNFAeo3cvpjlx18n0URiVOZFEd
xDvF8PFo/exKXtjRM+jk3K6+9doHYvSXn9klFbT8Wge87Qdll3gQzZE3L8QMXF0z4xbBH1lyTmVL
t5yZ0fxoE0jNlZFvn2w2EDnU4CKIld8w6Zjd5kdxomcwDzGiuuLzdiJllPt05USJcY4FHtn9YAVKWm
oIYY/o6xOUzU8fAz6yA1tQIDAQABo4IBLzCCASswEwYDVR0lBAwwCgYIKwYBBQUHAwkwgAQYDVR0g
BGIwYDBeBgorBgEEAc4fBAECMFAwJQYIKwYBBQUHAgIwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xp
Y3kwJwYIKwYBBQUHAgEWG2h0dHA6Ly93d3cuc2suZWUvYWphdGVtcGVsLzCBiQYDVR0jBIGBMH+A
FEgG3r6Mh1eVgHhj+pwjKyugOhb1oWGkXzBdMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUxCzAJ
BgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMRAwDgYDVQQDEwdK
dXVyLVNLggRFm6ANMB0GA1UdDgQWBBQ4Ah4wumZ6EXROll5wZOXedXpOFDANBgkqhkiG9w0BAQUF
AAOCAQEAJ/LvPUcvNRcBp+J78fZRofhk/ifKNLxCUoh8T3MjtU9u5R0KojRlye+1NU8MqH/zrKhr
6TPxuXD0cRrFQ9Hy60ll7lzzaegrQVNgq7UgQINvcuNxWZcGtEa3ba9M7tBpQeFxqp3CpBytGeVu
Xn65hqOBKdp/zYEiMUUkYNAT5A6SSPYLAOgARCl/ydBx+cw0l0fwYvw72FKZa2Mlt5DmXBccCtrQ
4l/sb95xfANCNe5n5sBvBhY4F+slWZUVJ8fTVh7iGaVFSayQfeAAci0m/4/ksiXBwfx6qhzyB3yq
cnSk489oBrrCegua/t+3LizfHpNZvDphKMPuAZ4uhcLfQA==

-----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:A
8: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:88:99:65:3E: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
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UECxMYU2VydGlmaXRzZWVyaW1pc3Rl
ZW51c2VkMRQwEgYDVQQDEwtFSUQtU0sgMjAwNzAeFw0wNzA0MTMxMDE2NDVaFw0xMDA0MTcwOTE2
NDVaMH8xCzAJBgNVBAYTAkVFMSIwIAYDVQQKExIBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMQ0w
CwYDVQQLEwRPQ1NQMSMwIQYDVQQDExpFSUQtU0sgMjAwNyBPQ1NQIFJFU1BPTkRFUjEUMBYGCSqG
SIb3DQEJARYJcGtpQHNrLmVlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD+Z0LZ6TjBzx4x
+UshExea1nIMsS86xAN6u/amL V8XQE+vodEld8iqtRsrvFvQ74isYOys1JKqiq+1ryic6j2FnMDZ
ueLiXZl51QWvuhWu+aT4BwEaA8rUxMgKJ94zWksrqSf9cjoaap+9DlDhEsrDa+/89CPl2rIZIB5l
qeHLQQIDAQABo1cwVTATBgNVHSUEDDAKBggrBgEFBQcDCTAfBgNVHSMEGDAWgBQcB/Scv6QlbLO0
niIfH5RIG1h6jTAdBgNVHQ4EFgQUMsMzikmZqG6CcdgnD5VAXfQeCrgwDQYJKoZIhveNAQEFBQAD
ggEBAH0cUFQ7LznD4R8XWj/6rsNhe0fme3Os7cyZGNkx1EWenkgdMHCV/gN3SyIfrjW7sEJM62sS
TX+8Kc2J+6b5YH0TcSmSDqYICn6zVbsq5MLtHW5wmwKucBJ5xFgoC3NNCEp8wVrzuQmm6xCvFWQV
Q6uNhjuxCQxcDKgL.wpL7iEcBEMmTTKkvqEtqrvu/LZ/a2OHytkEoXGheN8KlEeIv7AJBPVL8OCv4
UpgyU0rVnmIeX2F/KG3wmo4U3kVupuF9kaPrOeOGYG3ZzK2HNwfRNkZ/Ej7AuPazkumAHdsJBbpT
dBYq8d8er8XZKai24Ra/e5eEmcMye+O8lpxAA4ExY+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
ChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3Rl
ZW51c2VkMRQwEgYDVQQDEwtFSUQtU0sgMjAwNzAeFw0wOTEyMDExMTQxMzBaFw0xNjA4MjYxMzlz
MDBaMIGEMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEN
MAsGA1UECxMET0NTUDEoMCYGA1UEAxMfRUlELVNLIDIwMDcgT0NTUCBSRVNQT05ERVIgMjAxMDEY
MBYGCSqGSIb3DQEJARYJcGtppQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
so91KG7EHsjAxMairaCKUHSOyXp5rzxRq5Y9LDyplVbHfth34fbB7M5G+wnu5CZgJsfJ7DF3MjpA
7nIAHd5alAynIUl/CNXejf+XnJ/vyF1eQvAoWvnjBPVIS0mbaABgF54ybAGE2E7UKezVOAj7RoQV
AMHQcYVjxZW5OWz3yJX9KdaDZPOzqlGtRYKUASHiwAFwExKcqfaHOj0qO8+KdSvEBaVlpe5kunEV
Evn+kgNKBtzdH2XFMjVFa4im31KW+iq7mNQwUiZDSe9ho6T6UrWu7g8yTQowx3SYLTqVxR0YVgcY
NCx7nn1AVGNxK3oeonrHHqcBp6qSA1YXeQNfiQIDAQABo4HDMIHAMBMGA1UdJQQMMAoGCCsGAQUF
BwMIMGkGA1UdIARiMGAwXgYKKwYBBAHOHwQBAjBQMCUGCCsGAQUFBwICMBkaF1NLIHRpbWUgc3Rh
bXBpbmcgcG9saWN5MCcGCCsGAQUFBwIBFhtodHRRwOi8vd3d3L1nrLmVlL2FgYXRlbXBlbC8wHwYD
VR0jBBgwFoAUHAfl0nL+kJWyztJ4iHx+USBtYeo0wHQYDVR0OBBYEFPBOCDPMR+kfp7Ozk5U68E68
/AseMA0GCSqGSIb3DQEBBQUAA4IBAQCRaqmxZgJiJ+MLamb/P4vyS6azt6/tj8dZCK++V/3GnecR
m7CiZpR47EnW0NyDzCeeGyTWSkVlnZPnNvXRx700Nn0M4Inia5pNhSuVmWS3p5cV70vCbsfRD26+
6CZhkHWnL/J2xpqeacUI.tgPPy9gBTyC2ybQrl7dv7W5Qc+3UFywmE5N8ozQuEJroGz7P+yCbBEss
WcmIUNDNdO0xs6aQ21F+DV4FUB0lajuIL YFz4xM+81akYFVqaGPCVwbQgFSWRKmamj8FxfWjA4DC
rgkHVR1rA3tZyirfCBK9cfWpTCLr8zq9Ur0jTAeGrHRzHlUrB9mYZwyr0kNOyl9293xh

-----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:1
D: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:32:6
C: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:A
E:55:64:BA:71:15:12:F9:FE:92:03:4A:06:DC:DD:1F:65:C5:32:35:45:6B:88:A6:DF:52:96:FA:2A:BB: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----- MIIDzzCCAregAwIBAgIEScskSjANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL TEFTUzMtU0swHhcNMDkwMzI2MDY0NDI2WhcNMTIwNTA0MDU0NDI2WjCBgjELMAkGA1UEBhMCRUUx IjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmlmaXNrZXNrdXMxDTALBgNVBAsTBE9DU1AxAxJjAkBgNV BAMTHUtMQVNTMy1TSyBPQ1NQIFJFU1BPTkRFUiAyMDA5MRgwFgYJKoZIhvcNAQkBFglwa2lAc2su ZWUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKi6weNl7Wj7sL6JD4YUNtJXQ79KL53x5m4 QGRsijGJaV5YggE5zJyVZGlsX4FSd9JFIV597ypAUGDbLPf0nDdlSlGteP7zamyETl3GI6bKfkeU ulE707r7uC+8FFe9iHOOL20+pi7WFzwnyXT9yuWs0eCoKdjQvLpMiq0MBIm9AgMBAAGgjgcIwgb8w EwYDVR0lBAwwCgYIKwYBBQUIHAwkwaAYDVR0gBGEwXzBdBgorBgEEAc4fBAECME8wJQYIKwYBBQUH AgIwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xpY3kwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuc2su ZWUvYWphdGVtcGVsMB8GA1UdIwQYMBaAFOU7DJ1xPW+8Gb+a9G6/C5A652WMB0GA1UdDgQWBBT5 9PTkSIzYXNBxQQnAhqH3BttED0TANBgkqhkiG9w0BAQUFAAOCAQEAhyl3H6fo1bz3mD0JcD4eY1sl cwec92Qgkn6i9TsO5TlDQCJxiC/80zlh+H5dgIMcNQ6gNbr1cWsUw7xAanv2hGlg20IWq7uCyy5L DghFpO2BWDzTJjmiVTXzyVEvqST0W6efDtwi1tA8H7b+aAzc9ItWm7pYlucGvneKJq07t/UvU9ON SDUfVLPNMr8slwCMOexVDZ+eiBlvrLL3N7NouPs7UpFh/+m5JsERmeLbbrNYimHUUn2PJ/trJ3kB EVFToO+nFdBElfzC3bjSlbPXFxSOL+AqSgvRIaB4CEWUxa33wzoZNaVpCh5AupxQOGdr4u7ajw5h kV8Y9VZ7OFej6A== -----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-----

MIIELzCCAxegAwIBAgICAMswDQYJKoZIhvcNAQEFBQAwbTELMAkGA1UEBhMCRUUxIjAgBgNVBAoT
GUFTIFNlcnRpZml0c2VlcmimltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2VlcmimltaXN0ZWVudV
dXNlZDEXMBUGA1UEAxMOS0xBU1MzLVNLIDIwMTAwHhcNMTAwNDA4MDgwMTMxWhcNMTYwODI1MjIw
MDAwWjCBgiEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZ
QVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEmMCQGA1UEAxMdS0xBU1Mz
LVNLIDIwMTAgT0NTUCBSRVNQT05ERVIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDh
WwGpngF0sdGCgOgiyT12A/Vdm9sMPr/cUwZhU7DA5C8rU1yJhbrh28IMpv0eas6/+IC1oDxI24zj
fWIKlHwpBmhUTrFsmvmKRIu4a1F6VwNwYEdoAZrQDpzZSve6H6R/+0Uy0BAolebdhPUK22pKd8V1C
BY3de886Ray8uUJu09MAU8j+xsoUNOzyxiWdAVp1YTXRhhUt+EQVYJ22RBZ6+b9fPQvgb9aWgE/W
wqUh7OrgTnrGZVzgO46prfE7zkALG0FYZCzQTCMH8aIqqte0E3HwSVIKh9qwbRPB9WTDCtCqajb4
qgGRTXvWT4vA TlHvx8GpJ3roZkp5AlQno3hTAgMBAAGjgcIwgb8wAYDVR0gBGEwAzCBdBgorBgEE
Ac4fBAECME8wJQYIKwYBBQUHAgIwHwGRoXU0sgdGltZSBzdGFtcGluZyBwb2xpY3kwJgYIKwYBBQUH
AgEWGmh0dHA6Ly93d3cuc2suZWUvYWphdGVtcGVsMBMGA1UdJQQMMAoGCCsGAQUFBwMJMB8GA1Ud
IwQYMBaAFT11FBGM9KWOQo97skBEo+7WejtyMB0GA1UdDgQWBBQ3MJkXG2Go/6j4hem465aue3P5
qjANBgkqhkiG9w0BAQUFAAOCAQEAKhoVTlI1ECecFkyt9Qgr0XW3WEFprrqTDE4lycMlx+LNjWk3
0aknMldEtzIC5nCDX27NCWkpbN1o/3ddBv0cKMa05ZK8sHQxU6A5Oev8Dcp72/LFEChq5IDqgqW2
BiHIhytPfi93JIuV03b/Wgq3fpRyBd21VE9254W4A90zeNxDvdpqxIrD2Lonzm/V/oomzEHsp4kKx
XkPnRU4vGtTnxxAmxYp9OuLkvpUCLNoAWMbYqb4cbYzaZ9tQlkBy3nI352Rx5obYDb3R/ZVWuYLL
SocWL7b2QwlDP7LA8VNDqmQvioHt8GcyKXQ5/eWMyj2ePt58waVhwfSdd4nANKtq1g==

-----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:5
3:5C:89:85:BA:E1:D8: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:D1:4
C: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:3
D: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:3
8:78: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:	*15234502409810743543451622493997730 0289*
X509 Certificate	*-----BEGIN CERTIFICATE-----*

MIIEvDCCA6SgAwIBAgIQcpyVmdruRVxNgzl3N/NZQTANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTEx
MDMxODEwMjE0M1oXDTI0MDMxODEwMjE0M1owgZ0xCzAJBgNVBAYTAkVFMQ4wDAYDVQQIEwVIYXJq
dTEQMA4GA1UEBxMHVGFsbGlubjEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEN
MAsGA1UECxMET0NTUDEfMB0GA1UEAxMWU0sgT0NTUCBSRVNQT05ERVIgMjAxMTEYMBYGCSqGSIb3
DQEJARYJcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAihvGyhMVrgRe
HluKln1za6gvCE/mlSREmWjJFpL9llvuEUZoPFlypYA8g5u1VfgkeW5gDq25jAOg4FyXeDGla+pJ
n2h0o2Wc2aeppVG/emfGm/jA8jjeyMrwH8fAJrqVQ7c9X2xSwJEch/P2d8CfMZt5YF6gqLtPvG1b
+n6otBZA5wjlFD/inJBMUvqHSz3+PLfxO2/T3Wyk/c8M9HIMqTelqyiMGRgWehtiU1OsL9armv3d
QrHs1wm6vHaxfpfWB9YAFpeo9aYqhPCxVt/zn2NQB6vxyZS0hsOrXL7SxRToOJaqsnvIh/0erPPF
tRHUvbojYYgl+fzlz0ht6QJoNwIDAQABo4IBHTCCARkwEwYDVR0lBAwwCgYIKwYBBQUHAwkwHQYD
VR0OBBYEFKWhSGFt537NmJ50nCm7vYrecgxZMIGCBgNVHSAEezB5MHcGCisGAQQBzh8EAQIwaTA+
BggrBgEFBQcCAjAyHjAAUwBLACAAdABpAG0AZQAgAHMAdABhAG0AcABpAG4AZwAgAHAAbwBsAGkA
YwB5AC4wJwYIKwYBBQUHAgEWG2h0dHBzOi8vd3d3LnNrLmVlL2FyXRlbXBsbDBgNVHSMEGDAW
gBQS8lo+6lYcv80GrPHxJcmpS9QUmTA9BgNVHR8ENjA0MDKgMKAuhixodHRwOi8vd3d3LnNrLmVl
L3JlcG9zaXRvcnkvY3Jscy9lZWNjcmNhLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAw2sKwvTHtYGt
D8Jw9mNUuj/mWiBSBEBeY2LhW8V6tjBPAPp3s6iWOh0FbVR2LUyrqRwgT3fyWiGsiDm/6clqM+Ib
lLp/8ztlRQjquhW6XCD9SK02OQ9ZSdBwcmoAApZLGXQC34wdgmVihLTTNxONnDACBKz9U+Dy9a4Z
T4tpNkbH8jq/BMne8FzbvRt1bjpXBP7gjLX+zdx8/hp0Wq4tD+f9NVX0+vm9ahEKuzx4QzPnSB7h
hWM9OnLZT7noRQa+KWk5c+e5VoR5R2t7MjVl8Cd+2llxiSxqMSbU5/23BzAKgN+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:11:46:6C: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:E8:62:53:5C: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:B2:7:B: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 |
| | |

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:A 6:36: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
rJdk8iiOrcUN2FApNaI2wFnRIw9rsF8u9KPu3g47ZSuKKYkpdVVupTwt6gK+brQczfQSbO3xOCj7
cubcl5+6jDPXSh47zma10hh4U5VECOtCDBhlRfA/UJfMYj6BYgEhFuRQxEBgAF5yyEJX1X8Sco/
GQcha4Er5SyEhHvXu/vvg0OVfLRqH/7gGBBRLPMOsDImmXf+C0UYKs7ywFBf+M0VnWH9u0p7E8Xz
A8s3m2ivTdU/JYIU5Zy7NFeV9NJgZw3iaLCO1dbV2gBIWngGvqlwQ3coKHMs3tMBT25+WWmKVMsH
Fi254ysCAwEAAaOBwjCBvzATBgNVHSUEDDAKBggrBgEFBQcDCTBoBgNVHSAEYTBfMF0GCCsGAQQB
zh8EAQIwTzAIBggrBgEFBQcCAjAZGhdTSyB0aW1lIHN0YW1waW5nIHBvbGljeTAmBggrBgEFBQcC
ARYaaHR0cDovL3d3dy5zay5lZS9hamF0ZW1wZWwwHwYDVR0jBBgwFoAU5T8MnXE9b7wZv5r0br8J
/kDrnZYwHQYDVR0OBBYEFCRXW4FmpJ/GGw3/AXu5czpgogfsJMA0GCSqGSIb3DQEBBQUAA4IBAQB9
U7sG/M/w7eXBQh5tDOZ7XLCRmhrmGk9+1RdAP54SmMzc1nnglmfgl13ncaizPleu0p841a51XCY
qQMJbry47YkEnq48ImiAjEpkbaCZsZhX06uUpA9DlstEW/wBZzSCUoGsklbBolwTWAP97B7trizP
e102hNvD5IMaXrMqaH9hQcoYmKyJHBQmxW2bXxYjeXvIDcAQvevLP8IIOLqdib029GFcM7U889Fa
BcO4cPxx4kITXC2hAvdiZwGuDVAz15ByI8RAfNWrlmv+lBRSQpAecnLYozJYyRNcFPrYLd9aXbej
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:A8:1B:AC:97:64:F2:28:8E:AD:C5:0D:D8:5
0:29:35: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:B
E: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-----
MIIDuDCCAqCgAwIBAgIEPJilyDANBgkqhkiG9w0BAQUFADB8MRgwFgYJKoZIhvcNAQkBFglwa2lA
c2suZWUxCzAJBgNVBAYTAkVFMSIwIAYDVQQKExlBUyBTZXJ0aWZpdHNlZXJpbWlza2Vza3VzMQ8w
DQYDVQQLEwZFU1RFSUQxCjAIBgNVBAQTATExEjAQBgNVBAMTCUVTVEVJRC1TSzAeFw0wMjAzMjAx
NTA3NTJaFw0wNTAzMjQxNTA3NTJaMGoxCzAJBgNVBAYTAkVFMQ8wDQYDVQQKEwZFU1RFSUQxDTAL
BgNVBAsTBE9DU1AxITAfBgNVBAMTGEVTVEVJRC1TSyBPQ1NQIFJFU1BPTkRFUjEjMEYBYGCSqGSIb3
DQEJARYJcGtpQHNrLmVIMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC10BeCObXZZWcDX298
WqfdI6hpi9tuSbT4L+kowTj+aWz7PDsFpKQWqhxCdlicu67xCT0zAAjaK6x9cwasildre++IkscR
i00w20G5nTPocxpwGTHqwHx4ED7cceK4t4pbj/zB8f1uVNVii8ouG9ZEhH76j/lcx0X27Sq5AS0C
wwIDAQABo4HIXMIHUMBMGA1UdJQQMMAoGCCsGAQUFBwMJMBIGCSsGBAUFBzABBQQFMAMEATAwgYkG
A1UdIwSBgTB/gBR4F7UF+bNYzVmM3mdeRAZMdYZpXaFhpF8wXTEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVIMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1cEQ
MA4GA1UEAxMHSnV1cil TS4IEPERcgjAdBgNVHQ4EEgQUzpYj2gwIDYK9ahyGyKa0AkK5ys0wDQYJ
KoZIhvcNAQEFBQADggEBADrq0tGkwsrddEqUbsOpXi75Xs4GVkOysеysNqZZCvLqCF7qTSMiC+fz
RxQbXQDhuOT7QQvi3JAoA5zTlm2RvIO1fmrVnJ6CsObjxxvXicSLJ+blCG4uQYgEA+duDRgIClpmt
CCjtmxb+2cSJLGioaKiwn0YwgeEowOgjDMh2o4otm6FjtyT1GZsZm56U7WkFa7tSwkHKw427iZU
WVrED6W9AfATY14rNnAk8Jgz06w4rPnGE4kYjO+UqMLmFU2KImdrTp1O7b4YLCVlxH/e/He8r7FS
gzXSG4EqID/TMEdCLu7DSWR3SEgJPvKWCpNWzv2DRldHp+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-----
MIIDXTCCAkWgAwIBAgIEPolzuzANBgkqhkiG9w0BAQUFADCBjjEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2tlczEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwIL
TEFTTUzMtU0swHhcNMDMwNDAxMTExMDUxWhcNMDYwNDA1MTAxMDUxWjB9MQswCQYDVQQGEwJFRTEi
MCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEhMB8GA1UE
AxMYS0xBU1MzLVNLIE9DU1AgUkVTUE9OREVSMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUuwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGIAoGBALXQF4f5tdllZwNfb3xap93XqGmL225JtPgv6SjBOP5p
bPs8OwWkpBaqHEJ2WJy7rvEJPTMACNorrH1zBqylh2t774iSsxGLTTDbQhmdM+hzGnAZMerAfHgQ
Ptxo4ri3iluP/MHwWW5U1WKLyi4b1kSEfvqP8hzHRfbtKrkBLQLDAgMBAAGjVzBVMBMGA1UdJQQM
MAoGCCsGAQUFBwMJMB8GA1UdIwQYMBaAFOU/DJ1xPW+8Gb+a9G6/Cf5A652WMB0GA1UdDgQWBBTO
liPaDCUNgr1qHIbIprQCQrnKzTANBgkqhkiG9w0BAQUFAAOCAQEAd/8FCyPC9zXxcAZN67KCNU4+
XNJ8e+LmG602IBe+iS7Pw4pOgMKcbgULKh1IEBHQ2K7FSUWMZdPWkDIfaKVRh646yVbFZbIEmKNq4
LhRf13/hoUdrG5uRVmCsV03WSfgfUVfb1cZ8tDMIwCnsNXu22k9wykeHallpUmGUIbVZyggfKE2
NVQpm2FULiKWBFKXqbMtW5R3xmDS3bjrAIAdUdYhxhfdlCHCphsQf/FJlxb8UFOUa8SeRNr5eL7s8
znLnrC5pKPpWGbUNSlrhLJZHlcXfwbOamae6UVvjto6bMqRe2sxCsMA0dGz+tMiglfmTVlnxpEKB
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:01:01:05:00:03:81:8D: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:F0:59:6:E: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-----
MIIDXTCCAkWgAwIBAgIERCKLGDANBgkqhkiG9w0BAQUFADCBijEYMBYGCSqGSIb3DQEJARYJcGtp
QHNrLmVIMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDYwMzIzMTE0ODQwWhcNMDkwMzI3MTE00DQwWjB9MQswCQYDVQQGEwJFRTEi
MCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czENMAsGA1UECxMET0NTUDEhMB8GA1UE
AxMYS0xBU1MzLVNLIE9DU1AgUkVTUE9OREVSMRgwFgYJKoZIhvcNAQkBFglwa2lAc2suZWUwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKKTI8Acx0Gva9eeeBkM3fGTiNOEvjj2McN3tOJBMAEv
G/G7Npu0/2fAEKFFUv4NnPyH3MiC7s6R8PtPMhV5GBG6kWVztL/gQnlIjAbo1l654+jApIQjT3vd
VZDIYyS6lKlYoAdG40CgLlVtRihargQ77azlfORkyRfhKZcSQe8tAgMBAAGjVzBVMBMGA1UdJQQM
MAoGCCsGAQUFBwMIMB8GA1UdIwQYMBaAFOU/DJ1xPW+8Gb+a9G6/Cf5A652WMB0GA1UdDgQWBBQU
QsudE6pYaIJSuWurylGltfy52DANBgkqhkiG9w0BAQUFAAOCAQEAV+Vu+qzrHe7HDjMHq9DdOQfz
833QcMRY0huSgphMOgqNjqjPqTNpHPgNvE6HKGdQ0+VWr8IyRWcxnPMZNihmaCGMpFMpYuH0fx9n
sjXDbjat8MfGuX2m1EADGOwjtjMuoYTEGEUe3MBeFkmPFDIYpeuS+I4Qv34tOsGvFOpsDkobSATq
4EFw/5hI9WWaEMYkmBXdeokoVjbNpt+gtdGKNBU42AIxLrcc+YzAE1hj5qH99/hl0X6r63pTjUb
1ZMRjGQg7EL wmddms7wB5LKKi5kbfmag5hBtDKGs2s0xW1be4yINOrT9lqUYuPn9IwcHNg1lS42m
YVCbV97TltSvw==
-----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:3 E: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
QHNrLmVlMQswCQYDVQQGEwJFRTEiMCAGA1UEChMZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2tlczEh
MB8GA1UECxMYU2VydGlmaXRzZWVyaW1pc3RlZW51c2VkMQowCAYDVQQFEwExMRIwEAYDVQQDEwlL
TEFTUzMtU0swHhcNMDgxMDI4MDkzMzAzWhcNMTExMTAyMDgzMzAzWjCBlTELMAkGA1UEBhMCRUUx
IjAgBgNVBAoTGUFTIFNlcnRpZml0c2VlcmltaXNrZXNrdXMxITAfBgNVBAsTGFNlcnRpZml0c2Vl
cmltaXN0ZWVudXNlZDElMCMGA1UEAxMcU0sgUHJveHkgT0NTUCBSZXNwb25kZXIgMjAwODEYMBYG
CSqGSIb3DQEJARYJcGtpQHNrLmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnquv
UBkU+6dYowkCx7vTDH1S1znuqBusl2TyKl6txQ3YUCk1qXbAWdEjD2uwXy7lo+7eDjtlK4opiSll
VW6lPC3qArSutBzN9BKE7tE4KPty5tyXn7qMM9dKHjvOZrXSGHi0nlUQI6JlMGEhF8D9Ql8xiPoF
iASEW5FDEQGAAXnLlQlfVfxJyj8ZByFrgSvlL1SEe9c7+++DQ5V8tGoF/uAYEFEs8w6wMiaZd/4L
RRqqzvLAUF/4zRWdY2T7SnsTxfMDyzebaK9N1I8lghTlnLs0V5X00mBnDeJosl7V1tXaAEhamAa+
qXBDdygocyze0wFPbn5ZaYpUywcWLbnjKwIDAQABo4HdMIHaMA4GA1UdDwEB/wQEAwIHgDATBgNV
HSUEDDAKBggrBgEFBQcDCTBoBgNVHSAEYTBfMF0GCisGAQQBzh8EAQIwTzAlBggrBgEFBQcCAjAZ
GhdTSyB0aW1lIHN0YW1waW5nIHBvbGljeTAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5zay5lZS9h
amF0ZW1weWwzWwwHwYDVR0jBBgwFoAU5T8MnXE9b7wZv5r0br8J/kDmzYwHQYDVR0OBBYEFCRXW4Fm
pJ/GGw3/AXu5czpgogbJMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQEFBQADggEBALnuqrbcM13+ISq6
lzIbwaHr6Om2zAialZcAAU0t++lqs1lLTSA/cXoRuUlcjJ54Csh9pVPt3J76193H57/Ck/xKE+Yh
pHKFTdD3tPtgAU0prOhviVq7Gh5MR+sMNX2TKaWTj0qd8Ygeus4MB5uWSUWYCNIKnmgoZbV+Zt0A
yBHQVG9oRhqcEfK1iPUJw/sjkDUdghUHNUTcXpXfIPWCEvhQz+BX3TRNkR4NREvAwT/tHVtweJi+
mr7RPrbtvdYBjdTppFwZVZDpGC34AM6KtL+mpVeGkK73h5V/pDvQ1rmLQn2L2GJe6n9ztghE/BB5
zYJ1bWACaoJh5lEm+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:A8:1B:AC:97:64:F2:28:8E:AD:C5:0D:D8:5
0:29:35: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:F4:52:60:67:0D:E2:68:B0:8E:D5:D6:D5:DA:00:48:5A:98:06:B
E: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:
4876566507148265966307491874920824 8665

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIQJK/s6xJo0AJUF/eG7W8BWTANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEaMBgGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE0
MDkxNjA4NDAzOFoXDTE5MDkxNjA4NDAzOFowYzELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNl
cnRpZml0c2VlcmltaXNrZXNrdXMxDDAKBgNVBAsMA1RTQTEiMCAGA1UEAwwZU0sgVElNRVNUQU1Q
SU5HIEFVVEhPUklUWTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJPa/dQKemSKCNSw
lMUp9YKQY6zQOfs9vgUnbzTRHCRBRdsabZYknxTI4DqQ5+JPgw8MTkDvb6nfDZGd15t4oY4tHXXo
CfRrbMjJ9+DV+M7bd+vrBI8vi7DBCM59/VAjxBAuZ9P7Tsg8o8BrVqqB9c0ezlSCtFg8X0x2ET3Z
BtZ49UARh/XP0Tl7eRk/DtSLYauxJDPzXVEZmSJCTybclox93u8F5/o8GySbD5GYMhflOJgXmul/
Vz7eR0d5SxCMvJIReP7WfiJYaUjLYqL2wjFQe/nUItcGCn2KtqGCyH7vl+Xzefeat6Xjc8ebTgan2
FJ0UH0mHv98IWADKuTI2fXcCAwEAAaOBgjCBpzAOBgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwgwHQYDVR0OBBYEFLGwvfimoGkWbCDlUftc9DBic1cnMB8GA1UdIwQYMBaAFBLy
Wj7qVhy/zQas8fIElyaILIBSZMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly93d3cuc2suZWUvcmVw
b3NpdG9yeS9jcmxzL2VlY2NyY2EuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQCopcU932wVPD6eed+s
DBht4zt+kMfPPFXv1pIX0RgbizaKvHWU4oHpRH8zcgo/gpotRLlLhZbHtu94pLFN6cnpiyHNwevkm
UyvrB8WylONR1Yhwb4dLS8pBGGFR6eRdhGzoKAUF4B4dloXOj4p26q1yYULF5ZkZHxhQFNi5uxak9
tgCFIGtzXumjL5jBmtWeDTGE4YSa34pzDXjz8VAjPJ9sVuOmK2E0gyWxUTLXF9YevrWzRLzVFqw+
qewBV2l4ot/6miZOOT2wlA/meL7zr3hnfo7KSJQmMNUjZ6lh6RBlVvYI0t+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:6 7: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: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:F7:9 A: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:09:8 1: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
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2tlc2EoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTE5
MDEwMTIxMDAwMFoXDTI0MDEwMTIxMDAwMFowejENMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV
VEhPUklUWSAyMDE5MRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNNBMRswGQYD
VQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAqfl9D1lK8LveyTb3tlOJZfc0J+W3uG7czOZuQKigwkxq2JXrqndigVtSZWzN
noO+somaNgXqw0lpu+8P0NdUw+y1a4znJntvf7HK4WNrHO94DcrcxlJRdRkxRH/e3/0SE1FpX8B9
6IgyjeQj9Y3tgHYAfSMo0Sj2ANYcrNpF59NW/0nBzJ5QvXD80N1ybvVu4NALKFxTOEHPRmdFdpt
NNEaipwHyI.waSDpXCinXxBz6zV/jfsMYCxNl0cXlx+mkD97semLhGB27rmI8qEPM6Tue0iGp1Tb6
hIFdEQF2gZ8VPOsyJl3cpQd5GRkT63bOtHUm54TYCfw/P7NhO7pFLwIDAQABo4GcMIGZMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUnUvt/uXDNtWuqmMv
TSBvDyrTJxYwHwYDVR0jBBgwFoAUEvJaPupWHL/NBgzx8SXJqUvUFJkwLwYIKwYBBQUHAQEEIzAh
MB8GCCsGAQUFBzaBhhNodHRwOi8vYWlhLnNrLmVlVl0.0NBMA0GCSqGSIb3DQEBCwUAA4IBAQApC2BN
nwqlgm3KsBMbp0lWw2uGVzUXiu4Cfsol6290Jzn6UftA3HjOG33vg5DI3SV9Z97AfiqgbE4A9Czms
8vcHwtNRLIaAHuRVm6C/GWa4+nuzNFoAK1pjjBGoPWvfYhud/bAlbYY1qF6nHA50/tFT0GGixrnm
l9Ys20tuXM9pQaoO0YnoCvw8cvMlt68WqIEST+OoCZjpgdQRZ5lEJTmvE+LLBDuE87orGfxxswsy
+jnOfHX8MLBOhWgIrJ7RrXLNdKXOlbvhcU3vXl89gKtWWfr+OdVGdJc+/A3wdtTFhNdy7Ce0VliZ
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:12:13:51:6:9:5F: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:83:40:2C: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:3:2:26:5D: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:F7:77:5 8:33:07:54*

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 (granted): 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:	*1305472721370662516964525194522253092462*
X509 Certificate	-----BEGIN CERTIFICATE----- MIIEFjCCAv6gAwIBAgIQYjZ9dFrZQ6tdpFC5Xj/6bjANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDT15 MTIzMTIyMDAwMFoXDTI0MTIzMTIyMDAwMFowejEnMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV VEhPUklUWSAyMDIwMRcwFQYDVQRhDA5OVEJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD VQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAxdOHoO/xEAXVYd6m64QhKHoNZhT5L+wEkO59DH4K8lW1r/kEJusfY60zDY8 o9s96HYACcQOR9Yltg3T3neqRZJ5GEPt5uFzCWzuSdyxIWMacxu/sSYaln4bqbCd97ML4qVdvwPG LNGRu8Utuy0JvhyuoBICHUcgyw1O2ATlc+9SzdbGvKq15gazGXTpVUYgLplnkChp1ojZCvWFdKN 3dNGB5tqn3xsdfUfGDWxe4gLFFLeXjxo0pT2Y+5hJF1+r+PllZRnu1LKXEcrHxeyyZ+KL6wSLUyv fxZ++5hd0wR1pCnVgZ+hfYaGZ+YGRJXtiIA8DFqeKZ6qAhA8a6v99QIDAQABo4GcMIGZMA4GA1Ud DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUqD4KKP6RKqGdYfXN lT35pc1GkjEwHwYDVR0jBBgwFoAUEvJaPupWHL/NBqzx8SXJqUvUFJkwLwYIKwYBBQUHAQEElzAh MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMA0GCSqGSIb3DQEBCwUAA4IBAQAJ06Qp /kiOhcNbEsDUVGfLaVycKjEbrGGMWnAj18S08aWx7ijXtDD9mY5CxtRUl9IbjB/eyl/Rt8RDVURt IioiNckkxC/bOHxiCj2WNCvRxo8GT/qn4M1vV/Sy8vwx/ZIYsZrlRnuo7/dqPsQyxIgRGbUp12bV KO4KQb4DNOcA6KDwcPd2zv4nBT/4XW7qD07spW9LPVKEvstOU1MV1tzmjD0lC5ZL67FdB8kKEJCbb N6jVLVBOYjBopct5qzTLLPB5LTmV8l281XzTEqeFxbFy+wo7VOT6K36OYSd+9CnPn2M/l6VfrSCi 3OvaWcq+lggGR1kQzDsS4lN1JoyZqd39 -----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: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:D3:46:07:9B:6A:9F:7C:6C:75:F5:1F:18:35:B1:7B:88:0B:14:52:DE:3E:3C:68:D2:94:F6:63:EE:61:24:5D: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/granted

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

Status Starting Time

2019-12-03T22:00:00Z

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/*

1.28 - 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:	*142168993972586756930521877712410666755*

X509 Certificate	
	-----BEGIN CERTIFICATE-----
	MIIEWjCCA0KgAwIBAgIQCrJTQgwdM4hfdZRtSgVwszANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTIw MTIzMTIyMDAwMVoXDTI1MTIzMTIyMDAwMVowcjEnMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV VEhPUklUWSAyMDIxMRcwFQYDVQQRhDA5OVFJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD VQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAwmZuFcXZ3UGPjIEX0mldGSTiUxMcfG8Fh0f4VlAg6aN/buuRVaEpwrS7UfTD /HF7JojcJidFf7wTBd+B52oqYhya7rT/d11exeDtwIZpymksqC+F8bWoleJ3HkSByyGfuGcGGSno waCjcZqTT2YCT40PdJJPlaUqobjNC9dFP/FOzgHWu8hUiOAixZ+X22r0CVgTnNW0/xiaRPq/Pg pgDAsxIYDABonFKiCEHyk5T1rjV585lfwWBcPo5jnl9tIyT3ISB06QZ0i4rmFcPli/0XvyHrGNN pJNPJ9lb9d0VbcPwktoDr2nBFqBzpjRufwVPjQCBuDVidkuMEjLOTwIDAQABo4HgMIHdMA4GA1Ud DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUEDIBfAAH5r+iCV+i rQKE3Tk2/h8wHwYDVR0jBBgwFoAUEvJaPupWHL/NBqzx8SXJqUvUFJkwcwYIKwYBBQUHAQEEZzBl MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMEIGCCsGAQUFBzAChjZodHRwOi8vYy5z ay5lZS9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlci5jcnQwDQYJKoZIhvcNAQEL BQADggEBACnGDxtyt0EmeLyGhwW0l/rg6q9KStXW65qwNnTdW7QpY+3Q8Oc64zIAAOAkfcaSa1Bq IJmO7QMkSnpeEa5AH//48bdfZ0RYRGnEpoqq6L5Qt6iCHBduRDxrca0bR7s/UaIB9PMR6jNU7Y4h SlAZCTxZvsuOwgbYzU1kJlpc5mb4nSDU3qyL7vPeIgQAgLMOhMI78ZFSHGxGJf+BNOaHzD4IYBRd 81Facnr5+hfD2gNFPcuf9DPFVinKUG9c4XuKj6V30fGBBZoSfju53Jk6/aGfKwKWLpN13Sb4RMb+ 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:B8:67:06:19:2 9: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:0 0:68:9C: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:A F: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: *9341197341178141782522153967405961574*

X509 Certificate	

-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgIQBwcMIj8ecuJhcR6JfOMRZjANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYJcGtpQHNrLmVlMB4XDTIx
MTIzMTIyMDAwMVoXDTI3MTIzMTIyMDAwMVowcjEnMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV
VEhPUklUWSAyMDIyMRcwFQYDVQRhDA5OVEjFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD
VQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAlgz0fx7rjs9QCiaFmkHHIuLWTxxJCBGzK/SB9tEYpSfK0++TnOOby6de2cDf
nmin3Yk3F840xLM4gms8M4Fu/MOVG17Alv0vua4ygRmhH7O2dWM8ITyi+8sRuyeQC4o9+LS9aCzE
SZUKyYIf/KsM4DYQIE254mzU8YodMqoHPwsp4gAev+1zP2bdzQfQBbO9+cviCpzBjcEtHJquQH6W
7walBOMhrXMQBIOuj6qVkKUbvDN1spQcmLWGY1NooF2IQyCPyzLSxa1tlivhHNb3edLCRuklZwo
1yco6T/yJHxIwH36hX6AJ/s1btXYg+GRL602Rk7VBzTc30dhPLZIPwIDAQABo4HgMIHdMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUsnUQr3QDIUM34ksg
HzFY59QFNQcwHwYDVR0jBBgwFoAUEvJaPupWHL/NBqzx8SXJqUvUFJkwcwYIKwYBBQUHAQEEZzBl
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMEIGCCsGAQUFBzAChjZodHRwOi8vYy5z
ay5lZS9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlci5jcnQwDQYJKoZIhvcNAQEL
BQADggEBABInW9utp6qGo1QB57aGQ3tKST+f9aFmceDMZ+w0XGuQ+W/m4YKnVDmb0O8a+TykHaQn
wD7obf6hA8zV3NXFAW6JmLiy4wycnJwKPS3qmZ42dPANtlq3upvgPzMhbCzGaXxRZZrfb4ikZGSP
Jreer6Sgymv4wZku21ComlxFY52sQQdB2C43/cQwur9Xgx/XWoiS+ZSrNrU0RUu0b4YN5pM6WcGx
gcNOqul7vtkWS060QgmWss0l2n9rgfd+RVzjiKAr/364DCR++VCWcUj0uiCgmpo5o/NHUcy0BTX6
dTgOOcFAxLwQR4uOmAPEFPpKhXoPRfZLSo1yBW8cO3EemxU=
-----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:E F:93:9C:E3:9B:CB:A7:5E:D9:0D:F9E: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:8F: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:8 5:7E: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: *6720593471054379822270414603408987 3665*

X509 Certificate	-----BEGIN CERTIFICATE-----

MIIEWjCCA0KgAwIBAgIQMo9kZ98qZ1djdKF45mVRATANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQG
EwJFRTEiMCAGA1UECgwZQVMgU2VydGlmaXRzZWVyaW1pc2tlc2t1czEoMCYGA1UEAwwfRUUgQ2Vy
dGlmaWNhdGlvbiBDZW50cmUgUm9vdCBDQTEYMBYGCSqGSIb3DQEJARYcGtpQHNrLmVlMB4XDTIy
MTIzMTIyMDAwMVoXDTI4MTIzMTIyMDAwMVowejEnMCUGA1UEAwweU0sgVElNRVNUQU1QSU5HIEFV
VEhPUklUWSAyMDIzMRcwFQYDVQRbDA5OVFJFRS0xMDc0NzAxMzEMMAoGA1UECwwDVFNBMRswGQYD
VQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAnefs1HxAHAVoc7labGuHXp4IrX1cC9hDa/lidDrodPiFF6y+8EAQEzP22Lkr
rxPVybrep3kodxFj4aVw4i6Q3c8EYyLE1gbbtrB4vTxeQIB2f2HGZ56Hr3uNj8JD+/iFvCe/5iAE
so8dRVSX48kRRe8viAw6fniiXb+8iyfI8y0VIcfSveNLiQXkYNB+TxQ0f/5+PCTlFez4pIzw8p0Z
SIddUzldx2beyspNhAiju1cgy/bMULscv8j7YbFKZ4TmsUZHZuQc59MjaJjderlwtV/tLBrg3OqR
5nDq1Oi+aukjMNQX3F576yXlPnwtc2l3+0GrEGYst9yfpQk8c0xdcwIDAQABo4HgMIHdMA4GA1Ud
DwEB/wQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAdBgNVHQ4EFgQUuTR73sWfYH5L+mH3
/RD0UAlC7egwHwYDVR0jBBgwFoAUEvJaPupWHL/NBqzx8SXJqUvUFJkwcwYIKwYBBQUHAQEEZzBl
MB8GCCsGAQUFBzABhhNodHRwOi8vYWlhLnNrLmVlL0NBMEIGCCsGAQUFBzAChjZodHRwOi8vYy5z
ay5lZS9FRV9DZXJ0aWZpY2F0aW9uX0NlbnRyZV9Sb290X0NBLmRlci5jcnQwDQYJKoZIhvcNAQEL
BQADggEBACQXxeUVbmlei5NlN3f7lv426xyTHXlxaxTb3T6MrLmVOBtCxa99jqKTG6Ljz1N6m/w
E3GSnLVDL5Q77FqhJRasiyl3lJUjz82n0GL4L+C1JiW+n5dy6nUJUnSDHZhhD3LfnHxWLLfyRyWm
DltXVHbU/6Sgn2syAUrZ/alzuiY++iX0yoWYaMKhgfyz848r+nh+sK2pVp5rVT57D7x5+xFWDeyLQ
jhe9HImXyGCyvyiSChg+3cV+oQUY6VeMWS40+8E+rAHtxgvhN3YiSDGvOdNct6whea+daYyuJqu4
emGCDHKa63iPSXhuD2c/AhiqSesCuRsRCEVNr/iLC5ll37Q=

-----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:DB:8F:AF:13:D5:C9:BA:DB:AF:1A: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:8D: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:8B: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:D C: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-----

MIIDjzCCAxWgAwIBAgIQfwlWDTXOBgXEqiABoa6ncTAKBggqhkjOPQQDAjBdMRgwFgYDVQQDDA9T
SyBUU0EgQ0EgMjAyM0UxFzAVBgNVBAcMDk5L5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBT
b2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTIzMTAwMTExMzE1OFoXDTMwMDQwMTExMzE1N1ow
aDEjMCEGA1UEAwwaU0sgVElNRVNUQU1QSU5HIFVOSVQgMjAyNEUxFzAVBgNVBGEMDk5L5UUkVFLTEw
NzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAE6ie8TjQ1MsNdMX7X2fCAkHYLZZH24It4pSa4rxsKEvobnpZ1r6kk
Z8jdEAS2+06sr6cRvDKAFbCEs0ZStuBf6KOCAaowggGmMB8GA1UdIwQYMBaAFFoYwDTO17eZ3wiQ
wAR9GPNzlr3PMGYGCCsGAQUFBwEBBFowWDAzBggrBgEFBQcwAoYnaHR0cHM6Ly9jLnNrLmVll.1NL
X1RTQV9DQV8yMDIzRS5kZXIuY3J0MCEGCCsGAQUFBzABhhVodHRwOi8vb2NzcC5zay5lZS90c2Ew
gZ4GA1UdIASBjCBkzCBkAYGBACPegECMIGFMDsGCCsGAQUFBwIBFi9odHRwczovL3d3dy5za2lk
c29sdXRpb25zLmV1L2VuL3JlcG9zaXRvcnkvdHNhL.zBGBggrBgEFBQcCAjA6DDhUU1UgY2VydGlm
aWNhdGUgaGFzIGJlZW4gaXNzdWVkIGFjY29yZGluZyB0byBOQ1ArIHBvbGljeTAWBgNVHSUBAf8E
DDAKBggrBgEFBQcDCDAzBgNVHR8ELDAqMCigJqAkhiJodHRwOi8vYy5zay5lZS9zai190c2FfY2Ff
MjAyM2UiuY3JsMB0GA1UdDgQWBBT05pTRiTTkkODyNnyZ/56xX8UKUzAOBgNVHQ8BAf8EBAMCBsAw
CgYIKoZIzj0EAwIDaAAwZQIwGOjwcHvgTdwZcargDFJnao48XZJ6Qpo1rPOzFhpOXuB4TFweq0/
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: | | *721010654334666381752043073453 81995791* |

X509 Certificate	-----BEGIN CERTIFICATE----- MIIG+zCCBOOgAwIBAgIQNj4o++yE3RYvac/tiJs1DzANBgkqhkiG9w0BAQwFADBdMRgwFgYDVQQD DA9TSyBUU0EgQ0EgMjAyM1IxFzAVBgNVBGEMDk5UUkVFLTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJ RCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMB4XDTIzMTAwMTExMzEzMDJaFw0zMDA0MDEwMTEzMzMw MVowaDEjMCEGA1UEAwwaU0sgVElNRVNUQU1QSU5HIFVOSVQgMjAyNFIxFzAVBgNVBGEMDk5UUkVF LTEwNzQ3MDEzMRswGQYDVQQKDBJTSyBJRCBTb2x1dGlvbnMgQVMxCzAJBgNVBAYTAkVFMIIICIjAN BgkqhkiG9w0BAQEFAAOCAg8AMIICgKCAgEAoon1wQAzSATQU8rFn8Fn+2Bt+I6YJyW7KmHGRVMN hIAA2A3w4Xr7XAfpMRIGiCQZaENUJOz2ENN5YwJufcnMB8Bgh5Gigm6n4UbjgW4XAFJuzuD33mRY t7U2FS28YtibgJVXM8oelXFISdTYm2WnkNhKAwMgG+QPyiM2RiAgQj/ImKGUNXDBIzmWc8oAPu+f 7YHwIWCmg+dikH3oaxNNLCMldMAy1oIBK0ZfqnbOFZ4eqPSht2LvMmmlW7AixHWI+/iG/L9RGXju nIiHcHvBUYGR7L9pzI2GLWFw8b9HV4QEZXt7HWVPsTu6xb733x/+5JJbkyjLUO2TQ2/JscmF9IZp RqCNoX+gNgRkVE+qlbbc16xSVA+W8Zc+LAGSPyxjDfDWLusShB3CNuRECUCcleMr/42ueDN58YS jOVGzhoAk0oiYSngnqtbgJYWwQb5NcYcB56EioXusMxn0SFHyTsRudpJ2lmM9PREW52LGTLm0/Vw WMsB+FPqN/HXLOmYmdJA5zEfU3oEzxnkPsdazb53PARxgCZKpoRPNBHqLJ1oMTakZvDuT/ubGgsR jJLwNqQxIZ2bguPb9d9dwsYyxYWc85La0mRdH/VHrduGYfA/fTMrPGCn+XXnJUx1Z8gvh5AK7p1N KnJnJyhEBuaEDmFl0RyJh5jY5P/+ID+A9sUCAwEAAaOCAaowggGmMB8GA1UdIwQYMBaAFP25tFTt uXdg0bHtJiWEEhVKcpIZMGYGCCsGAQUFBwEBBFowWDAzBggrBgEFBQcwAoYnaHR0cHM6Ly9jLnNr LmVlL1NLX1RTQV9DQV8yMDIzUi5kZXIuY3J0MCEGCCsGAQUFBzzABhhVodHRwOi8vb2NzcC5zay5l ZS90c2EwgZ4GA1UdIASBljCBkzCBkAYGBACPegECMIGFMDsGCCsGAQUFBwIBFi9odHRwczovL3d3 F51kaRjAd+0wENvmoNROSHEpZ6+YlFYuzJ8bfpgl30LopxII1/0X+Hqk3shrDpz7/bXjJ+nh7S1h UKTLH1J6cS869RP7XZhzGiIgvWUuQF77ODum+tePuqgBPrvfGi9HwgdVbPKEm0tRZL/BiL5md6/ tJVW8OBe2nOA407SdK4+D1GJdEeu4CVJi9bF5ndNkwXK+EV3K8GVTb4xSMTcSccB7HaT3IbGmlWOj YdTG5dTfeAolpkeuuCcu+1DMpQxTkKdEEpmztOWgAxQ7zr9HK1oqPNgf9eJVTulLcwBK6lpqOPB0 JCVOmUPBC3lY5TcDOxnt3xrbsn58VHfIhkFsqwFmrwvnHcjVPtDMuX/iIWDu3/rp3j5imMGGi3KR Up8r8FOy3S1Yg7tF4nFCx5eFIrlbGmATekFRgxgHv/YNu2b+Ft+yWvygrdY1FJ+G4BnWBi5W30BG nY5fsTbEU9JSXj/O3WSFnJKHiBWnpu2iwk1Hl3KEk8nH8ekcEgl1M4gfY6L6xMp6jOYYmZnhYAtV ruUMS5iJmKu2/rhDCI0Y9a8eg8XKB/gEmBTJUx3L2FBD150kUvvhg2hYBF7nuDK1Q8AxGiYVs9XT ml3c4kInJM/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:E9:31:19:46:88:24:19:68:43:54:24: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:1:E:95:71:48:49:D4:DE:9B:65:A7:90:D8:4A:03:03:20:1B:E4:0F:CA:23:36:46:20:20:42:3F:C8:98: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:13:9E:1E:4A: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:FE:E4:92:5B:93:28:CB:50:ED:93:43:vdF: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:E4:4:4:09:40:9C: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: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:6:1:65: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:B 2:92: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

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*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*4201089684312876161037349692432633500*
X509 Certificate	-----BEGIN CERTIFICATE----- *MIIDxDCCAuqgAwIBAgIQH5sBlc4ZTj1hWvEFaRQX9DAKBggqhkjOPQQDAzBmMQswCQYDVQQGEwJF* *RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQQRhDA5OVFJFRS0xMDc0NzAxMzEh* *MB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIEPT1QgRzFFMB4XDTIxMTAwNDEyMTgxMloXDTM2MTAw* *NDEyMTgxMlowZzELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIElEIElFNvbHV0aW9ucyBBU1zEXMBUG* *A1UEYQwOTIRSRUUtMTA3NDcwMTMxIjAgBgNVBAMMGVNLIElEIEIFNvbHV0aW9ucyBPUkcgMjAyMUUw* *djAQBgcqhkjOPQIBBgUrgQQAIgNiAAT5UvJTY26GyX5dkIOsjGOvy4W1MFXjWgXW3q9aqT1yuEOU* *yuPnHtm/lTUiIXY5PCVviBhdqubUdP/U9bxOs6M6oTptGU9SJgQ7JYy9tK4HbpJPk+J3Iz1JHMqq3* *JCktyUWjggFaMIIBVjAfBgNVHSMEGDAWgBSGdE866zjysKtu7bmFm52DCUUxazAdBgNVHQ4EFgQU* */lnn/EN4/+wsw4Soo4DjI0ga1CgwDgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAw* *bQYIKwYBBQUHAQEEYTBfMCAGCCsGAQUFBzABhhRodHRwOi8vb2NzcC5zay5lZS9DQTA7BggrBgEF* *BQcwAoYvaHR0cDovL2Muc2suZWUvU0tfSURfU29sdXRpb25zX1JPT1RfRzFFLmRlci5jcnQwLwYD* *VR0fBCgwJjAkoCKgIIYeaHR0cDovL2Muc2suZWUvU0tfUk9PVF9HMUUuY3JsMFAGA1UdIARJMEcw* *RQYEVR0gADA9MDsGCCsGAQUFBwIBFi9odHRwczovL3d3dy5za2lkc29sdXRpb25zLmV1L2VuL3Jl* *cG9zaXRvcnkvQ1BTLzAKBggqhkjOPQQDAwOBiwAwgYcCQXQXw72bQj2lOzbDp3xy5TIFqBPQBIN0* *YbWV+TSenzGfqT6aQjHTZ9migRQeEXw97kXLSD3wN/g9LQ90k1dZvDQ3AkIAt+bOVtVzJr+43e8I* *Fl4Cot5wPywcml042EtuAT1SJ7lOkIUoaQZ6ZPj3pnI+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:35:2 2:21:76:39:3C: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

2024-02-08T05:00:41Z

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]	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		

1.34 - Service (granted): KLASS3-SK ORG 2021R

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*

Service digital identities

Certificate fields details

Version:

3

Serial Number:

104631294886120067599766131374780892342

X509 Certificate

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

MIIGszCCBJugAwIBAgIQTrdBH/kVRQFhWvLs8/TEtjANBgkqhkiG9w0BAQwFADBmMQswCQYDVQQG
EwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAx
MzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzFSMB4XDTIxMTAwNDEyMjYyMFoXDTM2
MTAwNDEyMjYyMFowZzELMAkGA1UEBhMCRUUxGzAZBgNVBAoMElNLIElEIFNvbHV0aW9ucyBBUzEX
MBUGA1UEYQwOTlRSRUUtMTA3NDcwMTMxIjAgBgNVBAMMGVNLIElEIFNvbHV0aW9ucyBPUkcgMjAy
MVIwggIhMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCv5c8Zz+xsh2xEQ3R4grFpZjzzJuRk
HXs0xhVHNhJG8WZh6NldtLBHJPVT1PD8au9ism51NJMrstdbuYVBuoGXIBf+1/lg0M4KaLEOb1w
gz/BXhBgRDMXjGdqlv24MnPx5Il0qTb2G7pBauksvTIOKWncM1CvcBA46zWjXHRGNv87BJcACaaU
9/DA4hZZ1/my0Z+d+Fdh2YNCqfXWEJ8Sz3UVO16QMas2g8mL5vsp0Viy4HAX5Gw+XwUmU+HKqdt
H8iW0zjTdUafOPdrbt0f1ivIi9Ft29CpBXxUPdgC798VnK3jsaUwGwlKbXf7coT+6ulGSvERGCe
WQ9yLfoswAieqDZ7Zp7iDG6CTMvMfh+dTdHqmkIWG2JYcFW9QVoCyQKTjvZfxtO1xAcVavvgXa+v
aXX8EsyQqnYF7Zkp5PzB5/x9jmX70HBHEPc1CLarxYpMLLPc3FqtMiX2wVqv5HttKuE8Q6xqmcQW
Mbj5l1xHBrMOD51ahOs3W9bq6NT/BsHvzZ+fSFcjRjb4Jq7OFN/ymA0hD4+rbrxgpkJ3w1iA2mL
yPT5BfwL2fEGMxtWxFj7y2ETzXN/mW34+CgvJcQHRYeXs9bvg1iXiRyTCZA0Mkw8Z8E56PvXbNn
hH6AOMg7S1YQ7yXFXzESEJaJ7mBZl5jPg4t/FThzPHnwwwIDAQABo4IBWjCCAVYwHwYDVR0jBBgw
FoAUlQ23ZBjCpptmdtj8/JpaJLwo1s0wHQYDVR0OBBYEFOLGphjgoLJ8oWgse1E8b2HyKY2MA4G
A1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMG0GCCsGAQUFBwEBBGEwXzAgBggrBgEF
BQcwAYYUaHR0cDovL29jc3Auc2suZWUvQ0EwOwYIKwYBBQUHMAKGL2h0dHA6Ly9jLnNrLmVlL1NL
X0lEX1NvbHV0aW9uc19ST09UX0cxUi5kZXIuY3J0MC8GA1UdHwQoMCYwJKAioCCGHmh0dHA6Ly9j
LnNrLmVlL1NLX1JPT1RfRzFSLmNybDBQBgNVHSAESTBHMEUGBFUdlAAwPTA7BggrBgEFBQcCARYv
aHR0cHM6L29.3d3cuc2tpZHNvbHV0aW9ucy5ldS9lbi9yZXBvc2l0b3J5L0NQUy8wDQYJKoZIhvcN
AQEMBQADggIBACtdi7QO74rBXo+wQnChGnhtpWZSdlSgqMKtBbO3hAvy7s27odXThZi9fLPEpqw9
ClSNSeGz6e5HGc258o4kYzhymMLF7Hync2S5OVvf325XMtXOR23MGC4Yn1ogZXNPlaZULvty/1Uz
SLbjdGDnkfdHWTEPJPskXHS1CM70ZM2wGtfAjPRW90wThSZAh6CS/KNlJTTOjYMDYknQPTESiUV3
3YiB7xL5wV/9ymoM03IvZ0ew0ktY1YNsfr4eb3FfcFmCiXMRmPYbdncxBvyzLXxHoZtZJq2y3SHp
Pb1lqWv+LQC6+c3YcEYYyzNVwCgpdOpvr3QU6imr2H8elcKCe5unD+gJFZC4+ITcF56RLQ/uzddw
ez+QYjWylg9ZEwfvZZOqoWzvhxNlgr2yUs8cPV6rK3I+STVvS4Bgwsg5OlVrbddwIlNHDVHbO3b6z
SkjqUhYcAHWCHzptbjtl5GOVs/55m2/knlrxl8MuDXPl5h2PosaVqO7dI+2Sl/rpDTwyPlfnwdV8
vKS6m81yc7H2pn29EspMBTE6/dRoaq2q0B17lt9ojuhkEus8QCbuFWs0avUnmDALqZq2qBg878WF
SEIxS87EJ6X/zFm9kf/u+4aCN9hul2YzqQ/saFpWsvg083GHz1gNiikXYeUwygZmqqQj8tbX+thc
E+XU/HSLWIHR

-----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:75:15:3B:5E:90:31:A B: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:C 0:6C: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:6 A:99:C4:16:31:B8:E5:57:C5:47:06:B3:0E:0F:9D:5A:84:EB:37:5B:D6:EA:E8:D4:FF:06:C1:EF:27:C0:9F:48:57:23:46:38:7E:36:AE:CE:14:DF:F2:98:0D:21:0F:8F:A8:6E: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	*2024-02-08T05:00:37Z*

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]*	*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 |

1.35 - Service (granted): EID-SK-Q 2021E

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

Service digital identities

Certificate fields details

Version:	3
Serial Number:	161893725775996041986690601031977427171

Public Key:

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIDizCCAuygAwIBAgIQecuY8QtISqphWu7gl1Bg4zAKBggqhkjOPQQDAzBmMQswCQYDVQQGEwJF
RTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRhDA5OVFJFRS0xMDc0NzAxMzEh
MB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzFFMB4XDTIxMTAwNDEyMDkwNFoXDTM2MTAw
NDEyMDkwNFowaTELMAkGA1UEBhMCRUUxGzAZBgNVBAoMElNLIElElEIFNvbHV0aW9ucyBBUzEXMBUG
A1UEYQwOTlRSRUUtMTA3NDcwMTMxJDAiBgNVBAMMG1NLIElElEIFNvbHV0aW9ucyBFSUQtUSAyMDIx
RTB2MBAGByqGSM49AgEGBSuBBAAiA2IABARd6setRXHlBuFzkZJwxhF6JYTAU79CcQhtICvctME5
AaGKUGblox+ssIrWmh5mCkbpyWJmsiqYhn3qyKmfmCdmjB09rOdKwz522D1m+UWFDQnwKVD/LBFi
fq2WMJQOj6OCAVowggFWMB8GA1UdIwQYMBaAFIZ0TzrrOPKwp+7tuYWbnYMJRTFrMB0GA1UdDgQW
BBTolOaPYRI99x/BLk/8FI8tC4LYHDAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIB
ADBtBggrBgEFBQcBAQRhMF8wIAYIKwYBBQUHMAGGFGh0dHA6Ly9vY3NwLnNrLmVVll0NBMDsGCCsG
AQUFBzAChi9odHRwOi8vYy5zay5lZS9TS19JRF9Tb2x1dGlvbnNfUk9PVF9HMUUuuZGVyLmNydDAv
BgNVHR8EKDAmMCSgIqAghh5odHRwOi8vYy5zay5lZS9TS19ST09UX0lcxRS5jcmwwUAYDVR0gBEkw
RzBFBgRVHSAAMD0wOwYIKwYBBQUHAgEWL2h0dHBzOi8vd3d3LnNraWWRzb2x1dGlvbnMuZXUvZW4v
cmVwb3NpdG9yeS9DUFMvMvMAoGCCqGSM49BAMDA4GMADCBiAJCANcDgGx2tAky5vu1LoyXKPqe7DlW
o/kDv6GR30OSYxB4FOm9xslclKUSObuyTsSvNY8yqk8souAMMShaJbW8G49BAkIA6+WMbJjw3Wly
7ezIxciQkKV4ODVK+fUxlP6a3CJ3SbhsGOnUQ/DandSsyDuxAYzXJQD3XqzO+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:81:04:00:22:03:62:00:04:5D: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:E0:3 A: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

2024-02-08T05:00:01Z

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]*	*1.3.6.1.4.1.10015.17.2*

Description		*Certificate Policy for Qualified Smart-ID*
Policy Identifier:		
Identifier	[OIDAsURN]	*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

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*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *746484452877302363572926908628739753173*

X509 Certificate

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

MIIGtTCCBJ2gAwIBAgIQOCjEgffj3n9hWvHCGo8aFTANBgkqhkiG9w0BAQwFADBmMQswCQYDVQQG
EwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQQRhDA5OVIFRS0xMDc0NzAx
MzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1QgRzFSMB4XDTIxMTAwNDEyMjEyMloXDTM2
MTAwNDEyMjEyMlowaTELMAkGA1UEBhMCRUUxGzAZBgNVBAoMEINLIElEIFNvbHV0aW9ucyBBUzEX
MBUGA1UEYQwOTIRSRUUtMTA3NDcwMTMxJDAiBgNVBAMMG1NLIElEIEINvbHV0aW9ucyBFSUQtU0Ay
MDIxUjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMw6wtLCsUzKKXHy7e1T/8tzpQzc
ED8IhIf353+KELujxX0hdVk5SoPvv3YObSvXjbvGpaaOOMRxwQCBxFv5qQ3ZGtvc8UydBpxpKi/
VHI3CUAXmPjtj7/Cx7cH7+zT0YyE41RT2bRpsxzU2LMflckJoSO+CeBStcaSZJ23LW/MXbegtmOo
orU68fq82HIJOuFxv5NZNiQdsh03ZeDRveEBkATyp4WjCTZtlyUKSleKxzfRDAtvuZhAuI6w84bt
VtUic6K/BuN6hHxwMR8uvInIZ76a/9n2N2t7JgYx8qoaq5dte8oqpSOucr1Y8imr+3T4byRZIL3E
HK4I33q0+4ICZSjy7UbMRfpz8DeuFGFX59tnDlaOD2UlsgP/dU28i6jruQOoI6X6Z+LQ/8OGgxXT
/nhJzgROs/KrrCUl20d4jOe79PT532wVeQhWc8+ethQd0sjLEV/1tRd5SqLGIBmv/+lPRVPdIk86
kS11OP/PwKVU2kH5loaYmhzIqLTp/ir0yFjS+0T5Ocf8UuBFazomdhPHNcy6PmaOQnV7rE9ZOFiV
FiZLPfcSBmnCW9Zceq05kvljbDmJnjmYihyQwcOQr4iIn458bPPFm18gxIVVn8mJAi/8Z37wNtAD
GS2Hj4xd+LSdQTHiJDOKwlnzVGc/8HI5Cy3tixi7U8vmSMN3AgMBAAGjggFaMIIBVjAJBgNVHSME
GDAWgBSVDbdkGMKmm2Z22Pz8mlokvCjWzTAdBgNVHQ4EFgcQUpW/iikyViDntwvVH12J+c6YD1YYw
DgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwbQYIKwYBBQUHAQEEYTBfMCAGCCsG
AQUFBzaABhhRodHRwOi8vb2NzcC5zay5lZS9DQTA7BggrBgEFBQcwAoYvaHR0cDovL2Muc2suZWUv
U0tfSURfU29sdXRpb25zX1JPT1RfRzFSLmNlcj5jcnQwYVDVR0fBCgwJjAkoCKgIIYaHR0cDov
L2Muc2suZWUvU0trfLk9PVF9HMVIuY3JsMFAGA1UdIARJMEcwRQYEVR0gADA9MDsGCCsGAQUFBwlB
Fi9odHRwczovL3d3dy5za2I/zza2lkc29sdXRpb25zLmVlL1L2VuL3JlcG9zaXRvcnkvQ1BTLzANBgkqhkiG
9w0BAQwFAAOCAgEAoLWe39b3tLZIKYJEIR55D9hP2VyRQ6v9bhKKNa+DiVxvIvpgRKEu1L0Obys+
Bu3h04HtzxS+smrLKV1CK7cQn4tdMkoVEU70KXjCknza1pgl5Z4R24T2R/iakhGt6Go38m5kfGMZ
7iv3N7ooFcWrptk/PjbGNxjcC/BkNsGqrJoIpa5uHUs/8dB1PfINTod2oLZhrRGKQl63Ahwa4NCx
RIu9972Kuxgph+ARbkIUR9GzFSe7SDSXA8nGxOILN/YbD0pN+PKvyuml4eKfQEDyu2w1/+Gkqz/k
RDIrE57IHvpr5VSkmunw8BpCSDxfESt9JrEhpkO2RHcVxh6LKMW9PXrvi1phNqLctFs2jDiQCexP
f8FWW4OhIHvFqAm4Yb4ShWKN6ATe45qloQ7ee+rz25jhhWwMQ0yL1e2kx+nPLoSTqj1vnwXRYLe
ynKDAEn4brXP0KzenSGU5Ywkg0TVfM4L7mSxYrsDyr+4PYw9+RrThtGbUXHl65lKFQxVBFdcdCnc
qn/O9TXedtzxUsxMbDrgkNz9B3TF3+o0SbN/xoPR/TYvIpmXxuANPyIBSHFvQcCTXSUrzBEzp7vd
0YM+Lexde+ZuCnlihOwDezT08TnOIWA/TqB+YrBVyc6KgrQbkZ+0KhlMTLiqnua5QVW7oMEFqdFU
ILlmHvppaa+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:01:01:05:00:03:82:02:0F: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:D3:1C:84:E3:5:4:53: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:A7:85: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:C3:86:83:15: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:05:57:0 1:47: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   *2024-02-08T05:00:20Z*

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]*   *1.3.6.1.4.1.10015.17.2*

Description   *Certificate Policy for Qualified Smart-ID*

Policy Identifier:

Identifier   *[OIDAsURN]*   *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*

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
MDEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2WKqpwAceqQ1DNnslvmj7AsSFgFR4g0U3ot8aLmIVT3cJ0rVN8PaQ4zuCIGf0xTM6mp1nQRqvtES
cYkijZ9ISW44KDs4P71rC/8MYuX0NL/AwDlevmjCEkvHvqCQw7SAJ5gFkObc6FGjMcOzzVDTLc/0
g9txSaFy6A2kTQYWY2a7DhqRDVBJphGbW8ir28DmH+AGRxj5l3vs6V8W/x1xy90yWunh8b/DNbS+
29YKQ04phwPl0Ks59qvsgm1wPppsx0xf/mp9HGC574q0zq2Ec7v4PAhu2FwY2t6Hj887KTWeVDUa
RsVtwKqqDWJdmJBG/Pa96H/k9v1t5Lln8NlxHQIDAMm9MA0GCSqGSIb3DQEBCwUAA4IBAQBit30I
5IzoldRcKYbWRLPrii5nNcmdLFfOVbjjfh/BcQV4G9claNtimuaw75Kq0eVuMaD1GBzn3gNSA7UF
pCURt5xtEt/TNdO4ht+SLkVuFeW7AgRSlsJM1LiNrQei7qkPRTYfsfwT4TGFbycy6oQVkHsFx0WS
ntG1TECDxNfatS4oKJQVp9pCw99CVpt2M1smIRFIsCgeVgwP6EqB0fwHpAZGZeX42VMmvLUFdk
ujBgW8phGP5yxDWGWHkY/1+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: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:E
9:E1:F1:BF:C3:15:B4:BE:DB:D6:0A:43:4E:29:87:03:E5:D0:AB:39:F6:AB:EC:82:6D:70:3E: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:54:35:1
A:46:C5:6D:C0:AA:AA:0D:62:5D:98:90:46:FC:F6:BD:E8:7F: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
3IeYUjkf9LPKTkMUrjeOofT57NjJd+5WUmrsTRDGJsW6CWN/rM40SB4EbXdrxeKR5TXqvTc8uKB8
vb7QdQTBYAEiy8y49jL0wApQ40B2wnAj7kpyeWHwvML wqeVyAxFxcR+gytsUxdRXl60l g7GvwlXp
Cqi8AlJ4vKykx99SBgsrya0CnR63v+Rgwv+0tc3A24b5SiE395Dzh1R9N1pgXWYNOPgn98A1cYWG
A0bwayHzpcqw+e4YcR6qO1gykUL sPNlnlGCkakiOshblezzB1WrSziT6lNAjNSev+M7Uo4j6bCB3
sFRtvINXJWM7AqLxn+zC1xVqihB+N9m0YmNkjQIDAPHnMA0GCSqGSIb3DQEBCwUAA4IBAQODUXshm
A1Kx+fPyMrbQkOim5FrSoTuLw4Jaxhhcw5wQLTnl0H25IwciqGisi7ou4fYffaQISbLfbXEpGG2a
aZ9DPGGeG//5NPvtLoxLYw3igmaCYi4QEQ+O8Q5bH/YgxJWlZha8qtDXYjBVq7giX+1Kkb4O87Bc
Bm9yGWXnDbu/Cbyvv+lnbhLff3N9AGlhEVZW4y/WNgd4RjRANYuKHLsNdBBT2jnxTirGzHRbcQ3Q
wxJUcTO+z8l7WUfiq6bVayReUnWrmYG6bbzU2lwUUusb+cZ2uvNNAjuUS+ngc8g9FLlty5ZcT
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:F3:87:54:7D: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:6 F: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
cmRUaW1lIEFTMB4XDTEwMDQwOTA5MzMzNFoXDTExMDUwOTA5MzMzNFowJjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
x77CtLsrKHF3SswUv5uBEilPF3hJS6J+WS4dKIFj4tE0xkxl7J7yMIDMf3Gk2tunTpZolsOKDPCb
sl/9Ss V8dY7y+yCT7bRT467yfi2zqTrFybHjXduYGSlvagNpYVw260he6gVH27D/IdpQv2eWOOSc
GAWcBOZTr6pZxEuX7b24luq7sSci8hv4ARpJamWBTLQX6sdxfiPhjnyMlacEGOQuEQgUjPKxAxo4
5ApwSHWESD7lAm2PQNacSZJg8+pkxrOq0s/7FrsgfJzQxIDhyF9BA7u28ilsCL60WdVbxqshmQBp
91yyuX3ZTHAkJ8Wp0kT8EwVfVnLutFWxzXp/4gwIDAOHjMA0GCSqGSIb3DQEBCwUAA4IBAQAAYwPU
IEPIzB88xdz9WTaC8/QNF/DbfYOYKOD5439rGPhWj0YBe6Sliohf3K0tfBrnaC)+Nw8Ewzl7f
UD6+9xJ4FLSSQPSsH3pxZliAdiLXKWXUNou6jiPTh9gSDBkkjHvWCMhHj7GNDdIEABbwfqsSlejz
NsQZGUVu9Z7vP0+flTGvqC3qIqschhpQWZqaD4YR73K06H+JEFn6vnGQ6UVsWM/KDaktvLStQui
/OwIqK8kyEm2cpCQOdkVPJZ7vTcGDgonWvbwaxf78xPJUqHSNkuWIHveV6dFIS949v1eJYEwvcsv
6DyVD6Ul8A2efjnQmjA4KbXucmWzm0KY

-----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:C6:4
C: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:A9:3A: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:F7:5
C: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
p430lCKJvdyzzdK95iX4IlSE3MyVDkiPeQWKdvM/O0K/skXMKxK9308G01VVPz4Q0Fe/zm9Hd/b0
tF6lNebGpi+CUfS13eq32JZvfy17UsGNZCtU0nnkuGUUfLCXqlEMVsqfxXu9RAhwaJE3Zw0GZLc4
jSF9xJy1HRSSryUkgp09pOl/PP5l0lgBeUESM0U3ALPvS5xjgMpYJAOshZCIS+rsyO1Cp83ymVNy
GAw2jUCgjHGHu/l+wbTw8b6C2pUnqcUacaemjctKhtf6hNs+5+uTPBW2q9oA8k2c0SQti7+V04H8
L8rvSdLacVuNDgiEjzqPIJV7oS62APrWlWOf3wlDAKIzMA0GCSgSIb3DQEBCwUAA4IBAQCCHTCm
S6YOLlnhSEMpOq6F6ZUPq7B4BIEVJPlZOkrPuGRnwXY3CP1CM01mMZFcNc7OMYwEVyJNt11Aj12k
B2yoCGCqABdYij78P2n4MzQykakymH/IQhTiP6rZ1glB1stye5yboAvezm5Cor9lbdGSf9QEv7DP
GYqqyEwDAqClhIgyKWBDTixcKkRFlP7hvDWCzYaDaCzaxcxN0Cjv0KTMoTDzK97lZJ2+qrBcgP/9
AEsZftPOlvzObbrRpnmwowwgNvYT3p3sI7irrIwHryQh8H1kU4AwxmHtuMDcVKvQQrxpCQuEITPl
BlelY2MdXKRoCcu4q//X5lq9YYP1XljH
-----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:48:8F: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:52:C1:8D:64:28:94:D2:79:E4:B8:65:14:7C:B0:97:AA:51:0C:56:CA:9F:C
5:7B:BD:44:08:70:68:91:37:67:0D:06:64: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:A
7:CD:F2:99:53:72:18:0C:36:8D:40:40:8C:71:87:BB:F9:7E:C1:B4:F0:F1:BE:82:DA: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:C
A:EF:49:D2:DA:79:5B:8D:0E:08:C4:8F:3A:8F:20:95:7B: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
cmRUaW1lIEFTMB4XDTEyMDUwMzA4NDEwM1oXDTEzMDYwMzA4NDEwM1owJjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0AjnC81sjs87Vv9e8XDGWcKaj7kJTxuaeWpC+WULglfyU2YSawqwb1PZbM9AT0Oi4Dz44tCG1o0K
caeik+vWFe7AU3GSSC9K4Y3+jrhKZEOhySn1y11DMdnl+Iv844R/IqS+XEKvP0c2LLn T0Bnmz6l8
GlUh2c9MJWXIXfNyfgymldyT3ssw/RabL/IksTdqMsa9B7ar81vtmEG2rzsU/jCl6I8U6N7Etv3hs
eALX/mcdWplpWn8uxAGUl8KqskF1itQ04BOU3P6Qk0WsLFBNCeQ2Rj+HcHPEdxtkT1eM0IbmOT71
FuS7YZjC5fqza+CoiSPKBMJioU+28KG1qOFC1QIDAOwjMA0GCSqGSIb3DQEBCwUAA4IBAQBfIgbU
f5jzWS5EwcLmi7OgQ4ejPme6ZO5M+SX4OJh8cTViXOpqrF6JmIaFi7auqTKa4KNtgWmeGziaqD3U
9WamJ2aU3xmtf+t9rHWns9dBE+JRVdwNljvOyEt+foSCENaFxtPRDqpaphx/fYC+jdCdNh+JHuKx
qf1tW9ktBFNxG7qxmSeBa4eC+RosAXtt0gbmHBVMOQJOApGKIlQznuJ3c5YrCRzza/+D9jSkyp19
6VO+aYmt2epLMTK5CvJlgIjvF/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:F2:53:6
6:12:6B: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:F8:8B:FC:E3:84:7F:22:A4:BE:5
C: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
uWgbOYOThEhCRi61hnP3GSdD+V4sjuQCehCt9MJ+yyFvrEcJcwvGhMaCBq7mUJul0yV5pCNoSH7g
LDaO8XByJ4acmV8DxKAH1KILSH/tashAjxQLMbReoIA9c/qKiwO1oK12z5OCN7rA9C7PBO8gk/sC
LFacOwgYtDCz7faY5l94AEaniIA62hT3PZ7Sd0IkcL5Gp9goJ2tZdQ+G58GBZawF+pfS2dzWSKKx
WiV/iMzZahRdaXUF7vCGsXDsVHqS3AbL7ZbIGCRVX0Thg+RCyRBqE12iPea8HWcVMxSJFHLhvSvK
HTpj3iA6WVIOCJGUlhcz7h373WCKtgwGx7U+tQIDAMRFMA0GCSqGSIb3DQEBCwUAA4IBAQC4F/Sn
PubK6gaCyw5/7+sMTMILecuEGZ3W3ScAWLY4KP04pS7ViqlJxCvH3brl52dc9gUG0h602hRlEhdc
Xpk96kcd108cr0mv666mGp97CT92vIL2E46mnz6QUG8uWyNls+7K3SCgfkAIU7+lypM0NjOLXfD
gCDRK2x3S7EAJh1mlqYSRHL9mst1sBLxjUMzi2xzOEGh5SaijIb0xelm2bp2J3JZrCvyjvGGA+95
xRwHrGL9sMFdksrY6u66gG9zea8qurkSzRYBv0OGNUHwQWpw95QPZ47llTq9ipqC+J67FIEZhcHT
UtgPfvx1ch19IS8GiSM72M6rAeS8Kq19

-----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:E4:02:7A: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:C8:40:8F:14:0B:31:B4:5E:A2:50:3D:73:FA:8A:8B:03:B5:A0:AD:76:CF:9
3:82:37:BA:C0:F4:2E:CF:04:EF:20:93:FB:02:2C:56:9C:3B:08:18:BA:30:B3:ED:F6:98:E6:5F:78:00:46:A7:88:80:3A:DA:14:F7:3D:9E:D2:77:42:24:70:BE:46:A7:88:28:27:6B:59:75:0F:86:E7:C1:81:65:AC:05:FA:97:D2:D9:D
C:06:4A:42:B1:5A:25:7E:94:CC:D9:6A:14:3D:69:75:05:EE:F0:86:B1:70:EC:54:7A: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:D
E: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:C2:35:8
2: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

<u>2.6.1 - History instance n.1 - Status: undersupervision</u>

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service Name

Name   *[en]*   *TSA2*

<u>**Service digital identities**</u>

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*

<u>2.7 - Service (withdrawn): TSA1</u>

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*

<u>**Service digital identities**</u>

Certificate fields details

Version: *1*

Serial Number: *1*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIICwDCCAagCAQEwDQYJKoZIhvcNAQELBQAwJjENMAsGA1UEAxMEVFNBMTEVMBMGA1UEChMMR3Vh
cmRUaW1lIEFTMB4XDTEyMTAxOTE3MzE0M1oXDTEzMTAxOTE3MzE0M1owJjENMAsGA1UEAxMEVFNB
MTEVMBMGA1UEChMMR3VhcmRUaW1lIEFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+OA6jsb8QE/mLd3RPZFW40+l9RiGhpVWtaPSNgJAu1emrld4SFmLpOWM5BPsK6tVj2waLNucmEuR
tG3r6H91E7EEgjsiBDxJaaREHytXMgpatMkt26X6Cg73Eb0pvD+5eBIh6VpksIWHtRrtq6ahde2w
pb9CUmF8nb9Jjl3qEsd3L9+EtSF4/EppRzOs4GDzKG+NGmBz95IEMGiIf0yh9Ot05b0Wj4xdOT7s
JONbF0lC5qpQiPoXMKeLzsWWj6RIctjjhJZ9s2xEyLfwM89Yb4/vdwVVaa9Rk36ZkCvuoJeP1c+F
KDXAJmNRGp2knEC1lQBZvXLG027bKmDdU0+WGwIDAKKPMA0GCSqGSIb3DQEBCwUAA4IBAQCR63M7
Z45TV0MW2cA1bYO1vmRSryLbBK7fC4+2T8BqCXC8PYVxRtdMrQMdLUvXolibDY8bUDlC3GI4LLMD
u1ivVcAcRJOCO4ii5KHxmK+mlmlnif8v7YTZllXAqPxbxJlYmpRNaEHFcDS7fciYzvohPzpbxRCK
b4Nu9rfA0YqJv2s0vZmkZPTQ7W1vwHQw/+7KeRL3v/oY6/ANP0eKcNURwdhV3es2kya3RyEXH6sJ
uv3iUGOlPTAp5h8T7RV0xjlDxnz6BcRMSxxpFhyaUJHaA8ELKQXqHx1jjz0Ycri/AdlM21F3wc5U
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:D8: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
cmRUaW1lIEFTMB4XDTEzMDUxNTEyNDA1MVoXDTE0MDUxNTEyNDA1MVowJjENMAsGA1UEAxMEVFNB
MjEVMBMGA1UEChMMR3VhcmRUaW1lIElFFTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mbkBqCyj5DTDvCRFqy9AubKiWtz1NczYGFG4Uu1YrtNpY7hOrutp2SxjBZGMwcXDXdzIceE28FCv
uPjhTF1MsSmWA3wRqEFIdoKtwJ3hYM4N8NKB8GHgDKRYKw5nY++1anjt+KoxhpZsRbaAvPZSkbON
r6trgSe9DUXE1WJ632LAvC0PGdd4LnUERxncrmnhs5N/mQwv4BJmMPHcZ2IpiMBCgJ2/v7r9Ubo
dVRkGr/EHMzp9RdehneT3IQpMDV+7oL1niOyXi6KVdlbqaLzmL8QTpQuopfhaA6uKaAegWkkEaYO
o50BK3xYKZjCUHwL+yH6Sw7ddgGNtBld7vtdpwIDALyRMA0GCSqGSIb3DQEBBQUAA4IBAQAjlFih
75+4WvKgcTr7CHVgftiGLaSCa93uq57kmebap1raFqigOkCYpqg3Jx5DDhdGcx93VjdqTt6qC8IA
vx2VJAywQXOisItifriXK5hXUJMWlXzqT6q6Kv1q3Ac8603QySfStmVg5vehW504bg2UnjjL2oY0
+X9c/D8nQRpeI8zVNAYYk2elAr3nNDrcR/kRtEfughvIK2F4S5R4UrNO2P7xTaiNdQwRuq3C3ZE
kA2HjPRXE3ktJoL80p7aWU6DKOOHZr6VQjcOHJiK5T/ZUHeOT10tM3BCPHzmmHAs1ziMkFFfltOm
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:D2:81:69:61:D9:0C:A4:58:2B:0E:67:63:EF:B5:6A:78:ED
:F8: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:B3:93:7F: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:C6:0 1: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-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDExEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xMjExMjYxMjI1MDhaFw0xNDEyMjYxMjI1MDhaMCExCzAJBgNVBAMTAkgxMRIwEAYD
VQQKEwlHdWFyZHRpbWWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6jdPpv5oA0BNH
cFTVZpB8CEjGZvWrx4KWgbAVhJiQuiLx2TgmRrimtAi7ogQ2qWPpJJbxgnKQUvpL913tMH1bIL2
PXYk2fR6xU/jF3DoBvQBA7TrX39OlcTn+GO/noh9/hz3/aSebyp452AyFow/g7IzvECf/kT8G+Oc
Ij4aWK/M7qbmrj98cB/j6t5kuBF26llyLzExJr4iJOTSuCaR7BT3yWuLC3rAUfXJaG0XiQxkmTd6
Ibt5GK8pSBtsQfKeJv9iTUS6I093rqZ8dSiP9/k2satrk9/hy464niGyXiKWfiEwWBcEe6okg7Fw
tZZ7ZHL42IA7qLBRmbl9qvbXAgMBc7MwDQYJKoZIhvcNAQELBQADggEBAEbHvn6BZArTuTDE+opw
N0NZ6FdtQ102tR1qWMcNGgKKICc1dvQpTCsUD5X4RL26pE0aNy9lB6HFa2vNiS4ZOz7LAbxKWn9D
wSTHZVCBmDz7cThAop6YaVd+f2cYk6aP4FnIWr0dfSTT1qxIWyFURip5TLC4vgu2FvRuQU3LTBcp
dbi5WwVSxxgS5VCzpEc5qUC7kZFGBV/aze6CAxUoE2nWrK3udj/8RUOSpUyaeF+f4oEAkR/xMKvd
1xuWjl09rRyOD71h7WhfmNAJDHYZVRVthl6XBJbv+DMOkjpltfcFUHyvZm9eXEZnUh+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:B8:11:76:EA:59:72:2F:31:31:26:BE:22:24:E4:D2:B8:26:91:EC:14:F7:C9:6B:8B:0
B: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:21:30:58:17:84:7
B: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:5 1: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
VQQKEwlHdWFyZHRpbWWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDGUFzXDI8KWQj8
/UcZLf1BecHHG3+YYoA3FwtZZidNjlbRepRdwypQx8p0RNbvcZC5eP7TnOLz8tCA95jBclLXOOMEK
LeIdbcEuERrVNNZ6MplCsLBfxf0rSZzPcgjUA8vnREZj+rLqYkUwt6P2qt3uwCT/Ymm6D25UG373
TX/058+7+8YIlispEowUPZt1E23ZzpTrObervZSigvy4V1+efOPQZq0lB/h71hkmw0+/zuWJ9vjTU
hS3sde86AqDl8s3q6G1FbVEH9lnJ8XZipam95lZx+kRCeBQYitw+lYcLcGFQKOJ0tuZuqMo3HnF
cJINkd27uA1Ymi938SVOCypfAgMBBbiswDQYJKoZIhvcNAQELBQADggEBAHR1TVGVIuBLeTtrflzX
P4bnsczEudLu36D0dTKcwTvBeGB4YEnaBp69vKT2/boNbdeZ0Pm6ft7PQYRzQg5v8NVlqmYwq8pA
xNhrywGOICOynoW7mnRbooDKVQ25Ct4vdJwdf/pcrJ0l9F1WX3MZ5rNgKTPW6sXrMReXojfFf2Y
wAvdwPhATjtRvnXYhkkN0aeXvkgPiPMctEP0lEiZclwWm+DjVFHOy8I1d4+38rvh25tuChxxcl/p
45/H7xpAndHO1qpKEu9DJy6q5eWBcNgvHVf7UTXSDtluRCOcS6g0Q2yz72sdW1Z/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:A 5:17:70: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:E7:44:46:6 3: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:E8:6D: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:E9:58:78: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
uKvpYGhic2lEd2FAQLDB4gnJI68Z7K9B+Njc8rvwKbrqix+N3ReqFz9IENbwtGrXj90SMFBoCofk
mUCe+fy5H/YYjihud7wnZUhYPw7DsYU+5eqAh9dNXNSD4gxOLDoZgID49G9953fS2pkgdZKIWpZI+/
hftiTDLD92NB0HYwoqEJZZGSM+RUKMxPeRiHz6goGcqoXp/WjcXyd5uiP4TQX8KsvAQQDTBrBs8D
FbFlL7MOEzM+vvV2PdFdU0bRAgMBDskwDQYJKoZIhvcNAQELBQADggEBAL/Invma9hUUj7tcZAKK
NlZm2bktd6jgzW+zFUbf7m1zfSLw3sg85mwFkl8hSDlV/d4pasJJCd8KmGLKi5T9BMTAjvzf1g2
orBGMArhZkYNnYkuJTHcxetLFqtyBxdMKGiObmhfTI1YNAckomnvsaus8ejsKKFxFTcWQ1TOcL3
v3N/sZ/c/pwVd80ZbTIo/k/dFwbRVkhuj3Q+DDi/8tlcGXSAppBVX+uFqDGudu3TZ8XQY7VX7ZSH
/2rIOSSZm0CbgAOFYQitDLKLlXEBS6R4W4n559L+dXIaStAR3U8Jmx8WXWMSsalFJVynyiVLUMMw
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:45:9B: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:B8:AC:A9:60:68:62:7B:62:04:77:61:40:40:B0:C1:E2:09:C9:97:AF:19:EC:AF:41:F8:D8:DC:F2:BB:F0:29:BA:E:A: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:13:33:3E: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/iby6KWNztiEjzuLl2oaqsUEVHq4kpAAj6/Hl+UPnIEwPEckB6rpGRgcN/+K+4bWJTr
xh/7S/k3sQtHozTAYIOf6TIC4xAK5rjkfRyJNWZMbKU5ShXGC+DMh5sn5ZLtxOLshP4bVjCDrKUb
+bNJCxYE/UT4N3bSPj3j45CgYnwqANWu2MFYcuuwSI6M+BiLWRA9HNLwHF3nVibCCJtyo17gN4oa
236h61/+hehqICa9xePBBRh9gao35dtFNOEUgEN+gjqXGkUBrcFst6SG0nGh67AGJcQeku3QKU8Z
81qocY9NhUKeXordC1C/XPsfAgMBWGEwDQYJKoZIhvcNAQELBQADggEBAGAdaaN8Zy/BWVBH+hLT
+LXFJLKmFxaqRKRtyPtuerCRHmKjlHw8JqlVjB1UDUy4BN1LL04k6twcpZX/ahuvlG0cwrdfi2/l
d++ngyMQ8ecFEvjvli5u9kqiWSFxwDtA7fU5rsTm+Qni5hklPA60VMQHkuylx5oHejoyvPoBEfi/
tQmO3QL+re7Cs06m8hkBrWndYK9jyot7G99wWlR5TEYzYQkze1L0oTjmySW/+Ekrs166XmRWHQu
YLgo5tLSD+oO6H2tfeiKQ5PO0+zDLwQJJYjvvITCVKudR7/sH1v6/B4nXuvch82gaAzlHK3EP6T
Q7CBC3cw+uZ7qkggdlY=

-----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:87:9B: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:B0:06:2 5:C4:1E:92:ED:D0:29:4F:19:F3:5A:A8:71:8F:4D:85:42:9E: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
dGltZTAeFw0xMjExMjYxMjUzMjJaFw0xNDEyMjYxMjUzMjJaMCExCzAJBgNVBAMTAkg1MRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzNmmpHjZG/rb8
xYUBH5TgSkSE9tkVl+JgtkeokY0BLZvrJhM9TZ/XX3AbN5aagWnMgxPDBCyTYcA7XzsW6iRIQK7
gvm+zbLi9bmLEcpQzEYdeQs4Bt39Hb4vtIHYOFQjdckSH0CCaiLoJVJxX4b5y1dczlJXN5n7pkBl
/YXXuIt4h/41bdZKw25j/KxEGWU/CmlZdrtDPzYW85aYk++dbO+uKspRkkIQZV+smpSUpbwrjOoN0
VjfrmbJ7s+iyvB94j6qvvST1537uFY6TOK//W3O4OrtEd8ze3aiePC517yTM8IQaUOrNy/pojan7
FkhvLcVi1duQILuAcDu7gaQjAgMBMMcwDQYJKoZIhvcNAQELBQADggEBADndrk/PCTqGVmbrtjFW
mYIjLyFgbUihSoHHf2+kw66Mzi77LFkDc+CYSz5M1plijsXQe+a+Kkrvpc9YKkvxnT81ttiSduRuj
CNw2lSrYlFVP91Hzxh6hl2mnRSF6LOLsNbZCaSJjkH4JPuFdnY7wUiozKFrnt/61/5qu4B7osH5o+
sLuCJKcgk0fXgssx41JM+ZUWf5JhS/QUUaPiW18s4SOZmNmO5w1lYVVG70bUOXsoGsVmrBNuuQei
kPPdE30OAf+4ODB82rudUZok/ZrSW69p+eiAbkLKqlVfd1Lx05xeLf/EBgIvlSXRUECHV2LDmTbw
Jq1wDjHh5NHN7Z8I22l=
-----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:B9:8B: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:5 1:92:42:10:65:5F: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-----

MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDExEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDkwODQ1NDNaFw0xNzAxMDkwODQ1NDNaMCExCzAJBgNVBAMTAkgxMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDLKt3SYJHx+Y0z
Qvpj433i9k23BtR7VxLy+FDL54GkqmAiCmaknWz/nRy19FM+kDfciM92OvSnneN+nOvykfoblJ0u
L2CIhN5vYITV9QvHxNNsij0urOiWu5cXut6N6T+iZPOl93EmNeozJhgzG7FeDJid5W4kRBE9api
RBPp3YFehl0crycBgLY6kHlvvoH33Agws W9Zbp2B7jWU92GdH1D3aBw5JwhEhSl01sqjcI7Odbh7
PZaygsXpoVRyW1T5PzDDR1+qoWHoak/oN9l0NXMEAVyswpytQ0rckOIbnXhfA7va2WLQ8+Gulm7w
KwquS2wtqgBPbyvO7rP4L/AfAgMB4EEwDQYJKoZIhvcNAQELBQADggEBAI52GHcEe75qB8Sps07G
3TVA+XXh+PGFZYSMrH5bsn1uJvaDNDb1fl1dQCK+YibtoxzVM0pdyBVlHFWsex1wTpdmstsmZYP8
Xaj9ezabN6nPSCz6pdzhFUKM2XG0kuny6JLAFuNjqsh13SxsATARL6yZv7L2Pl5VcIXHbcpRhNaq
iTcTKxLfXqfTgSX1f1RGNJl/r4SoiTBT+PfJ2TcJtcSGTuRunaTeGVIe+QGlrv0fWXAlZylGTFsz
gq2e2hh/1i9KFixD7gS1lPvSRrxHVWdTEjM9BHSjMd/y6L6jQ9Ti9qW+UYz2CRo8sOYgfB7axA1m
Vmv/W60TQr2pkCl7GDM=

-----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:C7:C4:D3:6C:8A:3D:2E:AC:E8:96:B8:97:97:BA:2E:8D:E9:3F:A5:64:F
3: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:F7:68:1
C:39:27:08:44:85:22:34:D6:CA:A3:70:8E:CE:75:B8:7B:3D:96:B2:82:C5:E9:A1:54:72:5B: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:D
9:62: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:39:8 0:72:1A: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
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8ojFnaqso7obL
fS6sDn8Mj22s/ZcmY2NbwfGyl2xX+1FpEjgwrwea8Uq6YS55Mvux/oRcBh2UsgFxnn0IlzSLgrmR
x0t42PVuufygeXVGy+voYjxsOJUkP8uFqdv+QhLPUHTyVzMKHlYvVEa434dfHKiSK2nwWkpFVqEQ2
hITU/uSv3ZAX64F+7iJulIracfdZ0QC6ucdOsxAFwC3FEH+HfPpV2rb6nhsBu8hxJGWOqDHoCcd3
y0H2+7n/BE1pmOCkuT0j1KU2NwUrEvWfRna2xyx+zNfl9PmcNRrIT0yytr4ghCuQJbcGpA7+EGf
5jGKfGjL1xL6GXwnb3W23SPDAgMBHWMwDQYJKoZIhvcNAQELBQADggEBALxmxs0QzRhDIICmedBn
gmOGYIBd9sJ3TtWXak+4cJemPttrKPetWlDnSHyW2leuO6nelUtvKSXVET1qbX0Y2bn37qPseBu
3284qWLi2fAYhhOKfz2PEuUmck0+p3wKH6iDgsXgjmQuu6wO9m1+Y8qB/K+mSw8gpxjBU38aPCg
QtPZnIAbBPpju2NBb241ep+aOIonKQRO+KcsPMwYzLt0xEmkjopq4dRI0i+NI/m3EVc1JClsIvSD
37tUBQIbEpvv7OrXbv37xvY9Cr4JRWrrjrRO6n1d2NSxdagHjwobdBgPCQXGqroMxUNL0EprVmlb
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:28: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:51:6 9:12:38:30: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: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:27:6F: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:D9:99:7 8: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
dGltZTAeFw0xNDEyMDQwOTI4MTFaFw0xNzAxMDQwOTI4MTFaMCExCzAJBgNVBAMTAkgzMRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC15sVKLBcJ6NRM
FmMZvyBy/kKCcBr8zwozbZ+3cyuKeRk8s2+9IEH0xkIpE9MxCmDaW65rpk24aX01A9LvYaMJn8b
zE9H955wuRTWZbUpW22iJjLxjq3x6bM2mwMB/BRkWPK/0BZ8mO1XOXFGh6eRD5OqLXDen3AXno3L
gxpibK7jHekfX1aT2G35c2zDcZmif86bQiFSxPxI/xJXiJcswX3Xl1CoEdoyiOhyYIl1756QKzNL
/yzXy4W7Fczk5gjax+ke9snndPg/ZnPzKLHJowNyPzobhG0R7W7eG/S7BpxMTEG3alA3BZvV2gmV
Dw8Bp8t6mNNtxgbWL6fqKQdrAgMBh5cwDQYJKoZIhvcNAQELBQADggEBACyCZSs4DiVR9FvRRUCe
XAU4zpvIO2+nIAqL/SnK657aHNbnnQKqtBdoW4N/Gf6Pxz27B7PB1c1p1qgmKzvVewKfiwh+37XoC
IxqenoLzwALGN0wPnc3dVB1Jl8DMEMtECB5ktZMd/BI8fge6VlYBDnDXa+qu13hbTHYuWV0dIoks
eNOoNU9twcABn14E0AsEwfalZpXps9LQgjVx609pZwDFRQo3igzY4qKxpivUD0xyrjjsh5UebldL
j2K7gtFubrenuQuRerVFIJ82VmNsAdFFzyVsCXdUdULO+wxcnIjCUIAY2l8CEM70z/UXmuCCqnoq
PmmXk/oEIdqPLZQqR3c=
-----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:B
3:6F: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:B5:29:5B:6D:A2:96:32:F1:8E:AD:F1:E9:B3:36:9B: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:83:1A: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:E4: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:F E: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-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwITELMAkGA1UEAxMCSDQxEjAQBgNVBAoTCUd1YXJk
dGltZTAeFw0xNDEyMDUwOTQwMzVaFw0xNzAxMDUwOTQwMzVaMCExCzAJBgNVBAMTAkg0MRIwEAYD
VQQKEwlHdWFyZHRpbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCgdoH5rbrx9r/C
kW7gdHjEGtJIVYP9/sF26W0yMVvyEApwXJk9ccM5FNeJlnHO94DQ4jQIYGU8MnFu0Xs8FlrRI47v
Pikjsdl/HfGW8zQFvPq/CGR2JWtoTW/OS3TLlhuKsgZ4ynsIZs7VrU9H1bk/OyAgtvK3sbdyELF6
JYIy0t2mN5kXHPgFYs3PCifQteLEDsYLdxKKtwnEpR8Vyptw/9iNHPssvnqwpa/U5UL0Q/0dF4fxp
YNwVdgTKL5bpjaI6l2NmYBdhI8L9aTdEXsP+kSA/+pB5iqNGZ9vIrfweRLsqb8fIILjgIheJwgOK
MMTdfIsxfN8nJPr6ICAjd37DAgMBmHswDQYJKoZIhvcNAQELBQADggEBAHh80N8rHNR29mMguKbY
l5b6Enhls0VWx/F3oDe+gfZ3p+ASXIHPqZG8+e0BwDZh0QykZ3g8ctSBL4yOEUi5PEhilECuny++N
qFItHheyUXFFJih5qCqP8w+qiseVignlIRH/oumNXMt0HZUeWvh0G43Nc/6OdW2g2OtjUKjQ3Wtb
NP9Znx+okruUA2OrWpYN0V5PgE5FXrrssIykYb6ou3xThvmkowHddyl3x/koUdInfra5YUAY9hzf
FfUC8SdRg805OSy+EwI+dE006j91dR1EyNKZhqEg1Q5Wb2BGGRXbAYDOGeuX6NE9X+V2gKqD+kau
xfz+t2f6IzWEueaexo8=
-----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:70:5
C: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:C
A: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:B
8: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
VQQKEwlHdWFyZHRppbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC60wohNDbrmyAL
/7WupGYRFg8sBizryJup1HDV7YJvhVAo7jt63nrzuxqnADeqlzeek2GuYugh5LbYRR8EeBtxE3ss
IahIc5TLKPZj1hzJ+Tsw39BrbYebQUwusxU+BUclQ9TpxgSAM6eXa5w2pt9o8eiHVMxzXQ5c5BE0
XGSSH4IRRoej/xnealXgxNIFvEm14sFvkAg04WQQwD9ZTmWMY80WHeYDFr+v7N520r19GMyTc8Yo
R8DfWl0ILBYrcG1yDXu6gZlaLD+Xrb633Qn7WRgWD0ejCh9taWbEDBwoc6aM8yZDLfBsExYQSn8R
MCcVXZjDZv5k7+IQaozgj0q7AgMBarkwDQYJKoZIhvcNAQELBQADggEBALnzytGvxyDEf8IDaErx
1VaZpUcZrWSifiBc3jK3h3PvFTuaY98DT9keY2X1vM9mSeMBusRdMbIkFROA6+uUUNEXlp7lQEoZ
9/N1H4vCGscvZWBOua668qw2PrUCQoD5pP1SDH/0JpK4wX+Xk8bdi+Q6cHu2p606r4PBUVv2oR5
y+LaghTC10pT+4+EQ8rDPmseiatvSa9dJdz3RM/blR+Kt9OO5nBYpPBQJuvDTJ1rfWSfr7JD0ejD
OVeG9O0fN0j26L/sChV5uZxRMs/mvIlRibHqXU0+oeOGCCsZGb6YN27nLFh5TUdqtGRtJuu3f/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:58:8D: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: *13303434141265161953998710116*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIFcDCCBGCgAwIBAgIMKvxXwd+2ViRgXqVkMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlHbG9iYWxTaWduIFF1YWxpZmll
ZCBDQSAxMB4XDTE5MTAwMjEyMDIyM1oXDTIwMTAwMjEyMDIyM1owgaIxCzAJBgNVBAYTAkVFMQ4w
DAYDVQQIEwVIYXJqdTEQMA4GA1UEBxMHVGFsbGlubjEVMBMGA1UEChMMR3VhcmR0aW1lIEFTMRUw
EwYDVQQDEwxHdWFyZHRpbWUgQVMxKTAnBgkqhkiG9w0BCQEWGnB1YmxpY2F0aW9uc0Bn7WFyZHRp
bWUuY29tMRgwFgYDVQRhEw9WQVRFRS0xMDExMTQxMTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCt1f0R2cimqb2iM0/zVB00PfcY/w2zkpWSKuHlcyFMyxPaDsUFAxBlHpBn4bk9QEyp
WB/RpK15SPV1Veb5oL7o7A+62O7SXdA4jEyajyFVvP+mK/cXsSQ/x7Bb7r9woPH2Fmm1zExAkjrp
yW2H9jjBav2TSD5sLW1/ANfg0O9c1QgClmiZc2dKMCmXLvB5gVSa4PiZ1RGQ+IcHVzfQhEIrmywp
oe9MFfyB22eQfskqXcdopNLF8Ix3iHE9hp75yrhmuOrFG32vDbdgQTGwJBbRe8QDidyVQiuKwiJa
YPnhAryZXXgnrI7PIddFib7aE3MQDHEmW4VPqKlITX2r4HyFAgMBAAGjggIBMIIB/TAOBgNVHQ8B
Af8EBAMCBkAwgYUGCCsGAQUFBwEBBHkwdzBABggrBgEFBQcwAoY0aHR0cDovL3NlY3VyZS5nbG9i
YWxzaWduLmNvbVS9jYWNlcnQvZ3NxY2ExZxc2hhMmc0Lml9dDARSMFAwQwYLKwYBBAGgMgEoIwEw
NDAyBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5jb20vcmVwb3NpdG9yeS8wwCQYH
BACL7EABAzAJBgNVHRMEAjAAMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwuZ2xvYmFsc2ln
bi5jb20vZ3NxY2ExZxc2hhMmc0LmNybDAlBgNVHREEHjAcgRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1l
LmNvbTA3BggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACO
RgEGAJAgBgNVHSUEGTAXBgkqhkiG9y8BAQUGCisGAQQBgjcKAwwwHwYDVR0jBBgwFoAUIrDfbzzLJ
IRaqCxwGA4bwXcdpzRowHQYDVR00BBYEFPe+Zbcss+aHPvl0aNUGuBxgwHg1MA0GCSqGSIb3DQEB
CwUAA4IBAQALCkY2JkPjPdJV8NS+2gm3MDVurit5dp6AjRLIEoo2tmgQkosYnfyPXaJH4iF9k2E
B8K4piO+9ASljeEwifGaHAbpfY9IXYM87RRbuw2Q1YScog4ev6NdvhIZjSTQzu5wJ/dJB5rE9JP
tN9eAY3ihQXB/lhSuX1M2p82wCBma51+jZnyQgOVwXXgX/+RqotnAzmRt63NqfAQkAOp3NPW2EPk
eoFz1Lv5eBxGZapggF0l5alhYWhR/96McP3isQAtflLnakwAPgHvJ9rxWnTAhOB6N0kWRiEClgnG
xOnZT1TQVVTDpXwBYsgtZ1cv82ag2sH75vCKnyFlxHHlgCo+

-----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:CB:13:D
A: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:DE:EE:D2:5D:D0:38:8C:4C:9A:8F:21:55:BC:FF:A6:2B:F7:17:B1:24:3F:C7:B0:5B:EE:BF:70:A0:F1:F6:16:6
9: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:A
C: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:

100067200787907560082741310892

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIFYDCCBEigAwIBAgIMIFVdZnGni6mwPnWsMA0GCSqGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlHbG9iYWxTaWduIFF1YWxpZmll
ZCBDQSAxMB4XDTIwMDgyMDExMDY1NFoXDTIzMDgyMTExMDY1NFowgcxCzAJBgNVBAYTAkVFMRYw
FAYDVQQIEw1IYXJqdSBtYWFrb25kMRAwDgYDVQQHEwdUYWxsaW5uMRkwFwYDVQQLExBLU0kgUHVi
bGljYXRpb25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT8OcMRYwFAYDVQQDDA1HdWFyZFRpbWUgT8Oc
MSkwJwYJKoZIhvcNAQkBFhpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1lLmNvbTEYMBYGA1UEYRMPVkFU
RUUtMTAxMTE0MTEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAntxxAxMzPwFmNY09
BYpYGUZeNQIwmUrbE3Msz+VaBapglX5oapUljmWuXV0wOXcEMdIxbbhI4wArKuhjZICduZnvfe/T
JSuINrOeGI+FE/9Le0BLrCPT4sX2XIV6oV6/IyN1uUbGD0ISF3StFynI4S68VgQSFCcNtfLvcIZm
5rMwdw3dh/w5FQQeVmH4/bgr3mc8OCRXkoFW6+LtwRJig1I4RYR0unME0q+IXOKXV0H6GcJtK82L
lqS0bor53qLlVDNfoBnEACD27TeKiyZsL9dwMtU+TcsMC6GEc/ldEkvfSKxu8QnA/i5/JtvGmCHr
2D6CxDGCDNrI7ro8+rXk8QIDAQABo4IBxDCCAcAwDgYDVR0PAQH/BAQDAgZAMIGFBggrBgEFBQcB
AQR5MHcwQAYIKwYBBQUHMAKGNGh0dHA6Ly9zZWN1cmUuZ2xvYmFsc2lnbi5jb20vY2FjZXJ0L2dz
cWNhMXNoYTJnMy5jcnQwMwYIKwYBBQUHMAGGJ2h0dHA6Ly9vY3NwLmdsb2JhbHNpZ24uY29tL2dz
cWNhMXNoYTJnMNDBZBgNVHSAEUjBQMEMGCysGAQQBoDlBKCMBMDQwMgYIKwYBBQUHAgEWJmh0dHBz
Oi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkvMAkGBwQAi+xAAQMwCQYDVR0TBAIwADAI
BgNVHREHjAcgRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1lLmNvbTA3BggrBgEFBQcBAwQrMCkwCAYG
BACORgEBMAgGBgQAjkYBBDATBgYEAISGAQYwCQYHBACORgEGAjAgBgNVHSUEGTAXBgkqhkiG9y8B
AQUGCisGAQQBgjcKAwwwHwYDVR0jBBgwFoAUrDfbzzLJIRaqCxwGA4bwXcdpzRowHQYDVR0OBBYE
FOM9BPC4T+QE2IBZskLYBs5DbC03MA0GCSqGSIb3DQEBCwUAA4IBAQCYULFVSQs6zmVrmYT5Rkex
oTFYkBD9Kxui4RhX35yz/FLv0QaGhIQmkD9oLc5CYNzL4WgbH4uhEH4npEXGj6Q+HMRvkU4g/HyP
NohgzojxZFe5QLYPvAI3E/ED5RLUcI2/Co8bEqn0RYHs3yK+cnUvzd443JOXoR2WsX88sKC2HFxu
gOJlm9gtuQtmCX46Ws98cwsW4NnP2mp/s9y8Fh/IEcQIFQG3rpxIt3ROS7RfGJ06hPIwGCMEh4kp
az0eYf4SA0kpl5FqvF7JD/W+McQZS7o2VGaygXqo4a5g+jra99df1WOShiCb3fkDxftCPHOZ/utG
2jSKmXIORlcOy/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:3D: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:8B: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:2
E: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 (granted): 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:

11835583698131848642139306192

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIGsTCCBJmgAwIBAgIMJj4qVehNPMq23LjQMA0GCSqGSIb3DQEBCwUAMH8xCzAJBgNVBAYTAkJF
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMTowOAYDVQQDEzFHbG9iYWxTaWduIEdDQyBSNDUg
UXVhbGlmaWVkIFFTQ0QgU2lnbmluZyBDQSAyMDIwMRkwFwYDVQRhExBOVFJCRS0wNDU5MTM0MjU2
MB4XDTIxMDEwNjEyNDEyNFoXDTIzMDEyMTExMDY1NFowgccxCzAJBgNVBAYTAkVFMRYwFAYDVQQI
Ew1IYXJqdSBtYWFrb25kMRAwDgYDVQQHEwdUYWxsaW5uMRkwFwYDVQQLExBLU0kgUHVibGljYXRp
b25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT8OcMRYwFAYDVQQDDA1HdWFyZFRpbWUgT8OcMSkwJwYJ
KoZIhvcNAQkBFhpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1lLmNvbTEYMBYGA1UEYRMPVkFURUUtMTAx
MTE0MTEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr0PRuQ/kZTcxbY+Khgtmtytq
K7fwX6hOxnozDX5/YX1G6GQUVCCqLvDPO4u3oELiwW12eW8InJsdeUxhbnly1mqFs+J1asWM1Fdj
pgTEjwhayhURFEZ5VMTyL+CfBUe0nGRJ2Zmqtphh/GFk2hf0KZS24vGdTaERBO5LD8YFzZOLeTmF
PBSDqsdPz026YLtecGndLj4ZCxq0Z7cA7UYoZvtkmwPo1RKzNX53vQ3p8fPbQq0mlxLIeC70vObd
I0gjLHzj5viplAbd8oEa+jl0NJjPQpwM0LyN9yeJZjo4iyeaudNXIvGxrMpvfxmJQs6cFVQGfQZ
WvwVrB1z6LNzaQIDAQABo4IB4jCCAd4wDgYDVR0PAQH/BAQDAgZAMIGjBggrBgEFBQcBAQSBljCB
kzBOBggrBgEFBQcwAoZCaHR0cDovL3NIY3J0L3NIY3VyZS5nbG9iYWxzaWduLmNvbS9nY2NyNDNny
NDVxdWFscXNjZHNpZ25pZ25jYTIwMjAuY3J0MEEGCCsGAQUFBzABhjVodHRwOi8vb2NzcC5nbG9iYWxz
aWduLmNvbS9nc2djY3I0NXF1YWxxc2Nkc2lnbmNhMjAyMDBZBgNVHSAEUjjBQMEMGCysGAQQBoDIB
KCQCMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkv
MAkGBwQAi+xAAQMwCQYDVR0TBAIwADAIBgNVHREEHjAcgRpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1l
LmNvbTA3BggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAl5GAQYwCQYHBACO
RgEGAjAgBgNVHSUEGTAXBgkqhkiG9y8BAQUGCisGAQQBgjcKAwwwHwYDVR0jBBgwFoAULBbpbOncU
LIeGRvxwFI9sdZl0oRgwHQYDVR0OBBYEFAaesnAAInelqQMdEfF2n4qsTHQXMA0GCSqGSIb3DQEB
CwUAA4ICAQAiR/0mlTxAqooHW7mPhxK0MromXCKtSJ0F6TadHl1U95WfuORXKWxO1BtX87ObZJ8h
pZzX1j6SD1e+5H47pmZC1TAMoEGjmnLjRo7y794FQYoYwlcjfByZswLVtkoiy34U2S+VDOLWrEds
O0KR7TeE5gQ4ZwQ5D34Dvb3O9fgOqLNcqWCRYmvwPYSwNK5zm8pO864iyCyohXxoZF4zyxhK0qmq
ib016ADdXMb16OevELELA3sDJCV+yOU90d4fvXdM3R/UFv15NLvB8G+7ehrP3XQuTxbBoaerzSJS
7uhy7Bcl1kOQO+M:59xvFX9GzBHto2SDPiGbgu5/uFJocQE9ntxGCZF5ypxaAamvaPtfUQdtrhKA
KszBHjlPdHZ2L3iUl/8So/BA847Q5KhH1rwyOFVz93Ow9oY+GcHW7fM3SumXgYxNvQUk4ZGRK24O
ZsxbEyGVoCwHXj4JTkuXpPZcbE3lk8Mp8igi96RrQD3zBlvVfK7QZW9WPZ+8OUC9laX2ogbMLAaE
SWvG4Wzr08sHTlYLQZBnTCymjL/ud+8gFmeXuPoWxvqsGF+FZyGDZibERC0L0rgAQ4IqXEsFNI09
Esc6RQ1oJnmsTtcaOCVq81Vv/8FuD9SK8YExEltRlvNfd1IadNTr4vWMm/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:E8:6 4:14:54:20: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:D9:9 9: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:19:0B:1A:B4:67:B7:00:ED:46:28:66:FB:64:9B:03:E8:D 5:12: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:C 6: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:6 8:10:1F: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/granted

Service status description   [en]

undefined.

Status Starting Time

2021-02-13T22:00:00Z

2.22 - Service (granted): 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
MRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMTowOAYDVQQDEzFHbG9iYWxTaWduIEdDQyBSNDUg
UXVhbGlmaWVkIFFTQ0QgU2lnbmluZyBDQSAyMDIwIwIwWMRkwFwYDVQRhExBOVFJCRS0wNDU5MTM0MjU2
MB4XDTIzMDgwMTEzNTUzM1oXDTI2MDcyODAwMDAwMFowgccxCzAJBgNVBAYTAkVFMRYwFAYDVQQI
Ew1IYXJqdSBZWFrb25kkMRAwDgYDVQQHEwdUYWxsaW5uMRkwFwYDVQQLExBLU0kgUHVibGljYXRp
b25zMRYwFAYDVQQKDA1HdWFyZFRpbWUgT80cMRYwFAYDVQQQDDA1HdWFyZFRpbWUgT80cMSkwJwYJ
KoZIhvcNAQkBFhpwdWJsaWNhdGlvbnNAZ3VhcmR0aW1lLmNvbTEYMBYGA1UEYRMPVkFURUUtMTAx
MTE0MTEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqddlsZ9Nc5xsctW09zEjN3Hi
8R/j2gl5eLg1+AIqLp+ZpmCo+teFtEGGstanKW07nrcM9qMsL30R/MIkeyI+ass6AbpQfE84XdkT
LBy92qAHqxYTYkvXGxK8z6zZh2vIZCfecCG8iDFxh0vozQBtHRi8BqsC9R5V2LSmsuIX87rRner9
WKwJbUDpM8uAYTXc8dfK5/rhAPx06oxSIs+kcvvqi9Hfv4NSZSUTIhdWyDvjuttYjhNa1vDwaortO
owPKL7dfQtTUUnqWRMxZP6ishhSuATr4rp27lZSorw3hTwHoQeQHzQ865UdQSe92abiPGHP8Hqju
33SCom3MfMtoRQlDAQABo4ICLTCCAikwDgYDVR0PAQH/BAQDAgZAMIGjBggrBgEFBQcBAQSBljCB
kzBOBggrBgEFBQcwAoZCaHR0cDovL3NIY3VyZS5nbG9iYWxzaWduLmNvbS9jYWNlcnQvZ3NnY2Ny
NDVxdWFFscXNjZHNpZ25jYTIwMjAuY3J0MEEGCCsGAQUFBzABhjVodHRwOi8vb2NzcC5nbG9iYWxz
aWduLmNvbS9nc2djY3I0NXF1YWxxc2Nkc2lnbmNhMjAyMDBZBgNVHSAEUjBQMEMGCysGAQQBoDIB
KCQCMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkv
MAkGBwQAi+xAAQMwCQYDVR0TBAIwADBJBgNVHR8EQjBAMD6gPKA6hjhodHRwOi8vY3JsLmdsb2Jh
bHNpZ24uY29tL2dzZ2NjcjQ1cXVhbHFzY2RzaWduY2EyMDIwLmNybDBBgNVHREEHjAcgRpwdWJs
aWNhdGlvbnNAZ3VhcmR0aW1lLmNvbTA3BggrBgEFBQcBAwQrMCkwCAYGBACORgEBMAgGBgQAjkYB
BDATBgYEAI5GAQYwCQYHBACORgEGAjAgBgNVHSUEGTAXBgkqhkiG9y8BAQUGCisGAQQBgjcKAwww
HwYDVR0jBBgwFoAUBbpb0ncULIeGRvxwFl9dZl0oRgwHQYDVR0OBBYEFl6z5c12tsdIDk3ha6tm9
8I4I/L13MA0GCSqGSIb3DQEBCwUAA4ICAQAnDWBUO1WUttYZgPzzh3E1vf6/jsWyr2zVKemOOb2w
+HBGVmsjGVRogTTeNfmumWc+X44iESZ6BpLETali8F/ygMjhblE8Ttrh/3fduXhgUZQnM6AJIfNV
kiyT95kvZJaRwZTjFGlb1J9Wtv4dfGwkm3XvjTV0g/m+4JVg7nOhEWpXP1X4sqYZtqckiVOp0pNd
D52KHTPNSFvLpa35+iJxxlyJjFQUYUIAX99RBqbxk4D0Gwdie17T40zRWP5CzgPiFnCwyiGstslv
0cNLyBhwTYzpQyxNxWnr6jZ8BSxNKhDRq91x2vaSI4JjEROr4m6K/RB1WPM6NCQcgC84UG+/xT1
oFGMPY066pkKDQfg119txahlH/qcG7XbXRblm0DP6uSe3IuQJz0UT+2k0WHNRleuUsCgshf4A82X
oRIBGbPeg7pOf1YCay6P4to/eBC09qc4l/fv6aa/MRPaW/ZmnSONMy446Wx0aAWQ8XQJV9wRJUDH
H9NM0GokpyYOIaLDHFCBQ0M463y7Pl9Bcap/d2WIG0iRG8LvqQl7qXMVvYDv6H2CeHTl2nHvaZx1
jeH+OBmxkHh/nAqvnogN3mLjFWlYhcgM2+7dhi/lDNS+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:B8:35: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:8:B: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/granted

Service status description [en] undefined.

Status Starting Time

2023-08-20T09:00:01Z

3 - Signature node - Id: id-8ba4ca665b529667055f87f5dfa46eaf

Signing Time	*2024-02-07T10:29:55Z*

TSL Scheme Operator certificate fields details

Version:	*3*
Serial Number:	*11132080187539732902*

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIDrDCCApSgAwIBAgIJAJp9F/NFeDmmMA0GCSqGSIb3DQEBDQUAMG0xLjAsBgNVBAMMJUVzdG9u
aWFuIFRydXN0ZWQgTGlzdCBTY2hlbWUgT3BlcmF0b3IxIzAhBgNVBAYTAkVFMS4wLAYDVQQKDCVF
c3RvbmlhbiBJbmZvcm1hdGlvbiBTeXN0ZW0gQXV0aG9yaXR5MB4XDTE5MDEyNTA5NDAwNloXDTI4
MDcyNDA5NDAwNlowbTEuMCwGA1UEAwwlRXN0b25pYW4gVHJ1c3RlZCBMaXN0IFNjaGVtZSBPcGVy
YXRvcjEjMAkGA1UEBhMCRUUxLjAsBgNVBAoMJUVzdG9uaWFuIEluZm9ybWF0aW9uIFN5c3RlbSBB
dXRob3JpdHkwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBMux4ivfdlZy9W75NgMWf
D7ahajygYHCp8Tw9LxQ0vkmpuyaNNlXU+uj+yflWfekVgMoLaQrCpVIN0FF8ZMnnlsK600hpgnQN
I+snPxU1u9BK6P87ZpoQU2wvan2oqjWflm06ybLzvvJrPJVNoVelrUDTY6SPngMbyqqpsdXo+dW8
916ZoRUcEkTFWjQXVjhY1Lqsorbpaop1iv9BV2SXmsh4szRlqpu4dDSElWViBn0+A1ptiSAt7JIN
r0DDjfiswqI+dhvjftxq+IEaqUoMtGPKgz7SDqKKyg/KBO1ZGunUZE+91HKUASt+sPy3O3wMZM1Sp
Ze1INEXQ0EQ4gytdAgMBAAGjTzBNMAwGA1UdEwQFMAMCAQAwCwYDVR0PBAQDAgeAMB0GA1UdDgQW
BBScAndEhykw8vEHVFuQ7XPtHnqFajARBgNVHSUECjAIBgYEAJE3AwAwDQYJKoZIhvcNAQENBQAD
ggEBAHaLeIDZmUA9Bcv7TjuQW2Q3cFWFSmKc8aT5HaRKBxRRy10j9czqT439w/smT4De8JYyULXU
+SoUX6/5sjmcpYxczFIC6imH8XLTgOca3vRAhek5iM80+h6v8CvxQHrsqNiSrLImE4LWfXWhQ/WP
cyQdNrHCFrynJ9Gf6Q1DzQBRstpj5l8WjE+ME+w+vDj+VHHjJ4wd5NkJhwwaF5PFB6uRrdb95e1d
qLe4CTALe6+dh2QYhzSWZ+AZ2GaF+LlFreHhyV0sl+KwcNKSzSotStHL0zPTnq/yxPNaihhFmAlP
dZdwq7vTN+yn5PAqEcfhTn06Gf5yDZjmf5JO5eMpzM=
-----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:A
9: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:B2: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:A1:15:1C:12:44:C5:5A:34:17:56:38:58:D4:BA:AC:A2:B6:E9:6A:8A:75:8A:FF:41:57:64:97:9A:C8:
7B:B3:34:65:AA:9B:B8:74:34:84:95:65:62:06:7D:3E:03:5A:6D:89:20:2D:EC:92:0D:AF:40:C3:8D:FB: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:E
F:75:1C:A5:00:4A:DF:AC:3F:2D:CE:DF:03:19:33:54:A9:65: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*

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*