AS Sertifitseerimiskeskus
SEB-kaardi sertifikaatide ja tühistusnimekirja profiil

Versioon 1.0
Kehtiv alates 21.09.2012

Versiooni info		
Kuupäev	**Versioon**	**Muudatused**
21.09.2012	1.0	Versioon 1.0

1 Üldist

Käesolev dokument käsitleb SEB-kaardi sertifikaatide profiile ja minimaalseid nõudeid nendele.

2 Kasutatud mõisted ja lühendid

Lühend	Definitsioon
SEB-kaart	SEB poolt välja antav kaart, millega on seotud digitaalset isikusamasuse kontrolli ja digitaalset allkirjastamist võimaldavad Sertifikaadid.
Sertifikaadi omanik	SEB-kaardi kasutaja, kelle isikuandmetega on seotud SEB-kaardile kantud digitaalsed andmed.

3 Sertifikaadi tehniline profiil

SK väljastab X.509 versioon 3 sertifikaate vastavalt soovituslikus standardis RFC 3280 [1] toodud juhistele.

3.1 Kohustuslikud väljad

SEB-kaardile väljastatavas sertifikaadis peavad vähemalt olema välja toodud järgmised andmed:

Väli	OID	Kirjeldus
Version		Sertifikaadi vormingu versiooninumber: V3
Serial number		Sertifikaadi järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber
Signature Algorithm		Sertifikaadi signeerimisalgoritm:sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer		Sertifikaadi väljaandja andmed
e-mailAddress	1.2.840.113549.1.9.1	Sertifitseerija e-posti aadress: pki@sk.ee
id-at-countryName	2.5.4.6	Riigi tunnus: EE
id-atorganizationName	2.5.4.10	Sertifitseerija nimi SR-s: AS Sertifitseerimiskeskus
id-at-commonName	2.5.4.3	Sertifitseerija eraldusnimi: EID-SK 2011
Subject		Sertifikaadi omaniku andmed
id-at-serialNumber	2.5.4.5	Sertifikaadi omaniku isikukood
id-at-givenName	2.5.4.42	Sertifikaadi omaniku eesnimed
id-at-surname	2.5.4.4	Sertifikaadi omaniku perekonnanimi
id-at-commonName	2.5.4.3	Sertifikaadi üldnimi kujul: <PEREKONNANIMI>,<EESNIMED>,<ISIKUKOOD>
id-atorganizationalUnitName	2.5.4.11	Sertifikaadi kasutusvaldkond Digitaalset isikutuvastust võimaldavas sertifikaadis: *authentication* Digitaalallkirjastamist võimaldavas sertifikaadis: *digital signature*
id-atorganizationName	2.5.4.10	EID (10004252; AS SEB Pank)
id-at-countryName	2.5.4.6	Sertifikaadi taotluses märgitud isikukoodi välja andnud riigi kood vastavalt RFC 3280 toodud juhistele.

Valid from		Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Valid to		Sertifikaadi kehtivuse lõppemise aeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele. Üldjuhul sertifikaadi väljastamise aeg + 1825 päeva (5 aastat).
Public key		Avalik võti ASN.1 kujul koosneb vähemalt 2048 bitisest moodulist.
Key Usage	2.5.29.15	Sertifikaadi põhikasutusala Digitaalset isikutuvastust võimaldavas sertifikaadis on tähistatud ainult üks võtmekasutusala: *Digital Signature;* Digitaalallkirjastamist võimaldavas sertifikaadis on tähistatud ainult üks võtmekasutusala: *Non-Repudiation*
Enhanced Key Usage	2.5.29.37	Võtme laiendatud kasutusala. Kasutusel ainult digitaalset isikutuvastust võimaldavas sertifikaadis: Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Microsoft smart card logon (1.3.6.1.4.1.311.20.2.2)
Subject Alternative Name	2.5.29.17	Sertifikaadiomaniku e-posti aadress. Kasutusel ainult digitaalselt isikutuvastust võimaldavas sertifikaadis. Kasutatakse RFC822 Name identifikaatorit, kuhu on kantud sertifikaadiomaniku tööalaseks kasutuseks mõeldud e-posti aadress
Certificate Policies	2.5.29.32	Sertifitseerimispoliitika. Viide sertifikaadi väljastamisel lähtutud põhimõtetele. Viidatakse põhimõtete unikaalsele tunnusele - OID-le kui ka selle asukohale SK avalikul veebilehel: Policy Identifier= 1.3.6.1.4.1.10015.13.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
Authority Key Identifier	2.5.29.35	Sertifitseerija avaliku võtme räsi
Subject Key Identifier	2.5.29.14	Käesoleva sertifikaadi avaliku võtme räsi
CRL Distribution Points	2.5.29.31	http://www.sk.ee/repository/crls/eid2011.crl
Basic Constraints	2.5.29.19	Piirang, mis näitab sertifikaadi tüüpi (lõppkasutaja sertifikaat): *Subject Type=End Entity, Path Length Constraint=None*
Thumbprint algorithm		Räsimisel kasutatakse sha1 algoritmi.
Thumbprint		Sertifikaadi räsi

3.2 Mittekohustuslikud väljad

SEB-kaardile väljastatavas sertifikaadis võivad lisaks kohustuslikele andmetele olla välja toodud järgmised andmed:

1.3.6.1.5.5.7.1.3 id-pe-qcStatements	1.3.6.1.5.5.7.1.3	Kvalifitseeritud sertifikaadi tunnus.

		Sertifikaatidesse kantakse järgmised tunnused: -EU digitaalallkirja direktiivile 1999/93/EC lisadele I ja II vastava kvalifitseeritud sertifikaadi tunnus {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1} -Tunnus, mis märgib et serifikaadiga seotud privaatvõti asub turvalisel allkirja andmise vahendil vastavalt EU digitaalallkirja direktiivi 1999/93/EC lisale III {id-etsi-qcs-QcSSCD}, {0.4.0.1862.1.4}

4 Tühistusnimekirja (CRL-i) profiil

Tühistusnimekiri väljastatakse kaks korda päevas ja sisaldab nii peatatud kehtivusega kui ka kehtetuks tunnistatud sertifikaate. Nimekiri on koostatud vastavalt tühistusnimekirjade vormingule x.509 versioon 2 (vt RFC 3280) [1].

CRL komponent	OID	Viide RFC 3280	Märkused
CertificateList		5.1.1	
tBSCertList		5.1.1.1	vaata järgmist tabeli osa
signatureAlgorithm		5.1.1.2	Tühistusnimekirja allkirjastamise algoritm: sha1WithRSAEncryption
signatureValue		5.1.1.3	Signatuur
tBSCertList		5.1.2	
version		5.1.2.1	Tühistusnimekirja vormingu versioon: V2
Signature		5.1.2.2	väärtus sõltub valitud algoritmist
Issuer		5.1.2.3	UTF8 kodeeritud CRL-i väljastaja eraldusnimi
e-mailAddress	1.2.840.113549.1.9.1		pki@sk.ee
id-at-countryName	2.5.4.6		EE
id-at-organizationName	2.5.4.10		AS Sertifitseerimiskeskus
id-at-commonName	2.5.4.3		EID-SK 2011
thisUpdate		5.1.2.4	Tühistusnimekirja väljastuskuupäev ja kellaaeg. UTC aeg
nextUpdate		5.1.2.5	Järgmise tühistusnimekirja väljastamise kuupäev. UTC aeg. Tühistusnimekirja avaldamise intervall on määratud sertifitseerimispoliitika dokumendis.
revokedCertificates		5.1.2.6	Kehtetuks tunnistatud või peatatud kehtivusega sertifikaatide loetelu.
Revocation Date	2.5.29.24		Kehtivuse peatamise/kehtetuks tunnistamise kuupäev ja kellaaeg
Reason code	2.5.29.21		Põhjus (peatatud kehtivusega sertifikaatide puhul 6 – Certificate Hold)
Serial Number			Kehtetuks tunnistatud või peatatud kehtivusega sertifikaadi number
CRL Number	2.5.29.20	5.2.3	Järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber
Authority Key Identifier	2.5.29.35	5.1.2.7	SK vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i signeerimiseks) identifikaatorh
Issiuing Distribution Point	2.5.29.28		Tühistusnimekirja levituspunkt: http://www.sk.ee/repository/crls/eid2011.crl

Väljal authorityKeyIdentifier esitatakse SK vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i signeerimiseks) identifikaator, mis on oluline SK sertifikaatide ahela loomiseks.

Väli CRL number on monotoonselt kasvav arv ning määrab konkreetse, SK poolt välja antud, CRL-i järjekorranumbri.

Samuti võib sertifitseerimisteenuse osutaja võimalusel kasutada ka CRL Entry laiendusi, järgides RFC 3280-s esitatud nõudeid ja soovitusi.

5 Viidatud dokumendid

Viidatud dokumendid:

[1] RFC 3280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile

[2] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile