SK asutuse sertifikaatide ja tühistusnimekirja profiil

Versioon 3.0
Kehtiv alates 22.06.2016

Versiooni info		
Kuupäev	**Versioon**	**Muudatused/täiendused**
22.06.2016	3.0	Kinnitatud versioon
24.03.2016	2.1	Versioon 3.0 mustand. Punkt 2.1 eemaldatud erand SHA-1 signeerimisalgoritmi kohta; Punkt 2.2.1 lisatud kvalifitseeritud sertifikaadi tunnus.
13.01.2015	2.0	Kinnitatud versioon
14.11.2014	1.5	Versioon 2.0 mustand. - punkt 2.1 - täiendatud lubatud võtmealgoritmide nimekirja; - punkt 3.1 - muudetud tühistusnimekirja signeerimisalgoritmi; - punkt 4 - täiendatud viidatud dokumentide nimekirja.
20.06.2014	1.4	- veebiserveri sertifikaadi mõiste asendatud SSL serveri sertifikaadiga; - muudetud ja täiendatud sertifikaatide tehnilist profiili; - lisatud asutuse sertifikaadi täiendavad muutumatud laiendused; - restruktureerimine
14.02.2011	1.3	- p 1 – sertifikaatide jaotusest on kustutatud Tarkvara signeerimissertifikaat - p 3.2.2 – lisatud „Data Encipherment“ väärtus autentimise ja krüpteerimise sertifikaadile. - p 3.3.2 – muudetud OID väärtust ja CPS aadress
10.05.2010	1.2	Täiendatud on punkt 1, kus on välja toodud erinevate sertifikaatide nimetused. Täpsustatud on sertifikaadi väljade kirjeldusi ja on muudetud välja „CRL Distribution Point” väärtust.
13.08.2009	1.1	Profiil on viidud vastavusse Digitaalallkirja seadusest tulenevatele nõuetele. Eemaldatud „seadmesertifikaatide“ mõiste.
15.02.2005	1.0	Esmane versioon.

1. Sissejuhatus

Käesolev dokument käsitleb KLASS3-SK CA alt väljastatavate sertifikaatide profiile ja minimaalseid nõudeid nendele. Täpse sertifikaadi profiili võib täiendavalt kokku leppida sertifikaadi taotlemisel.

Mõiste „Asutuse sertifikaat“ all mõeldakse organisatsioonile väljastatavat sertifikaati. Asutuse sertifikaadid jagunevat alljärgnevalt:

- Digitempel;
- SSL server;
- Client Autent server;
- VPN;
- Krüpto; ja
- B4B.

SSL serveri sertifikaat sobib veebi serveri (https), ftp serveri (ftps) ja teistele SSL/TLS serveritele.

1.1. Sisukord

1.2. Mõisted ja Lühendid

1.2.1. Mõisted

Vaata CPS p.10

Mõiste	Kirjeldus
Objekti identifikaator	Unikaalne objekti tunnuskood (OID).
Sertifitseerija	Sertifikaate väljastav üksus.

Mõiste	Kirjeldus
Sertifitseerimispoliitika	Reeglid, millega nähakse ette, kuidas kasutavad sertifikaati teatavad kasutajarühmad või kuidas sertifikaati kohaldatakse teatavat laadi rakenduste puhul, ning ühised turbenõuded.
Sertifitseerimispõhimõtted	Sertifitseerija sertifikaatide väljastamise, haldamise, kehtetuks tunnistamise, uuendamise ja võtmete uuendamise hea tava kirjeldus.
Jagatud kontroll	Turvameede, millega tagatakse juurdepääs turvaobjektidele vaid kahe või enama võtmeisiku samaaegsel rakendamisel.

1.2.2. Kasutatud Lühendid

Vaata CPS p.11

Lühend	Kirjeldus
CP	Sertifitseerimispoliitika (*Certification Policy*)
CPS	Sertifitseerimispõhimõtted (*Certification Practice Statement*)
CRL	Sertifikaatide tühistusnimekiri (*Certificate Revocation List*)
FQDN	Võrguseadme täielik nimi (*Fully Qualified domain name*)
OID	Objekti identifikaator, unikaalne objekti tunnuskood (*Object Identifier*)
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
EECCRCA	EE Certification Centre Root CA, SK tipmine sertifitseerija

2. Sertifikaadi tehniline profiil

Asutuse sertifikaat on koostatud vastavalt X.509 versioon 3 standardile ja soovituslikus standardis RFC 5280 [2] toodud juhistele.

2.1. Põhiväljad

Väli	OID	Kohustuslikkus	Väärtus	Muudetav	Kirjeldus
Version		jah	Version 3	ei	Sertifikaadi vormingu versiooni number
Serial Number		jah		ei	Sertifikaadi unikaalne järjenumber
Signature Algorithm	1.2.840.113549.1.1.11	jah	sha256WithRSAEncryption	ei	Sertifikaadi allkirjastamise algoritm vastavalt RFC 5280 toodule.
Issuer		jah		ei	Sertifikaadi väljastaja

Väli	OID	Kohustuslikkus	Väärtus	Muudetav	Kirjeldus
Distinguished name					eraldusnimi
Common Name (CN)	2.5.4.3	jah	KLASS3-SK 2010		Sertifitseerija nimi
Organizational Unit (OU)	2.5.4.11	jah	Sertifitseerimisteenused		AS Sertifitseerimiskeskuse teenuse liik
Organization (O)	2.5.4.10	jah	AS Sertifitseerimiskeskus		Organisatsioon
Country (C)	2.5.4.6	jah	EE		Riigi kood: EE – Eesti
Subject Distinguished Name		jah		jah	Sertifikaadi omaniku (seadme) eraldusnimi või pseudonüüm
Serial Number	2.5.4.5	jah			Sertifikaadi taotluses märgitud juriidilise isiku registri kood. SSL serveri sertifikaadi puhul seda välja ei kasutata.
Common Name (CN)	2.5.4.3	jah			Sertifikaadi üldnimi - kliendi nimi ja soovi korral kasutusfunktsioon. SSL serveri sertifikaadi puhul ei ole kohustuslik, kuid kui määratud, peab olema täidetud Subject Alternative Name väljadest kas ühe IP aadressiga või domeeninimega.
Organizational Unit (OU)	2.5.4.11	ei			Sertifikaadi taotluses märgitud organisatsiooni allüksuse nimi. Kui kasutatakse SK poolt väljastatud turvaseadet, siis toote inglise keelsed nimetused.
Organization (O)	2.5.4.10	jah			Sertifikaadi taotluses

Väli	OID	Kohustuslikkus	Väärtus	Muudetav	Kirjeldus
					märgitud kliendi (asutuse) nimetus.
Locality (L)	2.5.4.7	jah			Sertifikaadi taotluses märgitud kliendi asukoha asula nimi. Ei ole kohustuslik, kui on määratud State (S).
State (S)	2.5.4.8	jah			Sertifikaadi taotluses märgitud kliendi asukoha maakonna nimi. Ei ole kohustuslik, kui on määratud Locality (L).
Country (C)	2.5.4.6	jah			Sertifikaadi taotluses märgitud kliendi asukoha riigi kood vastavalt RFC 5280 toodud juhistele.
Valid from		jah		ei	Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud vastavalt RFC 5280 toodud juhistele.
Valid to		jah		ei	Sertifikaadi kehtivuse lõppemise aeg. Informatsioon kodeeritud vastavalt RFC 5280 toodud juhistele.
Subject Public Key		jah	RSA 2048, RSA 4096 või ECC 256, ECC 320, ECC 384, ECC 512, ECC 521	ei	RSA algoritmi alusel genereeritud avalik võti vastavalt RFC 4055 toodud juhistele. ECC avalik võti on genereeritud vastavalt RFC 5639 või FIPS Publication 186-4.
Signature		jah		ei	Sertifikaadi väljastanud sertifitseerija kinnitusallkiri.

2.2. Sertifikaadi laiendused

2.2.1. Asutuse sertifikaadi muutumatud laiendused

Laiendus (inglise keeles)	**OID**	**Väärtused ja piirangud**	**Kriitilisus**	**Kohustus-likkus**
Basic Constraints	2.5.29.19	SubjectType=End Entity Path Length Constraint=None	Mittekriitiline	jah
CRL Distribution Points	2.5.29.31	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/klass3/klass3-2010.crl	Mittekriitiline	jah
Key Usage	2.5.29.15	Vt punkt 2.2.2 "Asutuse sertifikaadi muudetavad laiendused"	Kriitiline	jah
Extended Key Usage	2.5.29.37	Vt punkt 2.2.2 "Asutuse sertifikaadi muudetavad laiendused"	Mittekriitiline	jah
AuthorityKeyIdentifier	2.5.29.35		Mittekriitiline	jah
SubjectKeyIdentifier	2.5.29.14		Mittekriitiline	jah
id-pe-qcStatements[1]	1.3.6.1.5.5.7.1.3	Kvalifitseeritud sertifikaadi tunnus. Sertifikaat peab sisaldama järgmisi tunnuseid: • Kvalifitseeritud sertifikaadi tunnus vastavalt EU digitaalallkirja direktiivile 1999/93/EC lisadele I ja II vastava {id-etsi-qcs-QcCompliance}, {0.4.0.1862.1.1} • Tunnus, mis märgib et serifikaadiga	Mittekriitiline	jah

[1] Seda laiendust sisaldab ainult Digitempli sertifikaat. See laiendus näitab, et sertifikaat on väljastatud STO poolt, mis vastab kvalifitseeritud sertifikaate väljastavale STO'le seatud tingimustele. Tunnus on koostatud vastavalt standardile ETSI TS 101 862 v 1.3.2.

Laiendus (inglise keeles)	OID	Väärtused ja piirangud	Kriitilisus	Kohustus-likkus
		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}		

2.2.2. Asutuse sertifikaadi täiendavad muutumatud laiendused

Laiendus (inglise keeles)	OID	Väärtused ja piirangud	Kriitilisus	Kohustus-likkus
Authority Information Access	1.3.6.1.5.5.7.1.1	calssuers (OID 1.3.6.1.5.5.7.48.2) http://www.sk.ee/certs/KLASS3-SK_2010_ECCRCA.pem.crt ocsp (OID 1.3.6.1.5.5.7.48.1) http://ocsp.sk.ee/ssl	Mittekriitiline	jah

2.2.3. Asutuse sertifikaadi muudetavad laiendused

Laiendus	Digitempel	SSL server	Client Autent server	VPN	Krüpto	B4B
Võtme kasutusala „Key Usage“						
Non-Repudiation	X					
Digital Signature		X	X	X	X	X
Data Encipherment			X		X	
Key Encipherment		X	X	X	X	X
Key Agreement						
Võtme laiendatud kasutusala “Extended key usage”						
Client Authentication			X	X		X
Server Authentication		X				
Code Signing						
Email Protection						
IPSEC End System				X		
IPSEC Tunnel						
IPSEC User						
Muud laiendused						

Laiendus	Digitempel	SSL server	Client Autent server	VPN	Krüpto	B4B
Subject Alternative Name[2]						
- rfc822Name			X			
- DNSName		X				
- IPAddress		X				

2.3. Sertifitseerimispoliitikad

Certificate Policies, OID 2.5.29.32

2.3.1. Üldist

Sertifitseerimispoliitika kirjeid VÕIB sertifikaadis olla rohkem kui üks.

Alam CA sertifikaadis PEAB olema sertifikaadi väljastaja sertifitseerimispoliitikat kirjeldav kirje.

2.3.2. Asutuse sertifikaadi sertifitseerimispoliitika

Element	Tüüp	Väärtus
PolicyIdentifier		1.3.6.4.1.10015.7.1.3
PolicyQualifier		
User Notice	UTF8 string	Asutuse sertifikaat. Corporate ID.
CPS		https://www.sk.ee/repository

Sertifitseerimispoliitika laiendus ei ole kriitiline.

3. Tühistusnimekirja profiil

SK väljastab tühistusnimekirju vastavalt RFC 5280 toodud juhistele.

[2] SSL serveri sertifikaadi puhul peab olema täidetud vähemalt üks Subject Alternative Name väljadest DNSName või IPAddress vähemalt ühe väärtusega. Täidetud võivad olla mõlemad ja ka mitme väärtusega. Client Autent serveri sertifikaadi puhul ei ole Subject Alternative Name e-maili väli rfc822Name kohustuslik.

3.1. Põhiväljad

Väli	OID	Kohustuslikkus	Väärtus	Kirjeldus
Version		jah	Version 2	Tühistusnimekirja vormingu versioon vastavalt X.509-le.
Signature Algorithm			sha256WithRSAEncryption	Tühistusnimekirja allkirjastamise algoritm vastavalt RFC 5280 toodule.
Issuer Distinguished Name		jah		Sertifikaadi väljastaja eraldusnimi
Common Name (CN)	2.5.4.3	jah	KLASS3-SK 2010	Sertifitseerija nimi
Organizational Unit (OU)	2.5.4.11	jah	Sertifitseerimisteenused	AS Sertifitseerimiskeskuse teenuse liik.
Organization (O)	2.5.4.10	jah	AS Sertifitseerimiskeskus	Organisatsioon
Country (C)	2.5.4.6	jah	EE	Riigikood vastavalt RFC 5280 toodud juhistele.
Effective Date				Tühistusnimekirja väljastuskuupäev ja kellaaeg. Informatsioon on kodeeritud vastavalt RFC 3280 toodud juhistele.
Next Update				Järgmise tühistusnimekirja väljastamise kuupäev ja kellaaeg. Tühistusnimekirja väljastustingimused on toodud ka KLASS3-SK CP punktis 2.4.2.
Revoked Certificates				Tühistatud sertifikaatide loetelu.
Serial Number				Tühistatud sertifikaadi number.
Revocation Date				Tühistamise kuupäev ja kellaaeg. Informatsioon kodeeritud vastavalt RFC 5280 toodud juhistele.
Reason Code	2.5.29.21			Sertifikaadi tühistamise põhjuskood. Väljal

Väli	OID	Kohustuslikkus	Väärtus	Kirjeldus
				kasutatakse järgmisi põhjuskoode: 1 – võtmekaotus (*keyCompromise*); 2 – CA võtmekaotus (*cACompromise*); 3 – nimemuutus (affiliationChanged); 4 – asendati uue sertifikaadiga (*superseded*); 5 – organisatsiooni tegevuse lõpetamine (*cessationOfOperation*).
Signatuur				Tühistusnimekirja väljastanud sertifitseerija kinnitusallkiri.

3.2. Tühistusnimekirja laiendused

Väli	OID	Väärtused ja piirangud	Kriitilisus
CRL Number	2.5.29.20	Tühistusnimekirja järjekorranumber	Mittekriitiline
Issuing Distribution Point	2.5.29.28	Tühistusnimekirja levituspunkt	Mittekriitiline

4. Viidatud ja seonduvad dokumendid

[1] AS Sertifitseerimiskeskus, sertifitseerimispõhimõtted;

[2] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[3] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[4] RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[5] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[6] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation;

[7] FIPS PUB 186-4.