Asutuse sertifikaatide ja tühistusnimekirja profiil

Versioon 1.3

Sisukord

Dokumendi versioonid

Versiooni number	*Kuupäev*	*Kirjeldus*
1.3	14.02.2011	- p.1 – sertifikaatide jaotusest on kustutatud Tarkvara signeerimissertifikaat -p3.2.2 – lisatud „Data Encipherment“ väärtus autentimise ja krüpteerimise sertifikaadile. P3.3.2 – muudetud OID väärtust ja CPS aadress
1.2	10.05.2010	Täiendatud on punkt 1, kus on välja toodud erinevate sertifikaatide nimetused. Täpsustatud on sertifikaadi väljade kirjeldusi ja on muudetud välja „CRL Distribution Point” väärtust.
1.1	13.08.2009	Profiil on viidud vastavusse Digitaalallkirja seadusest tulenevatele nõuetele. Eemaldatud „seadmesertifikaatide“ mõiste.
1.0	15.02.2005	Esimene versioon

1. Üldist

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

- **Digitaalse templi sertifikaat**

- **Veebiserveri sertifikaat**
- **Client Autent serveri sertifikaat**
- **VPN sertifikaat**
- **Krüptosertifikaat**
- **B4B sertifikaat**

Käesolev dokument käsitleb asutuse sertifikaatide profiile ja minimaalseid nõudeid nendele. Täpse sertifikaadi profiili võib täiendavalt kokku leppida sertifikaadi taotlemisel.

2. Kasutatud mõisted ja lühendid

Mõiste	*Kirjeldus*
OID	*Object Identifier* – mingile objektile antud standarditega reguleeritud tunnuskood
FQDN	*Fully Qualified domain name* – võrguseadme täielik nimi

3. Sertifikaadi tehniline profiil

Asutuse sertifikaat on koostatud vastavalt X.509 versioon 3 standardile ja soovituslikus standardis RFC 3280 [1] toodud juhistele.

3.1. Põhiväljad

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Muudetav sertifikaadi taotlemisel*	*Kirjeldus*
Version		jah	Version 3	Ei	Sertifikaadi vormingu versiooni number.
Serial Number		jah		Ei	Sertifikaadi unikaalne järjenumber
Signature Algorithm		jah		Ei	sha1withRSA
Issuer Distinguished Name		jah		Ei	Sertifikaadi väljastaja eraldusnimi
Common Name (CN)	2.5.4.3	jah	KLASS 3-SK 2010		Sertifitseerija nimi
Organizational Unit (OU)	2.5.4.11	jah	Sertifitseerimisteenused		AS Sertifitseerimiskeskuse teenuse liik

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Muudetav sertifikaadi taotlemisel*	*Kirjeldus*
Organization (O)	2.5.4.10	jah	AS Sertifitseerimiskeskus		Organisatsioon
Country (C)	2.5.4.6	jah	EE		Riigikood: EE – Eesti
E-Mail (E)		jah	pki@sk.ee		AS Sertifitseerimiskeskuse kontakt e-posti aadress
Subject Distinguished Name		jah		Jah	Sertifikaadi omaniku (seadme) eraldusnimi, nimi või pseudonüüm.
E-mail (E)					Kontakt e-posti aadress.
Serial Number	2.5.4.5	Jah			Sertifikaadi taotluses märgitud juriidilise isiku registri kood. Veebiserveri sertifikaadi puhul ei kasutata seda välja
Common Name (CN)	2.5.4.3	jah			Sertifikaadi üldnimi - kliendi nimi ja soovi korral kasutusfunktsioon. Veebisertifikaadi puhul FQDN.
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 märgitud kliendi (asutuse) nimetus.
Locality (L)	2.5.4.7	Ei			Sertifikaadi taotluses märgitud kliendi asukoha asula nimi.
State (S)	2.5.4.8	Ei			Sertifikaadi taotluses märgitud kliendi asukoha maakonna nimi.

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Muudetav sertifikaadi taotlemisel*	*Kirjeldus*
Country (C)	2.5.4.6	jah			Sertifikaadi taotluses märgitud kliendi asukoha riigi kood vastavalt RFC 3280 toodud juhistele.
Valid From		jah		Ei	Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Valid To		jah		Ei	Sertifikaadi kehtivuse lõppemise aeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Subject Public Key		jah		Ei	RSA algoritmi alusel koostatud avalik võti.
Signature		jah		Ei	Sertifikaadi väljastanud sertifitseerija kinnitusallkiri.

3.2. Sertifikaadi laiendused

3.2.1. Asutuse sertifikaadi muutumatud laiendused

Laiendus(inglise keeles)	*OID*	*Väärtused ja piirangud*	*Kriitilisus*	*Kohustuslikkus*
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Mittekriitiline	Jah
CRL Distribution Points	2.5.29.31	http://www.sk.ee/crls/klass3/klass3-2010.crl	Mittekriitiline	Jah
Key Usage	2.5.29.15	Vt punkt 3.2.2. "Asutuse sertifikaadi muudetavad laiendused"	Kriitiline	Jah
Enhanced Key Usage	2.5.29.37	Vt punkt 3.2.2. " Asutuse sertifikaadi muudetavad laiendused "	Mittekriitiline	Jah
AuthorityKeyIdentifier	2.5.29.17		Mittekriitiline	Jah
SubjectKeyIdentifier	2.5.29.35		Mittekriitiline	Jah

3.2.2. Asutuse sertifikaadi muudetavad laiendused

	Digi-Tempel	*WWW server*	*Autentimine*	*VPN*	*Krüpteerimine*	*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 *"Enhanced key usage"*					
Client Authentication			X	X		X
Server Authentication		X				
Code Signing						
Email Protection						
IPSEC End System				X		
IPSEC Tunnel						
IPSEC User						
	Muud laiendused					
	Subject Alternative Name					
- RFC822 Name			X			
- DNS name		X				
- IP		X				

3.3. Sertifitseerimispoliitikad (Certificate Policies, OID: 2.5.29.32)

3.3.1. Üldist

Sertifitseerimispoliitika kirjeid VÕIB sertifikaadis olla rohkem kui üks.
Asutuse sertifikaadis PEAB olema sertifikaadi väljastaja sertifitseerimispoliitikat kirjeldav kirje.

3.3.2. Asutuse sertifikaadi sertifitseerimispoliitika

Element	*Tüüp*	*Väärtus*
Sertifitseerija sertifitseerimispoliitika		
PolicyIdentifier		1.3.6.4.1.10015.7.1.2.2
Policy Qualifier		
User Notice	UTF8 string	Asutuse sertifikaat. Corporate ID.
CPS		http://www.sk.ee/cps

Sertifitseerimispoliitika laiendus ei ole kriitiline.

4. Tühistusnimekirja (CRL) profiil

AS Sertifitseerimiskeskus väljastab tühistusnimekirju vastavalt RFC 3280 toodud juhistele.

4.1. Põhiväljad

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
Version		jah	Version 2	Tühistusnimekirja vormingu versioon vastavalt X.509 le.
Signature Algorithm			sha1withRSA	Tühistusnimekirja allkirjastamise algoritm vastavalt RFC 3280 toodule.
Issuer Distinguished Name		jah		Sertifikaadi väljastaja eraldusnimi
Common Name (CN)	2.5.4.3	jah	KLASS 3-SK	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 3280 toodud juhistele
Effective Date				Tühistusnimekirja väljastuskuupäev ja kellaaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Next Update				Järgmise tühistusnimekirja väljastamise kuupäev ja kellaaeg. Tühistusnimekirja väljastustingimused on toodud ka käesoleva 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 3280 toodud juhistele.
Reason	2.5.29.21			Sertifikaadi tühistamise

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
Code				põhjuskood. Väljal kasutatakse järgmiseid 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

4.2. Tühistusnimekirja laiendused

Väli	*OID*	*Väärtus ja piirangud*	*Kriitilisus*
CRL Number	2.5.29.20	Tühistusnimekirja järjekorra number	Mittekriitiline
Issuing Distribution Point	2.5.29.28	Tühistusnimekirja levituspunkt	Mittekriitiline

5. Viidatud dokumendid

[1] RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile