

# Asutuse sertifikaatide ja tühistusnimekirja profiil

Versioon 1.2

## Sisukord

<b>ASUTUSE SERTIFIKAADI JA TÜHISTUSNIMEKIRJA PROFIIL.....</b>	<b>1</b>
<b>SISUKORD.....</b>	<b>1</b>
DOKUMENDI VERSIOONID .....	1
1. ÜLDIST .....	1
2. KASUTATUD MÕISTED JA LÜHENDID .....	2
3. SERTIFIKAADI TEHNILINE PROFIIL .....	2
3.1. Põhiväljad.....	2
3.2. Sertifikaadi laiendused.....	4
3.3. Sertifitseerimispoliitika (Certificate Policies, OID: 2.5.29.32).....	5
4. TÜHISTUSNIMEKIRJA (CRL) PROFIIL.....	6
4.1. Põhiväljad.....	6
4.2. Tühistusnimekirja laiendused .....	7
5. VIIDATUD DOKUMENDID .....	7

## Dokumendi versioonid

<i>Versiooni number</i>	<i>Kuupäev</i>	<i>Kirjeldus</i>
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**
- **Tarkvara signeerimissertifikaat**

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

## 2. Kasutatud mõisted ja lühendid

<i>Mõiste</i>	<i>Kirjeldus</i>
OID	<i>Object Identifier</i> – mingile objektile antud standarditega reguleeritud tunnuskoode
FQDN	<i>Fully Qualified domain name</i> – võrguseadme täielik nimi

## 3. Sertifikaadi tehniline profiil

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

### 3.1. Põhiväljad

<i>Väli</i>	<i>OID</i>	<i>Kohustuslikkus</i>	<i>Väärtused</i>	<i>Muudetav sertifikaadi taotlemisel</i>	<i>Kirjeldus</i>
Version		jah	Version 3	Ei	Sertifikaadi vormingu versiooni number.
Serial Number		jah		Ei	Sertifikaadi unikaalne järjenumbr
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
Organization (O)	2.5.4.10	jah	AS Sertifitseerimiskeskus		Organisatsioon

<i>Väli</i>	<i>OID</i>	<i>Kohustuslikkus</i>	<i>Väärtused</i>	<i>Muudetavsertifikaadi taotlemisel</i>	<i>Kirjeldus</i>
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.
Country (C)	2.5.4.6	jah			Sertifikaadi taotluses märgitud kliendi asukoha riigi kood vastavalt RFC 3280 toodud juhisteile.

<i>Väli</i>	<i>OID</i>	<i>Kohustuslikkus</i>	<i>Väärtused</i>	<i>Muudetavsertifikaadi taotlemisel</i>	<i>Kirjeldus</i>
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

<i>Laiendus( inglise keeles)</i>	<i>OID</i>	<i>Väärtused ja piirangud</i>	<i>Kriitilisus</i>	<i>Kohustuslikkus</i>
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Mittekriitiline	Jah
CRL Distribution Points	2.5.29.31	<a href="http://www.sk.ee/crls/klass3/klass3-2010.crl">http://www.sk.ee/crls/klass3/klass3-2010.crl</a>	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

	<i>DigiTe mpel</i>	<i>WWW server</i>	<i>Auten- timine</i>	<i>VPN</i>	<i>Krüpteeri mine</i>	<i>B4B</i>	<i>Tarkvara sigeerimine</i>
<b>Võtme kasutusala "Key Usage"</b>							
Non-Repudiation	X						X
Digital Signature		X	X	X	X	X	
Data Encipherment							
Key Encipherment		X	X	X	X	X	
Key Agreement							
<b>Võtme laiendatud kasutusala "Enhanced key usage"</b>							
Client Authentication			X	X		X	
Server Authentication		X					
Code Signing							X
Email Protection							
IPSEC End System				X			
IPSEC Tunnel							
IPSEC User							
<b>Muud laiendused</b>							
<b>Subject Alternative Name</b>							
- RFC822 Name			X				
- DNS name		X					
- IP		X					

### 3.3. Sertifitseerimispoliitika (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

<i>Element</i>	<i>Tüüp</i>	<i>Väärtus</i>
<b>Sertifitseerija sertifitseerimispoliitika</b>		
PolicyIdentifier		1.3.6.4.1.10015.7.1.2.1
Policy Qualifier		
User Notice	UTF8 string	Asutuse sertifikaat. Corporate ID.
CPS		<a href="http://www.sk.ee/repository/cid/">http://www.sk.ee/repository/cid/</a>

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	Sertifitseeri 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 kellaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Next Update				Järgmise tühistusnimekirja väljastamise kuupäev ja kellaeg. 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 kellaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Reason	2.5.29.21			Sertifikaadi tühistamise

<i>Väli</i>	<i>OID</i>	<i>Kohustuslikkus</i>	<i>Väärtused</i>	<i>Kirjeldus</i>
Code				põhjuskood. Väljal kasutatakse järgmiseid põhjuskode: 1 – võtmekaotus ( <i>keyCompromise</i> ); 2 – CA võtmekaotus ( <i>cACompromise</i> ); 3 – nimemuutus ( <i>affiliationChanged</i> ); 4 – asendati uue sertifikaadiga ( <i>superseded</i> ); 5 – organisatsiooni tegevuse lõpetamine ( <i>cessationOfOperation</i> ).
Signatuur				Tühistusnimekirja väljastanud sertifitseerija kinnitusallkiri

#### 4.2. Tühistusnimekirja laiendused

<i>Väli</i>	<i>OID</i>	<i>Väärtus ja piirangud</i>	<i>Kriitilisus</i>
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