SK alam CA sertifikaadi ja tühistusnimekirja profiil

Versioon 2.0

Sisukord

SK ALAM CA SERTIFIKAADI JA TÜHISTUSNIMEKIRJA PROFIIL.....1

SISUKORD 1
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. Sertifitseerimispoliitikad (Certificate Policies, OID: 2.5.29.32) 4
4. TÜHISTUSNIMEKIRJA (CRL) PROFIIL 5
4.1. Põhiväljad 5
4.2. Tühistusnimekirja laiendused 6
5. VIIDATUD DOKUMENDID 6

Dokumendi versioonid

Versiooni number	*Kuupäev*	*Kirjeldus*
2.0	17.12.2015	Muudetud punkti 1. Üldist Muudetud punkti 3. Sertifikaadi tehniline profiil Muudetud punkti 3.1. Põhiväljad Muudetud punkti 3.2. Sertifikaadi laiendused Muudetud punkti 3.3. Sertifitseerimispoliitikad (Certificate Policies, OID: 2.5.29.32) Muudetud punkti 4. Tühistusnimekirja (CRL) profiil Muudetud punkti 4.1. Põhiväljad Muudetud punkti 5. Viidatud dokumendid
1.1	01.10.2010	Esimene versioon

1. Üldist

Käesolev dokument käsitleb EE Certification Centre Root CA alt väljastatavate alam CA sertifikaatide ja OCSP Responderi 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

3. Sertifikaadi tehniline profiil

Alam CA sertifikaat või OCSP Responderi sertifikaat on koostatud vastavalt X.509 versioon 3 standardile ja soovituslikus standardis RFC 5280 [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	sha384WithRSAEncryption või sha256WithRSAEncryption	Ei	Sertifikaadi allkirjastamise algoritm vastavalt RFC 5280 toodule.
Issuer Distinguished Name		jah		Ei	Sertifikaadi väljastaja eraldusnimi
Common Name (CN)	2.5.4.3	jah	EE Certification Centre Root CA		Sertifitseerija nimi
Organizational Unit (OU)	2.5.4.11	jah	Certification services		AS Sertifitseerimiskeskuse teenuse liik (inglise keeles)
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 kontaktaadress
Subject Distinguished		jah		Jah	Sertifikaadi omaniku eraldusnimi, nimi või

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Muudetav sertifikaadi taotlemisel*	*Kirjeldus*
Name					pseudonüüm.
Common Name (CN)	2.5.4.3	jah			Vastava alam CA nimetus (nt. KLASS3-SK 2010, ESTEID 2007).
Organizational Unit (OU)	2.5.4.11	Ei			AS Sertifitseerimiskeskuse teenuse liik
Organization (O)	2.5.4.10	Jah	AS Sertifitseerimiskeskus		Sertifikaadi taotluses märgitud kliendi nimi.
Organization Identifier	2.5.4.97	Ei	NTREE-10747013	Jah	AS Sertifitseerimiskeskuse registrikood ETSI EN 319 412-1 vormingus
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	EE		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, 4096	Ei	RSA algoritmi alusel koostatud avalik võti.
Signature		Jah		Ei	Sertifikaadi väljastanud sertifitseerija kinnitusallkiri.

3.2. Sertifikaadi laiendused

Laiendus(inglise keeles)	*OID*	*Väärtused ja piirangud*	*Kriitilisus*	*Kohustus-likkus*
Basic Constraints	2.5.29.19	Subject Type=CA Path Length Constraint=0 (OCSP Responderi sertifikaadi puhul CA:False)	Kriitiline	Jah
Certificate Policies	2.5.29.32	Vastavalt peatükile 3.3	Mittekriitiline	Jah
Name Constraints	2.5.29.30		Mittekriitiline	Ei
CRL Distribution Points	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/EECCRCA.crl	Mittekriitiline	Jah
Key Usage	2.5.29.15	Certificate Signing, CRL Signing	Kriitiline	Jah
Extended Key Usage	2.5.29.37		Mittekriitiline	Ei
Authority Information Access	1.3.6.1.5.5.7.1.1		Mittekriitiline	Ei
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7.48.1.5	Tühi (NULL)	Mittekriitiline	Ei (kasutusel OCSP responderi sertitifikaadi korral)
AuthorityKeyIdentifier	2.5.29.35	Väljastaja sertifikaadi sertifikaadi SubjectKeyIdentifier väärtus	Mittekriitiline	Jah
SubjectKeyIdentifier	2.5.29.14	160-bitine SHA-1 räsi avalikust võtmest	Mittekriitiline	Jah

3.3. Sertifitseerimispoliitikad (Certificate Policies, OID: 2.5.29.32)

Sertifitseerimispoliitika kirjeid VÕIB sertifikaadis olla rohkem kui üks. Antud poliitika OID esineb end-entity sertifikaadis, näiteks OCSP Responderi puhul.

Element	*Tüüp*	*Väärtus*
Sertifitseerija sertifitseerimispoliitika		
PolicyIdentifier		1.3.6.4.1.10015.100.1

Element	*Tüüp*	*Väärtus*
Policy Qualifier		
User Notice	UTF8 string	Lühikirjeldus, milliseid sertifikaate vastava CA alt välja antakse (nt „kasutatakse isikuttõendavale dokumendile kantavate sertifikaatide väljastamiseks“)
CPS		https://www.sk.ee/cps

Sertifitseerimispoliitika laiendus ei ole kriitiline.

4. Tühistusnimekirja (CRL) profiil

AS Sertifitseerimiskeskus väljastab tühistusnimekirju vastavalt RFC 5280 toodud juhistele.

4.1. Põhiväljad

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*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	EE Certification Centre Root CA	Sertifitseerija nimi
Organizational Unit (OU)	2.5.4.11	jah	Certification services	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 kodeeritud vastavalt RFC 5280 toodud juhistele.
Next Update				Järgmise tühistusnimekirja

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
				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 5280 toodud juhistele.
Reason Code	2.5.29.21			Sertifikaadi tühistamise 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 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc5280.txt.