Asutuse digitaalse kinnituse sertifikaadi ja tühistusnimekirja profiil

Projekt. Versioon 0.1

Sisukord

Dokumendi versioonid

Versiooni number	*Kuupäev*	*Kirjeldus*
0.1	1.04.2003	Esimene versioon
0.2	12.05.2003	Terminoloogia parandused

1. Üldist

Käesolev dokument kirjeldab asutuse digitaalsete kinnituse andmist ja e-maili signeerimist võimaldava sertifikaadi profiili.

2. Kasutatud mõisted ja lühendid

Mõiste	*Kirjeldus*
OID	*Object Identifier* – mingile objektile antud standarditega reguleeritud tunnuskood

3. Sertifikaadi tehniline profiil

AS Sertifitseerimiskeskus väljastab X.509 versioon 3 sertifikaate vastavalt soovituslikus standardis RFC 2459 [1] toodud juhistele.

3.1. Põhiväljad

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
Version		jah	Version 3	Sertifikaadi vormingu versiooni number.
Serial Number		jah		Sertifikaadi unikaalne järjenumber
Signature Algorithm		jah		sha1withRSA
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: EE – Eesti
E-Mail (E)		jah	pki@sk.ee	AS Sertifitseerimiskeskuse kontaktaadress
Subject Distinguished Name		jah		Sertifikaadi omaniku (seadme) eraldusnimi)
E-mail (E)				Kontaktaadress.
Serial Number	2.5.4.5	Jah		Sertifikaadi taotluses märgitud asutuse äriregistri kood.
Common Name (CN)	2.5.4.3	jah		Sertifikaadi taotluses märgitud asutuse nimi.

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
Organizational Unit (OU)	2.5.4.11	ei		Sertifikaadi taotluses märgitud organisatsiooni allüksuse nimi.
Organization (O)	2.5.4.10	jah		Sertifikaadi taotluses märgitud asutuse nimi.
Locality (L)	2.5.4.7	ei		Sertifikaadi taotluses märgitud organisatsiooni asukoha asula nimi.
State (S)	2.5.4.8	ei		Sertifikaadi taotluses märgitud organisatsiooni asukoha maakonna nimi.
Country (C)	2.5.4.6	jah		Sertifikaadi taotluses märgitud organisatsiooni asukoha riigi kood vastavalt RFC 2459 toodud juhistele.
Valid From		jah		Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud vastavalt RFC 2459 toodud juhistele.
Valid To		jah		Sertifikaadi kehtivuse lõppemise aeg. Informatsioon kodeeritud vastavalt RFC 2459 toodud juhistele.
Subject Public Key		jah		RSA algoritmi alusel koostatud avalik võti pikkusega 1024 bitti.
Signature		jah		Sertifikaadi väljastanu sertifitseerija kinnitusallkiri.

3.2. Nimed sertifikaatides

Eraldusnimede kodeerimisel arvestatakse RFC2459-s toodud nõudmisi, mille alusel peavad kõigis alates aastast 2004 väljaantavates sertifikaatides olema nimed kodeeritud andmetüübina UTF8String. Kuni selle hetkeni on kõik nimed kodeeritud kui Unicode.

3.3. Sertifikaadi laiendused

3.3.1. Asutuse digitaalse kinnituse sertifikaadi laiendused

Laiendus(inglise keeles)	*OID*	*Väärtused ja piirangud*	*Kriitilisus*	*Kohustus-likkus*
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Mittekriitiline	Jah
CRL Distribution	2.5.29.31	http://www.sk.e	Mittekriitiline	Jah

Laiendus(inglise keeles)	*OID*	*Väärtused ja piirangud*	*Kriitilisus*	*Kohustus-likkus*
Points		e/crls/klass3/crl.crl		
Key Usage	2.5.29.15	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	Kriitiline	Jah
Enhanced Key Usage	2.5.29.37		Mittekriitiline	Jah
Client Authentication	1.3.6.1.5.5.7.3.2			Jah
Secure Email	1.3.6.1.5.5.7.3.4			
AuthorityKeyIdentifier	2.5.29.17		Mittekriitiline	Jah
SubjectKeyIdentifier	2.5.29.35		Mittekriitiline	Jah
SubjectAlternativeName	2.5.29.17			Jah
RFC822Name	[1]	Kontaktaadress		Jah

3.4. Sertifitseerimispoliitikad (*Certificate Policies, OID: 2.5.29.32*)

Element	*Tüüp*	*Väärtus*
PolicyIdentifier		AS Sertifitseerimiskeskuse poolt asutusele väljastatud asutuse signeerimispoliitika unikaalne OID. Vaata punkt 3.4.1.
Policy Qualifier		
User Notice	UTF8 string	Sertifikaadi rakendusvaldkonna kirjeldus. Näiteks: Väljastatud <<subjekti eraldusnime common name (CN) väli>> ametlike kirjade digitaalseks kinnitamiseks. Kehtib koos isiku digitaalallkirjaga.
CPS		http://www.sk.ee/signing_policies/<<signeerimispoliitika OID>>.ddoc
PolicyIdentifier		1.3.6.4.1.10015.7.1.1.1
Policy Qualifier		
User Notice	UTF8 string	Väljastatud asutuse digitaalsete kinnituste signeerimiseks vastavalt viidatud signeerimispoliitikale.
CPS		http://www.sk.ee/cps/

Sertifitseerimispoliitika laiendus ei ole kriitiline.

3.4.1. Signeerimispoliitika OID

Sertifitseerimispoliitikate väljal kasutatav signeerimispoliitika OID on asutuse signeerimispoliitika unikaalne tunnus, mis on registreeritud AS

Sertifitseerimiskeskuses vastavas registris. Signeerimispoliitika OID koosneb järgmistest komponentidest:

OID element	Sisu
1.3.6.1.4.1.10015.	AS Sertifitseerimiskeskuse OID
5.	Signeerimispoliitika tunnus
Kümnendnumber.	Organisatsiooni tunnus. Asutuse registreerimiskood äriregistris
Kümnendnumber.	Signeerimispoliitika dokumendi tunnus
Kümnendnumber	Signeerimispoliitika dokumendi versiooni tunnus

Näide:

1.3.6.1.4.1.10015.5.1.1.1

4. Tühistusnimekirja (CRL) profiil

AS Sertifitseerimiskeskus väljastab tühistusnimekirju vastavalt RFC 2459 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 2459 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 2459 toodud juhistele
Effective Date				Tühistusnimekirja väljastuskuupäev ja kellaaeg. Informatsioon kodeeritud

Väli	*OID*	*Kohustuslikkus*	*Väärtused*	*Kirjeldus*
				vastavalt RFC 2459 toodud juhistele.
Next Update				Järgmise tühistusnimekirja väljastamise kuupäev ja kellaaeg. Tühistusnimekirja väljastustingimused on toodud ka käesoleva CP punktis…….
Revoked Certificates				Tühistatud sertifikaatide loetelu.
Serial number				Tühistatud sertifikaadi number
Revocation date				Tühistamise kuupäev ja kellaaeg. Informatsioon kodeeritud vastavalt RFC 2459 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 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile