Sertifikaadid Eesti Vabariigi isikutunnistusel

Kehtiv alates 1.jaanuarist 2010

Versioon 3.3

SISUKORD

ÜLDIST

Käesolev dokument kirjeldab Eesti Vabariigi isikutunnistusele (ID-kaart) kantavate digitaalsete sertifikaatide profiili. Standardi lisas A esitatakse tehniline lisainformatsioon ning tuuakse ära sertifikaatide näidised.

Antud dokument ei käsitle teisi isikutunnistuses sisalduvaid andmekogumeid.

Käesoleva profiili koostamisel on lähtutud järgmistest alusdokumentidest:

A. Eesti Vabariigi seadused

1) isikut tõendavate dokumentide seadus (RT I 1999, 25, 365; 2006, 29, 221);
2) digitaalallkirja seadus (RT I 2000, 26, 150; 92, 597; 2007, 24, 127);
3) isikuandmete kaitse seadus (RT I 2007, 24, 127);
4) Teede- ja Sideministeeriumi 3. oktoobri 2000.a määrus nr 83 “Teenuse osutajate infosüsteemide auditeerimise kord” (RTL 2000, 108, 1655);

B. IETFi (Internet Engineering Task Force http://www.ietf.org) **dokumendid**

1) RFC3280 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile (http://www.ietf.org/rfc/rfc3280.txt);
2) RFC3039 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile (http://www.ietf.org/rfc/rfc3039.txt).

1 TERMINID JA MÄÄRATLUSED

Kasutatakse järgmisi termineid ja määratlusi.

Mõiste	**Seletus**
isikutunnistus, ID-kaart	isikut tõendavate dokumentide seaduse alusel väljastatav isikut tõendav dokument;
isikutunnistuse kehtivusperiood	ajavahemik isikutunnistuse väljastamise hetkest kuni tema väljastamisel määratud kehtivuse lõpptähtajani. Isikutunnistuse tegelik kehtivusaeg võib olla lühem võimaliku kehtetuks tunnistamise tõttu;
SR	Sertifitseerimise Register (digitaalallkirja seaduse alusel);
STO	Sertifitseerimisteenuse osutaja digitaalallkirja seaduse mõttes;
OID	mingile objektile antud standarditega reguleeritud tunnuskood (*inglise keeles: Object Identificator*)
eraldusnimi	sertifikaadi omaniku või väljastaja unikaalne nimi sertifikaatide infrastruktuuris;
sertifikaat	digitaalne dokument, milles avalik võti seotakse üheselt selle omanikuga;
sertifikaadi väljaandja	sertifikaadi väljastanud STO;

Mõiste	Seletus
signeerimissertifikaat	STO sertifikaat, millega signeeritakse tema poolt välja antud sertifikaadid;
sertifikaadi omanik	subjekt, kellele konkreetne sertifikaat on välja antud;
sertifikaadi kehtivusperiood	ajavahemik sertifikaadi moodustamisest kuni tema väljastamisel määratud kehtivuse lõpptähtajani. Sertifikaadi tegelik kehtivusaeg võib olla lühem võimaliku kehtetuks tunnistamise tõttu.

2 SERTIFIKAATIDE LOETELU JA OTSTARVE

Isikutunnistusele kantakse kaks sertifikaati:

1) sertifikaat isiku digitaalseks tuvastamiseks, e-posti signeerimiseks ja krüpteerimiseks;
2) sertifikaat digitaalseks allkirjastamiseks, millega saab sertifikaadi omanik anda digitaalallkirja digitaalallkirja seaduse mõttes.

Sertifikaate väljastab sertifitseerimisteenuse osutaja,

a) kes vastab digitaalallkirja seaduses toodud nõuetele;
b) kes vastab Teede- ja Sideministeeriumi 3. oktoobri 2000.a määruses nr 83 "**Teenuse osutajate infosüsteemide auditeerimise kord**" esitatud nõuetele;
c) kes vastab "Euroopa Parlamendi ja Nõukogu direktiiv 1999/93/EÜ, 13.detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta" toodud kvalifitseeritud sertifikaatide väljaandja (qualified certificate issuer) toodud nõuetele.

3 ANDMED SERTIFIKAATIDES

Mõlemasse sertifikaati kantakse kohustuslikult järgmised andmed:

1) sertifikaadi väljaandja andmed;
2) sertifikaadiomaniku andmed;
3) sertifikaadi tehnilised andmed.

Sertifikaati kantavate andmete kooslust kirjeldatakse täpsemalt punktides 4.1 kuni 4.3 ja tehnilisi detaile lisas A.

3.1 Väljaandja andmed

Sertifikaatidesse kantakse järgmised kohustuslikud väljaandja (STO) andmed:

Atribuut	Atribuudi OID	ASN.1 tüüp	Kirjeldus	Näide
C (countryName)	{id-at-countryName} { 2,5,4,6 }	DirectoryString: PrintableString	Maatähis	EE
O (organization)	{id-at-organization} { 2,5,4,10}	DirectoryString: PrintableString	Sertifitseerimis-teenuse osutaja nimi, mis on äriregistris ja SRR-is	AS Sertifitseeri-miskeskus
OU (organizationUnit)	{id-at-organizationalUnit } { 2,5,4,11}	DirectoryString: PrintableString	Sertifitseerimisteenuse nimi	ESTEID
CN (commonName)	{id-at-commonName} { 2,5,4,3 }	DirectoryString: PrintableString	Sertifitseerimisteenuse sertifitseerija eraldusnimi	ESTEID-SK

Sertifikaatidesse võidakse kanda lisaks järgmised väljaandja (STO) andmed:

Atribuut	Atribuudi OID	ASN.1 tüüp	Kirjeldus	Näide
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: PrintableString	SRR registrikood	1
E (e-mailAddress)	{1,2,840,113549,1 ,9,1}	DirectoryString: IA5String	Sertifitseerimisteenuse osutaja e-posti aadress.	pki@sk.ee

3.2 Sertifikaadiomaniku andmed

Sertifikaadiomaniku eraldusnimes esitatakse sertifikaatides kohustuslikult järgmised atribuudid:

Atribuut	Atribuudi OID	ASN.1 tüüp	Kirjeldus	Näide
C (countryName)	{id-at-countryName} { 2,5,4,6 }	DirectoryString: PrintableString	Maatähis	EE
O (organization)	{id-at-organization} { 2,5,4,10}	DirectoryString: PrintableString	Sertifikaadi tüüp	ESTEID
OU (organizationUnit)	{id-at-organizationalUnit } { 2,5,4,11}	DirectoryString: PrintableString	Sertifikaadi kasutusvaldkond	isikutuvastussertifikaadis: *authentication* digitaalset allkirja võimaldavas sertifikaadis: *digital signature*
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: BMPString või UTF8* või PrintableString	Perekonnanimed	MÄNNIK
G (givenName)	{id-at-givenName} { 2,5,4,42 }	DirectoryString: BMPString või UTF8* või PrintableString	Eesnimed	MARI-LIIS
S (serialNumber)	{id-at-serialNumber} { 2,5,4,5 }	DirectoryString: PrintableString	Isikukood	47101010033
CN (commonName)	{id-at-commonName} { 2,5,4,3 }	DirectoryString: BMPString või UTF8* või PrintableString	Perekonna- ja eesnimed, isikukood (eraldatud komaga)	MÄNNIK,MARI-LIIS,47101010033

3.3 Sertifikaadi tehnilised andmed

Sertifikaadi tehniliste andmetena kantakse sertifikaatidesse järgmised andmed:

1) sertifikaadi vormingu versioon;
2) sertifikaadi STO-põhine järjekorranumber;
3) sertifikaadi signeerimisalgoritm;
4) sertifikaadi kehtivusperiood;
5) sertifikaadis sisalduv avalik võti ja selle esitusalgoritm;
6) STO avaliku võtme identifikaator;
7) isiku avaliku võtme identifikaator;
8) sertifikaadi põhikasutusvaldkond;
9) sertifitseerimispõhimõtete identifikaator ja viide;
10) tühistusnimekirjade levituspunkti viide;
11) isiku e-posti aadress (ainult isiku digitaalseks tuvastamiseks kasutatavas sertifikaadis);
12) STO lisanimi;
13) sertifikaadi täiendav kasutusvaldkond (ainult isiku digitaalseks tuvastamiseks kastutatavas sertifikaadis);
14) kvalifitseeritud sertifikaadi tunnus.

* BMPString või UTF8 tüüpi kodeeringut kasutatakse siis, kui nimes esineb tähti, mida ei ole ASCII7 kooditabelis.

Lisa A
SERTIFIKAADIKOHANE TEHNILINE LISAINFORMATSIOON

A.1 Üldist

Järgnevalt esitatakse detailsemalt sertifikaadi andmeväljade sisu. Kursiivkirjas on toodud vastavad inglisekeelsed terminid.

A.2 Sertifikaadi põhiväljad

A.2.1 Sertifikaadi vormingu versioon *(version)*

Väljal esitatakse sertifikaadi vormingu versiooni number.

Isikutunnistuses kasutatakse X.509 v3 sertifikaate, seega välja väärtuseks seatakse 2.

A.2.2 Sertifikaadi STO-põhine järjekorranumber *(serialNumber)*

Väljal esitatakse sertifikaadi järjekorranumber, mis ühe STO poolt välja antud sertifikaatide hulgas peab olema unikaalne.

A.2.3 Sertifikaadi signeerimisalgoritm *(signatureAlgorithm)*

Väljaga määratakse ära krüptoalgoritm, mida STO kasutab väljastatavate sertifikaatide signeerimiseks.

Isikutunnistuse sertifikaatides kasutatakse algoritmi SHA-1 ning välja väärtuseks on seega:

- **sha1WithRSAEncryption** { 1, 2, 840, 113549, 1, 1, 5 }.

A.2.4 Sertifikaadi kehtivusperiood *(validity)*

Sertifikaatidesse kantakse sertifikaadi kehtivusaeg, mille jooksul STO garanteerib sertifikaadi kehtivusinfo levitamise. Sertifikaadid kehtivad üldjuhul ***1825 päeva (5 aastat***) sertifikaadi väljastamisest, kuid mitte kauem kui isikutunnistus.

Kuupäevad sertifikaadis esitatakse vastavalt RFC3280-le.

A.2.5 Sertifikaadis sisalduv avaliku võti ja selle esitusalgoritm *(subjectPublicKeyInfo)*

Väli sisaldab sertifikaadiomaniku avaliku võtit koos selle esitusalgoritmiga.

Krüptoalgoritmina kasutatakse (**AlgorithmIdentifier** väljal) isikutunnistuse sertifikaatides:

- **rsaEncryption** { 1, 2, 840, 113549, 1, 1, 1 }.

A.3 Sertifikaadi laiendused

Kasutatavad sertifikaadilaiendused on toodud järgnevas tabelis:

Laienduse nimi	Täpne ASN.1 nimi ja OID	Esitus	Kriitiline
AuthorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2,5,29,35}	**JAH**	EI OLE
SubjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2,5,29,14}	**JAH**	EI OLE
KeyUsage	{id-ce-keyUsage} {2,5,29,15}	**JAH**	**ON**
CertificatePolicies	{ id-ce-certificatePolicies} {2,5,29,32}	**JAH**	EI OLE
SubjectAltName (isiku digitaalseks tuvastamiseks ettenähtud sertifikaadis)	**{** id-ce-subjectAltName} {2,5,29,17}	**JAH**	EI OLE
IssuerAltName	**{** id-ce-issuerAltName} {2,5,29,18}	**JAH**	EI OLE
CRLDistributionPoints	**{**id-ce-CRLDistributionPoints} {2,5,29,18}	**JAH**	EI OLE
ExtKeyUsage (isiku digitaalseks tuvastamiseks ettenähtud sertifikaadis)	{id-ce-extKeyUsage} {2,5,29,37}	**JAH**	**ON**
ExtKeyUsage (digitaalseks allkirjastamiseks ettenähtud sertifikaadis)	{id-ce-extKeyUsage} {2,5,29,37}	**EI**	EI OLE
BasicConstraints	{id-ce-basicConstraints} {2,5,29,18}	**JAH**	EI OLE
qcStatements	{id-pe-qcStatements} {1,3,6,1,5,5,7,1,3}	**JAH**	EI OLE

Laienduse juures tähendab märge “Esitus” laienduse olemasolu või selle puudumist sertifikaadis.

Kui laiendus on olemas, siis märge “kriitiline” tähendab seda, et sertifikaati käsitlevad tarkvararakendused peavad alati kontrollima selle sisu.

A.3.1 STO avaliku võtme identifikaator *(authorityKeyIdentifier)*

Väljal esitatakse STO vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud sertifikaadi signeerimiseks) identifikaator, mis on oluline STO sertifikaatide ahela loomiseks.

Kasutatakse ainult **keyIdentifier** välja.

See on mittekriitiline laiendus.

A.3.2 Isiku avaliku võtme identifikaator *(subjectKeyIdentifier)*

Väljal esitatakse antud sertifikaadis sisalduva avaliku võtme identifikaator, mis on vajalik selle avaliku võtme kiireks identifitseerimiseks (juhul, kui sertifikaadiomanikul on antud STO käest võetud mitu sertifikaati).

Vastavalt RFC3280-le kasutatakse meetodit 1.

See on mittekriitiline laiendus.

A.3.3 Sertifikaadi põhikasutusvaldkond *(keyUsage)*

Sertifikaatides kasutatakse väärtusi

- **DigitalSignature,**
- **NonRepudiation,**
- **KeyEncipherment,**
- **DataEncipherment,**

järgmiselt:

Isiku digitaalseks tuvastamiseks mõeldud sertifikaadis kasutatakse väärtusi

- DigitalSignature,
- KeyEncipherment,
- dataEncipherment,

Digitaalseks allkirjastamiseks mõeldud sertifikaadis kasutatakse ainult väärtust

- nonRepudiation.

See on **kriitiline** laiendus.

A.3.4 Sertifitseerimispõhimõtted *(certificatePolicies)*

Väljal esitatakse viide sertifitseerimispõhimõtetele, mille alusel sertifikaat on välja antud. Viites antakse vastav *URL* ja *OID*- identifikaator.

See on mittekriitiline laiendus.

A.3.5 Tühistusnimekirjade levituspunktid *(cRLDistributionPoints)*

Väli viitab STO poolt väljastatava ja antud sertifikaatidega seotud sertifikaatide tühistusnimekirjale (täpsemalt *Certificate Revocation List - CRL* asukohale *URL*-ina). Juurdepääsuprotokollina võib olla kasutusel nii LDAP kui HTTP.

See on mittekriitiline laiendus.

A.3.6 Isiku e-posti aadress *(Subject Alternative Name)*

Väljal esitatakse sertifikaadi omaniku e-posti aadress. E-posti aadress sisaldub vaid isiku digitaalseks tuvastamiseks kasutatavas sertifikaadis.

E-posti aadress luuakse isiku ees- ja perekonnanime(de)st (eesnimed.perekonnanimed@eesti.ee) vastavalt sertifikaadis G ja SN väljadel olevatele väärtustele, teostades eelnevalt vajalikud teisendused vastavalt käesolevale punktile. Korduvate nimede puhul, kui samade nimedega e-posti aadress on juba väljastatud, lisatakse nimedele järjestikuline kümnendarv järgmises vormis: eesnimed.perekonnanimed.N@eesti.ee. Alamdomeeniks on eesti.ee.

Aadressis on iga nime eraldavaks ühikuks punkt. Juhul, kui nimes on sidekriips, kasutatakse sidekriipsu. Muud märgid peale sidekriipsu asendatakse punktiga.

Nimedes tehakse järgmiste tähemärkide puhul asendused:

jrk	Täht	Tähekood	Asendustäht	Asenduskood
1	A	0041		
2	a	0061		
3	B	0042		
4	b	0062		
5	C	0043		
6	c	0063		
7	D	0044		
8	d	0064		
9	E	0045		
10	e	0065		
11	F	0046		
12	f	0066		
13	G	0047		

14	g	0067		
15	H	0048		
16	h	0068		
17	I	0049		
18	i	0069		
19	J	004A		
20	j	006A		
21	K	004B		
22	k	006B		
23	L	004C		
24	l	006C		
25	M	004D		
26	m	006D		
27	N	004E		
28	n	006E		
29	O	004F		
30	o	006F		
31	P	0050		
32	p	0070		
33	Q	0051		
34	q	0071		
35	R	0052		
36	r	0072		
37	S	0053		
38	s	0073		
39	Š	0160	S	0053
40	š	0161	s	0073
41	Z	005A		
42	z	007A		
43	Ž	017D	Z	005A
44	ž	017E	z	007A
45	T	0054		
46	t	0074		
47	U	0055		
48	u	0075		
49	V	0056		
50	v	0076		
51	W	0057		
52	w	0077		
53	Õ	00D5	O	004F
54	õ	00F5	o	006F
55	Ä	00C4	A	0041
56	ä	00E4	a	0061
57	Ö	00D6	O	004F
58	ö	00F6	o	006F

59	Ü	00DC	U	0055
60	ü	00FC	u	0075
61	X	0058		
62	x	0078		
63	Y	0059		
64	y	0079		
65	À	00C0	A	0041
66	à	00E0	a	0061
67	Á	00C1	A	0041
68	á	00E1	a	0061
69	Â	00C2	A	0041
70	â	00E2	a	0061
71	Ã	00C3	A	0041
72	ã	00E3	a	0061
73	Ā	0100	A	0041
74	ā	0101	a	0061
75	Ă	0102	A	0041
76	ă	0103	a	0061
77	Å	00C5	A	0041
78	å	00E5	a	0061
79	Ą	0104	A	0041
80	ą	0105	a	0061
81	Æ	00C6	A	0041
82	æ	00E6	a	0061
83	Ć	0106	C	0043
84	ć	0107	c	0063
85	Č	010C	C	0043
86	č	010D	c	0063
87	Ç	00C7	C	0043
88	ç	00E7	c	0063
89	Ď	010E	D	0044
90	ď	010F	d	0064
91	Đ	0110	DJ	0044; 004A
92	đ	0111	dj	0064; 006A
93	Ð	00D0	DH	0044; 0048
94	ð	00F0	dh	0064; 0068
95	È	00C8	E	0045
96	è	00E8	e	0065
97	É	00C9	E	0045
98	é	00E9	e	0065
99	Ê	00CA	E	0045
100	ê	00EA	e	0065
101	Ē	0112	E	0045
102	ē	0113	e	0065
103	Ė	0116	E	0045

104	ė	0117	e	0065
105	Ë	00CB	E	0045
106	ë	00EB	e	0065
107	Ě	011A	E	0045
108	ě	011B	e	0065
109	Ę	0118	E	0045
110	ę	0119	e	0065
111	Ğ	011E	G	0047
112	ğ	011F	g	0067
113	Ģ	0122	G	0047
114	ģ	0123	g	0067
115	Ì	00CC	I	0049
116	ì	00EC	i	0069
117	Í	00CD	I	0049
118	í	00ED	i	0069
119	Î	00CE	I	0049
120	î	00EE	i	0069
121	Ī	012A	I	0049
122	ī	012B	i	0069
123	İ	0130	I	0049
124	ı	0131	i	0069
125	Ï	00CF	I	0049
126	ï	00EF	i	0069
127	Į	012E	I	0049
128	į	012F	i	0069
129	Ķ	0136	K	004B
130	ķ	0137	k	006B
131	Ĺ	0139	L	004C
132	Í	013A	l	006C
133	Ľ	013D	L	004C
134	ľ	013E	l	006C
135	Ļ	013B	L	004C
136	ļ	013C	l	006C
137	Ł	0141	L	004C
138	ł	0142	l	006C
139	Ń	0143	N	004E
140	ń	0144	n	006E
141	Ñ	00D1	N	004E
142	ñ	00F1	n	006E
143	Ň	0147	N	004E
144	ň	0148	n	006E
145	Ņ	0145	N	004E
146	ņ	0146	n	006E
147	Ò	00D2	O	004F
148	ò	00F2	o	006F

149	Ó	00D3	O	004F
150	ó	00F3	o	006F
151	Ô	00D4	O	004F
152	ô	00F4	o	006F
153	Ō	014C	O	004F
154	ō	014D	o	006F
155	Ő	0150	O	004F
156	ő	0151	o	006F
157	Ø	00D8	O	004F
158	ø	00F8	o	006F
159	Œ	0152	OE	004F; 0045
160	œ	0153	oe	006F; 0065
161	Ŕ	0154	R	0052
162	ŕ	0155	r	0072
163	Ř	0158	R	0052
164	ř	0159	r	0072
165	Ŗ	0156	R	0052
166	ŗ	0157	r	0072
167	Ś	015A	S	0053
168	ś	015B	s	0073
169	Ş	015E	S	0053
170	ş	015F	s	0073
171	ß	00DF	ss	0073; 0073
172	Ť	0164	T	0054
173	ť	0165	t	0074
174	Ţ	0162	T	0054
175	ţ	0163	t	0074
176	Þ	00DE	TH	0054; 0048
177	þ	00FE	th	0074; 0068
178	Ù	00D9	U	0055
179	ù	00F9	u	0075
180	Ú	00DA	U	0055
181	ú	00FA	u	0075
182	Û	00DB	U	0055
183	û	00FB	u	0075
184	Ū	016A	U	0055
185	ū	016B	u	0075
186	Ů	016E	U	0055
187	ů	016F	u	0075
188	Ű	0170	U	0055
189	ű	0171	u	0075
190	Ų	0172	U	0055
191	ų	0173	u	0075
192	Ý	00DD	Y	0059
193	ý	00FD	y	0079

194	Ÿ	0178	Y	0059
195	ÿ	00FF	y	0079
196	Ź	0179	Z	005A
197	ź	017A	z	007A
198	Ż	017B	Z	005A
199	ż	017C	z	007A

Tabelis on toodud rahvusvahelises standardis ISO/IEC 10646 (Unicode'is) määratletud UTF-32 kodeeringus tähekoodid kuueteistkümnendkujul.

E-posti aadresside näidised:

- Mari-Liis Männik: mari-liis.mannik@eesti.ee
- Jaan Tamm: jaan.tamm.2@eesti.ee

See on mittekriitiline laiendus.

A.3.7 STO lisanimi *(Issuer Alternative Name)*

Välja väärtus saadakse STO vastava signeerimissertifikaadi väljalt *SubjAltName* ning ta esitab lisainformatsiooni STO kohta.

See on mittekriitiline laiendus.

A.3.8 Sertifikaadi lisakasutusvaldkond *(Extended Key Usage)*

Isiku digitaalseks tuvastamiseks mõeldud sertifikaadis kasutatakse järgmisi väärtusi:

- **ClientAuthentication,**
- **SecureEmail.**

See on isiku digitaalseks tuvastamiseks kasutatavas sertifikaadis **kriitiline** laiendus.

Digitaalseks allkirjastamiseks kasutatavas sertifikaadis see laiendus puudub.

A.3.9 Põhipiirangud *(Basic Constraints)*

See laiendus näitab, et antud sertifikaadi omanikuks on lõppkasutaja.

See on mittekriitiline laiendus.

A.3.10 Kvalifitseeritud sertifikaadi tunnus *(qcStatements)*

See laiendus näitab, et sertifikaat on väljastatud STO poolt, mis vastab kvalifitseeritud sertifikaate väljastava STO'le seatud tingimustele. Tunnus on koostatud vastavalt standardile ETSI TS 101 862 v 1.3.2.

Digitaalset allkirjastamist võimaldav sertifikaat sisaldab vähemalt järgmist tunnust:

- **EU digitaalallkirja direktiivile 1999/93/EC lisadele I ja II vastava kvalifitseeritud sertifikaadi tunnus** {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1}

See on mittekriitiline laiendus.

A.4 Sertifikaatide tühistusnimekirjade profiil

Sertifikaatide tühistusnimekirja (*CRL*) formaadiks on x.509v2 (defineeritud RFC3280-s).

STO poolt tühistusnimekirja koostamisel järgitakse ka antud dokumendis toodud soovitusi.

A.4.1 CRL-i laiendused

Kõik STO poolt väljastatavad CRL-id peavad sisaldama kohustuslikult välju:

- **Authority Key Identifier** {id-ce-authorityKeyIdentifier}, {2,5,29,35};
- **CRL number** {id-ce-cRLNumber}, {2,5,29,20}.

Väljal **authorityKeyIdentifier** esitatakse STO vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i signeerimiseks) identifikaator, mis on oluline STO sertifikaatide ahela loomiseks.

Väli **CRLnumber** on monotoonselt kasvav arv ning määrab konkreetse, STO poolt välja antud, CRL-i järjekorranumbri.

STO võib välja anda ka *deltaCRL*-e, järgides RFC3280-s esitatud nõudeid. *DeltaCRL*-i olemus on esitatud samas RFC-s.

Samuti võib STO võimalusel kasutada ka *CRL Entry* laiendusi, järgides RFC3280-s esitatud nõudeid ja soovitusi.

A.5 Näitesertifikaadid

Järgnevalt esitatakse eeltoodud profiili alusel loodud sertifikaadinäidised.

A.5.1 Digitaalset isikutuvastamist võimaldav sertifikaat

SERTIFIKAADI VÄLI	SISUNÄIDE
SERTIFIKAADI VORMINGU VERSIOON	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	3BD9 1AEB
STO ERALDUSNIMI	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	28. jaanuar 2007 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	31. jaanuar 2012 23:59:59
SERTIFIKAADI ERALDUSNIMI	Serial Number=47101010033 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS,47101010033 OU = authentication O = ESTEID C = EE
AVALIK VÕTI	RSA(1024 bits) 3081 8902 8181 00C2 AFE1 0488 4987 6C2D 4382 78FF D4E6 9F2C AEE7 2676 F3E7 33C1 8A38 706C 0F95 DF89 596A 95B8 B808 5A09 9FC7 4390 B642 AE78 AB46 00AF 647A 283B 7A44 7E25 1827 C0F5 06A0 30C1 75C1 8159 FAC5 455F 6BDB 844A 8665 1A36 2126 1370 A480 E9D5 719C 6F7D E8F5 04BF 87BF 25C3 3F20 9635 A273 05EE EB64 20BE A39E 42C6 B1D2 58A6 5425 B302 0301 0001
SERTFIKAADI LISAKASUTUSVALDKOND	Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4)
TÜHISTUSNIMEKIRJADE LEVITUSPUNKTID	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
ISIKU E-POSTI AADRESS	RFC822 Name=mari-liis.mannik@eesti.ee
SERTIFITSEERIMISPÕHIMÕTTED	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
KVALIFITSEERITUD SERTIFIKAADI TUNNUS	id-etsi-qcs-QcCompliance
SERTIFIKAADI PÕHISKASUTUS-VALDKOND	Digital Signature , Key Encipherment , Data Encipherment(B0)
PÕHIPIIRANGUD	Subject Type=End Entity Path Length Constraint=None
RÄSI ALGORITM	sha1
RÄSI	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1

A.5.2 Digitaalset allkirjastamist võimaldav sertifikaat

SERTIFIKAADI VÄLI	SISUNÄIDE
SERTIFIKAADI VORMINGU VERSIOON	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	3BD9 1AEB
STO ERALDUSNIMI	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	28.jaanuar 2007 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	31.jaanuar 2012 23:59:59
SERTIFIKAADI ERALDUSNIMI	Serial Number=47101010033 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS, 47101010033 OU = digital signature O = ESTEID C = EE
AVALIK VÕTI	RSA(1024 bits) 3081 8902 8181 00CD 8EAE 9276 61D2 FAB8 BC78 7F56 62F2 C43E 55E2 5E8A 1C75 B373 EEAB 5BAC A563 BF55 4CEE 1EA5 1F54 933F 1969 D50D 2595 52EC A878 4DD8 B121 9A1D B872 9B76 22AB A299 A982 1AA5 0DBB 501F 2B5A 3387 DB2A A75B 56D3 DFD3 E486 2565 5E6A E390 355E 6327 7EF4 5806 6854 F2F2 1FA1 F744 5457 9C62 6F47 3BA4 12F4 5548 2696 4827 3990 0302 0301 0001
TÜHISTUSNIMEKIRJADE LEVITUSPUNKTID	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
SERTIFITSEERIMISPÕHIMÕTTED	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
KVALIFITSEERITUD SERTIFIKAADI TUNNUS	id-etsi-qcs-QcCompliance
SERTIFIKAADI PÕHIKASUTUS-VALDKOND	Non-Repudiation(40)
PÕHIPIIRANGUD	Subject Type=End Entity Path Length Constraint=None
RÄSI ALGORITM	sha1
RÄSI	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1