Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel

Versioon 6.0
Kehtiv alates 1. jaanuarist 2016

Versiooni info		
Kuupäev	**Versioon**	**Muudatused/täiendused**
01.01.2016	6.0	Punktis 3.2 muudetud sertifikaadiomaniku andmete ASN.1 tüüpe. Punktis 4 uuendatud viidatud ja seonduvate dokumentide viiteid. Lisas A punktis 2.3 täiendatud kasutatavate sertifikaadi signeerimisalgoritmide nimekirja. Lisas A punktis A.2.5 täiendatud sertifikaadis sisalduva avaliku võtme pikkusi. Lisas A punktis A.3 uuendatud sertifikaadi laiendused. Lisas A punktis A.3.4 täiendatud sertifitseerimispõhimõtted. Lisas A punktis A.3.7 täiendatud STO lisanime kirjeldust. Lisas A punktis A.3.10 muudetud kvalifitseeritud sertifikaadi tunnuse kasutust. Lisas A punktides A.5.1 ja A.5.2 parandatud näitesertifikaatide kirjeldusi.
01.01.2015	5.0	Punktis 4.1 uuendatud viited Eesti Vabariigi seadustele. Lisas A punktis A.2.3 eemaldatud SHA-1 kasutatavate sertifikaatide signeerimisalgoritmide nimekirjast.
01.12.2014	4.0	Muudetud dokumendi nimi. Parandatud dokumendi sõnastust ja vormindust. Dokument viidud vastavusse dokumendiga RFC5280. Punktis 1 täpsustatud käesoleva dokumendi sisu. Punktis 1.2.1 lisatud uued mõisted Residendi digi-ID, E-residendi digi-ID, E-residendi mobiil-ID, Dokument; ära kaotatud mõisted Isikutunnistus ja Isikutunnituse kehtivusperiood. Punktis 3.1 parandatud sertifikaadis sisalduvaid väljaandja andmeid. Punktis 3.2 parandatud sertifikaadis sisalduvaid sertifikaadiomaniku andmeid. Lisas A punktis A.2.3 täiendatud kasutatavate sertifikaadi signeerimisalgoritmide nimekirja. Lisas A punktis A.2.4 muudetud sertifikaatide kehtivusperioodi kirjeldust. Lisas A punktis A.2.5 täiendatud sertifikaadis sisalduvate avalike võtmete ja nende esitusalgoritmide nimekirja. Lisas A punktides A.5.1 ja A.5.2 parandatud näitesertifikaatide kirjeldusi.

01.06.2014	3.5	Kõik versiooni 3.4 planeeritud muudatused viiakse sisse versiooni 3.5, välja arvatud Mobiil-ID sertifikaatide kehtivusaja piiramine.
01.05.2014	3.4	Lisatud versiooni info tabel. Viidatud ja seonduvad dokumendid viidud eraldi punkti 4 alla. Parandatud dokumendi sõnastust ja vormindust. Punktis 1 täpsustatud käesoleva dokumendi sisu. Punktis 1.2.1 lisatud uued mõisted EL-kaart, Digi-ID, Mobiil-ID, parandatud mõisted ID-kaart ja Isikutunnistus. Lisas A punktis A.2.4 lahti kirjutatud erinevate dokumentide sertifikaatide kehtivusperioodid. Lisas A punktis A.3.6 täiendatud isiku e-posti aadressi loomise reegleid punkti kasutamise osas (muudatus kehtib alates 28.02.2013). Lisas A punktis A.3.10 täiendatud kvalifitseeritud sertifikaadi tunnuse laiendusi (muudatus kehtib alates 28.02.2013). Lisas A punktides A.5.1 ja A.5.2 täiendatud näitesertifikaatides kvalifitseeritud sertifikaadi tunnuseid (muudatus kehtib alates 28.02.2013). **See versioon ei hakanud kunagi kehtima, kuna selle eelduseks olnud määrust mobiil-ID vormis digitaalse isikutunnistuse väljaandmise üksikasjade kohta, millega oli plaanis muuta perioodil 01.05.2014 kuni 31.12.2014 väljaantavate Mobiil-ID sertifikaatide kehtivusaega, Vabariigi Valitsus vastu ei võtnud.**
01.01.2010	3.3	Versioon avalikustamiseks.

1. Sissejuhatus

Käesolev dokument kirjeldab Eesti Vabariigi isikut tõendavatele dokumentidele kantavate digitaalsete sertifikaatide profiilid. Standardi lisas A esitatakse tehniline lisainformatsioon ning tuuakse ära sertifikaatide näidised.

Antud dokument ei käsitle teisi isikut tõendavates dokumentides sisalduvaid andmekogumeid.

1.1. Sisukord

1.2. Mõisted ja lühendid

Kasutatakse järgmisi termineid ja määratlusi.

1.2.1. Mõisted

Vaata CPS p.10

Mõiste	Kirjeldus
ID-kaart	ID-kaart on Eesti kodaniku ja Eestis püsivalt elava Euroopa Liidu kodaniku kohustuslik isikut tõendav dokument.
EL-kaart	Elamisloakaart on Eestis kehtiva elamisloa või viibimisloa alusel püsivalt elava välismaalase kohustuslik isikut tõendav dokument, mida väljastatakse aastast 2011.
Digi-ID	Digitaalne isikutunnistus on ID-kaardiga analoogiline kiipkaart, millega saab elektroonilises keskkonnas oma isikut tuvastada ja anda digitaalset allkirja.
Residendi digi-ID	Digitaalne isikutunnistus, mis on väljastatud Eesti kodanikule ja välismaalasele, kellele on varem välja antud isikutunnistus või elamisloakaart või kes taotleb isikutunnistust või elamisloakaarti samaaegselt digitaalse isikutunnistusega

Mõiste	Kirjeldus
E-residendi digi-ID	Digitaalne isikutunnistus, mis on väljastatud isikule, kellel puudub õigus või vajadus taotleda Eesti Vabariigi isikutunnistust või elamisloakaarti.
Mobiil-ID	Eesti Vabariigi poolt välja antav Mobiil-ID vormis digitaalne isikutunnistus.
E-residendi mobiil-ID	Eesti Vabariigi poolt välja antav Mobiil-ID vormis digitaalne isikutunnistus, mis on väljastatud isikule, kellel puudub õigus või vajadus taotleda Eesti Vabariigi isikutunnistust või elamisloakaarti.
Dokument	Üldiselt ID-kaart, EL-kaart, Digi-ID ja Mobiil-ID.
Eraldusnimi	sertifikaadi omaniku või väljastaja unikaalne nimi sertifikaatide infrastruktuuris;
Sertifikaat	digitaalne dokument, milles avalik võti seotakse üheselt selle omanikuga;
Sertifikaadi väljaandja	sertifikaadi väljastanud STO;
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.

1.2.2. Kasutatud lühendid

Vaata CPS p.11

Lühend	Kirjeldus
SR	Sertifitseerimise Register (digitaalallkirja seaduse alusel);
STO	Sertifitseerimisteenuse osutaja digitaalallkirja seaduse mõttes;
OID	mingile objektile antud standarditega reguleeritud tunnuskood (inglise keeles: *Object Identificator*).

2. Sertifikaatide loetelu ja otstarve

Dokumentidele kantakse kahte tüüpi sertifikaate:

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

Sertifikaate väljastab STO.

3. Andmed sertifikaatides

Sertifikaati kantakse kohustuslikult järgmised andmed:

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

Sertifikaati kantavate andmete kooslust kirjeldatakse täpsemalt punktides 3.1 kuni 3.3 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	Sertifitseerimisteenuse osutaja nimi, mis on äriregistris ja SRR-is	AS Sertifitseerimiskeskus
CN (commonName)	{id-at-commonName} { 2,5,4,3}	DirectoryString: PrintableString	Sertifitseerimisteenuse sertifitseerija eraldusnimi	ESTEID-SK 2011

Sertifikaatidesse võidakse kanda lisaks järgmised väljaandja (STO) andmed:

Atribuut	Atribuudi OID	ASN.1 tüüp	Kirjeldus	Näide
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-atcountryName} { 2,5,4,6 }	DirectoryString: PrintableString	Maatähis	EE
O	{id-	DirectoryString:	Sertifikaadi tüüp	ESTEID[1]

1 O atribuudi väärtus on erinev toodud näitest sõltuvalt dokumendi tüübist.

ID-kaart ja EL-kaart O = ESTEID

Digi-ID: O = ESTEID (DIGI-ID)

Mobiil-ID: O = ESTEID (MOBIIL-ID)

E-residendi digi-ID: O = ESTEID (DIGI-ID E-RESIDENT)

E-residendi mobiil-ID: O = ESTEID (MOBIIL-ID E-RESIDENT)

Atribuut	Atribuudi OID	ASN.1 tüüp	Kirjeldus	Näide
(organization)	atorganization} { 2,5,4,10}	UTF8		
OU (organizationUnit)	{id-atorganizationalUnit } { 2,5,4,11}	DirectoryString: UTF8	Sertifikaadi kasutusvaldkond	isikutuvastus sertifikaadis: *authentication* digitaalset allkirja võimaldavas sertifikaadis: *digital signature*
SN (surName)	{id-at-surName} { 2,5,4,4}	DirectoryString: UTF8	Perekonnanimed	MÄNNIK
G (givenName)	{id-at-givenName} { 2,5,4,42 }	DirectoryString: UTF8	Eesnimed	MARI-LIIS
S (serialNumber)	{id-atserialNumber} { 2,5,4,5 }	DirectoryString: PrintableString	Isikukood	47101010033
CN (commonName)	{id-atcommonName } { 2,5,4,3 }	DirectoryString: UTF8	Perekonna- ja eesnimed, isikukood (eraldatud komaga)	MÄNNIK,MARILIIS,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.

4. Viidatud ja seonduvad dokumendid

Käesoleva profiili koostamisel on lähtutud järgmistest alusdokumentidest:

4.1. Eesti Vabariigi seadused

[1] Isikut tõendavate dokumentide seadus, avaldatud: https://www.riigiteataja.ee/akt/123032015016&leiaKehtiv;
[2] Digitaalallkirja seadus, avaldatud: https://www.riigiteataja.ee/akt/114032014012&leiaKehtiv.

4.2. IETFi dokumendid

(Internet Engineering Task Force http://www.ietf.org)

[3] RFC5280 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, http://www.ietf.org/rfc/rfc5280.txt;
[4] RFC3739 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, http://www.ietf.org/rfc/rfc3739.txt.

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.

Dokumentides 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.

Dokumentide sertifikaatide signeerimiseks kasutatakse RSA ja SHA-256 algoritme ning välja väärtusteks on seega:

- **sha256WithRSAEncryption** { 1.2.840.113549.1.1.11 }.

A.2.4 Sertifikaadi kehtivusperiood (*validity*)

Sertifikaatidesse kantakse sertifikaadi kehtivuse alguse ja lõpu aeg.

Sertifikaadi kehtivuse lõpu kuupäev ühtib Dokumendi kehtivuse lõpu kuupäevaga.

Kuupäevad sertifikaadis esitatakse vastavalt RFC5280-le.

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

Väli sisaldab sertifikaadiomaniku avalikku võtit koos selle esitusalgoritmiga.

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

- **rsaEncryption** { 1.2.840.113549.1.1.1 }, 2048 bitiseid võtmeid;
- **ecPublicKey** { 1.2.840.10045.2.1 }, prime256v1 { 1.2.840.10045.3.1.7 }.

ID-kaardi, EL-kaardi ja digi-ID puhul väljastatakse üks paar sertifikaate rsaEncryption krüptoalgoritmiga võtmepikkusega 2048 bitti. Mobiil-ID puhul väljastatakse kaks paari sertifikaate, nii rsaEncryption krüptoalgoritmiga võtmepikkusega 2048 bitti kui ecPublicKey krüptoalgoritmiga võtmepikkusega 256 bitti.

A.3 Sertifikaadi laiendused

Kasutatavad sertifikaadilaiendused on toodud järgnevas tabelis:

Laienduse nimi	Täpne ASN.1 nimi ja OID	Esitus	Kriitilin e
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} {2,5,29,31}	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} {2,5,29,19}	JAH	EI OLE
qcStatements (digitaalseks allkirjastamiseks ettenähtud sertifikaadis)	{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 RFC5280-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, sertifitseerimispoliitikale või lepingule, 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.

Kui märkide asendamisel punktidega tekib e-posti aadress kujul, kus on järjest mitu punkti, siis asendatakse korduvad punktid ühekordse punktiga (nt. isik nimega ANTS E. PALUSAAR saab enda e-posti aadressiks ants.e.palusaar@eesti.ee) Juhul kui teisenduse tulemusena tekib e-posti aadressi algusesse või vahetult enne @ märki punkt, siis need punktid kaotatakse (nt. kui isiku nimi on MARK GIREE' siis tema e-posti aadressiks saab mark.giree@eesti.ee).

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		

jrk	Täht	Tähekood	Asendustäht	Asenduskood
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

jrk	Täht	Tähekood	Asendustäht	Asenduskood
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

jrk	Täht	Tähekood	Asendustäht	Asenduskood
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	OE	0152	OE	004F; 0045
160	oe	0153	oe	006F; 0065
161	Ŕ	0154	R	0052
162	ŕ	0155	r	0072
163	Ř	0158	R	0052
164	ř	0159	r	0072

jrk	Täht	Tähekood	Asendustäht	Asenduskood
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 laiendus on sertifikaadis ainult juhul kui väljastaja sertifikaadis on Subject Alternative Name.

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 väljastavale STO'le seatud tingimustele. Tunnus on koostatud vastavalt standardile ETSI TS 101 862 v 1.3.2.

Digitaalset allkirjastamist võimaldavasse sertifikaati kantakse vähemalt järgmised tunnused:

- EU digitaalallkirja direktiivile 1999/93/EC lisadele I ja II vastava kvalifitseeritud sertifikaadi tunnus {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1}
- Tunnus, mis märgib et serifikaadiga seotud privaatvõti asub turvalisel allkirja andmise vahendil vastavalt EU digitaalallkirja direktiivi 1999/93/EC lisale III {id-etsi-qcs-QcSSCD}, {0.4.0.1862.1.4}

See on mittekriitiline laiendus.

A.4 Sertifikaatide tühistusnimekirjade profiil

Sertifikaatide tühistusnimekirja (CRL) formaadiks on x.509v2 (defineeritud RFC5280-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 RFC5280-s esitatud nõudeid. DeltaCRL-i olemus on esitatud samas RFC-s.

Samuti võib STO võimalusel kasutada ka CRL Entry laiendusi, järgides RFC5280-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	32 3b b3 3a 2a a6 af 23 4f fe de f2 3b 73 4a ed
STO eraldusnimi	CN = ESTEID-SK 2011 O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
Sertifikaadi signeerimisalgoritm	sha256RSA
Sertifikaadi kehtivuse algus	28. jaanuar 2015 09:15:24
Sertifikaadi kehtivuse lõpp	31. jaanuar 2020 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(2048 bits) 30 82 01 0a 02 82 01 01 00 a9 cd 81 7e fd 38 ed 57 58 e5 90 dd a0 d1 38 a8 99 8a c0 98 69 df d2 fc 63 62 22 d4 b2 b2 34 5f 76 5b 3a 8d 38 8a 64 0b 74 b8 c1 de 12 f9 0e 88 b4 bb 50 f4 9a 4d 84 a9 a3 44 ef e6 55 e0 b9 70 7f 6b 7c 0c 24 6a 60 62 66 5f 12 44 c1 6c 6c 34 a4 ea 8b 21 0b db 5f be 49 66 62 5f 8b 07 63 47 ba 29 5d cd f1 8c 89 54 07 71 09 3d c0 7c ba e1 44 11 c6 69 50 99 79 4f 7a e0 14 69 b1 af 8d fc 91 4a e0 ff dd 31 39 b5 8b 37 b0 05 af c7 ce aa 9e 54 e6 82 f9 25 7a 6a db f3 60 b2 66 f9 62 58 97 77 8f e1 d2 1f 8f 8a be e7 4f cc e3 40 40 f1 f0 4b 41 08 f5 e8 ae a7 0e 55 19

Sertifikaadi väli	Sisunäide
	6f 9e 21 5c 1b 19 86 db 1f 7f 93 d1 b9 08 66 15 65 fe b1 c0 fb c3 53 bd 22 24 66 c7 55 f5 db 83 f2 ca 04 cb 5f 8c 7e b9 da 14 f8 78 57 b0 12 ee 82 7e 66 5c 03 6c 4b 2a 4f 2e ad 3f 6a f4 4c 9f 9c 9d e8 e0 59 02 03 01 00 01
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/repository/crls/esteid2011.crl
Isiku e-posti aadress	RFC822 Name=mari-liis.mannik@eesti.ee
Sertifitseerimispõhimõtted	[1]Certificate Policy[2]: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Contract 1.11-9 http://www.sk.ee/cp [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
Sertifikaadi põhiskasutus-valdkond	Digital Signature , Key Encipherment , Data Encipherment(B0)
Põhipiirangud	Subject Type=End Entity Path Length Constraint=None

A.5.2 Digitaalset allkirjastamist võimaldav sertifikaat

Sertifikaadi väli	Sisunäide
Sertifikaadi vormingu versioon	V3
STO-põhine unikaalne järjekorranumber	39 9a be 9a ad 4b 67 56 4f fe de ef 6a 48 c0 90
STO eraldusnimi	CN = ESTEID-SK 2011 O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
Sertifikaadi signeerimisalgoritm	sha256RSA
Sertifikaadi kehtivuse algus	28. jaanuar 2015 09:15:24
Sertifikaadi kehtivuse lõpp	31. jaanuar 2020 23:59:59
Sertifikaadi eraldusnimi	Serial Number=47101010033 G = MARI-LIIS SN = MÄNNIK CN = MÄNNIK,MARI-LIIS, 47101010033 OU = digital signature

[2] Vaata punkti A.3.4 Sertifitseerimispõhimõtted.

Sertifikaadi väli	Sisunäide
	O = ESTEID C = EE
Avalik võti	RSA(2048 bits) 30 82 01 0a 02 82 01 01 00 ba ea e3 d1 c4 c2 75 71 74 2b 68 14 1f be c3 a1 03 f1 e7 a6 bd 50 8a 98 ab e8 64 08 69 c3 92 52 9e f3 f2 4a 4f ee b6 f8 47 6a 65 d9 62 df b3 a2 9c a6 5c 36 4d 95 22 b4 cd 97 e8 49 0d 6d 63 2d 60 4c fb 31 57 f5 74 33 1c f5 25 ce 76 f4 39 bd 9e f0 34 34 58 7d bf 86 65 c4 a5 52 04 28 ac 25 59 4a 15 58 39 79 82 34 f8 87 24 69 1a 52 33 84 08 90 ab 8a d9 f7 d7 c6 92 60 c4 d4 03 bb 3e 32 91 de 8b b6 37 2e f4 b7 9a c7 fb 7d 28 34 84 11 83 1e b0 71 2d 6d c2 d1 b6 6b 40 34 15 dd 76 99 c2 69 57 c0 96 37 54 e5 76 e7 36 59 0b e7 77 98 26 23 ad 07 a9 8c bc 9c d8 1a 8c ac 4f 04 8b 9a 74 7d 90 6b 1e 68 59 53 e3 66 83 3b 6c 0b 09 ef 09 7d ae 6e 7b 8b 53 ac 51 ad 83 f8 cc bd be b2 b3 80 b9 2b 52 e9 a5 57 a8 29 b3 a6 63 ac 49 5a 88 c8 c6 9d 55 e7 5b 03 b7 3b c7 34 42 61 e2 99 02 03 01 00 01
Tühistusnimekirjade levituspunktid	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/esteid2011.crl
Sertifitseerimispõhimõtted	[1]Certificate Policy[2]: PolicyIdentifier=1.3.6.1.4.1.10015.1.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Contract 1.11-9 **Error! Bookmark not defined.** http://www.sk.ee/cp [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/
Kvalifitseeritud sertifikaadi tunnus	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD
Sertifikaadi põhikasutus-valdkond	Non-Repudiation(40)
Põhipiirangud	Subject Type=End Entity Path Length Constraint=None