Sertifikaadid Eesti Vabariigi isikutunnistusel

SISUKORD

1. Ülevaade

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

Antud dokument ei käsitle teisi isikutunnistuses sisalduvaid andmekogumeid.

Käesoleva dokumendi koostamisel on lähtutud järgmistest alusdokumentidest:

A. Eesti Vabariigi seadused

1) isikut tõendavate dokumentide seadus (RT I 1999, 25, 365; 2000, 25, 148; 26, 150; 40, 254; 86, 550; 2001, 16, 68; 31, 173; 56, 338);
2) digitaalallkirja seadus (RT I 2000, 26, 150; 92, 597; 2001, 56, 338);
3) isikuandmete kaitse seadus (RT I 1996, 48, 944; 1998, 59, 941; 111, 1833; 200, 50, 317; 92, 597; 104, 685);
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) RFC2459 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile (http://www.ietf.org/rfc/rfc2459.txt);
2) RFC3039 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile (http://www.ietf.org/rfc/rfc3039.txt);
3) Internet Draft – Internet X.509 Public Key Infrastructure - Certificate and CRL Profile draft-ietf-pkix-new-part1-08.txt (http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-08.txt).

2. Mõisted

Järgnevalt esitatakse tekstis esinevate mõistete lühiseletused.

Mõiste	Seletus
isikutunnistus -	isikut tõendavate dokumendite seaduse alusel väljastatav isikut tõendav dokument;
isikutunnistuse kehtivusperiood -	ajavahemik isikutunnistuse väljastamise hetkest kuni tema väljastamisel määratud kehtivuse lõpptähtajani. Isikutunnistuse tegelik kehtivusaeg võib tema kehtetuks tunnistamise tõttu olla lühem;
SRR -	Sertifitseerimise Riiklik Register (digitaalallkirja seaduse alusel);
STO -	sertifitseerimisteenuse osutaja digitaalallkirja seaduse mõttes;
eraldusnimi -	subjekti unikaalne nimi või nimetus sertifikaatide infrastruktuuris;
sertifikaat -	digitaalne dokument, milles avalik võti seotakse üheselt selle omanikuga;
sertifikaadi väljaandja -	sertifikaadi väljastanud isik (STO digitaalallkirja seaduse mõttes);
signeerimissertifikaat -	STO sertifikaat, millega signeeritakse tema poolt välja antud sertifikaadid;
sertifikaadi omanik -	subjekt, kellele konkreetne sertifikaat on välja antud;
sertifikaadi kehtivusperiood -	ajavahemik sertifikaadi moodustamise hetkele järgneva päeva kella 0.00-st (GMT +002) kuni tema väljastamisel määratud kehtivuse lõpptähtajani. Sertifikaadi tegelik kehtivusaeg võib tema kehtetuks tunnistamise tõttu olla

lühem.

3. Sertifikaatide loetelu ja otstarve

Isikutunnistusele kantakse kaks sertifikaati:

1) sertifikaat isiku digitaalseks tuvastamiseks;
2) sertifikaat digitaalseks allkirjastamiseks.

Sertifikaadi isiku digitaalseks tuvastamiseks annab välja teenuse osutaja, kes vastab Teede- ja Sideministeeriumi 3. oktoobri 2000.a määruses nr 83 "**Teenuse osutajate infosüsteemide auditeerimise korď**' esitatud nõuetele.

Sertifikaadi digitaalseks allkirjastamiseks annab välja digitaalallkirja seaduses esitatud nõuetele vastav STO.

Sertifikaat isiku digitaalseks tuvastamiseks on ette nähtud selle omaniku tuvastamiseks mistahes elektroonilist isikutuvastust nõudvas suhtluses.

Sertifikaat digitaalseks allkirjastamiseks on sertifikaat, millega saab sertifikaadi omanik anda digitaalallkirja digitaalallkirja seaduse mõttes.

Isikutunnistusele kantud sertifikaadid kehtivad kuni **1100 päeva** (3 aastat ja 4 päeva), kuid mitte kauem isikutunnistuse kehtivuse lõpptähtajast.

4. Andmed sertifikaatides

Mõlemasse sertifikaati kantakse kohustuslikult järgmised andmed:

1) sertifikaadi väljaandja andmed;
2) sertifikaadiomaniku andmed;
3) sertifikaadi kehtivusandmed;
4) sertifikaadipõhised andmed.

Sertifikaati kantavate andmete kooslust kirjeldatakse täpsemalt punktides 4.1-4.4 ja tehnilisi detaile peatükkides 5 ja 6.

4.1. Väljaandja andmed

Sertifikaatidesse kantakse järgmised väljaandja (STO) andmed:

1) SRR-s registreeritud nimi;
2) SRR-i registrisse kantud registrikood.

4.2. Sertifikaadiomaniku andmed

Sertifikaatidesse kantakse järgmised sertifikaadiomaniku andmed:

1) eesnimi või –nimed;
2) perekonnanimi;
3) isikukood.

4.3. Sertifikaadi kehtivusandmed

Sertifikaatidesse kantakse kohustuslikult 2 kuupäeva:

1) sertifikaadi moodustamise kuupäev ja kellaaeg;
2) sertifikaadi kehtivuse lõppemise kuupäev ja kellaaeg.

Vt ka viited punktides 4.4 ja 6.2.4

4.4. Sertifikaadi tehnilised andmed

Sertifikaadi tehniliste andmetena kantakse sertifikaatidesse järgmised andmed:

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

5. Nimed sertifikaatides

Kõigis sertifikaatides on kaks eraldusnime, väljaandja ja omaniku nimi. Lisaks eeltooduile kantakse sertifikaati STO lisanimi.

Sertifikaatides esitatud väljaandja (STO) konkreetse signeerimissertifikaadi eraldusnimi peab sisaldama käesoleva dokumendis punktis 4.1 toodud andmeid.

Sertifikaadiomaniku eraldusnimes (*DN - distinguished name*) esitatakse sertifikaatides järgmised atribuudid:

Atribuut	**Kirjeldus**	**Näide**
CountryName	Maatähis	'EE'
O (Organisation)	Sertifikaadi tüüp	'ESTEID'
OU (Organisational Unit)	Sertifikaadi kasutusvaldkond	['*authentication*','*digital signature*']
SN (Surname)	Perekonnanimed	'Kask'
G (GivenName)	Eesnimed	'Juhan'
SERIAL NUMBER (Serialnumber)	Isikukood	'37011126789'
CN (CommonName)	Perekonna- ja eesnimed, isikukood (eraldatud komaga)	'Kask,Juhan,37011126789'

Märkused.

1. Sertifikaadi tüüp "ESTEID" väljal *O* võetakse kasutusele isikutunnistuste sertifikaatide koondamiseks ühte harusse.

2. Sertifikaadi kasutusvaldkond defineeritakse *DN*-s väljal *OU* (*Organisational Unit*) ja inglise keeles (selle üldise kasutatavuse huvides), vastavalt siis *authentication* (sertifikaat on mõeldud isiku digitaalseks tuvastamiseks) või *digital signature* (sertifikaat on mõeldud digitaalseks allkirjastamiseks).
Välja *OU* kasutatakse siinkohal selle sobivuse tõttu ning ühilduvuse tagamiseks.

3. Atribuudis *CommonName* on eraldajaks valitud "koma", kuna eraldaja "tühik" võib olla vaikimisi juba isikunimede koosseisus (nt kahe- või enamaosaline eesnimi).

6. Lisa

6.1. Sertifikaadikohane tehniline lisainformatsioon

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

6.2. Sertifikaadi põhiväljad

6.2.1. Sertifikaadi vormingu versioon (*version*)

Väljal esitatakse sertifikaadi vormingu versiooni number.
Isikutunnistuses kasutatakse X.509 v3 sertifikaate, seega välja väärtuseks seatakse 2.

6.2.2. Sertifikaadi STO-põhine järjekorranumber (*serialNumber*)

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

6.2.3. 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 }

6.2.4. Sertifikaadi kehtivusperiood (*validity*)

Sertifikaatide kehtimahakkamise ajaks märgitakse STO infosüsteemis konkreetse sertifikaadi moodustamise kuupäevast järgmine kuupäev ja kellaaeg 00:00. Kehtivuse lõppemise kuupäevaks märgitakse isikusertifikaatides ***1100 päeva*** eelnimetatud tähtajast hilisem kuupäev ja kellaaeg või isikutunnistuse kehtivuse lõpptähtaeg, kui see on varasem.

Kuupäevad sertifikaadis esitatakse vastavalt RFC2459-le.

6.2.5. 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 }.

6.3. Sertifikaadi laiendused

Kasutatavad sertifikaadila iendused on toodud järgnevas tabelis:

Laienduse nimi	Isikutunnistus	
	Esitus	**Kriitiline**
AuthorityKeyIdentifier	**JAH**	EI OLE
SubjectKeyIdentifier	**JAH**	EI OLE
KeyUsage	**JAH**	**ON**
CertificatePolicies	**JAH**	EI OLE
SubjectAltName (isiku digitaalseks tuvastamiseks ettenähtud sertifikaadis)	**JAH**	EI OLE
IssuerAltName	**JAH**	EI OLE
CRLDistributionPoints	**JAH**	EI OLE
ExtKeyUsage (isiku digitaalseks tuvastamiseks ettenähtud sertifikaadis)	**JAH**	**ON**
ExtKeyUsage (digitaalseks allkirjastamiseks ettenähtud sertifikaadis)	**EI**	EI OLE
Authority Information Access	**JAH**	EI OLE
Basic Constraints	**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.

6.3.1. 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.

6.3.2. 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 RFC2459-le kasutatakse meetodit 1.

See on mittekriitiline laiendus.

6.3.3. 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.

6.3.4. Sertifitseerimispõhimõtted (*certificatePolicies*)

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

See on mittekriitiline laiendus.

6.3.5. 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.

6.3.6. 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, allkriipsust ning juhuslikult loodud neljanumbrilisest kombinatsioonist. 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:
š – s;
ž – z;
õ – o;
ä – a;
ö – o;
ü – y.

E-posti aadressi näidis: mari.sert_0123@eesti.ee.

See on mittekriitiline laiendus.

6.3.7. STO lisanimi (*Issuer Alternative Name*)

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

See on mittekriitiline laiendus.

6.3.8. 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.

6.3.9. STO lisateenused (*Authority Information Access*)

Väli sisaldab lisainformatsiooni STO teenuste kohta ning täidetakse STO poolt.
Kui STO pakub näiteks OCSP (*Online Certificate Status Protocol*)-teenust, antakse selle laienduse kaudu edasi selle asukoht *URL*-ina.
See on mittekriitiline laiendus.

6.3.10. Basic Constraints

See laiendus näitab, et antud sertifikaadi omanikuks on lõppkasutaja.

See on mittekriitiline laiendus.

6.4. Sertifikaatide tühistusnimekirjade profiil

Sertifikaatide tühistusnimekirja (*CRL*) formaadiks on x.509v2 (defineeritud RFC2459-s).
STO poolt tühistusnimekirja koostamisel järgitakse ka antud dokumendis toodud soovitusi.

6.4.1. CRL-i laiendused

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

- **Authority Key Identifier;**
- **CRL number.**

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 RFC2459-s esitatud nõudeid. *DeltaCRL*-i olemus on esitatud samas RFC-s.
Samuti võib STO võimalusel kasutada ka *CRL Entry* laiendusi, järgides RFC2459-s esitatud nõudeid ja soovitusi.

6.5. Näitesertifikaadid

Järgnevalt esitatakse eeltoodud profiili alusel loodud sertifikaadinäidised

6.5.1. Digitaalset isiku tuvastamist võimaldav sertifikaat

SERTIFIKAADI VÄLI	INGLISEKEELNE NIMETUS	SISUNÄIDE
SERTIFIKAADI VORMINGU VERSIOON	VERSION	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	SERIAL NUMBER	3BD9 1AEB
STO ERALDUSNIMI	ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	SIGNATURE ALGORITHM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	VALID FROM	28. jaanuar 2002. A. 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	VALID TO	31. jaanuar 2005 23:59:59
SERTIFIKAADI ERALDUSNIMI	SUBJECT	Serial Number=60110260002 G = MARI SN = SERT CN = SERT,MARI,60110260002 OU = authentication O = ESTEID C = EE
AVALIK VÕTI (1024 bitti)	PUBLIC KEY	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	EXTENDED KEY USAGE	Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4)
TÜHISTUSNIMEKIRJADE LEVITUSPUNKTID	CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
ISIKU E-POSTI AADRESS	SUBJECT ALTERNATIVE NAME	RFC822 Name=mari.sert_0123@eesti.ee
SERTIFITSEERIMISPÕHIMÕTTED	CERTIFICATE POLICIES	[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/
SERTIFIKAADI PÕHISKASUTUS-VALDKOND	KEY USAGE	Digital Signature , Key Encipherment , Data Encipherment(B0)
RÄSI ALGORITM	THUMBPRINT ALGORITHM	sha1
RÄSI	THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1

6.5.2. Digitaalset allkirjastamist võimaldav sertifikaat

SERTIFIKAADI VÄLI	INGLISEKEELNE NIMETUS	SISUNÄIDE
SERTIFIKAADI VORMINGU VERSIOON	VERSION	V3
STO-PÕHINE UNIKAALNE JÄRJEKORRANUMBER	SERIAL NUMBER	3BD9 1AEB
STO ERALDUSNIMI	ISSUER	CN = ESTEID-SK SN = 1 OU = ESTEID O = AS Sertifitseerimiskeskus C = EE E = pki@sk.ee
SERTIFIKAADI SIGNEERIMISALGORITM	SIGNATURE ALGORITHM	sha1RSA
SERTIFIKAADI KEHTIVUSE ALGUS	VALID FROM	28.jaanuar 0:00:00
SERTIFIKAADI KEHTIVUSE LÕPP	VALID TO	31.jaanuar 23:59:59
SERTIFIKAADI ERALDUSNIMI	SUBJECT	Serial Number=60110260002 G = MARI SN = SERT CN = SERT,MARI,60110260002 OU = digital signature O = ESTEID C = EE
AVALIK VÕTI (1024 bitti)	PUBLIC KEY	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	CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/esteid/esteid.crl
SERTIFITSEERIMISPÕHIMÕTTED	CERTIFICATE POLICIES	[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/
SERTIFIKAADI PÕHIKASUTUS-VALDKOND	KEY USAGE	Non-Repudiation(40)
RÄSI ALGORITM	THUMBPRINT ALGORITHM	sha1
RÄSI	THUMBPRINT	973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1