

**SERTIFIKAADID EESTI VABARIIGI
ISIKUTUNNISTUSEL**

**Certificates on identity cards of republic of
Estonia**



EESSÕNA

Eesti standardi EVS 828:2004 "Sertifikaadid Eesti Vabariigi isikutunnistusel" on koostanud Privador AS, tehnilise ekspertiisi tegi AS Sertifitseerimiskeskus.

Standardi kiitis heaks ja esitas Standardikeskusele vastuvõtmiseks infotehnoloogia standardimise tehniline komitee EVS/TK 4.

Standardi väljaandmist on toetanud Riigi Infosüsteemide Arenduskeskus.

Standard on koostatud esmakordselt.

Standard on kinnitatud ja kasutusele võetud Eesti standardina EVS 828:2004 Eesti Standardikeskuse 05.11.2004 käskkirjaga nr 108.

SISUKORD

1	KÄSITLUSALA	1
2	MÕISTED	1
3	SERTIFIKAATIDE LOETELU JA OTSTARVE	2
4	ANDMED SERTIFIKAATIDES	2
4.1	Väljaandja andmed	3
4.2	Sertifikaadiomaniku andmed	4
4.3	Sertifikaadi tehnilised andmed	4
Lisa A		6
A.1	Sertifikaadikohane tehniline lisainformatsioon	6
A.2	Sertifikaadi põhiväljad	6
A.2.1	Sertifikaadi vormingu versioon (<i>version</i>)	6
A.2.2	Sertifikaadi STO-põhine järjekorranumber (<i>serialNumber</i>)	6
A.2.3	Sertifikaadi signeerimisalgoritm (<i>signatureAlgorithm</i>)	6
A.2.4	Sertifikaadi kehtivusperiood (<i>validity</i>)	6
A.2.5	Sertifikaadis sisalduv avalik võti ja selle esitusalgoritm (<i>subjectPublicKeyInfo</i>)	6
A.3	Sertifikaadi laiendused	7
A.3.1	STO avaliku võtme identifikaator (<i>authorityKeyIdentifier</i>)	7
A.3.2	Isiku avaliku võtme identifikaator (<i>subjectKeyIdentifier</i>)	7
A.3.3	Sertifikaadi põhikasutusvaldkond (<i>keyUsage</i>)	8
A.3.4	Sertifitseerimispõhimõtted (<i>certificatePolicies</i>)	8
A.3.5	Tühistusnimekirjade levituspunktid (<i>cRLDistributionPoints</i>)	8
A.3.6	Isiku e-posti aadress (<i>Subject Alternative Name</i>)	8
A.3.7	STO lisanimi (<i>Issuer Alternative Name</i>)	9
A.3.8	Sertifikaadi lisakasutusvaldkond (<i>Extended Key Usage</i>)	9
A.3.9	Põhipiirangud (<i>Basic Constraints</i>)	9
A.3.10	Kvalifitseeritud sertifikaadi tunnus (<i>qcStatements</i>)	9
A.4	Sertifikaatide tühistusnimekirjade profiil	9
A.4.1	CRL-i laiendused	10
A.5	Näitesertifikaadid	10
A.5.1	Digitaalset isikutuvastamist võimaldav sertifikaat	11
A.5.2	Digitaalset allkirjastamist võimaldav sertifikaat	12

SERTIFIKAADID EESTI VABARIIGI ISIKUTUNNISTUSEL

1 KÄSITLUSALA

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

Antud standard ei käsitleni teisi isikutunnistuses sisalduvaid andmekogumeid.

Käesoleva standardi 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; 2002, 61, 375; 63, 387; 90, 516; 2003, 13, 65; 15, 87);
- 2) digitaalallkirja seadus (RT I 2000, 26, 150; 92, 597; 2001, 56, 338);
- 3) isikuandmete kaitse seadus (RT I 2003, 26, 158);
- 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>).

2 MÕISTED

Järgnevalt esitatakse tekstis esinevate mõistete lühiseletused.

<u>Mõiste</u>	<u>Seletus</u>
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;