SERTIFIKAADID EESTI VABARIIGI ISIKUTUNNISTUSEL

Certificates on identity card of Republic of Estonia

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESSÕNA

Käesolev Eesti standard:

- on Eesti standardi EVS 828:2004 uustöötlus;
- on kinnitatud Eesti Standardikeskuse 30.09.2009 käskkirjaga nr 175;
- jõustub sellekohase teate avaldamisel EVS Teataja 2009. aasta oktoobrikuu numbris.

Standardi koostamisettepaneku esitas EVS/TK 4 Infotehnoloogia, standardi uustöötluse koostas AS Sertifitseerimiskeskus, standardi on heaks kiitnud tehniline komitee EVS/TK 4.

Standardi uustöötlusega on ajakohastatud standardit ja viidud kooskõlla väljakujunenud praktikaga. Standardi uustöötlus on vastavuses Eesti digitaalallkirja seadusega ja isikut tõendavate dokumentide seadusega ning Euroopa Parlamendi ja nõukogu direktiivi 1999/93/EÜ nõuetega. Standardi uustöötlus on koostatud kakskeelse (et, en) väljaandena.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: ID-kaart, isikutunnistus, sertifikaadi profiil, sertifikaat
Hinnagrupp RN

FOREWORD

This Estonian standard:

— is new version of standard EVS 828:2004;

— is implemented by decree of Estonian Centre for Standardisation 30.09.2009 no 175;

— becomes valid with notice in EVS Teataja, issue October 2009.

The proposal for new version of Estonian standard EVS 828:2004 “Certificates on Identity Card of the Republic of Estonia” is made by technical committee EVS/TK 4 Infotechnology, standard has been prepared by the Estonian Certification Centre (AS Sertifitseerimiskeskus), standard approved by EVS/TK 4.

The new version of standard gives conformity with Estonian law of digital signature and Directive 1999/93/EC of European Parliament and Council about Community framework for digital signature. Also the composition of Certificates is amended with text for identification of Qualified Certificate. The new version of standard issued in two languages (et, en).

ICS 35.040 Character sets and information coding
Descriptors: ID-card, identity card, certificate profile, certificate
Price group RN

SISUKORD

TABLE OF CONTENT

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 käsitle 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; 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).

2 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse järgmisi termineid ja määratlusi.

Termin	Määratlus
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;
SRR	Sertifitseerimise Riiklik 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;

1 SCOPE

This standard describes profile of personal digital certificates stored on Estonian Republic Identity card (ID card). Annex A presents additional technical information and example of certificates.

This standard does not describe other data collections stored in the Identity card.

This standard is based on the following documents:

A. Legal acts of Estonian Republic

1) Identity Documents Act (RT I 1999, 25, 365; 2006, 29, 221);
2) Digital Signature Act (RT I 2000, 26, 150; 92, 597; 2007, 24, 127);
3) Personal Data Protection Act (RT I 2007, 24, 127);
4) Decree of the Minister of Transport and Communications “Service provider's information systems' auditing procedure” (issued 03.10.2000, no 83, RTL 2000, 108, 1655)

B. IETF (Internet Engineering Task Force http://www.ietf.org) **documents**

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 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

Term	Definition
Identity card, ID-card	Document identifying its holder and issued on the basis of a legal act
Identity card validity period	Period starting at issuing the Identity card and ending at the validity end time specified at the moment of issuing. Actual document validity period may be shorter due to the document possibly being revoked
SRR	National Register of Certification Service Providers (SRR - *Sertifitseerimise Riiklik Register*) according to Estonian Digital Signatures Act
CSP	Certification Service Provider according to Estonian Digital Signatures Act
OID	Object Identifier. Unique sequence of numbers to identify any digital data, defined in ITU-T recommendation X.208.
Distinguished name	Unique subject name in the infrastructure of certificates
Certificate	Digital document where a public key is associated with the owner of the key
Certificate issuer	Person who issues the certificate (CSP in the context of Digital Signatures Act)

Termin	Määratlus
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.

3 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 (qualified certificate) väljastajale toodud nõuetele.

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 kuni 4.4 ja tehnilisi detaile lisas A.

4.1 Väljaandja andmed

Sertifikaatidesse kantakse järgmised kohustuslikud väljaandja (STO) andmed: