



Küberneetika AS
Infotehnoloogia osakond

Dok. DO-ÜV-C-21-1299

IDENTIFITSEERIMISKAARTIDE RAHVUSVAHELISED STANDARDID

ÜLEVAADE

23 lk.

Töö täitjad:

Jaan Priisalu
Olev Sepp
Margus Freudenthal
Tarvi Martens

Tallinn 1999

ANNOTATSIOON

Töös antakse ülevaade identifitseerimiskaartide (edaspidi: ID-kaartide) rahvusvahelistest standarditest ning hinnanguid nende kohaldamiseks/ülevõtmiseks Eestis ning Eesti ID-kaardi programmi raames. Ülevaade on koostatud ID-kaardi töörühma (TK4ID) ekspertide poolt ning toimus Eesti Informaatikakeskuse ja Küberneetika AS vahel sõlmitud lepingu nr. 918/2403/R2-2 “Identifikaatorkaardi standardite koostamine ja ekspertiiside läbiviimine” raames.



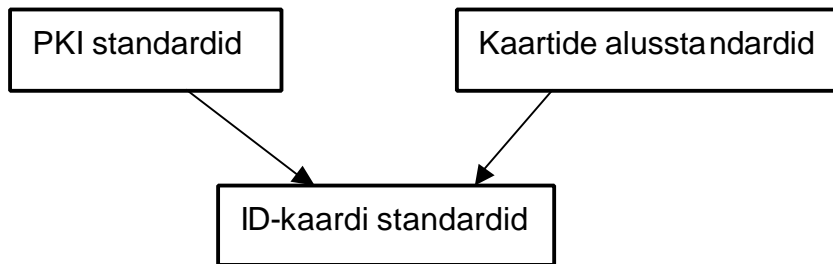
SISUKORD

<u>1.</u>	<u>SISSEJUHATUS</u>	4
<u>2.</u>	<u>ISO/IEC STANDARDID</u>	5
<u>3.</u>	<u>CEN STANDARDID</u>	7
<u>4.</u>	<u>SEIS JA FINEID STANDARDID</u>	13
<u>5.</u>	<u>IETF STANDARDID</u>	14
<u>6.</u>	<u>MUUD STANDARDID</u>	20
6.1	<u>RSA PKCS</u>	20
6.2	<u>ETSI</u>	21
6.3	<u>INFOSEC</u>	21
6.4	<u>Open Group</u>	22
6.5	<u>PKI Forum</u>	22
<u>7.</u>	<u>KOKKUVÕTE</u>	23

1. SISSEJUHATUS

Rahvusvahelised standardid jagunevad mitmeti. On olemas üldaktsepteeritud rahvusvahelised standardimisorganisatsioonid (ISO, IETF), regionaalsed organisatsioonid (Euroopa, riikide standardid) ning tööstusstandardid, mis on välja töötatud üksikute firmade või erinevate firmade koostöös.

Vaadeldes ID-kaardi alaseid standardeid, saaksime olemasolevad standardid tinglikult jaotada järgmise skeemi alusel:



PKI standardite all mõistame siin avaliku võtme infrastruktuuri ja selle rakendustega seonduvat (näiteks ISO, IETF PKIX, RSA PKCS jne.). Kaartide alustandardid käsitlevad eelkõige kiipkaarti ennast (tüüpiliselt ISO/CEN standardid). ID-kaardi standardid käsitlevad juba konkreetset elektroonset isikutunnistuse rakendust. Tänapäeval on siin määravaks FINEID standardid (edasiarendus Rootsi SEIS standarditest), PKIX “Qualified Certificates” ning PKCS #15.

2. ISO/IEC STANDARDID

Juhtiv standardiorganisatsioon ISO on antud alal keskendunud paljuski (kiip)kaartide põhitehnoloogiate standardiseerimisele. Samas on esindatud ka PKI standardimise komponente, mis on paljuski üle võetud IETF-i samasuunalisest tööst. ISO standardid võiksid olla põhilised allikad ülevõtmisel Eesti standarditeks, seda eelkõige tiitellehe meetodil. Identifitseeritud on kahe standardi ülevõtmise otsene vajadus:

- ISO/IEC 7812: 1993
- ISO/IEC 7816: 1993

Järgnev on loetelu ISO/IEC olulistest standarditest.

ISO/IEC 7812-1: 1993 Identification cards - Identification of issuers - Part 1: Numbering system.

ISO/IEC 7816-3: 1989 Information technology - Identification cards - Integrated circuit cards with contacts. Part 3: Electronic signals and transmission protocols.

ISO/IEC 7816-4: 1994 Information technology - Identification cards - Integrated circuit cards with contacts. Part 4: Inter-industry commands for interchange.

ISO/IEC 7816-5: 1993 Information technology - Identification cards - Integrated circuit cards with contacts. Part 5: Registration system for applications in IC card.

ISO/IEC 7816-6: 1995 Information technology - Identification cards - Integrated circuit cards with contacts. Part 6: Inter-industry data elements.

ISO/IEC 8824: 1988 Information technology - Open system interconnection - Specification of Abstract Syntax Notation One (ASN.1).

ISO/IEC 8825-1: 1995 Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

ISO 8859-1: 1987 Information processing - 8-bit single-byte coded graphic character sets- Part 1: Latin alphabet No. 1.

ISO/IEC 9594-2: 1995 Information technology - Open systems interconnection – The Directory - Part 2: Models. (X.501).

ISO/IEC 9594-6: 1993 Information technology - Open systems interconnection – The Directory - Part 6: Selected attribute types. (X.520).

ISO/IEC 9594-8: 1995 Information technology - Open systems interconnection – The Directory - Part 8: Authentication framework. (X.509).



ISO/IEC 9796-2: 1997 Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function

ISO/IEC 9798-3: 1993 Information technology - Security techniques - Entity authentication mechanisms -- Part 3: Entity authentication using a public key algorithm.

ISO/IEC DIS 10118-3 Hash-functions – Part 3: Dedicated hash-functions

ISO/IEC DIS 11770-3 Information technology - Security techniques - Key management – Part 3: Mechanisms using asymmetric techniques

ISO/IEC CD 13888-3 Non-repudiation – Part 3: Using asymmetric techniques

ISO/IEC CD 14888-1 Digital signatures with appendix – Part 1: General

ISO/IEC CD 14888-3 Digital signatures with appendix – Part 3: Certificate-based mechanisms

3. CEN STANDARDID

CEN standardid lähtuvad põhijoontes ISO vastavast tööst, palju on ülevõetud standardeid. Spetsiifilised standardid üldjuhul on kas tootja- või keskkonnakesksed ning seetõttu ei paku otsust huvi. Alljärgnev on standardite loetelu ning esialgne hinnang nende ülevõtmise vajalikkusele.

EN 726

Identification card systems - Telecommunications integrated circuit(s) cards and terminals

Meil ei ole täna tootjaid, keda asi tegelikult huvitaks. Spetsialistile huvitav lugemine, defineeritakse ära terve keskkond.

EN 742:1993

Identification card systems - Intersector ID-1 card location of contacts for cards and devices used in Europe

ISO7816-2 selle koha peal abiks. Prantslaste ülaasetus on de facto kadunud. Ei ole üldse huvitav.

EN 753

Identification card systems - Intersector thin flexible cards

Üherkordsed piletikaardid. Eestis pole kasutust näinud, küll aga Prantsusmaal. Võidakse kasutusele võtta. Täna pole huvitav

EN 1038:1995

Identification card systems - Telecommunication applications - Integrated circuit(s) card payphone

Mobiilside arengukiirust arvestades ebavajalik.

ENV 1257-1:1994

Identification card systems - Rules for Personal Identification Number handling in intersector environments - Part 1: PIN presentation

ENV 1257-2:1997

Identification card systems - Rules for Personal Identification Number handling in intersector environments - Part 2: PIN protection

ENV 1257-3:1997

Identification card systems - Rules for Personal Identification Number handling in intersector environments - Part 3: PIN verification

See võiks olla huvitav rida. PIN-i hoidmise ja pruukimise üle on palju vaidlusi, eriti polüfunktsionaalse kaardi puhul. Tahaks, et keegi võtaks PIN-i standardid ette ja teeks väikese uurimuse.

ENV 1284:1996

Identification card systems - Intersector rules for locking and unlocking of integrated circuit(s) cards

Jälle vajalik ja uurimata teema. Keegi peaks selle standardi läbi lugema ja ütlema, kas iva kah sees on.

ENV 1292:1995

Identification card systems - Integrated circuit(s) cards and interface devices - Additional test methods

Ei ole huvitav, tootjatele.

EN 1332-2:1998

Identification card systems - Man-machine interface - Part 2: Dimensions and location of a tactile identifier for ID-1 cards

Ei ole huvitav, kaartide ja lugemismoodulite tootjatele (minu arusaamist mööda).

EN 1362:1997

Identification card systems - Device interface characteristics – Classes of device interfaces

Ei saa sisu nägemata aru. Ilmselt pole vaja.

ENV 1375-1:1994

Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics

Peaks arutama. Vaga vaja ei ole.

EN 1387:1996

Machine readable cards - Health care applications - Cards: General characteristics

Haigekassa rida. Peaks nende käest küsima. Ei usu, et üle võtta vaja oleks.

ENV 1545-1:1998

Identification card systems - Surface transport applications - Part 1: General data elements

ENV 1545-2:1998

Identification card systems - Surface transport applications - Part 2: Transport payment related data elements

Kui kasutataks, siis oleks huvitav. Peaks TC224 käest küsima, kas selle standardi järgi tehtud süsteeme looduses kah eksisteerib. Kui jah, siis tiitelleht.

CR 1750:1999

Identification card systems - Inter-sector messages between devices and hosts - Acceptor to acquirer messages

Ootame. Reaalses elus on igal operaatoril oma protokoll. Kui keegi on näinud standardset süsteemi, võiks mulle kah öelda.

ENV 1855:1996

Identification card systems - Intersector integrated circuit(s) card systems - Tolerance ranges for IC cardss

Ei huvita.

EN 1867:1997

Machine-readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers

Haigekassa. Ilmselt ei huvita.

EN 24909:1989

Bank cards - Magnetic stripe data content for track 3 (ISO 4909:1987, ed. 2)

Ei huvita, keegi ei kirjuta enam vabu vahendeid kaardile.

EN 27810:1989

Identification cards - Physical characteristics (ISO 7810:1985, ed. 1)

Ei huvita, ISO koopia

EN 27811

Identification cards - Recording technique

Ei huvita, ISO koopia.

EN 27813:1992

Identification cards - Financial transaction cards (ISO 7813:1990, ed. 3)

Ei huvita, kõik teavad ISO-t.

EN 27816-1:1989

Identification cards - Integrated circuit(s) with contacts - Part 1: Physical characteristics (ISO 7816-1:1987, ed. 1)

EN 27816-2:1989

Identification cards - Integrated circuit(s) with contacts - Part 2: Dimensions and location of the contacts (ISO 7816-2:1988, ed. 1)

EN 27816

Identification cards - Integrated circuit(s) cards with contacts

Ei huvita. ISO.

EN 27982-1:1991

Bank telecommunication - Funds transfer messages - Part 1: Vocabulary and data elements (ISO 7982-1:1987, ed. 1)

Ei huvita.

EN 28583:1995

Financial transaction card originated messages - Interchange message specifications (ISO 8583:1993)

Kellel vaja, need on juba ISO-t lugenud.

EN ISO 8583-2:1998

Financial transaction card originated messages - Interchange message specifications - Part 2: Application and registration procedures for Institution Identification

Codes (IIC) (ISO 8583-2:1998)

Ei huvita.

EN ISO 8583-3:1998

Financial transaction card originated messages - Interchange message specifications - Part 3: Maintenance procedures for codes (ISO 8583-3:1998)

Ei huvita.

EN 29564-1:1993

Banking - Personal Identification Number management and security – Part 1: PIN protection principles and techniques (ISO 9564-1:1991)

Huvitab kas see või ISO. Urida.

EN 29564-2:1993

Banking - Personal Identification Number management and security – Part 2: Approved algorithm(s) for PIN encipherment (ISO 9564-2:1991)

See sisaldab PIN ploki formaate. PIN-i edastamine on üldse üks halb idee, nõuab terve keti usaldust. Kui seda siiski teha vaja on, siis on PIN ploki formaadid abiks, et taasesitusründeid vältida. Kiipkaardid kontrollivad PIN-i ise, seega aeguv tehnoloogia. Pole oluline.

EN ISO 9807:1996

Banking and related financial services - Requirements for message authentication (retail) (ISO 9807:1991)

Käsitleb MAC-i. Ei ole otseselt kaardi rida.

EN 29992-1:1993

Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Part 1: Concepts and structures (ISO 9992-1:1990)

Ei.

EN 30202-1:1993

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 1: Card life cycle (ISO 10202-1:1991)

ISO pakub huvi. Hämmastavalt tihti teevad inimesed projekteerimisel selle vea, et jätavad elutsüklist mingi osa ära.

EN ISO 10202-3:1998

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 3: Cryptographic key relationships (ISO 10202-3:1998)

Ei tea.

EN ISO 10202-6:1995

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 6: Cardholder verification (ISO 10202-6:1994)

Tahaks enne töökava näha. Seoses terminali usaldamise probleemiga võiks ümberavaatamisele minna.

EN ISO 11568-1:1996

Banking - Key management (retail) - Part 1: Introduction to key management (ISO 11568-1:1994)

EN ISO 11568-2:1996

Banking - Key management (retail) - Part 2: Key management techniques for symmetric ciphers (ISO 11568-2:1994)

EN ISO 11568-3:1996

Banking - Key management (retail) - Part 3: Key life cycle for symmetric ciphers (ISO 11568-3:1994)

Ei huvita.

EN ISO/IEC 7501-1:1995

Identification cards - Machine readable travel documents - Part 1: Machine readable passport (ISO/IEC 7501-1:1993)

Ei huvita.

EN ISO/IEC 7810:1996

Identification cards - Physical characteristics (ISO/IEC 7810:1995)

Võtab ISO kui üldse.

EN ISO/IEC 7811

Salvestusmeetodid pigem ISO-lt. Lugejate arv võiks olla 50.

EN ISO/IEC 7812

See läks ülevõtmisse.

EN ISO/IEC 7813:1996

Identification cards - Financial transaction cards (ISO/IEC 7813:1995)

Ei huvita.

EN ISO/IEC 7816-4:1996

Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange (ISO/IEC 7816-4:1995)

Kas see või ISO. Süsteemide programmeerijatele vajalik. Tiitelleht.

EN ISO/IEC 7816-5:1995

Identification cards - Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers (ISO/IEC 7816-5:1994)

Läks ülevõtmisse.

EN**ISO/IEC****7816-5:1995/A1:1997**

Identification cards - Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers - Amendment 1 (ISO/IEC 7816-5:1994/Amd 1:1996)

EN ISO/IEC 7816-6:1997

Identification cards - Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements (ISO/IEC 7816-6:1996)

Tarkvaratootjatele huvitav (kas see või ISO). Tiitelleht.

EN ISO/IEC 10373:1995

Identification cards - Test methods (ISO/IEC 10373:1993)

Ei huvita.

EN ISO/IEC 10536-1:1994

Identification cards - Contactless integrated circuit(s) cards - Part 1: Physical characteristics (ISO/IEC 10536-1:1992)

Ei huvita.

Kokkuvõtteks:

Komplekssena pakub CEN standarditest eraldi huvi polüfunktsionaalne kaart:

1. PIN
2. Ühised andmeelemendid ISO 7816-6
3. Kaardi lukustamine
4. Võtmehaldus

4. SEIS JA FINEID STANDARDID

1995. aastal algatati Rootsis projekt SEIS (Secure Electronic Information in Society) Selle eesmärgiks oli turvaliste IT-lahenduste väljatöötamine ning propageerimine ühiskonnas. Konsortsiumis teevad koostööd Rootsi suuremad tööstuskonsernid, riigisasutused ning IT-firmad, teiste hulgas näiteks Nordbanken, Swedish Post, Ericsson, Volvo, ABB, SEB.

SEIS-projektist on välja kasvanud Rootsi riiklikud standardid, mis on kinnitatud SIS (*Swedish Institute of Standards*) poolt:

1. SS 614330: Electronic ID Application.
2. SS 614331: Electronic ID Certificate.
3. SS 614332: Electronic ID Card - Swedish Profile

Soome riigi ID-kaardi-alane standardimistegevus põhineb Rootsi SEIS-standarditel, mida on ka oluliselt edasi arendatud. Nn. FINEID standardiperekond kaasab ka rahvusvaheliste standardite (PKCS #15) tulemusi. Dokumendid on:

FINEID-S1 Electronic ID Application
FINEID-S3 Certificate Specification
FINEID-S4-1 FINEID Implementation profile 1 (16.04.1999)
FINEID-S5 Directory Specification

FINEID-P18 FINEID pilot card and certificate specification

FINEID-dokumendid on saadaval Internetis aadressil

<http://www.vaastorekisterikeskus.fi/fineidspec.htm>

Eesti ID-kaardi standardiseerimisel on otstarbekas aluseks võtta just FINEID standardid.

5. IETF STANDARDID

Kuigi IETF (*Internet Engineering Task Force*) ei tegele otseselt ID-kaardi standarditega, on tal oluline roll PKI-alaste rahvusvaheliste standardite väljatöötusel, mis omakorda on aluseks PKI tehnoloogial põhinevates ID-kaardi süsteemides. Esitame siinkohal lühiülevaate IETF-i PKIX-töögrupi poolt välja töötatud standarditest ja standardikavanditest. Lisamaterjali PKIX kohta leiab võrgust <http://www.ietf.org/html.charters/pkix-charter.html>.

RFC 2459: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

Staatus: proposed standard

Antud standard algab sissejuhatusesega PKI üldpõhimõtetest (sertifikaadid, CA-d, CRL-d). Edasi defineeritakse Internetis kasutamiseks mõeldud X.509 sertifikaadi ja CRL-i formaat (ning üldkasutatavad laiendused) ja pannakse paika sertifikaatide töötlemise reeglid.

Seotud standardid:

Sellest lähtub enamik PKIX standardeid.

RFC 2510: Internet X.509 Public Key Infrastructure: Certificate Management Protocols

Staatus: proposed standard

Standard kirjeldab protokolle, mida kasutatakse sertifikaatide haldamiseks (sertifikaadi taotlemine, RA ja CA vaheline suhtlus jms.).

Dokument sisaldab:

- PKI arhitektuuri, milles on RFC 2459-ga võrreldes täpsemalt määratletud, millised subjektid omavahel milliseid protokolle kasutavad.
- Operatsioonidele esitatavaid nõudeid ja kitsendusi.
- Protokollides kasutatavate andmestruktuuride kirjeldust.
- PKI poolt nõutavate funktsioonide loetelu.
- Lühiülevaadet erinevate transpordiprotokollide kasutamise kohta.

Seotud standardid:

RFC 2549 defineerib üldise arhitektuuri ja sertifikaadi formaadi.

RFC 2511 defineerib sertifikaadi taotlemise teate formaadi.

PKCS #10 (RFC 2314) sertifikaadi taotlemise teate alternatiivne formaat.

RFC 2511: Internet X.509 Certificate Request Message Format

Staatus: proposed standard

Tegemist on mõnevõrra põhjalikuma standardiga kui PKCS #10 (RFC 2314). Lisaks sertifikaaditaotluse formaadile on paika pandud ka *challenge/response* protokoll, millega CA teeb kindlaks, et sertifikaadi taotleja tõepoolest omab antud avaliku võtmega sobivat salajast võtit.

RFC 2527: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

Staatust: informational

Standard annab juhendeid sertifitseerimispõhimõtete (*certification policy* ja *certification practice statement*) koostamiseks. Tekst põhineb suure osas *American Bar Association*'i vastavasisulisel standardil.

RFC 2528: Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates

Staatust: informational

Standard sisaldab KEA kasutamiseks vajalikke definitsioone.

Seotud standardid:

Aluseks on RFC 2459.

RFC 2559: Internet X.509 Public Key Infrastructure: Operational Protocols - LDAPv2

Staatust: proposed standard

Kirjeldataud on LDAPv2 operatsioone, millega on võimalik hallata kataloogis olevaid sertifikaate.

Seotud standardid:

RFC 1777 sisaldab LDAPv2 operatsioonide täielikku loetelu.

Muudetakse varsti aegunuks draft-ietf-pkix-ldap-v3-01.txt poolt.

RFC 2587: Internet X.509 Public Key Infrastructure: LDAPv2 Schema

Staatust: proposed standard

Standard defineerib alamhulga LDAPv2 võimalustest, mis on vajalikud LDAP protokollide kasutamiseks PKI raames.

Seotud standardid:

RFC 1777 sisaldab LDAPv2 operatsioonide täielikku loetelu.

RFC 2560: X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

Staatust: proposed standard

OSCP on protokoll, mille abil on võimalik sertifikaadi staatuse reaajas kindlaks teha. Defineeritud on päringu ja vastuse formaat ning nõuded tagastatavale vastusele. Transpordiprotokolli valik on jäetud lahtiseks.

Seotud standardid:

Kasutatud on RFC 2459-s defineeritud mõisteid ja ASN tüüpe.

RFC 2585: Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP

Staatust: proposed standard

Kirjeldatakse HTTP ja FTP kasutamist sertifikaatide ja CRL-de hankimiseks vastavatest andmebaasidest.

STANDARDIPROJEKTID (draftid)

Internet X.509 Public Key Infrastructure PKIX Roadmap

Failinimi: draft-ietf-pkix-roadmap-04.txt

Dokument võtab kokku PKIX töögrupi poolt tehtud töö ning avab tehtud otsuste tagamaid.

Tekst ise koosneb järgmistest osadest:

- PKIX sertifitseerimise ideoloogia tutvustamine (analoogiline RFC 2459-le, kuid selgem ja tehnilistest üksikasjadest vaba).
- PKIX poolt väljastatud dokumendid. Iga dokumendi jaoks on ära toodud lühike sisukokkuvõte ning staatust (eriti kasulik on see draftide puhul, et teada, kas mingil tekstil on lootust standardiks pääseda).
- Nõuanded realiseerijatele, kus selgitatakse põhjalikumalt mõningaid vaidlusalaseid küsimusi.

Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

Failinimi: draft-ietf-pkix-new-part1-00.txt

Antud draft peaks tulevikus asendama RFC 2459-t. Eelmisest põhjalikumalt on kirjeldatud sertifikaatide valideerimise küsimusi, eriti sertifikaatide ahela valideerimist. Samuti on lisatud materjal CRL-ide valideerimise kohta.

Internet X.509 Public Key Infrastructure: Time Stamp Protocol (TSP)

Failinimi: draft-ietf-pkix-time-stamp-04.txt

Kirjeldatakse lihtsat ajatempli protokoll, kus klient saadab serverile päringu ning saab vastuseks ajatempli.

Internet X.509 Public Key Infrastructure: Data Certification Server Protocols

Failinimi: draft-ietf-pkix-dcs-03.txt

Defineeritakse protokoll, mille abil notar (*Data Certification Server*) saab pakkuda järgmiseid teenuseid:

- Andmete omamise kinnitus – tõend, et klient omas andmeid antud ajahetkel.
- Signatuuride sertifitseerimine – tõend, et signatuur oli kehtiv antud ajahetkel.
- Avaliku võtme sertifikaadi sertifitseerimine – tõend, et sertifikaat oli kehtiv antud ajahetkel.

Seotud standardid:

draft-ietf-pkix-time-stamp-02.txt kirjeldab ajatempliteenust, mis moodustab alamhulga DCS serveri poolt pakutavatest võimalustest.

Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

Failinimi: draft-ietf-pkix-qc-02.txt

Qualified Certificate on sertifikaat, mis antakse välja füüsilisele isikule ja mis peaks võimaldama isiku ühest identifitseerimist. Antud standard esitab nõudeid, millele peavad vastama taolised sertifikaadid.

Kvalifitseeritud sertifikaatide kohta saab infot aadressilt

<http://www accurata.se/QC/main.html>

Seotud standardid:

RFC 2459 defineerib sertifikaadi formaadi.

Basic Event Representation Token

Failinimi: draft-ietf-pkix-bert1-01.txt

Standard kirjeldab andmestruktuuri, millega on võimalik esitada mingit sündmust. Mõeldud kasutamiseks näiteks ajatemplite süsteemis.

Internet X.509 Public Key Infrastructure: Extending trust in non repudiation tokens in time

Failinimi: draft-ietf-pkix-extend-trust-non-repudiation-token-00.txt

Kirjeldatakse meetodeid, millega on võimalik pikendada aeguma kippuvate ajatemplite ja signatuuride eluiga (näiteks juhul kui kasutatud võtmepikkus osutub ebapiisavaks). Üldjuhul seisnevad need meetodid andmete teistkordsel ajatembeldamisel ja/või notariseerimisel.

Seotud standardid:

draft-ietf-pkix-dcs-00.txt kirjeldab notariseerimisprotokolli.

draft-ietf-pkix-time-stamp-01.txt kirjeldab ajatempli protokolli.

Internet X.509 Public Key Infrastructure: Operational Protocols - LDAPv3

Failinimi: draft-ietf-pkix-ldap-v3-01.txt

Sama, mis RFC 2559, kuid järgmise LDAP versiooni jaoks.

Seotud standardid:

Nõutakse ühildumist ka standarditega RFC 2559 ja RFC 2587.

An Internet Attribute Certificate Profile for Authorization**Failinimi:** draft-ietf-pkix-ac509prof-01.txt

Atribuutsertifikaat seab vastavusse isiku volitused ning nime (või isikusertifikaadi numbri). Atribuutsertifikaate kasutatakse näiteks isikute õiguste kindlakstegemiseks arvutisüsteemis.

Antud standard defineerib atribuutsertifikaadi formaadi ja töötlemise korra.

Seotud standardid:

RFC 2459 defineerib aluseks viidatava sertifikaadi formaadi.

Limited Attribute Certificate Acquisition Protocol**Failinimi:** draft-ietf-pkix-laap-00.txt

Defineeritakse laiendused RFC 2510-s toodud protokollile, mis võimaldavad kiireid ja lihtsaid atribuutsertifikaatide kohta tehtavaid päringuid. Suurema osa tööst (kehtivus, mitme sertifikaadi seast sobiva valimine) teeb ära server. Protokoll on mõeldud kasutamiseks kompaksete ja lühikese elueaga sertifikaatide jaoks. Pikema elueaga sertifikaatide puhul võib osutada otstarbekamaks LDAP serveri kasutamisele.

Seotud standardid:

RFC 2510 defineerib kasutatava protokoll skeleti.

Certificate Management Messages over CMS**Failinimi:** draft-ietf-pkix-cmc-05.txt

Defineeritakse protokoll sertifikaadi taotlemiseks, kasutades olemasolevaid vastavasisuliste teadete süntaksi standardeid.

Seotud standardid:

On püütud saavutada ühilduvust järgmistega:

RFC 2630: Cryptographic Message Syntax

PKCS #10 (RFC 2314): Certification Request Syntax

RFC 2511: Internet X.509 Certificate Request Message Format

Simple Certificate Validation Protocol (SCVP)**Failinimi:** draft-ietf-pkix-scvp-01.txt

SCVP on protokoll, mille abil klient saab serverilt küsida sertifikaadi korrektsust (mitte segi ajada staatusega, mille tagastab OCSP). Sobib kasutamiseks järgmistel juhtudel:

- Kui klient ei suuda/taha ise kõiki sertifikaatide ahelaid läbi käia.
- Kui asutus soovib turvapoliitikat tsentraalselt hallata (näiteks suvalisel hetkel ümber defineerida CA, keda kõige rohkem usaldatakse).

Seotud standardid:

RFC 2560 defineerib OSCP, mis on veidi sarnane antud protokolliga.

RFC 2459 defineerib üldise arhitektuuri ja sertifikaadi formaadi.

OCSP Extensions

Failinimi: draft-ietf-pkix-ocsp-00.txt

Defineeritakse laiendused OSCP-le, mis sisaldavad SCVP protokolliga pakutavaid funktsioone.

Seotud standardid:

RFC 2560 defineerib aluseks oleva OSCP protokolliga.

draft-ietf-pkix-scvp-01.txt defineerib analoogiliste võimalustega protokolliga.

Using HTTP as a Transport Protocol for CMP

Failinimi: draft-ietf-pkix-cmp-http-00.txt

RFC 2510 jaotises 5 kirjeldatud protokolliga realiseerimine HTTP abil.

Using TCP as a Transport Protocol for CMP

Failinimi: draft-ietf-pkix-cmp-tcp-00.txt

RFC 2510 jaotises 5.2 kirjeldatud protokolliga edasiarendus.

6. MUUD STANDARDID

Peale eeltoodute moodustavad olulise osa rahvusvahelisest standardipagasist veel mitmesugused Euroopa standardi-initsiatiivid ning *de facto* tööstusstandardid, mis on välja arendatud firmade (või nende koostöökogude) poolt. Toome siin ära tähtsamad:

6.1 RSA PKCS

Firma RSA Inc. (nüüd: Security Dynamics) poolt on koostöös teiste firmadega rida huvipakkuvaid *de facto* tööstusstandardid, mida tuntakse lühendi **PKCS** (*Public-Key Cryptography Standards*) kaudu. Täpsem info on saadaval <http://www.rsasecurity.com/rsalabs/pkcs/>

Alljärgnevalt on toodud osaliselt kommenteerituna oluliste PKCS standardite nimistu. Iseäranis huvipakkuvad ID-kaardi seisukohalt on PKCS #11 (Cryptoki) ja PKCS #15.

PKCS #1 (RFC 2437): RSA Cryptography Specifications version 2.0

PKCS #3: Diffie-Hellman Key Agreement Method

PKCS #6: Extended-Certificate Syntax Standard

Laiendab X.509 sertifikaadi definitsiooni, tekitades võimaluse mitmesuguste atribuutide lisamiseks.

PKCS #7 (RFC 2315): Cryptographic Message Syntax

Standard defineerib viisi, kuidas kasutada edastatavate teadete juures krüptograafilisi primitiive (signatuur, krüptimine jms.). Lisaks edastatavate teadete formaadile kirjeldatakse ka teadete töötlemiseks vajalikke protseduure. Puudutatakse ka võtmevahetuse probleeme, kuid sertifikaatide haldus standardiseerimisele ei kuulu. Antud standardil põhineb enamik krüptograafiaga seotud standardeid.

Seotud standardid:

Sama asja uuem ja parem variant on RFC 2630.

PKCS #9 - Selected Attribute Types

Defineeritakse mitmeid atribuute PKCS #6 tarvis.

Seotud standardid:

PKCS #6 sisaldab sertifikaadi formaadi definitsiooni.

PKCS #10 (RFC 2314): Certification Request Syntax version 1.5

Defineeritakse formaat teatele, mis saadetakse CA-le sertifikaadi omandamise eesmärgil. Teade koosneb kolmest osast:

- Sertifikaadi taotlemise informatsioon: nimi, avalik võti, muu info.
- Signatuuri algoritmi tunnus.
- Esimeses punktis olevate andmete signatuur.

Standard ei käsitle CA poolt nõutavaid tegevusi, s.h. tagastatava sertifikaadi formaati.

Seotud standardid:

Toetab PKCS #6 atribuute.

PKCS #11: Cryptographic Token Interface Standard

PKCS #15: Cryptographic Token Information Format Standard

6.2 ETSI

ETSI (*European Telecommunications Standards Institute*) on Euroopa Komisjoni poolt sponsoreeritav organisatsioon, mis toodab vajalikke standardeid. Täpsem info aadressilt <http://www.etsi.org>. Huvipakkuvad dokumendid on:

Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services

Dokumendi number: EG 201 057 V1.1.2 (1997-07)

Dokument algab võrdlemisi pika sissejuhatusega, milles seletatakse usaldatava kolmanda osapoolega seotud operatsioonide põhimõtteid, TTP poolt pakutavaid teenuseid, seaduslaseid küsimusi jms. Lisaks esitatakse üldine raam, millele peaksid vastama TTP kohta mitmesuguseid nõudmisi esitavad standardid.

Electronic signature standardization for business transactions

Täistekst, pikem kirjeldus

Dokumendi number: ES 201 733 *final draft* (23.11.1999)

<http://www.etsi.org/sec/el-sign.htm>

Standard lähtub PKIX poolt koostatud dokumentidest ning püüab üles ehitada arhitektuuri, mille abil oleks võimalik produtseerida kohtus aktsepteeritavaid digitaalsignatuure.

Standard defineerib erinevad digitaalsignatuuri liigid (harilik signatuur, ajatempliga signatuur, arhiveeritud signatuur jne.), nende formaadid ning samuti muude vajalike asjade (sertifikaat, CRL) formaadid. Kirjeldatakse signatuuri verifitseerimise protsessi. Signatuur peab sisaldama ka viidet signeerimispoliitikale, mis kirjeldab konkreetse signatuuri tekitamise ja verifitseerimise meetodikat, loetleb usaldatavad kolmandad osapooled, määrab osapoolte vastutuse määra jms.

Seotud standardid:

RFC 2630

PKIX poolt välja antud standardid

6.3 INFOSEC

INFOSEC peaks olema samuti Euroopa komisjoni poolt sponsoreeritud organisatsioon, mis andmeturbega tegeleb. Digitaalsignatuuri osas pole küll veel standarditeni jõutud, kuid selleteemalisi aruandeid võib lugeda aadressilt <http://www.cordis.lu/infosec/>.

6.4 OPEN GROUP

Open Group on tarkvaratootjate poolt sponsoreeritav organisatsioon, mis püüab saavutada ühilduvust eri tootjate poolt tehtud asjade vahel. Täpsem info aadressilt <http://www.opengroup.org>. Open Group'i materjalides pakub huvi juhend:

Architecture for Public-Key Infrastructure (APKI)

Document Number: G801

Antud dokument lähtub IETF PKIX standarditest ning püüab kirjeldada avaliku võtme infrastruktuuri. Juhend loetleb PKI poolt pakutavaid teenuseid ning loetleb standardeid, mida oleks võimalik nende teenuste realiseerimisel kasutada

6.5 PKI FORUM

PKI Forum on värskest (13.12.1999) moodustatud mittetulunduslik koostööorganisatsioon infoturbega tegelevate firmade vahel. PKI Forum on endale ülesandeks seadnud PKI infrastruktuuri ning sellel põhinevate toodete ja teenuste kasutuselevõtu kiirendamise. Ilmselgelt pole veel mingitele tulemustele jõutud. Lisainformatsiooni saab aadressilt <http://www.pkiforum.org/>.

KOKKUVÕTE

Eestis ei ole palju kaarditootjaid, need vähesed ostavad originaali. Eestis on süsteemide integreerijad ja tarkvaratootjad, kes suudavad ingliskeelt lugeda. Seega sobib ülevõtus tiitellehe meetod.

Kas ülevõtmisel eelistada ISO või CEN standardeid? Kui ISO variant on olemas, siis sõltub kõik finantsvõimalustest. Kui raha Euroopa standardite ülevõtmiseks on ja ISO omade jaoks mitte, siis võib vastava Euroopa standardi võtta.

PKIX standardeid pole vaja “üle võtta”, need kehtivad *de facto* piirideta Interneti maailmas niigi.

Eesti ID-kaardi standardimisel on mõistlik aluseks võtta FINEID standardid, PKCS#15 ja IETF-I Qualified Certificates standardid. Sellest on pikemalt juttu eraldi töös Eesti ID-kaardi standardiseerimise kohta.