



Küberneetika AS
Infotehnoloogia osakond

Dok. DO-ST-T-24-1299

EESTI STANDARDIKAVANDID EID-KAARTIDE VALDKONNAS

Töö täitja:

Olev Sepp

Tallinn 1999



ANNOTATSIOON

Eesti ID-kaardi programmi raames on käivitunud või käivitumas esimesed pilootprojektid ning on tekkinud reaalne vajadus ühiste ID-kaardi standardide järele, mis hõlbustaksid pilootprojektides kasutatavate kaartide valikut, rakenduste loomist ning kaartide aktsepteerimist. Käesolevas dokumentides vaadeldakse tulevaste Eesti EID-kaartide standardite loomise alusdokumente ja -standardeid ning antakse võimalikud lähtekohad Eesti EID-kaardi standardiseeria koostamiseks.

SISUKORD

1. SISSEJUHATUS	4
2. ELEKTROONILISE IDENTIFITSEERIMISE (EID) RAKENDUS: STANDARDIETTEPANEK.....	4
2.1 Alusdokumendid	4
2.2 Argumendid	4
2.3 Ettepanek	5
3. EID-SERTIFIKAAT: STANDARDIETTEPANEK	5
3.1 Alusdokumendid	5
3.2 Argumendid	5
3.3 Ettepanek	6
4. EID-KAARDI PROFIL: STANDARDIETTEPANEK.....	6
4.1 Alusdokumendid	6
4.2 Argumendid	6
4.3 Ettepanek	7
5. LISAD.....	8
5.1 Mõisted	8
5.2 ISO-standardid	11
5.3 SEIS-dokumendid	12
5.4 FINEID-dokumendid.....	12
5.5 Saksa digitaalalkirjakaardi spetsifikatsioon.....	12
5.6 Olulised RSA PKCS-seeria standardid	13
5.7 IETF-PKIX internetidokumendid	13
5.7.1 RFC 2459: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile	13
5.7.2 <i>Internet Draft</i> : Internet X.509 Public Key Infrastructure Qualified Certificates Profile	13
5.7.3 <i>Internet Draft</i> : Internet X.509 Public Key Infrastructure Certificate and CRL Profile	14

1. SISSEJUHATUS

Eesti ID-kaardi programmi läbiviimiseks on vajalik kehtestada Eesti EID-kaardi alased standardid, mida järgiksid tulevikus Eestis kõik väljaantavad EID-kaardid.

Käesoleva töö eesmärgiks on esitada konkreetset ettepanekud Eesti standardikavanditeks EID-kaartide valdkonnas. Töö aluseks on võetud Rootsi (SEIS-seeria ning riiklikud SIS-standardid) ja Soome (FINEID-seeria spetsifikatsioonid) vastavad dokumendid, samuti rahvusvaheliste standardiorganisatsioonide (RSA Labs PKCS-seeria, ISO, IETF-PKIX jt.) vastavad arendusdokumendid.

Rootsi ja Soome töödest lähtutakse põhjusel, et neis riikides on viimastel aastatel toimunud kõige intensiivsem arendustöö EID-kaartide vallas. Soomes käivitus riiklik EID-kaardi projekt 1. detsembril 1999 ning Eestil on otstarbekas selle arengust ja tulemustest juhinduda kohaliku EID-kaardi programmi elluviimisel.

2. ELEKTROONILISE IDENTIFITSEERIMISE (EID) RAKENDUS: STANDARDIETTEPANEK

Standardis kirjeldatakse EID(elektrooniline identifitseerimine)-rakenduse kataloogstruktuuri ja andmefailide sisu. Defineeritakse juurkataloog ja EID-rakenduse alamkataloogid ning neis sisalduvad failid. Kirjeldatakse kataloogide poole pöördumise mehhanisme ning EID-rakenduse kasutusalgoritmi.

2.1 ALUSDOKUMENDID

Sobivate alusdokumentidena (vt. ka p.5 Lisad) võib selle standardi jaoks nimetada järgmisi:

- a) Rootsi standard: SIS 614330 (ehk SEIS S1 dokument)
- b) Soome FINEID-spetsifikatsioon: FINEID-S1 Electronic ID Application v1.1
- c) Saksa DIN standard: DIN.SIG NI-17.4 v1.0
- d) RSA Labs: PKCS#15 v1.0 koos Lisaga #1

2.2 ARGUMENDID

A. Rootsi SEIS-S1 sisaldub PKCS#15-s.

B. Soome FINEID-S1 v1.1 väidab, et nad on arvesse võtnud kõik viimased PKCS#15 modifikatsioonid (ka. Lisa #1). Failide struktuur ja sisu on vastavalt PKCS#15-le, kaardi käsustik põhineb ISO/IEC 7816-4 ja ISO/IEC FDIS 7816-8. Väidetavalt on arvesse võetud ka Saksa DIN.SIG dokumenti, näiteks krüptoalgoritmide kodeeringud on sealt pärit.

C. PKCS#15 peamised puudused Saksa (DIN.SIG) poolelt vaadatuna:

- 1) biomeetria puudumine
- 2) rakenduste poole pöördumise mehhanism nõrgalt lahendatud
- 3) autentimisteenuse ja -protokollide puudulikkus
- 4) nõrk toetus signeerimisfunktsioonile
- 5) toetuse puudumine cv-sertifikaatidele (*card verifiable certificates*)
- 6) lisaks väiksemad puudujäägid

Nad on andnud terve rea soovitusi nende puuduste kõrvaldamiseks, muuhulgas:

- 1) soovitavad PKCS#15-le lisada eraldi signeerimist käsitleva peatüki
- 2) võtta kasutusele SSD (*security service descriptor*), et defineerida eraldi kõik kaardis kasutatavad krüptoteenused (kasutaja autentimine, signeerimine, võtmekrüpteerimine, muu autentimine)

Samas on sakslased nõus sellega, et DIN.SIG ning PKCS#15 rakendused suudavad kaardil kooseksisteerida ning nad ei välista teineteist. Lähenemiseks tuleb aga arendada eelkõige PKCS#15 standardit.

D. RSA Labs on tutvustanud oktoobris 1999 oma nägemust PKCS#15 uuest versioonist ver1.1 ning prognooside järgi võib see valmis saada 1Q/2000. Seal ei lahendata küll veel kõiki sakslaste tõstetud probleeme, kuid siiski viiakse muuhulgas ka mitmed soovitatud muudatused sisse (näiteks on mainitud biomeetriat).

2.3 ETTEPANEK

Võtta Eesti standardi aluseks FINEID S1 v1.1 dokument, mis omakorda põhineb standardil PKCS#15.

On tõenäoline, et PKCS#15 läheneb järgmise aasta jooksul DIN.SIG-le. Soomlased kasutavad juba oma ID-kaardi projektis PKCS#15-l põhinevat kaarti. Eesti senine ainuke ID-kaardi pilootprojekt kasutab samuti PKCS#15 kaarte. DIN.SIG rakendusliku poolega on esialgu väljaspool Saksamaad vähe kogemusi.

Standardidokumendi *FINEID-S1 Electronic ID Application v1.1* väljatrükk on lisatud käesolevale aruandele.

PKCS#15: Cryptographic Token Information Format Standard v1.0 ja

PKCS#15: Cryptographic Token Information Format Standard v1.0 Amendment 1 Draft #1 on mahalaaditavad Internetist aadressilt

<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html>

3. EID-SERTIFIKAAT: STANDARDIETTEPANEK

Standard kirjeldab EID-rakenduses kasutatavate (isiku)sertifikaatide omadused, vormingu ja sisu. Esitatakse nende sertifikaatide laiendused ja kasutamise tingimused.

3.1 ALUSDOKUMENDID

Võimalike alusdokumentidena (vt. ka p.5 Lisad) võib selle standardi jaoks nimetada järgmisi:

- a) Rootsi standard: SIS 614331 (ehk SEIS S3 dokument)
- b) Soome FINEID-spetsifikatsioon: FINEID-S3 Certificate specification v0.93
- c) RFC 2459: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
- d) *Internet-Draft*: Internet X.509 Public Key Infrastructure Qualified Certificates Profile (*QC-Profile*)
- e) I-D: Internet X.509 Public Key Infrastructure Certificate and CRL Profile

3.2 ARGUMENDID

A. Rootsi standard allub *RFC2459*-le.

B. Soomlased peatasid oma dokumendi FINEID-S3 arenduse.

- C. Soomlased deklareerisid, et nende EID-sertifikaatide aluseks on *RFC2459* ja *QC-Profile* arendusdokumendid
- D. *RFC2459* uus versioon on parem kui eelmine.

3.3 ETTEPANEK

Võtta Eesti standardi aluseks sarnaselt Soomele dokumendid *RFC2459* ja *Qualified Certificates*.

Eelpoolnimetud dokumendid on mahalaaditavad Internetist järgmistelt aadressitelt:

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

<http://www.ietf.org/rfc/rfc2459.txt>

Internet Draft: Internet X.509 Public Key Infrastructure Qualified Certificates Profile

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-qc-02.txt>

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

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-00.txt>

4. EID-KAARDI PROFIIL: STANDARDIETTEPANEK

Standardis kirjeldatakse Eesti EID-kaartide rakendusprofiil, st. määratakse väljaantavatele kaartidele muuhulgas:

- 1) Kaardi parameetrid ja füüsilised omadused (formaadi tüüp ning visuaalselt loetavate andmete paigutus kaardil)
- 2) Krüpteerimisvõtmete kasutusala ja omadused, näit. pikkus bittides
- 3) PIN-koodide funktsioonid
- 4) Kaardikohaste failide ligipääsutingimused
- 5) Nõuded kaardis paiknevatele sertifikaatidele

4.1 ALUSDOKUMENDID

Võimalike alusdokumentidena (vt. ka p.5 Lisad) võib selle standardi jaoks nimetada järgmisi:

- a) Rootsi standard: SIS 614332 (ehk SEIS S4 dokument)
- b) Soome FINEID-spetsifikatsioon: FINEID-S4-1 Implementation Profile 1 ver1.1

4.2 ARGUMENDID

A. Rootsi dokument on aegunud.

B. Soome FINEID-S4-1 Implementation Profile ver1.1 põhineb järgnevatel dokumentidel:

- 1) PKCS#15 elektroonilise identifitseerimise profiil
- 2) *RFC2459*
- 3) *Qualified Certificates Profile*



4.3 ETTEPANEK

Ülaltoodud asjaoludele tuginedes võtta Eesti EID-kaardi rakendusprofiili aluseks järgmised dokumendid:

- 1) PKCS#15
- 2) *RFC2459*
- 3) *Qualified Certificates Profile*

ning Eesti rakendusprofiili eeskujuna kasutada esialgselt dokumenti *FINEID-S4-1 Implementation Profile 1 v1.1*, mille väljatrükk on lisatud ka käesolevale aruandele.

5. LISAD

5.1 MÕISTED

Dokumendi tekstis esinevate ja valdkonda puudutavate mõistete ja lühendite lühiseletused.

Termin	Ingliskeelne vaste	Seletus
API	API (Application Program Interface)	Rakendusliides (rakendusprogrammi ja operatsioonisüsteemi vahel)
Avalik võti	Public key	Meetod krüptoloogias, kus infoga on seotud 2 võtit: avalik ja privaatne. Avalik võti on kõigile teada, salajane võti vaid selleks volitatuile. Vt. ka privaatvõti
CEN	CEN	European Standards Center pr. k.
DES	Data Encryption Standard	Salajasel võtmel baseeruv krüpteerimisalgoritm
Digitaalalkiri	Digital Signature	Andmekogumile lisatud andmed või rakendatud transformatsioon, mis võimaldab andmekogumi saajal kindlaks andmete allikat ja terviklust ning kaitsta (nt saaja sooritatava) võltsimise eest
Elektrooniliselt kustutatav programmeeritav ainult loetav mälu	EEPROM	Kiipkaartides kasutatav mäluliik. Sisu on võimalik ülekirjutada.
Elektrooniline ID	Electronic ID (EID)	Elektrooniline identiteet (ID-kaardi korral kaardis paiknevad salajased võtmed, sertifikaadid ja muu informatsioon)
Elliptilistel kõveratel baseeruv krüptosüsteem	ECC - Elliptic Curves Cryptography	Avaliku võtme krüptosüsteem, võtmepikkus efektiivsem kui RSA-l
FINEID	Finnish Electronic Identification - FINEID	Soome dokumentide seeria elektroonilise identifitseerimise standardimiseks
HTTP	HTTP (Hypertext Transmission Protocol)	Protokoll HTML-dokumentide vahetuseks Internetis
Isikutuvastus-kood, PIN-kood	Personal identification number, PIN	Isikuidentifitseerimisnumber, 4 kuni 12-kohaline number, kasutatakse paroolina kaardivaldaja autentimisel
IDEA	International Data Encryption Algorithm	Salajasel võtmel baseeruv krüpteerimisalgoritm
Identifikaator, ID	Identification	Unikaalne objekti tunnuscode



	number	
Identifitseerimine	Identification	Objekti või isik identiteedi kontrollimine
IETF	IETF (Internet Engineering Task Force)	
IT	IT (Information Technology)	Infotehnoloogia
Kaardi väljaandja	Card issuer	Asutus (või ta vahendaja), kes väljastab kaardivaldajale kaardi
Kaardivaldaja	Cardholder	Isik, kellele kaart on välja antud
Kiibi operatsioonisüsteem COS	Chip operating system, COS	Kaardivalmistaja poolt protsessorikaarti salvestatud püsitarvara, mis realiseerib lugejale nähtavad kaardi andmetöötlusfunktsioonid
Kiip, integraallülitus	Integrated circuit (IC)	Kaarditehnikas: integraallülitus, mis on paigaldatud kiipkaarti andmetöötlus- ja mälu funktsioonide täitmiseks
Kiipkaart	Integrated circuit card (ICC)	Kaart, milles on üks või mitu kiipi
Krüpteerimine	Encryption	Informatsiooni töötlusviis, mille puhul muudetakse informatsioon loetamatuks neile, kes ei oma selleks vajalikke teadmisi või õigusi
Kontaktivaba kaart	Contactless card	Kiipkaart, millel ei ole elektrilisi sidestuskontakte
Kontaktkaart	Card with contacts	Siin: ISO 7816/2 standardile vastavate elektriliste kontaktidega kiipkaart
LDAP-protokoll	LDAP (Lightweight Directory Access Protocol)	Klient-server protokoll kataloogiteenuste kasutamiseks
Mask	Mask	Kiipkaardi protsessori juhtprogramm
Pangaterminal, ATM	Automated teller machine	Seade, mis identifitseerib ja sooritab lihtsamaid pangaoperatsioone, nt. Väljastab sularaha
PKCS	Public Key Cryptography Standards	Seeria avaliku võtme krüptograafial põhinevaid standardidokumente, arendajaks RSA Labs
PKI	PKI (Public Key Infrastructure)	Avaliku võtme rakenduskeskkond
Polüfunktsionaalne kaart	Multifunctional card	Kiipkaart, kus on salvestatud mitme erineva rakenduse jaoks vajalikud andmed, annab märgatavaid eeliseid avatud kaardisüsteemis
Privaatvõti	Private key	Võtmepaarist pärit krüpteerimisvõti, mida teab vaid selle omanik. Vt. Avalik võti
Protsessor	Processor	Andmetöötlusfunktsioone täitev elektronlülitus
Rakendus	Application	Programm (nt. Kiipkaardis), mis annab talle



		teatud välised funktsioonid
Rakenduse pakkuja	Application supplier	Juriidiline isik, kes vastutab rakendusfaili eest peale selle eraldamist
Rakendusfail	Application data file	Ühte või mitut teenust toetav fail kiibis
Rakendusfaili eraldamine	Application data file allocation	Turvaline rakendusfailile kiibis ruumi varumine selle järgnevas kasutamiseks rakenduse pakkuja poolt
Rakendusfaili personaliseerija	Application data file personalizer	Juriidiline isik, kes laeb algsed turva- ja tööparameetrid rakendusfailile kiibis määratud ruumi
Räsifunktsioon	Hash-function	Matemaatiline teisendus, mis seab sõnumile (suvalisele andmekogumile) vastavusse fikseeritud pikkusega andmekogumi (nn sõnumilühendi), kusjuures raske on leida kahte erinevat sõnumit, mille sõnumilühendid ühtivad.
Salajane võti	Secret key	Krüpteerimisvõti, mida teavad kõik omavahel konkreetset krüpteeritud informatsiooni vahetavad osapooled
SEIS	SEIS (Secured Electronic Information in Society)	Rootsis algatatud projekt elektroonilise ID rakenduskeskkonna arenduseks. SEISi kuuluvad mitmed suured riiklikud asutused ja erafirmad
SK - Sertifitseerimiskeskus	CA - Certification Authority	Institutsioon, mis annab välja sertifikaate
SP - Sertifitseerimispoliitika	CP - Certification Policy	Reeglite kogum, millele toetub oma tegevuses sertifitseerimiskeskus
Sertifikaat	Certificate	Dokument, mis tõestab tema väljaandja ning omaniku identiteeti, sisaldab eelnevalt kokkulepitud informatsiooni
S/MIME	S/MIME (Secure Multipurpose Internet Mail Extensions)	Elektronposti laiendus e-mailide turvaliseks vahetamiseks
Sõnumilühend	Hash	Etteantud andmekogumile räsifunktsiooni rakendades saadud teine andmekogum
Terviklus	Integrity	Andmekogumi omadus: informatsiooni pole muudetud pärast tema loomist
TTP	TTP (Trusted third party)	Usaldatav osapool kaardisüsteemi infrastruktuuris

5.2 ISO-STANDARDID

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 FDIS 7816-8 Information technology - Identification cards - Integrated circuit cards with contacts. Part 8: Security related interindustry commands.

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

5.3 SEIS-DOKUMENDID

Järgnevalt esitatakse käesoleva dokumendi koostamisel kasutatud Rootsi SEIS grupiga seotud standardid ja spetsifikatsioonid koos dokumentide versiooninumbrite ja avaldamiskuupäevadega.

Riiklikud EID-kaardi standardid (avaldatud 14.09.1998):

SS 614330	Electronic ID Application	(SEIS S1)
SS 614331	Electronic ID Certificate	(SEIS S3)
SS 614332	Electronic ID Card - Swedish Profile	(SEIS S4)

Täiendavad, kuid praeguseks edasiarendamata dokumendid:

SEIS G05 SEIS Cards - Functional Requirements

SEIS - S10 SEIS Certificate Policy Ver 1.0 (august 1998)

SEIS-dokumendid on saadaval Internetis aadressil <http://www.seis.se>

5.4 FINEID-DOKUMENDID

Järgnevalt esitatakse käesoleva dokumendi koostamisel kasutatud Soome FINEID-spetsifikatsioonid koos dokumentide versiooninumbrite ja avaldamiskuupäevadega.

Aktuaalsed dokumendid:

FINEID-S1	Electronic ID Application	ver1.1 (24.10.1999)
FINEID-S4-1	FINEID Implementation profile 1	ver1.1 (23.11.1999)
FINEID-S5	Directory Specification	ver1.1 (30.11.1999)

Aegunud dokumendid:

FINEID-S3	Certificate Specification	ver0.93 (19.11.1998, arendus peatatud)
FINEID-P18	FINEID pilot card and certificate specification	(12.10.1998, arendati vaid pilootprojekti tarbeks)

FINEID tehnilised spetsifikatsioonid on saadaval Internetis aadressil <http://www.vaestorekisterikeskus.fi/fineidspec.htm>

5.5 SAKSA DIGITAALALLKIRJAKAARDI SPETSIFIKATSIOON

Saksa DIN standard DIN.SIG NI-17.4, mis spetsifitseerib kiipkaardiliidese digitaalallkirja kaardile vastavalt SigG (digitaalallkirja seadus) ja SigV-le (digitaalallkirja normatiivid).

DIN.SIG NI-17.4 ver1.0 (avaldatud 15.12.1998) on kättesaadav Internetis aadressil http://www.sit.gmd.de/SICA/papers/din_sig.pdf

5.6 OLULISED RSA PKCS-SEERIA STANDARDID

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

PKCS#11: Cryptographic Token Interface Standard

PKCS#15: Cryptographic Token Information Format Standard v1.0 (23.04.1999)

PKCS#15: Cryptographic Token Information Format Standard v1.0 Amendment 1
Draft #1 (20.10.1999)

RSA PKCS standardid on saadaval Internetis aadressil

<http://www.rsa.com/rsalabs/pubs/PKCS/>

5.7 IETF-PKIX INTERNETIDOKUMENDID

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

Dokument on avaldatud jaanuaris 1999. Kättesaadav aadressilt:

<http://www.ietf.org/rfc/rfc2459.txt>

Standard juhatab sisse PKI (*Public Key Infrastructure*) üldpõhimõtted, muuhulgas sertifikaadid, CA-d (*Certificate Authority*) ja CRL-d (*Certificate Revocation List*). Defineeritakse Internetis kasutamiseks mõeldud X.509 sertifikaadi ja CRL-i formaat (ning üldkasutatavad laiendused) ning fikseeritakse sertifikaatide käsitlemise reeglid.

5.7.2 Internet Draft: Internet X.509 Public Key Infrastructure Qualified Certificates Profile

Dokument on avaldatud oktoobris 1999 ning on järgnevad 6 kuud avatud kommentaarideks ja parandusteks (see ongi *Internet Draft* omapära). Kättesaadav aadressilt:

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-qc-02.txt>

Kvalifitseeritud sertifikaatide (*Qualified Certificates*) profiil põhineb dokumendile *RFC 2459: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile* ning on mõeldud kasutamiseks Internetis. Termin "kvalifitseeritud" viitab siinjuures sellele, et tegemist on erilise sertifikaadiga, mille sisu püüab järgida kehtivat seadusandlust. Kvalifitseeritud sertifikaat väljastatakse eranditult üksikisikule tõendamaks nende isikusamasust. Dokumendi eesmärgiks on defineerida üldine andmete esitusviis, sõltumata kohalikust seadusloomest. Sertifikaadi profiili loomisel püütakse siis tagada maksimaalsed võimalused kohalike seadusloomest tulenevate vajaduste rahuldamiseks. Oluline on ka märkida, et standardidokumendis ei defineerita kvalifitseeritud sertifikaatidele mingeid seadusloomealaseid nõudmisi.

Täiendavalt võib kvalifitseeritud sertifikaatide kohta kohta lugeda materjale aadressilt:

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

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

Dokument on avaldatud oktoobris 1999 ning on järgnevad 6 kuud avatud kommentaarideks ja parandusteks. Kättesaadav aadressilt:

<http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-00.txt>

Uus profiil põhineb dokumendile *RFC 2459: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile* ning peaks lähitulevikus hakkama seda asendama. Võrreldse alusdokumendiga on tehtud mitmeid parandusi ja selgitusi, kuid peamine erinevus on sertifikaadi ahelate käsitluses. Uues profiilis on põhjalikumalt kirjeldatud nimetatud ahelate valideerimist, valideerimise algoritmi ja muid seonduvaid nüansse. Lisaks X.509v3 laienduste põhjalikumale käsitlemisele on lisatud ka täiesti uus peatükk CRL-de valideerimisest.