

*Dok. DO-MM-C-5-0699*

Cybernetica

**Rakendusjuhised ID-kaardi pilootprojektide  
läbiviimiseks**

24 lk.

Töö täitja:

Olev Sepp

Tallinn 1999



## ANNOTATSIOON

Eesti ID-kaardi programm on jõudnud esimeste pilootprojektide algatamiseni. Nende läbiviimine ja tulemuste analüüs peaksid andma aluse Eesti ID-kaardi profiili koostamiseks. Käesolevad rakendusjuhised püüavad konkreetset pilootsüsteemi spetsifitseerimata anda üldiseid praktilisi suuniseid ID-kaardi alaste pilootprojektide läbiviimiseks Eesti ID-kaardi programmi eesmärkide raames.

## SISUKORD

<b>1. SISSEJUHATUS.....</b>	<b>4</b>
<b>2. ID-KAARDI PILOOTSÜSTEEMI LOOMINE.....</b>	<b>5</b>
2.1 Pilootsüsteemi koostisosad .....	5
2.2 Elektrooniline identifitseerimine.....	5
2.3 Sertifitseerimine .....	6
2.3.1 Sertifitseerimiskeskus .....	6
2.3.2 Sertifikaadid .....	6
2.3.3 Sertifitseerimispoliitika .....	7
2.4 ID-kaart pilootsüsteemis.....	8
2.4.1 Kaardi füüsilised ja tehnilised omadused.....	8
2.4.2 Kaardivaldaja identifitseerimine pilootsüsteemis .....	9
2.4.3 EID-rakendus kaardil .....	9
2.4.4 ID-kaardis paikneva info turvalisuse tagatised.....	9
2.5 ID-kaardi eluiga pilootsüsteemis.....	10
2.6 ID-kaardi poolt pakutavad teenused .....	11
2.6.1 Identifitseerimine ID-kaardiga .....	11
2.6.2 Digitaalsignatuur.....	11
2.6.3 Elektrondokumendi päritolu, autentsus ja terviklus.....	12
2.6.4 Elektrondokumentide ajaliste tingimuste ja salgamise vääramise verifitseerimine.....	12
2.6.5 Andmete krüpteerimine.....	12
2.6.6 Sideseansside krüpteerimine.....	12
2.7 Elektrondokumendi käsitlus pilootsüsteemis .....	13
2.8 Tarkvaraliidesed.....	13
2.9 Pakutavate teenuste turvanõuded .....	13
2.9.1 Teenuste turvasemed .....	13
2.9.2 Nõuded kasutatavatele krüptoloogilistele meetoditele.....	14
2.9.3 Soovitusi krüptoalgoritmide ja võtmepikkuse valikuks .....	14
<b>3. PILOOTPROJEKTIDE LÄBIVIIMINE.....</b>	<b>16</b>
3.1 Pilootprojekti arendusetapid .....	16
3.2 Soovitused pilootsüsteemi riist- ja tarkvarahangeteks .....	16
3.2.1 Pilootsüsteemi riistvarahange .....	16
3.2.2 Pilootsüsteemi tarkvarahange .....	17
3.3 ID-kaartide personaliseerimine, väljaandmine ja haldamine .....	17
3.4 Pilootprojekti krüpteerimisvõtmed ja nende haldamine .....	18
3.4.1 Pilootprojekti kasutatavate võtmete klassifikatsioon.....	18
3.4.2 Avaliku võtmega krüptosüsteemile võtmepaaride genereerimine .....	18
3.4.3 Sertifitseerimiskeskuse võtmete haldus .....	18
3.5 Pilootsüsteemi testimine .....	18
<b>4. LISA.....</b>	<b>20</b>
4.1 Mõisted.....	20
4.2 Refereeritavate ning alusstandardite loetelu .....	22
4.3 Relevantsete arendusdokumentide loetelu .....	23
4.3.1 SEIS-dokumendid.....	23
4.3.2 FINEID-dokumendid .....	24
4.3.3 RSA PKCS-seeria standardid .....	24
4.4 Kasutatud kirjandus.....	24

## 1. SISSEJUHATUS

Eesti ID-kaardi programmi edukas läbiviimine eeldab sobivate pilootprojektide käivitamist ja käigushoidmist. Pilootprojektides tuleb tervikuna uurida kogu ID-kaardi elutsüklit, väljaandmisest kuni tema kehtivuse lõppemiseni. Pilootprojektide tulemuste analüüs peab andma aluse Eesti ID-kaardi profiili koostamiseks ning lahendama mitmed probleemid, mis seni on ID-kaardi süsteemide projekteerimisel esile kerkinud.

Antud dokument vaatleb pilootprojektide seda osa, mis tegeleb elektroonilise identifitseerimisega ning ID-kaardil paikneva EID-rakendusega. ID-kaartide teisi võimalikke rakendusi pilootprojektides siinkohal ei vaadelda. Märkida tuleb seda, et need võimalikud rakendused ei tohiks kuidagi häirida EID-rakenduse toimimist kaardil. Vastasel juhul pole vastava pilootprojekti tulemusi ID-kaardi programmi raames võimalik adekvaatselt hinnata.

Antud dokument ei spetsifitseeri ühtegi konkreetset projekti, siin esitatakse vaid üldised soovitusel ja tingimused pilootprojektide spetsifikatsioonide koostamiseks ning pilootsüsteemide ehitamiseks. Projekti lõpp-spetsifikatsioon võib siintoodud soovitustest ka vajadusel irduda ning kasutada teisi meetodeid.

Käesoleva dokumendi koostamisel on lähtutud vastavatest Soome ja Rootsi ID-kaardi projektide dokumentidest ning neile aluseks olevast RSA PKCS-seeria standardist PKCS#15: Cryptographic Token Information Format Standard v1.0 (vt. p. 4.3).

## 2. ID-KAARDI PILOOTSÜSTEEMI LOOMINE

Järgnevalt kirjeldatakse ID-kaardi pilootprojekti käigus loodava pilootsüsteemi ülesehitust ja komponente ning antakse soovitusel pilootprojekti initsialiseerimiseks. Edaspidi kasutatakse lihtsustamise huvides tekstis termini "ID-kaart" asemel vajadusel üldist terminit "kaart", kuna teiste funktsioonidega kaarte ja kandjaid ei käsitleta.

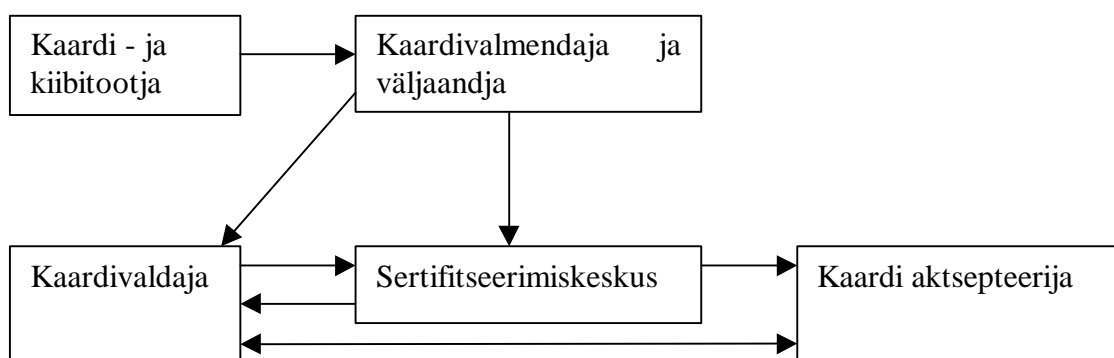
### 2.1 PILOOTSÜSTEEMI KOOSTISOSAD

ID-kaardi pilootsüsteemi loomisel tuleb tähelepanu pöörata järgmistele süsteemi komponentidele:

- 1) Sertifitseerimiskeskus, mis omab konkreetset sertifitseerimispoliitikat
- 2) Kiibitootja
- 3) Kaarditootja ja personaliseerija
- 4) Kaardivalmendaja ja väljaandja
- 5) Kaardivaldajad
- 6) Sertifikaadid, nende väljaandmine ja tühistamine
- 7) Kaardi rakenduskeskkond (kaarti aktsepteerivad terminalid, asutused jne.)
- 8) Lõppkasutaja tarkvara kaardivaldaja arvutis
- 9) Serveritarkvara kaardi aktsepteerija infosüsteemis

Märkus: Kaardivalmendaja võib esineda ka sertifitseerimiskeskuse ülesannetes.

Pilootsüsteemi lihtsustatud ülesehitus on toodud järgmisel joonisel, nooltega on näidatud informatsiooni ja teenuse osutamise suund:



### 2.2 ELEKTRONILINE IDENTIFITSEERIMINE

Elektronilise identifitseerimise puhul kasutatakse avaliku võtmega krüptosüsteemi, kus identifitseeritavale genereeritud võtmepaar (privaatne + avalik võti) tagab nõutud funktsioonide täidetavuse.

Isiku täielikuks elektrooniliseks identifitseerimiseks on vajalikud:

- Isiku nimi
- Unikaalne isikukood
- Isiku avalik võti
- Isiku ainuvalduses olev privaatvõti
- Informatsioon kasutatava(te)st krüptoalgoritmidest

Identifitseeritavale luuakse elektrooniline identiteet, so. tema konkreetset avalikku võtit ja omaniku kohta lisainfot sisaldav sertifikaat. Sertifikaadi kandjaks on antud juhul kaart. Avalikule võtmele vastav privaatvõti on vaid kaardis ning teda pole võimalik sealt väljutada. Sertifikaate annab välja sertifitseerimiskeskus, keda usaldavad nii identifitseerija kui identifitseeritav. Sertifitseerimiskeskus tagab juurdepääsu sertifikaatidele ning korraldab ka nende tühistamist.

Kaardivaldaja identiteeti ehk oma privaatvõtme kuuluvust kontrollib kaardi aktsepteerija kaardivaldaja sertifikaadis sisalduva avaliku võtme ning sertifikaatide tühistusnimekirja abil. Avaliku võtme seotuse vastava sertifikaadiga garanteerib sertifitseerimisautoriteet ehk -keskus, signeerides oma privaatvõtmega kõik väljaantavad sertifikaadid.

## **2.3 SERTIFITSEERIMINE**

### **2.3.1 Sertifitseerimiskeskus**

Sertifitseerimiskeskus (edaspidi SK) tegeleb avaliku võtme rakenduskeskkonnas sertifikaatide väljastamisega ning muuhulgas peab (vt. lähemalt p. 2.3.3):

- Tagama oma sertifitseerimispoliitika väljatöötamise ja rakendamise
- Genereerima pilootsüsteemis kasutatavad krüpteerimisvõtmed ja väljastama sertifikaadid
- Avalikustama oma avaliku(d) võtme(d) ja sertifikaadi(d)
- Haldama ning avalikustama sertifikaatide tühistusnimekirja
- Haldama kaardivaldajate andmebaasi
- Tagama vajadusel ajatempliteenuse
- Tagama sertifitseerimisel organisatsioonilised ja infotehnoloogilised turvameetmed

SK tegevuse alused sätestab üheselt tema sertifitseerimispoliitika (SP) (vt. p. 2.3.3)

### **2.3.2 Sertifikaadid**

SK poolt väljaantavad sertifikaadid peavad pilootprojekti tulemuste adekvaatse hindamise huvides vastama standardile ITU-T X.509v3 (versioon 3), toodud ka standardis ISO/IEC 9594-8 (X.509), vormingule ning sisaldama vähemalt järgmisi andmeid:

- Sertifikaadi number
- Sertifikaadi unikaalne nimi
- Sertifikaadi looja

- Kaardivaldaja nimi
- Kaardivaldaja isikukood
- Kaardivaldaja avalik võti
- Sertifikaadi kehtivusaeg
- Sertifikaadi kasutuskood (võtme iseloomu järgi)
- Sertifikaadi staatus
- Kasutatava räsifunktsiooni ja krüptoalgoritmi nimi
- Sõnumilühend, mis on saadud eelnevalt toodud infole räsifunktsiooni rakendades
- Sõnumilühendi digitaalsignatuur, mis on loodud SK privaatvõtme

Konkreetses pilootprojekti puhul on võimalikud täiendavad formaadi laiendused, näiteks SEIS ja FINEID-sertifikaatide baasil. Kasutatavate sertifikaatide formaati peab toetama rakenduskeskkonna tarkvara (nii SK kui ka sertifikaate aktsepteeriv tarkvara).

Iga privaatvõtme (ehk avaliku võtme krüptosüsteemi võtmepaari) kohta kaardil antakse välja üks eelpoolnimetatud nõuetele vastav sertifikaat.

### **2.3.3 Sertifitseerimispoliitika**

Sertifitseerimispoliitika (SP) on reeglite kogum, millest SK juhindub oma tegevuses. SP koostamisel võib aluseks võtta vastava SEIS dokumendi SEIS10 : Certificate policy (vt. p. 4.3).

SP kooskõlalikus, piisavus ja läbipaistvus on aluseks tema poolt väljaantavate sertifikaatide usaldamisele avaliku võtme rakenduskeskkonnas.

SP sisaldab vähemalt järgnevalt toodud peatükke.

#### **2.3.3.1 Üldised tingimused**

- 1) SK ning sertifitseeritavate definitsioonid ning SK üldandmed
- 2) SK ning sertifitseeritavate õigused ja kohustused ning vastutuse määrad antud SP-st kõrvalekaldumisel
- 3) SK finantsvastutus
- 4) SK teenustasud
- 5) SK tegevuse seaduslikkus
- 6) SK kontaktinfo avalikustamise kord, sagedus ja kanalid
- 7) SK SP-le vastavuse kontrollimise meetodid
- 8) Nõuded SK poolt hoitava informatsiooni konfidentsiaalsusele ning nende nõuete tagatus
- 9) Intellektuaalse omandi kaitse tingimused
- 10) SK poolt sõlmitavate lepingute tingimused

#### **2.3.3.2 Sertifikaadi taotlejate identifitseerimine**

- 1) Taotleja isikuandmete tuvastamine ja kontrollimine
- 2) Taotlejale esitatavad nõuded

### ***2.3.3.3 Sertifikaatide väljaandmine ja tühistamise alused***

- 1) Taotluste esitamise kord
- 2) Sertifikaatide väljaandmine
- 3) Sertifikaatide aktsepteerimine
- 4) Sertifikaatide tühistamine
- 5) Sertifikaatide tühistamise tehnilised üksikasjad ja tingimused
- 6) Sertifikaatide tühistusnimekirjade avalikustamise üksikasjad ja reeglid
- 7) Privaatvõtme avalikustumise käsitlemine
- 8) Nõuded sertifikaatide väljaandmise ja tühistamise protseduuride turvalisusele
- 9) SK andmemassiivide arhiveerimine ja käsitlemine
- 10) SK tegevuse lõpetamise eritingimused (näit. andmebaaside üleandmine)

### ***2.3.3.4 Turvalisusnõuded organisatsioonilistele ja protseduurireeglitele***

- 1) SK tark- ja riistvara füüsiline turvalisus ning kaitsemehhanismid
- 2) SK tark- ja riistvara organisatsiooniline turvalisus ning kaitsemehhanismid
- 3) SK personali valiku- ja usalduskriteeriumid

### ***2.3.3.5 Tehnilised turvalisuse nõuded***

- 1) Avaliku võtme krüptosüsteemi võtmepaaride genereerimine ja salvestamine
- 2) Võtmete ja sertifikaatide edastamine sertifitseeritavatele
- 3) Kasutatavad krüptoalgoritmid ja võtmepikkused
- 4) Privaatvõtmete avalikustumise kaitse
- 5) Nõuded võtmete genereerimise protseduurile SK-s
- 6) SK privaatvõtme kaitse
- 7) Nõuded SK infosüsteemi turvalisusele

### ***2.3.3.6 Sertifikaatide ja nende tühistusnimekirjade profiilid***

- 1) Sertifikaatide ja nende tühistusnimekirjade versioonide tähistus
- 2) Sertifikaadi semantika ja laienduste kasutamine

## **2.4 ID-KAART PILOOTSÜSTEEMIS**

### **2.4.1 Kaardi füüsilised ja tehnilised omadused**

Aluskaart on ID-1 formaadis plastikkaart, mis järgib standardit ISO 7810. Kaardil asuv kiip sisaldab asümmeetrilist krüptosüsteemi toetavat protsessorit ning vähemalt 8kB EEPROM mälu. Kaart peab olema vastav ISO 7816 standardile, omama kaitstud failstruktuuri ja kataloogide juurdepääsu. Kui rakendused pilootsüsteemis seda nõuavad, siis peab kaart sisaldama ka kontaktivaba kaardi liideseid, st. kaart peab kuuluma hübriidkaartide klassi.

## 2.4.2 Kaardivaldaja identifitseerimine pilootsüsteemis

Kaardivaldaja identifitseerimiseks on mitmed võimalused. Siinkohal jätame vaatluse alt kõrvale biomeetrilised meetodid ning käsitleme kaardivaldaja teadmusel (nt. salakood) põhinevat identifitseerimist.

Kaardivaldajat identifitseeritakse PIN-koodi abil. Identifitseerija võrdleb kaardivaldaja poolt antud PIN-koodi kaardil paiknevaga. Kui kaardil on teisi rakendusi peale EID, siis neile juurdepääs on lubatud läbi vastavate PIN-koodide. Ka EID rakenduse erinevate alamteenuste (autentimine, digitaalsignatuur, võtme krüpteerimine) aktiveerimine on kaitstud omaette PIN-koodidega.

PIN-koodile esitatavad nõudmised:

- Koodi pikkus on vähemalt 6 märki
- Kood sisaldab vähemalt kaht erinevat märki
- Pärast kolme ebaõnnestunud PIN-koodi sisestust lukustuvad kõik selle PIN-koodiga seotud kaardi funktsioonid
- Lukustunud PIN-koodi saab avada kas kaardi väljaandja või kaardivaldaja ise eelnevalt kokkulepitud meetodil (nt. täiendav salakood)
- Kaardil asuva PIN-koodi tuvastamine väljaspool kaarti on infotehnoloogiliselt võimatu (vastavad failid on lugemiseks kaitstud)
- Suvalise kaardis asuva privaativõtme kasutamine nõuab vastava PIN-koodi kasutamist

Konkreetse pilootprojekti kohaselt fikseeritakse:

- PIN-koodi maksimumpikkus
- PIN-koodis sisalduvate numbrite vähim hulk
- PIN-koodi muutmise võimalused
- PIN-koodi(de) valiku tingimused (kas seab väljaandja või kaardivaldaja)

## 2.4.3 EID-rakendus kaardil

EID-rakendus annab järgmised võimalused:

- Kaardilt sertifikaadi lugemine
- Kaardis oleva privaativõtmega kaardile väljastpoolt vastava avaliku võtmega krüpteeritud info või kaardis genereeritud salajase võtme krüpteerimine
- Kaardilt muu EID-rakendusekohase info lugemine

Selleks peab kaart oskama, kasutades sisestatud PIN-koodi, valida:

- vastavat kaardile salvestatud privaativõtit
- PIN-koodile vastavat sertifikaati

## 2.4.4 ID-kaardis paikneva info turvalisuse tagatised

Kaardil paikneva kiibi ehitus peab vastama rahvusvahelistele standardidele.

Kaardi operatsioonisüsteem peab olema võimeline tagama:

- piiratud juurdepääsu- ja lugemisõigused kaardis asuvatele failidele ja kataloogidele
- kaardis paiknevate privaatvõtmete kasutamise ainult kaardi sees ning selleks lubatud juhtudel
- sertifikaatide ülekirjutuskaitse ning EID-rakendusega seotud informatsiooni piiratud lugemisõigused

## 2.5 ID-KAARDI ELUIGA PILOOTSÜSTEEMIS

ID-kaardi eluiga koosneb järgmistest etappidest:

- 1) Kiibi valmistamine
- 2) Aluskaardi valmistamine
- 3) Kiibi paigaldamine aluskaardile
- 4) Kaardi valmendamise ehk kiipi operatsioonisüsteemi (maski) programmeerimine
- 5) Kaardi personaliseerimine (kaardile visuaalse info ja kaarti infofailide ehk antud juhul sertifikaatide sisestamine)
- 6) Kaardi väljastamine kaardi tulevasele valdajale
- 7) Kaardiga opereerimine
- 8) Kaardi kehtivusaja lõppemine või kaardi kadumine või kaardi varastamine
- 9) Kaardi tühistamine ja/või kaardi hävitamine
- 10) Kaardi korduvkasutus ja/või kaardi hävitamine

Esimesed 4 etappi toimuvad reeglina pilootsüsteemi raamidest väljaspool ning nende puhul tuleb usaldada kaardivalmistajat. Kaardivalmistaja tööprotsesside vastavust rahvusvahelistele standardidele on otstarbekas täiendavalt hinnata või aktsepteerida vastavaid auditeid.

Kaartide personaliseerimine ja tulevaste valdajateni toimetamine toimub pilootsüsteemi sees ning see peab vastama eelnevalt kehtestatud protseduurireeglitele. Kaartide personaliseerija peab tagama organisatsioonilised ja infotehnoloogilised turvameetmed, et kogu protsessi puudutav teave jõuaks vaid selleks volitatud isikuteni, välistatud oleks salajase informatsiooni leke ning protsessi ainuisikuline suunamine. Kaardid peavad jõudma nende tulevaste valdajateni süsteemis aktsepteeritud meetodil, kus võimalused kaartide kadumiseks või nende sattumine valede isikute kätte on minimiseeritud. Kaartidega seotud PIN-koodid peavad jõudma kaardi valdajateni sõltumatult ja eraldatult kaardist.

Kaartide kadumise või varastamise korral peab kaardi valdajatele olema tagatud nende kohese sulgemise võimalus. Sulgemine võib olla kas tingimuslik või lõplik, sõltuvalt kehtestatud kaartidesulgemise tingimustest. Soovitav on kasutada tingimuslikku sulgemist, kus kaart suletakse esialgu ajutiselt ning hiljem lõplikult, kui tühistamine oli laekunud põhjendatult ning selleks volitatud isikult.

Kasutusest kõrvaldatud kaartide hävitamise kord sätestatakse kaartide väljaandja poolt täiendavalt, sõltuvalt pilootsüsteemis kehtestatud üldistest nõuetest ja kaardivaldaja vastutuse määrast.

## 2.6 ID-KAARDI POOLT PAKUTAVAD TEENUSED

### 2.6.1 Identifitseerimine ID-kaardiga

Kaardivaldaja verifitseerimine toimub kahes etapis:

- Kaart verifitseerib kaardivaldaja PIN-koodi
- Pilootsüsteem verifitseerib kaarti

Kaardi verifitseerimine pilootsüsteemis võib erineda sõltuvalt kaardi kasutusvaldkonnast. Teatud teenuste puhul tuleb nõuda kaardi sidusresiimis verifitseerimist, teatud teenuste puhul pole see tingimata vajalik ning kaardid verifitseeritakse vallasresiimis.

Vallasresiimis verifitseerimine võib toimuda näiteks läbipääsukontrolli puhul. Kaartide (so. tegelikult sertifikaatide) tühistusnimekirja uuendatakse sel juhul verifitseerija juures kindla ajaperioodi möödudes. Ajaperiood valitakse lähtuvalt konkreetse verifitseerija (antud juhul läbipääsukontroller) riskiastmest ja positsioonist pilootsüsteemis. Mida olulisem süsteemiosa, seda lühem peab see ajaperiood olema.

Sidusresiimis verifitseerimine peab toimuma tingimata järgmiste teenuste puhul:

- a) arvutivõrgule juurdepääs
- b) digitaalsignatuuri andmine
- c) krüpteeritud sideseansside initsialiseerimine

Kaartide (so. tegelikult sertifikaatide) tühistusnimekirjad peavad sel juhul verifitseerijale suvalisel ajahetkel kättesaadavad olema.

Täiendavate teenuste puhul peab tühistusnimekirjade verifitseerijale kättesaadavuse määra hindama vastavalt pilootsüsteemi spetsifikatsioonidele.

Verifitseerimismeetod(id) ja nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

### 2.6.2 Digitaalsignatuur

Digitaalsignatuur elektrondokumentidele luuakse kaardis, kasutades selleks vastavat privaativõtet ning räsifunktsiooni.

Kaardivaldajate volitused signeerimiseks ja signeeritavate elektrondokumentide skoop määratakse pilootsüsteemis täiendavalt vastavate reeglitega. Signeeritud elektrondokumendi käsitlemisest pilootsüsteemis vt. p. 2.7

Digitaalsignatuuri loomiseks kasutatavad meetodid ja nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

### 2.6.3 Elektrondokumendi päritolu, autentsus ja terviklus

Elektrondokumendi päritolu, autentsuse ja tervikluse kontrollimiseks seatakse järgmised nõuded:

- Kasutatavad meetodid ja algoritmid ja nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.
- Kasutatavad räsifunktsioonid ja nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

### 2.6.4 Elektrondokumentide ajaliste tingimuste ja salgamise vääramise verifitseerimine

Signeeritud elektrondokumendi ajatempel koos vastaval ajahetkel kehtinud sertifikaatide tühistusnimekirjadega tõendab, et elektrondokumendi signatuur oli antud ajahetkel kehtiv.

Elektrondokumendi signatuur ja ajatempel koos vastaval ajahetkel kehtinud tühistusnimekirjaga peavad EID-rakenduskeskkonnas tõendama, et:

- Dokument on välja saadetud tema väidetava looja poolt
- Dokument on välja saadetud tema väidetava looja poolt antud ajal
- Dokument on vastu võetud
- Dokument on vastu võetud antud ajal
- Kasutatavad meetodid ja algoritmid ning nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

Elektrondokumentide puhul peab olema tagatud nende arhiveeritavus koos nende loomisel kehtinud sertifikaatide tühistusnimekirja(de)ga. Vt. ka p. 2.7

### 2.6.5 Andmete krüpteerimine

Andmete krüpteerimine toimub protseduuri käigus genereeritava sümmeetrilise võtme abil. Võtmevahetus osapoolte vahel toimub vastava, kaardis oleva, privaatvõtme abil.

- Kasutatavad meetodid ja algoritmid ning nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

### 2.6.6 Sideseansside krüpteerimine

Sideseansside krüpteerimiseks tarvitatakse seansi käigus genereeritavat salajast sümmeetrilist võtit. Võtmevahetuseks osapoolte vahel kasutatakse vastavat kaardil paiknevat privaatvõtit.

- Kasutatavad meetodid ja algoritmid ning nende kasutamise detailid peavad olema avalikud ja üldtunnustatud. Vt. ka p 2.9.

## 2.7 ELEKTRONDOKUMENDI KÄSITLUS PILOOTSÜSTEEMIS

Elektrondokumentide signeerimine pilootsüsteemis sätestatakse iga konkreetse projekti puhul eraldi.

Vastav üldine kord peab määrama järgnevad üksikasjad:

- 1) pilootsüsteemis signeerimise kord ja meetod
- 2) signeeritavate dokumentide loetelu ja/või skoop
- 3) signeerija vastutuse määr ja kestvus
- 4) ajatempliteenuse kasutamise kord ja meetod
- 5) ajatempliteenuse kasutamise korral sertifikaatide tühistusnimekirjade arhiveerimise kord ja kasutamise meetodid
- 6) ajatempliteenuse mittekasutamise korral elektrondokumendi tõestatavus ja selle ajalised piirangud
- 7) elektrondokumentide arhiveeritavus
- 8) elektrondokumentide verifitseerimise kord ja meetod
- 9) vastutus elektrondokumendi verifitseerimisel
- 10) elektrondokumendi signatuuri vaidlustatavus
- 11) võimalikud eritingimused signeerimisel

## 2.8 TARKVARALIIDISED

Pilootsüsteemis kasutatav lõppkasutaja tarkvara peab tagama järgneva funktsionaalsuse ning kasutusvõimalused:

- Kasutada tugevat sümmeetrilist krüptoalgoritmi (vt. 2.9)
- Genereerida nimetatud algoritmi abil krüpteerimisvõtmeid
- Kasutada sama avaliku võtmega krüptosüsteemi, mida kasutatakse ID-kaardil
- Suhtlust läbi kaardilugeja ID-kaardiga
- Kasutada räsifunktsiooni (vt. 2.9)
- Suhelda üle arvutivõrgu teenusepakkuja serveriga
- Säilitama avalikke võtmeid sisaldavaid teenusepakkuja sertifikaate
- Võimaldama teenusepakkuja-poolset kliendi (lõppkasutaja) autentimist

Tarkvara peab toetama PC/SC spetsifikatsiooni ja/või PKCS#11 standardit, samuti SSL, S/MIME ja HTTP/HTTPS protokolle.

Toodud nõuetele vastavad ja näiteks sobivad standardtarkvaraks veebilehitsejad MS IE (toetab PC/SC) ja Netscape Communicator (toetab Cryptoki ehk PKCS#11).

## 2.9 PAKUTAVATE TEENUSTE TURVANÕUDED

### 2.9.1 Teenuste turvasemed

ID-kaardi EID-rakendus pakub eelkõige 3 teenust:

1. Autentimine
2. Digitaalsignatuur

### 3. Krüpteeritud võtmevahetus

Igäihe jaoks neist võiks kaardis olla üks avaliku võtme sertifikaat (vastav standardile X.509v3) ning sellele vastav privaatvõti. Lisaks sellele peab kaart oskama arvutada räsifunktsioone ning signatuure anda.

Arvestades erinevatele teenustele esitatavaid nõudmisi turvalisuse suhtes tuleb võtmepikkuse ning algoritmi valikul neist nõudmistest lähtuda.

Kõige enam turvalisust nõudev on digitaalsignatuur, kuna signeeritav dokument peab olema verifitseeritav ka aastate pärast. Seega vajab ta pikemaajalist turvalisusgarantiid. Digitaalsignatuuriks kasutatava võtmepaari võtmed on soovitatav valida maksimaalse pikkusega, mida pilootprojekti eelarve (kaardi mälu ja maksumust silmas pidades) ja tarkvara ekspordipiirangud (vt. ka p. 2.9.3) võimaldavad.

Lühemaajalist turvalisust nõuavad autentimine ja sümmeetriliste võtmete krüpteerimine privaatvõtmetega, kuna need ei vaja hilisemat tõestamist. Võimalik on need kaks funktsiooni ühendada ühte sertifikaati ning kasutada mõlema tarvis üht avaliku võtme krüptosüsteemi võtmepaari. Võtmepikkus pole enam niivõrd oluline ning mälu kokkuhoiu huvides võib piirduda lühemate võtmetega.

#### 2.9.2 Nõuded kasutatavatele krüptoloogilistele meetoditele

Nõuded tulenevad eelkõige pilootsüsteemi mastaabist ja rakenduskeskkonnast. Väikesemastaabilise ja sisevõrgus läbiviidava pilootprojekti puhul pole tugevate krüptoalgoritmide ja pikkade võtmete kasutamiseks põhjust. Kui pilootsüsteemil on aga ühisosa avaliku võrguga (i.e. Internet), siis peavad turvanõuded olema oluliselt kõrgemad. Tähelepanu tuleb pöörata läbi avaliku võrgu toimuvale infovahetuse turvalisusele, pilootsüsteemis kasutatava tarkvara võimalikele puudujääkidele, samuti pilootsüsteemi sisevõrgu kaitsele väliste rünnakute eest.

Kasutatavad meetodid peavad olema avalikud, informatsioon nende tööpõhimõtete ja rakenduste kohta kõigile kättesaadav. Soovitatav on kasutada algoritme, mille vastu pole seni teada edukaid ründeid, ka teoreetiliselt mitte. Algoritmide valikul tuleb silmas pidada ka pilootsüsteemis kasutatava tarkvara (SK ja lõppkasutaja arvutid) ühilduvust.

#### 2.9.3 Soovitusi krüptoalgoritmide ja võtmepikkuse valikuks

Krüptoalgoritmide ja nende tugevuse valikul tuleb arvestada krüptotoodete ekspordipiirangutega. Kui me soovime kasutada pilootsüsteemis näiteks firmade Netscape või Microsoft tarkvara (näiteks nende veebilehitsejad), siis maksimaalne võtmepikkus RSA-algoritmi puhul on 512 bitti ning DES algoritmi puhul 40 bitti. Seega tuleb meil kaardil paiknevates sertifikaatides RSA võtme pikkuse valikul ning salajaste võtmete genereerimisel arvestada neid piiranguid. Erijuhul on võimalik ekspordida eelnimetatud tarkvara ka pikema lubatud võtmepikkusega versioonidena.

Räsifunktsioonidest võib sobivatena välja pakkuda RIPEMD 128/160, SHA-1 ja MD5.



Avaliku võtmega krüptosüsteemide korral võib välja pakkuda RSA-d, DSA-d või elliptilisi kõveratel baseeruvaid krüptosüsteeme.

Näiteks, RSA kasutamise korral peaks võtmepikkuseks olema vähemalt 512 bitti.

Kasutatav kaart peaks oskama arvutada ja kasutada kas 3DESi või IDEA-d. Võtmepikkus tuleks valida sõltuvalt nõutud turvatasemest ning tarkvara päritolust. Ühekordne DES on ebapiisava turvalisusega.

### 3. PILOOTPROJEKTIDE LÄBIVIIMINE

#### 3.1 PILOOTPROJEKTI ARENDUSETAPID

Järgnevalt esitatakse näitena ühe pilootprojekti läbiviimise plaan ajalisel järgnevuses. Konkreetne projekt võib tuua siinesitatule täiendusi või muudatusi, samuti võivad toodud alamtegevused ajaliselt üksteise suhtes ümber paikneda.

- 1) pilootsüsteemi ülesannete, eesmärkide ja teenuste spetsifitseerimine
- 2) pilootkaardi väline disain ning sellele kantava informatsiooni määratlemine
- 3) pilootkaardi sisu määratlemine ning rakenduste defineerimine
- 4) kaardivaldajate jt. andmebaaside projekteerimine
- 5) pilootsüsteemi riistvaralise topoloogia spetsifitseerimine
- 6) pilootsüsteemis krüpteerimisvõtmete genereerimise korra kinnitamine
- 7) pilootsüsteemi riist- ja tarkvaraliste nõuete spetsifitseerimine
- 8) kaartide personaliseerimise ja väljastamise protseduuride spetsifitseerimine
- 9) pilootsüsteemis esinevate riskide hindamine
- 10) sertifitseerimisteenuse ja sertifikaatide tühistusnimekirjade haldamise protseduuride spetsifitseerimine
- 11) pilootsüsteemile riist- ja tarkvarahankekonkursi korraldamine
- 12) kaartide kasutamise ja tühistamise korra kinnitamine
- 13) personali väljaõpe
- 14) pilootsüsteemi testimise spetsifitseerimine
- 15) pilootsüsteemi riist- ja tarkvara installeerimine
- 16) sertifitseerimisteenuse testimine
- 17) pilootsüsteemi testimine
- 18) pilootsüsteemi testimise hindamine
- 19) kaartide väljastamise algus
- 20) pilootsüsteemi töö jälgimine ja hindamine
- 21) pilootsüsteemi töö korrigeerimine
- 22) pilootsüsteemi laiendamine

#### 3.2 SOOVITUSED PILOOTSÜSTEEMI RIIST- JA TARKVARAHANGETEKS

##### 3.2.1 Pilootsüsteemi riistvarahange

Pilootsüsteemi riistvarahange koosneb järgmistest osadest:

- 1) SK riistvara
- 2) kaartide personaliseerimisseadmed
- 3) pilootkaardid
- 4) kaardilugejad
- 5) lõppkasutaja riistvara

Kõiki ülaltoodud riistvara liike võib hankida sõltumatult, kuid kasulik on esimesed kaks koos tarnida (vt. ka tarkvarahangeid p. 3.2.2). Kaardid ja kaardilugejad on soovitatav tarnida sõltuvalt tootjate pakkumiste ulatusest ja tingimustest ja kaartidele esitatavatest nõudmistest. Riistvarahange ajakava sõltub pilootprojekti üldisest ajakavast.

### 3.2.2 Pilootsüsteemi tarkvarahange

Pilootsüsteemi tarkvarahange koosneb järgmistest osadest:

- 1) SK tarkvara
- 2) kaartide personaliseerimisprotsessi tarkvara
- 3) rakenduste tarkvara
- 4) lõppkasutaja tarkvara

Kõiki ülaltoodud tarkvara liike võib hankida sõltumatult, kuid kasulik on esimesed kaks koos tarnida. Üldjuhul pakutakse neid ka koos sobiva riistvaraga. Rakendustarkvara peab järgima SK tarkvara omapära ning eritingimusi. Lõppkasutaja tarkvara valik sõltub vastavast riistvarast ning pilootsüsteemi rakenduste spetsifikatsioonidest.

Tarkvarahangete ajakava sõltub pilootprojekti üldisest ajakavast.

### 3.3 ID-KAARTIDE PERSONALISEERIMINE, VÄLJAANDMINE JA HALDAMINE

Kaardid peavad olema valmistatud vastavalt neile esitatud tehnilistele spetsifikatsioonidele ning omadused vastama rahvusvahelistele ISO-standardidele 7810, 7812, 7616:1-6

Kaardid peavad olema personaliseeritud turvalises ning kontrollitud keskkonnas, kaardile salvestatud võtmete salastatus garanteeritud.

Kaardis peavad sisalduma kaardinumber, salajased võtmed ja sertifikaadid ning EID rakendus.

Kaardi väljaandmisel peab kaardi väljaandja:

- Veenduma kaardivaldaja isikusamasuses nii taotluse esitamisel kui kaardi kättesaamisel
- Tagama, et kaardivaldaja on aru saanud ja aktsepteerinud kaardi kasutamise tingimusi
- Tagama kaardivaldaja isikuinformatsiooni säilimise tervikliku ja muutumatuna

Kaardi väljaandja peab kaartide andmebaasis säilitama vähemalt järgmist kaardikohast infot:

- järjekorranumber
- väljaandmise aeg
- kaardivaldaja nimi ja isikukood
- kaardil paiknev visuaalne info
- kaardi kehtivusaeg
- kaardi tühistusinfo

Vaata ka p. 2.3.3.

### **3.4 PILOOTPROJEKTI KRÜPTEERIMISVÕTMED JA NENDE HALDAMINE**

#### **3.4.1 Pilootprojektis kasutatavate võtmete klassifikatsioon**

Pilootsüsteemis erinevate osapoolte kasutatavad võtmed erinevad üksteisest oma kasutusala ja omaniku staatuse poolest.

Võtmed võib klassifitseerida järgmiselt (ühe SK korral):

- Sertifitseerija võtmed
- Pilootsüsteemi administraatori võtmed
- Kaardivaldaja võtmed

Iga grupi võtmed jagunevad veel omakorda alamgruppideks, sõltuvalt võtmete kasutusest. Võtmete genereerimise alused ja tingimused sätestab vastav, pilootsüsteemis kehtestatud, kord.

Vaata ka p. 2.3.3.

#### **3.4.2 Avaliku võtmega krüptosüsteemile võtmepaaride genereerimine**

Võtmepaaride genereerimine peab toimuma välismaailmale suletud süsteemis ja turvanõuetele vastavalt. Kasutatav riistvara ning tarkvara peab olema dokumenteeritud ning nende turvalisus tõestatav sertifitseerijale. Kõik väljaviigud süsteemist peavad olema kirjeldatud ja jälgitavad. Protsessi käigus genereeritud salajased võtmed kustutatakse (vahemälust) pärast nende salvestamist lõppkandjale, nende salvestumine mittekontrollitavale infokandjale peab olema välistatud. Võtmete genereerimise protseduur peab tagama genereeritavate võtmete unikaalsuse.

Võtmete genereerimise peab läbi viima selleks volitatud ja valdkonnas pädev personal, järgides protsessi läbiviimiseks kehtestatud normatiive.

Vaata ka p. 2.3.3.

#### **3.4.3 Sertifitseerimiskeskuse võtmete haldus**

SK salajased võtmed peavad olema salvestatud turvalisel moel kandjale, mis pole kiipkaart, kuid vastab SP ettekirjutustele. Selleks sobib näiteks turvamoodul. Nende võtmete hoidmiseks võib kasutada ka täiendavaid krüpteerimisvõtmeid.

Vaata ka p. 2.3.3.

### **3.5 PILOOTSÜSTEEMI TESTIMINE**

Pilootsüsteemi käivitamise eelduseks on selle töö eelnev plaanipärane testimine. Testitakse iga süsteemi funktsiooni eraldi ning seejärel komponentide koostööd. Testimiseks koostatakse testplaani, fikseeritakse testimise eesmärgid ning tulemuste fikseerimise ja hindamise kriteeriumid. Testimine viiakse läbi pilootsüsteemivälise vaatlajate juuresolekul ning riist- ja tarkvaratarnijate nõustamisel. Testimise käigus



ilmnenud pilootsüsteemi puudujäägid likvideeritakse sõltuvalt konkreetse vea mõjust ülejäänud süsteemi tööle kas enne pilootsüsteemi käivitamist või selle käigusolemise ajal.

Kasutatakse järgmisi testiliike:

- 1) funktsionaalsustestid
- 2) koormustestid
- 3) riistavaralised testid
- 4) tarkvaralised testid
- 5) protseduuritestid

## 4. LISA

### 4.1 MÕISTED

Aruande 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
Digitaalsignatuur	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-1
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 number	Unikaalne objekti tunnuscode
Identifitseerimine	Identification	Objekti või isiku 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 püsitarkvara, 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
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 järgneva 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

## 4.2 REFEREERITAVATE NING ALUSSTANDARDITE LOETELU

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

### **4.3 RELEVANTSETE ARENDUSDOKUMENTIDE LOETELU**

#### **4.3.1 SEIS-dokumendid**

Riiklikud standardid (avaldatud 18.09.1998):

SS 614330            Electronic ID Application

SS 614331            Electronic ID Certificate



SS 614332      Electronic ID Card - Swedish Profile

Täiendav dokument:

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.ee>

#### **4.3.2 FINEID-dokumendid**

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.vaestorekisterikeskus.fi/hst.htm>

#### **4.3.3 RSA PKCS-seeria standardid**

PKCS-11: Cryptographic Token Interface Standard

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

RSA PKCS standardid on saadaval Internetis aadressil

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

#### **4.4 KASUTATUD KIRJANDUS**

IBM Redbook - Smart Cards: A Case Study, 1998 (kättesaadav Internetis  
<http://www.redbooks.ibm.com/abstracts/sg245239.html>)

M. Hendry - Smart Card - Security and Applications, Artech House, 1997