EstEID

(Eesti riikliku avaliku võtme infrastruktuur digitaalallkirja seaduse alusel)

Turvakiibi rakendus ja liides

V 2.01

Koostas: ID Süsteemide AS

Sisukord

1 Saateks 4
2 Seonduvad standardid 4
3 Kasutatud lühendid 5
4 EstEID turvakiibi rakenduse objektid ja operatsioonid 5
4.1 EstEID turvakiibi objektid 5
4.1.1 PIN1, PIN2 ja PUK 6
4.1.2 3DESKey1 ja 3DESKey2 7
4.1.3 Kaardihaldusvõtmed CMK1, CMK2a, CMK2b ja CMK3 7
4.1.3.1 Kaardihaldusvõtmete genereerimine ja salvestamine 7
4.1.3.2 Autentimisobjektide asendamise võti – CMK1 7
4.1.3.3 Uute võtmepaaride genereerimise autentimise võti – CMK2a 7
4.1.3.4 Sertifikaatide ülelaadimise käsujadade moodustamise võti – CMK2b 7
4.1.3.5 Lisarakenduse laadimise turvalise käsujada moodustamise võti – CMK3 7
4.1.3.6 Kaardikohaste CMK'de moodustamise protseduur 7
4.1.3.7 Kaardihalduskoodi tuletamise protseduur 8
4.1.4 Sertifikaadid 8
4.1.5 Kaardi kasutaja salajased võtmed 8
4.1.6 Kaardi kasutaja isikuandmete fail 8
4.2 EstEID turvakiibi operatsioonid 9
4.2.1 Sertifikaatide ja andmete lugemine 10
4.2.1.1 Sertifikaatide lugemine 10
4.2.1.2 Kasutaja isikuandmete faili lugemine 10
4.2.2 Autentimisobjektide haldamine 10
4.2.2.1 PIN1, PIN2 ja PUK väärtuste muutmine 10
4.2.2.2 PIN1 ja PIN2 järjestikuste valesisestuste loenduri nullimine 10
4.2.2.3 3DESKey'le väärtuste omistamine 10
4.2.3 Kaardi kasutaja autentimine 10
4.2.3.1 Kaardi kasutaja autentimine PIN1, PIN2 ja PUK abil 10
4.2.3.2 Kaardi kasutaja autentimine 3DESKey1 ja 3DESKey2 abil 10
4.2.4 Operatsioonid salajaste võtmetega 10
4.2.5 Kaardihaldusoperatsioonid 11
4.2.5.1 PIN-koodide asendamine 11
4.2.5.2 Uute võtmepaaride genereerimine 11
4.2.5.3 Sertifikaatide ülelaadimine 11
4.2.5.4 Lisarakenduste laadimine ja kustutamine 11
4.2.5.5 Turvatud käsujadade moodustamine 12
4.3 EstEID failisüsteem 12

4.4 Objektid EstEID kaardil väljaandmise hetkel 14
5 EstEID abiprotseduurid....14
5.1 EstEID turvaline kommunikatsioon 14
5.2 3DESKey tuletamine paroollausest 14
6 EstEID kaardi turvastruktuur 14
6.1 Turvakeskkondade ja operatsioonide risttabel 14
6.2 Kommentaarid turvakeskkondade kohta 16
6.2.1 PKI keskkond (SE#01) 16
6.2.2 PKI keskkond turvatud kommunikatsiooniga (SE#02) 16
6.2.3 Sertifikaatide ülelaadimise keskkond (SE#03) 16
6.2.4 Autentimisobjektide asendamise keskkond (SE#04) 16
6.2.5 Lisarakenduste laadimise keskkond (SE#05) 16
6.2.6 Dekrüptimisoperatsioonide keskkonnad (SE#6, SE#7) 16
7 Juhiseid kaarti kasutavate rakenduste kirjutajaile 16
7.1 EstEID kiibi käsustik 16
7.2 EstEID kiibi ATR ajaloolised baidid 16
7.3 EstEID kiibi erinevused standardsest MICARDO 2.1 17
7.3.1 ATR modifikatsioon 17
7.3.2 EEPROM initsialiseerimine ja kaardi formateerimine 17
7.4 Üldiseid juhiseid 17
7.4.1 Seadmete avamine eksklusiivses režiimis. 17
7.4.2 Muutuva pikkusega PIN-koodid 17
7.4.3 Transaktsiooniaja minimiseerimine 17
7.4.4 Rakenduste koodide signeerimine 17

1 Saateks

Käesolev dokument spetsifitseerib Eesti riikliku avaliku võtme infrastruktuuri (EstEID) turvakiibi versioon 2.01 liidese ja andmesisu.

2 Seonduvad standardid

ISO 7816-1: Identification cards - Integrated circuit(s) cards with contacts. Part 1: Physical Characteristics

ISO 7816-2: Identification cards - Integrated circuit(s) cards with contacts. Part 1: Physical Characteristics

ISO 7816-3: Identification cards – Integrated circuit(s) cards with contacts. Part 3: Electronic signals and transmission protocols.

ISO 7816-4: Identification cards – Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange

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

ISO 9594-8: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework

PKCS#1 v1.5, RSA Cryptography Standard, November 1, 1993

PKCS#1 v2.0, RSA Cryptography Standard, October 1, 1998

PKCS#5 v2.0, Password-Based Cryptography Standard, March 25, 1999

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

Micardo 2.1 Chip Card Operating System User Manual

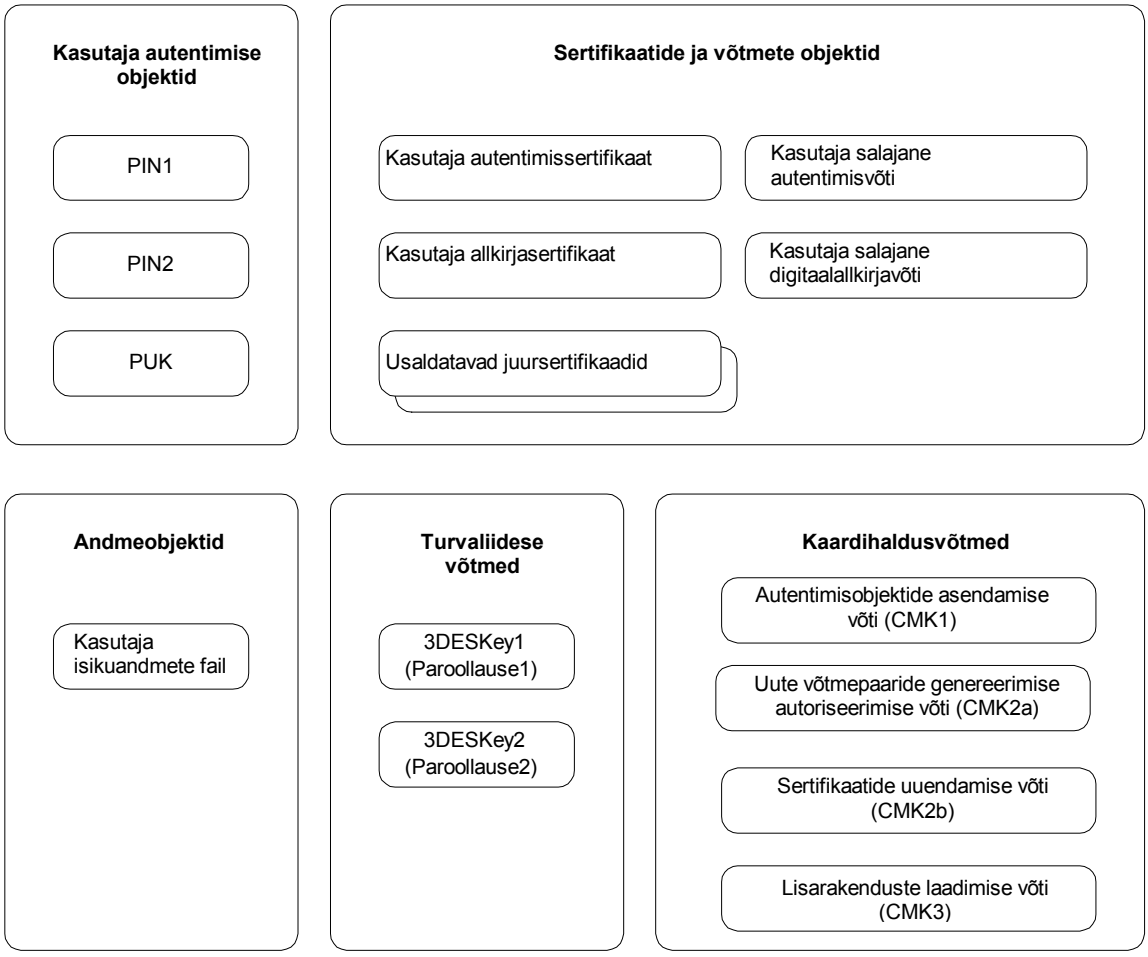
3 Kasutatud lühendid

APDU	Kiibi rakendusprotokolli ühik
LSB	Noorim bitt
MF	Juurkataloog turvakiibi failisüsteemis
Kaardihalduskeskus	Institutsioon, kes teostab EstEID kaartide haldamise operatsioone kiibi haldaja volitusel
Kaardi haldaja	Institutsioon, kes vastutab EstEID kaardihalduse protseduuride läbiviimise eest

4 EstEID turvakiibi rakenduse objektid ja operatsioonid

4.1 EstEID turvakiibi objektid

EstEID olevad objektid on kujutatud järgneval joonisel:



Objekt	Funktsioon kaardil
PIN1	Kaardi kasutaja autoriseerimine: 1. autentimisvõtme kasutamiseks 2. järgmiste operatsioonide läbiviimiseks: a. uute võtmepaaride genereerimine b. sertifikaatide ülelaadimine c. lisarakenduste laadimine (kustutamine)
PIN2	Kaardi kasutaja autoriseerimine: 1. allkirjastamisvõtme kasutamiseks 2. paroollausete asetamiseks
PUK	PIN-koodide lahtiblokeerimine pärast nende blokeerumist lubatava järjestikuste valesisestuskordade ületamisel.
3DESKey1	3DES võti turvaliseks andmevahetuseks operatsioonidel autentimisvõtmega.
3DESKey2	3DES võti turvaliseks andmevahetuseks operatsioonidel allkirjastamisvõtmega.
Kasutaja autentimissertifikaat ja salajane autentimisvõti	Kaardi kasutaja elektroonne tuvastamine
Kasutaja signeerimissertifikaat ja salajane signeerimisvõti	Kaardi kasutaja elektronallkirja arvutamine ja kontroll.
Usaldatavad juursertifikaadid	EstEID juursertifikaatide turvaline edastamine.
Kasutaja isikuandmete fail	Sisaldab kaardi kasutaja isikuandmeid.
CMK1	3DES-võti, mille abil turvatakse PIN-koodide asendamise protseduur
CMK2a	3DES-võti, mille abil autoriseeritakse uute võtmepaaride genereerimine.
CMK2b	3DES-võti, mille abil moodustatakse turvatud käsujadad kasutajasertifikaatide ülelaadimiseks.
CMK3	3DES-võti, mille abil moodustatakse turvatud käsujadad lisarakenduste kaardile laadimiseks.

4.1.1 PIN1, PIN2 ja PUK

PIN1, PIN2 ja PUK koosnevad numbritest ‘0’..’9’.

Järgnevas tabelis on toodud PIN ja PUK koodide lubatavad pikkused:

	Minimaalne pikkus (numbrit)	Maksimaalne pikkus (numbrit)
PIN1	4	12
PIN2	5	12
PUK	8	12

EstEID kaardile ei ole võimalik seada PIN- ega PUK-koode, mille pikkus ei mahu tabelis toodud piiridesse. PIN- ja PUK-koodid on muutuva pikkusega, kaardiga suhtlevad rakendused peavad toetama muutuva pikkusega PIN-koode.

PIN-koodid edastatakse kaardile ASCII-vormingus.

PIN- ega PUK-koodid ei ole kaardilt väljaloetavad. PIN- ja PUK-koodidega on seotud järjestikuste valesisestuste loendurid. PIN1 blokeerub pärast 3 järjestikust valesisestust. PIN2 blokeerub samuti pärast 3 järjestikust valesisestust.

Kummagi PIN-koodi võib lahti blokeerida PIN-koodide asendamise protseduuri abil.

PUK-kood blokeerub samuti pärast 3 järjestikust valesisestust. Blokeerunud PUK-koodiga kaardi võib muuta taas kasutatavaks PIN-koodide asendamise protseduuri abil.

4.1.2 3DESKey1 ja 3DESKey2

Nende 3DES-võtmete abil toimub turvaline andmevahetus kaardi ja host-rakenduse vahel. Kaardi personaliseerimisel seatakse võtmete väärtuseks 00..00 – see võti ei ole kasutatav. Nende võtmetega operatsioonide sooritamiseks peab kaardi kasutaja need esmalt 3DESKkey asetamise protseduuri abil kaardile seadma. Neid võtmeid ei ole võimalik kaardilt välja lugeda, küll aga eelpoolmainitud protseduuri abil asendada.

Nende võtmetega on seotud valesisestuste loendurid algväärtusega 0xFF. Loenduri väärtus väheneb ühe võrra pärast iga ebaõnnestunud operatsiooni. Loenduri väärtus ei taastu - kui loendur on jõudnud nulli, ei ole võti enam kasutatav.

3DESKey1 ja 3DESKey2 tuletatakse Paroollause1 ja Parollause2'st vastavalt 3DESKey paroollausest tuletamise protseduurile.

4.1.3 Kaardihaldusvõtmed CMK1, CMK2a, CMK2b ja CMK3

4.1.3.1 Kaardihaldusvõtmete genereerimine ja salvestamine

Need neli salajast 3DES-võtit genereerib kaartide personaliseerija turvalises keskkonnas. Neid võtmeid kasutatakse kaardikohaste CMK'de arvutamiseks, mis laetakse personaliseerimise käigus kaardile. Neid võtmeid ei saa kaardilt välja lugeda ega muuta.

Kaardihalduskeskus kasutab neid võtmeid järgmiste protseduuride läbiviimiseks:

a) PIN-koodide asendamine;

b) uute võtmepaaride genereerimise autoriseerimine;

c) turvaliste laadimiskäsujadade moodustamine (sertifikaadid ja lisarakendused).

4.1.3.2 Autentimisobjektide asendamise võti – CMK1

Autentimisobjektide asendamise võtit (CMK1) kasutatakse autentimisobjektide asendamise protseduuri läbiviimiseks.

4.1.3.3 Uute võtmepaaride genereerimise autentimise võti – CMK2a

Selle võtme abil autoriseerib kaardihalduskeskus uue võtmepaari genereerimise kaardil.

4.1.3.4 Sertifikaatide ülelaadimise käsujadade moodustamise võti – CMK2b

Selle võtme abil moodustab Kaardihalduskeskus kaardil olevate sertifikaatide turvalise uuendamise käsujadad.

4.1.3.5 Lisarakenduse laadimise turvalise käsujada moodustamise võti – CMK3

Selle võtme abil moodustab Kaardihalduskeskus lisarakenduste turvalise kaardile laadimise käsujadad.

4.1.3.6 Kaardikohaste CMK'de moodustamise protseduur

Kaardikohased CMK'd genereeritakse keskuse CMK'dest, krüptides kaardihalduskoodi (vt "Kaardihalduskoodi tuletamise protseduur" allpool) vastava keskuse CMK'ga 3DES-algoritmi abil CBC-režiimis, kus IVC=0. Saadud tulemuses seatakse iga baidi noorim bitt nii, et bait oleks paaritu.

4.1.3.7 Kaardihalduskoodi tuletamise protseduur

Kaardihalduskood on kaardikohane ning tuletatakse alljärgnevalt:

1: arvutatakse kaardi kasutaja isikukoodi SHA-1 räsi.

2: võetakse sellest 16 vasakpoolsemat baiti.

4.1.4 Sertifikaadid

EstEID kaardil on järgmised sertifikaadid:

- kaardi kasutaja autentimissertifikaat
- kaardi kasutaja allkirjasertifikaat
- EstEID sertifitseerimiskeskuse juursertifikaat

Sertifikaadid on kaardil salvestatud jadafailides ning neid võib kaardilt lugeda sertifikaatide lugemise protseduuri abil. Peale salvestamise ei teosta EstEID kaardi kiip sertifikaatidega mingeid operatsioone.

Sertifikaadid salvestatakse kaardile ning neid uuendatakse sertifikaatide laadimise protseduuri abil.

Kaardi kasutaja sertifikaadifailide maht on 600H baiti ning juursertifikaadi faili maht on 700H baiti.

Sertifikaadifailide FID'd on järgmised:

Sertifikaat	FID
Autentimissertifikaat	AA CE
Allkirjasertifikaat	DD CE
Juursertifikaat (kui on kaardil)	CA CE

4.1.5 Kaardi kasutaja salajased võtmed

EstEID kaardil on kaks salajast võtit, mis on seotud vastavalt kaardi kasutaja autentimissertifikaadiga ja kaardi kasutaja allkirjasertifikaadiga.

Salajased võtmed genereeritakse:

a) esmaselt kaardi personaliseerimisel (kaardisiseselt),

b) uute võtmepaaride genereerimise protseduuri käigus (samuti kaardisiseselt).

Kaardilt ei ole võimalik salajasi võtmeid välja lugeda. Võtme pikkus on 1024 bitti ning EstEID salvestab võtit CRT vormingus.

Salajaste võtmete avalik eksponent genereeritakse juhusliku väärtusena.

Võtmetega on seotud kasutuskordade loendurid algväärtusega 0xFFFFFF, mida vähendatakse ühe võrra pärast iga võtmega sooritatud operatsiooni.

Kuna need võtmed ei ole kaardivälistele rakendustele nähtavad, siis ei käsitle käesolev dokument nende paigutust kaardil.

4.1.6 Kaardi kasutaja isikuandmete fail

Kaardi kasutaja isikuandmete fail sisaldab kaardi kasutaja isikuandmeid. See fail on loetav isikuandmete faili lugemise protseduuri abil ning on mõeldud kaardi kasutaja andmete saamiseks elektroonsel kujul järgmistel juhtudel:

1. Kui kaardile ei ole laetud sertifikaati.
2. Host-rakendus ei töötle sertifikaate.
3. Uute sertifikaatide päringu moodustamiseks.

See fail täidetakse personaliseerimise ajal ning hiljem ei ole võimalik sellese kirjutatud andmeid muuta.

Kaardi kasutaja isikuandmete fail on muutuva kirjepikkusega formateeritud fail. Faili maksimaalne pikkus on 170H baiti, maksimaalne kirje pikkus on 32H baiti ja kirjete arv on 16(Dec). Fail sisaldab allpooltoodud kirjed. Sümbolid on kodeeritud ANSI koodilehekülje nr 1252 järgi vastavalt ISO 8859-1.

Kirje nr	Sisu	Maksimaalne pikkus
1	Perekonnanimi	28_d baiti
2	Eesnime rida 1	15_d baiti
3	Eesnime rida 2	15_d baiti
4	Sugu	1_d baiti
5	Kodakondsus	3_d baiti
6	Sünniaeg	10_d baiti
7	Isikukood	11_d baiti
8	Dokumendi seerianumber	8_d baiti
9	Kehtivuse viimane päev	10_d baiti
10	Sünnikoht	35_d baiti
11	Väljaandmise kuupäev	10_d baiti
12	Elamisloa tüüp	50_d baiti
13	Märkuste rida 1	50_d baiti
14	Märkuste rida 2	50_d baiti
15	Märkuste rida 3	50_d baiti
16	Märkuste rida 4	50_d baiti

4.2 EstEID turvakiibi operatsioonid

EstEID turvakiibi abil on võimalik teostada järgmisi operatsioone:

1. Sertifikaatide ja andmete lugemise operatsioonid
    a. sertifikaatide lugemine;
    b. kaardi kasutaja isikuandmete faili lugemine.
2. Kaardi kasutaja autentimise objektide haldamine
    a. PIN1, PIN2 ja PUK väärtuste muutmine;
    b. PIN1 ja PIN2 järjestikuste valesisestuste loendurite nullimine;
    c. 3DESKey'dele väärtuste omistamine.
3. Kaardi kasutaja autentimine
    a. kaardi kasutaja autentimine PIN1, PIN2 ja PUK abil;
    b. kaardi kasutaja autentimine 3DESKey1 ja 3DESKey2 abil.
4. Operatsioonid salajaste võtmetega
5. Kaardihaldusoperatsioonid
    a. autentimisobjektide asendamine;
    b. uute võtmepaaride genereerimine;
    c. sertifikaatide ülelaadimine;
    d. lisarakenduste laadimine ja kustutamine;

e. turvaliste laadimiskäskude jadade moodustamine.

4.2.1 Sertifikaatide ja andmete lugemine

4.2.1.1 Sertifikaatide lugemine

Sertifikaate loetakse kaardilt käsuga READ BINARY. Sertifikaadid on alati vabalt loetavad; mingit autentimist nende lugemiseks ei nõuta.

4.2.1.2 Kasutaja isikuandmete faili lugemine

Selle faili sisu võib alati lugeda käskudega READ RECORD, autentimist ei nõuta. Faili sisu kohta vt "4.1.6 Kaardi kasutaja isikuandmete fail".

4.2.2 Autentimisobjektide haldamine

4.2.2.1 PIN1, PIN2 ja PUK väärtuste muutmine

PIN1, PIN2 ja PUK väärtusi võib alati muuta käsuga CHANGE REFERENCE VALUES.

PIN1'le ja PIN2'le võib anda uued väärtused käsu RESET RETRY COUNTER asendava modifikatsiooni abil. Selle operatsiooni teostamiseks on vaja eelnevalt verifitseerida PUK või teostada operatsioon 3DESKey1'ga turvatuna PIN1 jaoks ja 3DESKey2'ga turvatuna PIN2 jaoks.

4.2.2.2 PIN1 ja PIN2 järjestikuste valesisestuste loenduri nullimine

PIN1 ja PIN2 blokeerumise korral võib need lahti blokeerida käsuga RESET RETRY COUNTER. Selle operatsiooni teostamiseks on vaja eelnevalt verifitseerida PUK või teostada operatsioon 3DESKey1'ga turvatuna PIN1 jaoks ja 3DESKey2'ga turvatuna PIN2 jaoks.

Blokeerunud PUK-koodiga kaardi võib muuta taas kasutatavaks PIN-koodide asendamise protseduuri abil.

4.2.2.3 3DESKey'le väärtuste omistamine

3DESKey1 on 3DESKeys faili kirjes 1 ja 3DESKey2 kirjes 2. Nendele võtmetele omistatakse väärtused käsu UPDATE RECORD abil.

Tavaliselt tuletatakse võtmete väärtused paroollausetest 3DESKey väärtuse tuletamise protseduuri järgi.

3DESKey'le väärtuse omistamise tingimuseks on, et PIN2 oleks verifitseeritud või kommunikatsioon oleks turvatud sama võtmega (eelmise versiooniga).

4.2.3 Kaardi kasutaja autentimine

4.2.3.1 Kaardi kasutaja autentimine PIN1, PIN2 ja PUK abil

Kaardi kasutaja autentimine PIN1, PIN2 või PUK abil toimub käsuga VERIFY. See operatsioon on teostatav piiranguteta.

4.2.3.2 Kaardi kasutaja autentimine 3DESKey1 ja 3DESKey2 abil

Kaardi kasutaja loetakse autendituks, kui nende võtmete abil toimub turvaline kommunikatsioon kaardi ja host-rakenduse vahel. Eraldi autentimise protseduuri ei ole.

4.2.4 Operatsioonid salajaste võtmetega

Autentimisvõtmega arvutatakse vastus (digitaalne allkiri) kutsungile SSL autentimise protseduuri käigus.

Toetatavad algoritmid on RSA ja SHA1withRSA. Teiste algoritmide kasutamist ei ole ette nähtud. Kasutatavad käsud on PERFORM SECURITY OPERATION – SIGN ja DECIPHER, vastavalt standardi PKCS#1 v 1.5 ja 2.0.

Autentimise salajase võtmega operatsiooni teostamise eelduseks on, et PIN1 on verifitseeritud või kommunikatsioon on turvatud 3DESKey1 abil.

Allkirjastamise salajast võtit kasutatakse digitaalallkirjade arvutamiseks.

Allkirjastamise salajase võtmega operatsiooni teostamise eelduseks on, et PIN2 on verifitseeritud või kommunikatsioon on turvatud 3DESKey2 abil. PIN2 verifitseerimine kehtib vaid ühe allkirja arvutamiseks. Järgmise allkirja arvutamiseks tuleb PIN2 verifitseerida uuesti.

4.2.5 Kaardihaldusoperatsioonid

4.2.5.1 PIN-koodide asendamine

See operatsioon koosneb järgmistest osadest:

1. saadakse autoriseering kaardihalduskeskusest CMK1 abil,
2. kaardile seatakse uued PIN1, PIN2 ja PUK (võivad olla kaardi kasutaja poolt sisestatud samas terminalis).

PIN1, PIN2 ja PUK hilisem muutmine toimub kaardi kasutaja äranägemisel.

Protseduur toimub järgmiselt (protseduur peab toimuma autoriseeritud büroos):

1. Pärast kaardi kasutaja isiku visuaalset tuvastamist loeb terminal kaardilt kutsungi.
2. Terminal saadab kutsungi turvaliselt, st teenindaja poolt allkirjastatult, Kaardihalduskeskusele.
3. Kaardihalduskeskus kontrollib, et teenindaja on autoriseeritud seda protseduuri läbi viima ning annab CMK1 kasutades autoriseeringu.
4. Pärast Kaardihalduskeskuse poolt autoriseeringu saamist lubab kaart kasutada käsku Reset Retry Counter ilma täiendava autoriseerimiseta ning asendada PIN- ja PUK-koode ilma nende eelnevaid väärtusi teadmata.

4.2.5.2 Uute võtmepaaride genereerimine

Uute võtmepaaride genereerimise kaardil võib teostada, kui Kaardihalduskeskuselt on saadud vastav autoriseering, kasutades CMK2a võtit.

Genereeritud võti muutub võtme uueks versiooniks, kusjuures võtme jooksev versioon säilib. Võtme uut versiooni on võimalik kasutada spetsiaalse protseduuri abil.

Sertifikaadi laadimisega seotud protseduur muudab võtme jooksva versiooni eelmiseks ning uue versiooni jooksvaks. Operatsioonid võtme vana versiooniga on teostatavad spetsiaalse protseduuri abil.

4.2.5.3 Sertifikaatide ülelaadimine

Sertifikaatide ülelaadimine toimub turvatud käsujada saatmisega EstEID kaardile. Selle turvatud käsujada moodustab Kaardihalduskeskus CMK2b abil (vt “4.2.5.5 Turvatud käsujadade moodustamine”).

Sertifikaadi ülelaadimine võib toimuda, kui PIN1 on kontrollitud, et tagada operatsiooni toimumine ainult kaardi kasutaja teadmisel.

Vajadusel modifitseerib sertifikaadi ülelaadimise käsujada salajaste võtmete viitasid, et seada võtme uus versioon jooksvaks versiooniks.

4.2.5.4 Lisarakenduste laadimine ja kustutamine

Selleks, et kaitsta EstEID kaardi väljaandja õigusi, saab lisarakenduste kaardile laadimine ja kaardilt kustutamine toimuda ainult väljaandja poolt autoriseeritult. Kaardi väljaandjal on samuti kontroll laetavate lisarakenduste struktuuri ja tööpõhimõtete üle.

EstEID kaart aktsepteerib uusi katalooge ja andmefaile moodustavaid käske ainult CMK3 abil turvatud käsujadades (vt “4.2.5.5 Turvatud käsujadade moodustamine”).

Lisarakenduse laadimise käsujada moodustamise protseduur on järgmine:

1. Lisarakenduse moodustaja annab rakendust loova koodi kaardihaldajale.
2. Kaardi haldaja inspekteerib koodi, hinnates lisarakenduse poolt võimalikult tarbitava mälu hulga jt omadused ning kinnitamise korral asub moodustama turvatud laadimiskoodijadasid.

Sama protseduur kehtib ka lisarakenduste kustutamise käsujadade kohta.

Lisarakenduse laadimine võib toimuda, kui PIN1 on kontrollitud, et tagada operatsiooni toimumine ainult kaardi kasutaja teadmisel.

4.2.5.5 Turvatud käsujadade moodustamine

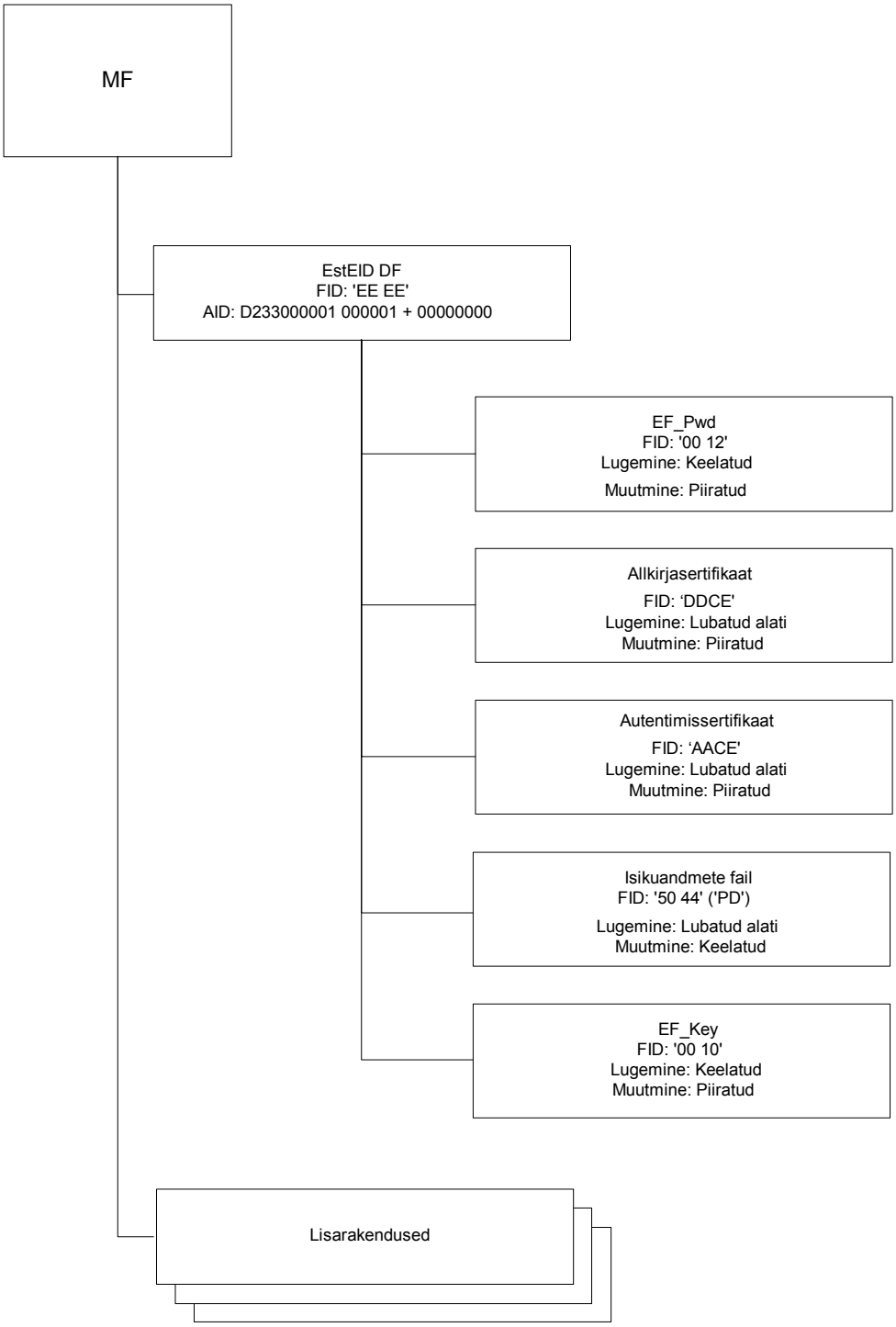
Turvatud laadimiskäskude jadad moodustatakse APDU-käskudele vastava võtmega MAC-koodide arvutamisega MICARDO PRO-SM režiimi jaoks.

Laadimiskäskude jadasid moodustab Kaardihalduskeskus ning need on üldkättesaadavad.

Laadimiskäskude jadad on kaardikohased.

4.3 EstEID failisüsteem

EstEID failisüsteem on kujutatud alljärgneval joonisel. Näidatud ei ole faile, millele kaardivälistel rakendustel puudub juurdepääs.


MF
EstEID DF
FID: 'EE EE'
AID: D233000001 000001 + 00000000
EF_Pwd
FID: '00 12'
Lugemine: Keelatud
Muutmine: Piiratud
Allkirjasertifikaat
FID: 'DDCE'
Lugemine: Lubatud alati
Muutmine: Piiratud
Autentimissertifikaat
FID: 'AACE'
Lugemine: Lubatud alati
Muutmine: Piiratud
Isikuandmete fail
FID: '50 44' ('PD')
Lugemine: Lubatud alati
Muutmine: Keelatud
EF_Key
FID: '00 10'
Lugemine: Keelatud
Muutmine: Piiratud
Lisarakendused

4.4 Objektid EstEID kaardil väljaandmise hetkel

Kasutajale üleandmise hetkel sisaldab EstEID kaart järgmisi andmeid:

Objekt	**Sisu**
Isikuandmete fail	Täidetakse personaliseerimise käigus
Autentimisvõti	Genereeritakse kaardil personaliseerimise käigus
Autentimissertifikaat	Laetakse kaardile personaliseerimise käigus
Allkirjastamisvõti	Genereeritakse kaardil personaliseerimise käigus
Allkirjastamissertifikaat	Laetakse kaardile personaliseerimise käigus
Juursertifikaadid	Laetakse kaardile personaliseerimise käigus
PIN1, PIN2 ja PUK	Seatakse personaliseerimise käigus
Kaardihaldusvõtmed CMK1, CMK2a, CMK2b, CMK3	Seatakse personaliseerimise käigus
3DESKey1 ja 3DESKey2	Täidetakse personaliseerimise käigus väärtustega 00...00

Personaliseerija trükib turvaümbrikusse kaardile seatud PIN1, PIN2 ja PUK, üleandmiseks kaardi kasutajale.

5 EstEID abiprotseduurid

5.1 EstEID turvaline kommunikatsioon

Seda protseduuri kasutakse juhul, kui kaardi kasutaja on autenditud paroollause abil. Protseduuri käigus vahetatakse andmeid EstEID kaardiga, turvatuna sessioonivõtmetega, mis on tuletatud 3DESKey1 ja 3DESKey2 abil. Vahetatavad andmed on krüptitud ning kaitstud krüptograafiliste kontrollsummade ja loenduritega.

5.2 3DESKey tuletamine paroollausest

Selle peatüki käesolevasse spetsifikatsiooni lülitamise eesmärk on tagada ühtne protseduur #DESKey tuletamiseks paroollausest. Protseduur on järgmine:

1: arvutatakse paroollause SHA-1 räsi;

2: võetakse räsi 16 vasakpoolsemat baiti;

3: iga baidi noorim bitt seatakse nii, et bait oleks paaritu.

6 EstEID kaardi turvastruktuur

Iga loogiline operatsioonide grupp on EstEID kaardil koondatud turvakeskkonda, mis piirab kättesaadavate operatsioonide valikut nii, et juurdepääs on vaid selles grupis vajalikele operatsioonidele. Näiteks, operatsioonid salajaste võtmetega ei ole kättesaadavad sertifikaatide ülelaadimise ajal, kuna viimane võib toimuda ebaturvalises või kaardi kasutaja poolt mittekontrollitavas keskkonnas.

6.1 Turvakeskkondade ja operatsioonide risttabel

Alljärgnevas tabelis on kokku võetud EstEID kaardis kasutatavad turvakeskkonnad ning operatsioonide kättesaadavus nendes:

	Isikuandmete faili lugemine	Kasutajasertifikaatide lugemine	Juursertifikaatide lugemine	Autentimisvõtme kasutamine	Allkirjastamisvõtme kasutamine	PIN1 lahtiblokeerimine (ka PIN1 asendamisega)	PIN2 lahtiblokeerimine (ka PIN2 asendamisega)	PIN1, PIN2 ja PUK muutmine	Väärtuse andmine PIN1'le	Väärtuse andmine PIN2'le	Väärtuse andmine 3DESKey1'le	Väärtuse andmine 3DESKey2'le	PUK lahtiblokeerimine ja uue väärtuse seadmine	Uute võtmepaaride genereerimine	Sertifikaatide ülelaadimine	Uute failide moodustamine MF kataloogis
PKI keskkond (SE#01)	ALW	ALW	ALW	PIN1	PIN2 Iga op. jaoks	PUK	PUK	ALW	NEV	NEV	PIN2	PIN2	NEV	NEV	NEV	NEV
PKI keskkond, turvatud kommunikatsiooniga (SE#02)	ALW	ALW	ALW	3DK1	3DK2	3DK1 ja PUK	3DK2 ja PUK	ALW	NEV	NEV	3DK1	3DK2	NEV	NEV	NEV	NEV
Sertifikaatide ülelaadimine (SE#03)	ALW	ALW	ALW	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	PIN1 ja A2	PIN1 ja SC2	NEV
Autentimisobjektide asendamine (SE#04)	ALW	ALW	ALW	NEV	NEV	A1	A1	NEV	A1	A1	NEV	NEV	A1	NEV	NEV	NEV
Lisarakenduste laadimine (SE#05)	ALW	ALW	ALW	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	NEV	PIN1 ja SC3
Dekrüptimine PIN-autentimisega (SE#6)	ALW	ALW	ALW	PIN1	PIN2 Iga op. jaoks	PUK	PUK	ALW	NEV	NEV	PUK	PUK	NEV	NEV	NEV	NEV
Dekrüptimine paroollausega autentimisega (SE#7)	ALW	ALW	ALW	3DK1	3DK2	NEV	NEV	ALW	NEV	NEV	3DK1	3DK2	NEV	NEV	NEV	NEV

Tähistuste seletused:

ALW – operatsioon on kättesaadav alati

NEV – operatsioon ei ole selles turvakeskkonnas kättesaadav

PIN1 – operatsioon on kättesaadav, kui PIN1 on kontrollitud

PIN2 – operatsioon on kättesaadav, kui PIN2 on kontrollitud

PIN2 iga op jaoks – operatsioon on kättesaadav, kui PIN2 on kontrollitud ning kontroll kehtib vaid ühe operatsiooni jaoks

PUK – operatsioon on kättesaadav, kui PUK on kontrollitud

3DK1 - operatsioon on kättesaadav, kui kommunikatsioon kaardiga on turvatud 3DESKey1 abil

3DK2 - operatsioon on kättesaadav, kui kommunikatsioon kaardiga on turvatud 3DESKey2 abil

A1 - operatsioon on kättesaadav, on saadud autoriseerimine Kaardihalduskeskusest CMK1 kasutades

A2 - operatsioon on kättesaadav, on saadud autoriseerimine Kaardihalduskeskusest CMK2a kasutades

SC2	-	operatsioon on kättesaadav, kui käsujada on turvatud CMK2b kasutades
SC3	-	operatsioon on kättesaadav, kui käsujada on turvatud CMK3 kasutades.

6.2 Kommentaarid turvakeskkondade kohta

6.2.1 PKI keskkond (SE#01)

See on PKI operatsioonide teostamiseks mõeldud turvakeskkond, kus kasutaja autentimine toimub PIN-koodide abil. Ühendust kaardi ja kaarti kasutava rakenduse vahel eraldi ei turvata. See turvakeskkond on sobiv kasutamiseks piiratud klaviatuuridega turvalistes keskkondades nagu näiteks pangaautomaadid. Täisklaviatuuriga keskkonnad võivad kasutada ka turvakeskkonda SE#2, kus kommunikatsioon host-rakenduse ja kaardi vahel on turvatud.

6.2.2 PKI keskkond, turvatud kommunikatsiooniga (SE#02)

See on PKI operatsioonide teostamiseks mõeldud turvakeskkond, kus kasutaja autentimine toimub 3DESKey1 ja 3DESKey2 abil. Seda turvakeskkonda võib kasutada täisklaviatuuriga seadmetes, kuna 3DESKey1 ja 3DESKey2 tuletatakse paroollausetest. Kuna siin on turvatud andmevahetus host-rakenduse ja kaardi vahel, siis on piraatkoodidel initsiatiivi saamiseks vähem võimalusi.

6.2.3 Sertifikaatide ülelaadimise keskkond (SE#03)

Selles turvakeskkonnas kasutatavad operatsioonid on uute võtmepaaride genereerimine ja sertifikaatide ülelaadimine. Operatsioonid saavad toimuda, kui PIN1 on kontrollitud, et tagada operatsiooni toimumine kaardi kasutaja teadmisel.

6.2.4 Autentimisobjektide asendamise keskkond (SE#04)

Selles turvakeskkonnas on kasutatav vaid autentimisobjektide asendamise operatsioon.

6.2.5 Lisarakenduste laadimise keskkond (SE#05)

Selles turvakeskkonnas on kasutatav vaid lisarakenduse laadimise operatsioon, mille toimumise eelduseks on PIN1 kontroll, et tagada operatsiooni toimumine kaardi kasutaja teadmisel.

6.2.6 Dekrüptimisoperatsioonide keskkonnad (SE#6, SE#7)

Nendes turvakeskkondades toimuvad kaardi kasutaja avalike võtmetega moodustatud krüptogrammide dekrüptimised kaardi kasutaja salajaste võtmetega.

7 Juhiseid kaarti kasutavate rakenduste kirjutajaile

7.1 EstEID kiibi käsustik

EstEID käesolev versioon on realiseeritud ORGA Micardo Public 2.1 kiipkaardil. Kaardi liides on dokumenteeritud ”Micardo 2.1 Chip Card Operating System User Manual”’s, mis on ORGA Micardo arendussüsteemi osa.

Kaardi liidese käsud, millele selles spetsifikatsioonis viidatakse, ei pruugi olla antud operatsiooni teostamise ainuvõimalikud viisid.

7.2 EstEID kiibi ATR ajaloolised baidid

EstEID käesoleva versiooni ajaloolised baidid on (kokku 14 baiti):

EstEID ver 1.0

Tulevased versioonid saavad suurema versiooninumbri.

7.3 EstEID kiibi erinevused standardsest MICARDO 2.1st

Siin on loetelu EstEID kiibi liidese erinevustest võrreldes standardse MICARD 2.1'ga, mis on kirjeldatud dokumendis "Micardo 2.1 Chip Card Operating System User Manual".

7.3.1 ATR modifikatsioon

Et tagada EstEID kaardi tõrgeteta töö võimalikult suures valikus PC/SC liidesega lugejates, on parameetri TA3 (informatsioonivälja maksimaalne pikkus) väärtuseks pandud 250 (standard MICARDO's 254).

7.3.2 EEPROM initsialiseerimine ja kaardi formateerimine

Need operatsioonid puuduvad.

7.4 Üldisi juhiseid

Käesolevas dokumendis toodud EstEID kaardi liidese ja tööpõhimõtete spetsifikatsioon ei eelda kohustuslikke ettekirjutusi EstEID kaarti kasutavate rakenduste programmeerimisele.

Samas võib aga ära tuua mõned juhised, mis võivad rakenduste programmeerimisel kasulikeks osutuda:

Kaardi kasutaja autoriseerimine PIN-koodiga või paroollausega?

PIN-koodiga autoriseerimist tuleb kasutada piiratud klaviatuuriga seadmetel. Täisklaviatuuriga seadmetel võib kasutada autoriseerimist kas PIN-koodidega või paroollausetega. Rakendus võib pakkuda ka kaardi kasutajale valikuvõimalust.

7.4.1 Seadmete avamine eksklusiivses režiimis

EstEID kiip on üheolekuline masin. Segaduste vältimiseks ning kaardi kaitsmiseks piraatkoodide eest on soovitatav avada kaardilugeja eksklusiivses režiimis.

7.4.2 Muutuva pikkusega PIN-koodid

EstEID kiibi PIN- ja PUK-koodid on muutuva pikkusega ning rakendusel ei ole koodi pikkust võimalik ette teada. Rakendus peab võimaldama muutuva pikkusega koodi sisestamist.

7.4.3 Transaktsiooniaja minimeerimine

Kuna EstEID kaarti kasutatakse keskkondades, kus töötavad korraga paljud programmid ning tavakasutaja kontroll keskkonna üle on nõrk, siis on soovitatav programmeerida rakendused nii, et operatsioonid kaardiga toimuksid võimalikult lühikeses ajavahemikus (üksteise järel) ning pärast operatsioonide lõpetamist (tulemuse saamist) lülitataks kaart välja, kuid jäetaks siiski antud rakenduse kasutusse. Sellisel moel toimimine vähendab esiteks võimalust, et kasutaja võtab kaardi lugejast enneaegselt välja ja teiseks väldib piraatkoodide juurdepääsu kaardile.

7.4.4 Rakenduste koodide signeerimine

Rakenduste koodid tuleb signeerida, et kasutaja saaks kontrollida EstEID kaarti töötleva tarkvara auentsust.