Vabariigi Valimiskomisjon

Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Üldosa

versioon 1.3

dokument: EHA-03-05-1.3
kuupäev: 16.09.2009

Muudatuste ajalugu

kuupäev	versioon	kirjeldus	autor
08.02.2007	1.0	Muudatuste arvestuse algus.	Uve Lokk
11.02.2007	1.1	Muudetud protseduuride liigendust	Tarvi Martens
08.05.2009	1.2	Lisatud üldskeem, parandatud peatükki "Partitisiooni loomine ja häälestus"	Uve Lokk
16.09.2009	1.3	läbivad parandused ja täiendused.	Uve Lokk

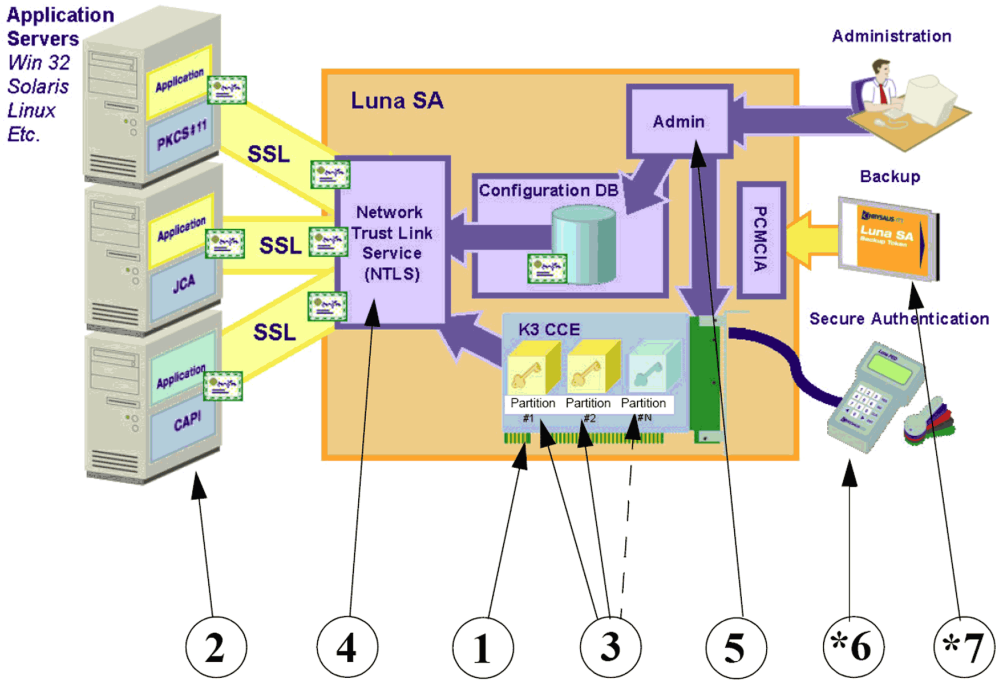
Sisukord

1. Sissejuhatus

Dokumendi ülesandeks on

- kirjeldada raudvaralisest turvamooduli (edaspidi lühendatult HSM) ülesehitust ja funktsioone ja häälestusvõimalusi,
- seletada, miks HSMi tegevusjuhendis (dokument EHA-03-06-*) üht-või-teist tehakse nii nagu seal kirjas on.

2. Turvamooduli ülevaade



Joonis 1 HSMi ülevaade. 1- krüptomootor, 2 - kliendid, 3 - partitsioonid, 4 - NTLS, 5 - käsuliides, 6 - PED ja PEDi võtmed, 7 – varundustoken (Joonise allikas: Luna SA originaaldokumentatsioon)

Raudvaraliseks turvamooduliks on SafeNet'i toode Luna SA. Mooduli peamisteks komponentideks on (vt. joonis 1):

krüptomootor - krüptograafiliste ülesannete täitmiseks ja krüptograafiliste võtmete hoidmiseks. Aga samuti administratiivse ligipääsu kontrolliks ja sätete halduseks. Krüptomootoril on osa sätteid häälestatavad (vt. tabel 2).

partitsioon - loogiline piirkond krüptomootoris. Igal partitsioonil on oma sätted, ligipääsutunnused ja krüptoobjektid (võtmed, serifikaadid). E-hääletuse HSMis saab luua vaid ühe partitsiooni.

klient - rakendustarkvara või -server, mis pöördub turvamooduli partitsiooni poole krüptoobjektide loomiseks, kasutamiseks või kustutamiseks. E-hääletuse kontekstis on kliendiks häälte lugemise rakendusserver (edaspidi HLR).

Network Trust Link (NTL) - asümmeetriliselt krüpteeritud (privaat- ja avalik võti) kliendi ja HSMi vaheline TCP/IP-võrguprotokollil põhinev ühendus.

käsuliides - keskkond HSMi haldamiseks.

ligipääsukontroll - koosneb kahest komponendist: PIN-koodi sisestusseadmest ehk PEDist (ingl. k. „PIN Entry Device") ja hulgast värvilistest võtmetest (võtmetest lähemalt vt. "3.1 Võtmed"). Värvilised võtmed on autentimistokenid, PED on vahendusliides

- edastamaks võtmete infot krüptomootorile;
- võtmete PINi sisestuseks

varundustoken - andmekandja partitsiooni varundamiseks.

HSMi metallkaanega kaitstud esiküljel asub mooduli sisse-/väljalülitamisnupp, haldus(jada-)liides, PEDi ühendusliides ning varundustokeni sisestusliides; seadme tagaküljel asuvad kaks võrguliidest ning elektripistik.

3. Mõisted

Süsteemi võtmepaar – kahest asümmeetrilisel RSA krüptoalgoritmil põhinevast bitistringist kogum. Üheks stringiks on avalik võti ning teiseks privaatvõti. Avaliku võtmega krüpteeritud digitaalne objekt / string on dekrüpteeritav vaid sama võtmepaari privaatvõtmega.

Süsteemisertifikaat – süsteemi privaatvõtmega allkirjastatud süsteemi avalik võti. Süsteemisertifikaat imporditakse valijarakendusse ning sellega krüpteeritakse elektrooniline hääl.

4. 'Värvilised' võtmed ja rollid

4.1. 'Värvilised' võtmed

korpusevõti - tavaline mehaaniline võti HSMi esikaane avamiseks. Varuvõti olemas.

värviline võti - võtmekujulisse värvilisse plastikkesta „pakendatud" programmeeritav mälukiip. Värviline võti on kas hall, sinine, punane, must või roheline.

PIN - autentimisel teatud värviliste võtmetega kasutatav vabalt määratav 4-16 numbrist koosnev arv. PIN on võimalik jätta ka määramata, sel juhul ei ole võtme kasutamine PINiga kaitstud.

MofN - ehk „mitu-mitmest"-skeem. On olemas N võrdväärset võtit. Selleks, et nende võtmetega seotud protsessi käivitada, on vaja M võtme kohalolu.

hall võti - staatilise infoga (st. võtmel olevat infot ühegi protsessi või tegevuse käigus üle ei kirjutata) PINita värviline võti. Varuvõti olemas.

sinine võti - dünaamilise infoga (st. võtmel olev info on ülekirjutatav) PINiga värviline võti. Varuvõtit on võimalik luua.

punane võti - dünaamilise infoga PINita värviline võti. Varuvõtit on võimalik luua.

must võti - dünaamilise infoga PINiga värviline võti. Varuvõtit on võimalik luua.

rohelised võtmed - MofN-võtmed. PINi ei kasutata. Varuvõtmeid N-M tükki

grupivõti - sinise ja musta võtmega seotud võimalus kasutada sama võtit mitme partitsiooniga, ent eri PINidega. Sisuliselt on grupivõti ka punane võti, kui sama võtmega seotakse mitu serverit.

võtme kasutamine - värviline võti sisestatakse PEDi parema külje keskosas olevasse pilusse ning keeratakse veerand ringi päripäeva. Õnnestunud kasutamisel läheb PEDil põlema roheline signaaltuli „KEY IN".

4.2. Rollid

HSMi puhul on võimalik eristada kuut rolli:

1. serveriülem - tunnus: serveri salasõna
2. turvaülem - tunnus: sinine võti
3. rakenduseülem - tunnus: must võti, partitsiooni salasõna
4. lähtestaja - tunnus: hall võti
5. varundusülem - tunnus: punane võti
6. statistid - tunnus: roheline võti

Tabel 1. Protseduuride ja kasutajatunnuste seosed

toiming	korpusevõti	admin'i parool	sinine võti	rohelised võtmed	hall võti	punane võti	partitsiooni parool	must võti
serveri sisselülitamine; PEDi ühendamine; ligipääs jada- ja varundusliidesele	e							

toiming	korpusevõti	admin'i parool	sinine võti	rohelised võtmed	hall võti	punane võti	partitsiooni parool	must võti
admin: syslog *; hsm: näita sätteid (hsm sh); partitsioon: näita partitsiooniteavet (par s) ja sätteid (par showP), partitsioonide nimekiri (par l), pakettide nimekiri (package -list, -listfile); kliendihaldus (cli *)	e	e						
hsm: init	e	e			+			
hsm: sätte muutmine (hsm changePo); package verify, update; partitsioon: loomine (par cr), sätete muutmine (par changePo)	e	e	+	+				
HLR: objektide loetelu (cmu list), kustutamine (cmu delete)	e						+	+
partitsioon: näita partitsiooni objekte (par showC); partitsiooni aktiveerimine (par ac)	e	e		+			+	+
HLR: objektide (sertifikaatide loomine (cmu gen)	e	e		e			+	e
partitsioon: varundamine (par b)	e	e	+	+		+	+	+
partitsioon: taastamine	e[1]	e[1]	e[1]	e[1], +	e[1]	+	e[1]	e[1], +

e - eeldus: need võtmed/salasõnad peavad olema eelnevalt kasutatud

e[1] - eeldus: uue seadme kasutajatunnus

E-hääletamise puhul on rollid koondatud, mille järel viimased näevad välja järgmiselt:

1. serveriülem - tunnusteks korpusevõti, serveri salasõna ning hall võti;
2. turvaülem - tunnusteks punane, sinine ja must võti ning partitsiooni salasõna;
3. statistid - N rohelise võtme omanikku. Statistiks ei tohi olla serveri- ega turvaülem. Eesti e-hääletuse kontekstis on statistideks Vabariigi Valimiskomisjoni liikmed.

5. Objektid

Objektideks on:

- turvamoodul
- võtmed
- salasõnad
- varundustoken

Nende hoidmisel peaks silmas pidama, et

- võtmeid hoitaks eraldi salasõnadest
- eri rolli võtmeid koos ei tohi hoida
- varundustoken'it tuleb hoida eraldi punasest võtmest

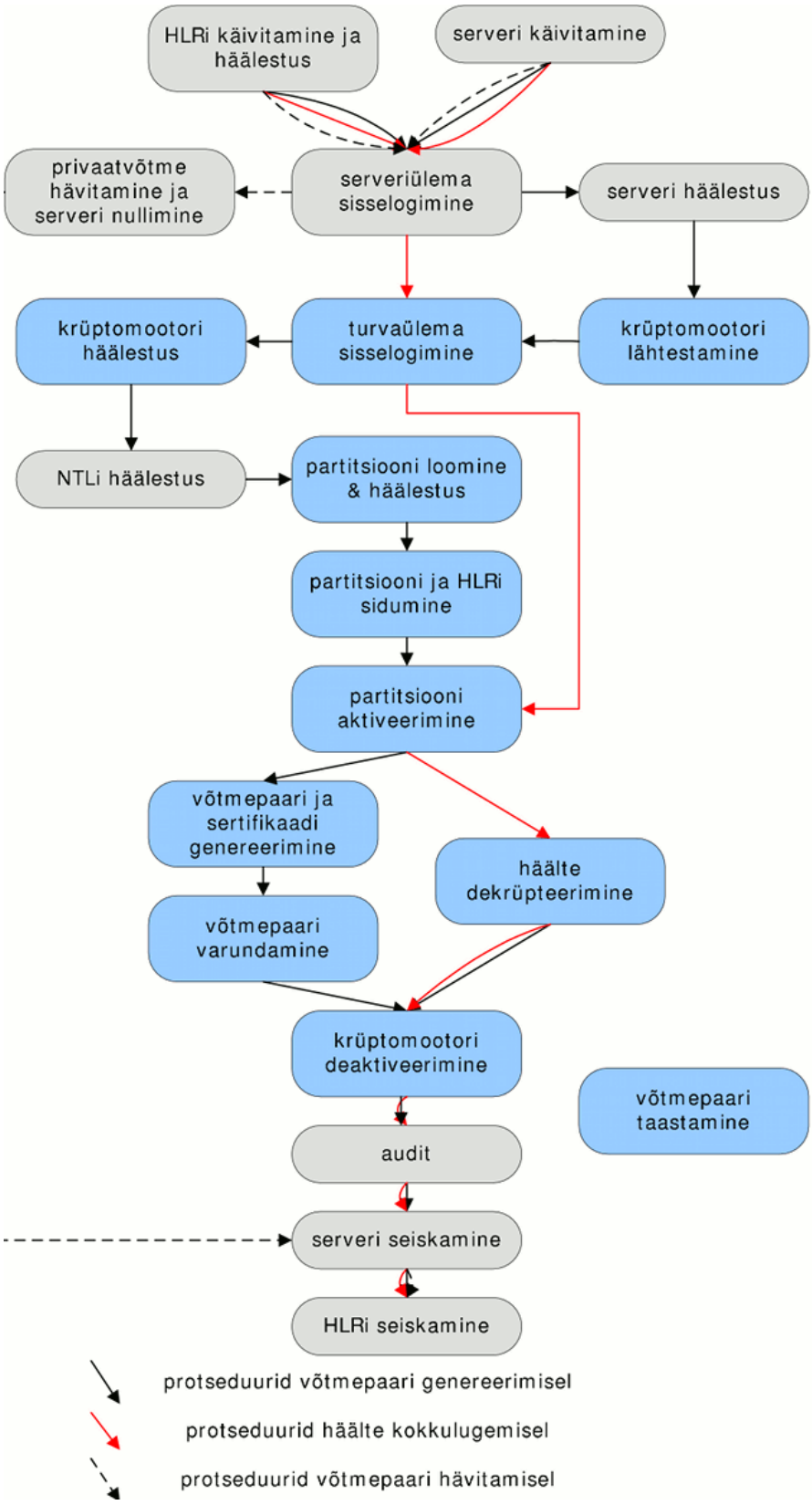
Seega on varuobjektidele vaja minimaalselt kolme hoiupaika:

1. süsteemiülema võtmed
2. turvaülema võtmed
3. salasõnad + varundustoken

6. Protseduurid

Protseduure on kokku neli, millest igaühel on mitu alamprotseduuri:

- süsteemi võtmepaari loomine
    - HSMi käivitamine
    - HLRi käivitamine ja häälestus
    - serveriülema sisselogimine
    - HSMi häälestus
    - krüptomootori lähtestamine
    - turvaülema sisselogimine
    - krüptomootori häälestus
    - partitsiooni loomine ja häälestus
    - NTLi häälestus
    - partitsiooni ja HLRi sidumine
    - partitsiooni aktiveerimine
    - võtmepaari ja sertifikaadi genereerimine



Joonis 2 Protseduuride üldskeem.

    - süsteemisertifikaadi eksport
    - võtmepaari varundamine
    - partitsiooni deaktiveerimine ja süsteemiülema deautoriseerimine
    - HSMi seiskamine
    - HLRi seiskamine
- häälte kokkulugemine (võtmepaari testimine)
    - HSMi käivitamine
    - HLRi käivitamine ja häälestus
    - serveriülema sisselogimine
    - turvaülema sisselogimine
    - partitsiooni aktiveerimine
    - häälte dekrüpteerimine ja kokkulugemine
    - partitsiooni deaktiveerimine ja süsteemiülema deautoriseerimine
    - HSMi seiskamine
    - HLRi seiskamine
- süsteemi võtmepaari taastamine
- privaatvõtme hävitamine
    - HLRi käivitamine ja häälestus
    - HSMi käivitamine
    - serveriülema sisselogimine
    - krüptomootori lähtestamine
    - partitsiooni loomine
    - partitsiooni varundamine
    - serveri seiskamine
    - HLRi seiskamine

Nagu eelnevast näha, võivad eri protseduurid sisaldada samu alamprotseduure.

6.1. Protseduuride kirjeldus

6.1.1. Süsteemi võtmepaari loomine

Protseduuri käigus luuakse süsteemi võtmepaar, seejärel süsteemisertifikaat. Viimane imporditakse klientserverisse (HLRi).

6.1.2. Häälte kokkulugemine (võtmepaari testimine)

Protseduuri eesmärgiks on dekrüpteerida ning kokku lugeda valijate antud elektroonilised hääled. Mainitud protseduur sooritatakse häältelugemisrakenduse abil.

Enne kui luuakse häälte lugemise rakendusserveri NTLi võtmed, keeratakse HLRi kell ühe päeva võrra tagasi. Seda juhuks, kui HSM ja HLR peaks ajavööndeid erinevalt mõistma. Vastasel juhul võib juhtuda, et HLRis genereeritud võti hakkab

HSMis kehtima alles tulevikus, mis teeb aga edasised võtmeprotseduurid võimalikuks alles tund aega hiljem. Pärast NTLi võtmepaari loomist muudetakse HLRi kellaaeg õigeks.

Võtmepaari testimiseks viiakse läbi sama protseduur mis häälte kokkulugemisel. Eesmärgiks on testida süsteemi võtmepaari korrektsust, ent ka seda, et valijarakenduses oleks õige süsteemisertifikaat. Hääletada saab piiratud ligipääsuga ning tulemus ei ole juriidiliselt kehtiv.

6.1.3. Privaatvõtme hävitamine ja HSMi nullimine

Süsteemi privaatvõti tuleb kustutada, välistamaks selle hilisemat sattumist kasutaja kätte, kelle valdusesse võivad olla sattunud ükskõik-mis-põhjusel elektroonilised hääled, veel hullem kui koos isikuandmetega (digitaalallkiri).

Protseduuri eesmärgiks on hävitada süsteemi privaatvõti, et oleks välistatud hilisem võimalik hääletaja isikuandmetega ümbrikus oleva hääle dekrüpteerimine. Selleks on vaja

1. hävitada HSMis olev süsteemi privaatvõti;
2. hävitada varundustokenile varundatud süsteemi privaatvõti;
3. taaslähtestada punased võtmed

Ehkki varundustokenil olev süsteemi võtmepaar on pärast punaste võtmete taaslähtestamist tootja väitel kättesaamatu, oleks siiski mõistlik hävitada varundustoken'il olev info. Lihtsaim moodus selleks on järgmine:

1. HSMi taaslähtestamine, mille käigus luuakse uus domeen (punaste võtmete info kirjutatakse üle) ning hävitatakse partitsioon koos kõigi oma objekti-dega; selle käigus värvilisi võtmeid ei kasutata grupivõtmetena;
2. uue, tühja partitsiooni loomine, kusjuures grupivõtit musta võtme korral ei kasutata;
3. eelmises punktis mainitud partitsiooni varundamine; selle käigus kirjuta-takse üle varundustokenil olev teave, kaasa arvatud süsteemi privaatvõti

6.1.4. Süsteemi võtmepaari taastamine

Protseduur juhuks, kui partitsioon või HSM peaks riknema. Sel juhul saab süsteemi võtmepaari uue HSMi uuele partitsioonile taastada.

Protseduur eeldab, et

- on olemas
    - häälestatud HLR;
    - süsteemi võtmepaariga varundustoken;
    - uus HSM;
- osalevad vana (riknenud) HSMi punase, musta ja roheliste võtmete hoidjad;

6.2. Alamprotseduuride kirjeldus

Järgnevalt kirjeldame alamprotseduure, mis tehakse läbi HSMi protseduuride käigus.

6.2.1. HSMi käivitamine

Alamprotseduuri käigus

- kontrollitakse, et server ei oleks füüsiliselt kompromiteeritud;
- seatakse HSM käivitusvalmis;
- lülitatakse HSM sisse.

Vajalik on hõbedane metallist korpusevõti. Uusi salasõnu ja võtmeid ei looda.

6.2.2. HLRi käivitamine ja häälestus

alamprotseduuri eesmärgiks on HLRi käivitamine ja tema häälestus. Selle käigus sätitakse kasitsi õigeks HLRi kell (isoleeritud süsteem!), ning häälestatakse TCP/IP-protokoll ja minicom-klientrakendus. Protseduuriks on tarvis teada HLRi kasutaja ‚root' salasõna. Taaskäivitada tuleb ka süsteemilogi-teenus, et see arvestaks õigekssätitud ajaga. Uusi salasõnu ja võtmeid ei looda.

6.2.3. Serveriülema sisselogimine

Alamprotseduuri eesmärgiks on serveriülemale HSMI käsureale ligipääsu andmine.

Teadma peab vaikimisi määratud serveriülema salasõna. Juhul, kui süsteemi võtmepaari loomise protseduuri käigus ei kehti teadaolev serveriülema salasõna, tuleb see tühistada. Salasõna tühistamiseks tuleb püüda kasutajana 'admin' kümme korda HSMi sisse logida vale salasõna kasutades. Serveriülema uue salasõna määramisel peab arvestama, et

- salasõna võib koosneda neljast komponendist: suured tähed, väiksed tähed, numbrid ning erimärgid (näiteks $%., jne.).
- salasõnas peab ülalmainitud neljast komponendist olema kasutatud kolme.

Häälte kokkulugemise protseduuril seda võtet kasutada ei tohi, kuna 10-kordne valede kasutajatunnustega ligipääsu katsetamine kustutab HSM'ist partitsiooni koos süsteemi võtmepaariga.

Uusi võtmeid ei looda.

6.2.4. HSMi häälestus

Protseduuri eesmärgiks on sättida HSM valmis võrgutööks. Selle käigus häälestatakse TCP/IP-protokoll ning kustutatakse varasemad NTLi kliendid. Protseduur eeldab, et serveriülem on HSMi sisse loginud.

HSMi häälestuses on lähtutud järgmisest:

- nimelahendust (DNS) ei kasutata. Seetõttu ei oma tähtsust ka seadme- ja domeeninime omistamine.

- SSH-ga ligipääsuks piiranguid ei seata (ligipääs kindlalt füüsiliselt võrguliideselt, kindlalt IP-aadressilt), kuna seade töötab kontrollitud, isoleeritud võrgus.

Samut peab silmas pidama, et NTLi võtmepaari loomise hetkeks tuleks HSM'i kell ühe päeva jagu tagasi keerata. Vastasel juhul võidakse luuakse võtmed, mille kehtivus algab HLR'i jaoks alles tund pärast nende loomist.

Kasutaja 'admin' salasõna loomise nõudeid vaata eelmisest punktist "Serveriülema sisselogimine".

Luuakse kasutaja 'admin' salasõna, uusi võtmeid ei looda.

6.2.5. Krüptomootori lähtestamine

Alamprotseduuri eesmärgiks on anda krüptomootorile edasiseks tööks vajalikud keskkonnaparameetrid. Selle käigus lähtestatakse krüptomootor, luuakse ja seotakse viimasega uued kasutajatunnused – punane, sinine ning N rohelist võtit. „Mitu-mitmest"-kasutamine tuleb määrata lähtestamisel, kusjuures silmas peab pidama, et M<N. Samuti määratakse krüptomootori märgis (ingl. k. „label"), mis on vajalik krüptomootori tuvastamiseks. Määramata jätta seda ei saa. Antud dokumendis on märgiseks valitud „VVK".

Muudetavad sätted määratakse protseduuriga „Krüptomootori häälestus"

Juhul kui vana HSM on riknenud / hävinud, tuleb uue HSMi lähtestamisel tingimata kasutada vana punast võtit.

Alamprotseduuris võetakse kasutusele hall, sinine, punane ja N rohelist võtit. Sinisele võtmele luuakse PIN. Ühtegi salasõna tarvis ei ole.

6.2.6. Turvaülema sisselogimine

Alamprotseduuri eesmärgiks on aktiveerida krüptomootor, mis on eelduseks selle sätete häälestamiseks ning partitsiooni loomiseks ja aktiveerimiseks.

Selle käigus läheb vaja sinist ning M rohelist võtit. Uusi salasõnu ja võtmeid protseduuri käigus ei looda.

6.2.7. Krüptomootori häälestus

Alamprotseduuri käigus häälestatakse krüptomootori muudetavaid sätteid. Ehkki krüptomootori lähtestamisel tema varem määratud muudetavad sätted jäävad samaks, ei tee paha neid üle kontrollida.

Tabel 2. E-valimiste lahenduses kasutatavad krüptomootori parameetrid

parameeter	väärtus e-hääleta-mise lahenduses	destruktiivne?	seletus
Allow cloning	On	+	See parameeter peab olema varundamiseks ja kõrgkäideldavuseks lubatud
Allow non-FIPS algorithms	Off	+	Kas FIPS 140-2'le mittevastavad algoritmid on lubatud. Kuna e-valimiste tarkvaras on kasutusel vaid FIPS 140-2 vasta-vad krüptoalgoritmid, on parameetri väärtus „Off"
Allow MofN auto-activation	Off	-	lubab puhverdada roheliste võtmete infot 3 tunniks juhuks, kui HSM vahepeal suletakse
SO can reset partition PIN	On	+	„On": pärast x järjesti-kust ebaõnnestunud sisselogimiskatset partitsiooni kasutaja lukustatakse ning HSMi admin saab partitsiooni kasutaja salasõna muuta. „Off": pärast x järjes-tikust ebaõnnestunud sisselogimiskatset kasutaja kustutatakse
Allow network replication	Off	-	Juhul, kui kasutatakse kõrgkäideldavust, peab olema „On"
Allow Remote Authentication	Off	+	Vajalik mitme sead-mega lahenduse korral, kui kasutatakse vaid ühte PEDi

Samuti tuleb arvestada, et destruktiivsete sätete muutmisel peab kogu süsteemi võtmepaari loomise protseduuri alustama otsast peale.

Krüptomootori häälestuse käigus uusi võtmeid ja salasõnu ei looda, selle täitmine eeldab turvaülema sisselogimist (protseduur „turvaülema sisselogimine")

6.2.8. Partitsiooni loomine ja häälestus

Alamprotseduuri eesmärgiks on luua e-hääletamiseks sobivate sätetega partitsioon. Sätted määravad, mida saab teha tema objektidega; sätteid saab muuta pärast partitsiooni loomist.

Partitsiooni lähtestamisel määratav märgis on vabalt valitav tähe- ja/või numbrijada. See on vajalik partitsiooni tuvastamiseks ning HLRi partitsiooniga sidumiseks. Antud dokumendis on märgiseks valitud „PART".

Tabel 3. Partitsiooni muudetavad sätted

säte	väärtus	seletus
Allow private key cloning	On	Peab olema lubatud, et saaks varundada privaatvõtit
Allow private key unwrapping	Off	
Allow secret key cloning	On	Vaikeväärtus; ei muudeta, kuna sümmeetrilist krüpteerimist ei kasutata
Allow secret key wrapping	Off	
Allow secret key unwrapping	Off	
Allow multipurpose keys	On	Kuna kasutatakse vaid üht võtmepaari, peab privaatvõtmel olema kaks ülesannet: krüpteerimine-dekrüpteerimine ning avaliku võtme signeerimine (isesigneeritud sertifikaat)
Allow changing key attributes	Off	Võtmetele antakse loomisel õiged ülesanded, hilisemat muutmist me ei luba.
Ignore failed challenge responses	On	Kas partitsiooni salasõna ebaõnnestunud kasutamine suurendab järjestikust ebaõnnestunud sisselogimiste arvu.

säte	väärtus	seletus
Operate without RSA blinding	On	Kuna ajastusrünnet („timing attack") HSMi privaatvõtme vastu korral-dada ei saa ning kuna selle parameetri keelamine vähendab HSMi jõudlust, RSA „pimestamist" ei kasutata („On")
Allow signing with non-local keys	Off	partitsiooniväliste võtme-tega signeerimine on keelatud
Allow raw RSA operations	On	
Max non-volatile storage space	5	
Max failed user logins allowed	10	
Allow high availability recovery	On	
Allow activation	On	Juhul kui aktiveerimine on lubatud, puhverdatakse PED-võtmete info. Puhver-datud info kustutatakse pärast alglaadimist. Peab olema (tõenäoliselt) sisse lülitatud, et iga hääle dekrüpteerimisel võtmeid ei küsitaks.
Allow auto-activation	Off	Võtmete info puhverda-takse HSMi kõvakettale nii, et aktiveerimisinfo säilib ka juhul kui HSM on < 3 tunni välja lülitatud.
Minimum pin length	248	
Maximum pin length	255	
Allow Key Management Functions	On	
Perform RSA signing without confirmation	On	
Allow Remote Authentication	Off	

Protseduuri käigus luuakse PINiga must võti ning partitsiooni salasõna. Viimane genereeritakse HSMi poolt ning väljastatakse PEDi ekraanile.

6.2.9. NTLi häälestus

Üheks eelduseks, et kasutada HSMi krüptograafilisi funktsioone, on HSMi ja HLRi vaheline krüpteeritud NTL-ühenduse loomine. Selle käigus genereeritakse HLRis NTLi võtmepaar (HSMi võtmepaar loodi alamprotseduuriga „HSMi häälestus"), seejärel vahetavad osapooled avalikke võtmeid ning registreerivad need. HLRi avaliku võtme registreerimisel tuleb HSMis anda vastava võtme omanikule/kliendile ka vabalt valitud tinglik nimi, milleks antud dokumendis on „HLR.

Uusi võtmeid ja salasõnu alamprotseduuri käigus ei looda. Protseduur eeldab, et süsteemiülem on HSMi loginud, kasutaja 'root' on loginud HLRi ning et HSM on lähtestatud.

6.2.10. Partitsiooni ja HLRi sidumine

Alamprotseduuri eesmärgiks on luua HLRile tegelik võimalus kasutada turvamooduli partitsiooni – luua, kasutada ja kustutada süsteemi võtmepaari ja sertifikaati. Selleks, et HLR teaks, millise serveri millise partitsiooni poole ta pöörduma peab, tuleb HLR siduda õige partitsiooniga.

Protseduuri täitmiseks piisab serveriülema kasutajaõigusest, ent eeldab partitsiooni olemasolu.

Uusi võtmeid ja salasõnu ei looda.

6.2.11. Partitsiooni aktiveerimine

Protseduuri eesmärgiks on muuta aktiivseks (st. kasutatavaks) partitsioon ühes oma objektidega. Selleks on vaja partitsiooni salasõna ning musta võtit.

6.2.12. Süsteemi võtmepaari ja sertifikaadi loomine

Alamprotseduuri eesmärgiks on luua süsteemi võtmepaar ning valijarakenduse jaoks isesigneeritud sertifikaat. Selle käigus genereeritakse süsteemi võtmepaar, millega tohib nii krüpteerida-dekrüpteerida kui ka signeerida-verifitseerida. Pärast võtmepaari loomist signeeritakse süsteemi avalik võti sama paari privaatvõtmega (luuakse isesigneeritud sertifikaat) ning tekkinud sertifikaat imporditakse HLRi failisüsteemi. Vaikimisi ei anta süsteemi privaat- ja avalikule võtmele ühtegi kasutusülesannet; (de)krüpteerimise ja signeerimise luba antakse võtmetele nende genereerimisel vastavate parameetritega.

Alamprotseduuriks on vaja teada partitsiooni salasõna.

Võtmepaari loomisel peab kummalegi võtmele andma tingliku nime. Eelkõige on see vajalik partitsioonil olevate objektide äratundmiseks, kuna partitsiooni objektid on nummerdatud ning ei ole teada, mis number antakse avalikule, mis number aga privaatvõtmele. Antud dokumendis on avalikule võtmele antud nimi ‚avalik' ning privaatvõtmele nimi ‚privaat'.

Süsteemi avaliku võtme signeerimisel sama paari privaatvõtmega genereeritakse X.509-formaadis sertifikaat. Kuna sertifitseeritud avalikku võtit kasutatakse vaid andmete krüpteerimiseks, antakse sertifikaadile laiend „dataencipherment".

Genereeritud sertifikaat imporditakse binaarkujul (DER-vormingus) HLR'i.

Alamprotseduur hõlmab ka süsteemi avaliku võtme ja sertifikaadi avaliku võtme mooduli võrdlust.

6.2.13. Partitsiooni varundamine

Alamprotseduuri eesmärgiks on luua süsteemi võtmepaarist varukoopia juhuks, kui see peaks HSMis hävima või muutub kasutuskõlbmatuks HSM ise. Varundamise käigus

1. lähtestatakse varundustoken
2. logitakse turvaülemana (sinine võti) varundustokenile
3. varundustokenile genereeritakse sama domeen, mis on krüptomootoris
4. varundustokenile luuakse partitsioon
5. objektide kloonimiseks logitakse veelkord varundustokenisse nii turva- kui partitsiooniülemana

Vajalikud on mõlemad sinised, punased, mustad võtmed ning M rohelist võtit ning partitsiooni salasõna. Protsessi käigus luuakse varundustokenile oma sinise, musta ja punase võtme komplekt. Sinise ja musta võtme puhul kasutatakse grupivõtit ning samu PIN-koode, mis põhipartitsiooni korral, punase võtmega kasutatakse sama domeeni, mis põhipartitsiooniga.

6.2.14. Partitsiooni deaktiveerimine ja HSMi seiskamine

Alamprotseduuri eesmärgiks on keelata turvaülema õigusi nõudvate protseduuride sooritamine. Selle käigus deaktiveeritakse partitsioon ning turvaülem logib HSMist välja. Protseduuriks vajalikke võtmed ei ole, ent eeldatavalt on turvaülem loginud HSMi ning partitsioon on aktiveeritud.

Lõpetuseks seisatakse HSM ning lõpetatakse minicom'i seanss.

6.2.15. Süsteemi privaatvõtme hävitamine

Alamprotseduuri eesmärk on hävitada süsteemi privaatvõti, välistamaks hilisemat häälte dekrüpteerimist. Hävitamine seisneb

1. HSMi partitsiooni kustutamises;
2. varundustokenil oleva teabe / objektide ülekirjutamises;
3. punaste võtmete (kloonimis)teabe kustutamises.