Vabariigi Valimiskomisjon

Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Tegevusjuhis

versioon 2.3

dokument: EHA-03-06-2.3
kuupäev: 24.04.2014

Muudatuste ajalugu

kuupäev	versioon	kirjeldus	autor
31.01.2007	1.0	Muudatuste arvestuse algus.	Uve Lokk
11.02.2007	1.1	Lisatud alamprotseduuride liigendus.	Tarvi Martens
22.04.2009	1.2	Täiendatud ja parandatud protseduuri "E-häälestamise võtmepaari loomine".	Uve Lokk
24.04.2009	1.3	Parandatud protseduuri "Häälte kokkulugemine"	Uve Lokk
16.09.2009	1.4	Läbivad parandused ja -täiendused, põhjalikumalt täiendatud protseduuri "Süsteemi võtmepaari taastamine partitsioonile".	Uve Lokk
20.01.2011	2.0	Suuremad muudatused, mis tingitud raudvaralise turvamooduli vahetusest. Keelelised ning terminoloogilised parandused.	Uve Lokk
02.02.2011	2.1	Üldosa ja tegevusjuhise alamprotseduuri numbrite ühitamine	Uve Lokk
20.09.2013	2.2	Lühendatud protseduuri „Häälte kokkulugemine“: eemaldatud tarbetud tegevused	Uve Lokk
24.04.2014	2.3	Veidi täpsustusi ja täiendusi	Uve Lokk

Sisukord

1.Protseduurid

käskude tähistused:

`minicom` - käsk, mis antakse HLR'i käsurealt

`par ac` - käsk, mis antakse HSM'i käsurealt

Enter - PED'i vahendusel edastatav sisend

1.1. E-hääletamise süsteemi võtmepaari loomine

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
HSMi käivitamine (6.2.1)				
1.1.1	kontrolli HSMi külgedel olevaid turvakleebiseid	-		
1.1.2	ühenda PED HSMiga.	-		
1.1.3	ühenda HLR ja HSM omavahel jadakaabliga.	-		
1.1.4	ühenda HLRi võrguliides ja HSMi 1. (vasakpoolne) võrguliides võrgukaabliga	-		
1.1.5	ühenda HSM vooluvõrku, käivita see.	-		
HLRi käivitamine ja häälestus (6.2.2)				

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.6	ühenda printer HLR'iga ning käivita need			
1.1.7	logi HLR'i lokaalse administraatorina			
1.1.8	säti vajadusel õigeks HLRi kell. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`date KKPPTTMMAAAA`	teatab ekraanil õige kellaaja ja kuupäeva	

1.1.9	kontrolli, kas minicom on häälestatud korrektselt	`cat /etc/minicom/minirc.dfl`	`pr port /dev/ttyS0`
			`pu baudrate 115200`
			`pu bits 8`
			`pu parity N`
			`pu stopbits 1`
			Jätka punktiga 1.1.11
				häälestusfail ei ole korras

1.1.10	häälesta minicom	`vim /etc/minicom/minirc.dfl`	fail ‚minirc.dfl' vastab punktis 1.1.8 toodule	
1.1.11	kontrolli, kas võrguliides on häälestatud korrektselt	`cat /etc/network/interfaces`	vastab punktile 2.1; jätka punktiga 1.1.14	väljund ei ole korras, jätka järgmise punktiga
1.1.12	muuda võrguliidese häälestust	`vim /etc/network/interfaces`	fail ‚interfaces' vastab punktile 2.1	
1.1.13	taaskäivita HLRi võrguteenus	`/etc/init.d/networking restart`		

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.14	kustuta HLRi nimelahendusteave	`cat /dev/null > /etc/resolv.conf`		
Serveriülema sisselogimine (6.2.3)				
1.1.15	käivita minicom	`minicom`		
1.1.16	logi HSMi kasutajana ‚admin'. Juhul, kui salasõnaks ei ole ‚Riigikogu2004', tuleb püüda 3 korda vale salasõnaga sisse logida, misjärel salasõna lähtestatakse (‚chrysalis') ning seda on võimalik muuta			
HSMi häälestus (6.2.4)				
1.1.17	roteeri HSMi süsteemi logi	`sysl rotate`		
1.1.18	säti HSMi ajavööndiks Europe/Tallinn	`sysc timez se Europe/Tallinn`	teade ekraanil: "Timezone set to Europe/Tallinn. Command Result : 0 (Success)"	
1.1.19	säti õigeks HSMi kellaaeg. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahe-kohalise arvuna, PP - päev kahekohalise arvuna	`sysc t TT:MM AAAAKKPP`	teatab ekraanil õige kellaaja ja kuupäeva	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.20	vaheta kasutaja ‚admin' salasõna. Salasõna vahetatakse juhul, kui varem kehtis vaikesalasõna	`use p admin`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.21	logi kasutaja ‚admin' välja, testimaks uut salasõna	`exit`		
1.1.22	logi kasutaja ‚admin' uuesti sisse			
1.1.23	kustuta HSMi esimese võrguliidese TCP/IP protokolli konfiguratsioon	`ne i del -d eth0`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.24	kustuta HSMi teise võrguliidese TCP/IP protokolli konfiguratsioon	`ne i del -d eth1`		
1.1.25	muuda HSMi võrguliidese ip-aadress ja netmask.	`ne i -dev eth0 -i 10.0.0.3 \` `-n 255.255.255.0 -f`	teade ekraanil „Command Result : 0 (Success)"	
1.1.26	kontrolli, kas võrguliides sai häälestatud nii nagu vaja	`ne sh`	kuvatakse korrektsed võrguliidese parameetrid	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.27	keera HSMi kell 1 päeva jagu tagasi. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`sysc t TT:MM AAAAKKPP`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.28	genereeri uus seadme NTLi võtmepaar.	`sysc reg 10.0.0.3`	palutakse sisestada ‚proceed'	
1.1.29	kirjuta ‚proceed'	`proceed`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.30	taaskäivita NTLS-teenus	`se r ntls`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.31	kontrolli, et NTLS oleks õige võrguliidesega seotud	`ntls s`	teade ekraanil: "NTLS bound to network device: eth0 IP Address: "10.0.0.3" (eth0) Command Result : 0 (Success)"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.32	keera HSMi kell tagasi õigeks. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`sysc t TT:MM AAAAKKPP`	teade ekraanil: "Command Result : 0 (Success)"	
1.1.33	kontrolli HLRi võrguühendust HSMiga	`ping -c 3 10.0.0.3`	pingib	ei pingi
1.1.34	kontrolli HSMi võrguühendust HLRiga	`ne p 10.0.0.2`	pingib	ei pingi
1.1.35	kontrolli, kas HSMis on registreeritud kliente	`cl l`	kliente ei ole, jätka punktiga 1.1.37	kliente on (ekraanil teade: „registered client 1: [kliendi_nimi]”)
1.1.36	kustuta registreeritud kliendid	`cl d -f -c [kliendi_nimi]`	teade ekraanil: "'client delete' successful"	
Krüptomootori lähtestamine (6.2.5)				
1.1.37	vii HSM tehasehäälestusse	`hs fa`	palutakse sisestada kinnituseks 'proceed'	
1.1.38	Kirjuta 'proceed'	`proceed`	Teade ekraanil: "Command Result : 0 (Success)"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.39	lähtesta HSM. [M] ja [N] on MofN'i komponendid. N - Vabariigi Valimiskomisjoni (VVK) liikmete arv, M - otsuseks vajalik VVK liikmete arv	`hs ini -f -l VVK -mo -mv [M] \ -n [N]`	PED: "Insert a SO / HSM Admin PED Key""	
1.1.40	kasuta esimest sinist võtit	Enter	PED: "This PED Key has a valid Identity for SO / HSM Admin. Reuse Id?"	
1.1.41	vajuta PEDil nuppu 'No'	No	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.42	vajuta PEDil nuppu 'Yes'	Yes	PED: "Enter new PED PIN"	
1.1.43	sisesta PIN	****	PED: "Copy this PED Key?"	
1.1.44	vajuta PEDil nuppu 'Yes'	Yes	PED: "Insert target PED Key."	
1.1.45	kasuta teist sinist võtit	Enter	PED: "This PED Key is for SO / HSM Admin. Overwrite?"	
1.1.46	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.47	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?"	
1.1.48	vajuta PEDil nuppu 'No'	No	PED: "insert a SO / HSM Admin PED Key"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.49	kasuta sinist võtit	Enter	PED: "Enter PED PIN"	
1.1.50	sisesta PIN	****	PED: "Insert a Domain PED Key"	
1.1.51	kasuta esimest punast võtit	Enter	PED: "This PED Key has a valid Identity for Domain. Reuse Id?"	
1.1.52	vajuta PEDil nuppu 'No'	No	Are you sure you want to overwrite this PED Key?"	
1.1.53	vajuta PEDil nuppu 'Yes'	Yes	PED: "Copy this PED Key?"	
1.1.54	vajuta PEDil nuppu 'Yes'	Yes	PED: "Insert target PED Key"	
1.1.55	kasuta teist punast võtit	Enter	PED: "This PED Key is for Domain. Overwrite?"	
1.1.56	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.57	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?"	
1.1.58	vajuta PEDil nuppu 'No'	No	PED: "Insert 1st M of N PED Key"	
1.1.59	kasuta rohelist võtit	Enter	PED: "This PED Key is for M of N. Overwrite?	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.60	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.61	vajuta PEDil nuppu 'Yes'	Yes	Palutakse sisestada järgmine roheline võti	
1.1.62	tegevusi 1.1.59 - 1.1.61 tuleb korrata kokku M korda		Teade ekraanil "'hsm init' successful. /---/ Command Result : 0 (Success)"	
Turvaülema sisselogimine (6.2.6)				
1.1.63	logi turvaülem sisse	`hs logi`	PED: "Insert a SO / HSM Admin PED Key"	
1.1.64	kasuta sinist võtit	Enter	PED: „ Enter PED PIN”	
1.1.65	sisesta sinise võtme PIN	****	PED: „Insert 1st M of N PED Key”	
1.1.66	kasuta M rohelist võtit	Enter	Teade ekraanil: "'hsm login' successful. /---/ Command Result : 0 (Success)"	
Krüptomootori häälestus (6.2.7)				
1.1.67	kontrolli HSMi sätteid	`hs showP`	kõik on nii nagu punktis 2.2, jätka protseduuriga 1.1.70	jätka järgmise punktiga

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.68	muuda HSMi sätet. Sätte kood "Kood"on käsu hs showP väljundi veerus ‚Code', X'i väärtus: 1=lubatud, 0=keelatud	`hs changePo -p Kood \ -v X`	teade „'hsm changePolicy' successful"	teade „'hsm changePolicy' failed"
1.1.69	kontrolli HSMi sätteid	`hs showP`	kõik on nii nagu punktis 2.2	kõik ei ole nii nagu punktis 2.2; tagasi punkti 1.1.68
Partitsiooni loomine ja häälestus (6.2.8)				
1.1.70	loo partitsioon	`par cr -f -par PART`	PED: „Insert a User / Partition Owner PED Key."	
1.1.71	kasuta esimest musta võtit	Enter	PED: "This PED Key has valid Identity for User / PartitionOwner Reuse Id?"	
1.1.72	vajuta PEDil nuppu 'No'	No	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.73	vajuta PEDil nuppu 'Yes'	Yes	PED: "Enter new PED PIN:"	
1.1.74	loo musta võtme PIN	****	PED: "Copy this PED Key?"	
1.1.75	vajuta PEDil nuppu 'Yes'	Yes	PED: "Insert target PED Key."	
1.1.76	kasuta teist musta võtit	Enter	PED: "This PED Key is for USER/PartitionOwner. Overwrite?"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.77	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.78	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?"	
1.1.79	vajuta PEDil nuppu 'No'	No	PED kuvab partitsiooni salasõna, vormingus '****-****-****-****'. Pane see kirja.	
1.1.80	vajuta PEDil nuppu 'Enter'	Enter	Teade ekraanil: "'partition create' successful. Command Result : 0 (Success)"	
1.1.81	kontrolli, kas partitsioon loodi	`par l`	kuvatakse partitsiooni number ja nimi	
1.1.82	keela privaatvõtme ‚lahti-mähkimine'	`par changePo -pa PART -po 2 \ -v 0`	teade ekraanil: „Policy „Allow private key unwrapping" is now set to: 0"	
1.1.83	keela võtme atribuutide muutmine	`par changePo -pa PART -po 11 \ -v 0`	teade ekraanil: „Policy „Allow changing key attributes" is now set to: 0"	
1.1.84	keela väliste võtmetega signeerimine	`par changePo -pa PART -po 17 \ -v 0`	teade ekraanil: „Policy „Allow signing with non-local keys" is now set to: 0"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.85	luba partitsiooni aktiveerimine	`par changePo -pa PART -po 22 \ -v 1`	teade ekraanil: „Policy „Allow activation” is now set to: 1”	
1.1.86	keela partitsiooni automaatne aktiveerimine	`par changePo -pa PART -po 23 \ -v 0`	teade ekraanil: „Policy „Allow auto-activation” is now set to: 0”	
1.1.87	keela kaugautentimine	`par changePo -pa PART -po 30 \ -v 0`	teade ekraanil: „Policy „Allow Remote Authentication” is now set to: 0”	
NTLi häälestus (6.2.9)				
1.1.88	mine kataloogi /usr/lunasa/cert	`cd /usr/lunasa/cert`		
1.1.89	Impordi HSMi NTLi avalik võti HLRi. HLR võib teatada, et ta pöördub tundmatu HSMi poole. Impordi ajal küsitakse serveriülema salasõna.	`ctp admin@10.0.0.3:server.pem .`	kataloogi tekib fail ‚server.pem’	
1.1.90	registreeri HSMi NTLi avalik võti	`vtl addServer –n 10.0.0.3 \ –c server.pem`	teade „New server 10.0.0.3 successfully added to server list.”	
1.1.91	loo HLRi NTLi võtmepaar	`vtl createCert –n 10.0.0.2`	teade, et loodi privaatvõti & sertifikaat ning tuuakse ära nende asukohad	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.92	ekspordi HLRi NTLi avalik võti HSMi. Ekspordi ajal küsitakse serveriülema salasõna.	`ctp client/10.0.0.2.pem \` `admin@10.0.0.3:`	protsessi käigus küsitakse HSMi admin'i salasõna. Kui see on õige, kuvatakse laadimisprotsessi	
1.1.93	registreeri HSMis HLRi NTLi avalik võti	`cl reg -c HLR -i 10.0.0.2`	ekraanil teade: „'client register' successful'."	
Partitsiooni ja HLRi sidumine (6.2.10)				
1.1.94	seo HLR partitsiooniga	`cl a -c HLR -p PART`	teade „'client assignPartition' successful."	
1.1.95	kontrolli, kas HLR seoti partitsiooniga	`cl s -c HLR`	väljund: ClientID: HLR IPAddress: 10.0.0.2 Partitions: „PART"	
1.1.96	kontrolli HLRis, kas partitsiooni sidumine õnnestus	`vtl verify`	teade, kus on märgitud HSMi seerianumber ja partitsiooni nimi 'PART'.	
Partitsiooni aktiveerimine (6.2.11)				
1.1.97	aktiveeri partitsioon	`par ac -par PART`	teade ekraanil: "Please enter the password for the partition"	
1.1.98	sisesta partitsiooni salasõna	`****-****-****-****`	PED: „Insert a USER / Partition Owner PED Key:"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.99	kasuta musta võtit		PED: „Enter PED PIN:"	
1.1.100	sisesta PIN	****	ekraan: „'partition activate' successful"	
Süsteemi võtmepaari ja sertifikaadi loomine (6.2.12)				

1.1.101	genereeri võtmepaar, kusjuures AAAA on aasta, KK-kuu number kahekohalise arvuna, PP - päeva number kahekohalise arvuna; startdate - võtmepaari genereerimise kuupäev, enddate - viimasele valimistulemuste kinnitamise päevale järgnev päev
	Võtmepaari genereerimisel küsitakse partitsiooni salasõna
		`cmu gen –modulusbits=2048 \`
		`-publicexponent=65537 \`
		`-encrypt=1 -decrypt=1 \`
		`-sign=1 -verify=1 \`
		`-startdate=AAAAKKPP \`
		`-enddate=AAAAKKPP \`
		`-labelpublic=avalik \`
		`-labelprivate=privaat`
			tagasisidet ei ole, partitsioonile tekitatakse kaks objekti - privaat- ja avalik võti	„Failure to login to HSM" - vale partitsiooni salasõna
				„Unknown option encountered" - vigane käsk, kontrolli käsu vastavust juhisele

1.1.102	kontrolli, kas võtmepaar loodi. Kontrolli käigus küsitakse partitsiooni salasõna	`cmu list`	teade „handle=[pub_nr] label=avalik, handle=[priv_nr] label=privaat"	„Failure to login to HSM" - vale partitsiooni salasõna

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel

1.1.103	Genereeri avalikust võtmest autoallkirjastatud sertifikaat, kusjuures AAAA on aasta, KK-kuu number kahekohalise arvuna, PP - päeva number kahekohalise arvuna; startdate - võtmepaari genereerimise kuupäev, enddate - viimasele valimistulemuste kinnitamise päevale järgnev päev.
	Genereerimise käigus küsitakse partitsiooni salasõna
		`cmu selfsign \`
		`-publichandle=[pub_nr] \`
		`-privatehandle=[priv_nr] \`
		`-startdate=AAAAKKPP \`
		`-enddate=AAAAKKPP \`
		`-serialNumber=1 -C=EE \`
		`-O=”Vabariigi Valimiskomisjon” \`
		`-CN=VVK \`
		`-keyusage=dataencipherment`
			tagasisidet ei ole, partitsioonile tekitatakse objekt, nimega VVK (vt. ka järgmine punkt)	„Failure to login to HSM” - vale partitsiooni salasõna
				„Unknown option encountered” - vigane käsk, kontrolli käsu vastavust juhisele

1.1.104	kontrolli, kas sertifikaat loodi Kontrolli käigus küsitakse partitsiooni salasõna.	`cmu list`	teade „handle=[sert_nr] label=VVK, handle=[pub_nr] label=avalik, handle=[priv_nr] label=privaat”	

1.1.105	ekspordi sertifikaat binaarkujul HSMist klienti.
	Ekspordi käigus küsitakse partitsiooni salasõna
		`cmu export -binary \`
		`-handle=[sert_nr] \`
		`-output=/usr/lunasa/cert/vvk.der`
			tagasisidet ei ole, kataloogi tekib fail vvk.der	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel

1.1.106	kontrolli HSMis oleva avalikku võtme moodulit.
	Pärast käsu andmist tuleb tühjale ekraanile sisestada partitsiooni salasõna, ekraanil selle küsimisest ei teatata.
		`cmu getAttribute \`
		`-handle=[pub_nr] \`
		`-attribute=modulus | \`
		`sed –r 's/(.{72})/\1\r\n/g' | \`
		`tr [a-f] [A-F] | unix2dos | lpr`
			printer trükib välja HSMis oleva avaliku võtme mooduli	

1.1.107	tähista HSMi avaliku võtme mooduli väljatrükk			

1.1.108	kontrolli HLRi eksporditud sertifikaadis olevat avalikku võtme moodulit.	`openssl x509 -inform DER \`
		`-in vvk.der -text -modulus |  \`
		`grep Modulus\= | \`
		`sed –r 's/(.{72})/\1\r\n/g' | \`
		`unix2dos | lpr`
			printer trükib välja sertifikaadis oleva avaliku võtme mooduli	

1.1.109	tähista sertifikaadis oleva avaliku võtme mooduli väljatrükk			
1.1.110	võrdle kaht väljatrükki		väljatrükitud moodulid on identsed	
1.1.111	märgista tühi DVD-toorik ning sisesta see HLRi DVD-seadmesse			
1.1.112	kopeeri sertifikaat märgistatud DVD-plaadile	`growisofs -Z /dev/dvd -R -J \` `/usr/lunasa/cert/vvk.der`	sertifikaat kopeeriti DVD-plaadile	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
Partitsiooni varundamine (6.2.13)				
1.1.113	Sisesta varunduskaart ükskõik kumba seadme esipaneelil olevast kahest kaardipesast			
1.1.114	Kontrolli, kas varunduskaart on korrektselt sisestatud	`t s`	ekraanil teatatakse selle pesa number, kus varunduskaart asub ning viimase nimi, seerianumber ja püsivara versioon.	
1.1.115	nulli varunduskaart	`t f`	Käsk palutakse kinnitada sõnaga "proceed"	
1.1.116	kirjuta "proceed"	`proceed`	teade ekraanil: "'token factoryReset' successful"	
1.1.117	anna varunduskäsk	`par b -f -par PART`	teade ekraanil: „Please enter the password for the partition”	
1.1.118	sisesta partitsiooni salasõna	`****-****-****-****`	PED: "Insert a SO / HSM Admin PED Key"	
1.1.119	kasuta esimest sinist võtit		PED: "This PED key has a valid identity for SO / HSM Admin. Reuse Id?"	
1.1.120	vajuta PEDil nuppu 'Yes'	Yes	PED: "Enter new PED PIN"	
1.1.121	sisesta sinise võtme PIN	****	PED: "Confirm new PED PIN"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.122	kinnita sinise võtme PIN	****	PED: "Copy this PED key?"	
1.1.123	vajuta PEDil nuppu 'Yes'	Yes	PED: "Insert target PED Key."	
1.1.124	kasuta teist sinist võtit	Enter	PED: "This PED Key is for SO / HSM Admin. Overwrite?"	
1.1.125	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.126	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?"	
1.1.127	vajuta PEDil nuppu 'No'	No	PED: "Insert a SO / HSM Admin PED Key"	
1.1.128	kasuta sinist võtit	Enter	PED: "Enter PED PIN"	
1.1.129	sisesta sinise võtme PIN	****	PED: "Insert a Domain PED Key. Press ENTER"	
1.1.130	kasuta punast võtit	Enter	PED: "This PED Key has a valid Identity for Domain. Reuse Id?"	
1.1.131	vajuta PEDil nuppu 'Yes'	Yes	PED: "Copy this PED Key?"	
1.1.132	vajuta PEDil nuppu 'No'	No	PED: "Another copy of this PED Key?"	
1.1.133	vajuta PEDil nuppu 'No'	No	PED: "Insert a USER / PartitionOwner PED Key."	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.134	kasuta esimest musta võtit	Enter	PED: "This PED Key has valid identity for User / PartitionOwner. Reuse Id?"	
1.1.135	vajuta PEDil nuppu 'Yes'	Yes	PED: "Enter new PED PIN"	
1.1.136	sisesta musta võtme PIN	****	PED: "Confirm new PED PIN"	
1.1.137	kinnita musta võtme PIN	****	PED: "Copy this PED Key?"	
1.1.138	vajuta PEDil nuppu 'Yes'	Yes	PED: "Insert target PED Key."	
1.1.139	kasuta teist musta võtit	Enter	PED: "This PED Key is for USER / PartitionOwner. Overwrite?"	
1.1.140	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.1.141	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?"	
1.1.142	vajuta PEDil nuppu 'No'	No	PED: "Insert a SO / HSM Admin PED Key."	
1.1.143	kasuta sinist võtit	Enter	PED: "Enter PED PIN"	
1.1.144	sisesta sinise võtme PIN	****	PED: "Insert 1st of MofN PED Key."	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.145	kasuta M rohelist võtit	Enter	Iga õnnestunud kasutamise järel palub PED sisestada järgmise rohelise võtme. Kui vajalik arv võtmeid on kasuta-tud, teatab PED: "Insert a USER / Partition Owner PED Key"	
1.1.146	kasuta musta võtit	Enter	PED: "Enter PED PIN"	
1.1.147	sisesta musta võtme PIN	****	Ekraanil teade kolme objekti ("VVK", "avalik", "privaat") kloonimisest	
1.1.148	kontrolli varunduskaardi sisu	t showC	PED: "Insert a User / Partition Owner PED Key"	
1.1.149	kasuta musta võtit	****	Ekraanil kuvatakse varunduskaardi andmed ning varunduskaardil oleva kolme objekti nimi ja tüüp	
1.1.150	eemalda varunduskaart HSMist.			
Partitsiooni deaktiveerimine ning HSMi ja HLRi seiskamine (6.2.14)				
1.1.151	partitsiooni deaktiveerimine	par dea -p PART	Teade ekraanil: "'partition deactivate' successful /---/ Command Result : 0 (Success)"	teade ekraanil: „Error: 'partition deactivate' failed"

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.1.152	turvaülema väljalogimine	`hs logo`	Teade ekraanil: "'hsm logout' successful. /---/ Command Result : 0 (Success)"	
1.1.153	seiska HSM	`sysc a p`	Seiskamise kinnituseks palutakse sisestada ‚proceed'	
1.1.154	kirjuta ‚proceed'	`proceed`	HSM seiskub	
1.1.155	sule minicom: vajuta järgemööda klaviatuurklahve Ctrl+a, z, x, ‚Enter'		ekraanil HLRi käsurida	
1.1.156	seiska HLR	`halt -p`	HLR seiskub	

1.2. Häälte kokkulugemine

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
HSMi käivitamine (6.2.1)				
1.2.1	kontrolli HSMi külgedel olevaid turvakleebiseid			
1.2.2	ühenda PED HSMiga.	-		
1.2.3	ühenda HLR ja HSM omavahel jadakaabliga.	-		
1.2.4	ühenda HLRi võrguliides ja HSMi 1. (vasakpoolne) võrguliides võrgukaabliga			
1.2.5	ühenda HSM vooluvõrku, käivita see			
HLRi käivitamine ja häälestus (6.2.2)				
1.2.6	käivita HLR			
1.2.7	logi HLR'i lokaalse administraatorina	root, *********		

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.2.8	säti vajadusel õigeks HLRi kell. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahe-kohalise arvuna, PP - päev kahe-kohalise arvuna	`date KKPPTTMMAAAA`	teatab ekraanil õige kellaaja ja kuupäeva	

1.2.9	kontrolli, kas minicom on häälestatud korrektselt	`cat /etc/minicom/minirc.dfl`	`pr port /dev/ttyS0`
			`pu baudrate 115200`
			`pu bits 8`
			`pu parity N`
			`pu stopbits 1`
			Jätka punktiga 1.2.11
				häälestusfail ei ole korras

1.2.10	häälesta minicom	`vim /etc/minicom/minirc.dfl`		
Serveriülema sisselogimine (6.2.3)				
1.2.11	käivita minicom	`minicom`	5 sekundi pärast ekraanil teade: „Welcome to minicom”	
1.2.12	logi HSMi kasutajana ‚admin’. Kasuta varem määratud salasõna			
1.2.13	säti õigeks HSMi kellaaeg. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahe-kohalise arvuna, PP - päev kahe-kohalise arvuna	`sysc t TT:MM AAAAKKPP`	teatab ekraanil õige kellaaja ja kuupäeva	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
NTLi häälestus (6.2.9)				
1.2.14	kontrolli HLRis, kas kliendi-serveri-vaheline turvaühendus töötab	`vtl verify`	teade, kus on märgitud HSMi seerianumber ja partitsiooni nimi. Partitsiooni nimi peab olema õige. Jätka punktiga 1.2.29	Veateade. Jätka järgmise punktiga
1.2.15	mine kataloogi /usr/lunasa/cert	`cd /usr/lunasa/cert`		

1.2.16	kustuta vanad sertifikaadid	`rm server.pem`
		`rm client/*`
		`rm server/*`		

1.2.17	Impordi HSMi NTLi avalik võti HLRi. HLR võib teatada, et ta pöördub tundmatu serveri poole. Impordi ajal küsitakse serveri-ülema salasõna.	`ctp admin@10.0.0.3:server.pem .`	kataloogi tekib fail ‚server.pem'	
1.2.18	registreeri HSMi NTLi avalik võti	`vtl addServer -n 10.0.0.3 \` `-c server.pem`	teade „New server 10.0.0.3 successfully added to server list."	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.2.19	keera HLRi tarkvara kellaaeg ühe päeva võrra tagasi. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`date KKPPTTMMAAAA`	teatab ekraanil „õige” kellaaja ja kuupäeva	
1.2.20	loo HLRi NTLi võtmepaar	`vtl createCert –n 10.0.0.2`	teade, et loodi privaatvõti & sertifikaat ning tuuakse ära nende asukohad	
1.2.21	keera HLRi tarkvara kellaaeg tagasi õigeks. TT - tund kahe-kohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`date KKPPTTMMAAAA`	teatab ekraanil õige kellaaja ja kuupäeva	
1.2.22	ekspordi HLRi NTLi avalik võti HSMi. Ekspordi ajal küsitakse serveriülema salasõna.	`ctp client/10.0.0.2.pem \` `admin@10.0.0.3:`	protsessi käigus küsitakse HSMi admin’i salasõna. Kui see on õige, kuva-takse laadimisprotsessi	
1.2.23	kontrolli, kas HSMis on registreeritud kliente	`cl l`	kliente ei ole, jätka punktiga 1.2.25	kliente on (ekraanil teade: „registered client 1: [kliendi_nimi]”)

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.2.24	kustuta registreeritud kliendid	`cl d -f -c [kliendi_nimi]`	teade ekraanil „'client delete' successful"	
1.2.25	registreeri HSMis HLRi avalik võti	`cl reg –c HLR –i 10.0.0.2`	ekraanil teade: „'client register' successful'."	
1.2.26	seo HLR partitsiooniga	`cl a -c HLR -p PART`	teade „'client assignPartition' successful."	
1.2.27	kontrolli, kas HLR seoti partit-siooniga	`cl s -c HLR`	väljund: ClientID: HLR IPAddress: 10.0.0.2 Partitions: „PART"	
1.2.28	kontrolli HLRis, kas partitsiooni sidumine õnnestus	`vtl verify`	teade, kus on märgitud HSMi seerianumber ja partitsiooni nimi. Partitsi-ooni nimi peab olema õige	
Partitsiooni aktiveerimine (6.2.11)				
1.2.29	aktiveeri partitsioon	`par ac -par PART`	terminal. "Please enter the password for the partition"	
1.2.30	sisesta partitsiooni salasõna	`****-****-****-****`	PED: „Insert a USER / Partition Owner PED Key. Press ENTER"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.2.31	kasuta musta võtit	Enter	PED: „Enter PED PIN:"	
1.2.32	sisesta musta võtme PIN	****	PED: „insert 1st of MofN PED Key. Press ENTER"	
	kasuta M rohelist võtit.		Iga õnnestunud kasutamise järel palub PED sisestada järgmise rohelise võtme. Kui vajalik arv võtmeid on kasutatud, teatab terminal: „ ‚hsm login' successful." terminal: „'partition activate' successful"	
Häälte kokkulugemine				
1.2.33	Vt. EHA-03-03-* „Süsteemiülema juhend" punkt 6.2			
Partitsiooni deaktiveerimine ja HSMi seiskamine (6.2.14)				
1.2.34	partitsiooni deaktiveerimine	`par dea -p PART`	teade ekraanil „'partition deactivate' successful"	teade ekraanil: „Error: 'partition deactivate' failed"
1.2.35	seiska HSM	`sysc a p`		
1.2.36	sulge minicom: vajuta järgemööda klaviatuurklahve Ctrl+a, z, x, ‚Enter'		ekraanil HLRi käsurida	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.2.37	sulge HLR	`halt -p`		

1.3. Süsteemi võtmepaari taastamine

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
HSMi käivitamine (6.2.1)				
1.3.1	kontrolli HSMi külgedel olevaid turvakleebiseid	-		
1.3.2	ühenda PED HSMiga	-		
1.3.3	ühenda HLR ja HSM omavahel jadakaabliga.	-		
1.3.4	käivita HSM			
1.3.5	ühenda HLRi võrguliides ja HSMi 1. (vasakpoolne) võrguliides rist-võrgukaabliga			
HLRi käivitamine (6.2.2)				
1.3.6	käivita HLR ning logi sisse lokaalse administraatorina			
1.3.7	säti vajadusel õigeks HLRi kell. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`date KKPPTTMMAAAA`	teatab ekraanil õige kellaaja ja kuupäeva	
Serveriülema sisselogimine (6.2.3)				

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.8	käivita minicom	`minicom`	5 sekundi pärast ekraanil teade: „Welcome to minicom”	
1.3.9	logi seadmesse kasutajana ‚admin’. Juhul, kui salasõnaks ei ole teada, püüa 3 korda vale salasõnaga sisse logida, misjärel salasõna lähtestatakse (‚chrysalis’) ning seda on võimalik muuta			
HSMi häälestus (6.2.4)				
1.3.10	roteeri HSMi süsteemi logi	`sysl rotate`		
1.3.11	säti HSMi ajavööndiks Europe/Tallinn	`sysc timez se Europe/Tallinn`	teade „Timezone set to Europe/Tallinn”	teade „Error: The specified timezone is invalid”
1.3.12	säti õigeks HSMi kellaaeg. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahekohalise arvuna, PP - päev kahekohalise arvuna	`sysc t TT:MM AAAAKKPP`	teatab ekraanil õige kellaaja ja kuupäeva	
1.3.13	vaheta kasutaja ‚admin’ salasõna. Salasõna vahetatakse juhul, kui varem kehtis vaikesalasõna	`use p admin`	teade ekraanil „passwd: allauthentication tokens updsated successfully”	
1.3.14	logi kasutaja ‚admin’ välja	`exit`		

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.15	logi kasutaja ‚admin' uuesti sisse			
1.3.16	kustuta HSMi esimese võrguliidese TCP/IP protokolli konfiguratsioon	`ne i del -d eth0`	teade ekraanil „Interface eth0 removed successfully"	
1.3.17	kustuta HSMi teise võrguliidese TCP/IP protokolli konfiguratsioon	`ne i del -d eth1`		
1.3.18	muuda HSMi võrguliidese ip-aadress ja netmask.	`ne i s -d eth0 -i 10.0.0.4 \` `-n 255.255.255.0 -f`	teade ekraanil „Command Result : 0 (Success)"	
1.3.19	kontrolli, kas võrguliides sai häälestatud nii nagu vaja	`ne sh`	kuvatakse korrektsed võrguliidese parameetrid	
1.3.20	keera HSMi kell 1 päeva jagu tagasi. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahe-kohalise arvuna, PP - päev kahe-kohalise arvuna	`sysc t TT:MM AAAAKKPP`	teatab ekraanil kellaaja ja kuupäeva	
1.3.21	genereeri uus seadme NTLi võtmepaar.	`sysc reg 10.0.0.4`	jätkamiseks palutakse sisestada ‚proceed'	
1.3.22	kirjuta ‚proceed'	`proceed`	teade ekraanil „'sysconf regenCert' successful"	
1.3.23	taaskäivita NTL-teenus	`se r ntls`		

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.24	keera HSMi kell tagasi õigeks. TT - tund kahekohalise arvuna, MM - minut kahekohalise arvuna, AAAA - aasta, KK - kuu kahe-kohalise arvuna, PP - päev kahe-kohalise arvuna	`sysc t TT:MM AAAAKKPP`	teatab ekraanil õige kellaaja ja kuupäeva	
1.3.25	ühenda arvutivõrgu ristkaabli üks ots HLRi võrguliidesega, teine ots HSMi ülemise (tähistatud „1”-ga) võrguliidesega			
1.3.26	kontrolli HLRi võrguühendust HSMiga	`ping -c 3 10.0.0.4`	pingib	ei pingi
1.3.27	kontrolli HSMi võrguühendust HLRiga	`ne p 10.0.0.2`	pingib	ei pingi
1.3.28	kontrolli, kas HSMis on registreeritud kliente	`cl l`	kliente ei ole, jätka punktiga 1.3.30	kliente on (ekraanil teade: „registered client 1: [kliendi_nimi]”)
1.3.29	kustuta registreeritud kliendid	`cl d -f -c [kliendi_nimi]`	teade ekraanil „’client delete’ successful”	
Krüptomootori lähtestamine (6.2.5)				

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.30	vii HSM tehasehäälestusse	`hs fa`	"The remote PED vector (RPV) has been erased on HSM. Command Result : 0 (Success)"	
1.3.31	lähtesta HSM. [M] ja [N] on MofN'i komponendid. N - Vabariigi Valimiskomisjoni (VVK) liikmete arv, M - otsuseks vajalik VVK liikmete arv	`hs ini -f -l VVK -mo -mv [M] \` `-n [N]`	PED: „insert a SO / HSM Admin PED Key"	
1.3.32	kasuta uut esimest sinist võtit	Enter	PED: „This PED Key has a valid Identity for SO / HSM Admin. Reuse Id?"	
1.3.33	vajuta PEDil nuppu 'No'	No	PED: "Are you sure you want to overwrite this PED Key?"	
1.3.34	vajuta PEDil nuppu 'Yes'	Yes	PED: "Enter new PED PIN"	
1.3.35	sisesta PIN	*****	PED: "Copy this PED Key?"	
1.3.36	vajuta PEDil nuppu "Yes"	Yes	PED: "Insert target PED Key"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.37	kasuta teist uut sinist võtit	Enter	PED: "This PED Key is for SO / HSM Admin. Overwrite?"	
1.3.38	vajuta PEDil nuppu 'Yes'	Yes	PED: "Are you sure you want to overwrite this PED Key"	
1.3.39	vajuta PEDil nuppu 'Yes'	Yes	PED: "Another copy of this PED Key?""	
1.3.40	vajuta PEDil nuppu 'No'	No	PED: "insert a SO / HSM Admin PED Key"	
1.3.41	kasuta uut sinist võtit	Enter	PED: "Enter PED PIN"	
1.3.42	sisesta PIN	*****	PED: "Insert a Domain PED Key. Pess ENTER"	
1.3.43	kasuta vana punast võtit	Enter	PED: "This PED Key has a valid Identity for Domain. Reuse Id?"	
1.3.44	vajuta PEDil nuppu 'Yes'	Yes	PED: "Copy this PED Key?"	
1.3.45	vajuta PEDil nuppu "No"	No	PED: Insert 1st M of N"	
1.3.46	kasuta rohelist võtit	Enter	PED: "This key is for M of N. Overwrite?"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.47	vajuta PEDil nuppu "Yes"	Yes	PED: "Are you sure you want to overwrite this PED Key?"	
1.3.48	vajuta PEDil nuppu "Yes"	Yes	Palutakse sisestada järgmine roheline võti.	
1.3.49	Tegevusi 1.3.45-1.3.47 tuleb korrata kokku M korda		teade ekraanil: "'hsm init' successful. /---/ Command Result : 0 (Success)"	
Turvaülema sisselogimine (6.2.6)				
1.3.50	logi turvaülem sisse	`hs logi`	PED: „insert a SO / HSM Admin PED key”	
1.3.51	kasuta uut sinist võtit	Enter	PED: „ Enter PED PIN”	
1.3.52	sisesta sinise võtme PIN	*****	PED: „insert 1st M of N PED Key”	
1.3.53	kasuta M korda rohelist võtit		teade ekraanil: „ ' login ' successful. /---/ Command Result : 0 (Success)”	
Krüptomootori häälestus (6.2.7)				

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.54	kontrolli HSMi sätteid	`hs showP`	kõik on nii nagu punktis 2.2, jätka protseduuriga 1.3.57	jätka järgmise punktiga
1.3.55	muuda HSMi sätet. Sätte kood on käsu ‚hs sh' väljundis veerus ‚Code', X'i väärtus sõltub sellest, kas säte on lubatud (1) või keelatud (0)	`hs changePo -p [sätte_kood] \` `-v X`	teade „'hsm changePolicy' successful"	teade „'hsm changePolicy' failed"
1.3.56	kontrolli HSMi sätteid	`hs showP`	kõik on nii nagu punktis 2.2	kõik ei ole nii nagu punktis 2.2; tagasi punkti 1.3.55
Partitsiooni loomine ja häälestus (6.2.8)				
1.3.57	loo partitsioon	`par cr -f -par PART`	PED: „Insert a User / Partition Owner PED key. Press Enter"	
1.3.58	kasuta esimest uut musta võtit	Enter	PED: „This PED Key has valid Identity for User / PartitionOwner. Reuse Id?"	
1.3.59	vajuta PEDil nuppu NO	No	PED: „Are you sure you want to overwrite this PED Key?"	
1.3.60	vajuta PEDil nuppu "Yes"	Yes"	PED: "Enter new PED PIN:"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.61	loo musta võtme PIN	*****	PED: „copy this PED Key?”	
1.3.62	vajuta PEDil nuppu "Yes"	Yes	PED: "Insert target PED Key. Press ENTER"	
1.3.63	kasuta teist uut musta võtit	Enter	PED: "This PED Key is for USER / PartitionOwner. Overwrite?"	
1.3.64	vajuta PEDil nuppu "Yes"	Yes	PED:"Are you sure you want to overwrite this PED Key?"	
1.3.65	vajuta PEDil nuppu "Yes"	Yes	PED: "Another copy of this PED Key?"	
1.3.66	vajuta PEDil nuppu "No"	No	PED kuvab partitsiooni salasõna, vormingus "****-****-****-****".	
1.3.67	pane PEDil kuvatav partitsiooni salasõna kirja		salasõna kirja pandud	
1.3.68	vajuta PEDil nuppu "Enter"	Enter	Teade ekraanil: ""'partition create' successful"	
1.3.69	kontrolli, kas partitsioon loodi	par l	kuvatakse partitsiooni number ja nimi	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.70	keela privaatvõtme ‚lahti-mähkimine'	`par changePo -pa PART -po 2 \ -v 0`	teade ekraanil: „Policy „Allow private key unwrapping" is now set to: 0"	
1.3.71	keela võtme atribuutide muutmine	`par changePo -pa PART -po 11 \ -v 0`	teade ekraanil: „Policy „Allow changing key attributes" is now set to: 0"	
1.3.72	keela väliste võtmetega signeerimine	`par changePo -pa PART -po 17 \ -v 0`	teade ekraanil: „Policy „Allow signing with non-local keys" is now set to: 0"	
1.3.73	luba partitsiooni aktiveerimine	`par changePo -pa PART -po 22 \ -v 1`	teade ekraanil: „Policy „Allow activation" is now set to: 1"	
1.3.74	keela partitsiooni automaatne aktiveerimine	`par changePo -pa PART -po 23 \ -v 0`	teade ekraanil: „Policy „Allow auto-activation" is now set to: 0"	
1.3.75	keela kaugautentimine	`par changePo -pa PART -po 30 \ -v 0`	teade ekraanil: "Policy "Allow Remote Authentication" is now set to: 0"	
NTLi häälestus (6.2.9)				
1.3.76	mine kataloogi /usr/lunasa/cert	`cd /usr/lunasa/cert`		

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.77	kustuta eelmise HSMi NTLi avalik võti	`rm server.pem`		
1.3.78	vaata, kas on registreeritud HSM'e	`vtl listServers`		
1.3.79	juhul, kui on registreeritud HSM'e, kustuta need	`vtl deleteServer -n \ [serveri_nimi]`		
1.3.80	Impordi HSMi NTLi avalik võti HLRi. HLR võib teatada, et ta pöördub tundmatu HSMi poole. Impordi ajal küsitakse serveriülema salasõna.	`ctp admin@10.0.0.4:server.pem .`	kataloogi tekib fail ‚server.pem'	
1.3.81	registreeri HSMi NTLi avalik võti	`vtl addServer –n 10.0.0.4 \ –c server.pem`	teade „New server 10.0.0.3 successfully added to server list."	
1.3.82	loo HLRi NTLi võtmepaar	`vtl createCert –n 10.0.0.2`	teade, et loodi privaatvõti & sertifikaat ning tuuakse ära nende asukohad	
1.3.83	ekspordi HLRi NTLi avalik võti HSMi. Ekspordi ajal küsitakse serveriülema salasõna.	`ctp client/10.0.0.2.pem \ admin@10.0.0.4:`	protsessi käigus küsitakse HSMi admin'i salasõna. Kui see on õige, kuvatakse laadimisprotsessi	
1.3.84	registreeri HSMis HLRi NTLi avalik võti	`cl reg -c HLR -i 10.0.0.2`	ekraanil teade: „'client register' successful'."	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
Partitsiooni ja HLRi sidumine (6.2.10)				
1.3.85	seo HLR partitsiooniga	`cl a -c HLR -p PART`	teade „'client assignPartition' successful."	
1.3.86	kontrolli, kas HLR seoti partit-siooniga	`cl s -c HLR`	väljund: ClientID: HLR IPAddress: 10.0.0.2 Partitions: „PART"	
1.3.87	kontrolli HLRis, kas partitsiooni sidumine õnnestus	`vtl verify`	teade, kus on märgitud HSMi seerianumber ja partitsiooni nimi. Partitsi-ooni nimi peab olema 'PART'	
Partitsiooni aktiveerimine (6.2.11)				
1.3.88	aktiveeri partitsioon	`par ac -par PART`	teade ekraanil: "Please enter the password for the partition"	
1.3.89	sisesta partitsiooni salasõna	`****-****-****-****`	PED: "Insert a USER / PartitionOwner PED Key:"	
1.3.90	kasuta uut musta võtit		PED: „Enter PED PIN:"	
1.3.91	sisesta PIN	`*****`	PED: "insert 1st M of N PED Key"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.92	sisesta järjekorras M rohelist võtit		teade ekraanil: "'partition activate' successful"	
Süsteemi võtmepaari ja sertifikaadi taastamine				
1.3.93	sisesta varunduskaart HSMi esipaneeli olevasse PCMCIA-pessa		kaks lühikest helisignaali, varunduskaart on pesas	
1.3.94	kontrolli, et tegu oleks õige varunduskaardiga	`t showC`	PED: "Insert a USER / PartitionOwner PED Key:"	
1.3.95	kasuta vana musta võtit		PED: "Enter PED PIN:"	
1.3.96	sisesta PIN	`*****`	PED: "Insert 1st M of N PED Key"	
1.3.97	kasuta järjekorras M vana rohelist võtit		ekraanil kuvatakse varunduskaardi nimi ning sellel olevad objektid.	
1.3.98	anna käsk võtmete taastamiseks	`par rest -par PART -r`	teade ekraanil: "please enter the password for the partition"	
1.3.99	sisesta partitsiooni salasõna	`****-****-****-****`	teade ekraanil: "Are your sure you wish to erase all objects in the partition named [ParNimi]?"	
1.3.100	kirjuta 'proceed'	`proceed`	PED: "Insert black PED key:"	

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.101	kasuta vana musta võtit		PED: "Enter PED PIN:"	
1.3.102	sisesta PIN, vajuta PEDil nuppu ENT	*****, ENT	PED: "Insert green PED key:"	
1.3.103	kasuta M vana rohelist võtit		teade ekraanil: "Restore successful."	teade ekraanil: "Segmentation fault". Üks kasutajatunnustest valesti sisestatud; alusta punktist 1.3.98
1.3.104	kontrolli, kas võtmepaar loodi. Kontrolli käigus küsitakse partitsiooni salasõna	`cmu list`	teade „handle=[pub_nr] label=avalik, handle=[priv_nr] label=privaat”	„Failure to login to HSM” - vale partitsiooni salasõna
Partitsiooni deaktiveerimine ja HSMi seiskamine (6.2.14)				
1.3.105	partitsiooni deaktiveerimine	`par dea -p PART`	teade ekraanil „’partition deactivate’ successful”	teade ekraanil: „Error: ’partition deactivate’ failed”
1.3.106	turvaülema väljalogimine	`hs logo`	teade ekraanil: „’hsm logout’ successful.”	
1.3.107	seiska HSM	`sysc a p`	seiskamise kinnituseks palutakse sisestada ‚proceed’	
1.3.108	kirjuta ‚proceed’	`proceed`	lühike helisignaal	
1.3.109	lülita HSM välja			

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.3.110	sule minicom: vajuta järgemööda klaviatuurklahve Ctrl+a, z, x, ‚Enter'		ekraanil HLRi käsurida	

1.4. Privaatvõtme hävitamine ja HSMi nullimine

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
HSMi käivitamine (6.2.1)				
1.4.1	kontrolli HSMi külgedel olevaid turvakleebiseid			
1.4.2	ühenda PED HSMiga			
1.4.3	ühenda HLR ja HSM omavahel jadakaabliga.			
1.4.4	käivita HSM			
HLRi käivitamine (6.2.2)				
1.4.5	käivita HLR, logi HLR'i lokaalse administraatorina	`root, *********`		
1.4.6	käivita minicom	`minicom`	5 sekundi pärast ekraanil teade: „Welcome to minicom"	
1.4.7	vajuta kaks korda Enter-klahvi		teade ekraanil: „hsm ttyS0 login:"	
1.4.8	logi seadmesse kasutajana ‚admin'			
Süsteemi privaatvõtme hävitamine (6.2.15)				

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.4.9	nulli HSM. Käsu kinnita-miseks tuleb terminalis sisestata 'proceed'	`hs fa`	terminal: "Command Result : 0 (Success)"	
1.4.10	kontrolli, et HSM oleks nullitud	`hs sh`	teminalis teated, et (1) "HSM IS ZEROIZED!, (2) "There are no partitions"	
1.4.11	sisesta varunduskaart esipaneelil olevasse pesasse			
1.4.12	nulli varunduskaart. Käsu kinnitamiseks tuleb terminalis sisestata 'proceed'	`t f`	terminalis teade "'token factoryReset' successful."	
1.4.13	kontrolli, et varunduskaart oleks nullitud	`t showC`	terminalis teade "The backup token is currently zeriozed. /.../ Error: 'token showContents' failed."	
1.4.14	eemalda varunduskaart HSMist			
1.4.15	kontrolli, kas HSMis on registreeritud kliente	`cl l`	kliente ei ole, jätka punktiga 1.4.17	kliente on (ekraanil teade: "registered client 1: [kliendi nimi]")

nr.	tegevus	käsk	tulemus õnnestumisel	tulemus ebaõnnestumisel
1.4.16	kustuta registreeritud kliendid	`cl d -f -c [kliendi_nimi]`	teade ekraanil: "'client delete' successful"	
1.4.17	määra kasutaja 'admin' parooliks 'Riigikogu2004'	`use p admin`		
1.4.18	seiska HSM	`sysc a p`		

2.Lisad

2.1. kliendi võrguliidese häälestusfail /etc/network/interfaces

```
# /etc/network/interfaces -- configuration file for ifup(8), ifdown(8)

# The loopback interface
auto lo
iface lo inet loopback

# The first network card - this entry was created during the Debian installation
# (network, broadcast and gateway are optional)
auto eth0
iface eth0 inet static
      address 10.0.0.2
      netmask 255.255.255.0
      network 10.0.0.0
      broadcast 10.0.0.255
```

2.2. muudetavate krüptomootori parameetrite väärtused

Description	Value	Code	Destructive
Allow cloning	On	7	Yes
Allow non-FIPS algorithms	Off	12	Yes
Allow MofN auto-activation	Off	13	No
SO can reset partition PIN	On	15	Yes
Allow network replication	Off	16	No
Allow Remote Authentication	Off	20	Yes
Force user PIN change after set/reset	Off	21	No

2.3. muudetavate partitsioonisätete väärtused

```
The following policies describe the current configuration
of this partition and may be changed by the HSM Administrator.

Description                              Value        Code
===========                              =====        ====
Allow private key cloning                On           0
Allow private key unwrapping             Off          2
Allow secret key cloning                 On           4
Allow secret key wrapping                On           5
Allow secret key unwrapping              On           6
Allow multipurpose keys                  On           10
Allow changing key attributes            Off          11
Ignore failed challenge responses        On           15
Operate without RSA blinding             On           16
Allow signing with non-local keys        Off          17
Allow raw RSA operations                 On           18
Max non-volatile storage space           5            19
Max failed user logins allowed           10           20
Allow high availability recovery         On           21
Allow activation                         On           22
Allow auto-activation                    Off          23
Minimum pin length (inverted: 255 - min) 248          25
Maximum pin length                       255          26
Allow Key Management Functions           On           28
Perform RSA signing without confirmation On           29
Allow Remote Authentication              Off          30
```