
E-valimised. Süsteemiülema juhend

Väljalase 1.22.1

Cybernetica AS

04.02.2015

Sisukord

1	Süsteemi ülevaade	3
1.1	Sissejuhatus	3
2	Süsteemi algseadistamine	7
2.1	Nõuded arvutile	7
2.2	E-hääletamissüsteemi paigalduspakkide valmistamine	7
2.3	Süsteemi paigaldamine	10
2.4	Kaugseire ja statistika (jälgimisjaam)	10
3	Ühised tegevused seadistusperioodil	15
3.1	Jälgimisjaama logimise testimine	15
3.2	Sertifikaatide konfiguratsiooni laadimine	15
3.3	Serveri häälestamine parameeter-haaval	17
3.4	Serveri häälestamine paigaldusfailiga	20
3.5	Konfiguratsiooni kontrollimine	24
3.6	Valimisinfo muutmine	24
4	HES protseduurid	25
4.1	Seadistusperiood	25
4.2	Hääletusperiood	28
5	HTS protseduurid	29
5.1	Seadistusperiood	29
5.2	Hääletusperiood	30
5.3	Tühistusperiood	30
6	HLR protseduurid	33
6.1	Seadistusperiood	33
6.2	Lugemisperiood	33
7	Prooviläbimise korraldamine	37
7.1	Valijate nimekirja kontrolli keelamine	37
7.2	Valijate nimekirja kontrolli lubamine	37
7.3	Hääletuse algoleku taastamine	38
8	Süsteemi haldustoimingud	39
8.1	Serverite ettevalmistamine kiirtaastamiseks	39
8.2	Varukoopiate tegemine	39
8.3	Varukoopiast taastamine	39

8.4	Töö failide ja kataloogidega	39
8.5	DVD-plaatide kirjutamine	41
8.6	Süsteemsete teadete kohandamine	41

Redaktsioon 1.22.1

Dokument: EHA-03-03-1.22

Kuupäev: 04.02.2015

Redaktsioonide ajalugu

Kuupäev	Versioon	Kirjeldus ja muudatused	Autor
23.08.2005	1.0	Koostatud dokument.	Märt Laur
03.10.2005	1.1	Täiendused süsteemi paigaldamise osas.	Uve Lokk
04.10.2005	1.2	Parandused vastavalt tagasisidele.	Märt Laur
28.04.2006	1.3	Täiendused algoleku taastamise, veateadete kasutamise, valijanimekirjade uuendamise ning operaatori kasutajaliidese osas.	Märt Laur
08.05.2006	1.4	Täiendused logiutiliidi ja paigaldatavate pakside osas, lisandus lokaal et_EE.UTF8.	Märt Laur
11.05.2006	1.5	Täiendused kaardilugeja paigalduse, logiutiliidi ja valimisidentifikaatorite kustutamise osas.	Märt Laur
06.06.2006	1.6	Täiendused vastavalt VVK nõutud muudatustele rakendustes.	Märt Laur
17.12.2006	1.7	Paigaldusjuhised läksid eraldi dokumenti. Kustutatud aegunud funktsionaalsusega seotud teavet. Lisatud teave valijate nimekirja kontrolli kohta.	Märt Laur
15.01.2007	1.8	Täiendused vastavalt tagasisidele	Märt Laur
29.03.2009	1.9	Muutused seoses Europarlamendi ja Etchiga	Sven Heiberg
10.05.2009	1.10	Nimekirjade printimise täiendused	Sven Heiberg
25.08.2009	1.11	Hääletuse järkjärguline peatamine	Sven Heiberg
13.12.2010	1.12	BDOC, Mobiil-ID	Sven Heiberg
10.01.2011	1.13	Joonise parandus	Sven Heiberg
06.08.2013	1.14	Muudatused seoses KOV2013, kontrollitavuse ja Wheezyga	Sven Heiberg
31.08.2013	1.15	GitHub protseduuri testimine, täiendused pakisõltuvuste osas	Sven Heiberg
18.09.2013	1.16	Monitooringu ja kontrollitavuse täpsustused	Sven Heiberg
03.10.2013	1.17	Paigaldusprotseduuride ülevaatlikkust parandatud	Sven Heiberg
07.10.2013	1.18	Valimisinfo muutmine	Sven Heiberg
18.04.2014	1.19	Muudatused seoses EP2014 valimisega	Sven Heiberg
24.04.2014	1.20	Parandatud sõnastused; Parandatud failinimed; Parandatud erisused tarkvaras ja tekstis; Täpsustatud operatsioonisüsteemi versioon; Täiendatud github sertifikaatide kontroll; Nimetatud lisapakid paigaldusplaadile; Täpsustatud sõltuvuspakid; Kirjeldatud apache'i sätteid jälgimisjaamas; Lisatud BDOC 2.1; Lisatud ESTEID sertifikaadid bdoc.conf jaoks; Kontrollsummad valikulised; Failivormingute täpsustused; Paigalduspaki conf faili spetsifikatsioon; HES Apache sätete täpsustused; Hääletamise alguse ja lõpu automaatne seadistamine; Hääletamistulemuse eksport.	Sven Heiberg
05.05.2014	1.21	Apache'i direktiivi SSLCertificateChainFile kasutamise täpsustamine	Sven Heiberg

Jätub järgmisel lehel

Tabel 1 – jätk eelmisele leheküljele

Kuupäev	Versioon	Kirjeldus ja muudatused	Autor
29.12.2014	1.22	Dokument teisendatud RST-vormingusse; Sõnastuse parandused; Ajakohastatud tarkvara versioone; Pakkide versiooninumbrid ja sõltuvused genereeritakse lähtekoodi põhjal; Lisatud nimekiri dokumentidest, millele käesolevast juhendist viidatakse; Eemaldatud termin “logiserver”, selle asemel on kasutusel “jälgimisjaam”; Lisatud märkused töötajate rollide kohta võrreldes teiste dokumentidega; Parandatud jälgimisjaama spetsialistiliidesesse ID-kaardiga autentimise juhiseid; IP-aadresside lisaandmete paigaldus toimub välisel andmekandjal; Haldustoimingud kolitud omaette lõiku; Prooviläbimise korraldamine kolitud omaette lõiku. Eemaldatud failide printimine ja kustutamine, täpsustatud failide eksportimist; Valijate nimekirja uuendamine kolitud HESi ja HTSi vastavatest lõikudest seadistusperioodi ühistegevuste jaotisesse; Lisatud jälgimisjaama syslogi testimise lõik; Lisatud jälgimisjaama paigaldamisel operaatorilt küsitavate küsimuste kirjeldused; Täpsustatud varukoopia loomist ja sellelt taastamist; Lisatud failide sirvimise ja eksportimise kirjeldused.	Ivar Smolin
03.02.2015	1.22.1	Testperioodi järgne kirjavigade parandus	Sven Heiberg

Süsteemi ülevaade

1.1 Sissejuhatus

Käesolev dokument käsitleb tööd e-hääletustarkvaraga süsteemiülema vaatepunktist ning kirjeldab tarkvara kõiki võimalusi kogu e-hääletusprotsessi ulatuses. Süsteemiülemalt eeldatakse e-hääletuse põhiterminoloogia tundmist.

1.1.1 Lisamaterjalid

Käesolevas dokumendis viidatakse järgnevatele e-hääletamisega seotud dokumentidele:

- EHA-02-01-1.0 E-hääletamise organisatsioon ja infrastruktuur;
- EHA-03-02-1.7 E-hääletamise käsiraamat;
- EHA-03-06-2.3 Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Tegevusjuhised;
- EHA-03-10-4.2 Operatsioonisüsteemi paigaldus;
- EHK-02-04-1.7 Tehnilised nõuded riistvarale;
- EHK-04-03-1.16 Olekupuud.

1.1.2 E-hääletamise etapid

E-hääletusprotsess jaguneb neljaks kohustuslike tegevustega etapiks. Enamik e-hääletussüsteemi funktsionaalsusest on lubatud vaid kindlas hääletuse etapis. Etapid on järgnevad:

- **Seadistusperiood** - Süsteem algseadistatakse, paigaldatakse e-hääletustarkvara ning laaditakse info konkreetsete hääletuste kohta.
- **Hääletusperiood** – Valijad osalevad e-hääletusel. Serverid tegelevad häälte vastuvõtmise ja talletamisega.
- **Tühistusperiood** – Fikseeritakse lõplik e-hääletanute nimekiri. Hääled sortitakse, korduvad ja kehtetud hääled tühistatakse. Terve tühistusperioodi vältel võetakse vastu tühistus-/ennistusnimekirju. Perioodi lõppedes fikseeritakse arvesse minevad hääled ja koostatakse loendamisele minevate häälte nimekiri.
- **Lugemisperiood** – Hääled loetakse kokku ja sisestatakse valimiste infosüsteemi.

1.1.3 Süsteemi logid

Kõik serverikomponendid täidavad töö käigus üldiste sündmuste logi. Lisaks kasutab süsteem veel viit hääletuse-spetsiifilist logifaili. Need on:

- LOG1 – Vastuvõetud hääled;
- LOG2 – Tühistatud hääled;
- LOG3 – Lugemisele läinud hääled;
- LOG4 – Kehtetud hääletussedelid;
- LOG5 – Arvesse läinud hääled.

Logide tervikluse kontrollimisel peab LOG2 ja LOG3 ühend andma LOG1 sisu ning LOG4 ja LOG5 ühend LOG3 sisu.

1.1.4 Dokumendis kasutatavatest tavadest

Tekst, mille peab sisestama kasutaja, on toodud rasvases kirjas. Näiteks:

Kas soovite jätkata (jah/ei) **jah**

1.1.5 Mõisted ja definitsioonid

Olekupuu Failisüsteem, kus hoitakse e-hääletuse tööks vajalikku teavet – hääli, vahetulemusi, logisid jm. Olekupuu tehniline kirjeldus on dokumendis EHK-04-03-1.16 Olekupuu, mis tarnitakse e-hääletuse CD-l.

HES Hääleedastusserver. HES tuvastab ID-kaardi või Mobiil-ID alusel hääletaja ning tema valimisõiguse, edastab hääletajale tema piirkonna kandidaadid ja võtab vastu krüpteeritud ja digiallkirjastatud e-hääle. HES edastab hääled hääletalustusserverisse ja edastab sealt saadud tulemuskoode hääletajale. Lõpetab töö pärast hääletusperioodi lõppu.

HTS Hääletalustusserver. HTS võtab vastu ja salvestab HESilt saadetud e-hääled. Pärast eelhääletamise lõppu eemaldab HTS korduvad hääled ning võtab vastu ja täidab e-hääle tühistusi ja ennistusi. Lõpuks eraldab HTS hääle sisemised ümbrikud välimistest ning paneb need valmis hääletelugemisirakenduse jaoks

HLR Häälelugemisirakendus. HLR on vallasrežiimis komponent, kuhu kantakse üle krüpteeritud hääled, millelt on eemaldatud digitaalalkiri. HLRi avalikku võtit kasutatakse valija valiku krüpteerimisel. HLR kasutab süsteemi privaativõtit, summeerib hääled ning väljastab e-hääletamise tulemused.

HSM Riistvaraline krüptomoodul (*Hardware Security Module*), mis sooritab kõiki e-hääletamise privaativõtmega seonduvaid toiminguid.

Jälgimisjaam Väline rsyslog server, kuhu HES ja HTS suunavad oma logid

OCSP responder Digitaalalkirja kehtivuskinnituste server.

DigiDoc teenus Teenus, mis vahendab suhtlust HES ja Mobiil-ID kasutajate vahel

VVK Vabariigi Valimiskomisjon.

Privaativõtme nimi Privaativõtme genereerimisel HSMis määratud privaativõtme nimi.

VIS valimiste infosüsteem.

Kesksüsteem Vabariigi Valimiskomisjoni vastutuse all olev süsteemiosa. Tegeleb hääle vastuvõtmisega, töötlemisega ja koondtulemuse väljastamisega.

1.1.6 Hääletamisse kaasatud töötajate rollid

Administraator Valmendab ja paigaldab e-hääletamise tarkvara, hoolitseb süsteemi käivitamise ja mahavõtmise eest, jälgib tehnilisi logisid.

Märkus: Dokumendis EHA-03-02-1.7 E-hääletamise käsiraamat on rolli *Administraator* nimeks *E-hääletamise läbiviimise süsteemadministraator*

Auditeerija Lahendab e-hääletamisega seotud kaebusi, kasutades Kesküsteemist pärit logiteavet. Käivitab ka auditprotseduure logide terviklikkuse kontrolliks.

HES operaator Tegeleb volitatud isikute haldusega, jälgib tehnilisi logisid, impordib andmeid süsteemi, muudab süsteemi olekut, väljastab tulemusi.

Märkus: Dokumendis EHA-03-02-1.7 E-hääletamise käsiraamat on *HES operaator* osa rollist *Hääleedastamisserveri ja hääletalletamisserveri operaator*.

HTS operaator Tegeleb volitatud isikute haldusega, jälgib tehnilisi logisid, impordib HTSi digitaalselt allkirjastatud tühistus- ja ennistusavaldusi, muudab süsteemi olekut, väljastab tulemusi.

Märkus: Dokumendis EHA-03-02-1.7 E-hääletamise käsiraamat on *HTS operaator* osa rollist *Hääleedastamisserveri ja hääletalletamisserveri operaator*.

HLR operaator Töötaja, kes teostab enne hääle kokkulugemist ettevalmistavaid tegevusi: e-hääletanute nimekirja koostamine ning e-hääle ettevalmistamine kokkulugemiseks.

Turvamooduli haldur Töötaja, kes initsialiseerib turvamooduli ja loob võtmehaldusprotseduurid. Testib turvamoodulis loodud võtit. Tegeleb avaliku osa transpordi ning integreerimisega kliendirakendusse. E-hääletuse lõpetamisel hävitab privaatvõtme ja selle koopiad. Algatab koos võtmehalduriga hääle kokkulugemise.

Märkus: Dokumendis EHA-03-02-1.7 E-hääletamise käsiraamat on rolli *Turvamooduli haldur* nimeks *Turvamooduliga seotud rollid (serveriülem, turvaiülem, rakendusülem, lähtestaja, varundusülem, statistid)*

Valimisinfo haldur VVK ametnik, kes tegeleb valimisjaoskondade, ringkondade ja valikute- kandidaatide (valimistel) või vastusevariantide (rahvahääletusel) nimekirja koostamisega ning vastutab nende nimekirjade laadimise eest enne e-hääletamise algust. Kõik nimekirjad peale valijate nimekirja on digitaalselt allkirjastatud.

VVK volitatud tühistaja Isik, kes signeerib tühistus- ja ennistusavalduste faile.

Võtmehaldur Osapool, kes tegeleb koos turvamooduli halduriga süsteemi võtmepaari genereerimise, haldamise ja kasutamisega. Avalik võti integreeritakse Valija rakendusesse, privaatvõti antakse õigel ajal kasutamiseks HLR-le. NB! Võtmehalduri rolli täidab mitu koos getusevad isikut.

1.1.7 Operaatori kasutajaliides

Operaatori kasutajaliides on tekstipõhine kestprogramm (*shell*), mille menüüde kaudu saab turvalisuse eesmärgil sooritada vaid kindlaksmääratud tegevusi. Kasutajaliidese tekstid kasutavad UTF-8 kodeeringut. Kasutajaliidese sisenemine toimub lokaalselt vastavalt kasutajana *hes*, *hts* või *hlr*. Kaugpöörduse võimaldamine e-hääletamise serveritesse ei ole soovitatav.

Menüüdes liikumiseks tuleb sisestada menüü ja/või alammenüü number. Vaatame näiteks osa hääleedastusserveri menüüst:

```
[1] Tegele valimistega
    (1) RKTEST2015
[2] Üldine konfiguratsioon
    (1) Laadi sertifikaadid
    (2) Säti HTSi konfiguratsioon
[3] Ekspordi kõik
```

*hes*Operaator >

Näiteks kui operaatori viiba *hes*Operaator > järele sisestada 2 2, avaneb menüüpunkt *Säti HTSi konfiguratsioon*. Kui põhimenüü sisaldab alammenüüsid, siis tuleb alati sisestada mõlema – põhimenüü ja

alammenüü – number, nii nagu eelmises näites. Kui põhimenüü (nt *Ekspordi kõik*) ei sisalda alammenüüsid, siis tuleb sisestada ainult põhimenüü number, praegusel juhul 3.

Menüüdes tagasi liikumiseks vajutage klahvikombinatsiooni `Ctrl-d`. Selle peale sisenetakse sammu võrra kõrgemasse menüüsse. Sama klahvivajutusega saab katkestada ka käimasolevaid toiminguid, nt failinimedest sisestamist.

1.1.8 Töö mitme DVD-ga

DVD asetamisel draivi monteeritakse selle sisu automaatselt kataloogi `/dvd`. Sama toimub siis, kui üritada veel monteerimata `/dvd` kausta sisu vaadata. Võib juhtuda, et mõne toiminguga käigus tekib vajadus laadida andmeid mõne teise DVD pealt. Näiteks kui sertifikaatide laadimisel nõutakse:

Sisesta OSCP tipmise CA sertifikaadi asukoht:

ja selgub, et seadmes pole õige meedium, siis ärge kirjutage viiba järgi midagi, vaid vajutage lihtsalt `Enter`-klahvi. Süsteem monteerib ketta lahti ja väljastab plaadi, mille järel on võimalik draivi asetada õige sisuga plaat.

1.1.9 Ülevaade toimingutest

Seadistusperioodi toimingud

Seadistusperioodil tuleb paigaldada kõik serverid ja serveritarkvara ning tarkvara häälestada. Samuti tuleb serveritesse kanda volitatud isikute isikukoodid.

Hääletusperioodi toimingud

Hääletusperioodi ajal võtab hääleedastusserver (HES) krüpteeritud hääli vastu, tuvastab valijate andmebaasi põhjal hääletaja valimisõiguse ning tema valimisringkonna. Kui selle käigus tõrkeid ei ilmne, saadab HES hääle hääletalustserverile (HTS). HTS salvestab hääled. Hääletamise ajal pöörduakse kehtivuskinnituse teenuse poole valija digitaalallkirjale kehtivuskinnituse saamiseks. Pärast e-hääletamise lõppu eemaldatakse HES võrgust.

Tühistusperioodi toimingud

Pärast eelvalimiste lõppu tühistatakse korduvad hääled. Volitatud isikud koostavad valimisjaoskondade kaupa e-hääletanute nimekirjad ning saadavad koos eelhääletanute ümbrikutega valimisjaoskondadesse. Arvesse läheb iga valija puhul ainult viimasena antud e-hääli. Hääle andmise aega kontrollitakse digitaalallkirja kehtivuskinnituse aja järgi.

Digitaalallkirjastatud tühistuskannete fail imporditakse HTSi, mis teostab tühistused. Tühistamise põhjuseks võib olla korduv hääli või tühistamine tühistusavalduse alusel. Avalduse alusel tühistatud hääli saab ennistada ehk muuta taaskehtivaks. Hääled ennistatakse HTSi imporditud digitaalallkirjastatud ennistusavalduste faili alusel.

Pärast tühistusperioodi sorteeritakse vastu võetud hääled valimisringkondade kaupa. Häältelt eemaldatakse digitaalallkirjad, mille tulemusel pole enam võimalik kindlaks teha hääletaja isikut, seepärast eksporditakse hääled välisele andmekandjale.

Lugemisperioodi toimingud

Lugemisperiood on e-hääletamise viimane etapp. Häätelugemisele on sisendiks šifreeritud hääled, millelt on eemaldatud digitaalallkiri. HLR summeerib süsteemi privaatvõtme abil hääled ning väljastab e-hääletamise tulemused.

Hääle lugemiseks peab HLRis olema fail, kus on krüptitud hääled, millelt on eemaldatud allkirjad. Faili terviklikkus tagatakse faili kontrollsumma võrdlemisega. Kontrollsumma on salvestatud ka andmekandjale, millega viiakse andmed HTSst HLRi. Faili autentsus tuleb tagada e-hääletussüsteemi väliste meetoditega.

Süsteemi algseadistamine

2.1 Nõuded arvutile

Kõik e-hääletamise teenust osutavad serverid peavad olema sihtotstarbelised, s.t. sisaldama ainult e-hääletamise läbiviimiseks vajalikku tarkvara. Kogu muu tarkvara tuleb paigaldada ja seadistada alates nullist – eelmise hääletamise aegset serverikonfiguratsiooni ei tohi kasutada.

Täpsed riistvaralised nõudmised asuvad dokumendis EHK-02-04-1.7 Tehnilised nõuded riistvarale.

2.2 E-hääletamissüsteemi paigalduspakkide valmendamise

Elektroonilise hääletamise kesksüsteem on realiseeritud Linux Debian 7.7 operatsioonisüsteemile. Kesksüsteemi komponentide paigaldamiseks tuleb valmendada paigalduspakid ja paigaldusrepositoorium CD-plaadil. Tarkvara lähtekood on arendaja poolt tarnitud CD-plaadil ning publitseeritud avalikkusele keskkonnas GitHub (<https://github.com/vvk-ehk/evalimine>). Paigalduspakkide valmendamise käigus tuleb veenduda, et arendaja poolt tarnitud ja GitHub'is publitseeritud versioonid ühtivad.

2.2.1 Ettevalmistused paigalduspakkide valmendamiseks

Paigalduspakkide valmendamiseks on vaja e-hääletamise tarneplaadil asuvat faili `/utiliidid/intcheck.py`, mis tuleb laadida valmendusarvutisse ning seada käivitusbitt:

```
> chmod +x intcheck.py
```

`intcheck.py` on utiliit kataloogide tervikluse kontrolliks. Utiliit võtab argumentideks kataloogi ja `*.icf` faili ning veendub, et kataloogi struktuur ja failide sisu vastavad jätkuvalt loomisaegsetele.

Valmendamine eeldab, et on seadistatud Linux Debian 7.7 operatsioonisüsteemiga 64-bitine valmendusarvuti, kuhu on paigaldatud järgmised pakid koos sõltuvustega:

```
> aptitude -R install build-essential fakeroot debhelper devscripts \  
python2.7-dev libxml2-dev libssl-dev swig chrpath libtool automake \  
python-gdbm python-zsi xsdcxx libxerces-c-dev libxml-security-c-dev \  
genisoimage
```

Valmendamise käigus on vajalikud utiliidid `unzip`, `tar` ja `wget`, mis tulevad paigaldada järgnevalt:

```
> apt-get install unzip tar wget
```

Järgnevas eeldame, et käsklused on antud kasutaja kodukataloogis, kus paikneb ka utiliit `intcheck.py`.

Lähtekoodi laadimiseks GitHub keskkonnast tuleb süsteemi paigaldada usaldatud CA sertifikaadid:

```
> aptitude -R install ca-certificates
```

Tarkvara lähtekood laaditakse GitHub keskkonnast alla ZIP-failina, mis on tarkvara uusima versiooni jaoks keskkonna poolt automaatselt tekitatud. Toimingu käivitamiseks peab valmendusarvuti olema ühendatud interneti ning tuleb anda käsklus:

```
> mkdir github
> cd github
> wget https://github.com/vvk-ehk/evalimine/archive/master.zip
```

Seejärel tuleb lähtekood lahti pakkida:

```
> unzip master.zip
> cd ..
```

Seejärel tuleb e-hääletamise tarneplaadilt laadida valmendusarvutisse e-hääletuse tarkvara lähtekood ning see lahti pakkida:

```
> mkdir original
> cd original
> tar xzvf /media/cdrom/kesksüsteem/source/evote_1.1.2.tar.gz
> cd ..
```

E-hääletamise tarneplaadil on fail `ivote-server.icf.ddoc`. Veendu allkirja korrektsuses, eralda fail `ivote-server.icf` ning laadi see valmendusarvutisse kasutaja kodukataloogi. Käivita utiliit:

```
> ./intcheck.py verify github/evalimine-master/ivote-server ivote-server.icf
> ./intcheck.py verify original/ivote-server ivote-server.icf
```

Tervikluse kontrolli võib lugeda edukaks, kui mõlemad operatsioonid lõpetavad oma töö teatega:

```
OK - Integrity check successful
All directory and file checksums verified correctly
```

2.2.2 Paigalduspakkide valmendamine ja paigaldusplaadi loomine

Kuna nüüd on kindel, et lähtekoodid tarneplaadil ja GitHubis on identsed, võib valmendada paigalduspakid:

```
> cd github/evalimine-master/ivote-server
> make debuild
...
> cd ..
```

Paigalduspakkide kuvamine:

```
> ls *.deb
evote-common_1.1.2_amd64.deb
evote-hes_1.1.2_all.deb
evote-hlr_1.1.2_amd64.deb
evote-hts_1.1.2_all.deb
evote-prepare_1.1.2_all.deb
```

Soovi korral võib luua ka Debiani paigaldusplaadi tõmmise (ISO 9660 vormingus), kuhu võib lisada kesksüsteemi mitteavalikustatud komponente sisaldava paki `evote-analyzer_1.0.0_all.deb` ning jälgimisjaama paki `ivote-monitor_1.0.2_amd64.deb`:

```
> mkdir debs
> cp *.deb debs
> cd debs
> ../ivote-server/debian/repo.py evote-amd64-installer . amd64
```

```
> ls *.iso
evote-amd64-installer.iso
```

Seda tömmist on võimalik kasutada e-hääletamise kesksüsteemi paigaldusplaadi loomiseks.

2.2.3 HES paigalduspakid

HESi paigaldamiseks on vaja järgmisi pakke:

- `evote-common_1.1.2_amd64.deb`;
- `evote-hes_1.1.2_amd64.deb`.

Pakkidel on järgmised sõltuvused: `adduser`, `apache2`, `at`, `autofs`, `dvd+rw-tools`, `kbd`, `less`, `libxerces-c3.1`, `libxml-security-c16`, `locales`, `lvm2`, `openssl`, `python-gdbm`, `python-m2crypto`, `python-psutil`, `python-zsi`, `python2.7`, `rsyslog`, `sudo`, `sysstat`

Pakid muudavad järgmiste komponentide seadistusi:

- `rsyslog`;
- `Apache2`.

Kesksüsteemi mitteavalikustatud komponendid paigaldatakse pakist

- `evote-analyzer_1.0.0_all.deb`.

Pakil `evote-analyzer` ei ole täiendavaid sõltuvusi, kuid see muudab pakist `evote-hes` paigaldatud faile.

HESi paigaldamisel küsitakse operaatorilt jälgimisjaama aadressi kujul `<nimi|IP>:port`. Näiteks:

```
log-server:514
```

Märkus: HESi paigaldamisel jäetakse Apache veebiserver seisma ja veebiserveri sätetesse lisatakse HESi virtuaalhosti sätteid, mida on vaja täiendada veebiserveri privaativõtme ja SSL-sertifikaatidega (vaata [HESi veebiserveri seadistamine](#) (lk 25)). Apache veebiserver käivitatakse uuesti vaid juhul, kui veebiserveri sätteid töötavad.

2.2.4 HTS paigalduspakid

HTSi paigaldamiseks on vaja järgmisi pakke:

- `evote-common_1.1.2_amd64.deb`;
- `evote-hts_1.1.2_amd64.deb`.

Pakkidel on järgmised sõltuvused: `adduser`, `apache2`, `at`, `autofs`, `dvd+rw-tools`, `fontconfig`, `kbd`, `less`, `libxerces-c3.1`, `libxml-security-c16`, `locales`, `lvm2`, `openssl`, `python-gdbm`, `python-m2crypto`, `python-psutil`, `python2.7`, `rst2pdf`, `rsyslog`, `sudo`, `sysstat`, `ttf-dejavu-core`

Pakid muudavad järgmiste komponentide seadistusi:

- `rsyslog`;
- `Apache2`.

HTSi paigaldamisel küsitakse operaatorilt jälgimisjaama aadressi kujul `<nimi|IP>:port`. Näiteks:

```
log-server:2514
```

2.2.5 HLR paigalduspakid

HLRi paigaldamiseks on vaja järgmisi pakke:

- `evote-common_1.1.2_amd64.deb`;
- `evote-hlr_1.1.2_amd64.deb`.

Pakkidel on järgmised sõltuvused: `adduser`, `at`, `autofs`, `dos2unix`, `dvd+rw-tools`, `kbd`, `less`, `libxerces-c3.1`, `libxml-security-c16`, `locales`, `lvm2`, `openssl`, `python-gdbm`, `python-m2crypto`, `python2.7`, `rsyslog`

Täiendavalt tuleb paigaldada HSM draiverid.

2.2.6 Jälgimisjaama paigalduspakid

Jälgimisjaama paigaldamiseks on vaja pakki `ivote-monitor_1.0.2_amd64.deb`.

Pakil on järgmised sõltuvused: `adduser`, `apache2`, `mysql-server`, `procp`s, `python-geoip`, `python-matplotlib`, `python-mysqldb`, `python-psutil`, `python-pycountry`, `rsyslog`.

Pakk muudab järgmiste komponentide seadistusi:

- `rsyslog`;
- MySQL;
- Apache2.

Jälgimisjaama paki paigaldamisel küsitakse operaatorilt järgmisi andmeid:

- jälgimisjaama veebihosti nimi. See on aadress, mille kaudu pääseb ligi jälgimisjaama veebiliidestele (*Robotliides* (lk 11) ja *Toeliides* (lk 12)).
- Hääletusperioodi algus- ja lõpuaeg. Selle põhjal on võimalik statistika genereerimisel eristada hääletusperioodi käigus kogutud andmeid muul ajal (nt prooviläbimise käigus) kogutud andmetest.

2.3 Süsteemi paigaldamine

Süsteemi paigaldamist kirjeldab eraldi dokument `EHA-03-10-4.2 Operatsioonisüsteemi paigaldus`.

2.4 Kaugseire ja statistika (jälgimisjaam)

E-hääletamise serverid HES ja HTS saavad oma logiteated kesksesse jälgimisjaama. Logiteadete saatmine toimub teenuse `syslog` ja andmesideprotokolli UDP abil. Jälgimisjaama aadress küsitakse operaatorilt HESi ja HTSi paigaldamise käigus.

Tähelepanu: Süsteemi parema auditeeritavuse huvides on kasulik jälgimisjaam seadistada enne teiste süsteemi kuuluvate serverite paigaldamist.

Syslog

Jälgimisjaamas tuleb tarkvarapaki `ivote-monitor` paigaldamise järel määrata hostid, millelt `syslog` teenus logiteateid vastu võtab. Selleks tuleb failis `/etc/rsyslog.d/im-rsyslog.conf` asendada stringid `XXXHESXXX` ja `XXXHTSXXX` tegelike hostinimedega. Mitme HESi korral tuleb iga HESi jaoks kirjeldada eraldi seadistused. Seejärel tuleb `syslog` taaskäivitada:

```
> sudo vi /etc/rsyslog.d/im-rsyslog.conf
> sudo service rsyslog restart
```

Märkus: Syslogi testimiseks vaata lõiku *Jälgimisjaama logimise testimine* (lk 15).

IP-aadresside lisaandmed

IP-aadresside lisaandmete paigaldamiseks tuleb lisaandmete failid kirjutada välisele andmekandjale ja paigaldada need jälgimisjaama. Andmefailid asuvad järgnevatel aadressidel:

- GeoIP: <http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz>
- TOR-võrgu noded: http://torstatus.blutmagie.de/ip_list_exit.php/Tor_ip_list_EXIT.csv
- Spamhaus'i rämpsunimekirjad:
 1. <http://www.spamhaus.org/drop/drop.txt>
 2. <http://www.spamhaus.org/drop/edrop.txt>

GeoIP teenuse toimimiseks tuleb anda järgmised käsud:

```
> cd /var/log/ivote-monitor
> cp /dvd/GeoLiteCity.dat.gz .
> gunzip GeoLiteCity.dat.gz
> chown imonitor.www-data GeoLiteCity.dat
> chmod +r GeoLiteCity.dat
```

TOR-võrgu nodede tuvastamiseks tuleb anda järgmised käsud:

```
> cd /var/log/ivote-monitor
> cp /dvd/Tor_ip_list_EXIT.csv .
> chown imonitor.www-data Tor_ip_list_EXIT.csv
> chmod +r Tor_ip_list_EXIT.csv
```

Spamhaus'i rämpsunimekirjade rakendamiseks tuleb anda järgmised käsud:

```
> cd /var/log/ivote-monitor
> cp /dvd/drop.txt /dvd/edrop.txt .
> chown imonitor.www-data drop.txt
> chown imonitor.www-data edrop.txt
> chmod +r drop.txt
> chmod +r edrop.txt
```

Veebiserveri sertifikaatide konfiguratsioon

Pärast paigaldamist tuleb kontrollida failis `/etc/apache2/sites-enabled/im-apache` paiknevat Apache'i sertifikaatide konfiguratsiooni. Selles asuvad vaikevõti ja sertifikaat tuleb välja vahetada, samuti tuleb määrata kasutaja sertifikaate väljastavate sertifitseerimiskeskuste ahelafail.

Direktiiv `SSLCertificateFile` määrab veebiserveri autentimiseks kasutatava sertifikaadifaili raja:

```
SSLCertificateFile /etc/ssl/certs/webcert.pem
```

Direktiiv `SSLCertificateKeyFile` määrab direktiivis `SSLCertificateFile` näidatud sertifikaadile vastava privaatvõtme faili raja:

```
SSLCertificateKeyFile /etc/ssl/private/webkey.pem
```

Direktiiv `SSLCACertificateFile` määrab usaldatavate sertifitseerimiskeskuste sertifikaate sisaldava faili raja:

```
SSLCACertificateFile /etc/ivote-monitor/id.crt
```

2.4.1 Robotliides

Hetkel unikaalsete valijate poolt antud hääle arvu näitav robotliides on kättesaadav URLil `https://<jälgimisjaam>/robot.cgi`. Robotliidese poole pöördumine ei nõua autentimist.

2.4.2 Toeliides

Ligipääs statistikalehele `https://<jälgimisjaam>/stat.cgi` on ID-kaardi põhine. Pääsuõiguste määramiseks tuleb jälgimisjaamas avada või luua tekstifail `/etc/ivote-monitor/stat-ik` ja sisestada sinna isikukoodid, üks kood rea kohta. Faili võib lisada ka kommentaare. Näiteks:

```
# esimene kommentaar
# teine kommentaar
47101010033
37102216522
37001516011
# kolmas kommentaar
37702216517
```

2.4.3 Spetsialistiliides

Spetsialistiliides on harilik Linuxi käsurealiides, kuhu pööratakse SSH abil. Spetsialistiliidese kaudu sisseloginud kasutajal on võimalik logifailide vaadata kataloogist `/var/log/ivote-monitor`.

Kasutajate autentimine ID-kaardi abil

SSH teenusesse on võimalik autentida ID-kaardi avaliku võtmega abil, kasutades selleks PKCS#11 toega SSH klienti **kitty.exe** (<http://kitty.9bis.net/>).

Soovituslik on keelata spetsialistiliideses parooliga autentimine. Seda saab teha, kui failis `/etc/ssh/sshd_config` määrata parameeter `PasswordAuthentication`:

```
PasswordAuthentication no
```

Volitatud kasutajate faili asukoht (`/etc/ssh/kasutajad`) tuleb failis `/etc/ssh/sshd_config` määrata parameetriga `AuthorizedKeysFile`:

```
AuthorizedKeysFile /etc/ssh/kasutajad
```

Tähelepanu: SSH seadistusfailis `/etc/ssh/sshd_config` tehtud muutuse rakendamiseks tuleb SSH teenus taaskäivitada:

```
> service ssh restart
[ ok ] Restarting OpenBSD Secure Shell server: sshd.
```

ID-kaardi isikutuvastamise sertifikaadiga autenditava kasutaja ülesseadmine käib järgmiselt:

1. Looge kasutajale konto:

```
> adduser --disabled-password kasutajanimi
> usermod -a -G www-data kasutajanimi
```

2. Salvestage kasutaja ID-kaardi isikutuvastamise sertifikaat PEM-vormingus faili `usercert.cer`;

3. Eraldage sertifikaadist kasutaja avalik võti ja salvestage see faili `userpubkey.pem`:

```
> openssl x509 -in usercert.cer -pubkey -noout > userpubkey.pem
```

4. Teisendage avalik võti PKCS#8 vormingusse, varustage kasutaja tunnusega ja salvestage see SSH volitatud kasutajate faili `/etc/ssh/kasutajad`:

```
> KEY=`ssh-keygen -i -m PKCS8 -f userpubkey.pem`
> echo "$KEY kasutaja@eesti.ee" >> /etc/ssh/kasutajad
```

5. Kontrollige, kas lisatud kirje on kujul `ssh-rsa PKCS8-võti kasutajatunnus`:


```
> tail -1 /etc/ssh/kasutajad  
ssh-rsa AAAAB3NzaC1yc2EAAAELGuiTAAAAIEAxZf/TuSrGJEU1PlfkY9jJ33VOYVZ9Vao0Uiytlf8  
7HJu/78fCIB7m05J7ibpMhsZoZ4DElU7ve0VwbvdDS3srh1OhiQcUjpnTlx4rIMlVkHwadrHtmF+BNi  
DwbLbbdD5y3puGcLH+sLuwba6Vuc3aU0QuqzenYmY9pV7w9y0wc= kasutaja@eesti.ee
```

Ühised tegevused seadistusperioodil

Selles jaotises kirjeldatud tegevused on ühised keskkondadele HES, HTS ja HLR. Neile tegevustele omakorda järgnevad protseduurid on üldjoontes iga serveri jaoks erinevad ning leiavad seetõttu käsitlemist igas jaotises eraldi: *HES protseduurid* (lk 25), *HTS protseduurid* (lk 29), *HLR protseduurid* (lk 33).

Kõige esimene seadistustegevus on kõigis keskkondades *sertifikaatide konfiguratsiooni laadimine* (lk 15), HESi ja HTSi puhul on kasulik ka *testida logiteadete jõudmist jälgimisjaama* (lk 15).

Pärast esmaste seadistuste rakendamist on süsteemiülemal kaks võimalikku lähenemisviisi:

- muuta seadistatavaid parameetreid eraldi menüüvalikutest;
- muuta seadistatavaid parameetreid tervikuna, kasutades digitaalselt allkirjastatud paigaldusfaili.

Teise lähenemisviisi korral võib süsteemiülem parameetreid hiljem ükshaaval üle kontrollida/häälestada. Mõlema lähenemisviisi korral tuleb lõpuks veenduda konfiguratsiooni korrasolekus. Mõlemat lähenemisviisi saab kasutada ka olukorras, kus on vaja valimisinfort muuta.

3.1 Jälgimisjaama logimise testimine

HESi ja HTSi seadistamise alguses on kasulik testida, kas serveris genereeritud logiteated jõuavad jälgimisjaama logidesse.

HES ja HTS genereerivad iga minuti järel süsteemi statistikat sisaldavad logiteated. Nende ilmumist jälgimisjaama logidesse saab näha käsuga:

```
> tail -f /var/log/ivote-monitor/*-monitoring.log
...
^C
```

Kui logiteateid ei ilmu, siis võib kontrollida, kas jälgimisjaama `syslog` teenusel on korrektsed sätted (vt. *syslog* (lk 10)), kas HESi ja HTSi jaoks on logiserver korrektselt määratud (käsud `dpkg-reconfigure evote-hes` ja `dpkg-reconfigure evote-hts`) ja kas võrgukonfiguratsioon võimaldab teadete jõudmise jälgimisjaama.

3.2 Sertifikaatide konfiguratsiooni laadimine

Sertifikaatide konfiguratsiooni laadimisega luuakse vajalikud eeldused digitaalselt allkirjastatud failide kontrolliks.

E-hääletamise süsteem toetab allkirjastatud sisendfailide ja hääle töötlemiseks BDOC 2.1 digitaalallkirja vormingut.

3.2.1 Konfiguratsioonifaili redigeerimine

Digitaalallkirjade ja kehtivuskinnituste kontrolli tarbeks tuleb süsteemi laadida konfiguratsioonipakk, mis määrab BDOC häälestuse. Näidiskonfiguratsioon tarnitakse kataloogis `kesksüsteem/test-config`. Konfiguratsioonis tuleb määrata OCSP responderi aadress, OCSP responderi sertifikaadid ning CA sertifikaadid. Samuti tuleb näidata BDOC verifitseerimiseks vajalikud XML-failid.

Konfiguratsioonipaki struktuur on kahetasemeline:

```
JUURKATALOOG\
  bdoc.conf
  CA\
  OCSP\
  SCHEMA\
```

Kataloog CA sisaldab PEM vormingus CA sertifikaate. Failid peavad vastama järgmistele tingimustele:

- Fail on PEM vormingus;
- Fail on UNIXi reavahetustega;
- Fail sisaldab üht ja ainult üht sertifikaati.

CA kataloogis peavad olema kõik sertifikaadid nendest ahelatest, kust väljastatakse ID-kaardi, Digi-ID ja Mobiil-ID sertifikaate. Teistest ahelatest sertifikaate CA kataloogis olla ei tohi.

Teadaolevalt peavad CA kataloogis olema järgmised sertifikaadid:

Sertifikaat	SHA-1 räsi
Juur-SK	409D 4BD9 17B5 5C27 B69B 64CB 9822 440D CD09 B889
EE Certification Centre Root CA	C9A8 B9E7 5580 5E58 E353 77A7 25EB AFC3 7B27 CCD7
ESTEID-SK 2007	305D 9B27 3E69 8527 625B 64CC CBAF BFDB 32A6 4264
ESTEID-SK 2011	4626 7416 F753 B312 8062 230F 9C1F B0AB 7D3E EC1A

Kataloog OCSP sisaldab PEM vormingus OCSP responderite sertifikaate. Failid peavad vastama järgmistele tingimustele:

- Fail on PEM vormingus;
- Fail on UNIXi reavahetustega;
- Fail sisaldab üht ja ainult üht sertifikaati.

OCSP kataloogis peavad olemas responderite sertifikaadid, mis väljastavad kinnitusi CA kataloogis paiknevate CAde poolt väljastatud sertifikaadide kohta. Teadaolevalt peavad OCSP kataloogis olema järgmised sertifikaadid:

Sertifikaat	SHA-1 räsi
ESTEID-SK 2007 OCSP RESPONDER 2010	C5D9 E7BB A16E A652 CA01 34CB 7E61 C579 CD63 8F46
SK OCSP RESPONDER 2011	7539 613C 0FE7 9F90 678E 3059 B33D 8E6F F430 0E9C

Kataloog SCHEMA sisaldab järgmisi e-hääletuse plaadil tarnitud faile:

- `datatypes.dtd`
- `XadES.xsd`
- `xades-signatures.xsd`
- `xmldsig-core-schema.xsd`
- `XMLSchema.dtd`

Fail `bdoc.conf` võib välja näha näiteks järgmine:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="schema/conf.xsd">

  <param name="digest.uri">http://www.w3.org/2001/04/xmllenc#sha256</param>
```

```
<ocsp issuer="ESTEID-SK 2007">
  <url>http://ocsp.sk.ee/</url>
  <cert>ESTEID-SK 2007 OCSP RESPONDER 2010.crt</cert>
  <skew>300</skew>
  <maxAge>60</maxAge>
</ocsp>

<ocsp issuer="ESTEID-SK 2011">
  <url>http://ocsp.sk.ee/</url>
  <cert>SK OCSP RESPONDER 2011.crt</cert>
  <skew>300</skew>
  <maxAge>60</maxAge>
</ocsp>

</configuration>
```

Parameeter `digest.uri` viitab räsifunktsioonile, mida kasutatakse kehtivuskinnituse võtmisel.

Grupp OCSP seadistab OCSP responderi nende kliendisertifikaatide tarbeks, mille väljaandja CN on `issuer`. Märgendiga `<cert>` tähistatud sertifikaat peab asuma OCSP kataloogis. Väljaandja CN-ile vastav sertifikaat peab asuma CA kataloogis. Seadistusfailis võib olla mitu gruppi.

3.2.2 Konfiguratsioonifaili laadimine

Konfiguratsioonifaili laadimiseks tuleb tegutseda järgmiselt:

1. Valige menüüst *Üldine konfiguratsioon* → *Laadi sertifikaatide konfiguratsioon*;
2. Sisestage konfiguratsiooni asukoht (näiteks `/home/evote/bdoc`).

Laadimise tulemuse kohta kuvatakse sellekohane teade.

Tähelepanu:

- Konfiguratsioonipakki saab välja vahetada ainult tervikuna;
- Kuna HESis kasutatakse sertifikaatide konfiguratsiooni ka veebiserveri sätetes, siis taaskäivitab konfiguratsiooni laadimine ka veebiserveri. Selleks nõutakse kasutaja `hes` parooli.

3.3 Serveri häälestamine parameeter-haaval

Parameeterhaaval häälestades tuleb igas serveris iga toimuva valimise kohta seadistada

- valimisidentifikaator;
- valimise kirjeldus;
- volitatud isikud;
- valimisinfo.

3.3.1 Valimisidentifikaatori sisestamine

Enne hääletuse algust tuleb luua VVK nõutavale valimisidentifikaatorile vastav olekupuuharu. Valimisidentifikaatorid on osapooltele (HES, HTS, HLR) ühised. Sisestatud identifikaatori nime pole hiljem enam võimalik muuta, küll aga on võimalik seda seadistusperioodil (ja ainult seadistusperioodil) kustutada.

1. Valige peamenüüst *Loo uus valimisidentifikaator*;
2. Sisestage VVK nõutav valimise identifikaator, näiteks `RKTEST2015`. Olekupuusse luuakse uus sellenimeline haru;

3. Sisestage valimiste tüüp, milleks võib olla üks neljast valikuvariandist: rahvahääletus, kohalike omavalitsuste valimised, riigikogu valimised, europarlamenti valimised;
4. HTSi kasutajaliideses tuleb sisestada valimiste selgitav kirjeldus (näiteks Riigikogu valimised 2015). Teistes serverites pole seda võimalik teha. Kirjeldust on võimalik hiljem muuta.

Sisestage valimiste identifikaator: RKTEST2015
Loon HES olekupu kataloogi: evconfig/questions/RKTEST2015
Loon alamkataloogi common/rights
Loon alamkataloogi hes
Loon alamkataloogi hes/voters
Lõpetasin töö edukalt

3.3.2 Valimiste kirjelduse muutmine

Valimisidentifikaatorit selgitavat kirjeldust saab sisestada ja muuta ainult HTSi kasutajaliideses.

1. Valige peamenüüst *Tegele valimistega* ning soovitud valimise identifikaator;
2. Valige menüüst *Konfigureeri* → *Muuda valimiste kirjeldust*;
3. Sisestage uus valimiste kirjeldus.

3.3.3 Volitatud isikute määramine

Enamik e-hääletamise süsteemis kasutusel olevatest nimekirjadest peavad olema digitaalselt allkirjastatud. Selleks, et süsteemi saaks importida ainult VVK volitatud isikute poolt allkirjastatud nimekirju, tuleb süsteemis määrata volitatud isikud. Volitusi on kolme tüüpi:

1. Jaoskondade ja ringkondade nimekirja allkirjastajad;
2. Valikute nimekirja allkirjastajad (ainult HESis ja HLRis);
3. Tühistus- ja ennistusnimekirja allkirjastajad (ainult HTSis).

Tähelepanu: Igat tüüpi volitatud isikuid peaks olema vähemalt kaks, et tagada käideldavus juhuks, kui ühel isikul pole võimalik oma kohuseid täita.

Volituste andmiseks tuleb tegutseda järgmiselt:

1. Valige menüüst “Tegele valimistega” ning käimasoleva valimise identifikaator;
2. Valige menüüst *Konfigureeri* → *Volitused*;
3. Valige menüüst *Anna isikule volitused*;
4. Sisestage volitatud töötaja isikukood (isikukoodid koos neile määratud volituste tüübiga edastab VVK);
5. Valige volituse tüüp või valik *Kõik volitused*.

Kasutajale kuvatakse teade volituse andmise õnnestumise või nurjumise kohta.

Süsteem salvestab vastavate volitustega kasutaja. Isikule kirjelduse (nime) lisamiseks tuleb jääda samasse menüüsse ja tegutseda järgmiselt:

1. Valige menüüst *Anna isikule kirjeldus*;
2. Sisestage isikukood;
3. Sisestage isiku kirjeldus (näiteks “Tamm, Jaan”).

Süsteem salvestab isikukoodile vastava kirjelduse.

3.3.4 Valimisinfo laadimine

Valimisinfot saab laadida ainult enne hääletamisperioodi algust.

1. Valige peamenüüst *Tegele valimistega* ning käesoleva valimise identifikaator;
2. Valige *Konfigureeri*
3. Sõltuvalt serverist valige kas *Laadi HES valimiste failid*, *Laadi HTS valimiste failid* või *Laadi HLR valimiste failid*;
4. Sisestage BDOC-vormingus valimisjaoskondade/-ringkondade faili asukoht. Näiteks: `/dvd/districts.RKTEST2015.bdoc`;
5. Sisestage BDOC-vormingus valikute faili asukoht. Valikute fail sisaldab, sõltuvalt valimiste tüübist, kandidaatide või vastusevariantide digiallkirjastatud nimekirju. Näiteks: `/dvd/choices.RKTEST2015.bdoc`;
6. Sisestage valijate faili asukoht. Näiteks: `/dvd/voters.RKTEST2015`.
7. Sisestage valijate faili signatuuri avaliku võtme asukoht. Näiteks: `/dvd/pubkey.pem`.

Süsteem kontrollib valimisringkondade ja valikute failide signatuuri ning signeerijate volitusi, samuti ka ringkonna olemasolu ning valiku unikaalsust. Valijate faili puhul kontrollitakse faili signatuuri vastavust avalikule võtmele. Failides olevad jaoskonnad, valikud ja valijad salvestatakse serveri valimisinfo koosseisu. Protseduuri käigu kohta kuvatakse infot, näiteks:

```
Valimised: RKTEST2015
Kontrollin jaoskondade faili volitusi
Kontrollin jaoskondade nimekirja: 100%
Jaoskondade nimekiri OK
Kontrollin valikute faili volitusi
Kontrollin valikute nimekirja: 100%
Valikute nimekiri OK
Kontrollin valijate faili avalikku võtit
Kontrollin valijate faili terviklikkust
Valijate nimekiri OK
Paigaldatud 45 ringkonda ja 135 jaoskonda
Paigaldatud 5000 valikut
Paigaldan valijate faili võtit
Võti on paigaldatud
Sulgen baase
. . . . .
Valijad on paigaldatud. Teostati 100000 lisamist ja 0 eemaldamist
Valimiste failide laadimine oli edukas
```

Tähelepanu: Serveris HLR valijate nimekirja ega selle signatuuri avalikku võtit ei laadita.

3.3.5 Valijate nimekirja uuendamine

Valijate nimekirja uuendamine toimub vaid HESIS ja HTSis. HLRis valijate nimekirja ei kasutata.

Seadistusperioodil on võimalik teostada valijate nimekirja kõiki uuendusi: lisamine, kustutamine ja muutmine (ehk kustutamine + lisamine).

Hääletusperioodil on võimalik valijate nimekirja isikuid lisada ja neid sealt kustutada. Kustutamine on võimalik vaid kahel juhul: kui põhjuseks on tõkendi rakendamine või jaoskonna vahetus. Eemaldamiskirjete failis võib olla antud ka muu põhjus, kuid hääletamisperioodil keeldub e-hääletuse süsteem selliseid kirjeid sisaldavaid faile töötlemast.

Pärast hääletusperioodi lõppu pole valijate nimekirju enam võimalik uuendada.

Valijate nimekirja uuendamiseks tuleb tegutseda järgnevalt:

1. Valige peamenüüst *Tegele valimistega* ning käesoleva valimise identifikaator;

2. Valige *Konfigureeri* → *Laadi valijate faili täiendused*;

3. Sisestage valijate faili asukoht. Näiteks: `/dvd/voters.RKTEST2015_changes`

Juhul, kui nimekirja laadimisel tekiks lahknevusi (näiteks üritatakse eemaldada valijat, keda nimekirjas polnud), nõutakse jätkamiseks kinnitust. Rakendatakse ainult kooskõlalisi andmeid. Kõik laadimisel tekkinud veateated ja lahknevused kantakse logifaili `valijate_nimekirjade_vigade_logi`, mida saab sirvida operaatori kasutajaliidese kaudu.

Süsteem lisab failis olevatest lisamise tüübiga kirjetest valijate andmed, kontrollib valija unikaalsust (isikukoodi alusel) ning valimisjaoskonna olemasolu. Toiminguga lõppedes väljastatakse teave lisamiste ja eemaldamiste kohta, näiteks:

```
Teostasin 7 lisamist ja 13 eemaldamist
Muudatuste rakendamine lõppes edukalt
```

3.3.6 Nimekirjade uuendamise ajaloo vaatamine

Jaoskondade ja valikute nimekirjade ajalugu kuvatakse kõigis serverites. Valijate nimekirjade ajalugu kuvatakse vaid HESis ja HTSis. HLRis valijate nimekirja ei kasutata.

Nimekirjade serverisse laadimise ajaloo vaatamiseks tuleb peamenüüst valida *Üldine konfiguratsioon* → *Nimekirjade uuendamise ajalugu*. Selle tulemusena kuvatakse teavet kõigi käimasolevate valimiste käigus nimekirjadega tehtud toimingute kohta, näiteks:

```
RKTEST2015
  Jaoskondade nimekiri
  01. 2015.01.01 18:08:22 - RKTEST2015.districts.bdoc
      D491AB52 7472F286 59DBD2B6 B7F4ED10
      D8D68865 F523BC2B 0E466D7E 813C6681

  Valikute nimekiri
  01. 2015.01.01 18:12:49 - RKTEST2015.choices.bdoc
      8332969D 0596C421 008AE2AE A7EA90FB
      6F232527 E366AFCA 8B214584 BAA50040

  Valijanimekirjad
  01. 2015.01.01 18:15:29 - RKTEST2015.voters
      0546BBE8 5F0CC3F4 26F3F594 10B430B9
      ABCAE2B2 ED2E5447 55C9D311 DC32C515
      Algne: lisamisi 2, eemaldamisi 0
      Kokku peale laadimist: 2

  02. 2015.01.01 21:20:45 - RKTEST2015.changes.voters
      91FB89A1 156B25B3 DCA2657A 18A67B8F
      A0F6DAE1 B7707DA6 FF2B3FD8 46B692BF
      Muudatused: lisamisi 55, eemaldamisi 0
      Kokku peale laadimist: 57
```

Märkus: Kui nimekirjade loetelu ei mahu korraga ekraanile, saab seda klahvikombinatsioonide `Shift+PageUp` ja `Shift+PageDown` abil üles-alla kerida.

3.4 Serveri häälestamine paigaldusfailiga

3.4.1 Ülevaade protseduurist

Serveri häälestamine paigaldusfailiga lihtsustab mitme serveri seadistamist ja/või serverite korduvat seadistamist. Paigaldusfail on BDOC-vormingus digitaalselt allkirjastatud fail, mis sisaldab endas kogu vajalikku

konfiguratsiooni HES ja HTS tarkvara hääletusperioodi tarbeks seadistamiseks. HLR vajab täiendavalt paigaldusfailile ka HSMi seadistamist.

Protseduur eeldab, et sertifikaatide konfiguratsioon on serverisse laaditud.

1. Valige peamenüüst *Üldine konfiguratsioon* → *Laadi valimiste seaded paigaldusfailist*;
2. Sisestage BDOC-vormingus paigaldusfaili asukoht. Näiteks: `/dvd/RKTEST2015-konfiguratsioon.bdoc`;
3. Paigaldusfaili allkirja kontrollitakse ning tulemuse kohta kuvatakse infot, näiteks:

```
Allkirjastaja: serialNumber=47101010000,GN=EESNIMI,SN=PERENIMI,CN=PERENIMI,
EESNIMI\,47101010000,OU=digital signature,O=ESTEID,C=EE
Kas paigaldame valimised? (jah/ei)?
```
4. Juhul kui allkirjastaja isik ei ole volitatud paigaldusfaili allkirjastama, sisestage küsimusele *Kas paigaldame valimised? (jah/ei)?* vastuseks **ei**. Sel juhul paigaldusfaili ei rakendata;
5. Juhul kui allkirjastaja isik on volitatud paigaldusfaili allkirjastama, sisestage küsimusele *Kas paigaldame valimised? (jah/ei)?* vastuseks **jah**. Sel juhul rakendatakse paigaldusfaili.

Serveris HES asendab paigaldusfaili rakendamine järgmised protseduurid:

- *Valimisidentifikaatori sisestamine* (lk 17);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19);
- *HTSi sätete määramine* (lk 26);
- *Mobiil-ID parameetrite seadistamine* (lk 26).
- *Valimisseansi sätete määramine* (lk 27).

Serveris HTS asendab paigaldusfaili rakendamine järgmised protseduurid:

- *Valimisidentifikaatori sisestamine* (lk 17);
- *Valimiste kirjelduse muutmine* (lk 18);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19);
- *Kontrollitavuse parameetrite määramine* (lk 29).

Serveris HLR asendab paigaldusfaili rakendamine järgmised protseduurid:

- *Valimisidentifikaatori sisestamine* (lk 17);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19).

3.4.2 Paigaldusfaili struktuur

Paigaldusfaili BDOC konteineri sisu koosneb üldisest seadefailist ning iga häälestatava valimise failidest.

- `config` – seadefail (UTF8, Unix-i reavahetused);
- `VALIMISED.valikud.bdoc` – BDOC vormingus valikute fail;
- `VALIMISED.jaoskonnad.bdoc` – BDOC vormingus jaoskondade fail;
- `VALIMISED.hääletajad.txt` – valijate nimekirja.
- `VALIMISED.hääletajad.txt.signature` – valijate nimekirja allkiri;
- `VALIMISED.voterskey` – PEM vormingus avalik võti valijate nimekirja allkirja kontrollimiseks;

Nimekirju võib olla mitme valimise jagu, nende täpsed nimed ei ole kohustuslikud.

Faili config struktuur on järgmine:

Näitefail ühe valimise jaoks:

```
# MOBIIL-ID SEADED
# *. viitab et parameeter on ühtne kõigile käimasolevatele hääletustele
# Ülejäänud sätted on ühe valimise spetsiifilised

# Mobiil-ID teenuse URL
*.mobidurl: https://www.openxades.org:8443/DigiDocService

# Mobiil-ID teenuse nimi
*.mobidservice: Testimine

# Mobiil-ID autentimisteade
*.mobidauthmsg: E-hääletamine, autentimine

# Mobiil-ID allkirjastamisteade
*.mobidsignmsg: E-hääletamine, hääle allkirjastamine

# Hääletamiseaeg maksimaalne kestus minutites
*.sessionlength: 60

# HTS SEADED

# HTS URL ja port
*.hts: 193.40.99.42:80

# Hääle kontrollimise aeg minutites
*.verifytimeout: 30

# Hääle kontrollimise maksimaalne kordade arv
*.verifymaxtries: 3

# Valimiste identifikaatorid. Iga identifikaatori kohta tuleb eraldi blokk
# valimise spetsiifilisi parameetreid
*.elections: RKTEST2015

# Valimise RKTEST2015 failide nimed ja volituse
# Tüüp 2 on Riigikogu
RKTEST2015.type: 2

# Jaoskondade nimekirja laadimise õiguse
# saavad isikukoodid 37101010021 ja 37709270285
RKTEST2015.JAOSK: 37101010021 37709270285

# Valikute nimekirja laadimise õiguse saab isikukood 37101010021
RKTEST2015.VALIK: 37101010021

# Tühistusnimekirjade laadimise õiguse saab isikukood 37101010021
RKTEST2015.TYHIS: 37101010021

# Kõigi nimekirjade laadimise õiguse saab isikukood 47101010033
RKTEST2015.ALL: 47101010033

# Valijate nimekirja faili nimi paigalduspakis
# NB! Pakis peab olema ka vastav signatuurifail
# antud juhul RKTEST2015.voters_1.signature
```

```
RKTEST2015.voters: RKTEST2015.voters_1

# Valikute nimekirja faili nimi paigalduspakis
RKTEST2015.choices: RKTEST2015.choices.bdoc

# Jaoskondade/ringkondade nimekirja faili nimi paigalduspakis
RKTEST2015.districts: RKTEST2015.districts.bdoc

# Valimise kirjeldus
RKTEST2015.description: Riigikogu valimised 2015

# Valijanimekirjade kontrollimise avalik võti
# NB! Tegemist on avaliku võtme, mitte sertifikaadiga
RKTEST2015.voterskey: public_key.pem
```

Näitefail mitme valimise jaoks. Erinevus on mitme identifikaatori defineerimine *.elections real ning igale identifikaatorile vastava bloki defineerimine:

```
# Mobiil-ID seaded
*.mobidurl: https://www.openxades.org:8443/DigiDocService
*.mobidservice: Testimine
*.mobidauthmsg: E-hääletamine, autentimine
*.mobidsignmsg: E-hääletamine, hääle allkirjastamine

# Hääletamiseseansi maksimaalne kestus minutites
*.sessionlength: 60

# HTS seaded
*.hts: 193.40.99.42:80
*.verifytimeout: 30
*.verifymaxtries: 3

# Valimiste identifikaatorid
*.elections: RKTEST2015 RHTEST2015

# Valimise RKTEST2015 failide nimed ja volitused
RKTEST2015.type: 2
RKTEST2015.ALL: 37101010021
RKTEST2015.voters: RKTEST2015.voters_1
RKTEST2015.choices: RKTEST2015.choices.bdoc
RKTEST2015.districts: RKTEST2015.districts.bdoc
RKTEST2015.description: Riigikogu valimised 2015
RKTEST2015.voterskey: public_key_rk.pem

# Valimise RHTEST2015 failide nimed ja volitused
RHTEST2015.type: 0
RHTEST2015.JAOSK: 37101010021 37709270285
RHTEST2015.VALIK: 37101010021
RHTEST2015.TYHIS: 37101010021
RHTEST2015.voters: RHTEST2015.voters.txt
RHTEST2015.choices: RHTEST2015.choices.bdoc
RHTEST2015.districts: RHTEST2015.districts.bdoc
RHTEST2015.description: Saaremaa Rahvahääletus 2015
RHTEST2015.voterskey: public_key_rh.pem
```

HTS seadistus HESis erineb võrreldes jaotisega *HTSi sätete määramine* (lk 26), kuna määratakse vaid IP-aadress ja port. URLide jaoks kasutatakse vaikeväärtuseid /hts.cgi ja /hts-verify-vote.cgi. Väärtuste hilisem muutmine on võimalik HESi kasutajaliideses.

3.5 Konfiguratsiooni kontrollimine

Konfiguratsiooni kontrollimiseks tuleb peamenüüst valida *Vaata konfiguratsiooni hetkeseisu*, mille peale kuvatakse andmed serveri sätete ja kõigi serveri andmetes kirjeldatud valimiste kohta:

Laaditud konfiguratsiooniandmed:

```
Valimisidentifikaator(id) - olemas
  "RKTEST2015" jaosk., valik., häälet. failid - olemas
Sertifikaadid - olemas
HTSi konfiguratsioon - olemas
  HTSi IP aadress: 10.10.10.6:80
  HTSi URL: /hts.cgi
  HTSi hääle kontrolli URL: /hts-verify-vote.cgi
Mobiil-ID konfiguratsioon - olemas
  DigiDocService URL: https://www.openxades.org:9443
  Teenuse nimi: Testimine
  Teade autentimisel: E-hääletamine, autentimine
  Teade signeerimisel: E-hääletamine, hääle allkirjastamine
Seansi konfiguratsioon - olemas
  Valimisseansi kehtivusaeg minutites: 60
```

Süsteem lubab hääletusperioodi algatada vaid siis, kui kõik nõutud andmed on laaditud ja korrektsed.

3.6 Valimisinfo muutmine

Valimisinfo muutmine on võimalik vaid seadistus- ja hääletusperioodidel. Seadistusperioodil on võimalik muuta kogu valimisinfot, hääletamisperioodil vaid valijate nimekirju.

Seadistusperioodi valimisinfo muutmiseks tuleb kõigis muudatusest mõjutatud serverites toimida järgnevalt:

- *Kustutada muutmist vajav valimisidentifikaator* (lk 24);
- *Laadida uuenenud valimisinfo* (lk 24).

3.6.1 Valimisidentifikaatori kustutamine

Valimisidentifikaatori kustutamine kustutab kogu identifikaatoriga seotud info.

Valimisidentifikaatori kustutamiseks tuleb toimida järgnevalt:

1. Valige peamenüüst *Kustuta valimisidentifikaator*;
2. Sisestage valimisidentifikaator, mida soovite eemaldada (näiteks RKTEST2015);
3. Kui kustutamine õnnestub, siis kuvab süsteem peamenüüd ilma valimisidentifikaatorita.

3.6.2 Uuenenud valimisinfo laadimine

Uuenenud valimisinfo laadimiseks tuleb läbi viia üks kahest protseduurist:

- 3.2 *Serveri häälestamine parameeter-haaval* (lk 17); või
- 3.3 *Serveri häälestamine paigaldusfailiga* (lk 20).

HES protseduurid

Hääleedastusserver on töös seadistusperioodil ja hääletusperioodil. Tühistusperioodis ja lugemisperioodis HES ei osale.

4.1 Seadistusperiood

Enne järgmiste alajaotiste täitmist tuleb alltoodud järjekorras läbida seadistusperioodi protseduurid, mida kirjeldab jaotis *Ühised tegevused seadistusperioodil* (lk 15):

- *Jälgimisjaama logimise testimine* (lk 15);
- *Sertifikaatide konfiguratsiooni laadimine* (lk 15);
- *Valimisidentifikaatori sisestamine* (lk 17);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19);
- *Konfiguratsiooni kontrollimine* (lk 24).

Mitme HESi kasutamise korral tuleb kõik toimingud iga HESi puhul eraldi läbi viia.

4.1.1 HESi veebiserveri seadistamine

Koos HESi tarkvaraga paigaldatakse masinasse ka veebiserveri vaikekonfiguratsioon, mis sisaldab muuhulgas ka veebiserveri sertifikaati ja klientide autentimiseks vajalikke sertifikaate. Enne HESi reaalsesse kasutusse andmist tuleb sertifikaatide konfiguratsioon üle vaadata.

Konfiguratsioon paikneb failis `/etc/apache2/sites-enabled/hes-apache`.

Nõuanne: Veebiserveri sätete korrektsuse kontrollimiseks on võimalik kasutada käsku:

```
> apachectl configtest
```

Serveri autentimine

Direktiiv `SSLCertificateFile` määrab veebiserveri autentimiseks kasutatava sertifikaadifaili raja:

```
SSLCertificateFile /etc/evote/ssl/webcert.pem
```

Direktiiv `SSLCertificateKeyFile` määrab direktiivis `SSLCertificateFile` näidatud sertifikaadile vastava privaatvõtme faili raja:

```
SSLCertificateKeyFile /etc/evote/ssl/webkey.pem
```

Direktiiv `SSLCertificateChainFile` määrab veebiserveri sertifikaadi usaldamiseks vajaliku KLASS3 CA sertifikaati sisaldava PEM-vormingus faili raja:

```
SSLCertificateChainFile /etc/evote/ssl/cacert.pem
```

Antud sertifikaati kasutavad kontrollrakendused HESi sertifikaadi kehtivuse verifitseerimiseks. Kuna verifitseerimine toimub CA Juur-SK suhtes ning vastav sertifikaat on kontrollrakendustele kaasa pakendatud, tuleb Apache seadistusfaili panna üks ja ainult üks SK sertifitseerimishierarhia sertifikaat, mis vastab järgnevatele parameetritele:

```
Serial Number: 1270027048 (0x4bb31328)
Issuer: emailAddress=pki@sk.ee, C=EE, O=AS Sertifitseerimiskeskus, CN=Juur-SK
Validity
  Not Before: Mar 31 09:17:28 2010 GMT
  Not After : Aug 26 14:23:01 2016 GMT
  Subject: C=EE, O=AS Sertifitseerimiskeskus, OU=Sertifitseerimisteenused,
          CN=KLASS3-SK 2010
```

Valijarakendus sisaldab kõiki HES sertifikaadi verifitseerimiseks vajalikke andmeid ning parameetri `SSLCertificateChainFile` väärtus Valijarakenduse käitumist ei mõjuta.

Kliendi autentimine

Direktiiv `SSLCACertificatePath` määrab klientide autentimiseks vajalikke sertifikaate sisaldava kataloogi raja. Kataloogis peavad sisalduma juursertifikaat ja nende CA'de sertifikaadid, mille poolt väljastatud ID-kaardi sertifikaadid veel kehtivad. Kataloogi sisu määratakse peamenüüst sertifikaatide konfiguratsiooni määra:

```
SSLCACertificatePath /var/evote/registry/common/bdoc/ca
```

4.1.2 HTSi sätete määramine

HES edastab vastu võetavad hääled hääletalteserverisse. Selleks tuleb HESis määrata HTSiga suhtlemise parameetrid.

1. Valige HESi peamenüüst *Üldine konfiguratsioon* → *Säti HTSi konfiguratsioon*;
2. Sisestage hääletalteserveri IP-aadress, port (vaikimisi 80), URL (vaikimisi `/hts.cgi`) ja hääle kontrolli URL (vaikimisi `/hts-verify-vote.cgi`).

Sätete vaatamiseks tuleb valida HESi peamenüüst *Vaata konfiguratsiooni hetkeseisu*.

4.1.3 Mobiil-ID parameetrite seadistamine

Selleks, et hääleedastusserver võimaldaks Mobiil-ID'ga hääletada, tuleb HESis määrata Mobiil-ID teenuse URL, nimi ja autentimis- ning allkirjastamisteed.

1. Valige HESi peamenüüst *Üldine konfiguratsioon* → *Muuda Mobiil-ID sätteid*;
2. Sisestage DigiDocService'i URL, teenuse nimi ning autentimisel ja allkirjastamisel kuvatavad sõnumid.

Sätete vaatamiseks tuleb valida HESi peamenüüst *Vaata konfiguratsiooni hetkeseisu*.

4.1.4 Valimisseansi sätete määramine

Valimisseansi sätete määramisega sisestatakse valimisseansi kehtivusaeg. Selleks tuleb tegutseda järgnevalt:

1. Valige HESi peamenüüst *Üldine konfiguratsioon* → *Muuda valimisseansi sätteid*;
2. Sisestage seansi kestus minutites.

Sätete vaatamiseks tuleb valida HESi peamenüüst *Vaata konfiguratsiooni hetkeseisu*.

4.1.5 Hääletusperioodi automaatse alguse ja lõpu seadistamine

HESis on võimalik määratlda perioodidevahelisteks automaatseteks üleminekuteks järgnevad kellaajad:

- Hääletusperioodi alustamise aeg;
- Nimekirjade väljastamise lõpetamise aeg;
- Ajavahemik nimekirjade väljastamise lõpetamise ja hääletusperioodi lõpetamise vahel.

Kõiki automaatseks määratud tegevusi on võimalik ka tühistada.

Hääletusperioodi automaatseks alustamise aja määramiseks toimige järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Seadista hääletusperioodi automaatne algus*;
2. Süsteem küsib hääletusperioodi algusaega. Sisestage soovitud algusaeg vormingus %d.%m.%Y %H:%M (näiteks 01.11.2015 9:00). Määratud ajal algab hääletusperiood;
3. Süsteem ajastab hääletusperioodi alguse määratud ajale.

Hääletusperioodi automaatse alguse kustutamiseks toimige järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Kustuta hääletusperioodi automaatne algus*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
3. Süsteem kustutab hääletusperioodi automaatse alguse aja.

Hääletusperioodi automaatseks lõpetamise aja määramiseks toimige järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Seadista hääletusperioodi automaatne lõpp*;
2. Süsteem küsib hääletusperioodi lõpuaega. Sisestage soovitud lõpuaeg vormingus %d.%m.%Y %H:%M (näiteks 10.11.2015 9:00). Määratud ajal lõpeb nimekirjade väljastamine;
3. Süsteem küsib vahemikku nimekirjade väljastamise automaatse lõpu ja hääle vastuvõtmise automaatse lõpu vahel. Sisestage soovitud ajavahemik minutites (näiteks 15). Hääle vastuvõtmine lõpeb määratud aja möödudes pärast nimekirjade väljastamise lõpetamist;
4. Süsteem ajastab hääletusperioodi lõpu määratud ajale.

Hääletusperioodi automaatse lõpetamise aja kustutamiseks toimige järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Kustuta hääletusperioodi automaatne lõpp*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
3. Süsteem kustutab hääletusperioodi automaatse lõpu aja.

4.1.6 Serverite ühtsuse kontroll

Hääleedastusserver võimaldab kontrollida, kas HESi ja HTSi valijanimekirjad on identsed. Kuna mõlemasse serverisse laaditakse töö käigus valijanimekirjade uuendusi, on serverite ühtsuse kontrolli kasulik teha alati pärast valimisinfo ja selle uuenduste laadimist.

Kontrollimiseks tuleb valida HESi peamenüüst *Kontrolli HES ja HTS serverite kooskõllisust*.

4.1.7 Seadistusperioodi lõpetamine

Seadistusperioodi lõpetamine toimub hääletusperioodi alustamise käigus ja on kirjeldatud lõigus *Hääletusperioodi alustamine* (lk 28).

4.2 Hääletusperiood

Toimub häälte vastuvõtmine ja talletamine.

4.2.1 Hääletusperioodi alustamine

Kui olete veendunud, et server on korrektse alginfoga seadistatud (pärast seadistusperioodi pole enam võimalik alginfot määrata!), siis tuleb seadistusperioodi lõpetamiseks ja hääletusperioodi alustamiseks tegutseda järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Alusta hääletusperioodi*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**. Seadistusperiood lõpeb ja algab hääletusperiood.

4.2.2 Hääletusperioodi lõpetamise alustamine

Hääletusperioodi lõppedes on võimalik peatada kandidaatide nimekirjade väljastamine valijatele, samal ajal jätkuvalt hääli vastu võttes. See loob tingimused selleks, et uusi valijaid enam ei lisandu, kuid need, kel protseduur pooleli, saavad oma hääle siiski edastada.

1. Valige peamenüüst *Üldine konfiguratsioon* → *Lõpeta nimekirjade väljastamine*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**.

Kui nimekirjade väljastamine sai peatatud ekslikult, siis on võimalik väljastamist taastada:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Taasta nimekirjade väljastamise*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**.

4.2.3 Hääletusperioodi lõpetamine

Kui olete veendunud, et kõik hääled on talletatud, tuleb HESi lõppolekusse viimiseks tegutseda järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Lõpeta hääletusperiood*.
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**. HES viiakse seisuga "Hääletusperioodi lõpp".

HTS protseduurid

Hääletalletusserver on töös seadistusperioodil, hääletusperioodil ja tühistusperioodil. Lugemisperioodis HTS ei osale.

5.1 Seadistusperiood

Enne järgmiste alajaotiste täitmist tuleb läbida seadistusperioodi protseduurid, mida kirjeldab jaotis *Ühised tegevused seadistusperioodil* (lk 15):

- *Jälgimisjaama logimise testimine* (lk 15);
- *Sertifikaatide konfiguratsiooni laadimine* (lk 15);
- *Valimisidentifikaatori sisestamine* (lk 17);
- *Valimiste kirjelduse muutmine* (lk 18);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19);
- *Konfiguratsiooni kontrollimine* (lk 24).

5.1.1 Kontrollitavuse parameetrite määramine

Kontrollitavuse parameetrite määramiseks tuleb tegutseda järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Seadista kontrollitavus*;
2. Sisestage ajapiirang hääle kontrollimiseks minutites. Piirang määrab, kui kaua on valijal pärast hääletamist võimalik oma häält kontrollida;
3. Sisestage lubatud arv kordusi hääle kontrollimiseks.

Sätete vaatamiseks tuleb valida HTSi peamenüüst *Vaata konfiguratsiooni hetkeseisu*.

5.1.2 Seadistusperioodi lõpetamine

Seadistusperioodi lõpetamine toimub hääletusperioodi alustamise käigus ja on kirjeldatud lõigus *Hääletusperioodi alustamine* (lk 30).

5.2 Hääletusperiood

Hääletusperioodil toimub hääle vastuvõtmine ja talletamine.

5.2.1 Hääletusperioodi alustamine

Kui olete veendunud, et server on korrektse alginfoga seadistatud (pärast seadistusperioodi pole enam võimalik alginfot määrata!), siis tuleb seadistusperioodi lõpetamiseks tegutseda järgnevalt:

1. Valige peamenüüst *Üldine konfiguratsioon* → *Alusta hääletusperioodi*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**. Seadistusperiood lõpeb ja algab hääletusperiood.

5.2.2 Hääletusperioodi lõpetamine

Sellel sammul toimub automaatselt korduvate hääle tühistamine ja e-hääletanute nimekirja koostamine.

1. Valige peamenüüst *Üldine konfiguratsioon* → *Alusta tühistusperioodi*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**. Hääletusperiood lõpeb ja algab tühistusperiood.

Tähelepanu: Hääletusperioodi lõpetamise järel eraldage HTS võrgust! Tühistusperioodil peab HTS olema vallasrežiimis!

Hääletusperioodi lõppedes kuvatakse statistilist infot etapi käigus töödeldud andmete kohta, näiteks:

```
RKTEST2015
Vastuvõetud hääle koguarv: 5000
Tühistatud korduvate hääle arv: 0
Hääletanute nimekirja kantud kirjete arv: 5000
```

5.2.3 E-hääletanute nimekirja eksportimine ja VIS'ile edastamine

Pärast üleminekut tühistusperioodi on võimalik e-hääletanute nimekirja eksportimine DVD-plaadile. Nimekirja on võimalik eksportida lihttekstina ja printimiseks sobilikus PDF vormingus.

1. Valige HTSi peamenüüst *Tegele valimistega* ning valimise identifikaator;
2. Valige *Eksporti*;
3. Valige kas *E-hääletanute nimekiri* või *E-hääletanute nimekiri (PDF)*;
4. Meediumile kirjutamine toimub vastavalt lõigule *DVD-plaatide kirjutamine* (lk 41).

VIS'ile edastamiseks vajalikud failid asuvad kirjutatud plaadil kataloogis `/evote-YYYYmddHHMMSS/XXXX`, kus YYYYmddHHMMSS on faili genereerimise kuupäev koos kellaaajaga ja XXXX on valimiste identifikaator.

Lihttekstilises vormingus kirjutatud plaat on sobiv VIS'ile edastamiseks. Plaadil asuvad järgmised failid:

- `haaletanute_nimekiri` - hääletanute nimekiri;
- `haaletanute_nimekiri.sha256` - hääletanute nimekirja kontrollsumma.

PDF-vormingu korral asub plaadil fail `haaletanute_nimekiri.pdf`, mis sisaldab hääletanute nimekirja printimiseks ettevalmistatud kujul.

5.3 Tühistusperiood

Tühistusperioodil koostatakse vaheauditi aruanne, tühistatakse korduvad hääled ja koostatakse hääletanute nimekiri ning loendamisele minevate hääle nimekiri.

5.3.1 Volituste andmine tühistus- ja ennistusnimekirjade laadijatele

VVK-st lähtuvad tühistuste ja kinnituste nimekirjad on digitaalselt allkirjastatud. Tühistus- ja ennistusavalduste failide importimisel kontrollitakse, kas nimekirjade allkirjastajad on kantud süsteemi volitatud laadijateks.

1. Valige HTSi peamenüüst *Tegele valimistega* ning käimasoleva valimise identifikaator;
2. Valige *Konfigureeri* → *Volitused*;
3. Valige *Anna isikule volitused*;
4. Sisestage volitatud tühistus-/ennistusnimekirja laadija isikukood;
5. Võimalike volituste seast valige *Tühistus- ja ennistusnimekirja laadija*.

Kasutajale kuvatakse teade volituse andmise õnnestumise või nurjumise kohta. Vajadusel korrake punkte 3-5 teiste volitatud isikute jaoks.

5.3.2 Tühistusavalduste faili import

Selle toiminguga käigus tuleb valimisjaoskondade koostatud, maakonna valimiskomisjonide poolt üle vaadatud ja VVK volitatud tühistaja poolt digitaalselt allkirjastatud tühistuskanded importida HTSi. Tühistusavaldusi on võimalik importida ainult tühistusperioodil.

1. Valige HTSi peamenüüst *Tegele valimistega* ning käimasoleva valimise identifikaator;
2. Valige *Rakenda tühistus/ennistusnimekirja*;
3. Sisestage tühistusnimekirja faili asukoht.

Protseduuri õnnestumisel kuvatakse nimekiri tühistamistest koos tulemusega.

5.3.3 Tühistamise ennistusavalduste faili import

Juhul, kui tuvastatakse, et mingi tühistamine oli teostatud ekslikult, siis on võimalik tühistamise ennistusavalduse alusel hääli ennistada. Protseduuri käigus impordib operaator VVK poolt kinnitatud, VVK volitatud tühistaja digitaalselt allkirjastatud ennistuskanded HTSi.

1. Valige HTSi peamenüüst *Tegele valimistega* ning käimasoleva valimise identifikaator;
2. Valige *Rakenda tühistus/ennistusnimekirja*;
3. Sisestage ennistusnimekirja faili asukoht.

Protseduuri õnnestumisel kuvatakse nimekiri ennistamistest koos tulemusega.

5.3.4 Vaheauditi läbiviimine

Vaheauditi käigus kontrollitakse serveri andmestruktuuride kooskõlalisust ja talletatud häälte terviklust.

1. Valige HTSi peamenüüst *Audit* → *Genereeri vaheauditi aruanne* või *Audit* → *Genereeri vaheauditi aruanne hääli verifitseerimata*. Verifitseerimise korral loetletakse üles kõik süsteemis talletatud hääled ning kontrollitakse iga talletaja kohta tema viimasena antud hääle digitaalselt allkirjastatavusest. Kui hääli ei verifitseerita, siis tuvastab süsteem lihtsalt erinevat liiki talletatud häälte arvu.
2. Audititulemuste kuvamiseks valige peamenüüst *Audit* → *Vaata vaheauditi aruannet*.

Audititulemuste eksportimiseks DVD-plaadile tuleb tegutseda järgnevalt:

1. Valige peamenüüst *Tegele valimistega* ning valimise identifikaator;
2. Valige menüüst *Ekspordi*;
3. Valige menüüst *Vaheauditi aruanne*;
4. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;

5. Meediumile kirjutamine toimub vastavalt lõigule *DVD-plaatide kirjutamine* (lk 41).

5.3.5 Tühistusperioodi lõpetamine

1. Valige peamenüüst *Üldine konfiguratsioon* → *Alusta lugemisperioodi*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**. Tühistusperiood lõpeb ja algab lugemisperiood.

Koos tühistusperioodi lõpetamisega toimub automaatselt ka lugemisele minevate häälte faili koostamine. Selle käigus salvestab süsteem nimekirja välisele andmekandjale, väljastab ekraanile vastuvõetud häälte koguarvu, tühistatud korduvate häälte arvu, ja e-hääletanute nimekirja faili kantud häälte arvu, näiteks:

E-hääletuse peatamine

RKTEST2015

Loendamisele minevate häälte arv: 5000

Avalduse alusel tühistatud häälte arv: 0

5.3.6 Häälte eksportimine pärast tühistusperioodi

1. Valige peamenüüst *Tegele valimistega*, seejärel valige käimasoleva valimise identifikaator;
2. Valige *Ekspordi*;
3. Valige *Loendamisele minevate häälte nimekirja*;
4. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
5. Meediumile kirjutamine toimub vastavalt lõigule *DVD-plaatide kirjutamine* (lk 41).

HLR protseduurid

Häätelugemisrakendus on töös seadistusperioodil ja lugemisperioodil. Hääletus- ja tühistusperioodi jooksul on HLR väljalülitatud olekus.

6.1 Seadistusperiood

Enne järgmiste alajaotiste täitmist tuleb alltoodud järjekorras läbida seadistusperioodi protseduurid, mida kirjeldab jaotis *Ühised tegevused seadistusperioodil* (lk 15):

- *Sertifikaatide konfiguratsiooni laadimine* (lk 15);
- *Valimisidentifikaatori sisestamine* (lk 17);
- *Volitatud isikute määramine* (lk 18);
- *Valimisinfo laadimine* (lk 19);
- *Konfiguratsiooni kontrollimine* (lk 24).

6.1.1 Turvamooduli algseadistamine

1. Valige peamenüüst *Üldine konfiguratsioon* → *Initsialiseeri HSM*;
2. Sisestage HSMi token'i nimi, näiteks: 20150101;
3. Sisestage valimiste-spetsiifilise privaatvõtme nimi, näiteks: `key_priv`;
4. Sisestage PKCS#11 teegi asukoht süsteemis. (Kui pole teisiti määratud, võib kasutada vaikeväärtust.)

6.2 Lugemisperiood

6.2.1 E-häälte ettevalmistamine lugemiseks

Häälte lugemine toimub võrgust eraldatult e. vallasrežiimis. Hääled pärinevad HTSist ja imporditakse HLRi välisel andmekandjal. Lugemine eeldab, et turvamoodul (HSM) on ühendatud serveriga ning serverisse on sisestatud turvamooduli konfiguratsioon.

6.2.2 E-hääle importimine

E-hääli impordib HLRi operaator, abistavad võtmehaldur ja turvamooduli haldur.

1. Täitke juhendi EHA-03-06-2.3 Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Tegevusjuhik punkt 1.2;
2. Valige HLR peamenüüst *Alusta lugemisperioodi*;
3. Asetage hääli sisaldav meedium HLRi seadmesse;
4. Valige HLR peamenüüst *Tegele valimistega* ning käimasoleva valimise identifikaator;
5. Valige *Konfigureeri* → *Impordi hääled lugemiseks*;
6. Sisestage häälefaili (vaikimisi: `loendamisele_minevate_haalte_nimekiri`) asukoht koos failitega. Kui tõrkeid ei esine, naastakse menüüsse.

6.2.3 E-hääle kokkulugemine

1. Valige HLR peamenüüst *Tegele valimistega* ning käimasoleva valimise identifikaator;
2. Valige menüüst *Loe hääled kokku*;
3. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
4. Sisestage turvamooduli PIN-kood. NB! Kood on tõstutundlik.

Kui sisestatud PIN-kood on õige ja tõrkeid ei teki, algab hääle lugemine. Kuna tegu on arvutusmahuka protseduuriga, võib selleks kuluda mitukümmend minutit. Lugemise ajal kuvatakse edenemisnäitrit:

```
Sisesta PIN: XXXX-XXXX-XXXX-XXXX
Dekrüpteerin hääli: 100%
Jagan hääled laiali: 100%
Hääled on jagatud.
Hääled (5000) on loetud.
Aega kulus 00:00:14
```

Protseduuri tulemusena salvestatakse hääletamistulemus süsteemi ja see tuleb eksportida välisele andmekandjale.

Kui hääled on edukalt dekrüpteeritud, tuleb jätkata HSMi partitsiooni deaktiveerimisega vastavalt juhendi EHA-03-06-2.3 Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Tegevusjuhik punktile 1.2.

Tulemuste eksportimiseks DVD-plaadile tuleb tegutseda järgnevalt:

1. Valige peamenüüst *Tegele valimistega* ning valige käimasoleva valimise identifikaator;
2. Valige menüüst *Ekspordi*;
3. Valige *Hääletamistulemus (allkirjadega)*;
4. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
5. Meediumile kirjutamine toimub vastavalt lõigule *DVD-plaatide kirjutamine* (lk 41).

Hääletamistulemus allkirjadega sisaldab endas HSM salajase võtmega signeeritud hääletamistulemust nii ringkondade kui jaoskondade kaupa, koos juhiste signatuuri kontrollimiseks.

6.2.4 Tulemuste sirvimine

Pärast hääle lugemist on võimalik vaadata valimistulemuste logi. Selleks tuleb tegutseda järgmiselt:

1. Valige HLR peamenüüst *Tegele valimistega* ning valimise identifikaator;
2. Valige *Sirvi*;
3. Valige *Arvestatud hääle logi*, kui soovite kuvada faili LOG5;

4. Valige *Hääletamistulemus (ringkondade kaupa)*, kui soovite näha tulemusi ringkondade kaupa;
5. Valige *Hääletamistulemus (jaoskondade kaupa)*, kui soovite näha tulemusi jaoskondade kaupa.

Prooviläbimise korraldamine

Prooviläbimine on protseduur e-hääletuse süsteemi töövalmiduse kontrollimiseks, mida tuleb teha seadistusperioodi lõpus ja mille käigus veendutakse e-hääletuse süsteemi võimes hääli vastu võtta.

Prooviläbimise korraldamiseks võib seadistusperioodil HES ja HTS menüüst valijate nimekirja kontrolli välja lülitada. See võimaldab hääletada kõigil, kellel on harilik (ehk mitte testotstarbeline) ID-kaart. Hääletaja hakkab kuuluma samasse ringkonda, millesse kuulub andmebaasis leiduv esimene laaditud valija. Hääletaja reanumber valijate nimekirjas ning nimi jäävad määramatuks, sest nimekirjade kontrolli väljalülitamisel seda teavet süsteemis pole.

Juhul kui protseduuri läbiviija omab õigust hääletada, tuleb prooviläbimist korraldada ilma valijate nimekirja kontrolli sätteid muutmata.

Juhul kui protseduuri läbiviimiseks keelati valijate nimekirja kontroll tuleb see kontroll enne hääletuse algoleku taastamist uuesti lubada.

Prooviläbimine koosneb jägmistest protsessidest:

1. *Valijate nimekirja kontrolli keelamine* (lk 37);
2. *Valijate nimekirja kontrolli lubamine* (lk 37);
3. *Hääletuse algoleku taastamine* (lk 38).

7.1 Valijate nimekirja kontrolli keelamine

Nimekirjade kontrolli keelamiseks tuleb tegutseda järgmiselt:

1. Valige HES või HTS peamenüüst *Üldine konfiguratsioon* → *Keela hääletajate nimekirja kontroll*;
2. Toimingu õnnestumisel kuvatakse teade *Hääletajate nimekirja kontroll keelatud*.

Tähelepanu: Ära unusta pärast prooviläbimist valijate nimekirja kontrolli tagasi sisse lülitada ja hääletuse algolekut taastada!

7.2 Valijate nimekirja kontrolli lubamine

Nimekirjade kontrolli lubamiseks tuleb tegutseda järgmiselt:

1. Valige HES või HTS peamenüüst *Üldine konfiguratsioon* → *Luba hääletajate nimekirja kontroll*;
2. Toimingu õnnestumisel kuvatakse teade *Hääletajate nimekirja kontroll lubatud*.

7.3 Hääletuse algoleku taastamine

Pärast proovihääletamist on võimalik HES ja HTS viia tagasi algolekusse. Hääletuse algoleku taastamiseks tuleb tegutseda järgmiselt:

1. Valige peamenüüst *Taasta algolek*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
3. Kuna algoleku taastamine kustutab kõik proovihääletamise käigus antud hääled, siis nõutakse veel kord kinnitust. Jätkamiseks sisestage **jah**;

HES/HTS viiakse tagasi seadistusperioodi. Toimingu käigus kustutatakse hääled ja logid.

Süsteemi haldustoimingud

8.1 Serverite ettevalmistamine kiirtaastamiseks

Serverite kiireks taastamiseks tuleb kasutada riist- või tarkvaralist kõvakettapeegeldust, mille seadistamise kirjeldamine jääb selle dokumendi skoobist välja.

8.2 Varukoopiate tegemine

Varukoopiaid on võimalik teha DVDR- ja DVDRW-meediumile. Varukoopiate tegemiseks tuleb tegutseda järgmiselt:

1. Valige peamenüüst *Varunda olekupuud* ja *apache logid*;
2. Kuna varundamise ettevalmistamine nõuab juurkasutaja õigusi, tuleb sisestada kasutaja hes või hts parool;
3. Meediumile kirjutamine toimub vastavalt lõigule *DVD-plaatide kirjutamine* (lk 41).

8.3 Varukoopiast taastamine

Varukoopiast taastamine toimub peamenüü valikust *Taasta olekupuud varukoopiast*.

1. Valige HES või HTS peamenüüst *Taasta olekupuud varukoopiast*;
2. Tegevusele küsitakse kinnitust. Jätkamiseks vastake **jah**;
3. Nõutakse veel kord kinnitust, kuna varukoopiast taastamine kustutab kõik antud hääled. Jätkamiseks sisestage **jah**.

Olekupuud faile ja katalooge loetleb dokument EHK-04-03-1.16 Olekupuud. Koos olekupuuga varundatakse ka veebiserveri Apache logifailid (kataloog `/var/log/apache2`).

8.4 Töö failide ja kataloogidega

8.4.1 Kataloogide sirvimine

Serveri failisüsteemis oleva kataloogis asuvate failide nimekirja vaatamiseks tuleb tegutseda järgmiselt:

1. Valige peamenüüst *Vaata kataloogi sisu*;

2. Sisestage kataloogi nimi;
3. Kataloogi nimekirja sirvimine toimub programmi **less** abi (vaata *Sirvimisprogrammi "less" kasutamine* (lk 41)).

8.4.2 Töö failidega

Operaatori kasutajaliides pakub võimalust valimisega seotud faile sirvida, ning neid ühe- või mitmekaupana DVD-le eksportida.

Failide sirvimine

Valimisega seotud faili sirvimiseks tuleb tegutseda järgmiselt:

1. Valige peamenüüst *Tegele valimistega* ning soovitud valimise identifikaator;
2. Valige *Sirvi*, avaneb nimekiri saadaolevatest failidest;

```
-----  
Peamenüü->Tegele valimistega "RKTEST2015"->Sirvi  
Olek: Hääletusperiood  
-----
```

```
[1] OSCP saadavuse logi  
[2] Rakenduse logi  
[3] Tühistamiste ja ennistamiste aruanne  
[4] Vigade logi  
[5] Tagasi (Ctrl+D)  
htsOperaator>
```

3. Sisestage sirvimiseks kuvatava faili number;
4. Faili sirvimine toimub programmi **less** abi (vaata *Sirvimisprogrammi "less" kasutamine* (lk 41)).

Failide eksportimine

Valimisega seotud faili või failide eksportimiseks tuleb tegutseda järgmiselt:

1. Valige peamenüüst *Tegele valimistega* ning soovitud valimise identifikaator;
2. Valige *Ekspordi*, avaneb nimekiri saadaolevatest failidest;

```
-----  
Peamenüü->Tegele valimistega "RKTEST2015"->Ekspordi  
Olek: Hääletusperiood  
-----
```

```
[1] OSCP saadavuse logi  
[2] Rakenduse logi  
[3] Tühistamiste ja ennistamiste aruanne  
[4] Vigade logi  
[5] Ekspordi kõik failid  
[6] Ekspordi mõned failid  
[7] Tagasi (Ctrl+D)  
htsOperaator>
```

3. Kui soovite ainult tühte faili eksportida, sisestage eksportimisele kuuluva faili number.
4. Kui soovite kõiki faile eksportida, valige *Ekspordi kõik failid*.
5. Kui soovite mitut faili eksportida, valige *Ekspordi mõned failid* ja sisestage komadega eraldatult soovitud failide numbrid menüüs;

```
htsOperaator> 6  
Sisesta eksporditavate failide numbrid komadega eraldatult: 2, 4
```

8.4.3 Sirvimisprogrammi “less” kasutamine

Failide ja kataloogide andmete sirvimiseks kasutatakse turvalises režiimis töötavat programmi **less**. Selles on võimalik kasutada järgmisi klahvikombinatsioone:

- q – vaatest väljumine;
- tühik – kerimine lehekülje võrra edasi;
- b – kerimine lehekülje võrra tagasi;
- / – otsimine (kaldkriipsu järele tuleb sisestada otsisõna ja vajutada `Enter`)

8.5 DVD-plaatide kirjutamine

DVD-plaatide kirjutamine on sarnane kõigil juhtudel (näiteks varukoopia tegemisel ja failide eksportimisel), kus süsteemis seda kasutatakse.

1. Sisestage kirjutatav meedium seadmesse. Ja vastake jätkamise küsimusele **jah**;
2. Sisestage meediumile kirjutamise kiirus;
3. Toimub varukoopia kirjutamine programmi **growisofs** abil. Toimingu käigus kuvab programm edenemisteavet.

8.6 Süsteemsete teadete kohandamine

Süsteemiülevaht saab kohandada lõppkasutajale hääletuse käigus näidatavaid HESi ja HTSi süsteemsete teadeid (sh veateadeid).

Serveri teated tarnitakse tekstifailis kesksüsteem/`teated.example`. Faili vorming on järgmine:

```
# Selgitav kommentaar 1
VÖTMESÕNA1=Kasutajale näidatava teate tekst

# Selgitav kommentaar 2
VÖTMESÕNA2=Kasutajale näidatava teate tekst

...jne
```

Tähelepanu: Teadete faili võtmesõnu ei tohi muuta!

Pärast muudatuste tegemist tuleb teadete fail uuesti laadida. Selleks tuleb tegutseda järgnevalt:

1. Valige HESi või HTSi peamenüüst *Laadi konfigureeritavad teated*;
2. Sisestage teadete faili asukoht;

Süsteem kuvab teate toimumise õnnestumise või nurjumise kohta.

Autoriõigused

© Cybernetica AS 2004-2015

Kõik õigused kaitstud

Cybernetica AS

Mäealuse 2/1

12618 Tallinn

Telefon: 639 7991

Faks: 639 7992

Internet: <http://www.cyber.ee>