IVXV süsteemihalduri juhend

Juhend

Versioon 1.0

20. september 2017

34 lk

Dok IVXV-JSH-1.0

Sisukord

PEATÜKK 1

Annotatsioon

Käesolev juhend käsitleb tööd elektroonilise hääletamise raamistiku IVXV kogumisteenuse tarkvaraga süsteemiülema vaatepunktist ning kirjeldab tarkvara kõiki võimalusi kogu e-hääletusprotsessi ulatuses. Süsteemiülemalt eeldatakse e-hääletuse põhiterminoloogia tundmist.

PEATÜKK 2

Ülevaade

2.1 Kogumisteenuse ülevaade

IVXV kogumisteenus on elektroonilise hääletuse käigus hääletajate teenindamiseks ja häälte kogumiseks mõeldud tarkvara.

Kogumisteenus koosneb mikroteenustest ja nende haldamiseks mõeldud haldusteenusest. Haldusteenuse kasutamine on käsureapõhine. Osade funktsioonide kasutamist on laiendatud veebipõhise liidesega, mida on kirjeldatud dokumendis `IVXV kogumisteenuse haldusliidese kasutusjuhend`.

Tähelepanu: Kogumisteenus paigaldatakse ja seadistatakse eraldi iga hääletuse läbiviimiseks. Ühe kogumisteenusega on korraga võimalik teenindada ainult ühte hääletust.

2.2 Lisamaterjalid

Käesolevas dokumendis kasutatakse mõisteid ja definitsioone, mis on kirjeldatud dokumendis `IVXV-ÜK-0.95 Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel`:

- E-hääletamise etapid;
- Süsteemi osapooled ja komponendid.

2.3 Mõisted ja definitsioonid

2.4 Kogumisteenuse kasutajate rollid

Kogumisteenuses on kasutusel järgnevad rollid:

1. **Kogumisteenuse haldur** tegeleb kogumisteenuse tehnilise haldamisega;
2. **Valimiste haldur** tegeleb valimiste seadistuste kehtestamisega;
3. **Vaataja** pääseb ligi haldusteenuse kaudu väljastatavatele seisundi- ja statistikaandmetele;

Rollide täpsem kirjeldus asub dokumendis `Elektroonilise hääletamise infosüsteemi IVXV seadistuste koostamise juhend`.

2.5 Süsteemi komponendid

Kogumisteenus

Haldusteenus on kogumisteenuse haldamise teenus. Haldusteenuse kaudu juhitakse ja jälgitakse kogumisteenust alates paigaldusest kuni mahavõtmiseni. Vaata lähemalt lõigus *Haldusteenus*.

Logikoguja on kogumisteenuse sisemine logiserver, mis kogub ja säilitab kõigi kogumisteenuste alamteenuste logisid. Logikogujasse kogutud logid antakse valimiste lõppedes üle korraldajale.

Sisemine varundus on kogumisteenuse varundusteenus, mis varundab kõigi alamteenuste andmeid ja teeb need lihtsa liidese (failisüsteemi kataloog) kaudu kättesaadavaks välisele varundusteenusele.

Alamteenused on kogumisteenuse eri lõikude eest vastutavad teenused.

Tugiteenused

Logiseire on kogumisteenuse logide analüüsiks ja jälgimiseks mõeldud seireprogramm.

Tehniline seire on kogumisteenuse tehnilise toimimise jälgimiseks mõeldud seireprogramm.

Väline varundus on kogumisteenuse sisemisest varunduse poolt varundatud andmete säilitamiseks mõeldud väline varundusteenus.

Välised teenused

Välised teenused on läbiviidavatele valimistele kehtestatud nõuetest sõltuvad teenused, millega kogumisteenus on võimeline liidestuma. Väliste teenuste hulka kuuluvad Registreerimisteenus, DigiDoc teenus, Ajatempliteenus, Mobiil-ID teenus, OCSP teenus vms.

2.6 Ülevaade toimingutest

- Hääletamiseelsel etapil:
  - Kirjeldatakse kogumisteenuse poolt kasutatavad *välised teenused*;
  - Valmistatakse ette kogumisteenuse *tugiteenused*;
  - Valmendatakse kogumisteenuse tarkvara;
  - Koostatakse kogumisteenuse seadistused (usaldusjuur, tehnilised seadistused ja valimiste seadistused);
  - Genereeritakse teenuse toimimiseks vajalikud krüptovõtmed ja sertifikaadid;
  - Valmistatakse ette kogumisteenuse käitamiseks vajalik taristu;
  - Paigaldatakse haldusteenus;
  - Rakendatakse seadistused haldusteenusele, mille põhjal haldusteenus paigaldab ja seadistab kogumisteenuse alamteenused.
- Hääletamisetapil
  - Jälgitakse teenuse toimimist;
  - Luuakse e-urnist varukoopiaid.
- Töötlusetapil
  - Eksporditakse kogumisteenusesse kogutud andmed:
    1. e-urn kogutud häältega
- Lugemisetapil
  - Lugemisetapil kogumisteenust ei kasutata;

PEATÜKK 3

Haldusteenus

Haldusteenus on kogumisteenuse haldamiseks mõeldud lahendus. Haldusteenus paigaldatakse eraldiseisvasse masinasse ja selle kaudu toimub kogumisteenuse juhtimine paigaldusest kuni seiskamiseni.

Haldusteenuse funktsioonid on:

1. Kogumisteenuse alamteenuste haldamine:
   1.1 Seadistuste ja valimisnimekirjade laadimine;
   1.2 Alamteenuste paigaldus selleks ettevalmistatud masinatesse;
   1.3 Alamteenustele seadistuste ja nimekirjade rakendamine;
2. E-urni allalaadimine töötlemiseks;
3. Valimiste üldstatistika jälgimine;
4. E-urni korrapärane varundamine;
5. Kogumisteenuse seisundi seire;

Haldusteenus suhtleb hallatavate teenustega üle SSH-kanali. Suhtluse algatab alati haldusteenus. Usaldus teenusmasinate vastu luuakse süsteemihalduri abiga pärast teenuseid majutavate masinate paigaldamist.

Teenust majutava masina paigaldamise järel loob haldur haldusteenusele ligipääsu teenusmasina juurkontole, et haldusteenusel oleks võimalik teenuse tarkvara paigaldada. Pärast viimase teenuse paigaldamist teenuseid majutavasse masinasse eemaldab haldusteenus ligipääsu juurkontole.

3.1 Haldusteenuse koosseis

Haldusteenuse kasutajaliides koosneb kahest osast:

1. Haldamise põhifunktsionaalsus on teostatud *käsureautiliitide* abil;
2. Graafiline kasutajaliides on veebipõhine liides, mille funktsionaalsuse tagavad käsureautiliidid.

Lisaks töötavad deemonprotsessid:

1. Veebiserver graafilise kasutajaliidese jaoks;
2. Agentdeemon teenuste seisundi jälgimiseks.

PEATÜKK 4

Süsteemi algseadistamine

Süsteemi algseadistamine tähendab süsteemi paigaldamist ning seadistamist läbiviidavate valimiste tarbeks.

4.1 Nõuded kasutatavale platvormile

Kogumisteenus töötab platvormil `Ubuntu 16.04 LTS (Xenial Xerus)`.

4.2 Väliste teenuste kaardistamine

Kogumisteenuse poolt toetatavate ja läbiviidavas hääletamises kasutatavate väliste teenuste (DigiDocService, OCSP jms) kaardistamise käigus koostatakse nimekiri välistest teenustest ja nendega andmevahetuseks vajalikest andmetest (võrguaadress, port jms).

Väliste teenuste andmed on sisendiks kogumisteenuse tehnilise seadistuse koostamisel (*Kogumisteenuse seadistuste koostamine*).

Väliste teenuste kaardistamise tulemusena on kogumisteenuse osutajal olemas nimekiri kogumisteenuse poolt kasutatavatest välistest teenustest koos teenuste kasutamiseks vajalike parameetritega.

4.3 Tugiteenuste ettevalmistamine

Kogumisteenuse tugiteenusteks on:

1. Tehnilise seire teenus;
2. Logiseire teenus;
3. Varundusteenus.

Tehnilise seire ettevalmistamine

Tehnilise seire teenus on Zabbix tarkvaral põhinev seire- ja teavitussüsteem. Zabbix serveri paigaldab ja seadistab kogumisteenuse osutaja iseseisvalt.

Seire toimimiseks on tarvis määrata seire eest vastutavad isikud ning tagada nende vahetu teavitamine seireprogrammi poolt avastatud kõrvalekalletest.

Lisaks standardsele tehnilisele seirele (teenusmasinate protsessori-/kettakasutus jms.) viib kogumisteenuse haldusteenus läbi alamteenuste seiret ja teavitab tehnilise seire serverit avastatud kõrvalekalletest.

Tehnilise seire ettevalmistamise tulemusena on kogumisteenuse osutajal olemas tehnilise seire server, kuhu on paigaldatud seiretarkvara ning kus on kirjeldatud tehnilise seire eest vastutavad isikud ja nende teavitamise meetodid.

Logiseire ettevalmistamine

Logiseire teenus koosneb rsyslog logiserverist koos analüüsi- ja visualiseerimistarkvaraga (Log Monitor, Grafana).

Logiseire ettevalmistamine ja integreerimine kogumisteenusega on kirjeldatud dokumendis `IVXV tegevuslogi seirelahendus`.

Logiseire ettevalmistamise tulemusena on kogumisteenuse osutajal olemas logiseire server, kuhu on paigaldatud logiseire tarkvara ning kus on kirjeldatud logiseire andmetele ligipääsevad isikud.

Varunduse ettevalmistamine

Varundusteenus on kogumisteenuse osutaja poolt paigaldatud ja seadistatud varundusserver, mis vastutab kogumisteenuse sisemises varundusserveris koostatud varukoopiate säilimise eest.

Varunduse ettevalmistamise tulemusena on kogumisteenuse osutajal olemas varundusserver, mis on suuteline kogumisteenuse varundusliidese kaudu andmeid varundama.

4.4 Kogumisteenuse tarkvara valmendamine

Kogumisteenuse tarkvara valmendamiseks käivitatakse tarkvara lähtekoodi kataloogis käsk **`dpkg-buildpackage`**. Edukaks valmendamiseks on tarvis tarvilike tarkvarapakkide paigaldamine. Kui käsu **`dpkg-buildpackage`** käivitamine katkeb vajalike pakkide puudumise tõttu, tuleb need pakid paigaldada käsi **`apt-get install`** abil. Vajaminevate pakkide nimekiri kuvatakse käsu **`dpkg-buildpackage`** väljundis, samuti on võimalik neid tuvastada faili `debian/control` sisu järgi (väli `Build-Depends`).

```
builder@builder $ sh -c "cd /output/src/ivxv.git && env DEB_BUILD_OPTIONS=nocheck␣
↪DEVELOPMENT=1 dpkg-buildpackage -b -uc"
dpkg-buildpackage: source package ivxv
dpkg-buildpackage: source version 1.0
dpkg-buildpackage: source distribution xenial
dpkg-buildpackage: source changed by IVXV Developer <info@ivotingcentre.ee>
dpkg-buildpackage: host architecture amd64
 dpkg-source --before-build ivxv.git
 fakeroot debian/rules clean
dh clean --with systemd --with python3
   dh_testdir
   debian/rules override_dh_auto_clean
...
dpkg-deb: building package 'ivxv-verification' in '../ivxv-verification_1.0_amd64.
↪deb'.
dpkg-deb: building package 'ivxv-voting' in '../ivxv-voting_1.0_amd64.deb'.
dpkg-deb: building package 'ivxv-storage' in '../ivxv-storage_1.0_amd64.deb'.
dpkg-deb: building package 'ivxv-dds' in '../ivxv-dds_1.0_amd64.deb'.
dpkg-deb: building package 'ivxv-log' in '../ivxv-log_1.0_all.deb'.
 dpkg-genchanges -b >../ivxv_1.0_amd64.changes
dpkg-genchanges: binary-only upload (no source code included)
 dpkg-source --after-build ivxv.git
dpkg-buildpackage: binary-only upload (no source included)
```

E-hääletamissüsteemi tarkvara valmendamise tulemusena on kogumisteenuse osutajal olemas hääletustarkvara deb-pakid.

4.5 Kogumisteenuse seadistuste koostamine

Kogumisteenuse seadistused koosnevad kolmest eraldiseisvast osast:

1. **Usaldusjuure seadistus** sisaldab andmed seadistuste (kaasa arvatud usaldusjuure enda) allkirjade kontrollimiseks ja nimekirja kogumisteenuse haldurite volitustest.
2. **Kogumisteenuse tehniline seadistus** määrab kogumisteenuse tehnilised parameetrid, hääletuse läbiviimiseks kasutatavad teenused, samuti ka kogumisteenuse koosseisu kuulvad alamteenused.
3. **Valimiste seadistus** määrab ühe valimise seadistuse.

Seadistuste koostamine on kirjeldatud dokumendis `Elektroonilise hääletamise infosüsteemi IVXV seadistuste koostamise juhend`. Kogumisteenusele rakendatavad seadistused peavad olema pakendatud BDOC konteinerisse ja olema signeeritud volitatud kasutaja poolt.

Kogumisteenuse seadistuste koostamise tulemusena on kogumisteenuse osutajal olemas kogumisteenuse seadistamiseks vajalikud seadistuspakid. Kõik seadistused on signeeritud isiku(te) poolt, kelle volitused on kirjeldatud usaldusjuure seadistustes.

4.6 Kogumisteenuse taristu paigaldamine

Kogumisteenuse taristu eraldatakse teenuse osutamiseks vastavalt koostatud seadistustele (*Kogumisteenuse seadistuste koostamine*).

Igas teenusmasinas:

1. peab olema seadistatud hostinimi (fail `/etc/hostname`);
2. peab olema paigaldatud SSH teenus (tarkvarapakk `openssh-server`);
3. peab olema paigaldatud tehnilise seire teenuse agent (tarkvarapakk `zabbix-agent`);
4. peab olema tagatud õige kellaaeg (näiteks õige kellaaja teenuse `ntp` abil).
5. peab olema seadistatud nimelahendus, mis võimaldab kõikide teenusmasinate aadresse lahendada;
6. peab olema seadistatud Eesti lokaat koos UTF-8 kooditabeli toega `et_EE.UTF-8` (kas tarkvarapakk `locales` koos nimetatud lokaadi seadistamisega või tarkvarapakk `locales-all`, mis paigaldab kõik toetatud lokaadid).

Märkus: Iga teenusmasina poolt kasutatav nimelahendus peab tagama, et suhtluseks kasutatavate hostide nimed lahenduvad korrektselt.

Vältima peab olukordi, kus hostinimi lahendub mitmeks aadressiks või teistele hostidele kättesaamatuks aadressiks.

Järgnev näide kirjeldab võimalikku olukorda failis `/etc/hosts`, kus opsüsteemi paigalduse järel on hostinimi `ivxv123` määratud kahele liidesele. Sellise seadistuse puhul võib tekkida olukord, kus aadressile `ivxv123` ühendusi vastu võtma seadistatud teenus hakkab kuulama kohalikul liidesel `127.0.0.1` ja pole avaliku liidese `192.168.10.1` kaudu teistele teenustele kättesaadav.

```
# /etc/hosts
127.0.0.1     ivxv123
192.168.10.1  ivxv123
```

Kogumisteenuse taristu jaoks eraldatud hostidest tuleb koostada nimekiri, kus on kirjas hosti asukohaks olev alamvõrk, hosti nimi, IP-aadress, SSH-serveri avalik võti ja hostile plaanitud teenused.

Kogumisteenuse taristu nimekirjas näide:

```
Valimiste infrastruktuuri andmed

  Alamvõrk: zone1

     IP-aadress: 172.16.238.10
     Hostinimi: admin
     SSH-serveri avalik võti:
       ecdsa-sha2-nistp256 AAAAE2VjZHNhLX...SgtbbE= root@admin

     IP-aadress: 172.16.238.41
     Hostinimi: ivxv1
     SSH-serveri avalik võti:
       ecdsa-sha2-nistp256 AAAAE2VjZHNhLX...mN8ul0= root@ivxv1

  Alamvõrk: zone2

     IP-aadress: 172.16.100.63
```

```
    Hostinimi: ivxv2
    SSH-serveri avalik võti:
      ecdsa-sha2-nistp256 AAAE2VjZHNhLXN...rtWT7A= root@ivxv2
```

Kogumisteenuse taristusse kuuluvad hostid tuleb lisada tehnilisse seiresse.

Kogumisteenuse taristu paigaldamise tulemusena on kogumisteenuse osutajal olemas dokumenteeritud platvorm kogumisteenuse paigaldamiseks ettenähtud konfiguratsiooniga. Kõik taristusse kuuluvad (virtuaal)masinad on tehnilise seire teenuse poolt kättesaadavad ja nende seisundis pole tuvastatud probleeme.

4.7 Haldusteenuse paigaldamine

Haldusteenuse paigaldamine toimub haldusteenuse hostil.

Haldusteenuse paigaldamiseks tuleb kopeerida **kõik** kogumisteenuse tarkvarapakid haldusteenuse masina kataloogi `/opt/`. Nendest pakkidest paigaldatakse haldusteenus, samuti kasutab haldusteenus neid pakke alamteenuste paigaldamiseks.

Haldusteenuse sõltuvuste paigaldamine:

```
root@admin # apt-get install --yes --quiet adduser openssh-server openssl rsyslog␣
↪rsyslog-relp sudo tzdata locales init-system-helpers python3-bottle python3-
↪dateutil python3-debian python3-docopt python3-jinja2 python3-openssl python3-
↪yaml python3:any apache2 language-pack-et libapache2-mod-wsgi-py3 python3-gdbm␣
↪python3-pkg-resources
Reading package lists...
Building dependency tree...
Reading state information...
adduser is already the newest version (3.113+nmu3ubuntu4).
rsyslog is already the newest version (8.16.0-1ubuntu3).
init-system-helpers is already the newest version (1.29ubuntu4).
language-pack-et is already the newest version (1:16.04+20160627).
locales is already the newest version (2.23-0ubuntu9).
locales on määratud käsitsi paigaldatuks.
openssh-server is already the newest version (1:7.2p2-4ubuntu2.2).
...
Paki python3-debian (0.1.27ubuntu2) paikasättimine ...
Paki python3-docopt (0.6.2-1build1) paikasättimine ...
Paki python3-markupsafe (0.23-2build2) paikasättimine ...
Paki python3-jinja2 (2.8-1) paikasättimine ...
Paki python3-openssl (0.15.1-2build1) paikasättimine ...
Paki python3-yaml (3.11-3build1) paikasättimine ...
Paki dh-python (2.20151103ubuntu1.1) paikasättimine ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for systemd (229-4ubuntu19) ...
```

Haldusteenuse paigaldamine:

```
root@admin # dpkg -i /etc/ivxv/debs/ivxv-common_1.0_all.deb /etc/ivxv/debs/ivxv-
↪admin_1.0_all.deb
Selecting previously unselected package ivxv-common.
(Andmebaasi lugemine ... 12008 files and directories currently installed.)
Preparing to unpack .../debs/ivxv-common_1.0_all.deb ...
Unpacking ivxv-common (1.0) ...
Selecting previously unselected package ivxv-admin.
Preparing to unpack .../debs/ivxv-admin_1.0_all.deb ...
Unpacking ivxv-admin (1.0) ...
Paki ivxv-common (1.0) paikasättimine ...
```

```
# Adding user group 'ivxv'
Adding group `ivxv' (GID 109) ...
...
Signature ok
subject=/CN=ivxv-admin-ui/O=IVXV kogumisteenuse haldusteenus/L=Somewhere/C=EE
Getting Private key
# Generating strong Diffie-Hellman group file
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
....................................+.....................................
.....................................................................+.............
.....................................................................................+.
.........++*++*
# Starting Apache web server
# Restarting rsyslog log server
```

Tähtis: Haldusteenuse edasine kasutamine toimub haldusteenuse konto alt. Selleks tuleb halduril luua SSH-ligipääs haldusteenuse kontole `ivxv-admin`. Soovitav on autentimine teha ID-kaardi põhiseks.

Haldusteenuse paigaldamise tulemusena on kogumisteenuse osutajal teenuse haldamiseks vajalik liides.

Kogumisteenuse taristu hõlmamine haldusesse

Haldusteenus kasutab kogumisteenuse haldamiseks SSH protokolli. Selleks, et haldusteenusel oleks võimalik teisi teenushoste usaldada, tuleb haldusteenusesse lisada hallatavate teenushostide SSH-serveri võtmed.

Näide hosti `ivxv1` SSH-võtmete lisamisest haldusteenuse usaldatavate hostide hulka:

```
ivxv-admin@admin $ ssh-keyscan ivxv1 >> ~/.ssh/known_hosts
# ivxv1:22 SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
# ivxv1:22 SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
# ivxv1:22 SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
```

Selleks, et haldusteenusel oleks võimalik teenushostidesse tarkvara paigaldada, tuleb haldusteenuse kontole `ivxv-admin` luua SSH-ligipääs teenushostide juurkasutaja kontole.

Märkus: Haldusteenus vajab juurkasutaja ligipääsu alamteenuse tarkvara paigaldamiseks. Pärast edukat paigaldamist ühel hostil eemaldab haldusteenus ligipääsu selle hosti juurkasutaja kontole.

Haldusteenuse konto SSH-võtmepaari avalik võti asub kasutaja `ivxv-admin` kodukataloogi all failis `.ssh/id_rsa.pub` ja see on genereeritud haldusteenuse paigaldamise käigus. Vajadusel võib haldur selle võtme asendada (kuid see peab toimuma enne, kui võti on üle kantud hallatavatesse teenusmasinatesse).

Teenusmasinas tuleb haldusteenuse konto SSH avalik võti panna faili

`/root/.ssh/authorized_keys`. See fail peab kuuluma juurkasutajale ja olema loetav ainult juurkasutaja poolt (faili pääsuõigused `0600`).

Kogumisteenuse taristu haldusesse hõlmamise tulemusena on haldusteenusel usaldusväärne ligipääs kogumisteenuse taristusse kuuluvatele teenusmasinate juurkasutaja kontodele.

Logiseire lahenduse ühendamine haldusteenusega

Logiseire lahenduse kasutamise korral peab haldusteenusel olema ligipääs logiseire lahendusele, et sealt kogutud statistikat alla laadida ja vajadusel värskendada logiseire poolt analüüsitavaid logisid.

Selleks, et haldusteenusel oleks usaldus logiseire teenuse vastu, tuleb haldusteenusesse lisada logiseire teenuse hosti (käesolevas näites nimega `logmonitor`) SSH-serveri võtmed:

```
ivxv-admin@admin $ ssh-keyscan -t ecdsa logmonitor >> ~/.ssh/known_hosts
```

Selleks, et haldusteenus pääseks logiseire kontole ligi, tuleb haldusteenuse konto SSH avalik võti panna logiseire konto `logmon` volitatud võtmete faili `~logmon/.ssh/authorized_keys`. See fail peab kuuluma logimonitori kasutajale ja olema loetav ainult selle kasutaja poolt (faili pääsuõigused `0600`).

Logiseire lahenduse haldusteenusega ühendamise tulemusena on tegevuslogi seirelahendus haldusteenusele kättesaadav ning haldusteenusel on võimalik seirelahendusest statistikaandmeid laadida ning seirelahenduse andmehoidlasse ajakohaseid logiandmeid üle kanda.

Haldusteenuse veebiliidese vaikimisi TLS-sertifikaadi asendamine

Haldusteenuse paigalduse käigus genereeritakse kasutajaliidese veebiserveri TLS-sertifikaat koos krüptovõtmega ja tugeva Diffie-Hellman grupifail (vaata https://weakdh.org/). Vajadusel on halduril võimalik need asendada (vaata märkust lõigus “*Nõuded kasutatavale platvormile*”).

Failide asukohad:

- Veebiserveri TLS-sertifikaadi võti: `/etc/ssl/private/ivxv-admin-default.key`
- Veebiserveri TLS-sertifikaat: `/etc/ssl/certs/ivxv-admin-default.crt`
- Diffie-Hellmani grupifail: `/etc/ssl/dhparams.pem`

Asendatud failide rakendamiseks tuleb veebiserver taaskäivitada käsuga **`service apache2 restart`** ja veenduda, et veebiliides töötab.

Haldusteenuse veebiliidese vaikimisi TLS-sertifikaadi asendamise tulemusena kasutab haldusteenuse veebiliides turvalist sertifikaati.

4.8 Haldusteenuse lähtestamine

Haldusteenuse lähtestamine toimub käsuga *ivxv-collector-init*. Selle käigus puhastatakse haldusteenuse andmekataloogid ja lähtestatakse andmebaas.

4.9 Seadistuste ja valimisnimekirjade rakendamine kogumisteenusele

---

Märkus: Käesolevas lõigus ja alamlõikudes tähendab “seadistuspakk” nii seadistusi sisaldavat faili kui valimisnimekirja faili, mis on signeeritud volitatud isiku poolt.

Kogumisteenusele tuleb rakendada järgmised seadistuspakid:

1. Usaldusjuur – laaditakse alati esimesena;
2. Kogumisteenuse tehniline seadistus – laaditakse enne valimiste seadistust;
3. Valimiste seadistus – laaditakse enne nimekirju;
4. Valikute nimekiri;
5. Valijate nimekiri.

Ettevalmistatud seadistuspakkide rakendamiseks tuleb läbi viia järgmised tegevused:

1. Ülekandmine haldusteenuse masinasse;
2. Laadimine haldusteenusesse;
3. Rakendamine alamteenustele.

Vihje: Seadistuspakkide ettevalmistamine on kirjeldatud lõigus “*Kogumisteenuse seadistuste koostamine*”.

Tähelepanu: Usaldusjuure seadistuse laadimisega kaasneb alati ka kogumisteenuse haldusteenuse andmebaasi lähtestamine!

Seadistuste ja valimisnimekirjade kogumisteenusele rakendamise tulemusena on kogumisteenus seadistatud ettenähtud perioodil osutama nõuetekohast häälte kogumise teenust.

Seadistuspaki ülekandmine haldusteenuse masinasse

Seadistuspaki transportimiseks haldusteenuse masinasse toimub üle SCP protokolli. Seadistuspakk peab olema kättesaadav haldusteenuse kasutajakontole `ivxv-admin`.

Näide:

```
$ scp seadistus.bdoc ivxv-admin@admin:
seadistus.bdoc              100%   15KB  79.5KB/s   00:00
```

Märkus: Kogumisteenus osutaja võib seadistuspakkide ülekandmiseks kasutada ka muid meetodeid, näiteks irdmeediat.

Seadistuspaki ülekandmise tulemusena on seadistuspakk haldusteenuse poolt ligipääsetaval andmekandjal.

Seadistuspaki laadimine haldusteenusesse

Seadistuspakk laaditakse haldusteenusesse käsuga *ivxv-cmd-load*. Selle käigus kontrollib haldusteenus seadistuspaki signeerinud isiku volitusi ja valideerib seadistuste sisu. Laadimise tulemusena on seadistuspakk valmis rakendamiseks hallatavatele teenustele.

Näide: Usaldusjuure laadimine haldusteenusesse:

```
ivxv-admin@admin $ ivxv-cmd-load trust /output/voting/HA-SETUP/config/trust.bdoc
command_file:INFO: Loading command file "/output/voting/HA-SETUP/config/trust.bdoc
↪" (trust root configuration)
command_file:INFO: Command file loaded
command_file:INFO: Command file successfully extracted
command_file:INFO: Reading files from command file
command_file:INFO: Validating trust root configuration
command_file:INFO: Files in trust root configuration package are valid
INFO: Config file is signed by: ORAV,IVAN,30809010001 2017-09-19T12:34:59Z
INFO: User ORAV,IVAN,30809010001 with role "admin" is authorized to execute "trust
↪" commands
INFO: Using signature "ORAV,IVAN,30809010001 2017-09-19T12:34:59Z" as config file␣
↪version
INFO: Loading command trust from file /output/voting/HA-SETUP/config/trust.bdoc
...
command_file:INFO: Command file successfully extracted
command_file:INFO: Reading files from command file
command_file:INFO: Validating trust root configuration
command_file:INFO: Files in trust root configuration package are valid
INFO: Resetting collector management database
db:INFO: Initializing management database /var/lib/ivxv/db/ivxv-management.db
INFO: Trust config file loaded successfully
INFO: Resetting user permissions
lib:INFO: Creating Apache Web Server user permission file /var/lib/ivxv/admin-ui-
↪permissions/ORAV,IVAN,30809010001-admin
```

Seadistuspaki haldusteenusesse laadimise tulemusena on haldusteenus valmis rakendama seadistuspakki alamteenustele. Seadistuspaki versiooni kuvatakse haldusteenuse olekuandmetes.

Seadistuste rakendamine alamteenustele

Haldusteenusesse laaditud seadistuspakid rakendatakse hallatavatele teenustele käsuga *ivxv-config-apply*. Rakendamine on võimalik tehniliste seadistuse laadimise järel,

kuna tehnilise seadistusega tekivad haldusteenusesse andmed hallatavate teenuste kohta.

Seadistuste rakendamise käigus haldusteenus:

- Paigaldab seadistatava teenuse tarkvara (tehnilise seadistuse laadimisel, kui pole eelnevalt paigaldatud);
- Kannab seadistuspaki üle hallatava teenuse hosti failisüsteemi;
- Valimiste seadistuse laadimisel lubab ja käivitab seadistatava teenuse.

Märkus: Seadistuste rakendamise järjekord on kirjeldatud utiliidi ivxv-config-apply abiteabe lõigus (vaata *ivxv-config-apply*).

Näide: Haldusteenusesse laaditud seadistuste rakendamine hallatavatele teenusele:

```
ivxv-admin@admin $ ivxv-config-apply
INFO: Technical config is signed by ÕIGE,VALIK,44444444444 2017-06-07T12:05:44Z
INFO: Service choices@choices1.ivxv.ee: Applying technical config
SERVICE choices@choices1.ivxv.ee: Installing service to host "ivxv1"
SERVICE choices@choices1.ivxv.ee: Querying state of the service software package
↪"ivxv-choices"
SERVICE choices@choices1.ivxv.ee: Copying software package files to service host
SERVICE choices@choices1.ivxv.ee: Checking state of dpkg database in service host
SERVICE choices@choices1.ivxv.ee: Installing dependencies for package "ivxv-common"
Reading package lists...
Building dependency tree...
Reading state information...
...
SERVICE voting@voting3.ivxv.ee: Set trust config file permissions in service host
SERVICE voting@voting3.ivxv.ee: Trust root config successfully applied to service
SERVICE voting@voting3.ivxv.ee: Applying technical config to service
SERVICE voting@voting3.ivxv.ee: Copying technical config to service host
SERVICE voting@voting3.ivxv.ee: Set technical config file permissions in service␣
↪host
SERVICE voting@voting3.ivxv.ee: Technical config successfully applied to service
SERVICE voting@voting3.ivxv.ee: Registering technical config version "ÕIGE,VALIK,
↪44444444444 2017-06-07T12:05:44Z" in management database
SERVICE voting@voting3.ivxv.ee: Registering service state as "INSTALLED" in␣
↪management database
INFO: Service voting@voting3.ivxv.ee: technical config config applied successfully
INFO: 15 configuration packages successfully applied
```

Seadistuste alamteenustele rakendamise tulemusena on hallatavad teenused seadistatud ja nende seisund on haldusteenusest jälgitav.

Kogumisteenuse krüptovõtmete rakendamine

Teenuste krüptovõtmete ja TLS-sertifikaatide rakendamine toimub käsuga *ivxv-secret-import*.

Vihje: Teenuse krüptovõtmete seisundit on võimalik väljastada käsuga **`ivxv-status --service=<service-id>`** (vaata *ivxv-status*)

Võtme laadimine teenusele:

```
$ ivxv-secret-import --service=<teenuse-id> tls-key tls.key
```

Sertifikaadi laadimine teenusele:

```
$ ivxv-secret-import --service=<teenuse-id> tls-cert tls.pem
```

Tähtis: Igale teenuse isendile tuleb rakendada selle isendi jaoks genereeritud võti ja sertifikaat!

Hääletamisteenuse ajatemplipäringute signeerimisvõtme rakendamine toimub käsuga *ivxv-secret-import*:

```
$ ivxv-secret-import tsp-regkey tspreg.key
```

Märkus: Hääletamisteenuse ajatemplipäringute signeerimisvõti on vaja rakendada vaid juhul, kui ajatempliteenust kasutatakse registreerimisteenuseks (tehnilises seadistuses on `qualification/protocol` välja väärtuseks `tspreg`).

Mobiil-ID identsustõendi võtme rakendamine toimub käsuga *ivxv-secret-import*:

```
$ ivxv-secret-import dds-token-key mobid-shared-secret.key
```

Märkus: Mobiil-ID identsustõendi võti on vaja rakendada vaid juhul, kui Mobiil-ID tugiteenus on kasutusel (tehnilises seadistuses on olemas plokk `auth.ticket`).

Kogumisteenuse krüptovõtmete rakendamise tulemusena on hallatavate teenuste suhtluskanalid varustatud kanali turvamiseks vajalike krüptovõtmetega, samuti on teenustel olemas krüptovõtmed muude oluliste operatsioonide jaoks.

PEATÜKK 5

Süsteemi haldustoimingud

5.1 Kogumisteenuse oleku jälgimine

Kogumisteenuse olekuandmed registreeritakse haldusteenuse andmebaasis. Oleku kuvamiseks on utiliit *ivxv-status*.

Olekus kuvatakse järgmisi andmeid:

- Valimise ID, faas, algus- ja lõpuaeg;
- Laaditud seadistuspakkide versioonid;
- Laaditud valimisnimekirjade versioonid;
- Teenuste nimekiri koos rakendatud seadistuste versioonidega, teenuse seisundi ja selle viimase tuvastamise ajaga;
- Väliste teenuste seisundid;
- Haldusteenuse andmehoidla statistika.

Sõltuvalt kogumisteenuse seisundis võib oleku kuvamise utiliit jätta mõned andmeblokid kuvamata. Täieliku andmestiku väljastamiseks vaata utiliidi *ivxv-status* abiteavet.

Alamteenuste oleku jälgimise ja haldusteenuse andmebaasis registreerimisega tegeleb haldusteenuse agentdeemon.

5.2 Korralduste rakendamine

Kogumisteenuse korraldused koostatakse signeeritud korralduspakkidena, millega kirjeldatakse kasutaja identifikaator (*Common Name* ehk CN väli ID-kaardilt) ja rollide nimekiri.

Korralduste valideerimine ja rakendamine toimub käsuga *ivxv-cmd-load*.

Valimise seadistuse valideerimise näide:

```
$ ivxv-cmd-load --validate-only election valimise-seadistus-TEST2017.bdoc
```

Valikute nimekirja korralduse rakendamise näide:

```
$ ivxv-cmd-load choices valikute-nimekiri-TEST2017.bdoc
```

Vaata ka:

- Käsu *ivxv-cmd-load* abiteave;
- Korralduste rollide kirjeldus ja korralduste koostamise juhend asuvad dokumendis `IVXV seadistuste koostamise juhend`.

5.3 Kasutajate haldus

Kasutajate algsed kirjeldused määratakse usaldusjuure seadistuses, hilisem haldus toimub vastavate korralduste abil.

Kasutajate halduse korraldused rakendatakse käsuga *ivxv-cmd-load* (vaata *Korralduste rakendamine*).

Kasutajaõiguste määramise korralduse rakendamise näide:

```
$ ivxv-cmd-load user ORAV,IVAN,30809010001-admin.bdoc
```

Tähelepanu: Juba lisatud kasutajate eemaldamine süsteemist pole võimalik. Kasutaja eemaldamise asemel tuleb kasutaja rolliks määrata “õigusteta kasutaja”.

Vaata ka:

- Kasutajate rollide kirjeldus ja volituste korralduste koostamise juhend asuvad dokumendis `IVXV seadistuste koostamise juhend`.
- Korralduste rakendamine on kirjeldatud lõigus *Korralduste rakendamine*.

5.4 Tarkvarauuenduste rakendamine

Tarkvarauuendused jagunevad kogumisteenuse vaatepunktist kaheks: operatsioonisüsteemi uuendused ja kogumisteenuse uuendused.

Operatsioonisüsteemi tarkvarapakkide uute versioonide paigaldamine pole kogumisteenuse dokumentatsioonis käsitletud. Süsteemiülem peab tagama ajakohaste turvauuenduste rakendamise kogumisteenuses kasutatavate operatsioonisüsteemidele;

Kogumisteenuse tarkvarapakkide uute versioonide paigaldamine toimub järgnevalt:

1. Uuenenud tarkvarapakid kopeeritakse haldusteenuse kataloogi `/etc/ivxv/debs` (soovitavalt juurkasutaja õigustes);

2. Haldusteenuse tarkvara uuendatakse juurkasutaja õigustes käsuga **`dpkg -i /etc/ivxv/debs/ivxv-common_1.0_all.deb /etv/ivxv/debs/ivxv-admin_1.0_all.deb`** (tegelik versiooninumber erineb käesolevas näites kasutatud versioonist);
3. Hallatavate teenuste tarkvara uuendamine toimub haldusteenuse kasutaja `ivxv-admin` õigustes käsuga *ivxv-update-packages*.

5.5 Varukoopiate tegemine

5.6 Varukoopiast taastamine

PEATÜKK 6

Kogumisteenuse seadistused

6.1 Logimise seadistused

Kogumisteenuse logi hoitakse logi tekkimise asukohas ja dubleeritakse logiserveritesse. Logide kogumiseks ja edastamiseks kasutatakse vaikimisi *syslog*-teenust `rsyslog`.

Kogumisteenus toetab kahte liiki logiservereid, mis kirjeldatakse kogumisteenuse tehnilises seadistuses.

1. Kogumisteenuse logikogumisteenus on kogumisteenuse sisemine teenus ja seda võib süsteemis olla mitu isendit.
2. Tegevusmonitooringu server on kogumisteenuse jaoks väline teenus ja seda võib olla ainult üks isend.

Kogumisteenusele tehniliste seadistuse rakendamisel paigaldab haldusteenus logikogumisteenuse(d) enne teise teenuseid, et teenuste poolt toodetav logi saaks võimalikult varakult ka logikogumisteenusesse kogutud.

Märkus: Kogumisteenuse logiteated tekivad pärast valimiste seadistuse esmakordset laadimist, kuna teenused käivitatakse selle seadistuse laadimise järel.

Logi tootva teenuse logimise korraldus

Logi tootva teenuse logimise seadistuse genereerib haldusteenus vastavalt tehnilistele seadistustele.

1. Iga teenus logib kohalikku *syslog*-teenusesse;
2. Kõigi teenusmasinate *syslog*-teenused on seadistatud kogumisteenuse logi salvestama kohalikku failisüsteemi (`/var/log/ivxv.log`);

3. Kõigi teenusmasinate (peale logikogumisteenuse) *syslog*-teenused on seadistatud edastama üle võrgu:
   3.1 Kõiki logikirjeid logikogumisteenusesse (protokoll: RELP);
   3.2 Kogumisteenuse logikirjeid tegevuslogi monitooringu serverisse (protokoll: UDP);

Logikogumisteenuse korraldus

Logikogumisteenuse seadistusfail tuleb teenuse tarkvarapakist (*ivxv-logcollector.conf*).

1. Logikogumisteenus võtab logikirjeid vastu RELP-protokolli kaudu;
2. Kogumisteenuse logikirjeid salvestatakse JSON-vormingus faili `/var/log/ivxv.log` (välja arvatud silumislogi);
3. Kogumisteenuse silumislogi ja teiste oluliste teenuste (haproxy, rsyslog, sshd) logi kirjutatakse rsyslogi standardvormingus faili `/var/log/ivxv-debug.log`.

PEATÜKK 7

Lisad

7.1 Utiliidid

Kogumisteenuse haldamise käsureautiliitide ülevaade ja abiteave.

Andmehoidla utiliidid

ivxv-create-data-dirs

`ivxv-create-data-dirs --help`:

```
Create IVXV Collector Management Service data directories.

NOTE: Directory owners and permissions are not set by this utility!

Usage: ivxv-create-data-dirs
```

ivxv-db-reset

`ivxv-db-reset --help`:

```
Reset IVXV Collector Management Service database.

Usage: ivxv-db-reset [--force]

Options:
    --force     Don't ask user confirmation
```

ivxv-db-dump

`ivxv-db-dump --help`:

```
Dump IVXV Collector Management Service database.

Usage: ivxv-db-dump
```

Teenuses seisundi utiliidid

ivxv-status

`ivxv-status --help`:

```
Output IVXV collector state.

Usage: ivxv-status [--json] [--filter=<filter-type> ...]
                   [--service=<service-id> ...]

Options:
    --json                   Output full data in JSON format.
                             Note: filters have no effect in JSON output.
    --filter=<filter-type>   Filter output by section. Possible values are:
                               * collector - collector status;
                               * election - election data;
                               * config - versions of loaded config;
                               * list - versions of loades lists;
                               * service - service information;
                               * ext - external service information;
                               * storage - storage information;
                               * smart - output only relevant data;
                               * all - output all data;
                             [Default: smart].
    --service=<service-id>   Filter output by service ID.
                             Note: This filter conflicts other section
                             filters than "smart" or "service".
```

Teenuse oleku kuvamisel näidatakse seadistamata teenuse juures ka vihjet järgmise sammu kohta, mida teenuse seadistamiseks tarvis teha on.

Kasutajate halduse utiliidid

ivxv-users-list

`ivxv-users-list --help`:

```
List IVXV Collector Management Service registered users.

Usage: ivxv-users-list
```

Seadistusutiliidid

ivxv-collector-init

`ivxv-collector-init --help`:

```
Initialize IVXV Collector.

Usage: ivxv-collector-init [--force]

Options:
    --force     Don't ask user confirmation
```

ivxv-cmd-load

`ivxv-cmd-load --help`:

```
Load command to IVXV Collector Management Service.

Usage: ivxv-cmd-load [--validate-only] <type> FILE

Options:
    <type>              Command type. Possible values are:
                        - election: election config
                        - technical: collector technical config
                        - trust: trust root config
                        - choices: choices list
                        - voters: voters list
                        - user: user account and role(s)
    --validate-only     Validate only.
```

ivxv-config-apply

`ivxv-config-apply --help`:

```
Apply IVXV collector config to IVXV services.

Usage: ivxv-config-apply [--type=<type>] ... [<service-id>] ...

Options:
    --type=<type>    Config type. Possible values are:
                     - election: election config file
                     - technical: collector technical config file
                     - choices: choices list
                     - voters: voters list
```

Seadistuste rakendamine hallatavatele teenustele on võimalik siis, kui haldusteenusesse on laaditud kogumisteenuse tehnilised seadistused.

Seadistuste rakendamise järjekord:

1. Tehnilised seadistused koos usaldusjuure seadistustega.
   1.1 Teenuse tarkvara paigaldamine;
   1.2 Haldusteenuse ligipääsu loomine hallatava teenuse kontole;
   1.3 Teenuse logimisseadistuste rakendamine;
   1.4 Haldusteenuse ligipääsu eemaldamine teenuse hosti juurkasutaja kontole (ainult juhul, kui teenusmasinas pole rohkem seadistamata teenuseid);
   1.5 Usaldusjuure rakendamine teenusele;
   1.6 Tehniliste seadistuste rakendamine teenusele;
2. Valikute nimekiri;
3. Valijate nimekirjad;

Logikogumisteenus erineb teistest hallatavatest teenustest:

1. Logikogumisteenus seadistatakse enne teisi teenuseid, et tagada võimalikult varajane logi kogumine.
2. Logikogumisteenustele ei rakendata muid seadistusi peale logikogumisteenuse seadistuste (usaldusjuure seadistusi, kogumisteenuse tehnilised seadistusi ja valimiste seadistusi logikogumisteenus ei vaja).

Valimisnimekirjade (valikute ja valijate nimekirjad) rakendamine tähendab nimekirja ülekandmist talletusteenusesse vastavat nimekirja teenindava teenuse kaudu.

Näiteks valikute nimekiri rakendatakse vaid ühele (juhuslikult valitud) nimekirjateenusele, mis kannab nimekirja talletusteenusesse. Talletusteenuse kaudu on nimekiri kättesaadav kõigile teistele nimekirjateenustele.

ivxv-secret-import

`ivxv-secret-import --help`:

```
Import secret data files to services.

This utility loads file that contains secret data to services.

Supported secret types are:

    tls-cert - TLS certificate for service.

            Certificate (and key) is used for securing
            communication between services and service instances.

    tls-key - TLS key for service.

            Key is used together with service certificate.

    tsp-regkey - PKIX TSP registration key for voting services.

            Key is used for signing Time Stamp Protocol requests.

            Key file must be in PEM format and
            must be not password protected.

    dds-token-key - Mobile ID identity token for
                    choices, dds and voting services.
```

```
            Key file must be 32 bytes long.

Usage: ivxv-secret-import [--service=<service-id>] <secret-type> <keyfile>
```

ivxv-logmonitor-copy-log

`ivxv-logmonitor-copy-log --help`:

```
Initialize IVXV Log Monitor.

This utility exports collected IVXV log files from Log Collector
Service to Log Monitor and initializes log analyzis in Log Monitor.

Usage: ivxv-logmonitor-copy-log [--force]

Options:
    --force     Don't ask user confirmation
```

ivxv-update-packages

`ivxv-update-packages --help`:

```
Update service packages in IVXV service hosts.

This utility checks versions of software packages in service hosts
and installs new versions if required.

Usage: ivxv-update-packages [--force]

Options:
    --force     Update even package version does not require update
```

Andmete eksportimise ja varundamise utiliidid

ivxv-votes-export

`ivxv-votes-export --help`:

```
Export collected votes from IVXV voting service.

Usage: ivxv-votes-export <output-file>
```

Deemonid

ivxv-agent-daemon

`ivxv-agent-daemon --help`:

```
IVXV Collector Management Service agent daemon.

Usage: ivxv-agent-daemon
```

Sisemised utiliidid

Tähelepanu: Sisemised utiliidid on kasutusel haldusdeemoni poolt alamteenuste haldamiseks ja neid ei ole reeglina tarvis eraldi käivitada.

ivxv-admin-helper

`ivxv-admin-helper --help`:

```
Usage:
    ivxv-admin-helper configure-etcd-apt-source
        Configure APT source for etcd

    ivxv-admin-helper create-ssh-access <account-name>
        Create management service access to account in service host

    ivxv-admin-helper init-host
        Initialize service host

    ivxv-admin-helper init-service <service-id>
        Initialize service data directory

    ivxv-admin-helper install-pkg <package-filename>
        Install IVXV package with dependencies

    ivxv-admin-helper remove-admin-root-access
        Remove management service access to service host root account

    ivxv-admin-helper rsyslog-config-apply
        Apply rsyslog config file for IVXV logging
```

7.2 Seadistusfailid

Logikogumisteenuse seadistusfail

```
1  # IVXV Internet voting framework
2
3  # Rsyslog configuration file for log collector service
4  # /etc/rsyslog.d/ivxv-logcollector.conf
5
6  # Collect log messages over RELP protocol
7  module(load="imrelp")
8  input(type="imrelp" port="2514")
9
10 # write IVXV log to /var/log/ivxv.log (up to level INFO)
11 if ($programname startswith 'ivxv-') and ($syslogseverity <= '6') then
12 action(
13     type="omfile"
14     file="/var/log/ivxv.log"
```

```
    template="ivxv-json"
)

# write IVXV debug log and log of related
# services (haproxy, rsyslog, sshd) to /var/log/ivxv-debug.log
if ($programname startswith 'ivxv-') or ($programname startswith 'rsyslog') or (
↪$programname == 'haproxy') or ($programname == 'sshd') then
action(
    type="omfile"
    file="/var/log/ivxv-debug.log"
)
```

7.3 Lisaseadistused

SSH 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/).

Turvakaalutustel tuleks keelata haldusliidese SSH-teenusesse parooliga autentimine. Parooliga autentimise keelamiseks tuleb seadistusfailis `/etc/ssh/sshd_config` määrata parameetri `PasswordAuthentication` väärtuseks `no`:

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```

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

> AuthorizedKeysFile /etc/ssh/kasutajad

Tähtis: 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. Kasutajale konto loomine:

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

2. Kasutaja ID-kaardi isikutuvastamise sertifikaadi salvestamine PEM-vormingus faili `usercert.cer` (ID-kaardi haldusvahendi abil);
3. Sertifikaadist kasutaja avaliku võtme eraldamine ja salvestamine faili `userpubkey.pem`:

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

4. Avaliku võtme teisendamine PKCS#8 vormingusse, kasutaja tunnusega varustamine ja salvestamine 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. Kontrollimine, kas lisatud kirje on kujul `ssh-rsa PKCS8-võti` kasutajatunnus:

```
# tail -1 /etc/ssh/kasutajad
ssh-rsa AAAAB3NzaC1yc2EAAAAELGuiTwAAAIEAxZf/
↪TuSrGJEU1PlfkY9jJ33VOYVZ9Vao0Uiytlf8
7HJu/
↪78fCIB7m05J7ibpMhsZoZ4DElU7ve0VwbvdDS3srh1OhiQcUjpznTlx4rIM1vkHwadrHtmF+BNi
DwbLbbdD5y3puGcLH+sLuwba6Vuc3aU0QuqzenYmY9pV7w9y0wc= kasutaja@eesti.ee
```

7.4 Andmehoidla

Haldusteenuse andmeid hoitakse failisüsteemis ja andmebaasis. Failisüsteemis hoitakse andmeid, mis on pärit välistest süsteemidest ja on haldusteenusesse üle kantud faili kujul. Andmebaasis hoitakse andmeid, mis on genereeritud haldusteenuse töö käigus.

Failisüsteemis hoitavad haldusteenuse andmed:

- `/etc/ivxv/` – kogumisteenusele rakendatud ja hetkel kehtivad seadistus- ja nimekirjafailid;
- `/var/lib/ivxv/` – kogumisteenuse haldusteenuse andmefailid;
- `/var/lib/ivxv/admin-ui-data/` – haldusteenuse veebiliidese jaoks serveeritavad JSON-failid;
- `/var/lib/ivxv/admin-ui-data/status.json` – kogumisteenuse seisundi koondandmed;
- `/var/lib/ivxv/admin-ui-permissions/` – haldusteenuse veebiliidese kasutajaõigused (Apache veebiserveri jaoks);
- `/var/lib/ivxv/ballot-box/` – allalaaditava e-urni salvestamise kataloog;
- `/var/lib/ivxv/commands/` – kogumisteenuse juhtimiseks rakendatud korraldusfailide ajalugu;
- `/var/lib/ivxv/commands/<command-type>-<timestamp>.bdoc` – digitaalselt allkirjastatud korraldus BDOC vormingus.
- `/var/lib/ivxv/db/` – haldusteenuse andmebaasi kataloog;
- `/var/lib/ivxv/db/ivxv-management.db` – haldusteenuse andmebaasi fail;
- `/var/lib/ivxv/upload/` – kogumisteenusesse veebiliidese kaudu laaditud failid;

Andmebaasis hoitavad haldusteenuse andmed (andmeväli - kirjeldus):

- `collector/status` – kogumisteenuse olek;
- `config/election` – kogumisteenuses rakendatud valimiste seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `config/technical` – kogumisteenuses rakendatud tehnilisele seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `config/trust` – kogumisteenuses rakendatud usaldusjuure seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `election/election-id` – valimiste identifikaator;
- `election/electionstart` – valimiste algusaeg;
- `election/electionstop` – valimiste lõpuaeg;
- `election/servicestart` – kogumisteenuse käivitamise aeg;
- `election/servicestop` – kogumisteenuse seiskamise aeg;
- `list/choices` – haldusteenusesse laaditud valikute nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/choices-loaded` – nimekirjateenustesse laaditud valikute nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/voters<list-number>` – haldusteenusesse laaditud valijate nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/voters<list-number>-loaded` – nimekirjateenustesse laaditud valijate nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `user/<idcode>` – haldusteenuse kasutaja nimi ja rollid kujul `<surname,name> <role>[,<role>]`;
- `service/<service-id>/service-type` – Teenuse liik;
- `service/<service-id>/technical-conf-version` – Teenusele rakendatud tehnilise seadistuse versioon;
- `service/<service-id>/election-conf-version` – Teenusele rakendatud valimiste seadistuse versioon;
- `service/<service-id>/state` – Teenuse olek;
- `service/<service-id>/last-data` – Teenuse viimase oleku hankimise aeg;
- `service/<service-id>/ip-address` – Teenuse IP-aadress;

Kasutatud tähised:

- `<command-type>` – korralduse liik:
  1. `trust` – usaldusjuure seadistused;
  2. `technical` kogumisteenuse seadistused;
  3. `election` valimiste seadistused;
- `<CN>` – ID-kaardi CN väli kujul `PEREKONNANIMI,EESNIMI,ISIKUKOOD`;
- `<config-type>` on seadistuse liik. Usaldusjuure seadistus on `trust`, valimiste seadistus on `election` ja kogumisteenuse tehniline seadistus on `tech`;

- `<list-number>` valimisnimekirja kahekohaline järjekorranumber, esimene nimekiri kannab numbrit 01.
- `<service-id>` teenuse identifikaator kogumisteenuse seadistustest;
- `<timestamp>` on ajatempel ISO-8601 vormingus.