IVXV seadistuste koostamise juhend

Juhend

Versioon 1.7.6

27.09.2021

65 lk

Dok IVXV-JSK-1.7.6

Sisukord

PEATÜKK 1

Annotatsioon

Käesolev dokument sisaldab elektroonilise hääletamise infosüsteemi IVXV rakenduste ja kogumisteenuse seadistuste ülevaadet ja koostamise juhendit.

PEATÜKK 2

IVXV seadistused valimise korraldamise protsessis

IVXV kasutamiseks valimise kontekstis tuleb süsteem ja sellega seotud rakendused seadistada nii, et on võimalik valijatelt häälte vastuvõtmine ning nende käitlemine vastavalt süsteemile seatud terviklus-, konfidentsiaalsus ja käideldavusnõuetele. Käesolev tehniline dokument annab ülevaate olulisimatest seadistustoimingutest ning on mõeldud täiendama elektroonilise hääletamise käsiraamatu poolt kirjeldatud protseduurireeglite täitmist.

2.1 Seadistuste koostamiseks vajalikud andmed

Valimise üldparameetrid Valimise üldparameetrid määravad valimise unikaalse identifikaatori kasutamiseks kõigi seotud komponentide poolt, küsimuste arvu ning identifikaatorid, hääletamisperioodi alguse- ja lõpuaja ning hääle kontrollimise seadistuse. Valimise üldparameetrite spetsifikatsiooni käsitletakse käesolevas dokumendis.

Algne valijate nimekiri Algne valijate nimekiri on kohandatud vormingus fail, mille vorming ning seotud protokollid on defineeritud dokumendis „IVXV protokollid“. Eesti riiklike valimiste korral tuleb algne valijate nimekiri Rahvastikuregistrist.

Valikute nimekiri Valikute nimekiri on JSON vormingus fail, mille vorming ning seotud protokollid on defineeritud dokumendis „IVXV protokollid“. Eesti riiklike valimiste korral tuleb valikute nimekiri valimiste infosüsteemist.

Ringkondade nimekiri Ringkondade nimekiri on JSON vormingus fail, mille vorming ning seotud protokollid on defineeritud dokumendis „IVXV protokollid“. Eesti riiklike valimiste korral tuleb ringkondade nimekiri valimiste infosüsteemist.

Rakenduste usaldusjuur Rakenduste usaldusjuur defineerib sertifitseerimishierarhia(d), mille alusel IVXV rakendused verifitseerivad digitaalallkirju. Eesti riiklike

valimiste korral määrab usaldusjuure koosseisu Riigi Valimisteenistus. Rakenduste usaldusjuure vormingut käsitletakse peatükis IVXV rakendused (ptk. 3).

Kogumisteenuse usaldusjuur Kogumisteenuse usaldusjuur defineerib sertifitseerimishierarhia(d), mille alusel IVXV kogumisteenuse komponendid verifitseerivad digitaalallkirju. Eesti riiklike valimiste korral määrab usaldusjuure koosseisu Riigi Valimisteenistus. Kogumisteenuse usaldusjuure vormingut ning seotud protokolle käsitletakse peatükis Kogumisteenus (ptk. 7).

Kogumisteenuse tehniline seadistus Kogumisteenuse tehniline seadistus kirjeldab IVXV mikroteenuste seadistuse ning isendite jaotumise. Eesti riiklike valimiste korral leiab kogumisteenuse osutaja Riigi Valimisteenistus. Tehniline seadistus kooskõlastatakse valimiste omaniku ja kogumisteenuse osutaja vahel. Tehnilist seadistust käsitletakse peatükis Kogumisteenuse tehnilise seadistususe koostamine (ptk. 7.3).

Kogumisteenuse võtmed ja sertifikaadid Kogumisteenuse mikroteenused suhtlevad omavahel TLS protokolli vahendusel. Vastavad sertifikaadid tuleb eksportida Valijarakendusse ja Kontrollrakendusse. Kogumisteenusega seotud võtmete loomist käsitletakse peatükis Kogumisteenuse krüptovõtmed (ptk. 7.7).

Häälte salastamise võtme spetsifikatsioon Häälte salastamise võtme jaoks kasutatav algoritm ning seotud tehnilised parameetrid fikseeritakse enne häälte salastamise võtme genereerimist. Võtme spetsifikatsiooni käsitletakse peatükis Häälte salastamise võtme spetsifikatsiooni valimine (ptk. 4.1).

2.2 Hääletamisperioodile eelnevad tegevused

Enne hääletamisperioodi algust teostatakse lähtuvalt eelnevatest andmetest järgmised tegevused:

1. Rakenduste paigaldamine (ptk. 3.1)
2. Rakenduste usaldusjuure kirjeldamine (ptk. 3.2)
3. Häälte salastamise võtme spetsifikatsiooni valimine (ptk. 4.1)
4. Häälte salastamise võtme genereerimine (ptk. 4.2)
5. Häälte salastamise võtme testimine (ptk. 4.3)
6. Kogumisteenuse usaldusjuure seadistamine (ptk. 7.2)
7. Kogumisteenuse tehnilise seadistususe koostamine (ptk. 7.3)
8. Kogumisteenusele valimise seadistuse koostamine (ptk. 7.4)
9. Ringkondade nimekirja laadimine Kogumisteenusesse
10. Valikute nimekirja laadimine Kogumisteenusesse
11. Valijate nimekirja (algne) laadimine Kogumisteenusesse
12. Kogumisteenuse volituste kirjeldamine (ptk. 7.6)
13. Valijarakenduse seadistamine (ptk. 8)
14. Kontrollrakenduse seadistamine (ptk. 9)

2.3 Hääletamisperioodi tegevused

1. Valijate nimekirjade (muudatused) laadimine Kogumisteenusesse

2.4 Hääletamisperioodile järgnevad tegevused

E-valimiskasti töötlemine

1. E-valimiskasti töötlemine - verifitseerimine (ptk. 5.1)
2. E-valimiskasti töötlemine - korduvhäälte tühistamine (ptk. 5.2)
3. E-valimiskasti töötlemine - häälte tühistamine ja ennistamine jaoskonnainfo põhjal (ptk. 5.3)
4. E-valimiskasti töötlemine - anonüümistamine (ptk. 5.4)

Häälte miksimine

1. Miksneti Verificatum paigaldamine (ptk. 10.1)
2. E-häälte miksimine (ptk. 10.2)
3. Miksimistõendi verifitseerimine (ptk. 10.3)

Hääletamistulemuse väljaselgitamine ja andmeaudit

1. E-häälte dekrüpteerimine (ptk. 4.4)
2. E-häälte korrektse teisendamise kontroll (ptk. 6.1)
3. E-häälte miksimistõendi kontroll (ptk. 6.2)
4. E-häälte lugemistõendi kontroll (ptk. 6.3)

PEATÜKK 3

IVXV rakendused

3.1 Rakenduste paigaldamine

IVXV rakendused on:

- võtmerakendus *key* (Võtmerakendus (ptk. 4)),
- töötlemisrakendus *processor* (Töötlemisrakendus (ptk. 5)),
- auditirakendus *auditor* (Auditirakendus (ptk. 6)).

IVXV rakendused on arendatud programmeerimiskeeles Java, kasutusel on Java 11. Rakendused on testitud Windows 10 ja Ubuntu 20.04 platvormil kasutades OpenJDK-d või Oracle Javat.

Rakendused tarnitakse ZIP-vormingus failidena:

```
<rakendus>-<tarnenumber>.zip
```

Peale ZIP-faili lahti pakkimist tekib kataloogipuu:

```
<rakendus>-<tarnenumber>
|-- bin
|   |-- <rakendus>
|   |-- <rakendus.bat>
|-- lib
|   |-- *.jar
```

Kui kataloogitee *<rakendus>-<tarnenumber>/bin* panna *PATH*'i, saab rakendust edaspidi käivitada käsurealt:

```
$ <rakendus>
```

Rakendusi paigaldades tuleb arvestada, et kesksüsteemi protokollides kirjeldatud raportid kasutavad ilma ajavööndita aja vormingut (*yyyymmddhhmmss*). Ajavööndiga ajamärgendi (näiteks hääletamise aeg kogumisteenuselt saadud e-valimiskastis) esitamiseks raportis teisendavad Java rakendused ajamärgendi esmalt operatsioonisüsteemi ajavööndisse ning seejärel eemaldavad ajavööndi info. Seetõttu tuleb rakendusi käivitavates masinates seadistada ajavöönd selliseks, millise kohalikus ajas soovitakse ajamärgendeid näha.

3.2 Rakenduste usaldusjuure kirjeldamine

Rakenduste kasutamine eeldab digitaalselt allkirjastatud seadistuste kasutamist. Allkirjade verifitseerimiseks vajalikud sertifikaadid tuleb rakendusele ette anda usaldusjuure koosseisus. Usaldusjuur on samuti digitaalselt allkirjastatud.

Usaldusjuure seadistuse koostab valimiste korraldaja.

ca Komadega eraldatud loetelu konteineris sisalduvatest CA sertifikaatidest ja vahesertifikaatidest.

ocsp Komadega eraldatud loetelu konteineris sisalduvatest OCSP sertifikaatidest.

tsa Komadega eraldatud loetelu konteineris sisalduvatest ATO sertifikaatidest.

Kõik sertifikaadid antakse PEM vormingus.

Rakendusele esitatakse usaldusjuur BDOC konteineris, kus usaldusjuure spetsifikatsioon on kirjeldatud failis *ivxv.properties* ning kõik juure elemendid on konteinerisse laaditud.

Näide

`ivxv.properties`:

```
1 ca = EE-GovCA2018.pem.crt, ESTEID2018.pem.crt, ESTEID-SK_2015.pem.
  ↪crt
2 ocsp = SK_OCSP_RESPONDER_2011.pem.crt
3 tsa = SK_TIMESTAMPING_AUTHORITY_2019.pem.crt, SK_TIMESTAMPING_
  ↪AUTHORITY_2020.pem.crt, SK_TIMESTAMPING_AUTHORITY_2021.pem.crt
```

3.3 Rakenduste käivitamine

Rakendusi käivitatakse käsurealt, nende toimimist juhitakse käsureaparameetrite ja digitaalselt allkirjastatud seadistustega. Kõik rakendused väljastavad vajadusel abiinfot:

```
$ <rakendus> --help

Rakendus 'rakendus'         - Rakendus

Kasutamine:
  <rakendus> <tööriist> --conf <conf> [--params <params>] [--force
↪<force>] [--quiet <quiet>] [--lang <lang>] [--container_threads
↪<container_threads>] [--threads <threads>]
  <rakendus> <tööriist> -h | --help
  <rakendus> -h | --help

Tööriistad:
  tool_foo          - Tegevuse FOO teostamine
  tool_bar          - Tegevuse BAR teostamine

Käsurea argumendid:
  -h --help              - Abi
  -c --conf (*)          - Konfiguratsioon
  -p --params            - Tööriista parameetrid
  -f --force             - Ära küsi kasutajalt kinnitust
  -q --quiet             - Vaikne käivitusrežiim
  --lang                 - Keel
  -ct --container_threads - Allkirjastatud konteinerite teegi poolt␣
↪kasutatav lõimede arv (<= 0 korral dünaamiline)
  -t --threads           - Rakenduse poolt paralleeltöötluse korral␣
↪kasutatav lõimede arv (<= 0 korral dünaamiline)
Rakendus lõpetas töö ilma vigadeta
```

Rakenduste kasutamisel tuleb määrata konkreetne tööriist, usaldusjuur ning seadistusfail:

```
$ <rakendus> tool_foo --conf usaldusjuur.asice --params tool_foo.
↪conf.asice

Konfiguratsiooni laadimine failist usaldusjuur.asice
Konfiguratsiooni allkirja kontrollimine
Konfiguratsiooni allkirja on andnud NIMI NIMESTE
Konfiguratsiooni allkirja andmise aeg on 24.12.2018 18:00
Konfiguratsiooni allkiri on korrektne ja kehtiv

FOO!

Rakendus lõpetas töö ilma vigadeta
```

Juhised rakenduste tööriistade ning nende seadistusfailide koostamise kohta antakse järgmistes peatükkides. Käsureaargumendid on kõigil rakendustel samad:

-h –help Abiinfo kuvamine kas rakenduse või konkreetse tööriista kohta.

-c –conf (*) Digitaalselt allkirjastatud fail usaldusjuurega. Kohustuslik parameeter.

-p –params Digitaalselt allkirjastatud tööriista parameetrid.

-f –force Ära küsi kasutajalt kinnitust.

-q –quiet Vaikne käivitusrežiim.

–lang Juhul kui rakendus on kompileeritud mitmekeelsena, siis keele valik. Vaikimisi on rakendustes võimaldatud ainult eesti keel.

-ct –container_threads Allkirjastatud konteinerite teegi poolt kasutatav lõimede arv. Vaikimisi valitakse lõimede arv teegi poolt dünaamiliselt lähtudes saadaolevate tuumade arvust.

-t –threads Rakenduse poolt paralleeltöötluse korral kasutatav lõimede arv. Vaikimisi valitakse lõimede arv rakenduse poolt dünaamiliselt lähtudes saadaolevate tuumade arvust.

Rakendustest eksisteerivad nii tooteversioonid kui testversioonid. Testrakendused on kohaldatud protseduuride efektiivseks testimiseks, kuid ei sobi valimiste tegelikuks läbiviimiseks. Näiteks ei võimalda võtmerakenduse testversioon kasutada kiipkaarte. Testversioonid rakendustest kuvavad käivitamisel hoiatuse:

```
**********************************************************************
*                            !!! HOIATUS !!!                         *
*                                                                    *
* Rakendus on käivitatud arendusrežiimis ning rakenduse käitumine    *
* võib erineda tavarežiimist.                                        *
* Rakenduse käivitamiseks tavarežiimis tuleb rakendus ümber          *
* kompileerida.                                                      *
**********************************************************************
```

3.4 Rakenduste käivituskeskkonna parameetrid

Suure e-valimiskasti auditeerimisel, töötlemisel või dekrüpteerimisel, võib olla tarvilik suurendada protsessi mälupiirangut.

Seda saab teha kasutades rakendusespetsiifilist keskkonnamuutujat `{RAKENDUS}_OPTS`, mis defineerib täiendavad argumendid Java virtuaalmasinale. `{RAKENDUS}` on üks kolmest `AUDITOR`, `KEY` või `PROCESSOR`. Protsessi mälupiirangu suurendamiseks tuleb kasutada argumenti `-Xmx{N}G`, kus `{N}` on mälupiirangu suurus gigabaitides.

Näiteks 10 gigabaidi mälu eraldamiseks töötlemisrakendusele tuleb seada `PROCESSOR_OPTS=-Xmx10G`.

Tabel 3.1: Rakenduste mälupiirangu parameetrid

Rakendus	Vaikimisi mälupiirang	Keskkonnamuutuja
Auditirakendus	8GB	`AUDITOR_OPTS`
Töötlemisrakendus	8GB	`PROCESSOR_OPTS`
Võtmerakendus	Puudub	`KEY_OPTS`

Rakendused töötavad nii 32-bitise kui 64-bitise Java andmemudeliga, samas efektiivseimaks toimimiseks tuleb rakendusi kasutada 64-bitisel platvormil 64-bitise Java andmemudeliga. Juhul kui rakendus ei suuda käivitamisel 64-bitist mudelit tuvastada kuvatakse hoiatus:

```
*****************************************************************
*                          !!! HOIATUS !!!                      *
*                                                               *
* 64-bitise Java andmemudeli tuvastamine ebaõnnestus. Rakendus on  *
* vähemefektiivsem. Rakenduse jõudluse suurendamiseks tuleb        *
* kasutada 64-bitise andmemudeliga Java keskkonda.                 *
*****************************************************************
```

Juhul kui rakenduse mälupiirang on 4GB või rohkem, ei ole 32-bitise andmemudeliga Java võimeline rakendust käivitama. Kuvatakse järgmine veateade:

```
Invalid maximum heap size: -Xmx4G
The specified size exceeds the maximum representable size.
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.
```

PEATÜKK 4

Võtmerakendus

Võtmerakendus *key* koosneb tööriistadest *groupgen*, *init*, *testkey*, *decrypt* ja *util*. Kõigi tööriistade kasutamine eeldab allkirjastatud usaldusjuure ja konkreetse tööriista seadistuste olemasolu. Alljärgnevalt kirjeldame konkreetsete tööriistade seadistusi.

4.1 Häälte salastamise võtme spetsifikatsiooni valimine

Kasutamaks ElGamali krüptosüsteemi häälte krüpteerimiseks, on oluline häälte salastamise võtme spetsifikatsiooni valimine ehk kasutatavate rühma parameetrite valimine, milles tehakse matemaatilisi operatsioone. Oluline on, et antud parameetrid oleksid valitud läbipaistvalt, vältimaks tagauste olemasolu, mille abil oleks võimalik ilma salajast võtit omamata krüpteeritud hääli avada.

Kuna turvalisuse jaoks peavad rühma parameetrid vastama teatud tingimustele, siis nende valimiseks pole kiiret meetodit. Sobivate rühmaparameetrite leidmiseks tuleb juhuslikult valida mingid parameetrid ja kontrollida, kas need vastavad antud tingimustele.

Rühma parameetrite genereerimise protsessi on võimalik läbipaistvalt läbi viia kahel viisil:

1. Kasutades teadaolevaid defineeritud parameetreid
2. Parameetreid avaliku algoritmi alusel deterministlikult genereerides

Teadaolevate parameetrite kasutamine

Mitmed standardid ja rakendused on juba defineerinud parameetrid, mida on sobiv kasutada ElGamal krüptosüsteemis. Kasutades laialt levinud parameetreid on suurem tõenäosus, et neid on sõltumatult kontrollitud.

Üheks selliseks standardiks on [RFC3526], mis kasutab samuti deterministlikku parameetrite genereerimist. Antud standardi korral saab kontrollida defineeritud parameetrite korrektsust järgneva Sage skriptiga:

```
#!/usr/bin/env sage

from sage.all import *

n = 3072
p_found = False
c = 0

while not(p_found):
    if (Mod(c,10000) == 0):
        print("c is: ", c)
    p = 2**n - 2**(n-64) - 1 + 2**64*(floor(2**(n-130)*pi.
↪n(prec=10000))+c)
    if is_pseudoprime(p):
        print(p, " is prime")
        q = (p-1)/2
        if is_pseudoprime(q):
            print(p, " is safe prime")
            p_found = True
    c = c + 1
```

Uute parameetrite deterministlik ja kontrollitav genereerimine

ElGamal krüptosüsteemi jaoks sobilikke parameetreid saab genereerida kasutades tööriista *groupgen*.

Võtmespetsifikatsiooni genereerimine on ajaliselt mahukas tegevus, mis võib olenevalt riistvarast kesta tunde. Ühekordselt genereeritud rühm on kasutatav mitmetel valimistel.

groupgen.paramtype ElGamal'i krüptosüsteemi töö aluseks oleva rühma tüüp. Toetatud väärtused:

1. mod - jäägiklassiring Zp
2. ec - elliptkõverad

groupgen.length ElGamal'i krüptosüsteemi töö aluseks olevat rühma iseloomustav turvaparameeter. Jäägiklassiringide korral on sobiv väärtus 3072. Elliptkõveraid kasutades on toetatud kõver P-384, mille kasutamiseks tuleb sisestada väärtus 384.

groupgen.init_template Asukoht, kuhu kirjutatakse rühma parameetrid. Väljund sobib kasutamiseks võtme genereerimise seadistuse koostamisel.

groupgen.random_source Juhuarvugeneraatori sisendiks kasutatavate allikate loetelu. Vaata ka Juhuarvude genereerimine võtmerakendus-es (ptk. 4.6).

Kasutades juhuslike parameetrite leidmiseks juhuarvugeneraatorit, mille algväärtus on üheselt defineeritav ning avalikustatud, võivad kolmandad osapooled kontrollida, et avaldatud rühma parameetrid on esimesed sellised leitud parameetrid, mis vastavad tingimustele. Näitekonfiguratsioon kasutab DPRNG'd avaliku seemnefailiga. Vaata ka Juhuarvude genereerimine võtmerakenduses (ptk. 4.6).

`key.groupgen.yaml`:

```
groupgen:
  paramtype: mod
  length: 3072
  init_template: key.init.template.yaml
  random_source:
  - random_source_type: DPRNG
    random_source_path: public_seed_file
```

Sellise seadistuse korral loetakse juhuarvugeneraatori algväärtus failist `public_seed_file`. Oluline on, et sellisel juhul käivitatakse võtmerakendus ühelõimelisena:

```
$ key groupgen --conf usaldusjuur.asice --params key.groupgen.asice␣
↪--threads 1
```

4.2 Häälte salastamise võtme genereerimine

Häälte salastamise võtme genereerimiseks kasutatakse võtmerakenduse tööriista *init*. Võti genereeritakse seadistustes näidatud läviskeemiga MofN, mis tähendab, et N võtmehaldurist peavad häälte dekrüpteerimisel osalema vähemalt M haldurit, vastasel juhul ei ole dekrüpteerimine võimalik.

init.identifier Valimise unikaalne identifikaator.

init.out Võtmerakenduse tööriista *init* väljundkataloog. Sellesse kataloogi tekivad

1. PEM vormingus allkirjavõtme sertifikaat (sign.pem)
2. PEM vormingus krüpteerimisvõtme sertifikaat (enc.pem)
3. PEM vormingus krüpteerimisvõti (pub.pem)
4. DER vormingus krüpteerimisvõti (pub.der)

init.skiptest Võtmeosakute kontrolltestide vahelejätmine.

init.fastmode Kaartidele automaatne terminalide määramine. Vaikimise väärtus on tõene.

---

init.paramtype ElGamal krüptosüsteemi aluseks oleva rühma parameetrid, mis ühtlasi määravad võtme turvataseme.

init.paramtype.mod Jäägiklassiringi määravad parameetrid kümnendesituses. Parameetrid võib luua võtmerakenduse tööriista *groupgen* kasutades.

init.paramtype.mod.p Jäägiklassiringi moodul.

init.paramtype.mod.g Jäägiklassiringi generaator.

---

init.signaturekeylen Võtmerakenduse poolt genereeritava allkirjastamise võtme pikkus.

init.signcn Võtmerakenduse poolt loodava allkirjastamise sertifikaadi subjekti nimi (väli *CN*).

init.signsn Võtmerakenduse poolt loodava allkirjastamise sertifikaadi järjekorranumber.

init.enccn Võtmerakenduse poolt loodava krüpteerimise sertifikaadi subjekti nimi (väli *CN*).

init.encsn Võtmerakenduse poolt loodava krüpteerimise sertifikaadi järjekorranumber.

---

init.required_randomness Juhuslikkuse allikatest loetava entroopia kohustuslik hulk baitides.

init.random_source Juhuarvugeneraatori sisendiks kasutatavate allikate loetelu. Vaata ka Juhuarvude genereerimine võtmerakenduses (ptk. 4.6).

---

init.genprotocol Võtme genereerimiseks kasutatava algoritmi ja läviskeemi spetsifikatsioon.

init.genprotocol.desmedt Algoritmi Desmedt korral genereeritakse võti usaldatava osakujagaja poolt ehk võtmerakenduse mälus. Privaatvõtme osakud talletatakse kiipkaartidel.

Täiendavalt tuleb määrata läviskeemi osaliste arv ja minimaalne kvoorum.

Kaartide arv 7 - võimalikud kvoorumid 1,2,3,4 - soovitatav kvoorum 4
Kaartide arv 8 - võimalikud kvoorumid 1,2,3,4 - soovitatav kvoorum 4
Kaartide arv 9 - võimalikud kvoorumid 1,2,3,4,5 - soovitatav kvoorum 5

init.genprotocol.desmedt.threshold Läviskeemi M väärtus - kvoorum.

init.genprotocol.desmedt.parties Läviskeemi N väärtus.

`key.init.yaml`:

```yaml
init:
  identifier: TESTCONF
  paramtype:
    mod:
      p: 58096059953699580627919159656392014021766122269029005337..
      g: 2
  out: initout
  skiptest: true
  fastmode: true
  signaturekeylen: 3072
  signcn: SIGNATURE
  signsn: 1
  enccn: ENCRYPTION
  encsn: 2
  required_randomness: 128
  random_source:
  - random_source_type: file
    random_source_path: randomness_file
  - random_source_type: system
  - random_source_type: DPRNG
    random_source_path: seed_file
  - random_source_type: stream
    random_source_path: /dev/urandom
  - random_source_type: user
    random_source_path: user_entropy.exe
  genprotocol:
    desmedt:
      threshold: 2
      parties: 3
```

4.3 Häälte salastamise võtme testimine

Häälte salastamise võtme testimine kontrollib võtme rekonstrueerimise võimekust selliselt, et iga osak osaleb vähemalt kahes kvoorumis. Testimiseks on vajalik kõigi osakute osalemine.

testkey.identifier Valimise unikaalne identifikaator.

testkey.out Krüpteerimise avaliku võtme asukoha kataloog.

testkey.threshold Testimiseks kasutatav lävi, sama mis võtme loomisel spetsifitseeritud.

testkey.parties Testimiseks kasutatav osapoolte arv, sama mis võtme loomisel spetsifitseeritud.

testkey.fastmode Kaartidele automaatne terminalide määramine. Vaikimise väärtus on tõene.

`key.testkey.yaml`:

```
testkey:
  identifier: TESTCONF
  out: initout
  threshold: 2
  parties: 3
  fastmode: false
```

4.4 E-häälte dekrüpteerimine

Elektrooniliste häälte dekrüpteerimiseks kasutatakse võtmerakenduse tööriista *decrypt*. Dekrüpteerimise õnnestumiseks peab osalema läviskeemi poolt määratud kvoorumi jagu võtmehaldureid. Kui rakendati skeemi 5of9, siis osaleb dekrüpteerimisel täpselt 5 võtmehaldurit. Vähema arvu haldurite korral ei ole dekrüpteerimine võimalik.

decrypt.identifier Valimise unikaalne identifikaator.

---

decrypt.protocol

decrypt.protocol.recover Algoritmi Desmedt korral genereeritakse võti usaldatava osakujagaja poolt ehk võtmerakenduse mälus. Privaatvõtme osakud talletatakse kiipkaartidel.

decrypt.protocol.recover.threshold Läviskeemi M väärtus - kvoorum, mis spetsifitseeriti võtme loomisel.

decrypt.protocol.recover.parties Läviskeemi N väärtus, mis spetsifitseeriti võtme loomisel.

---

decrypt.anonballotbox Töötlemisrakenduse või miksimisrakenduse poolt loodud e-valimiskast anonüümistatud häältega.

decrypt.anonballotbox_checksum Anonüümistatud häältega e-valimiskasti allkirjastatud SHA256 kontrollsummafail.

decrypt.questioncount Küsimuste arv anonüümistatud e-valimiskastis. Vaikimisi väärtus on 1.

decrypt.candidates Valimise valikute nimekiri allkirjastatud kujul.

decrypt.districts Valimise ringkondade nimekiri allkirjastatud kujul.

decrypt.provable Valikuline korrektse dekrüpteerimise tõestuse väljastamine. Vaikimisi väärtus on tõene.

decrypt.check_decodable Krüptogrammide korrektsuse kontrollimine enne dekrüpteerimist. Juhul kui krüptogrammide sisend ei tule usaldatud allikast, siis tuleb kontrollida krüptogrammide korrektsust. Usaldatud allikad on töötlemisrakendus ning miksija. Vaikimisi väärus on väär.

decrypt.out Võtmerakenduse tööriista *decrypt* väljundkataloog. Eduka dekrüpteerimise korral tekivad siia kausta:

1. Elektroonilise hääletamise tulemus
2. Elektroonilise hääletamise tulemuse signatuur
3. Loend kehtetutest sedelitest
4. Lugemistõend

`key.decrypt.yaml`:

```
decrypt:
  identifier: TESTCONF
  protocol:
    recover:
      threshold: 2
      parties: 3
  anonballotbox: TESTCONF-bb-4.json
  anonballotbox_checksum: TESTCONF-bb-4.json.sha256sum.bdoc
  candidates: TESTCONF.choices.bdoc
  districts: TESTCONF.districts.bdoc
  provable: true
  check_decodable: false
  out: decout
```

Pärast dekrüpteerimist on võimalik kontrollida väljastatud elektroonilise hääletamise tulemuse signatuuri korrektsust. Selleks tuleb teha järgnevad sammud:

1. Eraldada allkirja kontrollimise võti allkirjastamise sertifikaadist:

```
openssl x509 -in initout/sign.pem -noout -pubkey > sign.pub
```

2. Kontrollida hääletamise tulemuse allkirja:

```
openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt \
rsa_pss_saltlen:32 -sigopt rsa_mgf1_md:sha256 -verify sign.pub \
-signature decout/TESTCONF.tally.signature decout/TESTCONF.tally
```

Korrektse allkirja korral kuvatakse väärtust *Verified OK*.

4.5 Võtmerakenduse täiendavad tööriistad

util.listreaders Loetle ühendatud kaardilugejad.

`key.util.yaml`:

```
util:
  listreaders: true
```

4.6 Juhuarvude genereerimine võtmerakenduses

Võtmerakenduse tööriistad *groupgen* ja *init* vajavad oma tööks juhuarve, mille genereerimiseks on võimalik kasutada erinevaid entroopiaallikaid, mis võtmerakenduse poolt üheks allikaks kombineeritakse.

Kombineerimisel on oluline, et säiliks sisendite sõltumatus, st. kombineeritud väljund ei tohi olla kehvem ühestki sisendist. IVXV raamistikus toimub entroopia kombineerimine SHAKE-256 muutuva väljundipikkusega räsifunktsiooni abil (XOF), kasutades skeemi nagu on kirjeldatud [BDPA10].

Lõpliku pikkusega entroopiaallika kasutamisel loetakse kogu väärtus ning antakse see SHAKE-256 sisendiks. Piiramata pikkusega allika lisamisel salvestatakse selle viide kombineerija mällu.

Pärides kombineerijast töödeldud juhuslikkust, loetakse kõigepealt igast salvestatud entroopia allikast sama palju baite ning antakse see SHAKE-256 sisendiks. Seejärel kopeeritakse SHAKE-256 isend, muudetakse kopeeritud SHAKE-256 režiim lugemisele ning loetakse nõutud baitide jagu väljundit.

random_source Juhuarvugeneraatori sisendiks kasutatavate allikate loetelu.

random_source.random_source_type Juhuarvugeneraatori allika tüüp.

random_source.random_source_path Juhuarvugeneraatori allika seadistatav asukoht. Argument on valikuline sõltuvalt allika tüübist.

---

random_source_type: file Entroopia lugemine failist.

random_source_path: *randomness_file* Kasutatav fail.

---

random_source_type: system Operatsioonisüsteemi poolt pakutav entroopiaallikas (Linuxil */dev/urandom*).

---

random_source_type: DPRNG Deterministlik pseudojuhuslik generaator (DPRNG) on mõeldud baidijadade genereerimiseks, kasutades etteantud seemneväärtust. Sama seemneväärtuse korral genereerib meetod alati sama jada.

random_source_path: *seed_file* DPRNG seemneväärtus saadakse viidatud faili SHA256 räsides.

---

random_source_type: stream Entroopia lugemine voogseadmelt.

random_source_path: */dev/urandom* Kasutatav seade.

---

random_source_type: user Välise programmi käest üle sokli juhuslikkust hankiv entroopiaallikas. Kasutusel on IVXV-spetsiifiline protokoll.

random_source_path: *user_entropy.exe* Tee programmini, mis tuleb juhuslikkuse hankimiseks käivitada.

Entroopiaallikate kombineerimine kirjeldatud viisil võimaldab realiseerida erinevaid juhuarvude genereerimise stsenaariumeid. Näiteks häälte salastamise võtme genereerimise korral on vaja tagada võtme konfidentsiaalsus ning olla kindel, et genereerimisprotsess ei ole hiljem korratav. Näitekonfiguratsioon kasutab välist programmi kasutaja sisendi lugemiseks ning süsteemset juhuarvugeneraatorit:

`rnd.init.yaml`:

```
init:

  [...]

  required_randomness: 128
  random_source:
  - random_source_type: system
  - random_source_type: user
    random_source_path: server.exe
```

Rakendus käivitatakse mitmelõimelisena:

```
$ key init --conf usaldusjuur.asice --params rnd.init.asice
```

Häälte salastamise võtme spetsifikatsioon on erinevalt häälte salastamise võtmest avalik ning selle genereerimisel kasutatud juhuslikkuse võib samuti teha avalikuks. Näitekonfiguratsioon kasutab DPRNG'd avaliku seemnefailiga.

`rnd.groupgen.yaml`:

```
groupgen:

  [...]

  random_source:
    - random_source_type: DPRNG
      random_source_path: public_seed_file
```

Kui eesmärk on genereerimisprotsessi korratavus, tuleb rakendus käivitada ühelõimelisena:

```
$ key groupgen --conf usaldusjuur.asice --params rnd.groupgen.asice␣
↪--threads 1
```

PEATÜKK 5

Töötlemisrakendus

Töötlemisrakendus on käsurearakendus e-valimiskasti kontrollimiseks ja edasiseks töötlemiseks peale e-hääletamise lõppu.

Töötlemisrakenduse põhilised tööriistad on *check*, *squash*, *revoke* ja *anonymize*, mis käivitatakse loetletud järjekorras vastavalt ette nähtud valimisprotseduuridele. Põhitööriistade sisendi hulgas on alati kas kogumisteenuse või eelmise tööriista poolt väljastatud e-valimiskast ja e-valimiskasti digitaalselt allkirjastatud räsi. Väljundi hulgas on töötlemisetapi tulemuseks olev e-valimiskast koos allkirjastamata räsiga. Kuna rakendused käivitatakse internetiühenduseta arvutis, tuleb räsifailid tõsta digitaalseks allkirjastamiseks välisesse seadmesse. E-valimiskasti räsi arvutatakse funktsiooniga `hex(sha256(<fail>))`.

Lisaks põhitööriistadele on rakendusel veel neli täiendavat tööriista: *export*, *verify*, *stats* ja *statsdiff*.

Kõigi tööriistade kasutamine eeldab allkirjastatud usaldusjuure ja konkreetse tööriista seadistuste olemasolu. Faile väljastavatel tööriistadel tuleb seadistustes määrata väljundkausta asukoht. Väljundkausta ei tohi käivitamise ajal olemas olla, selle loob rakendus. Alljärgnevalt on kirjeldatud tööriistade seadistusi.

5.1 E-valimiskasti töötlemine - verifitseerimine

Kogumisteenusest väljastatud e-valimiskasti verifitseerimiseks kasutatakse tööriista *check*. valimiskasti verifitseeritakse usaldusjuure, valijate nimekirjade, ringkondade nimekirja ja registreerimisteenuse väljundi vastu.

Verifitseerimise käigus kontrollitakse järgmiseid põhilisi omadusi:

- Ringkondade nimekirja ja valijate nimekirjade andmeterviklus ja kooskõlalisus;

- E-valimiskasti andmeterviklus;
- E-hääletajate valimisõigus e. kuuluvus valijate nimekirja (kontrollitakse juhul kui valijate nimekirjad on seadistustes kirjeldatud);
- E-valimiskastis sisalduvate häälte vastavus digiallkirja vormingule;
- Registreerimisandmete andmeterviklus;
- E-valimiskastis sisalduvate häälte vastavus registreerimisandmetega.

E-valimiskasti verifitseerimine on töömahukas protsess. 4-tuumalise *i7* protsessoriga arvuti suudab ühe sekundi jooksul töödelda umbes 200 häält. Töötlemise jooksul kuvatakse kasutajale edenemisriba, mille alusel on võimalik ennustada töötlemisele kuluvat aega.

check.ballotbox Kogumisteenusest väljastatud e-valimiskast.

check.ballotbox_checksum Kogumisteenusest väljastatud e-valimiskasti digitaalselt allkirjastatud räsi.
Kui määramata, siis ei väljastata korrastatud e-valimiskasti järgmisteks etappideks. Kasulik mitte-lõpliku e-valimiskasti valimisaegseks kontrolliks.

check.districts Digitaalselt allkirjastatud ringkondade nimekiri.

check.registrationlist Registreerimisteenusest pärit registreerimisandmed. Kui määramata, siis ei kontrollita e-valimiskastis sisalduvate häälte vastavust registreerimisandmetega.

check.registrationlist_checksum Registreerimisandmete digitaalselt allkirjastatud räsi. Võib puududa, kui `registrationlist` puudub.

check.tskey Registreerimispäringute verifitseerimiseks kasutatav kogumisteenuse avalik võti registreerimispäringute tegemise sertifikaadist.

check.vlkey Valijate nimekirjade verifitseerimiseks kasutatav avalik võti. Argument on kohustuslik, kui valijate nimekirjad on antud.

check.voterlists Valijate nimekirjade loend. Kui on määramata, siis e-hääletanute hääleõigust ei kontrollita.

check.voterlists.path Valijate nimekirja fail.

check.voterlists.signature Valijate nimekirja allkiri, mis on antud algoritmiga `ecdsa-with-SHA256`.

check.districts_mapping Valijate nimekirjas oleva ringkonna ja jaoskonna teisendusfail (valikuline).

check.election_start Hääletamise algusaeg. Sellest varasema hääletusajaga hääli käsitletakse proovihäältena ning need lugemisele ei lähe.

check.voterforeignehak Alaliselt välisriigis elavate valijate ringkonnakuuluvuse tuvastamiseks kasutatav EHAK-kood. Vaikeväärtus „0000“.

check.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. Tervikluskontrolliga korrastatud e-valimiskast `<valimise id>-bb-1.json`;
2. Tervikluskontrolliga korrastatud e-valimiskasti räsi `<valimise id>-bb-1.json.sha256sum`;

3. E-valimiskasti töötlemisvigade raport `ballotbox_errors.txt` (valikuline);
4. Valijate nimekirjade töötlemisvigade raport `voterlist_errors.txt` (valikuline);
5. *Log1* fail ehk vastvõetud hääled `<valimise id>.<küsimuse id>.log1`.

`processor.check.yaml`:

```
check:
  ballotbox: TESTCONF.votes.zip
  ballotbox_checksum: TESTCONF.votes.zip.sha256sum.bdoc
  districts: TESTCONF.districts.bdoc
  registrationlist: TESTCONF.registration.zip
  registrationlist_checksum: TESTCONF.registration.zip.sha256sum.
↪bdoc
  tskey: TESTCONF.ts.key
  vlkey: TESTCONF.voterfile.pub.key
  voterlists:
    - path: TESTCONF.voters_1
      signature: TESTCONF.voters_1.signature
    - path: TESTCONF.voters_2
      signature: TESTCONF.voters_2.signature
  election_start: 2017-05-01T12:00:00+03:00
  out: out-1
```

5.2 E-valimiskasti töötlemine - korduvhäälte tühistamine

Korduvate e-häälte tühistamiseks kasutatakse tööriista *squash*. Tööriista sisendiks on tööriista *check* poolt koostatud e-valimiskast. Korduvhäälte tühistamisel jäetakse alles iga hääletaja kõige hilisema hääl ja eemaldatakse kõik varasemad hääled.

squash.ballotbox Tervikluskontrolliga korrastatud e-valimiskast.

squash.ballotbox_checksum Tervikluskontrolliga korrastatud e-valimiskasti digitaalselt allkirjastatud räsi.

squash.districts Digitaalselt allkirjastatud ringkondade nimekiri.

squash.enckey Krüpteerimise avaliku võtme faili asukoht (võtmerakenduse väljund). Võtit kasutatakse krüpteeritud häälte eelkontrolliks, eristamaks päriselt krüpteeritud hääli suvalisest binaarsest prügist.

squash.out Tööriista väljundkaust. Sellesse kausta luuakse:

1. Korduvhäältest puhastatud e-valimiskast `<valimise id>-bb-2.json`;
2. Korduvhäältest puhastatud e-valimiskasti räsi `<valimise id>-bb-2.json.sha256sum`;

3. E-hääletanute nimekiri JSON-vormingus `<valimise id>-ivoterlist.json`;
4. E-hääletanute nimekiri PDF-vormingus `<valimise id>-ivoterlist.pdf`;
5. Tühistamiste ja ennistamiste aruanne `<valimise id>-revocation-report.csv`;
6. *Log2* fail ehk tühistatud hääled `<valimise id>.<küsimuse id>.log2`.

`processor.squash.yaml`:

```
1 squash:
2   ballotbox: out-1/TESTCONF-bb-1.json
3   ballotbox_checksum: out-1/TESTCONF-bb-1.json.sha256sum.bdoc
4   districts: TESTCONF.districts.bdoc
5   enckey: TESTCONF-enc.pub.key
6   out: out-2
```

5.3 E-valimiskasti töötlemine - häälte tühistamine ja ennistamine jaoskonnainfo põhjal

Häälte tühistamiseks ja ennistamiseks jaoskonnainfo põhjal kasutatakse tööriista *revoke*. Tööriist saab sisendiks tööriista *squash* poolt koostatud e-valimiskasti ning rakendab sellele sisendiks antud tühistus- ja ennistusnimekirjad.

revoke.ballotbox Korduvhäältest puhastatud e-valimiskast.

revoke.ballotbox_checksum Korduvhäältest puhastatud e-valimiskasti digitaalselt allkirjastatud räsi.

revoke.districts Digitaalselt allkirjastatud ringkondade nimekiri.

revoke.revocationlists Tühistus- ja ennistusnimekirjade loend. Võib olla tühi.

revoke.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. Korduvhääletajate häältest puhastatud e-valimiskast `<valimise id>-bb-3.json`;
2. Korduvhääletajate häältest puhastatud e-valimiskasti räsi `<valimise id>-bb-3.json.sha256sum`;
3. Tühistamiste ja ennistamiste aruanne `<valimise id>-revocation-report.csv`;
4. E-hääletanute nimekiri JSON-vormingus `<valimise id>-ivoterlist.json`;
5. *Log2* fail e. tühistatud hääled `<valimise id>.<küsimuse id>.log2`.

`processor.revoke.yaml`:

```
revoke:
  ballotbox: out-2/TESTCONF-bb-2.json
  ballotbox_checksum: out-2/TESTCONF-bb-2.json.sha256sum.bdoc
  districts: TESTCONF.districts.bdoc
  revocationlists:
    - TESTCONF.revoke_1.bdoc
    - TESTCONF.revoke_2.bdoc
  out: out-3
```

5.4 E-valimiskasti töötlemine - anonüümistamine

E-valimiskasti anonüümistamiseks kasutatakse tööriista *anonymize*. Tööriist saab sisendiks tööriista *revoke* poolt koostatud e-valimiskasti ning eemaldab sellest valijate info.

anonymize.ballotbox Korduvhääletajate häältest puhastatud e-valimiskast.

anonymize.ballotbox_checksum Korduvhääletajate häältest puhastatud e-valimiskasti digitaalselt allkirjastatud räsi.

anonymize.out Tööriista väljundkaust. Sellesse kausta luuakse:

1. Hääletajate isikuandmetest puhastatud e-valimiskast `<valimis id>-bb-4.json`;
2. Hääletajate isikuandmetest puhastatud e-valimiskasti räsi `<valimise id>-bb-4.json.sha256sum`;
3. *Log3* fail e. lugemisele läinud hääled `<valimise id>.<küsimuse id>.log3`.

`processor.anonymize.yaml`:

```
anonymize:
  ballotbox: out-3/TESTCONF-bb-3.json
  ballotbox_checksum: out-3/TESTCONF-bb-3.json.sha256sum.bdoc
  out: out-4
```

5.5 Töötlemisrakenduse täiendavad tööriistad

Tööriist *verify*

Verify on lisavahend, millega saab verifitseerida digitaalselt allkirjastatud konteineri allkirja ning kuvada konteineri andmed.

verify.file Verifitseeritav fail.

`processor.verify.yaml`:

```
verify:
  file: processor.yaml.bdoc
```

Tööriist *export*

Export on lisavahend, millega saab eksportida kogumisteenusest väljastatud e-valimiskasti seest täielikke digitaalselt allkirjastatud hääle konteinereid. On võimalik eksportida nii kõiki hääli korraga, kui konkreetse valija hääli.

export.ballotbox Kogumisteenusest väljastatud e-valimiskast.

export.ballotbox_checksum Kogumisteenusest väljastatud e-valimiskasti digitaalselt allkirjastatud räsi.

export.voter_id Valija identifikaator (valikuline).

export.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. E-valimiskasti töötlemisvigade raport `ballotbox_errors.txt` (valikuline);
2. E-valimiskastist eksporditud häälte digitaalselt allkirjastatud konteinerid.

`processor.export.yaml`:

```
export:
  ballotbox: TESTCONF.votes.zip
  ballotbox_checksum: TESTCONF.votes.zip.sha256sum.bdoc
  out: out-export
```

Tööriist *stats*

Stats on lisavahend, millega saab arvutada häälte ja hääletajate statistikat e-valimiskasti põhjal. Statistikat on võimalik piiritleda ajavahemikuga ning väljundit on võimalik piiritleda koondandmetega kui ka ringkondade kaupa. NB! Tööriist ei kontrolli digitaalallkirju, häälte töötlemiseks tuleb kasutada *check*, *squash*, *revoke*, *anonymize* töövoogu.

stats.ballotbox E-valimiskast, mille põhjal statistika koostada. Kui faili laiendiks on `.json`, siis peab see olema olema töödeldud e-valimiskast. Vastasel juhul peab see olema kogumisteenusest väljastatud e-valimiskast.

stats.election_day Valimispäev. Kõikide e-hääletanute vanused arvutatakse statistika tarbeks selle kuupäeva suhtes.

stats.period_start Statistikaperioodi algusaeg (valikuline). Sellest varasema hääletusajaga hääli statistikasse ei kaasata.

stats.period_end Statistikaperioodi lõppaeg (valikuline). Sellest hilisema hääletusajaga hääli statistikasse ei kaasata.

stats.districts Digitaalselt allkirjastatud ringkondade nimekiri. Vajalik ringkondade kaupa statistika väljastamiseks. Kui on määramata, siis väljastatakse ainult koondstatistika.

stats.vlkey Valijate nimekirjade verifitseerimiseks kasutatav avalik võti. Argument on kohustuslik valijate nimekirjade kasutamise korral.

stats.voterlists Valijate nimekirjade loend. Vajalik kogumisteenusest väljastatud e-valimiskastist valija ringkonna tuvastamiseks.
Argument on kohustuslik, kui e-valimiskast on väljastatud kogumisteenusest ja statistikat väljastatakse ringkondade kaupa.

stats.voterlists.path Valijate nimekirja fail.

stats.voterlists.signature Valijate nimekirja allkiri, mis on antud algoritmiga `ecdsa-with-SHA256`.

check.voterforeignehak Alaliselt välisriigis elavate valijate ringkonnakuuluvuse tuvastamiseks kasutatav EHAK-kood. Vaikeväärtus „0000“.

stats.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. E-valimiskasti statistika JSON-vormingus `<valimise id>-stats.json` (`ELECTION-stats.json` kui valimist ei suudeta tuvastada);
2. E-valimiskasti statistika CSV-vormingus `<valimise id>-stats.csv` (`ELECTION-stats.csv` kui valimist ei suudeta tuvastada);
3. E-valimiskasti töötlemisvigade raport `ballotbox_errors.txt` (tekib vigade korral);
4. Valijate nimekirjade töötlemisvigade raport `voterlist_errors.txt` (tekib vigade korral).

`processor.stats.yaml`:

```
stats:
  ballotbox: TESTCONF.votes.zip
  election_day: 2018-11-11
  period_start: 2018-11-01T10:00:00+03:00
  period_end:   2018-11-07T22:00:00+03:00
  districts: TESTCONF.districts.bdoc
  vlkey: TESTCONF.voterfile.pub.key
  voterlists:
    - path: TESTCONF.voters_1
      signature: TESTCONF.voters_1.signature
    - path: TESTCONF.voters_2
      signature: TESTCONF.voters_2.signature
  out: out-stats
```

Tööriist *statsdiff*

Statsdiff on lisavahend, millega saab arvutada kahe statistikafaili vahet. Tulemuseks on kolmas statistikafail, mille kõik väärtused on pärit alusfailist, kust on lahutatud võrreldava faili väärtused.

statsdiff.compare Statistika võrdluse alusfail JSON-vormingus.

statsdiff.to Võrreldav statistika fail JSON-vormingus.

statsdiff.diff Tööriista väljundfail. Sellesse faili salvestatakse statistikate vahe JSON-vormingus.

`processor.statsdiff.yaml`:

```
1 statsdiff:
2   compare: out-stats/TESTCONF-stats.json
3   to: TESTCONF-voting-stats.json
4   diff: TESTCONF-stats-diff.json
```

PEATÜKK 6

Auditirakendus

IVXV võtmerakendus võimaldab kasutada tõestatavat dekrüpteerimist - koos tulemusega väljastatakse lugemistõend e-häälte korrektse avamise kohta. Vältimaks häälte salajasuse rikkumist lugemistõendi kontrollil võimaldab IVXV kasutada häälte miksimist, mis säilitab häälte sisu kuid eemaldab krüptograafiliselt seose konkreetse hääle ja selle hääle andnud isiku vahel.

IVXV kasutab e-häälte miksimiseks tarkvara Verificatum, mis võtab sisendiks krüpteeritud hääled ning annab väljundiks miksitud krüpteeritud hääled ja miksimistõendi.

Miksimistõendi ja lugemistõendi kontroll toimub auditirakendusega, mis koosneb tööriistadest *convert*, *mixer* ja *decrypt*.

1. Tööriist *convert* kontrollib, teisenduste korrektsust IVXV andmevormingute ja Verificatumi andmevormingute vahel.
2. Tööriist *mixer* kontrollib miksimistõendi korrektsust.
3. Tööriist *decrypt* kontrollib lugemistõendi korrektsust.

E-häälte korrektse kokkulugemise kontrolliks on vajalik ja piisav kasutada kõiki kolme auditirakenduse tööriista.

Kõigi tööriistade kasutamine eeldab allkirjastatud usaldusjuure ja konkreetse tööriista seadistuste olemasolu. Alljärgnevalt kirjeldame konkreetsete tööriistade seadistusi.

6.1 E-häälte korrektse teisendamise kontroll

Verificatumi poolt koostatud miksimistõendi formaat on erinev IVXV raamistikus kasutatavast formaadist, samuti erinevad IVXV ning Verificatumi krüpteeritud häälte formaadid. IVXV raamistikku on pakendatud adapterid formaaditeisendusteks, auditirakendus pakub võimalust nende teisenduste korrektsuse kontrolliks.

Tööriist *convert* kontrollib, et Verificatumi poolt väljastatud miksimistõend vastab failidele IVXV raamistikus.

convert.input_bb IVXV miksimiseelse e-valimiskasti asukoht.

convert.output_bb IVXV miksimisjärgse e-valimiskasti asukoht.

convert.pub IVXV avaliku võtme asukoht.

convert.protinfo Verificatumi miksimise protokollifaili asukoht.

convert.proofdir Verificatumi miksimistõendi asukoht.

file *auditor.convert.yaml*:

```
convert:
  input_bb: TESTCONF-bb-4.json
  output_bb: TESTCONF-shuffled.json
  pub: TESTCONF-pub.pem
  protinfo: prot.xml
  proofdir: mixnet/
```

6.2 E-häälte miksimistõendi kontroll

Tööriist *mixer* kontrollib Verificatumi miksimistõendi korrektsust.

mixer.protinfo Verificatumi miksimistõendi protokollifaili asukoht.

mixer.proofdir Verificatumi miksimistõendi asukoht.

mixer.threaded Kasuta mitmelõimelist implementatsiooni. Vaikimisi väärtus on väär. Kasutatavate lõimede arv sõltub käsurea-argumentidest. Käsurea-argumentide puudumise korral valitakse optimaalne lõimede arv lähtudes tuvastatud tuumade arvust.

`auditor.mixer.yaml`:

```
mixer:
  protinfo: prot.xml
  proofdir: mixnet/
  threaded: true
```

6.3 E-häälte lugemistõendi kontroll

Tööriist *decrypt* kontrollib lugemistõendi korrektsust.

decrypt.input Lugemistõendi asukoht

decrypt.pub Dekrüpteerimiseks kasutatud salajasele võtmele vastava avaliku võtme asukoht.

decrypt.out Lugemistõendi kontrolli tulemuste asukoht. Tegemist on kataloogiga kuhu salvestatakse sedelid, mille lugemistõend oli kehtetu.

`auditor.decrypt.yaml`:

```
1 decrypt:
2   input: decout/TESTCONF-proof
3   pub: initout/TESTCONF-pub.pem
4   out: auditout
```

PEATÜKK 7

Kogumisteenus

7.1 Ülevaade

Kogumisteenuse juhtimine toimub signeeritud korralduste abil. Korraldused koostatakse operaatori poolt tekstiredaktori abil või imporditakse Valimiste Infosüsteemist. Korraldused signeeritakse ID-kaardiga.

Nimekiri kogumisteenuse haldamise korraldustest:

1. Usaldusjuure seadistus;
2. Tehniline seadistus;
3. Valimiste seadistus;
4. Valikute nimekiri;
5. Ringkondade nimekiri;
6. Valijate nimekiri;
7. Valijate nimekirja vahelejätmine;
8. Kasutajate volituste määramine.

Lisaks korraldustele tuleb kogumisteenusele genereerida ka komplekt krüptovõtmeid.

Korralduste vorming

Kogumisteenuse korralduste vorming on enamasti YAML või JSON, valijate nimekirja puhul kasutatakse spetsiifilist vormingut.

YAML-vormingus korraldused:

1. Usaldusjuure seadistus;
2. Tehniline seadistus;
3. Valimiste seadistus.

JSON-vormingus korraldused:

1. Valikute nimekiri;
2. Kasutajate volituste määramine.

Kohandatud vormingus korraldused:

1. Valijate nimekiri.

YAML-vormingus korraldused

YAML-vormingus seadistustesse on võimalik kaasata väliseid faile. Selleks kasutatakse silti `!container`.

Näide:

```
# välja "ext_file" väärtus loetakse failist "certificate-file.pem"
ext_file: !container certificate-file.pem
```

Ettevaatust: Väliste failide kaasamisel tuleb arvestada sellega, et seadistused laaditakse süsteemi BDOC-vormingus konteinerites (vt. lõiku *Korralduspaki vorming*). See seab väliste failide kaasamisele järgmised nõuded:

- Kasutatavad välised failid peavad olema pakendatud seadistusfailiga samasse konteinerisse;
- Välised failid peavad asuma seadistusfailiga samas kataloogis.

Korralduspaki vorming

Korralduspakk on BDOC-vormingus konteiner, milles on korraldusfail ja signatuurid. Üks korralduspakk tohib sisaldada ainult ühte korraldust. YAML-vormingus seadistuse (usaldusjuure seadistus, tehniline seadistus ja valimiste seadistus) korral võivad failis olla ka seadistusfaili poolt kasutatavad välised failid.

7.2 Kogumisteenuse usaldusjuure seadistamine

Kogumisteenuse usaldusjuur sisaldab andmeid seadistuste (kaasa arvatud usaldusjuure enda) allkirjade kontrollimiseks ja nimekirja süsteemi esmastest volitustest.

Usaldusjuure seadistuse koostab valimiste korraldaja. Seadistusfaili nimi peab alati lõppema stringiga `trust.yaml`. Failinime võimalik eesliide peab alati lõppema punktiga.

Tähelepanu: Usaldusjuure seadistuste laadimine lähtestab kogumisteenuse. Seetõttu pole juba seadistatud kogumisteenuse usaldusahela muutmine võimalik. Volituste muutmine on võimalik vastavate korralduste abil.

container Kohustuslik väli. Alamblokk, mis sisaldab seadistusfailide allkirjade kontrollimise seadistust.

container.bdoc Alamblokk, mis sisaldab seadistusfailide BDOC-allkirjade kontrollimise seadistust.

container.bdoc.bdocsize Kohustuslik väli. BDOC konteineri maksimaalne lubatud suurus baitides.

container.bdoc.filesize Kohustuslik väli. BDOC konteineris olevate failide maksimaalne lubatud hõrendatud suuru baitides.

container.bdoc.roots Kohustuslik väli. Seadistuste allkirjastajate sertifikaatide usaldusjuured.

container.bdoc.intermediates Seadistuste allkirjastajate sertifikaatide vahesertifikaadid. Usalduse saavutamiseks peab nende sertifikaatide abil olema võimalik luua ahel allkirjastaja sertifikaadist usaldusjuureni.

container.bdoc.profile Kohustuslik väli. Seadistuste allkirjadelt nõutav BDOC profiil. Toetatud valikud on `BES` (põhiprofiil kirjeldatud BDOC spetsifikatsiooni jaotises 5), `TM` (ajamärkidega profiil kirjeldatud BDOC spetsifikatsiooni jaotises 6.1) ja `TS` (ajatemplitega profiil kirjeldatud BDOC spetsifikatsiooni jaotises 6.2).

container.bdoc.ocsp.responders Kasutatakse ainult juhul kui `container.bdoc.profile` on `TM` või `TS`.

Kehtivuskinnitusi väljastanud OCSP responderi sertifikaadid. Kui nende hulgast responderi sertifikaati ei leita, siis otsitakse OCSP vastuses olevate sertifikaatide hulgast selline, mis on antud välja sama väljastaja poolt, mis seadistuste allkirjastaja sertifikaat, ning on lubatud OCSP vastuste signeerimiseks. AIA loogika kasutamise korral võib väli olla tühi.

container.bdoc.tsp.signers Kohustuslik väli. Kasutatakse ainult juhul kui `container.bdoc.profile` on `TS`.

Ajatempliteenuseteenuse vastuse allkirjastamise sertifikaadid.

container.bdoc.tsp.delaytime Kohustuslik väli. Kasutatakse ainult juhul kui `container.bdoc.profile` on `TS`.

Maksimaalne ajanihe ajatempli loomise ja allkirjastamise vahel sekundites.

container.bdoc.tsdelaytime Kasutatakse ainult juhul kui `container.bdoc.profile` on `TS`.
Maksimaalne ajanihe ajatempli ja kehtivuskinnituse loomise vahel sekundites. Välja puudumise või väärtuse 0 korral peavad mõlemad olema loodud samal sekundil.

authorizations Kohustuslik väli. Esmane nimekiri kogumisteenuse halduri volitustega isikutest (vt. *Rollid*), mis rakendatakse süsteemile usaldusjuure laadimisel. Iga isiku kohta on kirje tema ID-kaardi välja `Common Name` (CN) väärtusega. Minimaalselt peab sisaldama usaldusjuure signeerinud isiku andmeid.

Näide

`example.trust.yaml`:

```yaml
# Usaldusjuure seadistuse näide

container:
  bdoc:
    bdocsize: 104857600  # 100 MiB
    filesize: 104857600  # 100 MiB
    roots:
      - !container TEST_of_EE_Certification_Centre_Root_CA.pem
    intermediates:
      - !container TEST_of_ESTEID-SK_2011.pem
      - !container TEST_of_ESTEID-SK_2015.pem
    profile: TS
    ocsp:
      responders:
        - !container TEST_of_SK_OCSP_RESPONDER_2020.pem
    tsp:
      signers:
        - !container DEMO_SK_TIMESTAMPING_AUTHORITY_2020.pem
      delaytime: 1
    tsdelaytime: 60

authorizations:
    - ORAV,IVAN,30809010001
    - ROPKA,KIVIVALVUR,32608320001
```

7.3 Kogumisteenuse tehnilise seadistususe koostamine

Tehniline seadistus määrab kogumisteenuse tehnilised parameetrid. Sama tehnilist seadistust peaks olema võimalik kasutada erinevate valimiste seadistustega[1].

Tehnilise seadistuse koostab kogumisteenuse osutaja.

Seadistusfaili nimi peab alati lõppema stringiga `technical.yaml`. Failinime võimalik eesliide peab alati lõppema punktiga.

debug Tõeväärtus, kas logidesse kirjutatakse silumisteateid.

---

filter Kohustuslik väli. Alamblokk, mis sisaldab ühenduste filtrite seadistusi.

filter.tls Kohustuslik väli. Alamblokk, mis sisaldab ühenduste TLS-filtri seadistusi.

filter.tls.handshaketimeout Kohustuslik väli. Maksimaalne aeg sekundites TLS-kätluse läbiviimiseks.

filter.tls.ciphersuites Kohustuslik väli. TLS-protokolli versioonis 1.2 rakendamiseks lubatud šifrikomplektid. Hetkel toetatud valikud on:

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

Kui TLS-kätluse käigus lepitakse kokku TLS-protokolli versioonis 1.3, siis šifrikomplekti seadistada ei saa ning kõik serveri poolt toetatud turvalised šifrid on lubatud. Hetkel on nendeks:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

filter.codec Kohustuslik väli. Alamblokk, mis sisaldab ühenduste kodekfiltri seadistusi.

filter.codec.rwtimeout Kohustuslik väli. Maksimaalne aeg sekundites valijalt tervikliku päringu lugemiseks. Maksimaalne aeg sekundites valijale tervikliku päringu kirjutamiseks.

[1] Aga mitte samaaegselt: kogumisteenus toetab ainult ühte valimist.

filter.codec.requestsize Päringu maksimaalne suurus baitides. Välja puudumise või väärtuse 0 korral päringu suurust ei piirata.

filter.codec.logrequests Tõeväärtus, kas logidesse kirjutatakse kõik sissetulnud päringud algkujul. Päringu logi talletatakse tavalogist eraldi.

---

network Kohustuslik väli. Loetelu kogumisteenuse võrgusegmentidest. Kõik kogumisteenuse võrgusegmentide parameetrid määrab kogumisteenuse osutaja.

network.*.id Kohustuslik väli. Võrgusegmendi identifikaator.

network.*.services Kohustuslik väli. Alamblokk, mis sisaldab kogumisteenuse selle võrgusegmendi mikroteenuste seadistust.

network.*.services.proxy Loetelu, mis sisaldab vahendusteenuste isendite seadistust.

network.*.services.mid Loetelu, mis sisaldab Mobiil-ID toeteenuste isendite seadistust.

network.*.services.choices Loetelu, mis sisaldab nimekirjateenuste isendite seadistust.

network.*.services.voting Loetelu, mis sisaldab hääletamisteenuste isendite seadistust.

network.*.services.verification Loetelu, mis sisaldab kontrollteenuste isendite seadistust.

network.*.services.storage Loetelu, mis sisaldab talletusteenuste isendite seadistust.

network.*.services.log Loetelu, mis sisaldab logikogumisteenuste isendite seadistust.

network.*.services.backup Varundusteenuse isendi seadistus.

network.*.services.*.id Kohustuslik väli. Mikroteenuse isendi identifikaator.

network.*.services.*.address Kohustuslik väli. Mikroteenuse isendi võrguaadress ja -port.

network.*.services.*.peeraddress Mikroteenuse isenditevahelise suhtluse võrguaadress ja -port. Kasutatakse ainult juhul, kui sama teenust pakkuvad isendid peavad omavahel suhtlema (nt talletusteenus).

---

logging Alamblokk, mis sisaldab loetelu mikroteenuste kauglogimise serveritest. Siin blokis kirjeldatakse:

- Logiseire teenus. Alati loetelus esimene. Logiseirele saadetakse IVXV logi alates tasemest INFO;
- Vajadusel ka täiendavad välised logikogujad, kuhu saadetakse täielik logi alates tasemest DEBUG.

Logimine toimub üle RELP protokolli.

Kõik logiserverite parameetrid määrab kogumisteenuse osutaja.

logging.address Kohustuslik väli. Logiserveri aadress (IP-aadress või hostinimi).

logging.port Logiserveri port (täisarv, vaikimisi *20514*).

---

storage Kohustuslik väli. Alamblokk, mis sisaldab talletusprotokolli seadistust.
Kõik talletusprotokolli parameetrid määrab kogumisteenuse osutaja.

storage.protocol Kohustuslik väli. Kogumisteenuse talletusprotokoll. Hetkel toetatud ainult `etcd`.

storage.conf Kohustuslik väli. Talletusprotokolli seadistus. Sisu sõltub `storage.protocol` parameetri väärtusest.

storage.conf.ca Kohustuslik väli. Kasutatakse ainult juhul kui `storage.protocol` on `etcd`.
Talletusteenuste TLS sertifikaatide väljastaja sertifikaat.

storage.conf.conntimeout Kohustuslik väli. Kasutatakse ainult juhul kui `storage.protocol` on `etcd`.
Maksimaalne aeg sekundites etcd serveriga ühenduse loomiseks.

storage.conf.optimeout Kohustuslik väli. Kasutatakse ainult juhul kui `storage.protocol` on `etcd`.
Maksimaalne aeg sekundites ühe talletusoperatsiooni teostamiseks.

storage.conf.bootstrap Kohustuslik väli. Kasutatakse ainult juhul kui `storage.protocol` on `etcd`.
Loetelu nende talletusteenuste identifikaatoritest, mis on osa algsest etcd klastrist. Vajalik, et talletusteenuse isend teaks esmasel käivitumisel, kas see loob uut klastrit või liitub olemasolevaga.
Esmases tehnilises seadistuses peab loetelu kattuma `network` blokis loetletud talletusteenuste identifikaatoritega. Hiljem teenuseid lisades või eemaldades ei tohi `storage.conf.bootstrap` väärtust uuendada.

---

backup Varunduse parameetrid.
Loetelu varundmise kellaaegadest vormingus HH:MM.

`example.technical.yaml`:

```yaml
# Tehnilise seadistuse näide

debug: true

filter:
  tls:
    handshaketimeout: 20
    ciphersuites:
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      # Vanemate nutiseadmete tugi.
      - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
      - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  codec:
    rwtimeout: 10
    requestsize: 16384  # 16 KiB
    logrequests: true

network:
  - id: default
    services:
      proxy:
        - id:          proxy@proxy1.ivxv.ee
          address:     proxy1.ivxv.ee:443
      mid:
        - id:          mid@mid1.ivxv.ee
          address:     mid1.ivxv.ee:443
      choices:
        - id:          choices@choices1.ivxv.ee
          address:     choices1.ivxv.ee:443
      voting:
        - id:          voting@voting1.ivxv.ee
          address:     voting1.ivxv.ee:443
      verification:
        - id:          verification@verification1.ivxv.ee
          address:     verification1.ivxv.ee:443
      storage:
        - id:          storage@storage1.ivxv.ee
          address:     storage1.ivxv.ee:2379
          peeraddress: storage1.ivxv.ee:2380

logging:
  - address: logserver1.ivxv.ee
    port: 20514
  - address: logserver2.ivxv.ee
    port: 514

storage:
  protocol: etcd
  conf:
    ca: !container etcd_CA.pem
    conntimeout: 5
    optimeout: 10
    bootstrap:
      - storage@storage1.ivxv.ee

backup: ["03:00", "09:00", "15:00", "21:00"]
```

7.4 Kogumisteenusele valimise seadistuse koostamine

Valimise seadistus määrab ühe valimise seadistuse.

Valimise seadistuse koostab valimiste korraldaja. Seadistusfaili nimi peab alati lõppema stringiga `election.yaml`. Failinime võimalik eesliide peab alati lõppema punktiga.

identifier Kohustuslik väli. Valimise unikaalne identifikaator.

questions Loetelu, mis sisaldab ühe või enama valimise küsimuse unikaalset identifikaatorit. Unikaalsus peab olema tagatud ainult konkreetse valimise küsimuste hulgas. Kohustuslik väli.

---

period Kohustuslik väli. E-hääletuse perioodi andmete alamblokk.

period.servicestart Kohustuslik väli. Kogumisteenuses häälte vastuvõtmise algusaeg. Sellest hetkest alates hakkab kogumisteenus ühendusi teenindama. See aeg peab eelnema valimise algusajale ning on mõeldud enne valimise algust proovihääle andmiseks.

Enne `electionstart` parameetriga määratud aega vastu võetud häälte puhul tagastatakse valijarakendusele hääle esitamise lõpus vastav veateade (hääl jõudis kohale enne valimise algust). Sellised hääled tühistatakse automaatselt töötlemise käigus.

period.electionstart Kohustuslik väli. E-hääletuse algusaeg. Sellest hetkest alates antud hääled lähevad häälte lugemisel arvesse.

period.electionstop Kohustuslik väli. E-hääletuse lõpuaeg. Sellest hetkest lõpetatakse valikute nimekirjade väljastamine.

period.servicestop Kohustuslik väli. E-hääletuse lõppemisaeg. Sellest hetkest lõpetatakse häälte vastuvõtmine ning teenused lõpetavad töö.

---

voting Hääle esitamise parameetrite alamblokk.

voting.ratelimitstart Valija poolt esitatud häälte kogus, mille järel rakendub talle hääletamissageduse piirang. Arvesse lähevad ka vigased hääled, kuna muidu saaks nendega süsteemi koormata piirangust hoolimata. Välja puudumise või väärtuse 0 korral rakendub piirang alates esimesest häälest.

voting.ratelimitminutes Aeg minutites, mis peab jääma kahe hääle esitamise vahele, kui valijale on rakendatud hääletamissageduse piirang. Välja puudumise või väärtuse 0 korral on hääletamissageduse piirangud välja lülitatud.

---

verification Kohustuslik väli. Hääle kontrollimise parameetrite alamblokk.

verification.count Kohustuslik väli. Suurim ühe hääle lubatud kontrollimiste arv.

verification.minutes Kohustuslik väli. Hääle kontrollimise perioodi kestus minutites. Pärast hääle andmist on selle perioodi vältel võimalik häält kontrollida.

verification.latestonly Tõeväärtus, kas kontrollida saab ainult valija viimati antud häält. Kui väärtus on väär või puudu, siis saab kontrollida kõiki valija hääli (teiste piirangute raames).

---

voterforeignehak Alaliselt välisriigis elavate valijate ringkonnakuuluvuse tuvastamiseks kasutatav EHAK-kood.

Kui parameeter on määratud, siis alaliselt välisriigis elavad valijad kuuluvad ringkondadesse, kuhu kuulub ka parameetris määratud EHAK-koodile vastav haldusüksus. Täiendavalt peab ringkondade nimekiri sisaldama sellise EHAK-koodiga haldusüksust.

Kui parameeter on määramata, siis kasutatakse EHAK-koodi „0000“. Kui parameeter on määramata ning ringkondade nimekiri ei sisalda vaikekoodile vastavat haldusüksust, siis valijate nimekiri ei tohi sisaldada alaliselt välisriigis elavaid valijaid.

ignorevoterlist Ringkonna identifikaator, mille valikud esitada kõigile valijatele. Kui see väärtus ei ole tühi, siis kogumisteenus ei kasuta valijate nimekirja ning esitab kõigile valijatele väärtusega määratud ringkonna valikud ja lubab hääletada kõigil, kellel õnnestub isikutuvastus ning hääle allkirja kontrollimine.

---

voterlist Kohustuslik väli. Valijate nimekirjade kontrollimise parameetrid.

voterlist.key Kohustuslik väli. ECDSA-võtmepaari avalik võti valijate nimekirjade allkirja kontrollimiseks.

vis Alamblokk, mis sisaldab Valimiste Infosüsteemi seadistust.

vis.url Kohustuslik väli. Valimiste Infosüsteemi URL.

vis.ca Valimiste Infosüsteemi TLS-sertifikaadi usaldusahel.

---

auth Kohustuslik väli. Alamblokk, mis sisaldab valija tuvastamise seadistust.

auth.ticket Alamblokk, mis sisaldab piletipõhise valija tuvastamise seadistust.

Piletipõhist valija tuvastamist kasutatakse Mobiil-ID puhul, kus `mid` teenus tuvastab valija ning väljastab talle pileti, millega teistele teenustele ennast tuvastada.

See alamblokk on tühi, aga tema olemasolek või puudumine määrab, kas piletipõhine valija tuvastus on lubatud või ei.

auth.tls Alamblokk, mis sisaldab TLS-põhise valija tuvastamise seadistust.

TLS-põhist valijatuvastust kasutatakse ID-kaardi puhul.

auth.tls.roots Kohustuslik väli. Valija TLS-klientsertifikaatide usaldusjuured.

auth.tls.intermediates Valija TLS-klientsertifikaatide vahesertifikaadid. TLS-autentimiseks peab nende sertifikaatide abil olema võimalik luua ahel valija klientsertifikaadist usaldusjuureni.

auth.tls.ocsp Alamblokk, mis sisaldab valija TLS-klientsertifikaatide oleku kontrollimise seadistust. Selle bloki puudumisel valija sertifikaatide kehtivust ei kontrollita välisest kehtivuskinnitusteenusest.

auth.tls.ocsp.url Kohustuslik väli. Valija TLS-klientsertifikaatide kehtivuskinnitusteenuse aadress.

auth.tls.ocsp.responders Valija TLS-klientsertifikaatide kehtivuskinnitusteenuse responderi sertifikaadid. Kui nende hulgast responderi sertifikaati ei leita, siis otsitakse vastuses olevate sertifikaatide hulgast selline, mis on antud välja sama väljastaja poolt, mis kontrollitav sertifikaat, ning on lubatud OCSP vastuste signeerimiseks.

auth.tls.ocsp.retry Valija TLS-klientsertifikaatide oleku kontrolli korduvkatsete arv. Juhul kui sertifikaadi oleku kontroll ebaõnnestub võrguvõi serverivea tõttu, saab seda automaatselt korrata. Välja väärtus määrab katsete arvu, mis tehakse lisaks algsele päringule. Seega kui väärtus on 1, siis tehakse kokku maksimaalselt kaks päringut. Välja puudumise või väärtuse 0 korral automaatseid korduvkatseid ei sooritata.

---

identity Tuvastatud valija X.500 eraldusnimest unikaalse identifikaatori tuletamise meetod. Hetkel toetatud valikud `commonname`, `serialnumber` ja `pnoee`.

Eesti elektrooniliste isikut tõendavate dokumentide korral on `commonname` puhul identifikaator kujul „PERENIMI,EESNIMI,ISIKUKOOD“ ning teiste valikute teise puhul „ISIKUKOOD“.

Kui `serialnumber` tagastab eraldusnimest `serialNumber` välja muutmata kujul, siis `pnoee` eemaldab sellelt enne mittekohustusliku „PNOEE-“ eesliite. Viimane on vastavuses standardi ETSI EN 319 412-1 jaotisega 5.1.3 Eesti isikukoodide jaoks, kuid lubab ka standardile mittevastavaid seerianumbreid.

---

age Alamblokk, mis sisaldab valija vanuse kontrolli seadistust. Kui see blokk puudub, siis valija vanust ei kontrollita.

age.method Kohustuslik väli. Valija sünniaja tuvastamiseks kasutatav meetod. Hetkel toetatud ainult `estpic`, mis eeldab, et valija unikaalne identifikaator on Eesti isikukood ning eraldab sealt sünniaja.

age.timezone Kohustuslik väli. IANA ajavööndi nimi, milles valija vanus arvutatakse ehk millises ajavööndis peab valija olema valimisealine.

age.limit Kohustuslik väli. Valija peab olema vähemalt nii vana, et hääletada. Kui väärtus on 0, siis valija vanust ei kontrollita.

---

vote Kohustuslik väli. Alamblokk, mis sisaldab häälte allkirjade kontrollimise seadistust.

vote.bdoc Alamblokk, mis sisaldab häälte BDOC-allkirjade kontrollimise seadistust.

vote.bdoc.bdocsize Kohustuslik väli. BDOC konteineri maksimaalne lubatud suurus baitides.

vote.bdoc.filesize Kohustuslik väli. BDOC konteineris olevate failide maksimaalne lubatud hõrendatud suurus baitides.

vote.bdoc.roots Kohustuslik väli. Häälte allkirjastajate sertifikaatide usaldusjuured.

vote.bdoc.intermediates Häälte allkirjastajate sertifikaatide vahesertifikaadid. Hääle arvesseminekuks peab nende sertifikaatide abil olema võimalik luua ahel allkirjastaja sertifikaadist usaldusjuureni.

vote.bdoc.profile Kohustuslik väli. Häälte allkirjadelt nõutav BDOC profiil. Toetatud valikud on `BES` (põhiprofiil kirjeldatud BDOC spetsifikatsiooni jaotises 5), `TM` (ajamärkidega profiil kirjeldatud BDOC spetsifikatsiooni jaotises 6.1) ja `TS` (ajatemplitega profiil kirjeldatud BDOC spetsifikatsiooni jaotises 6.2).

See peaks olema `BES`, kuna kõikide allkirjastamisvahendite puhul ei ole sissetulev hääl kvalifitseeritud (nt Eesti ID-kaart). Kogumisteenus kvalifitseerib häältel olevad allkirjad ise (vt `qualification`).

---

mid Alamblokk, mis sisaldab Mobiil-ID teenusepakkuja seadistust.

mid.url Kohustuslik väli. Mobiil-ID teenusepakkuja asukoht.

mid.relyingpartyuuid Kohustuslik väli. Mobiil-ID teenusepakkujaga kokkulepitud kliendi identifikaator.

mid.relyingpartyname Kohustuslik väli. Mobiil-ID teenusepakkujaga kokkulepitud kliendi nimi.

mid.language Kohustuslik väli. Mobiil-ID kasutajale kuvatavate sõnumite keel. Võimalikud väärtused `EST`, `ENG`, `RUS` ja `LIT`.

mid.authmessage Kohustuslik väli. Sõnum, mida Mobiil-ID kasutajale kuvada autentimise käigus.

mid.signmessage Kohustuslik väli. Sõnum, mida Mobiil-ID kasutajale kuvada allkirjastamise käigus.

mid.messageformat Autentimise ning allkirjastamise käigus kasutajale kuvatava sõnumi vorming. Võimalikud väärtused `GSM-7` (Mobiil-ID poolt kasutatav vaikeväärtus) ja `UCS-2`.

mid.authchallengesize Autentimise käigus Mobiil-ID teenusele saadetava pretensiooni pikkus. Võimalikud väärtused `32` (vaikeväärtus), `48` ja `64`.

mid.statustimeoutms Parameeter, mis edastatakse autentimise ja allkirjastamise staatuse päringu korral Mobiil-ID teenusele ning millega saab kontrollida, kui kaua ootab Mobiil-ID teenus kasutaja poolse tegevuse lõpptulemust, enne kui vastab, et tegevus on pooleli. Väärtuse puudumisel oodatakse võimalikult vähe: täpne aeg sõltub Mobiil-ID teenusest.

Antud parameetri abil saab vähendada ühe autentimise või allkirjastamise käigus Mobiil-ID teenusele saadetavate päringute arvu.

mid.roots Kohustuslik väli. Mobiil-ID sertifikaatide usaldusjuured.

mid.intermediates Mobiil-ID sertifikaatide vahesertifikaadid. Mobiil-ID autentimiseks peab nende sertifikaatide abil olema võimalik luua ahel Mobiil-ID sertifikaadist usaldusjuureni.

mid.ocsp Alamblokk, mis sisaldab valija Mobiil-ID sertifikaatide oleku kontrollimise seadistust.

mid.ocsp.url Kohustuslik väli. Valija Mobiil-ID sertifikaatide kehtivuskinnitusteenuse aadress.

mid.ocsp.responders Mobiil-ID sertifikaatide OCSP responderi sertifikaadid. Kui nende hulgast responderi sertifikaati ei leita, siis otsitakse vastuses olevate sertifikaatide hulgast selline, mis on antud välja sama väljastaja poolt, mis kontrollitav sertifikaat, ning on lubatud OCSP vastuste signeerimiseks.

---

qualification Loetelu välistest kvalifitseerivatest päringutest, mis tehakse iga hääle kohta, koos seadistustega.

Siin on kasutatud loetelu protokoll ja seadistus blokkidest selle asemel, et anda igale protokollile oma blokk, kuna kvalifitseerivate päringute järjekord on oluline ning seadistatav.

qualification.*.protocol Kohustuslik väli. Kvalifitseeriva päringu protokoll. Hetkel toetatud `ocsp` (harilik OCSP), `ocsptm` (OCSP ajamärgendina), `tsp` (PKIX ajatempel) ja `tspreg` (PKIX ajatempel registreerimistõendina).

qualification.*.conf Kohustuslik väli. Kvalifitseeriva päringu protokolli seadistus. Sisu sõltub `qualification.*.protocol` parameetri väärtusest.

qualification.*.conf.url Kohustuslik väli. Aadress, kuhu kvalifitseeriv päring tehakse.

qualification.*.conf.responders Kasutatakse ainult juhul kui `qualification.*.protocol` on `ocsp` või `ocsptm`.

OCSP reponderi sertifikaadid. Kui nende hulgast responderi sertifikaati ei leita, siis otsitakse vastuses olevate sertifikaatide hulgast selline, mis on antud välja sama väljastaja poolt, mis kontrollitav sertifikaat, ning on lubatud OCSP vastuste signeerimiseks. AIA loogika kasutamise korral võib väli jääda tühjaks.

qualification.*.conf.signers Kohustuslik väli. Kasutatakse ainult juhul kui `qualification.*.protocol` on `tsp` või `tspreg`. Ajatempliteenuseteenuse vastuse allkirjastamise sertifikaadid.

qualification.*.conf.delaytime Kohustuslik väli. Kasutatakse ainult juhul kui `qualification.*.protocol` on `tsp` või `tspreg`. Maksimaalne ajanihe ajatempli loomise ja allkirjastamise vahel sekundites.

qualification.*.conf.retry Kvalifitseeriva päringu korduvkatsete arv. Juhul kui päring ebaõnnestub võrgu- või serverivea tõttu, saab seda automaatselt korrata. Välja väärtus määrab katsete arvu, mis tehakse lisaks algsele päringule. Seega kui väärtus on 1, siis tehakse kokku maksimaalselt kaks päringut. Välja puudumise või väärtuse 0 korral automaatseid korduvkatseid ei sooritata.

Näide

`example.election.yaml`:

```yaml
# Valimiste seadistuse näide

identifier: TESTCONF
questions:
  - TESTQUESTION

period:
  servicestart:  2017-01-16T08:50:00+02:00
  electionstart: 2017-01-16T09:00:00+02:00
  electionstop:  2017-01-18T19:00:00+02:00
  servicestop:   2017-01-18T19:15:00+02:00

voting:
  ratelimitstart:   50
  ratelimitminutes:  5

verification:
  count:       3
  minutes:    30
  latestonly: false

voterlist:
  key: !container rr_pub.key

vis:
  url: https://vis-mock.local/vis3/
  ca:
    - |
      -----BEGIN CERTIFICATE-----

↪MIIDmzCCAoOgAwIBAgIDOBFTMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNVBAYTAkVF...
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      MRIwEAYDVQQKDAlTQ0NFSVYgT1kxHzAdBgNVBAsMFklWWFYgVGVzdCBDZXJ0aWZp
      Y2F0ZXMxEzARBgNVBAMMClNlcnZpY2UgQ0EwIBcNMjEwNjE3MTIwNTI0WhgPMjEy
      MTA1MjQxMjA1MjRaMFsxCzAJBgNVBAYTAkVFMRIwEAYDVQQKDAlTQ0NFSVYgT1kx
      HzAdBgNVBAsMFklWWFYgVGVzdCBDZXJ0aWZpY2F0ZXMxFzAVBgNVBAMMDnZpcy1t
      b2NrLmxvY2FsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzZW7yXGO
      SEt4qavm/vNJj9otKf9j8runLJcmoTGR61A5As2gluRnj3z6/U8An/
      VsX1dUG2qL
      sJecEXUkvXBSTw2IIyfA6lJNtaov44ytRB4fKpuFx+lb00WmuRf99uC0Tpp5K0Of
      7D5NO5dgtMXLrdpzuyJD6NP2xrp8Dio5a1TosHcQEVWJvR/
      dwCr02TmcQjvILOVN
      vJFr038Dg77NQKojOsag60KRrHcKc1WukgUPu4AJ2VFCmn67rCfp39tusbcndsNs
      EX7zGNghOk85CMoGWlYfnJm94oAoKUsYtpF1hinfBN/EikXZwJbsVFoSg4mo/
      te2
      MfwzK7E5j17JWwIDAQABo2owaDAdBgNVHQ4EFgQUI2yfomatZq3HLyL+DpqeBYO9
      /1EwHwYDVR0jBBgwFoAUbyNWl77jkIGrjVtW7Eu4+qpDXxYwDgYDVR0PAQH/
      BAQD
      AgOoMBYGA1UdJQEB/
      wQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQCA
      RsgmPcL4NaHxQGRxPS2agw2ihLPgkmZcUJhJ0ObnmVYBjCCpYxaNd0vCWBYejChj
      Q2cblFAuKUtc+pwSC2WDPV9rRwLNOQn/
      PR2dzeNRP7L0UmNyPcH5pwmltAJLFQqW
      OdnlXL8ehXSLeIdzlBkqNYZCrj4Ulv4W8cLosjCrmwTZ8OW2E/
      GSTY7YljsPZZt0
      uI5Sxz8VtlMJsVh0HWCQ4oAawp6BOgUAGdE9PIo2UlDHyUHBSDXDuZKTGut+yv1T
      NOq+xK3YM/CRFf/ujIuc1zx+dzkM9l72VJT2BQ6+LKeS5qzduJTG/
      8dJJFzgNB9p
      vo7reW+FURRS+CQI633D
      -----END CERTIFICATE-----

auth:
  ticket:
  tls:
    roots:
      - !container TEST_of_EE_Certification_Centre_Root_CA.pem
    intermediates:
      - !container TEST_of_ESTEID-SK_2011.pem
      - !container TEST_of_ESTEID-SK_2015.pem
    ocsp:
      url: http://demo.sk.ee/ocsp
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      responders:
        - !container TEST_of_SK_OCSP_RESPONDER_2020.pem
      retry: 2

identity: pnoee

age:
  method:   estpic
  timezone: Europe/Tallinn
  limit:    18

vote:
  bdoc:
    bdocsize: 32768  # 32 KiB
    filesize: 32768  # 32 KiB
    roots:
      - !container TEST_of_EE_Certification_Centre_Root_CA.pem
    intermediates:
      - !container TEST_of_ESTEID-SK_2011.pem
      - !container TEST_of_ESTEID-SK_2015.pem
    profile: BES

mid:
  url: https://tsp.demo.sk.ee/mid-api/
  relyingpartyuuid: 00000000-0000-0000-0000-000000000000
  relyingpartyname: DEMO
  language:    EST
  authmessage: Mobiil-ID autentimise testimine.
  signmessage: Mobiil-ID allkirjastamise testimine.
  messageformat: GSM-7
  authchallengesize: 64
  statustimeoutms: 5000
  roots:
    - !container TEST_of_EE_Certification_Centre_Root_CA.pem
  intermediates:
    - !container TEST_of_ESTEID-SK_2011.pem
    - !container TEST_of_ESTEID-SK_2015.pem
  ocsp:
    url: http://demo.sk.ee/ocsp
    responders:
      - !container TEST_of_SK_OCSP_RESPONDER_2020.pem

qualification:
  - protocol: tspreg
    conf:
      url: http://demo.sk.ee/tsa
      signers:
        - !container DEMO_SK_TIMESTAMPING_AUTHORITY_2020.pem
      delaytime: 1
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      retry: 2
  - protocol: ocsp
    conf:
      url: http://demo.sk.ee/ocsp
      responders:
        - !container TEST_of_SK_OCSP_RESPONDER_2020.pem
      retry: 2
```

7.5 Valijate nimekirja vahelejätmine

Valijate nimekirja vahelejätmine tähendab haldusteenuses registreerinud vigase valijate nimekirja asendamist tühja nimekirjaga.

Protseduur on vajalik olukorras, kus haldusteenus on Valimiste Infosüsteemist alla laadinud ja haldusteenuses registreerinud valijate muudatusnimekirja, mida pole võimalik kogumisteenusele rakendada (nimekiri on vigane või pole kooskõlas teiste kogumisteenuste seadistustega).

Valijate nimekirja vahelejätmine korralduse koostab valimiste korraldaja.

Seadistusfaili nimi peab alati lõppema stringiga `.skip.yaml`.

election Kohustuslik väli. Valimise unikaalne identifikaator.

skip_voter_list Kohustuslik väli. Vahele jäetava valijate muudatusnimekirja versioon.

changeset Kohustuslik väli. Vahele jäetava valijate muudatusnimekirja järjekorranumber.

Näide

`example.voters.skip.yaml`:

```
# Valijate muudatusnimekirja nr. 15 vahelejätmise korralduse näide

election: TESTCONF
skip_voter_list: "https://vis-ehs-api.ria.ee/ehs-election-voters-
↪changeset 2021-07-22T10:12:49Z"
changeset: 15
```

7.6 Kogumisteenuse volituste kirjeldamine

Kasutajatele volituste määramine käib süsteemis kirjeldatud rollide kaudu. Igale rollile on määratud komplekt õigusi ja kasutajal on kõik volitused, mis talle seotud rollide kaudu on määratud.

Volituste määramise korraldus määrab ühele kasutajale tema rollid süsteemis.

Volitused koostatakse JSON-vormingus failina, millega määratakse:

1. Korralduse sisu (`action=user-permissions`);
2. Volitatud kasutaja *Common Name* väli tema ID-kaardilt (väli `cn`);
3. Kasutaja rollide nimekiri komadega eraldatud nimekirjana (väli `roles`).

Faili vorming:

```
{
    "action": "user-permissions",
    "cn": "<kasutaja-CN">,
    "roles": "roll1[,roll2]"
}
```

Rollid

Kogumisteenuses on järgnevad rollid:

1. **Kogumisteenuse haldur** (`admin`) on ette nähtud kogumisteenuse tehniliseks haldamiseks;
2. **Valimiste haldur** (`election-conf-manager`) on ette nähtud valimiste seadistuste kehtestamiseks;
3. **Vaataja** (`viewer`) on ette nähtud haldusteenuse kaudu väljastatavate andmete vaatamiseks;
4. **Õigusteta kasutaja** (`none`). See roll on ette nähtud kasutajakonto kirje hoidmiseks olukorras, kus kasutajale pole ühtegi teist rolli määratud (näiteks pärast lisamist või pärast kõigist teistest rollidest eemaldamist).

Tabel 7.2: Rollide ja volituste maatriks

	admin	election-conf-manager	viewer	none
Üldseisundi ja statistika vaatamine	✓	✓	✓	-
Valimiste seadistuste rakendamine	✓	✓	-	-
E-valimiskasti allalaadimine	✓	✓	-	-
Kasutajate haldus	✓	-	-	-
Tehnilise seadistuse rakendamine	✓	-	-	-
Logide vaatamine	✓	-	-	-

Volituste reeglid

- Kasutaja võib olla mitmes rollis korraga;
- Roll annab kasutajale rolliga seotud õigused, ükski roll õigusi ära ei võta.

7.7 Kogumisteenuse krüptovõtmed

Kogumisteenuse andmevahetuse turvamiseks on tarvis luua komplekt krüptograafilisi võtmeid. Komplekti koosseis sõltub kogumisteenuse tehnilistest seadistustest.

1. Teenuse krüptovõti ja TLS-sertifikaat - kasutatakse teenuste omavahelise suhtluse turvamiseks kõigi teenuste puhul peale vahendusteenuse;
2. Hääletamisteenuse ajatemplipäringute signeerimisvõti - kasutatakse ajatemplipäringute signeerimiseks juhul, kui ajatempliteenus on registreerimisteenuseks;
3. Mobiil-ID tugiteenuse jagatud krüptimissaladus – kasutatakse sümmeetrilise AES-256 krüptimise jaoks. Krüptimissaladusega krüptib Mobiil-ID tugiteenus hääletajale väljastatava identsustõendi, mille abil hääletaja enda identiteeti teistele teenustele tõendab.

Teenuse krüptovõtme ja TLS-sertifikaadi genereerimine

Teenuse krüptovõti ja TLS-sertifikaat genereeritakse kõigile teenustele peale vahendusteenuse. Kõikide teenuste sertifikaadid peavad olema välja antud sama sertifitseerimiskeskuse (CA – *Certificate Authority*) poolt.

CA sertifikaadi genereerimine

Sertifitseerimiskeskuse krüptovõtme ja sertifikaadi genereerimine toimub järgneva käsuga:

```
$ openssl req -newkey ec -pkeyopt ec_paramgen_curve:P-256 -x509 -
↪nodes
  -days 365 -out ca.pem -keyout ca.key -utf8
  -subj "/C=EE/O=Example/OU=IVXV Test Certificates/CN=Service CA"
```

Käsu väljundiks on failid `ca.key` (võti) ja `ca.pem` (sertifikaat).

Teenuse isendi krüptovõtme ja TLS-sertifikaadi genereerimine

Teenuse isendi krüptovõtme ja sertifikaadipäringu genereerimine toimub järgneva käsuga:

```
$ openssl req -newkey ec -pkeyopt ec_paramgen_curve:P-256 -nodes
  -out <teenuse-id>-tls.csr -keyout <teenuse-id>-tls.key -utf8
  -subj "/C=EE/O=Example/OU=IVXV Test Certificates/CN=<teenuse-id>"
```

Käsu väljundiks on failid `<teenuse-id>-tls.key` (võti) ja `<teenuse-id>-tls.csr` (sertifikaadipäring).

Tähelepanu: Talletusteenuse puhul peab sertifikaadipäringus olema CN väärtuseks teenuse identifikaatori asemel hostinimi: erinevalt teistest teenustest ei kasutata talletusteenuse puhul alternatiivset TLS nime.

Teenuse isendi TLS-sertifikaadi genereerimine toimub järgneva käsuga:

```
$ openssl x509 -req -days 365 -CA ca.pem -CAkey ca.key -set_serial 1
  -extfile service-cert-openssl.cnf -extensions ext_<teenuse-tüüp>
  -in <teenuse-id>-tls.csr -out <teenuse-id>-tls.pem
```

Käsu väljundiks on fail `<teenuse-id>-tls.pem`.

Sertifikaadi genereerimiseks peab failisüsteemis olema seadistusfail `service-cert-openssl.cnf`.

Nimekiri 7.1: Fail service-cert-openssl.cnf

```
# IVXV Internet voting framework
#
# OpenSSL config file for service certificates

[ req ]
utf8                = yes
string_mask         = utf8only
distinguished_name = req_dn

[ req_dn ]
# Empty section needed by req. The actual DN will be supplied on␣
↪command line.

[ ext_admin_client ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, clientAuth
# no subjectAltName
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
[ ext_admin_ui ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth
# no subjectAltName

[ ext_choices ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: choices.ivxv.invalid

[ ext_mid ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth  # No clientAuth.
subjectAltName          = DNS: mid.ivxv.invalid

[ ext_storage ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth, clientAuth
# No subjectAltName.

[ ext_vis-mock.local ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth
subjectAltName          = DNS: vis-mock.local

[ ext_voting ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: voting.ivxv.invalid

[ ext_verification ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: verification.ivxv.invalid
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
[ ext_wildcard ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: *.ivxv.invalid
```

Hääletamisteenuse ajatemplipäringute signeerimisvõtme ja sertifikaadi genereerimine

Hääletamisteenuse registreerimispäringute tegemise võti genereeritakse järgneva käsuga:

```
$ openssl genrsa -out tspreg.key 2048
```

Käsu väljundiks on fail `tspreg.key`.

Hääletamisteenuse registreerimispäringute tegemise võtme sertifikaat genereeritakse järgneva käsuga:

```
$ openssl req -x509 -nodes -days 365 -out tspreg.pem -key tspreg.
↪key -utf8
  -subj "/C=EE/O=Example/OU=IVXV Test Certificates/CN=Collector␣
↪Registration"
```

Käsu väljundiks on fail `tspreg.pem`.

Märkus: Hääletamisteenuse ajatemplipäringute signeerimisvõti on vaja genereerida vaid juhul, kui ajatempliteenust kasutatakse registreerimisteenuseks.

Mobiil-ID tugiteenusele jagatud krüptimissaladuse genereerimine

Jagatud krüptimissaladus genereeritakse järgneva käsuga:

```
$ openssl rand -out mobid-shared-secret.key 32
```

Käsu väljundiks on 32 baidi suurune fail `mobid-shared-secret.key`, mida mobiil-ID teenus hakkab kasutama sümmeetrilise AES-256 krüptimise jaoks.

Märkus: Mobiil-ID tugiteenuse jagatud krüptimissaladus on vaja genereerida vaid juhul, kui Mobiil-ID tugiteenus on kasutusel.

PEATÜKK 8

Valijarakenduse seadistamine

Valijarakenduse seadistamist ning pakendamist käsitleb eraldi dokument.

PEATÜKK 9

Kontrollrakenduse seadistamine

Kontrollrakenduste seadistus on JSON formaadis.

1. Android-seadmed otsivad seadistust aadressilt „https://www.valimised.ee/kontrollrakendus/config.json“.
2. iOS-seadmed otsivad seadistust aadressilt „https://www.valimised.ee/kontrollrakendus/config.json“

Reaalne sisu võib kahel seadistusel olla samasugune ka siis kui võimalike erinevuste tekkimise jaoks kasutatakse ennetavalt erinevaid URLe. Varasemalt on erinevate URLide kasutamist õigustanud nt. iOS rakenduste pikem tarnetsükkel, mis nõuab testseadistuste avalikustamist.

Seadistus koosneb viiest peamisest rühmast

- `versions` - Rakenduse nõutud versioon
- `texts` - Kasutajaliideses kasutatavad tekstid
- `errors` - Kasutajaliideses kasutatavad veateated
- `colors` - Kasutajaliidese värvide koodid
- `params` - Rakenduse tööks vajalikud parameetrid
- `elections` - Igale küsimuse identifikaatorile vastav tekst kasutajaliideses

Kõiki seadistatavaid väärtusi näeb näidisseadistusest. Kõik väärtused on kohustuslikud.

9.1 Versioonide seadistamine

Kontrollrakenduse versioon peab olema suurem või võrdne seadistuses määratud versiooniga. Versioonid kuuluvad rühma `versions`:

- `android_version_code` - Android-rakenduse minimaalne versioonikood. Väärtus peab olema positiivne JSON täisarv.
- `ios_bundle_version` - iOS-rakenduse minimaalne versioonisõne. Väärtus peab olema JSON sõne, mis koosneb punktidega eraldatud positiivsetest täisarvudest.

9.2 Parameetrite seadistamine

Rakenduse tööks vajalikud parameetrid kuuluvad rühma `params`:

- `verification_url` - Nimekiri kogumisteenuse hostinimedest või IP-aadressidest koos pordiga. Järjekord pole oluline. Väärtus peab olema JSON loend ka ühe URL-i puhul.
- `verification_tls` - Nimekiri kogumisteenuse TLS sertifikaatidest PEM vormingus. Järjekord pole oluline. Väärtus peab olema JSON loend ka ühe sertifikaadi puhul.
- `help_url` - Abiinfo vaate URL
- `close_timeout` - Ajaaken, mil on kasutajal võimalik oma valikut näha enne rakenduse sulgumist. Millisekundites.
- `close_interval` - Intervall, millega uuendatakse `close_timeout` väärtust kasutajaliideses. Millisekundites.
- `con_timeout_1` - Kogumisteenusega ühenduse saamise esimese katse ajapiirang. Millisekundites.
- `con_timeout_2` - Kui esimese ringiga ei saadud ühendust ühegi kogumisteenuse instantsiga, proovitakse uuesti selle ajapiiranguga. Millisekundites.
- `public_key` - Valimiste avalik võti, millega krüpteeritakse valijate hääli. PEM vormingus.
- `tspreg_service_cert` - Ajatembeldusteenuse sertifikaat PEM vormingus.
- `ocsp_service_cert` - OCSP-teenuse sertifikaadid PEM vormingus. Järjekord pole oluline. Väärtus peab olema JSON loend ka ühe väärtuse puhul. Kui väli on tühi, siis tuvastatakse OCSP responderi sertifikaat automaatselt.
- `tspreg_client_cert` - Kogumisteenuse sertifikaat registreerimispäringute tegemiseks PEM vormingus.

9.3 Tekstide seadistamine

Kasutajaliideses kasutatavad tekstid kuuluvad rühma `texts`. Järgmised tekstid on parametriseeritavad:

- `lbl_close_timeout` - Kontrollrakenduse sulgemisteade koos loenduriga. Tekst peab sisaldama märgendit XX, mis asendatakse automaatselt rakenduse sulgemiseni jäänud ajaga sekundites.

9.4 Näide

```
{
  "appConfig": {
    "versions": {
      "android_version_code": 28,
      "ios_bundle_version": "2.1.1"
    },
    "texts": {
      "loading": "Laen...",
      "welcome_message": "Hääle kontollimiseks suunake nutiseadme␣
↪kaamera arvuti ekraanil kuvatavale QR-koodile",
      "lbl_vote": "Hääle kontrollimine",
      "lbl_vote_txt": "Teie QR-koodile vastav hääl on talletatud␣
↪valimiste serveris",
      "lbl_vote_signer": "Hääle allkirjastaja: ",
      "btn_next": "Edasi",
      "btn_more": "AbiInfo",
      "btn_packet_data": "Andmeside",
      "btn_wifi": "Wifi",
      "btn_verify": "Kuva minu valik",
      "lbl_no_choice": "Valikut ei tehtud",
      "lbl_choice": "Tuvastatud valik",
      "lbl_close_timeout": "Rakendus suletakse XX sekundi pärast!",
      "notification_title": "Valimisteenistus",
      "notification_message": "Kontrollimine lõpetatud"
    },
    "errors": {
      "no_network_message": "Veenduge, et nutiseadme andmeside on␣
↪võimaldatud",
      "get_config_message": "Valimiste seadistuse laadimine␣
↪ebaõnnestus",
      "bad_config_message": "Valimiste seadistuse viga",
      "bad_version_message": "Rakendus on aegunud",
      "problem_qrcode_message": "QR koodi ei õnnestunud tuvastada",
      "close_qrcode_message": "QR koodi ei õnnestunud tuvastada",
      "send_server_request_message": "Valimiste süsteemiga␣
↪ühendamine ebaõnnestus",
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      "bad_server_response_message": "Tehniline viga, palun␣
↪teavitage valimiste läbiviijat",
      "bad_device_message": "Selle seadmega pole võimalik häält␣
↪kontrollida",
      "bad_verification_message": "Valiku tuvastamine␣
↪krüptogrammist ebaõnnestus",
      "camera_permission_required_message": "Rakenduse kasutamiseks␣
↪peab olema kaamera kasutamine lubatud"
    },
    "colors": {
      "frame_background": "#AA444444",
      "main_window_foreground": "#FFFFFF",
      "error_window_foreground": "#FFFFFF",
      "loading_window_background": "#33B5E5",
      "loading_window_foreground": "#FFFFFF",
      "main_window": "#33B5E5",
      "main_window_shadow": "#005777",
      "error_window": "#FF0000",
      "error_window_shadow": "#770000",
      "btn_background": "#F0F0F0",
      "btn_foreground": "#727272",
      "btn_verify_foreground": "#FFFFFF",
      "btn_verify_background_start": "#30B4E5",
      "btn_verify_background_center": "#1AABE1",
      "btn_verify_background_end": "#00A1DC",
      "lbl_background": "#33B5E5",
      "lbl_foreground": "#FFFFFF",
      "lbl_shadow": "#008EC2",
      "lbl_outer_container_background": "#EAEAEA",
      "lbl_outer_container_foreground": "#878686",
      "lbl_inner_container_background": "#FFFFFF",
      "lbl_inner_container_foreground": "#878686",
      "lbl_close_timeout_foreground": "#454444",
      "lbl_close_timeout_background_start": "#FEEC00",
      "lbl_close_timeout_background_center": "#F9D303",
      "lbl_close_timeout_background_end": "#F7C804",
      "lbl_close_timeout_shadow": "#C6A002",
      "lbl_outer_inner_container_divider": "#E9E9E9"
    },
    "params": {
      "verification_url": ["collector1:port", "collector2:port",
↪"collector3:port"],
      "verification_tls": ["<collector1_tls_pem>", "<collector2_tls_
↪pem>", "<collector3_tls_pem>"],
      "help_url": "https://eh.valimised.ee/apps/help/index.html",
      "close_timeout": 30000,
      "close_interval": 1000,
      "con_timeout_1": 3000,
      "con_timeout_2": 15000,
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
      "public_key": "<valimiste_avalik_võti_pem>",
      "tspreg_service_cert": "<SK_TIMESTAMPING_AUTHORITY_CERT>",
      "ocsp_service_cert": [],
      "tspreg_client_cert": "<collector_tspreg_cert_pem>"
    },
    "elections": {
      "question-1": "Milline on looduskauneim koht?"
    }
  }
}
```

PEATÜKK 10

E-häälte miksimine

10.1 Miksneti Verificatum paigaldamine

Eeldused

Juhend on kasutamiseks distributsiooniga Ubuntu 20.04 LTS (Bionic Beaver) ja see eeldab, et käske käivitatakse lihtkasutaja õigustest, kellel on õigus privileegide eskaleerimiseks *sudo* käsu abil. Lisaks on eeldatud järgmiste failide olemasolu kasutaja kodukaustas:

Github repositooriumist (https://github.com/vvk-ehk/intcheck):

- `intcheck.py` - tööriist kataloogide täielikkuse kontrolliks

IVXV tarnefailist:

- `gmpmee.dirsha256sum` - gmpmee kataloogi räsi;
- `vmgj.dirsha256sum` - vmgj kataloogi räsi;
- `vcr.dirsha256sum` - vcr kataloogi räsi;
- `vmn.dirsha256sum` - vmn kataloogi räsi;
- `ivxv-verificatum-1.7.6~dev-runner.zip` - IVXV adapter Verificatumi kasutamiseks.

Valimise korraldaja käest:

- `data/bb-4.json` - anonümiseeritud e-valimiskast;
- `data/pub.pem` - häälte krüpteerimiseks kasutatud võti.

Kataloogis `data/` ei tohi olla ühtegi teist faili.

Pärast protsessi lõppu on kataloogis `data/` vajalikud järgnevad failid:

- `shuffled.json` - miksitud e-valimiskast;
- `proof.zip` - korrektse miksimise tõend.

Verificatumi ehitamine

Ehitamiseks vajalike pakkide paigaldamine:

```
sudo apt-get install --no-install-recommends -y autoconf autoconf␣
↪automake \
build-essential libgmp-dev libtool git openjdk-11-jdk-headless \
python unzip wget
```

Verificatumi lähtekoodi allalaadimine:

```
git clone https://github.com/verificatum/verificatum-gmpmee gmpmee
git clone https://github.com/verificatum/vmgj
git clone https://github.com/verificatum/vcr
git clone https://github.com/verificatum/vmn
```

Lähtekoodist puhaste arhiivide loomine täielikkuse kontrolliks:

```
cd gmpmee
git checkout 4aafc31
rm -rf .git/
cd ../vmgj
git checkout 8d7d412
rm -rf .git/
cd ../vcr
git checkout af9fd82
rm -rf .git/
cd ../vmn
git checkout bb00543
rm -rf .git/
cd ..
```

Verificatumi lähtekoodi täielikkuse kontrollimine:

```
chmod +x ./intcheck.py
./intcheck.py verify gmpmee gmpmee.dirsha256sum
./intcheck.py verify vmgj vmgj.dirsha256sum
./intcheck.py verify vcr vcr.dirsha256sum
./intcheck.py verify vmn vmn.dirsha256sum
```

gmpmee ehitamine:

```
cd gmpmee/
make -f Makefile.build
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
./configure
make
sudo make install
```

vmgj ehitamine:

```
cd ../vmgj/
make -f Makefile.build
./configure
make
sudo make install
```

vcr ehitamine:

```
cd ../vcr/
make -f Makefile.build
./configure --enable-vmgj
make
sudo make install
```

vmn ehitamine:

```
cd ../vmn/
make -f Makefile.build
./configure
make
sudo make install
```

IVXV Verificatumi adapteri ja käivitusskripti lahtipakkimine:

```
cd ..
unzip ivxv-verificatum-1.7.6~dev-runner.zip
```

Verificatumi teekide kopeerimine adapteri väliste teekide kataloogi:

```
cp /usr/local/share/java/verificatum-vmgj-1.2.2.jar mixer/lib/
↪verificatum-vmgj.jar
cp /usr/local/share/java/verificatum-vcr-vmgj-3.0.4.jar mixer/lib/
↪verificatum-vcr-vmgj.jar
cp /usr/local/share/java/verificatum-vmn-3.0.4.jar mixer/lib/
↪verificatum-vmn.jar
cp /usr/local/lib/libgmpmee.so.0.0.0 mixer/lib/libgmpmee.so.0
cp /usr/local/lib/libvmgj-1.2.2.so mixer/lib/libvmgj-1.2.2.so
```

10.2 E-häälte miksimine

Verificatumi miksneti käivitamine:

```
cd data
../mixer/bin/mix.py --pubkey pub.pem --ballotbox bb-4.json \
--shuffled shuffled.json --proof-zipfile proof.zip shuffle
```

10.3 Miksimistõendi verifitseerimine

Verificatumi adapteri abil saab miksimistõendit ka verifitseerida:

```
cd ..
mkdir verify
cp data/proof.zip verify
cd verify
../mixer/bin/mix.py verify --proof-zipfile proof.zip
```

Kirjandus

[BDPA10] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche: Sponge-Based Pseudo-Random Number Generators. CHES 2010: 33-47

[RFC3526] T. Kivinen, M. Kojo: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). IETF RFC3526, 2003