IVXV seadistuste koostamise juhend

Juhend

Versioon 1.0

20. september 2017

42 lk

Dok IVXV-JSK-1.0

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 selliselt, et on võimalik valijatelt häälte vastu võtmine ning nende käitlemine süsteemile seatud terviklus-, konfidentsiaalsus ja käideldavusnõuete raamides. Tehniline dokument annab ülevaate olulisimatest seadistustoimingutest ning on mõeldud täiendama elektroonilise hääletamise käsiraamatu poolt kirjeldatud protseduurireeglite täitmist.

2.1 Hääletamisperioodi algusele eelnevad andmed ja tegevused

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 ja kogumisteenuse usaldusjuur Rakenduste ja kogumisteenuse usaldusjuur defineerib sertifitseerimishierarhia(d), mille alusel IVXV süsteemi komponendid verifitseerivad digitaalallkirju. Eesti riiklike valimiste korral määrab usaldusjuure koosseisu Riigi Valimisteenistus. Usaldusjuure vormingut ning seotud protokolle käsitletakse peatükis *Usaldusjuur*.

Kogumisteenuse tehniline seadistus Kogumisteenuse tehniline seadistus kirjeldab IVXV mikroteenuste seadistuse ning jagunemise erinevate üksuste vahel. Eesti riiklike valimiste korral leiab kogumisteenuse osutaja Riigi Valimisteenistus. Tehniline seadistus kooskõlastatakse valimiste omaniku ja kogumisteenuse osutaja vahel. Tehnilist seadistust käsitletakse peatükis *Kogumisteenuse tehniline seadistus*.

Kogumisteenuse võtmed ja sertifikaadid Kogumisteenuse mikroteenused suhtlevad omavahel TLS protokolli vahendusel. Vastavad sertifikaadid tuleb eksportida Valijarakendusse ja Kontrollrakendusse.

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 genereerimine (VALIKULINE)*.

Enne hääletamisperioodi algust teostatakse lähtuvalt eelnevatest andmetest järgmised tegevused:

1. *Rakenduste usaldusjuure kirjeldamine*
2. *Häälte salastamise võtme spetsifikatsiooni genereerimine (VALIKULINE)*
3. *Häälte salastamise võtme genereerimine*
4. *Häälte salastamise võtme testimine*
5. Kogumisteenuse seadistamine
6. Valijarakenduse seadistamine
7. Kontrollrakenduse seadistamine

2.2 Hääletamisperioodi aegsed tegevused

Valijate nimekirjade uuendused

2.3 Hääletamisperioodi lõpule järgnevad tegevused

1. *E-urni töötlemine - verifitseerimine*
2. *E-urni töötlemine - korduvhäälte tühistamine*
3. *E-urni töötlemine - häälte tühistamine ja ennistamine jaoskonnainfo põhjal*
4. *E-urni anonüümistamine*
5. Häälte miksimine (valikuline)
6. Miksimistõendi kontrollimine
7. *Elektrooniliste häälte dekrüpteerimine*
8. *E-häälte lugemistõendi kontroll*
9. *E-häälte miksimistõendi kontroll*

PEATÜKK 3

Usaldusjuur

3.1 Rakenduste usaldusjuure kirjeldamine

Rakenduste usaldusjuur sisaldab andmeid seadistuste (kaasa arvatud usaldusjuure enda) allkirjade kontrollimiseks.

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 laetud.

Näide

`ivxv.properties`:

```
1 ca = conf-intermediate.pem, conf-root.pem
2 ocsp = ocsp-cert.pem
3 tsa = tsa-cert.pem
```

`ivxv.properties`:

```
ca = EE_Certification_Centre_Root_CA.pem.crt, ESTEID-SK_2011.pem.crt, ESTEID-SK_2015.pem.crt
ocsp = SK_OCSP_RESPONDER_2011.pem.cer
tsa = SK_TIMESTAMPING_AUTHORITY.pem.cer
```

3.2 Kogumisteenuse usaldusjuur

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 olema `trust.yaml`.

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.
Määrab Korraldaja.

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

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.checktimemark Kohustuslik väli. Tõeväärtus, kas seadistuste allkirjadel peavad olema BDOC spetsifikatsiooni jaotises 6.1 kirjeldatud ajamärgid. Kui tõene, siis ilma ajamärkideta allkirju ei usaldata. Kui väär, siis ajamärgid on lubatud, aga neid ei kontrollita.

authorizations Kohustuslik väli. Esmane nimekiri halduri volitustega isikutest, 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

`trust.yaml`:

```
# Usaldusjuure seadistuse näide

container:
  bdoc:
    bdocsize: 104857600  # 100 MiB
    filesize: 104857600  # 100 MiB
    checktimemark: true
    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

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

PEATÜKK 4

Võtmerakendus

Võtmerakendus 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 genereerimine (VALIKULINE)

Häälte salastamise võtme spetsifikatsioon genereeritakse kasutades tööriista *groupgen*. Võtmerakendus kasutab ElGamal'i krüptosüsteemi. Vastavalt aluseks olevale rühmale tuleb valida turvaparameeter, mis on hiljem aluseks rühma ja võtme genereerimisele.

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

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 2048, mis on samaväärne 2048 bitise RSA turvalisusega. 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.

groupgen.random_source.random_source_type Juhuarvugeneraatori allika tüüp.

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

`key.groupgen.yaml`:

```
groupgen:
  paramtype: mod
  length: 2048
  init_template: key.init.template.yaml
  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
```

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
2. PEM vormingus krüpteerimisvõtme sertifikaat
3. PEM vormingus krüpteerimisvõti

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.issuercn

init.signcn

init.signsn

init.enccn

init.encsn Võtmerakenduse poolt loodavate sertifikaatide DN väärtused.

---

init.required_randomness Juhuslikkuse allikatest loetava entroopia kohustuslik hulk baitides.

init.random_source Juhuarvugeneraatori sisendiks kasutatavate allikate loetelu.

init.random_source.random_source_type Juhuarvugeneraatori allika tüüp.

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

---

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`:

```
1 init:
2   identifier: TESTCONF
3   paramtype:
4     mod:
5       p:␣
  ↪3100662373957205559431637649681007865582127081875477675810174972 45.
  ↪..
6       g:␣
  ↪4581515311526584136500175248893367607586222161281486524028569284 35.
  ↪..
```

```
  out: initout
  skiptest: true
  fastmode: true
  signaturekeylen: 2048
  issuercn: TEST
  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.

out Krüpteerimise avaliku võtme asukoha kataloog.

threshold Testimiseks kasutatav lävi, sama mis võtme loomisel spetsifitseeritud.

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

fastmode Kaartidele automaatne terminalide määramine. Vaikimise väärtus on tõene.

`key.testkey.yaml`:

```
testkey:
  out: initout
  threshold: 2
  parties: 3
```

4.4 Elektrooniliste 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-urn anonüümistatud häältega.

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

decrypt.questioncount Küsimuste arv anonüümistatud e-urnis. 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: bb-4.json
  anonballotbox_checksum: bb-4.json.sha256sum.bdoc
  candidates: TESTCONF.choices.bdoc
  districts: TESTCONF.districts.bdoc
  provable: true
  check_decodable: false
  out: decout
```

4.5 Täiendavad tööriistad

util.listreaders Loetle ühendatud kaardilugejad.

`key.util.yaml`:

```
util:
  listreaders: true
```

PEATÜKK 5

Valijarakendus

Valijarakenduse seadistamist ning pakendamist käsitleb eraldi dokument.

PEATÜKK 6

Kontrollrakendus

Kontrollrakenduste seadistus on JSON formaadis. Android-seadmed otsivad seadistust aadressilt “https://eh.valimised.ee/apps/config_android.json”. iOS-seadmed otsivad seadistust aadressilt “https://eh.valimised.ee/apps/config_ios.json“

Reaalne sisu võib olla neil samasugune, kahe URL’i olemasolu on eelkõige võimalike erinevuste tekkimise jaoks ennatlik valik.

Seadistus koosneb viiest peamisest rühmast

- `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.

6.1 `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.
- `tspreg_client_cert` - Kogumisteenuse registreerimissertifikaat PEM vormingus.

6.2 Näide

```
{
  "appConfig": {
    "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!"
    },
    "errors": {
      "no_network_message": "Veenduge, et nutiseadme andmeside on␣
↪võimaldatud",
      "problem_qrcode_message": "QR koodi ei õnnestunud tuvastada",
      "bad_server_response_message": "Tehniline viga, palun␣
↪teavitage valimiste läbiviijat",
      "bad_device_message": "Selle seadmega pole võimalik␣
↪verifitseerida",
      "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,
      "public_key": "<valimiste_avalik_võti_pem>",
      "tspreg_service_cert": "<SK_TIMESTAMPING_AUTHORITY_CERT>",
      "ocsp_service_cert": ["<ESTEID-SK_2011_AIA_OCSP_RESPONDER_
↪CERT>","<ESTEID-SK_2015_AIA_OCSP_RESPONDER_CERT>"],
      "tspreg_client_cert": "<collector_tspreg_cert_pem>"
    },
    "elections": {
      "question-1": "Milline on looduskauneim koht?"
    }
```

```
    }
}
```

PEATÜKK 7

Kogumisteenus

7.1 Ülevaade

Kogumisteenuse juhtimine toimub signeeritud korralduste abil. Korraldused koostatakse tekstiredaktori abil ja signeeritakse ID-kaardiga.

Nimekiri kogumisteenuse haldamise korraldustest:

1. Usaldusjuure seadistus;
2. Tehniline seadistus;
3. Valimiste seadistus;
4. Valikute nimekiri;
5. Kasutajate volituste määramine;
6. Valijate nimekiri.

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 pool kasutatavad välised failid.

7.2 Valimise seadistus

Valimise seadistus määrab ühe valimise seadistuse.

Valimise seadistuse koostab valimiste korraldaja. Seadistusfaili nimi peab alati olema `election.yaml`.

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.

---

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.

---

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

Näide

`election.yaml`:

```
1  # Valimiste seadistuse näide
2
3  identifier: TESTCONF
4  questions:
5    - TESTQUESTION
6
7  period:
8    servicestart:  2017-01-16T08:50:00+02:00
9    electionstart: 2017-01-16T09:00:00+02:00
10   electionstop:  2017-01-18T19:00:00+02:00
11   servicestop:   2017-01-18T19:15:00+02:00
12
```

```
verification:
  count:    3
  minutes: 30
```

7.3 Tehniline seadistus

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

Seadistusfaili nimi peab alati olema `technical.yaml`.

Tehnilises seadistuses on laienduste seadistamiseks kaks erinevat lähenemist:

1. Kui sama funktsionaalsust saavad korraga pakkuda mitu laiendust, siis igaüks saab oma alambloki ning laiendus on seadistatud, kui blokk ei ole tühi. Näiteks `container`, kus `container.bdoc` on vaid üks võimalikest allkirjade kontrollimise laiendustest ning saab töötada rööbiti teiste `container.*` laiendustega.
2. Kui sama funktsionaalsust saab pakkuda korraga ainult üks laiendus, siis laienduse nimi tuuakse eraldi välja ning tema seadistus pannakse alamblokki. Näiteks `storage`, kus saab korraga kasutada ainult ühte talletusprotokolli. `storage.protocol` määrab laienduse ning seadistus läheb `storage.conf` blokki. Sellise struktuuriga saab korraga seadistada ainult ühe laienduse.

debug Tõeväärtus, kas logidesse kirjutatakse silumisteateid.
Määrab kogumisteenuse osutaja.

---

voterlist Kohustuslik väli. Valijate nimekirjade kontrollimise parameetrid.

voterlist.key Kohustuslik väli. RSA-võtmepaari avalik võti valijate nimekirjade allkirja kontrollimiseks.
Määrab Korraldaja.

---

auth Kohustuslik väli. Alamblokk, mis sisaldab valija tuvastamise seadistust.
Kõik valija tuvastamise parameetrid määrab Korraldaja.

auth.ticket Alamblokk, mis sisaldab piletipõhise valija tuvastamise seadistust.
Piletipõhist valija tuvastamist kasutatakse Mobiil-ID puhul, kus `dds` 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.

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

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.

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

Eesti elektrooniliste isikut tõendavate dokumentide korral on esimese valiku puhul identifikaator kujul “PERENIMI,EESNIMI,ISIKUKOOD” ning teise puhul “ISIKUKOOD”.

---

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

Kõik valija vanuse kontrollimise parameetrid määrab Korraldaja.

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.

Kõik BDOC-allkirjade kontrollimise parameetrid määrab Korraldaja.

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.checktimemark Kohustuslik väli. Tõeväärtus, kas häälte allkirjadel peavad olema BDOC spetsifikatsiooni jaotises 6.1 kirjeldatud ajamärgid. Kui tõene, siis ilma ajamärkideta hääli vastu ei võeta. Kui väär, siis ajamärgid on lubatud, aga neid ei kontrollita.

See peaks olema väär, kuna kõikide allkirjastamisvahendite puhul ei ole sissetuleval häälel ajamärki (nt Eesti ID-kaart). Ajamärgid ei ole siin kohustuslikud, kuna kogumisteenus küsib allkirjastaja sertifikaadile ise kehtivuskinnituse.

---

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.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.

---

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.dds 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.*.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 (loetelus esimene), vajadusel ka täiendavad serverid.
Kõik logiserverite parameetrid määrab kogumisteenuse osutaja.

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

logging.port Logiserveri port (täisarv, vaikimisi 514).

logging.protocol Kohustuslik väli. Logiserverisse logimise protokoll (*udp* või *tcp*, vaikimisi *udp*).

---

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.

---

dds Alamblokk, mis sisaldab Mobiil-ID teenusepakkuja seadistust.
Kõik Mobiil-ID teenusepakkuja parameetrid määrab Korraldaja.

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

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

dds.servicename Kohustuslik väli. Mobiil-ID teenusepakkujaga kokkulepitud teenusenimi.

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

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

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

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

dds.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.

Kõik kvalifitseerivate päringute parameetrid määrab Korraldaja.

qualification.*.protocol Kohustuslik väli. Kvalifitseeriva päringu protokoll. Hetkel toetatud `ocsp`, `ocsptm`, `tsp` ja `tspreg`.

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.

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.

---

stats E-hääletuse statistika laadimise parameetrid.
Kõik statistika laadimise parameetrid määrab Korraldaja.

stats.url Kohustuslik väli. E-hääletuse statistika laadimise URL.

stats.tlscert Kohustuslik väli. E-hääletuse statistika laadimise serveri TLS-sertifikaat.

technical.yaml:

```
# Tehnilise seadistuse näide

debug: true

voterlist:
  key: !container rr_pub.key

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
      responders:
        - !container TEST_of_SK_OCSP_RESPONDER_2011.pem

identity: serialnumber

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

vote:
  bdoc:
    bdocsize: 32768  # 32 KiB
    filesize: 32768  # 32 KiB
    checktimemark: false
    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

filter:
  tls:
    handshaketimeout: 10
  codec:
    rwtimeout: 5
```

```
network:
  - id: default
    services:
      proxy:
        - id:          proxy@proxy1.ivxv.ee
          address:     proxy1.ivxv.ee:443
      dds:
        - id:          dds@dds1.ivxv.ee
          address:     dds1.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: 514
    protocol: udp
  - address: logserver2.ivxv.ee
    port: 514
    protocol: tcp

storage:
  protocol: etcd
  conf:
    ca: !container etcd_CA.pem
    conntimeout: 5
    optimeout: 10

dds:
  url: https://tsp.demo.sk.ee/v2/
  language: EST
  servicename: Testimine
  authmessage: Mobiil-ID autentimise testimine.
  signmessage: Mobiil-ID allkirjastamise testimine.
  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:
    responders:
      - !container TEST_of_SK_OCSP_RESPONDER_2011.pem

qualification:
  - protocol: ocsptm
    conf:
      url: http://demo.sk.ee/ocsp
      responders:
        - !container TEST_of_SK_OCSP_RESPONDER_2011.pem
  - protocol: tspreg
    conf:
      url: http://demo.sk.ee/tsa
      signers:
        - !container DEMO_of_SK_TSA_2014.pem
      delaytime: 1

stats:
  url: http://stats.server/path.json
  tlscert: !container Stats_Server_Certificate.pem
```

7.4 Volitused

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 1. Rollide ja volituste maatriks

	admin	election- conf-manager	viewer	none
Üldseisundi ja statistika vaatamine	✓	✓	✓	-
Teenuste sertifikaatide paki allalaadimine	✓	✓	✓	-
Hääletusteenuste registreerimisvõtme allalaadimine	✓	✓	✓	-
Valimiste seadistuste rakendamine	✓	✓	-	-
E-urni 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.

7.5 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 rsa:2048 -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 rsa:2048 -nodes -keyout <teenuse-id>-tls.key
  -out etcd-<teenuse-id>-tls.csr -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.

Talletusteenuse 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.conf -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_choices ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature,␣
↪keyEncipherment, keyAgreement
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: choices.ivxv.invalid

[ ext_dds ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
keyUsage                = critical, digitalSignature,␣
↪keyEncipherment, keyAgreement
extendedKeyUsage        = critical, serverAuth  # No clientAuth.
subjectAltName          = DNS: dds.ivxv.invalid

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

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

[ ext_verification ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
```

```
keyUsage                = critical, digitalSignature,␣
↪keyEncipherment, keyAgreement
extendedKeyUsage        = critical, serverAuth, clientAuth
subjectAltName          = DNS: verification.ivxv.invalid
```

Hääletamisteenuse ajatemplipäringute signeerimisvõtme ja sertifikaadi genereerimine

Hääletusteenuse registreerimisvõti genereeritakse järgneva käsuga:

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

Käsu väljundiks on fail `tspreg.key`.

Hääletusteenuse registreerimisvõtme sertifikaat genereeritakse järgneva käsuga:

```
$ openssl req -new -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 on 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

Töötlemisrakendus

Töötlemisrakendus on käsurearakendus e-urni 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 koguja või eelmise tööriista poolt väljastatud e-urn ja e-urni digitaalselt allkirjastatud räsi. Väljundi hulgas on töötlemisetapi tulemuseks olev e-urn koos allkirjastamata räsiga. Kuna rakendused käivitatakse internetiühenduseta arvutis, tuleb räsifailid tõsta digitaalseks allkirjastamiseks välisesse seadmesse. E-urni räsi arvutatakse funktsiooniga `hex(sha256(<fail>))`.

Lisaks põhitööriistadele on rakendusel veel kaks täiendavat tööriista: *export* ja *verify*.

Kõigi tööriistade kasutamine eeldab allkirjastatud usaldusjuure ja konkreetse tööriista seadistuste olemasolu. Tööriistadel, mis väljastavad faile, tuleb seadistustes määrata väljundkausta asukoht, mida ei tohi käivitamise ajal eksisteerida. Alljärgnevalt kirjeldame konkreetsete tööriistade seadistusi.

8.1 E-urni töötlemine - verifitseerimine

Kogujast väljastatud e-urni verifitseerimiseks kasutatakse tööriista *check*. Urni 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-urni andmeterviklus,
- E-hääletajate valimisõigus e. kuuluvus valijate nimekirja (kontrollitakse juhul kui valijate nimekirjad on seadistustega antud),
- E-urnis sisalduvate häälte digiallkirja vormingule vastavus,
- Registreerimisandmete andmeterviklus,

- E-urnis sisalduvate häälte vastavus registreerimisandmetega.

E-urni verifitseerimine on töömahukas protsess. 4-tuumalise *i7* protsessoriga arvuti suudab 1 sekundi jooksul töödelda umbes 200 häält. Töötlemise jooksul kuvatakse kasutajale edenemisriba, mille alusel on võimalik ennustada töötlemisele kuluvat aega.

Suure e-urni verifitseerimisel võib olla tarvilik protsessile mälu juurde anda. Selleks tuleb seada keskkonnamuutuja `PROCESSOR_OPTS`. Näiteks 6 gigabaidi mälu eraldamiseks `PROCESSOR_OPTS=-Xmx6G`.

check.ballotbox Kogujast väljastatud e-urn.

check.ballotbox_checksum Kogujast väljastatud e-urni digitaalselt allkirjastatud räsi.

check.districts Digitaalselt allkirjastatud ringkondade nimekiri.

check.registrationlist Registreerimisteenusest pärit registreerimisandmed.

check.registrationlist_checksum Registreerimisandmete digitaalselt allkirjastatud räsi.

check.tskey Registreerimispäringute verifitseerimiseks kasutatav koguja avalik võti.

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

check.voterlists Valijate nimekirjade loend. Võib olla tühi, mis juhul e-hääletanute hääleõigust ei kontrollita.

check.voterlists.path Valijate nimekirja fail.

check.voterlists.signature Valijate nimekirja allkiri, mis on antud algoritmiga `sha256WithRSAEncryption`.

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

check.election_start Hääletamise algus. Varasema hääletusajaga hääli käsitletakse proovihäältena ning need lugemisele ei lähe.

check.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. Tervikluskontrolliga korrastatud e-urn `bb-1.json`,
2. Tervikluskontrolliga korrastatud e-urni räsi `bb-1.json.sha256sum`,
3. E-urni töötlemisvigade raport `ballotbox_errors.txt` (valikuline),
4. Valijate nimekirjade töötlemisvigade raport `voterlist_errors.txt` (valikuline),
5. *Log1* fail e. vastvõetud hääled `<valimise id>.<küsimuse id>.log1`.

`processor.check.yaml`:

```
1 check:
2   ballotbox: TESTCONF.votes.zip
3   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
```

8.2 E-urni töötlemine - korduvhäälte tühistamine

Korduvate e-häälte tühistamiseks kasutatakse tööriista *squash*. Tööriist saab sisendiks tööriista *check* poolt koostatud e-urni ning eemaldab sellest iga hääletaja kohta kõik hääled peale hiliseima.

squash.ballotbox Tervikluskontrolliga korrastatud e-urn.

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

squash.districts Digitaalselt allkirjastatud ringkondade nimekiri.

squash.out Tööriista väljundkaust. Sellesse kausta luuakse:

1. Korduvhäältest puhastatud e-urn `bb-2.json`,
2. Korduvhäältest puhastatud e-urni räsi `bb-2.json.sha256sum`,
3. E-hääletanute nimekiri *JSON* vormingus `ivoterlist.json`,
4. E-hääletanute nimekiri *PDF* vormingus `ivoterlist.pdf`,
5. Tühistamiste ja ennistamiste aruanne `revocation-report.csv`,
6. *Log2* fail e. tühistatud hääled `<valimise id>.<küsimuse id>.log2`.

`processor.squash.yaml`:

```
squash:
  ballotbox: out-1/bb-1.json
  ballotbox_checksum: out-1/bb-1.json.sha256sum.bdoc
  districts: TESTCONF.districts.bdoc
  out: out-2
```

8.3 E-urni töötlemine - häälte tühistamine ja ennistamine jaoskonnainfo põhjal

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

revoke.ballotbox Korduvhäältest puhastatud e-urn.

revoke.ballotbox_checksum Korduvhäältest puhastatud e-urni 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-urn `bb-3.json`,
2. Korduvhääletajate häältest puhastatud e-urni räsi `bb-3.json.sha256sum`,
3. Tühistamiste ja ennistamiste aruanne `revocation-report.csv`,
4. E-hääletanute nimekiri *JSON* vormingus `ivoterlist.json`,
5. E-hääletanute nimekiri *PDF* vormingus `ivoterlist.pdf`,
6. *Log2* fail e. tühistatud hääled `<valimise id>.<küsimuse id>.log2`.

`processor.revoke.yaml`:

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

8.4 E-urni anonüümistamine

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

anonymize.ballotbox Korduvhääletajate häältest puhastatud e-urn.

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

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

anonymize.out Tööriista väljundkaust. Sellesse kausta luuakse:

1. Hääletajate isikuandmetest puhastatud e-urn `bb-4.json`,
2. Hääletajate isikuandmetest puhastatud e-urni räsi `bb-4.json.sha256sum`,
3. *Log3* fail e. lugemisele läinud hääled `<valimise id>.<küsimuse id>.log3`.

`processor.anonymize.yaml`:

```
anonymize:
  ballotbox: out-3/bb-3.json
  ballotbox_checksum: out-3/bb-3.json.sha256sum.bdoc
  enckey: enc.pub.key
  out: out-4
```

8.5 Täiendavad tööriistad

Tööriist *verify*

Tööriist *verify* on täiendav tööriist, millega saab verifitseerida etteantud digitaalselt allkirjastatud konteineri digiallkirja ning kuvada välja konteineri info.

verify.file Verifitseeritav fail.

`processor.verify.yaml`:

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

Tööriist *export*

Tööriist *export* on täiendav tööriist, millega saab eksportida kogujast saadud e-urni seest täielikke digitaalselt allkirjastatud hääle konteinereid. On võimalik eksportida nii kõiki hääli korraga, kui konkreetse valija hääli.

export.ballotbox Kogujast väljastatud e-urn.

export.ballotbox_checksum Kogujast väljastatud e-urni digitaalselt allkirjastatud räsi.

export.voter_id Valija identifikaator (valikuline).

export.out Tööriista väljundkaust. Sellesse kausta tekivad:

1. E-urni töötlemisvigade raport `ballotbox_errors.txt` (valikuline),
2. E-urnist eksporditud häälte digitaalselt allkirjastatud konteinerid.

`processor.export.yaml`:

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

PEATÜKK 9

Auditirakendus

Auditirakendus koosneb tööriistadest *mixer* ja *decrypt*. Kõigi tööriistade kasutamine eeldab allkirjastatud usaldusjuure ja konkreetse tööriista seadistuste olemasolu. Allpool järgnevalt kirjeldame konkreetsete tööriistade seadistusi.

9.1 E-häälte miksimistõendi kontroll

Tööriist *mixer* kontrollib Verificatumi lugemistõendi korrektsust.

mixer.protinfo Verificatumi segamistõendi protokollifaili asukoht.

mixer.proofdir Verificatumi segamistõendi asukoht.

mixer.threaded Kasuta mitmelõimelist implementatsiooni. Kasutatavate lõimede arv sõltub rakenduse argumentidest. Vaikimisi väärtus väär.

`auditor.mixer.yaml`:

```
1 mixer:
2   protinfo: mixnet/ProtocolInformation.xml
3   proofdir: mixnet/
4   threaded: true
```

9.2 E-häälte lugemistõendi kontroll

Tööriist *decrypt* kontrollib dekrüpteerimistõendi korrektsust.

decrypt.input Dekrüpteerimistõendi asukoht

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

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

auditor.decrypt.yaml:

```
decrypt:
  input: decout/proof
  pub: initout/pub.pem
  out: auditout
```