

|  |
| --- |
| X-tee üleandmise testplaan |
| Testplaan  Redaktsioon: 1.4  29.12.2015  91 lk  Y-884-1 |

|  |  |  |  |
| --- | --- | --- | --- |
| Kuupäev | Nr | Kirjeldus. | Autor |
| 16.06.2015 | 0.1 | Esimene versioon | Karin Klooster |
| 02.07.2015 | 0.2 | Lisatud teststsenaariumid päringulogide töötlemise (ptk 2.3) ja halduslogimise kohta (ptk 2.11) | Karin Klooster |
| 31.08.2105 | 0.3 | SSL > TLS. Muudetud stsenaariumit 2.8. Täiendatud stsenaariumit 2.2.3. Muudetud stsenaariumit 2.3.4.6. Lisatud stsenaarium 2.3.4.4. Lisatud stsenaariumid keskserveri kõrgkäideldavuse testimiseks (ptk 2.13, muudetud ka ptk 1.4). Pisiparandused teststsenaariumites. | Karin Klooster |
| 18.09.2015 | 0.4 | Lisatud ja täiendatud keskserveri kõrgkäideldavuse teststsenaariumeid (ptk 2.13). Pisiparandused teststsenaariumites. | Karin Klooster |
| 21.09.2015 | 0.5 | Keskserveris ei ole enam tabelit distributed\_signed\_files (parandatud ptk 2.9) | Karin Klooster |
| 22.09.2015 | 0.6 | Lisatud info, et kõik selles dokumendis olevad testid on edukalt läbitud (1.2). | Karin Klooster |
| 26.10.2015 | 1.0 | Lisatud testsenaariumitesse SSCD seadme labeli tugi (muudetud stsenaariumeid 2.1.1 ja 2.1.3). Lisatud testsenaariumitesse sertifikaaditaotluse väljade automaatne täitmine (muudetud stsenaariumeid 2.1.3 ja 2.1.4). Lisatud testsenaariumid MTOM ja swaRef manustega päringute tegemise kohta (ptk 2.2.4). X-tee liikme turvaserveri kliendiks registreerimine asendatud alamsüsteemi turvaserveri kliendiks registreerimisega. Muudetud haldusteenuste osutaja seadistamise teststsenaariumeid, lisatud (2.1.6). Pisiparandused teststsenaariumites. | Karin Klooster |
| 29.10.2015 | 1.1 | Parandatud teststsenaariumit 2.13.3.4 | Karin Klooster |
| 10.11.2015 | 1.2 | Täiendatud serveri varundamise ja taastamise teststsenaariumeid (täiendatud 2.4.8, lisatud 2.13.3.5) | Karin Klooster |
| 16.12.2015 | 1.3 | Täiendatud keskserveri kõrgkäideldavusega seotud varundamise ja taastamise teststsenaariume (jaotis 2.13.5) | Marju Ignatjeva |
| 29.12.2015 | 1.4 | Lisatud teststsenaariumid WSDL validaatori testimiseks (2.2.2.1, 2.2.2.2, 2.2.5.1) | Karin Klooster |

Sisukord

[1 Sissejuhatus 6](#__RefHeading__1436_2115075793)

[1.1 Litsents 6](#__RefHeading__4852_1249486692)

[1.2 Eesmärk 6](#__RefHeading___Toc11443_1192923707)

[1.3 Testitav funktsionaalsus 6](#__RefHeading__1438_2115075793)

[1.4 Riistvara 6](#__RefHeading__1452_2115075793)

[1.5 Teadmiseks enne testimist 7](#__RefHeading__13824_1448969664)

[2 Testide kirjeldus 8](#__RefHeading__15171_908407261)

[2.1 Süsteemi paigaldamine ja esmane seadistamine 8](#__RefHeading__15173_908407261)

[2.1.1 Teststsenaarium: X-tee eksemplari AA keskserveri paigaldamine ja esialgne seadistamine 8](#__RefHeading__11749_1448969664)

[2.1.2 Teststsenaarium: Haldusteenuste turvaserveri TS1 paigaldamine ja seadistamine 10](#__RefHeading__11751_1448969664)

[2.1.3 Abistsenaarium: Turvaserveri kliendi sertifitseerimine 11](#__RefHeading__1492_1448969664)

[2.1.4 Abistsenaarium: Turvaserveri sertifitseerimine 12](#__RefHeading__1494_1448969664)

[2.1.5 Teststsenaarium: Haldusteenuste turvaserveri TS1 registreerimine keskserveris 13](#__RefHeading__11753_1448969664)

[2.1.6 Teststsenaarium: Haldusteenuste seadistamine turvaserveris TS1 14](#__RefHeading___Toc24741_1353917784)

[2.1.7 Teststsenaarium: Turvaserveri TS2 paigaldamine, seadistamine ja registreerimine 15](#__RefHeading__11755_1448969664)

[2.1.8 Abistsenaarium: Pääsuõiguse andmine teenuse vaatest 16](#__RefHeading__3136_1448969664)

[2.1.9 Abistsenaarium: Pääsuõiguse andmine teenuse kliendi vaatest 16](#__RefHeading__1756_1448969664)

[2.2 Turvaserveri klientide ja teenuste haldus 17](#__RefHeading__11757_1448969664)

[2.2.1 Teststsenaarium: Klientide registreerimine turvaserveritesse 18](#__RefHeading__11759_1448969664)

[2.2.2 Teststsenaarium: Test-teenuse seadistamine 20](#__RefHeading__4143_1448969664)

[2.2.3 Teststsenaarium: Test-teenuse kasutamine 21](#__RefHeading__11761_1448969664)

[2.2.4 Test-teenuse kasutamine MTOM ja swaRef manustega 22](#__RefHeading___Toc24743_1353917784)

[2.2.5 Teststsenaarium: WSDL värskendamine 24](#__RefHeading__11763_1448969664)

[2.2.6 Teststsenaarium: WSDLi inaktiveerimine 25](#__RefHeading__11765_1448969664)

[2.2.7 Teststsenaarium: TLS kasutamine sisevõrgus 25](#__RefHeading__11767_1448969664)

[2.2.8 Teststsenaarium: Kesksete teenuste seadistamine ja kasutamine 26](#__RefHeading__11769_1448969664)

[2.2.9 Teststsenaarium: Pääsuõiguse andmine X-tee liikmele. 28](#__RefHeading__11771_1448969664)

[2.2.10 Teststsenaarium: Pääsuõiguse andmine globaalsele grupile 28](#__RefHeading__11773_1448969664)

[2.2.11 Teststsenaarium: Pääsuõiguse andmine lokaalsele grupile. 29](#__RefHeading__11775_1448969664)

[2.2.12 Teststsenaarium: Sertifikaatide aktiveerimine ja inaktiveerimine 30](#__RefHeading__11777_1448969664)

[2.2.13 Teststsenaarium: Võtmevahetus turvaserveris 31](#__RefHeading__11779_1448969664)

[2.2.14 Teststsenaarium: Sertifikaatide OCSP vastused 32](#__RefHeading__11781_1448969664)

[2.3 Päringulogide arhiveerimine ja päringulogidest allkirjade eraldamine 34](#__RefHeading__45410_1322844446)

[2.3.1 Teststsenaarium: Päringulogide arhiveerimine, päringulogidest allkirjade eraldamine ja arhiivifaili krüptoahela verifitseerimine 34](#__RefHeading__11783_1448969664)

[2.3.2 Teststsenaarium: Pakkajatemplit ja pakksignatuuri sisaldavatest päringulogidest allkirjade eraldamine 35](#__RefHeading__45412_1322844446)

[2.3.3 Teststsenaarium: Päringu identifikaatoris failisüsteemi jaoks sobimatute sümbolite asendamine 37](#__RefHeading__60910_2134818282)

[2.3.4 Teststsenaarium: ASiC-konteinerite küsimine turvaserverist 37](#__RefHeading__45414_1322844446)

[2.3.5 Abistsenaarium: Signeeritud päringu verifitseerimine 41](#__RefHeading__44890_1322844446)

[2.4 Registreeritud objektide kustutamine 41](#__RefHeading__11785_1448969664)

[2.4.1 Teststsenaarium: X-tee liikme kustutamine keskserverist 41](#__RefHeading__11787_1448969664)

[2.4.2 Teststsenaarium: Turvaserveri omaniku kustutamine keskserverist 42](#__RefHeading__11789_1448969664)

[2.4.3 Teststsenaarium: Turvaserveri kustutamine keskserverist 43](#__RefHeading__11791_1448969664)

[2.4.4 Teststsenaarium: Turvaserveri kliendi kustutamine keskserverist 44](#__RefHeading__11793_1448969664)

[2.4.5 Teststsenaarium: Turvaserveri kliendi kustutamine turvaserverist 45](#__RefHeading__11795_1448969664)

[2.4.6 Teststsenaarium: Autentimissertifikaadi kustutamine keskserverist 46](#__RefHeading__11797_1448969664)

[2.4.7 Teststsenaarium: Autentimissertifikaadi kustutamine turvaserverist 46](#__RefHeading__11799_1448969664)

[2.4.8 Abistsenaarium: Serveri varundamine ja taastamine 48](#__RefHeading__7038_1448969664)

[2.5 Föderatsiooni tugi 55](#__RefHeading__11801_1448969664)

[2.5.1 Teststsenaarium: X-tee eksemplari BB keskserveri paigaldamine ja esialgne seadistamine 55](#__RefHeading__11803_1448969664)

[2.5.2 Teststsenaarium: Haldusteenuste turvaserveri TS3 paigaldamine, seadistamine ja registreerimine 56](#__RefHeading__11805_1448969664)

[2.5.3 Teststsenaarium: Kliendi registreerimine turvaserverisse TS3 58](#__RefHeading__11807_1448969664)

[2.5.4 Teststsenaarium: Föderatsiooni seadistamine 59](#__RefHeading__11809_1448969664)

[2.5.5 Teststsenaarium: Päringute vahendamine X-tee eksemplaride vahel 59](#__RefHeading__7845_1448969664)

[2.5.6 Teststsenaarium: Sisemise konfiguratsiooni signeerimisvõtme vahetamine 61](#__RefHeading__11811_1448969664)

[2.5.7 Teststsenaarium: Välimise konfiguratsiooni signeerimisvõtme vahetamine 62](#__RefHeading__11813_1448969664)

[2.5.8 Teststsenaarium: Föderatsiooni lõpetamine 63](#__RefHeading__11815_1448969664)

[2.5.9 Teststsenaarium: Konfiguratsioonivahendaja kasutamine 63](#__RefHeading__11817_1448969664)

[2.6 Teenusepakkuja turvaserveri dubleerimine 65](#__RefHeading__11819_1448969664)

[2.7 Kasutajate haldus ning eri rollides kasutajate õigused turvaserveris ja keskserveris 65](#__RefHeading__11821_1448969664)

[2.8 Metateenuste kasutamine 66](#__RefHeading__39498_2134818282)

[2.9 Keskserveri andmebaasi kirjete versioneerimine 66](#__RefHeading__53286_2134818282)

[2.9.1 Teststsenaarium: andmebaasikirjete muutmine kasutajaliidese kaudu 67](#__RefHeading__53288_2134818282)

[2.9.2 Teststsenaarium: andmebaasikirjete muutmine Postgresi käsurealt 67](#__RefHeading__53290_2134818282)

[2.9.3 Teststsenaarium: andmebaasikirjete muutmine ajalootoeta tabelites 67](#__RefHeading__53292_2134818282)

[2.9.4 Teststsenaarium: ajalootabeli toe säilimine peale keskserveri taastamist 68](#__RefHeading__53294_2134818282)

[2.10 Turvaserveri andmebaasi kirjete versioneerimine 68](#__RefHeading__53296_2134818282)

[2.10.1 Teststsenaarium: andmebaasikirjete muutmine kasutajaliidese kaudu 68](#__RefHeading__53298_2134818282)

[2.10.2 Teststsenaarium: andmebaasikirjete muutmine Postgresi käsurealt 69](#__RefHeading__53300_2134818282)

[2.10.3 Teststsenaarium: ajalootabeli toe säilimine peale turvaserveri taastamist 69](#__RefHeading__53302_2134818282)

[2.11 Halduslogimine 69](#__RefHeading__46999_1322844446)

[2.11.1 Haldustegevuste logimine keskserveris 69](#__RefHeading__47745_1322844446)

[2.11.2 Haldustegevuste logimine turvaserveris 70](#__RefHeading__47747_1322844446)

[2.11.3 Haldustegevuste logimine utiliidis signer-console 71](#__RefHeading__47749_1322844446)

[2.12 Kasutaja sessiooni aegumine keskserveris ja turvaserveris 72](#__RefHeading__53304_2134818282)

[2.13 Keskserveri kõrgkäideldavus 72](#__RefHeading__48842_937342822)

[2.13.1 Terminid ja lühendid 72](#__RefHeading__48844_937342822)

[2.13.2 Testimise käigus vajalik info 73](#__RefHeading__48846_937342822)

[2.13.3 Abistsenaariumid 73](#__RefHeading__48848_937342822)

[2.13.4 X-tee eksemplari CC keskserverite paigaldamine ja esialgne seadistamine 77](#__RefHeading__48850_937342822)

[2.13.5 Kõrgkäideldava süsteemi varundamine ja taaste 79](#__RefHeading___Toc43797_139069472)

[2.13.6 Konfiguratsiooniankrute genereerimine kõrgkäideldavas süsteemis 81](#__RefHeading___Toc43799_139069472)

[2.13.7 Halduslogimine kõrgkäideldavas süsteemis 81](#__RefHeading___Toc43801_139069472)

[2.13.8 X-tee eksemplari AA kõrgkäideldava keskserverite klastri seadistamine 82](#__RefHeading__48852_937342822)

[2.13.9 HA klastri tervisenäitajate vaatamine 85](#__RefHeading__48854_937342822)

[2.13.10 Andmebaaside replikeerumine 85](#__RefHeading__48856_937342822)

[2.13.11 Keskserveri aadressi muutmine 86](#__RefHeading__48858_937342822)

[2.13.12 Konfiguratsiooni sisu sõlmele vastavuse kontrollimine 87](#__RefHeading__48860_937342822)

[2.13.13 Haldusteenuste kasutamine 88](#__RefHeading__48862_937342822)

[2.13.14 Mitme konfiguratsiooniallikaga ankrute genereerimine 88](#__RefHeading__48864_937342822)

[2.13.15 Konfiguratsiooniallika kaudu konfiguratsiooni levitamise ajutine katkestamine föderatsioonis 89](#__RefHeading__48866_937342822)

[2.13.16 Mitme konfiguratsiooniallika vahel valimine 90](#__RefHeading__48868_937342822)

# Sissejuhatus

## Litsents

See töö on litsenseeritud. Creative Commons Attribution-ShareAlike 3.0 Unported License. Litsentsi koopia leiab: <http://creativecommons.org/licenses/by-sa/3.0/>.

## Eesmärk

Selles dokumendis antakse ülevaade X-tee versiooni 6.8.2 toimimise kontrollimiseks läbi viidud testidest. Kõik selles dokumendis olevad testid on edukalt läbitud.

## Testitav funktsionaalsus

Selles dokumendis kirjeldatud testidega kontrollitakse X-tee versiooni 6.8.2 järgmise funktsionaalsuse korrektset toimimist:

1. süsteemi paigaldamine;
2. X-tee liikmete, turvaserverite ja klientide haldus;
3. võtmeseadmete ja sertifikaatide haldus;
4. päringute vahendamine ühe X-tee eksemplari siseselt;
5. föderatsiooni seadistamine;
6. päringute vahendamine X-tee eksemplaride vahel;
7. konfiguratsioonihaldus;
8. konfiguratsioonivahendaja kasutamine;
9. keskserveri kõrgkäideldavus.

## Riistvara

Kõik testkeskkonna masinad peavad vastama X-tee 6.8.2 serverite riistvaranõuetele (vt. paigaldusjuhendid).

Testi alguses on kõik testserverid (va. üldised teenused) tühjad -- paigaldatud on vaid operatsioonisüsteem Ubuntu 14.04. Paigaldatakse kolm X-tee installatsiooni: AA, BB ja CC.

Testid viiakse läbi järgmistel serveritel.

* Installatsioonis AA on keskserverid KS1 ja KS3 (HA klaster) ja turvaserverid TS1 ja TS2.
* Installatsioonis BB on keskserver KS2 ja turvaserver TS3.
* Installatsioonis CC on keskserverid KS4 ja KS5 (HA klaster). Taaste testimisel kasutatakse keskservereid KS4a ja KS5a, mis võivad olla eraldi serverid või eelnevalt tühjendatud keskserverid KS4 ja KS5.
* Keskserver KS1 ja turvaserver TS2 on ühendatud HSMiga.
* Konfiguratsioonivahendaja ja turvaserver TS1 on ühendatud kiipkaardiga.
* Lisaks kuulub testkeskkonda konfiguratsioonivahendaja (CP).

Lisaks kasutatakse testide käigus järgmiseid ressursse:

* sertifitseerimisteenus(ed);
* ajatempliteenus(ed);
* testklient;
* test-teenus;
* arhiiviserver;
* asicverifier.

## Teadmiseks enne testimist

* Testimise käigus tuleb arvesse võtta, et keskserveris tehtud muutuste turvaserveriteni jõudmiseks kulub ~2 minutit.
* Mitme sertifitseerimisteenuse ja ajatempliteenuse samaaegset kasutamist ei ole testides eraldi kirjeldatud. Selle testimiseks võib keskserveris KS1 kirjeldada mitu heakskiidetud usaldusteenust ja TS1 ja TS2 konfigureerida kasutama erinevaid ajatempliteenuseid ning sertifikaate võtta erinevatelt sertifitseerimisteenustelt.
* Abistsenaariumid on mõeldud kasutamiseks teiste teststsenaariumite käigus. Need tuleks läbi teha teststsenaariumi sammudes, kus neile on viidatud.
* Veaolukordi tuleks testida teststsenaariumite käigus, sammudes, kus neile on viidatud.
* X-tee 6.8.2 lisandunud funktsionaalsuse testimiseks on vaja läbida järgmistes peatükkides toodud teststsenaariumid:
  + 2.2.2.1 Veaolukorrad: WSDL lisamine
  + 2.2.2.2 Veaolukorrad: WSDLi aadressi muutmine
  + 2.2.5.1 Veaolukorrad: WSDLi värskendamine

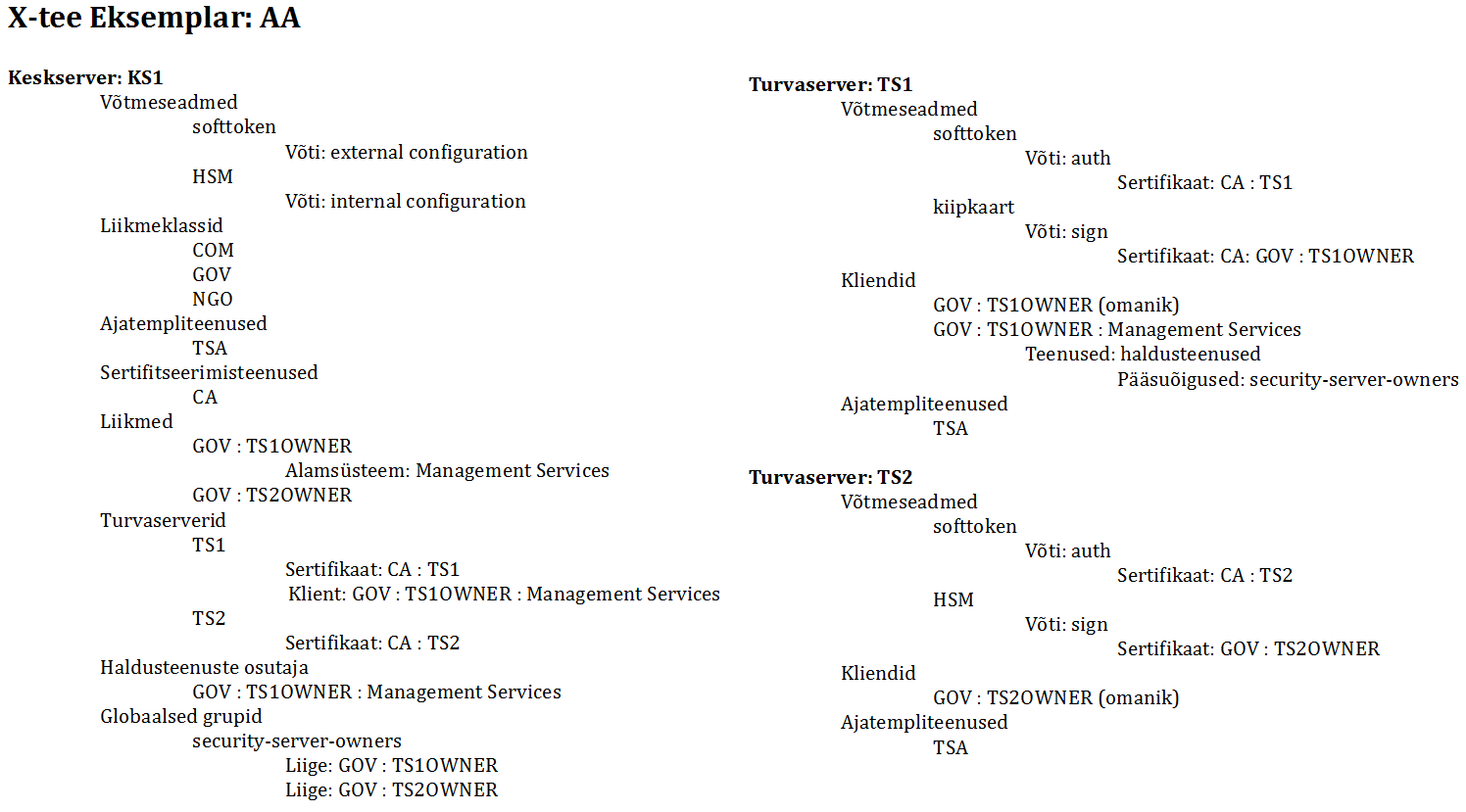
# Testide kirjeldus

## Süsteemi paigaldamine ja esmane seadistamine

Peatükis testitakse ühe X-tee infrastruktuuri esialgset paigaldamist ja seadistamist tavakasutuseks. Täpsemalt:

* Keskserveri ja turvaserveri pakkide paigaldamine ja initsialiseerimine.
* Riistvaraliste võtmeseadmete paigaldamine keskserverisse ja turvaserverisse.
* Keskserveri seadistamine, sh liikmeklasside, usaldusteenuste ja konfiguratsiooni seadistamine.
* Turvaserverite seadistamine, sh ajatempliteenuste seadistamine ning omanike ja turvaserverite registreerimine keskserveris (autentimissertifikaadi registreerimistaotlused).
* Keskserveri haldusteenuste turvaserveri seadistamine haldusteenuste osutamiseks.

Süsteemi seadistus selle peatüki testide lõpuks:



### Teststsenaarium: X-tee eksemplari AA keskserveri paigaldamine ja esialgne seadistamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1

Teststsenaarium:

1. Paigaldatakse keskserveri pakid.
2. Initsialiseeritakse keskserver (vt Veaolukorrad: keskserveri initsialiseerimine):
   * seadistatakse keskserveri aadress ja eksemplari identifikaator: **AA**;
   * initsialiseeritakse tarkvaraline võtmeseade: **PIN = 1234**.
3. Seadistatakse keskserver kasutama HSMi.
4. Seadistatakse liikmeklassid (vt Veaolukorrad: liikmeklasside seadistamine):
   * code: **GOV**, description: **Government organization**
   * code: **COM**, description: **Commercial enterprise**
   * code: **NGO**, description: **Non-governmental organization**
5. Seadistatakse sertifitseerimis- ja ajatempliteenused.
6. Konfiguratsiooniallikatele (nii sisemisele kui välimisele) genereeritakse võtmed:
   * **sisemise** konfiguratsiooniallika võti genereeritakse **HSM**ile
   * **välise** konfiguratsiooniallika võti genereeritakse **tarkvaralisele** seadmele
   * veendutakse, et nii HSM-le kui tarkvaralisele seadmele võtme genereerimisel on võimalik määrata võtme *label*.
7. Veendutakse, et:
   * allkirjavõti seatakse automaatselt aktiivseks, st kuvatakse tabelis rasvases kirjas
   * allkirjavõtme lisamisele järgnevalt genereeritakse automaatselt konfiguratsiooniallika ankur
8. Eksporditakse konfiguratsiooniallikate ankrud.
9. X-tee liikmeks lisatakse: Name: **TS1 Owner**, Class: **GOV**, Code: **TS1OWNER**
10. X-tee liikmele **TS1OWNER** lisatakse alamsüsteem **Management Services.**
11. Seadistatakse haldusteenused - haldusteenuste osutajaks määratakse alamsüsteem **TS1OWNER:Management Services**

Testi lõpuks, keskserveris

* ei tohi UI kuvada ühtegi globaalset veateadet (ühe minuti jooksul peale haldusteenuste osutaja seadistamist võib UI veel globaalseid veateateid kuvada, kuna konfiguratsiooni genereerimine toimub kord minutis);
* seadistatud peab olema vähemalt üks sertifitseerimisteenus ja vähemalt üks ajatempliteenus;
* sisemine (internal) konfiguratsiooniankur peab olema alla laetud;
* **TS1OWNER** peab olema X-tee liikmete nimekirjas ja **TS1OWNER:Management Services** seadistatud haldusteenuste osutajaks.
* Haldusteenuste vaates „Management Services' Security Server” välja väärtusena kuvatakse nuppu „Register”, kuna **TS1OWNER:Management Services** pole ühegi turvaserveri omanik ega klient.

#### Veaolukorrad: keskserveri initsialiseerimine

1. Keskserveri aadressiks sisestatakse ebakorrektne DNS nimi või IP-aadress.
2. "PIN" & "Repeat PIN" väljadesse sisestatakse erinevad väärtused.

#### Veaolukorrad: liikmeklasside seadistamine

1. Lisatakse olemasolev liikmeklass, nt code: Gov (liikmeklasside koode võrreldakse tõstutundetult).
2. Liikmeklassi lisamisel jäetakse code ja/või description väli tühjaks.
3. Proovitakse kustutada liikmeklass, millesse kuulub liikmeid.

* kuidas: lisa keskserverisse X-tee liige, ürita kustutada liikmeklassi, kuhu liige kuulub. Kustuta lisatud liige.

### Teststsenaarium: Haldusteenuste turvaserveri TS1 paigaldamine ja seadistamine

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* CA

Teststsenaarium:

1. Paigaldatakse turvaserveri pakid.
2. Laetakse üles keskserverist KS1 alla laetud sisemine konfiguratsiooniankur (vt Veaolukorrad: konfiguratsiooniankru üleslaadimine).
3. Initsialiseeritakse turvaserver (vt Veaolukorrad: Turvaserveri initsialiseerimine):

* seadistatakse turvaserveri kood: **TS1**,
* turvaserveri omanik: Class: **GOV**; Code: **TS1OWNER**,
  + Kuna TS1OWNER on KSis X-tee liikmeks registreeritud, peab klassi ja koodi täitumisel automaatselt täituma nime väli; lisaks peab koodi sisestamisel töötama autocomplete.
* initsialiseeritakse tarkvaraline võtmeseade: PIN = **1234**.

1. Turvaserverisse seadistatakse **kiipkaart**.
2. Seadistatakse omaniku allkirjasertifikaat, allkirjavõti genereeritakse **kiipkaardile** (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
3. Seadistatakse (vt Abistsenaarium: Turvaserveri sertifitseerimine) ja aktiveeritakse autentimissertifikaat.
4. Seadistatakse **ajatempliteenus**.

Testi lõpuks, turvaserveris

* ei tohi turvaserveri UI kuvada ühtegi globaalset veateadet;
* turvaserveri omaniku (TS1OWNER) allkirjasertifikaat peab olema olekus: status = "registered", OCSP response = "good";
* autentimissertifikaat peab olema olekus: status = "saved", OCSP response = "";
* System Parameters vaates peab olemas olema konfiguratsiooniankur ja ajatempliteenus;
* TS1OWNER peab klientide tabelis olema olekus "saved", vastav rida peab olema kuvatud rasvases kirjas.

#### Veaolukorrad: konfiguratsiooniankru üleslaadimine

1. Proovitakse laadida üles faili, mis ei ole XML - veateade: "Configuration anchor import failed: invalid anchor file".
2. Proovitakse laadida üles XML faili, mis ei ole konfiguratsiooniankur - veateade: "Configuration anchor import failed: invalid anchor file".
3. Proovitakse laadida üles välist ankrufaili - veateade: „Configuration anchor import failed: invalid anchor file“.

#### Veaolukorrad: Turvaserveri initsialiseerimine

1. Mõni andmeväljadest jäetakse täitmata.
2. "PIN" & "Repeat PIN" väljadesse sisestatakse erinevad väärtused.

### Abistsenaarium: Turvaserveri kliendi sertifitseerimine

(kasutatakse teststsenaariumide käigus)

1. Võtmeseadmele genereeritakse võti
   * veendutakse, et võtme genereerimisel on võimalik määrata võtme *label* (vastavas seadmes). Juhul kui *label* määratakse, kuvatakse seda võtme detailandmete vaates.
   * genereeritud võti peab olema kuvatud kollasel taustal (valituna aga rohelisel taustal)
2. Võtmele genereeritakse allkirjasertifikaadi taotlus, mis salvestatakse kohalikku failisüsteemi.
   * Veendutakse, et taotluse genereerimisel on võimalik valida allkirjasertifikaate väljastavate heakskiidetud sertifitseerimisteenuse osutajate vahel.
   * Veendutakse, et taotluse genereerimisel on võimalik valida, kas taotlus genereeritakse PEM või DER formaadis.
   * Veendutakse, et peale taotluse liigi, kliendi, sertifitseerimisteenuse ja taotluse formaadi valimist ja "OK" klõpsamist kuvatakse eeltäidetud "Subject Disinguished Name" modaalaken, kus:
     + Sertifitseerimisteenuse EJBCA puhul väärtus C on X-tee eksemplari identifikaator, väärtus O on kliendi liikmeklass ja väärtus CN on kliendi liikmekood.
     + Sertifitseerimisteenuse SK KLASS 3 puhul väärtus SN on kliendi liikmekood ja väärtus CN on kliendi nimi.
   * Peale sertifikaaditaotluse genereerimist peab võti olema kuvatud valgel taustal ja võtme all peab olema kuvatud rida "Request".
3. Sertifikaaditaotlus toimetatakse heakskiidetud sertifitseerimisteenuse osutajale ning võetakse vastu sertifikaaditaotluse alusel loodud allkirjasertifikaat.
4. Allkirjasertifikaat imporditakse turvaserverisse (vt Veaolukorrad: Allkirjasertifikaadi import).

Testi lõpuks, turvaserveri „Keys and Certificates“ tabelis

* loodud võti ja imporditud sertifikaat peavad olema kuvatud valgel taustal;
* võtme kasutusvaldkonnaks peab olema "sign";
* võtme küljes peab olema allkirjasertifikaat, mille olekuks: status = "registered", OCSP response = "good".

#### Veaolukorrad: Allkirjasertifikaadi import

1. Sertifikaadi välja andnud sertifitseerimisteenust pole heakskiidetud sertifitseerimisteenuste nimekirjas.
   * kuidas v1: kustuta enne sertifikaadi importi keskserverist sertifitseerimisteenus, oota, kuni muutus jõuab turvaserverisse ja proovi sertifikaat importida, lisa sertifitseerimisteenus keskserverisse tagasi.
   * kuidas v2: tee csr'ist sertifikaat KSis kirjeldamata sertifitseerimisteenuse juures.
2. Sertifikaadi tüüp ei ole allkirjasertifikaat.
   * kuidas: tee csr-ist CAs allkirjasertifikaadi asemel autentimissertifikaat
3. Imporditavale sertifikaadile vastavat võtit ei leita.
   * kuidas: genereeri lisaks üks võti, genereeri võtmele allkirjasertifikaadi taotlus, tee taotlusest CA juures sertifikaat, kustuta lisaks genereeritud võti, proovi sertifikaati importida.
4. Süsteem ei leia süsteemist sertifikaadis viidatud isikut.
   * kuidas: genereeri lisaks üks sertifikaaditaotlus, mille DNiks sisesta turvaserveris mitteeksisteeriva kliendi andmed. Tee taotlusest sertifikaat ja proovi seda importida. Kustuta lisaks tehtud sertifikaaditaotlus.
5. Imporditav fail ei ole PEM või DER formaadis. Veateade: „Upload failed: incorrect file format. Only PEM and DER files allowed“.
6. Imporditav sertifikaat on eelnevalt süsteemi salvestatud.

### Abistsenaarium: Turvaserveri sertifitseerimine

(Kasutatakse teststsenaariumite käigus.)

1. Tarkvaralisele võtmeseadmele genereeritakse võti
2. Võtmele genereeritakse autentimissertifikaadi taotlus (vt Veaolukorrad: autentimissertifikaadi taotluse genereerimine), mis salvestatakse kohalikku failisüsteemi.
   * Veendutakse, et taotluse genereerimisel on võimalik valida kõigi heakskiidetud sertifitseerimisteenuse osutajate vahel.
   * Veendutakse, et taotluse genereerimisel on võimalik valida, kas taotlus genereeritakse PEM või DER formaadis.
   * Veendutakse, et peale taotluse liigi, sertifitseerimisteenuse ja taotluse formaadi valimist ja "OK" klõpsamist kuvatakse eeltäidetud "Subject Disinguished Name" modaalaken, kus:
     + Sertifitseerimisteenuse EJBCA puhul väärtus C on X-tee eksemplari identifikaator ja väärtus CN on turvaserveri kood.
     + Sertifitseerimisteenuse SK KLASS 3 puhul väärtus SN on kliendi liikmekood ja väärtus CN on kliendi nimi.
3. Sertifikaaditaotlus toimetatakse heakskiidetud sertifitseerimisteenuse osutajale ning võetakse vastu sertifikaaditaotluse alusel loodud autentimissertifikaat.
4. Autentimissertifikaat imporditakse turvaserverisse (vt Veaolukorrad: autentimissertifikaadi importimine).

Testi lõpuks, turvaserveri „Keys and Certificates“ tabelis

* loodud võti ja imporditud sertifikaat peavad olema kuvatud valgel taustal,
* võtme kasutusvaldkonnaks peab olema "auth";
* võtme küljes peab olema autentimissertifikaat, mille olekuks: status = "saved", OCSP response = "disabled"

#### Veaolukorrad: autentimissertifikaadi taotluse genereerimine

1. Riistvaralisele võtmele ei tohi saada autentimissertifikaadi taotlust teha.
   * kuidas: genereeri riistvaralisele võtmele võti, proovi võtmele genereerida autentimissertifikaadi taotlust - "usage" väljas ei tohi saada valida väärtust "auth". Kustuta genereeritud võti.

#### Veaolukorrad: autentimissertifikaadi importimine

1. Sertifikaadi välja andnud sertifitseerimisteenuse osutajat pole heakskiidetud sertifitseerimisteenuste nimekirjas.
2. Sertifikaadi tüüp ei ole autentimissertifikaat.
   * kuidas: tee csr-ist CAs autentimissertifikaadi asemel allkirjasertifikaat.
3. Imporditav fail ei ole PEM või DER formaadis. Veateade: „Failed to import certificate: Incorrect file format. Only PEM and DER files allowed. “.
4. Imporditav sertifikaat on eelnevalt süsteemis salvestatud.

### Teststsenaarium: Haldusteenuste turvaserveri TS1 registreerimine keskserveris

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1

Teststsenaarium:

1. Turvaserverist **TS1** esitatakse autentimissertifikaadi registreerimistaotlus.
   * keskserveris KS1 peab esitatud taotlus olema olekus "waiting"
2. Keskserveris **KS1** lisatakse liikmele **TS1OWNER** turvaserver **TS1** (autentimissertifikaadi registreerimistaotluse vormistamine) (vt Veaolukorrad: autentimissertifikaadi registreerimistaotluse vormistamine).
   * keskserveris peab esitatud taotluse ja selle kaastaotluse olekuks olema "submitted for approval"
3. Keskserveris kinnitatakse registreerimistaotlus.

Testi lõpuks:

* keskserveris peab TS1OWNER detailvaate tabis "owned servers" olema kirjas TS1;
* keskserveris peavad olemas olema "approved" olekus autentimissertifikaadi registreerimise taotlused vaadetes:
  + members -> TS1OWNER detailvaate tabis "management requests"
  + security servers -> TS1 detailvaate tabis "management requests"
  + peamenüü punktist "management requests" avanevas tabelis
* turvaserveris peab autentimissertifikaat olema olekus: status = "registered", OCSP response = "good";
* turvaserveris peab TS1OWNER olema olekus "registered".

#### Veaolukorrad: autentimissertifikaadi registreerimistaotluse vormistamine

1. Proovitakse importida allkirjastamissertifikaati. Veateade: „Failed to import authentication certificate: This certificate cannot be used for authentication.“
2. Proovitakse importida faili, mis pole PEM või DER formaadis. Veateade: „Failed to import authentication certificate: Incorrect file format. Only PEM and DER files allowed.“
3. Server code väli jäetakse tühjaks. Veateade: „Missing parameter: serverCode. “

### Teststsenaarium: Haldusteenuste seadistamine turvaserveris TS1

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1

Teststsenaarium:

1. Keskserveris lisatakse haldusteenuste osutaja **TS1OWNER:Management Services** turvaserveri kliendiks:
   * Haldusteenuste vaates klõpsatakse „Management Services' Security Server” välja väärtusena kuvatavat nuppu „Register”, sisestatakse turvaserveri TS1 andmed ja klõpsatakse "Submit".
   * Veendutakse, et keskserveris KS1 ilmub peamenüü "Management Requests" vaatesse, TS1 ja TS1OWNER "Management Requests" tab'i taotlus tüübiga "Client registration", mille "Comments" väljas sisaldub "Management service provider registration" ja status on "APPROVED".
2. Turvaserveris lisatakse alamsüsteem **TS1OWNER:Management Services** turvaserveri kliendiks.
3. Turvaserveris seadistatakse alamsüsteemile **TS1OWNER:Management Services** haldusteenused (WSDL aadressi ja teenuste aadressi saab KS1 -> System settings -> management services):
   * lisatakse ja aktiveeritakse WSDL,
   * muudetakse teenuste aadress õigeks,
   * antakse teenuste pääsuõigused globaalsele grupile "**security-server-owners**".

Testi lõpuks, turvaserveris:

* **TS1OWNER:Management Services** peab klientide tabelis olema olekus "registered".
* **TS1OWNER:Management Services** details -> services vaates peab olemas olema (mitte-"disabled"-olekus) haldusteenuste WSDL, milles sisalduvate teenuste aadress peab olema korrektselt seadistatud
* **TS1OWNER:Management Services** details -> service clients vaates peab olemas olema globaalne grupp "security-server-owners", kellele on antud pääsuõigused kõikidele haldusteenuste WSDLis sisalduvatele teenustele.

### Teststsenaarium: Turvaserveri TS2 paigaldamine, seadistamine ja registreerimine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* CA

Teststsenaarium:

1. Paigaldatakse turvaserveri pakid.
2. Turvaserver initsialiseeritakse:
   * Laetakse üles keskserverist **KS1** alla laetud sisemine konfiguratsiooniankur.
   * Seadistatakse turvaserveri kood **TS2** ja omanik class: **GOV**, code: **TS2OWNER** ning initsialiseeritakse tarkvaraline võtmeseade PIN = **1234**.
     + omaniku nime väli peab klassi ja koodi täitmisel tühjaks jääma.
     + esialgsete seadistuste esitamisel antakse hoiatus, et omanik ei ole X-tee liige.
3. Turvaserver seadistatakse kasutama **HSM**i.
4. Turvaserveris seadistatakse omaniku allkirjasertifikaat, allkirjavõti genereeritakse **HSM**ile (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine):
5. Turvaserveris seadistatakse (vt Abistsenaarium: Turvaserveri sertifitseerimine) ja aktiveeritakse autentimissertifikaat.
   * autentimissertifikaat peab olema olekus: status = "saved", OCSP response = "";
6. Turvaserverist esitatakse keskserverisse turvaserveri autentimissertifikaadi registreerimistaotlus.
   * autentimissertifikaat peab olema olekus: status = "registration in progress", OCSP response = "";
   * keskserveris peab olema üldises haldustaotluste vaates (peamenüüst management services) kuvatud esitatud autentimissertifikaadi registreerimise taotlus olekus "waiting".
7. Turvaserveris seadistatakse **ajatempliteenus**.
8. Keskserveris lisatakse turvaserveri omanik: Name: **TS2 Owner**, Class: **GOV**, Code: **TS2OWNER** X-tee liikmeks.
9. Keskserveris lisatakse **TS2OWNER'ile** turvaserver **TS2** (vormistatakse turvaserveri autentimissertifikaadi registreerimistaotlus).
   * keskserveris peab olema TS2OWNER'i ja üldises haldustaotluste vaates kuvatud lisatud autentimissertifikaadi taotlus ja selle kaastaotlus olekus "submitted for approval".
10. Keskserveris kinnitatakse registreerimistaotlused.

Testi lõpuks:

* turvaserveri UI ei tohi kuvada ühtegi globaalset veateadet;
* turvaserveri omaniku allkirjasertifikaat peab olema olekus: status = "registered", OCSP response = "good";
* turvaserveri autentimissertifikaat peab olema olekus: status = "registered", OCSP response = "good";
* turvaserveri System Parameters vaates peab olemas olema konfiguratsiooniankur ja ajatempliteenus;
* turvaserveris peab klientide tabelis TS2OWNER olema olekus "registered", vastav rida peab olema kuvatud rasvases kirjas.
* keskserveris peab TS2OWNER detailvaate tabis "owned servers" olema olemas TS2.

### Abistsenaarium: Pääsuõiguse andmine teenuse vaatest

(Kasutatakse teststsenaariumite käigus.)

1. Turvaserveri klientide vaates vali klient ja ava kliendi teenuste (Services) vaade. Vali teenus ja klõpsa "Access Rights".
   * avanevas tabelis peavad olema kuvatud kõik teenuse pääsuõigust omavad subjektid.
2. Klõpsa "Add Subjects" ja tee tühi otsing (klõpsa "Search" ilma otsinguparameetreid sisestamata)
   * avanevas tabelis peavad olema kuvatud kõik X-tee keskserveris registreeritud alamsüsteemid ja globaalsed grupid ning antud kliendi lokaalsed grupid. Subjektid, millele on valitud teenuse pääsuõigus antud, peavad olema kuvatud hallis kirjas ja neid ei tohi saada valida.
3. Lisa pääsuõigus:
   * osadele kuvatud subjektidele valides tabelist rea(d) ja klõpsates "Add Selected to ACL" või
   * kõikidele kuvatud subjektidele, klõpsates "Add All to ACL".
4. Veendu, et teenuse ACL nimekirja on lisandunud (ainult) need subjektid, kellele andsid pääsuõiguse.

### Abistsenaarium: Pääsuõiguse andmine teenuse kliendi vaatest

(Kasutatakse teststsenaariumite käigus.)

#### Pääsuõiguse lisamine uuele teenuse kliendile

1. Turvaserveri klientide vaates vali klient (teenusepakkuja) ja ava kliendi teenuste klientide (Service Clients) vaade.
2. Lisa uus teenuste klient ("Add") ja tee tühi otsing (klõpsa "Search" ilma otsinguparameetreid sisestamata)
   * avanevas tabelis peavad olema kuvatud kõik X-tee keskserveris registreeritud alamsüsteemid ja globaalsed grupid ning antud kliendi lokaalsed grupid. Subjektid, mis on juba antud teenusepakkuja teenuste kliendid, peavad olema kuvatud hallis kirjas ja neid ei tohi saada valida.
3. Mine teenuste kliendi pääsuõiguste lehele ("Next") ja lisa uuele teenuste kliendile pääsuõigused:
   * osadele kuvatud teenustele, valides tabelist rea(d) ja klõpsates "Add Selected to ACL" või
   * kõikidele kuvatud teenustele, klõpsates "Add All to ACL".
4. Veendu, et teenuse kliendi ACL nimekirja on lisandunud (ainult) need teenused, millele andsid pääsuõiguse.

#### Pääsuõiguse lisamine olemasolevale teenuse kliendile

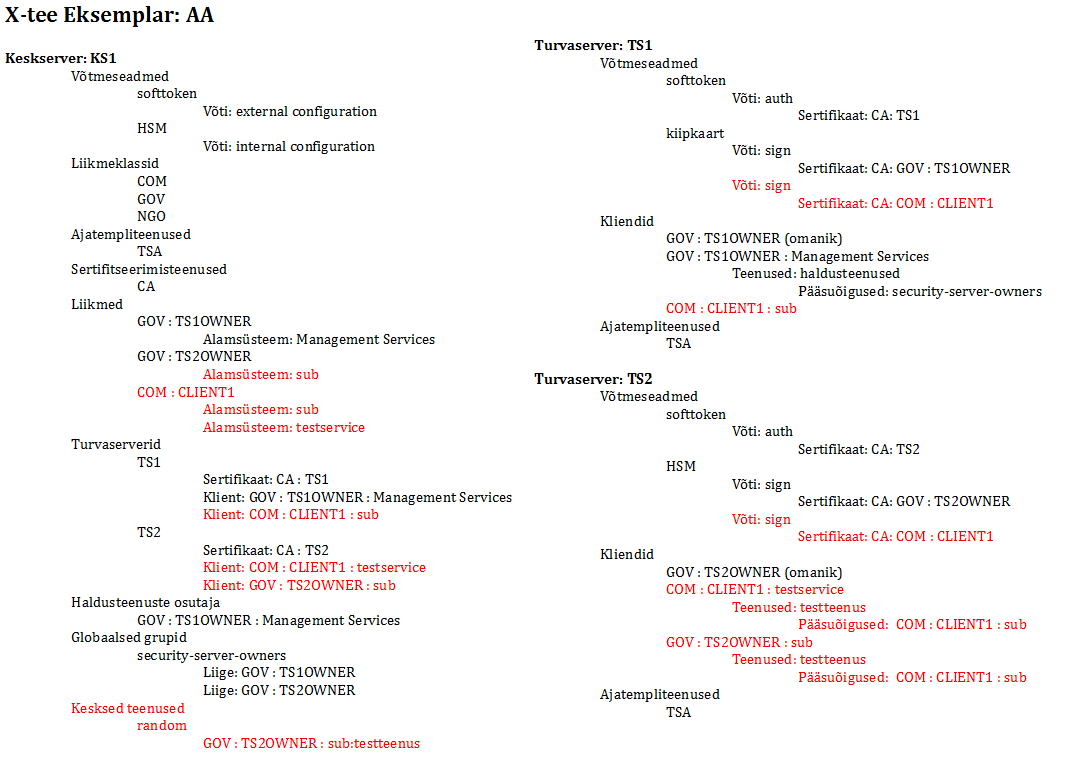
1. Turvaserveri klientide vaates vali klient (teenusepakkuja) ja ava kliendi teenuste klientide (Service Clients) vaade.
   * avanevas tabelis peavad olema kuvatud kõik antud kliendi teenuste pääsuõigusi omavad subjektid.
2. Ava teenuse kliendi pääsuõiguste vaade ("Acces Rights")
   * avanevas tabelis peavad olema kuvatud kõik teenusepakkuja teenused, mis on avatud valitud teenuse kliendile.
3. Vali kliendile teenuste lisamine("Add Services")
   * avanevas tabelis peavad olema kuvatud kõik teenusepakkuja teenused. Teenused, mille pääsuõigus on valitud teenuste kliendile eelnevalt antud, peavad olema kuvatud hallis kirjas ja neid ei tohi saada valida.
4. Lisa teenuse pääsuõigus:
   * osadele kuvatud teenustele, valides tabelist rea(d) ja klõpsates "Add Selected to ACL" või
   * kõikidele kuvatud teenustele, klõpsates "Add All to ACL".
5. Veendu, et teenuse kliendi ACL nimekirja on lisandunud (ainult) need teenused, millele andsid pääsuõiguse.

## Turvaserveri klientide ja teenuste haldus

Peatükis testitakse X-tee tavakasutust:

* klientide lisamist turvaserveritesse;
* teenuste, sh kesksete teenuste seadistamist ja kasutamist;
* alamsüsteemide sõltumatust teenuste kasutamise ja osutamise osas;
* pääsuõiguste haldust X-tee liikmete alamsüsteemide ja gruppide osas;
* sertifikaatide haldust.

Süsteemi seadistus selle peatüki testide lõpuks (muutused punasega):



### Teststsenaarium: Klientide registreerimine turvaserveritesse

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1
* Turvaserver TS2
* CA

Teststsenaarium:

1. Keskserveris lisatakse liige: Name: **Client One**; Class: **COM**; Code: **CLIENT1**
2. Turvaserveris **TS1** lisatakse kliendiks **CLIENT1** **alamsüsteem "sub"**, otsides CLIENT1 globaalsest nimekirjast ja kirjutades alamsüsteemi koodi käsitsi juurde. Turvaserverist saadetakse keskserverisse kliendi registreerimistaotlus.
   * lisatud klient peab klientide nimekirja ilmuma olekus "registration in progress";
   * taotluse saatmisel hoiatatakse kasutajat, et liikmele CLIENT1 registreeritakse uus alamsüsteem "sub";
   * keskserveris peab lisatud taotlus ilmuma turvaserveri, liikme ja üldisesse haldustaotluste nimekirja olekus "waiting".
3. Turvaserveris **TS1** sertifitseeritakse **CLIENT1** (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine).
4. Keskserveris vormistatakse liikme **CLIENT1 alamsüsteemi "sub"** turvaserveri **TS1** kliendiks registreerimise taotlus, alustades liikme detailandmetest: Members -> Used Servers -> Add.
   * keskserveris peavad kliendi registreerimise kaastaotlused olema turvaserveri, liikme ja üldises haldustaotluste nimekirjas olekus "submitted for approval".
5. Keskserveris kinnitatakse lisatud registreerimistaotlused.
6. Turvaserveris **TS2** lisatakse kliendiks **CLIENT1** alamsüsteem **"testservice"**, sisestades kliendi lisamise vaates kliendi andmed käsitsi. Turvaserverist saadetakse keskserverisse kliendi registreerimistaotlus.
   * andmete käsitsi lisamisel peab kliendi nimi täituma automaatselt liikmeklassi ja -koodi sisestamisel;
   * lisatud klient peab klientide nimekirja ilmuma olekus "registration in progress";
   * taotluse saatmisel hoiatatakse kasutajat, et liikmele CLIENT1 registreeritakse uus alamsüsteem "testservice";
   * keskserveris peab lisatud taotlus ilmuma turvaserveri, liikme ja üldisesse haldustaotluste nimekirja olekus "waiting".
7. Turvaserveris **TS2** sertifitseeritakse **CLIENT1** (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine).
8. Keskserveris vormistatakse liikme **CLIENT1 alamsüsteemi "testservice"** turvaserveri **TS2** kliendiks registreerimise taotlus, alustades serveri detailandmetest: Security Servers -> Clients -> Add.
   * keskserveris peavad kliendi registreerimise kaastaotlused olema turvaserveri, liikme ja üldises haldustaotluste nimekirjas olekus "submitted for approval".
9. Keskserveris kinnitatakse lisatud registreerimistaotlused.
10. Turvaserveris **TS2** lisatakse kliendiks **TS2OWNER alamsüsteem "sub"**. Turvaserverist saadetakse keskserverisse kliendi registreerimistaotlus.
    * lisatud klient peab klientide nimekirja ilmuma olekus "registration in progress";
    * taotluse saatmisel hoiatatakse kasutajat, et liikmele TS2OWNER registreeritakse uus alamsüsteem "sub";
    * keskserveris peab lisatud taotlus ilmuma turvaserveri, liikme ja üldisesse haldustaotluste nimekirja olekus "waiting".
11. Keskserveris vormistatakse liikme **TS2OWNER alamsüsteemi "sub"** turvaserveri **TS2** kliendiks registreerimise taotlus.
    * keskserveris peavad kliendi registreerimise kaastaotlused olema turvaserveri, liikme ja üldises haldustaotluste nimekirjas olekus "submitted for approval".
12. Keskserveris kinnitatakse lisatud registreerimistaotlused.

Testi lõpuks:

* Keskserveris peab liikmete nimekirjas olemas olema CLIENT1 ja tema detailandmete tabis "subsystems" peab kuvatama alamsüsteemi "sub" seotuna turvaserveriga TS1 ja alamsüsteemi "testservice" seotuna turvaserveriga TS2.
* Keskserveris peab turvaserveri TS1 detailandmete "Clients" tabis kuvatama kahte klienti: CLIENT1:sub ja TS1OWNER:Management Services.
* Keskserveris peab turvaserveri TS2 detailandmete "Clients" tabis kuvatama kahte klienti: CLIENT1:testservice ja TS2OWNER:sub.
* Keskserveris peavad CLIENT1, TS2OWNER, TS1, TS2 ja üldises haldustaotluste nimekirjas olema kliendi registreerimistaotlused olekus "approved".
* Turvaserveris TS1 peab klientide nimekirjas olemas olema CLIENT1:sub, olekus "registered".
* Turvaserveris TS1 peab võtmete ja sertifikaatide tabelis olemas olema CLIENT1 sertifikaat olekus status: "registered", OCSP response: "good".
* Turvaserveris TS2 peavad klientide nimekirjas olemas olema CLIENT1:testservice ja TS2OWNER:sub, olekus "registered".
* Turvaserveris TS2 peab võtmete ja sertifikaatide tabelis olemas olema CLIENT1 sertifikaat olekus status: "registered", OCSP response: "good".

### Teststsenaarium: Test-teenuse seadistamine

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Test-teenus (test-teenuse WSDL ja POST aadress)

Teststsenaarium:

1. Turvaserveri **TS2** kliendile **CLIENT1:testservice** lisatakse test-teenuse WSDL (vt Veaolukorrad: WSDL lisamine ja Veaolukorrad: WSDLi aadressi muutmine).
   * WSDL peab ilmuma tabelisse inaktiivses olekus - WSDLi rida peab olema kuvatud punases kirjas ja algama: "WSDL DISABLED".
2. Seadistatakse test-teenuse parameetrid (vt Veaolukorrad: teenuse parameetrite seadistamine).

* test-teenuse aadressile peab lisama parameetri db, mille väärtuseks on kliendi liikmekood, nt http://iks2-testhost:8080/testservice-0.1/xroad?db=CLIENT1 .

1. Seadistatakse test-teenuse pääsuõigused (vt Abistsenaarium: Pääsuõiguse andmine teenuse vaatest) - pääsuõigus antakse kliendile **CLIENT1:sub.**
2. Test-teenuse WSDL aktiveeritakse.

Testi lõpuks:

* Turvaserveris TS2 kliendi CLIENT1:testservice detailandmete tab'is "Service Clients" peab olemas olema klient CLIENT1:sub, kelle ACLis peab sisalduma test-teenus.

#### Veaolukorrad: WSDL lisamine

1. Proovitakse lisada WSDL aadressiga, mis ei ole korrektne URL.
2. Proovitakse lisada WSDL aadressiga, mis ei viita WSDLile.
3. Proovitakse lisada WSDL aadress, milline on juba lisatud.
4. Proovitakse lisada WSDL, milles sisalduv teenus on eelnevalt turvaserverisse laetud WSDLis kirjeldatud.
5. Proovitakse lisada WSDL, mis annab valideerimisel vea. Kuvatakse veateade "Failed to add WSDL: WSDL validation failed" ning validaatori väljund.
   * Valideerimisel antavad hoiatused ja vead on konfigureeritavad failis */usr/share/xroad/wsdlvalidator/etc/xroad6.properties*.
6. Proovitakse lisada WSDL, mis annab valideerimisel hoiatuse. Kuvatakse validaatori väljundit sisaldav hoiatus.

#### Veaolukorrad: WSDLi aadressi muutmine

1. WSDLi aadressiks sisestatakse WSDLi aadress, mis annab valideerimisel vea. Kuvatakse veateade "Failed to edit WSDL: WSDL validation failed" ning validaatori väljund.
2. WSDLi aadressiks sisestatakse WSDLi aadress, mis annab valideerimisel hoiatuse. Kuvatakse validaatori väljundit sisaldav hoiatus.

#### Veaolukorrad: teenuse parameetrite seadistamine

1. Teenuse aadress ei ole korrektne URL. Veateade: „Invalid URL format, must begin with 'http' or 'https' “.
2. Päringu maksimaalseks kestuseks sisestatakse väärtus, mis ei ole positiivne täisarv. Veateade: „Timeout value must be a positive integer.“
3. Päringu maksimaalseks kestuseks sisestatakse 0. Kuvatakse hoiatus: „A timeout value of zero is interpreted as an infinite timeout.“

### Teststsenaarium: Test-teenuse kasutamine

Testi käigus kasutatavad ressursid:

* Testklient

Teststsenaarium:

1. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu test-teenusele - päring peab õnnestuma.
2. Turvaserveri TS2 klient **CLIENT1:testservice** teeb päringu test-teenusele - päring peab ebaõnnestuma teatega "Request is not allowed".
3. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu test-teenusele ilma userId päiseväljata - päring peab õnnestuma.

**kuidas:** päringu võiks teha curliga või SOAPUIga, andes ette eelnevalt koostatud päringut sisaldava XML faili:

curl -v -d @<PÄRINGUT\_SISALDAVA\_FAILI\_NIMI>.xml -o <VASTUST\_SISALDAVA\_FAILI\_NIMI>.xml -H "Content-type: text/xml; charset=UTF-8" http://<TS1\_AADRESS>/cgi-bin/consumer\_proxy

xroadGetRandom (testteenus) päring:

<?xml version="1.0" encoding="UTF-8"?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xroad="http://x-road.eu/xsd/xroad.xsd" xmlns:id="http://x-road.eu/xsd/identifiers">

<SOAP-ENV:Header>

<xroad:client id:objectType="MEMBER">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>sub</id:subsystemCode>

</xroad:client>

<xroad:service id:objectType="SERVICE">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>testservice</id:subsystemCode>

<id:serviceCode>xroadGetRandom</id:serviceCode>

<id:serviceVersion>v1</id:serviceVersion>

</xroad:service>

<xroad:id>c60b7e66-1dc8-4203-a3c1-3235661f6a84</xroad:id>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<ns1:xroadGetRandom xmlns:ns1="http://consumer.ee.x-rd.net">

<request>

<seed>100</seed>

</request>

</ns1:xroadGetRandom>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

### Test-teenuse kasutamine MTOM ja swaRef manustega

Testi käigus kasutatavad ressursid:

* Testteenus
* MTOM ja swaRef manustega päringuid on mugav teha, kasutades SOAPUI tarkvara

#### Teststsenaarium: MTOM manusega päringu tegemine

1. SOAPUIs luuakse uus "SOAP Project" ning imporditakse test-teenuse WSDL.
2. Päring seadistatakse turvaserveri TS1 kliendi CLIENT1:sub päringuna testteenusele (xroadGetRandom päringu näidet vaata nt Teststsenaarium: Test-teenuse kasutamine).
3. Päringule lisatakse manus (attachment).
4. *Request Properties* nimekirjas määratakse parameetrite *Enable MTOM* ja *Force MTOM* väärtuseks *true*.
5. Tehakse SOAPUId kasutades turvaserveri TS1 kliendiga **CLIENT1:sub** päring test-teenusele. Päring peab õnnestuma.
6. Veendutakse päringu andmeid vaadates (päringu *Raw* vaade SOAPUIs), et *Content-Type* väärtus on *"application/xop+xml"*. Näiteks: Content-Type: multipart/related; type="application/xop+xml"; start="<rootpart@soapui.org>"; start-info="text/xml"; boundary="----=\_Part\_16\_22011978.1445589910549"

#### Teststsenaarium: swaRef manusega päringu tegemine

1. Test-teenuste WSDLi päisesse lisatakse nimeruum: xmlns:swi="<http://ws-i.org/profiles/basic/1.1/xsd>"
2. Test-teenuste WSDLi teenuse xroadGetRandom sisendparameetri *seed* järele lisatakse swaRef element XXX. Näide vastavast WSDLi lõigust:

<xsd:element name="seed"

type="xsd:decimal">

<xsd:annotation>

<xsd:appinfo>

<xrd:title>Random input

</xrd:title>

</xsd:appinfo>

</xsd:annotation>

</xsd:element>

<xsd:element name="XXX" type="swi:swaRef"/>

1. SOAPUIs luuakse uus "SOAP Project" ning imporditakse muudetud test-teenuse WSDL. Seejuures lastakse SOAPUIl genereerida näidispäringud (linnutatakse "*Create sample requests for all operations?"*).
2. Päring seadistatakse turvaserveri TS1 kliendi CLIENT1:sub päringuna testteenusele xroadGetRandom. Näidispäring (parameetri XXX cid väärtust ei muudeta, see peab vastama cid väärtusele, mis SOAPUI genereeritud näidispäringus xroadGetRandom teenusele tekkis):

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xroad="http://x-road.eu/xsd/xroad.xsd" xmlns:id="http://x-road.eu/xsd/identifiers">

<SOAP-ENV:Header>

<xroad:client id:objectType="MEMBER">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>sub</id:subsystemCode>

</xroad:client>

<xroad:service id:objectType="SERVICE">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>testservice</id:subsystemCode>

<id:serviceCode>xroadGetRandom</id:serviceCode>

<id:serviceVersion>v1</id:serviceVersion>

</xroad:service>

<xroad:id>45</xroad:id>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<xroad:xroadGetRandom>

<xroad:request>

<xroad:seed>8</xroad:seed>

<xroad:XXX>cid:775797073252</xroad:XXX>

</xroad:request>

</xroad:xroadGetRandom>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

1. Päringule lisatakse manus (attachment). Manuse *Part* parameetriks määratakse elemendi XXX *cid*-väärtus (see variant peab ilmuma manuse *Part* parameetri valikute hulka).
2. Tehakse SOAPUId kasutades turvaserveri TS1 kliendiga **CLIENT1:sub** päring test-teenusele. Päring peab õnnestuma.
3. Veendutakse, et päringu manuse tüübiks on SOAPUIs märgitud SWAREF.

### Teststsenaarium: WSDL värskendamine

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Test-teenus (WSDL, mis sisaldab teenuseid xroadGetRandom ja bodyMassIndex)
* Testklient

Teststsenaarium:

1. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu test-teenusele bodyMassIndex - päring peab õnnestuma.
2. Test-teenuse WSDList kustutatakse teenus bodyMassIndex ning värskendatakse turvaserveris WSDL (vt Veaolukorrad: WSDLi värskendamine).
   * Kasutajaliides peab värskendamisel teavitama kustunud teenustest.
   * kuidas:
     + v1: kommenteeri test-teenuse WSDList bodyMassIndex välja või
     + v2: asenda test-teenuse WSDL ainult xroadGetRandomit sisaldava WSDLiga
3. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu test-teenusele bodyMassIndex - päring peab ebaõnnestuma.
4. Test-teenuse WSDLile lisatakse teenus bodyMassIndex ning värskendatakse turvaserveris WSDL.
   * Kasutajaliides peab teavitama lisandunud teenustest.
   * kuidas:
     + v1: eemalda test-teenuse WSDList bodyMassIndex väljakommenteerimine või
     + v2: asenda ainult xroadGetRandomit sisaldav WSDL mõlemat teenust sisaldava WSDLiga.
   * WSDL värskendamisel ei tohi teenuste seaded muutuda (nt aadress ei tohi värskendamisel saada vaikeväärtusega üle kirjutatud).
5. Seadista teenuse bodyMassIndex aadress ja pääsuõigused (pääsuõigus anna kliendile CLIENT1:sub).
6. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu test-teenustele bodyMassIndex ja xroadGetRandom - päringud peavad õnnestuma.

#### Veaolukorrad: WSDLi värskendamine

1. Test-teenuse WSDL asendatatakse WSDLiga, mis annab valideerimisel vea ning värskendatakse turvaserveris WSDL. Kuvatakse veateade "Failed to refresh WSDL(s): WSDL validation failed" ning validaatori väljund.
2. Test-teenuse WSDL asendatatakse WSDLiga, mis annab valideerimisel hoiatuse ning värskendatakse turvaserveris WSDL. Kuvatakse validaatori väljundit sisaldav hoiatus.
   * Valideerimisel antavad hoiatused ja vead on konfigureeritavad failis */usr/share/xroad/wsdlvalidator/etc/xroad6.properties*.

### Teststsenaarium: WSDLi inaktiveerimine

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu testteenusele - päring peab õnnestuma.
2. Turvaserveris **TS2** inaktiveeritakse testteenuse WSDL ning sisestatakse klientidele edastatav veateade.
   * inaktiveeritud WSDLi rida peab olema kuvatud punases kirjas algusega "WSDL DISABLED"
3. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu testteenusele - päring peab ebaõnnestuma WSDL inaktiveerimisel sisestatud veateatega.
4. Turvaserveris aktiveeritakse testteenuse WSDL
   * aktiivse WSDLi rida peab olema kuvatud mustas kirjas ilma märketa "DISABLED"
5. Turvaserveri TS1 klient **CLIENT1:sub** teeb päringu testteenusele - päring peab õnnestuma.

### Teststsenaarium: TLS kasutamine sisevõrgus

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* Turvaserver TS2
* Testklient
* Test-teenus

Teststsenaarium:

1. Turvaserveris **TS1** genereeritakse uus sisemine TLS võti (System Parameters -> Internal TLS Certificate) ja eksporditakse sertifikaat.
2. Turvaserveris **TS1** seadistatakse kliendi **CLIENT1:sub** ühenduseks HTTPS\_ NO\_AUTH (Security Server Clients -> Internal Servers).
3. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele - päring peab ebaõnnestuma.
4. **Testklient** seadistatakse kasutama HTTPS ühendust. Selleks:

* märgista testkliendis märkeruut „Use SSL“,
* lae alla kliendi sertifikaat,
* lae testklienti üles turvaserverist TS1 alla laetud sertifikaat.

1. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele - päring peab õnnestuma.
2. Turvaserveris **TS1** seadistatakse kliendi **CLIENT1:sub** ühenduseks HTTPS.
3. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele - päring peab ebaõnnestuma.
4. Turvaserverisse TS1 kliendile **CLIENT1:sub** laetakse üles testkliendist alla laetud sertifikaat (Security Server Clients -> Internal Servers).
5. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab õnnestuma.
6. **Testklienti** laetakse turvaserveri **TS2** TLS sertifikaat.
7. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab ebaõnnestuma.
8. **Testklienti** laetakse turvaserveri **TS1** TLS sertifkaat.
9. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab õnnestuma.
10. Turvaserveri **TS2** testteenus konfigureeritakse HTTPS URLile. Teenuse TLS sertifikaadi kontroll on välja lülitatud.
11. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab õnnestuma.
12. Turvaserveris **TS2** konfigureeritakse testteenusele TLS sertifikaadi kontroll.
13. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab ebaõnnestuma.
14. Turvaserverisse **TS2** imporditakse **testteenuse** TLS sertifikaat.
15. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Kesksete teenuste seadistamine ja kasutamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1 (curl päringud)
* Turvaserver TS2

Teststsenaarium:

1. Keskserveris KS1 defineeritakse keskne teenus **random**: code = **xroadGetRandom**; version = **v1**; provider = **SUBSYSTEM:AA:COM:CLIENT1:testservice**.
2. Turvaserveri TS1 klient CLIENT1:sub teeb päringu testteenusele - päring peab õnnestuma.
3. Turvaserveri TS1 klient CLIENT1:sub teeb päringu **kesksele** teenusele - päring peab õnnestuma.
4. Testteenus konfigureeritakse turvaserveri **TS2** kliendile **TS2OWNER:sub** (sarnaselt Teststsenaarium: Test-teenuse seadistamine).
5. Keskserveris muudetakse keskse teenuse **random** osutajaks **SUBSYSTEM:AA:GOV:TS2OWNER:sub**
6. Turvaserveri TS1 klient CLIENT1:sub teeb päringu kesksele teenusele - päring peab õnnestuma.

**kuidas:** päringuid võiks teha curliga, andes ette eelnevalt koostatud päringut sisaldava XML faili:

curl -v -d @<PÄRINGUT\_SISALDAVA\_FAILI\_NIMI>.xml -o <VASTUST\_SISALDAVA\_FAILI\_NIMI>.xml -H "Content-type: text/xml; charset=UTF-8" http://<TS1\_AADRESS>/cgi-bin/consumer\_proxy

xroadGetRandom (testteenus) päring:

<?xml version="1.0" encoding="UTF-8"?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xroad="http://x-road.eu/xsd/xroad.xsd" xmlns:id="http://x-road.eu/xsd/identifiers">

<SOAP-ENV:Header>

<xroad:client id:objectType="MEMBER">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>sub</id:subsystemCode>

</xroad:client>

<xroad:service id:objectType="SERVICE">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>testservice</id:subsystemCode>

<id:serviceCode>xroadGetRandom</id:serviceCode>

<id:serviceVersion>v1</id:serviceVersion>

</xroad:service>

<xroad:userId>EE37702211234</xroad:userId>

<xroad:id>c60b7e66-1dc8-4203-a3c1-3235661f6a84</xroad:id>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<ns1:xroadGetRandom xmlns:ns1="http://consumer.ee.x-rd.net">

<request>

<seed>100</seed>

</request>

</ns1:xroadGetRandom>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

keskse teenuse päring:

<?xml version="1.0" encoding="UTF-8"?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xroad="http://x-road.eu/xsd/xroad.xsd" xmlns:id="http://x-road.eu/xsd/identifiers">

<SOAP-ENV:Header>

<xroad:client id:objectType="MEMBER">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>sub</id:subsystemCode>

</xroad:client>

<xroad:centralService id:objectType="CENTRALSERVICE">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:serviceCode>random</id:serviceCode>

</xroad:centralService>

<xroad:userId>EE37702211234</xroad:userId>

<xroad:id>799393c3-7f89-42f5-b9ae-213d1ff39491</xroad:id>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<ns1:xroadGetRandom xmlns:ns1="http://consumer.ee.x-rd.net">

<request>

<seed>100</seed>

</request>

</ns1:xroadGetRandom>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

### Teststsenaarium: Pääsuõiguse andmine X-tee liikmele.

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Turvaserverist TS2 tehakse kliendiga TS2OWNER:sub päring testteenusele. Päring peab ebaõnnestuma veateatega: "Request is not allowed".
2. Testteenuse pääsuõigus antakse kliendile TS2OWNER:sub (vt Abistsenaarium: Pääsuõiguse andmine teenuse vaatest)
3. Turvaserverist TS2 tehakse kliendiga TS2OWNER:sub päring testteenusele. Päring peab õnnestuma.
4. Testteenuselt eemaldatakse TS2OWNER:sub pääsuõigused.

### Teststsenaarium: Pääsuõiguse andmine globaalsele grupile

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserveris KS1 lisatakse globaalne grupp **GLOB1** (vt Veaolukorrad: Globaalse grupi loomine).
2. Turvaserveris TS2 antakse testteenuse pääsuõigus globaalsele grupile **GLOB1** (vt Abistsenaarium: Pääsuõiguse andmine teenuse vaatest).
3. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring testteenusele. Päring peab ebaõnnestuma veateatega: "Request is not allowed".
4. Keskserveris KS1 lisatakse **TS2OWNER:sub** globaalsesse gruppi **GLOB1**.
   * TS2OWNER detailvaate tab'is "Global Group Membership" peab olema kuvatud 2 gruppi: security-server-owners ja GLOB1.
5. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring **testteenusele**. Päring peab õnnestuma.
6. Keskserverist kustutatakse globaalne grupp GLOB1.
7. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring testteenusele. Päring peab ebaõnnestuma veateatega: "Request is not allowed"
8. Testteenuse pääsuõigus võetakse globaalselt grupilt **GLOB1.**

* **Teada ikaldus**: keskserverist globaalse grupi kustutamisel ei anta sellest teada turvaserveri omanikule, kelle teenustele on antud kustutatud grupi pääsuõigus. Võiks laheneda notify-ga.

#### Veaolukorrad: Globaalse grupi loomine

1. Proovitakse lisada globaalne grupp, mis juba eksisteerib (nt koodiga "security-server-owners"). Grupi lisamine peab ebaõnnestuma.
2. Grupi lisamisel jäetakse tühjaks "Code" ja/või "Description" väli. Grupi lisamine peab ebaõnnestuma.

### Teststsenaarium: Pääsuõiguse andmine lokaalsele grupile.

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Turvaserveris TS2 lisatakse kliendile **CLIENT1:testservice** lokaalne grupp **LOK1** (vt Veaolukorrad: Lokaalse grupi loomine).
2. **Testteenuse pääsuõigus** antakse lokaalsele grupile **LOK1** (vt Abistsenaarium: Pääsuõiguse andmine teenuse vaatest).
   * LOK1 peab ilmuma testteenuse osutaja teenuste klientide nimekirja.
3. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring testteenusele. Päring peab ebaõnnestuma veateatega: "Request is not allowed"
4. Turvaserveris TS2 lisatakse **TS2OWNER:sub** lokaalsesse gruppi **LOK1**.
5. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring testteenusele. Päring peab õnnestuma.
6. Turvaserveris TS2 **kustutatakse** lokaalne grupp LOK1.
   * Grupi kustutamisel peab grupp kustuma ka testteenuse pääsuõiguste nimekirjast ja teenuse klientide nimekirjast.
7. Turvaserverist TS2 tehakse kliendiga **TS2OWNER:sub** päring testteenusele. Päring peab ebaõnnestuma veateatega: "Request is not allowed".

#### Veaolukorrad: Lokaalse grupi loomine

1. Proovitakse lisada lokaalne grupp, mis juba eksisteerib. Grupi lisamine peab ebaõnnestuma.
2. Grupi lisamisel jäetakse tühjaks "Code" ja/või "Description" väli. Grupi lisamine peab ebaõnnestuma.

### Teststsenaarium: Sertifikaatide aktiveerimine ja inaktiveerimine

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* Turvaserver TS2
* Testklient

#### Autentimissertifikaadi aktiveerimine ja inaktiveerimine

1. Inaktiveeri turvaserveris TS1 autentimissertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab lõppema veaga: "Security server has no valid authentication certificate."
   * **Teada ikaldus**: turvaserverites puhverdatakse TLS sessioon ja kasutatavad sertifikaadid, sertifikaadi inaktiveerimine rakendub alles sessiooni aegumisel (~5 min). Sessiooni koheseks lõpetamiseks võib TS1 sisestada käsu: "sudo service xroad-proxy restart". Ikaldust parandab tulevikus notify süsteem.
   * Peale sertifikaadi inaktiveerimist kuvatakse sertifikaadi real veerus "OCSP response" olekut "disabled".
2. Aktiveeri turvaserveris TS1 autentimissertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
   * Mõned sekundid peale sertifikaadi aktiveerimist võivad päringud endiselt ebaõnnestuda, kuna turvaserver kontrollib sertifikaadi OCSP vastust.
3. Inaktiveeri turvaserveris TS2 autentimissertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab lõppema veaga: "Service provider did not send correct authentication certificate."
   * **Teada ikaldus**: turvaserverites puhverdatakse TLS sessioon ja kasutatavad sertifikaadid, sertifikaadi inaktiveerimine rakendub alles sessiooni aegumisel (~5 min). Sessiooni koheseks lõpetamiseks võib TS2 sisestada käsu: "sudo service xroad-proxy restart". Ikaldust parandab tulevikus notify süsteem.
   * Peale sertifikaadi inaktiveerimist kuvatakse sertifikaadi real veerus "OCSP response" olekut "disabled".
4. Aktiveeri turvaserveris TS2 autentimissertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
   * Mõned sekundid peale sertifikaadi aktiveerimist võivad päringud endiselt ebaõnnestuda, kuna turvaserver kontrollib sertifikaadi OCSP vastust.

#### Allkirjastamissertifikaadi aktiveerimine ja inaktiveerimine

1. Inaktiveeri turvaserveris TS2 kliendi CLIENT1 allkirjasertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab lõppema veateatega: "Failed to get signing info for member 'SUBSYSTEM:AA/COM/CLIENT1/testservice': Signer.UnknownMember: Could not find any certificates for member 'SUBSYSTEM:AA/COM/CLIENT1/testservice'".
   * **Teada ikaldus**: turvaserverites puhverdatakse TLS sessioon ja kasutatavad sertifikaadid, sertifikaadi inaktiveerimine rakendub alles sessiooni aegumisel (~5 min). Sessiooni koheseks lõpetamiseks võib TS2 sisestada käsu: "sudo service xroad-proxy restart". Ikaldust parandab tulevikus notify süsteem.
   * Peale sertifikaadi inaktiveerimist kuvatakse sertifikaadi real veerus "OCSP response" olekut "disabled".
2. Aktiveeri turvaserveris TS2 kliendi CLIENT1 allkirjasertifikaat. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
   * Mõned sekundid peale sertifikaadi aktiveerimist võivad päringud ebaõnnestuda veateatega "Failed to get signing info for member 'SUBSYSTEM:AA/COM/CLIENT1/testservice': Signer.InternalError: Member 'SUBSYSTEM:AA/COM/CLIENT1/testservice' has no suitable certificates", kuna turvaserver kontrollib sertifikaadi OCSP vastust.

### Teststsenaarium: Võtmevahetus turvaserveris

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Testklient
* CA

#### Allkirjavõtme vahetus

1. Tee turvaserveris **TS2** **CLIENT1**-le uus allkirjavõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
2. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
3. Kustuta vana allkirjavõti.
   * võtme kustutamisel kustutatakse ka sellega seotud sertifikaadid turvaserveri konfiguratsioonist.
   * võti jääb peale kustutamist alles seadmele - UIs kuvatakse võti kollasel taustal. Võtme seadmelt kustutamiseks vali võti ja vajuta uuesti "Delete".
4. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

#### Autentimisvõtme vahetus

1. Tee turvaserveris **TS2** uus autentimisvõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri sertifitseerimine)
2. Registreeri autentimissertifikaat keskserveris KS1 - selleks:
   * saada turvaserverist registreerimistaotlus,
   * vormista keskserveris vastav kaastaotlus (security servers -> details -> authentication certificates -> add) ja
   * kinnita taotlused.
3. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
4. Kui uue autentimisvõtme olekuks turvaserveris on saanud "registered", aktiveeri uus autentimisvõti ja kustuta vana autentimisvõti.
   * võtme kustutamisel kustutatakse ka sellega seotud sertifikaadid turvaserveri konfiguratsioonist.
   * võti jääb peale kustutamist alles seadmele - UIs kuvatakse võti kollasel taustal. Võtme seadmelt kustutamiseks vali võti ja vajuta uuesti "Delete".
5. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Sertifikaatide OCSP vastused

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Testklient
* CA

#### Allkirjasertifikaadi tühistamine

1. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. (selle sammuga veendutakse, et turvaserver on ühenduseks puhverdanud esimese sertifikaadi)
2. Tee turvaserveris **TS2** kliendile **CLIENT1** teine allkirjastamisvõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
3. Tühista **CA**s turvaserveri **TS2** kliendi **CLIENT1** esimene allkirjasertifikaat.
   * sertifikaadi tühistamisel peab OCSP response olekuks saama "revoked“.
   * Kuna turvaserver puhverdab OCSP vastuseid, võib oleku muutus võtta aega. OCSP vastuste võtmise intervalli saab muuta, sisestades keskserveri andmebaasi tabelisse *system\_parameters* süsteemse parameetri *ocspFreshnessSeconds* soovitud väärtusega. Parameetri *ocspFreshnessSeconds* vaikimisi väärtus on 3600.
4. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
5. Tühista **CA**s turvaserveri **TS2** kliendi **CLIENT1** teine allkirjasertifikaat.
6. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma.
7. Tee turvaserveris **TS2** kliendile **CLIENT1** uus allkirjastamisvõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
8. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
9. Kustuta tühistatud allkirjasertifikaadid.

#### Allkirjasertifikaadi peatamine ja taastamine

1. Peata **CA**s turvaserveri **TS2** kliendi **CLIENT1** allkirjasertifikaat.
   * sertifikaadi peatamisel peab OCSP response olekuks saama "suspended".
2. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma.
3. Taasta **CA**s turvaserveri **TS2** kliendi **CLIENT1** allkirjasertifikaat.
   * sertifikaadi taastamisel peab OCSP response olekuks saama "good".
4. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

#### Autentimissertifikaadi tühistamine

1. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. (selle sammuga veendutakse, et turvaserver on ühenduseks puhverdanud esimese sertifikaadi)
2. Tee turvaserverile **TS2** teine autentimisvõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri sertifitseerimine)
3. Registreeri autentimissertifikaat keskserveris (sertifikaadi olekuks peab turvaserveris saama "registered") ja aktiveeri sertifikaat turvaserveris.
4. Tühista **CA**s turvaserveri **TS2** esimene autentimissertifikaat.
   * sertifikaadi tühistamisel peab OCSP response olekuks saama "revoked".
5. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
6. Tühista **CA**s turvaserveri **TS2** teine autentimissertifikaat.
7. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma.
8. Tee turvaserverile **TS2** uus autentimisvõti ja -sertifikaat (vt Abistsenaarium: Turvaserveri sertifitseerimine)
9. Registreeri autentimissertifikaat keskserveris (sertifikaadi olekuks peab turvaserveris saama "registered") ja aktiveeri sertifikaat turvaserveris.
10. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.
    * **Teada ikaldus**: turvaserverites puhverdatakse TLS sessioon ja kasutatavad sertifikaadid, sertifikaadi aktiveerimine rakendub alles sessiooni aegumisel (~5 min). Sessiooni koheseks lõpetamiseks võib TS2 sisestada käsu: "sudo service xroad-proxy restart". Ikaldust parandab tulevikus notify süsteem.
11. Kustuta tühistatud autentimissertifikaadid.

#### Autentimissertifikaadi peatamine ja taastamine

1. Peata **CA**s turvaserveri **TS2** autentimissertifikaat.
   * sertifikaadi peatamisel peab OCSP response olekuks saama "suspended".
2. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma.
3. Taasta **CA**s turvaserveri **TS2** autentimissertifikaat.
   * sertifikaadi taastamisel peab OCSP response olekuks saama "good".
4. Tee turvaserverist TS1 kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

## Päringulogide arhiveerimine ja päringulogidest allkirjade eraldamine

Selles peatükis testitakse turvaserveris toimuvat päringulogide arhiveerimist, päringulogide küsimist turvaserverist, päringulogist allkirjade eraldamist ja päringute verifitseerimist.

### Teststsenaarium: Päringulogide arhiveerimine, päringulogidest allkirjade eraldamine ja arhiivifaili krüptoahela verifitseerimine

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* Turvaserver TS2
* Testklient
* Arhiiviserver
* Asicverifier

Teststsenaarium:

1. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. Seejuures salvestatakse päringu identifikaator.
2. Ajatembeldamine toimub vaikimisi iga 60 sekundi tagant ja päringulogi arhiveerimist kutsutakse vaikimisi välja iga 6 tunni tagant. Et testimise ajal ajatembeldamist ja arhiveerimist kiirendada, võib turvaserveris TS2 lisada faili /etc/xroad/conf.d/local.ini read, mis käivitavad ajatembeldamise iga päringu korral ning seavad arhiveerimisintervalliks 30 sekundit:

[message-log]

archive-interval=0/30 \* \* ? \* \*

timestamp-immediately=true

Muudatuste jõustumiseks restarditakse turvaserver TS2 (sisestades käsu: "sudo service xroad-proxy restart").

1. Seadistatakse päringulogide teisaldamine arhiiviserverisse: turvaserveris TS2 faili /etc/xroad/conf.d/local.ini lisatakse [message-log] sektsiooni rida:

archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.sh -r <arhiiviserveri URL>

1. Oodatakse kuni logisse salvestatud päring ajatembeldatakse ja arhiiviserverisse teisaldatakse (~30 sekundit). NB! Kui arhiivifailide arhiiviserverisse teisaldamist ei ole seadistatud, on arhiivifailid kättesaadavad turvaserveris TS2 kaustas /var/lib/xroad/
2. Veendutakse, et arhiiviserverisse on teisaldatud ZIP fail, mis sisaldab ASIC-konteineri faili(e) ja tekstifaili *linkinginfo*. Arhiivifaili nimi on kujul mlog-X-Y-Z.zip, kus X on esimese päringulogi kirje ajatempel (UTC aeg kujul YYYYMMDDHHmmss), Y on viimase logikirje ajatempel ning Z on (kümnest tähtnumbrilisest sümbolist [A-Za-z0-9] koosnev) random.
3. ZIP fail pakitakse lahti ja allkirjastatud päringut sisaldav .asice fail, mille nimi algab tehtud päringu identifikaatoriga (kui identifikaatoris on failisüsteemi jaoks sobimatuid sümboleid, siis need on asendatud, rakendades neile URL kodeerimist), ning tekstifail *linkinginfo* salvestatakse kettale.
4. Verifitseeritakse signeeritud päring, kasutades asicverifier utiliiti (vt Abistsenaarium: Signeeritud päringu verifitseerimine).
5. Tekstifaili *linkinginfo* esimene rida on kujul:

PREV\_HASH PREV\_ARCH\_FILE HASH\_ALG

*PREV\_ARCH\_FILE* – linkimisahelas oleva eelmise arhiivifaili nimi (kui eelmist arhiivifaili ei ole, siis väärtuseks „-“),  
 *PREV\_HASH* – eelmise arhiivifaili viimane räsisamm hex kujul (kui eelmist arhiivifaili ei ole, siis väärtuseks „-“),  
 *HASH\_ALG* – arhiivifailis kasutatava räsialgoritmi identifikaator (näiteks SHA-256, SHA-512).

Kõik ülejäänud read on kujul:

HASH\_1 ASIC\_FILE\_1

...

HASH\_N ASIC\_FILE\_N

*ASIC\_FILE\_\** - arhiivifailis olevate ASIC-konteinerite failinimed,  
 *HASH\_\** - räsisamm hex kujul.

1. Avatakse eelmine arhiivifail ning veendutakse, et sealse *linkinginfo* faili viimasel real olev räsisamm ühtib vaadeldava faili esimesel real oleva räsisammuga.
2. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Oodatakse kuni logisse salvestatud päring ajatembeldatakse ja arhiiviserverisse teisaldatakse.
3. Avatakse järgmine moodustatud arhiivifail ning veendutakse, et sealse *linkinginfo* faili esimesel real olev räsisamm ühtib vaadeldava faili viimasel real oleva räsisammuga ning esimesel real toodud eelmise arhiivifaili nimi ühtib eelmise arhiivifaili nimega.
4. Arhiivifaili krüptoahel verifitseeritakse, kasutades turvaserveris TS2 kaustas /usr/share/doc/xroad-addon-messagelog/archive-hashchain-verifier asuvat utiliiti archive-hashchain-verifier.rb (kasutatakse vastavalt samas kaustas toodud README-le, kasutamiseks peavad olema installitud Ruby ja gem rubyzip). Skripti esimeseks argumendiks on tee arhiivifailini ja teiseks argumendiks on eelmise räsisammu tulemus. Veendutakse, et verifitseerimise utiliit väljastab tulemusena verifitseeritavas arhiivifailis oleva *linkinginfo* faili viimasel real oleva räsisammu.

### Teststsenaarium: Pakkajatemplit ja pakksignatuuri sisaldavatest päringulogidest allkirjade eraldamine

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* Turvaserver TS2
* Arhiiviserver
* Asicverifier

Teststsenaarium:

1. Et turvaserver väljastaks pakkajatempleid, eemaldatakse turvaserveris TS2 failist /etc/xroad/conf.d/local.ini rida

timestamp-immediately=true

Muudatuste jõustumiseks restarditakse turvaserver TS2 (sisestades käsu: "sudo service xroad-proxy restart"). Ajatembeldamine toimub peale seda iga 60 sekundi tagant.

1. Et turvaserver väljastaks pakksignatuure, tehakse järjest viis manusega päringut turvaserverist TS1 kliendiga CLIENT1:sub testteenusele. Päringud tehakse curl-iga:

curl -raw -v http://<TS1\_AADRESS>:80 --data-binary @simple.query -H "Content-type: multipart/related; charset=UTF-8; boundary=jetty771207119h3h10dty"

simple.query päring:

--jetty771207119h3h10dty

Content-Type: text/xml; charset="utf-8"

<?xml version="1.0" encoding="utf-8"?>

<SOAP-ENV:Envelope

xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"

xmlns:xroad="http://x-road.eu/xsd/xroad.xsd"

xmlns:id="http://x-road.eu/xsd/identifiers">

<SOAP-ENV:Header>

<xroad:client id:objectType="MEMBER">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>sub</id:subsystemCode>

</xroad:client>

<xroad:service id:objectType="SERVICE">

<id:xRoadInstance>AA</id:xRoadInstance>

<id:memberClass>COM</id:memberClass>

<id:memberCode>CLIENT1</id:memberCode>

<id:subsystemCode>testservice</id:subsystemCode>

<id:serviceCode>xroadGetRandom</id:serviceCode>

<id:serviceVersion>v1</id:serviceVersion>

</xroad:service>

<xroad:userId>EE37702211234</xroad:userId>

<xroad:id>1234567890</xroad:id>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<ns1:xroadGetRandom xmlns:ns1="http://consumer.ee.xroad.net"></ns1:xroadGetRandom>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

--jetty771207119h3h10dty

Content-Type: multipart/mixed; charset=UTF-8; boundary=jetty1627004719h3h10du0

--jetty1627004719h3h10du0

Content-Type: text/plain

blaah

--jetty1627004719h3h10du0--

--jetty771207119h3h10dty--

1. Oodatakse kuni logisse salvestatud päringud ajatembeldatakse ja arhiiviserverisse teisaldatakse (~60 sekundit).
2. Veendutakse, et arhiiviserverisse on teisaldatud ZIP fail, mis sisaldab ASIC-konteineri faili(e) ja tekstifaili *linkinginfo*.
3. ZIP fail pakitakse lahti ja üks allkirjastatud päringut sisaldav .asice fail, mille nime alguses on <tehtud päringu identifikaator>-request, salvestatakse kettale.
4. Pakitakse lahti .asice fail ning veendutakse, et see sisaldab faile *sig-hashchain.xml* ja *ts-hashchain.xml* - järelikult on tegu pakkajatempli ja pakksignatuuriga.
5. Verifitseeritakse signeeritud päring kasutades asicverifier utiliiti (vt Abistsenaarium: Signeeritud päringu verifitseerimine).

### Teststsenaarium: Päringu identifikaatoris failisüsteemi jaoks sobimatute sümbolite asendamine

Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Arhiiviserver

Teststsenaarium:

1. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring tehakse curl-iga ning päringu identifikaatorisse lisatakse mõni failisüsteemi jaoks sobimatu sümbol (näiteks <xroad:id>abc#?"</xroad:id>).
2. Oodatakse kuni logisse salvestatud päringud ajatembeldatakse (ja arhiiviserverisse teisaldatakse).
3. Veendutakse, et arhiivifail sisaldab .asice faili, mille nimi algab tehtud päringu identifikaatoriga, milles failisüsteemi jaoks sobimatud sümbolid on asendatud, rakendades neile URL kodeerimist. Näiteks päringu identifikaatori *abc#?"* kasutamisel algab .asice faili nimi stringiga *abc%23%3F%22*.

### Teststsenaarium: ASiC-konteinerite küsimine turvaserverist

ASiC-konteinerite küsimisel tuleb arvestada, et tagastatavates ASiC-konteinerite failinimedes on päringu identifikaatorid URL-kodeeritud vältimaks ebasobivate sümbolite sattumist failinimedesse. Kuna päringu identifikaatorit kasutatakase ka ASiC-konteinerite küsimise päringu parameetri väärtusena (HTTP GET päring), siis võib ka seal osutuda vajalikuks mõnede erisümbolite URL-kodeerimist (näiteks "&", "?", jmt). ASiC-konteinerite päringute vastuseks tagastatavaid HTTP koode on võimalik vaadata Firebugi või mõnda muud brauseri veebiarendustööriista kasutades.

Testi käigus kasutatavad ressursid:

* Turvaserver TS1
* Turvaserver TS2
* Testklient
* Asicverifier

#### Päringu ja päringuvastuse küsimine

1. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. Seejuures salvestatakse päringu identifikaator.
2. Oodatakse kuni logisse salvestatud päring ajatembeldatakse.
3. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>

ning salvestatakse pakutud ZIP fail kohalikku failisüsteemi ja pakitakse lahti.

1. Veendutakse, et ZIP fail sisaldab kahte \*.asice faili: päringut ja päringuvastust, failide nimed algavad vastavalt

<päringu identifikaator>-request

ja

<päringu identifikaator>-response

1. Verifitseeritakse päring ja päringuvastus kasutades asicverifier utiliiti (vt Abistsenaarium: Signeeritud päringu verifitseerimine)

#### Päringu küsimine

1. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&requestOnly

ning salvestatakse pakutud ZIP fail kohalikku failisüsteemi ja pakitake lahti (vt Veaolukorrad: ASiC-konteinerite küsimine).

1. Veendutakse, et ZIP fail sisaldab ühte .asice päringufaili, faili nime algus on:

<päringu identifikaator>-request

#### Unikaalse päringuvastuse küsimine

1. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&responseOnly&unique

ning salvestatakse pakutud .asice fail kohalikku failisüsteemi.

1. Veendutakse, et faili nime algus on:

<päringu identifikaator>-response

1. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub sama päringu identifikaatoriga (nt curli kasutades) päring testteenusele. Päring peab õnnestuma.
2. Oodatakse kuni logisse salvestatud päring ajatembeldatakse.
3. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&responseOnly&unique

1. Veendutakse, et tagastatakse HTTP kood 500 ja veateade "query did not return a unique result: 2".

#### Puuduva ajatempliga päringu kirjete küsimine

Testitakse ajatempli puudumisel selle lisamise käskimist parameetriga *force*.

1. Sisestatakse URL, mille päringu kirje on ajatembeldamata ning veendutakse, et tagastatakse HTTP kood 500 ja veateade: "Some message signatures have not been timestamped yet!".
2. Sisestatakse URL, mille päringu kirje on ajatembeldamata, URL-i lõppu lisatakse &force ning veendutakse, et tagastatakse ZIP fail küsitud päringu kirjetega.
   * Kuidas: turvaserveris TS2 failist /etc/xroad/conf.d/local.ini eemaldatakse [message-log] sektsioonist rida

timestamp-immediately=true

Muudatuste jõustumiseks restarditakse turvaserver TS2 (sisestades käsu: "sudo service xroad-proxy restart").Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. Seejuures salvestatakse päringu identifikaator ning küsitakse antud identifikaatoriga päringu kirjeid turvaserverist TS2 enne kui need jõutakse ajatembeldada (st 60 sekundi jooksul).

#### ASiC-konteinerite küsimine üle HTTPS ühenduse

1. Turvaserveris TS2 seadistatakse kliendi CLIENT1:testservice ühenduseks HTTPS\_NO\_AUTH (Security Server Clients -> Internal Servers).
2. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. Seejuures salvestatakse päringu identifikaator.
3. Oodatakse kuni logisse salvestatud päring ajatembeldatakse.
4. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>

ning veendutakse, et tagastatakse HTTP kood 401 ja veateade: "Client (SUBSYSTEM:AA/COM/CLIENT1/testservice) specifies HTTPS NO AUTH but client made plaintext connection".

1. Brauserisse sisestatakse URL

https://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>

ning veendutakse, et tagastatakse päringukirjeid sisaldav ZIP fail.

1. Turvaserveris TS2 seadistatakse kliendi CLIENT1:testservice ühenduseks HTTPS (Security Server Clients -> Internal Servers).
2. Brauserisse sisestatakse URL

https://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>

ning veendutakse, et tagastatakse HTTP kood 401 ja veateade: "Client (SUBSYSTEM:AA/COM/CLIENT1/testservice) specifies HTTPS but did not supply TLS certificate".

1. Turvaserverisse TS2 kliendile CLIENT1:testservice laetakse üles kliendi sertifikaat (Internal TLS Certificates - Add) ning sama sertifikaat ja võti P12 formaadis imporditakse kasutatavasse brauserisse.
2. Brauserisse sisestatakse URL

https://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>

kui brauser küsib, millist sertifikaati enda tuvastamiseks kasutada, valitakse imporditud sertifikaat. Veendutakse, et tagastatakse päringukirjeid sisaldav ZIP fail.

1. Turvaserveris TS2 seadistatakse kliendi CLIENT1:testservice ühenduseks HTTP (Security Server Clients -> Internal Servers).

#### Veaolukorrad: ASiC-konteinerite küsimine

1. Sisestatakse URL, mis sisaldab päringu identifikaatorit, mida andmebaasis ei eksisteeri - veendutakse, et tagastatakse HTTP kood 404 ja veateade: "No signed documents found".
2. Sisestatavast URL-st eemaldatakse "&memberCode=CLIENT1" ning veendutakse, et tagastatakse HTTP kood 400 ja veateade: "Parameter "memberCode" must be specified.".
3. Sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&requestOnly&responseOnly

ning veendutakse, et tagastatakse HTTP kood 400 ja veateade: Parameters "requestOnly" and "responseOnly" cannot be used at the same time.

1. Sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&unique

ning veendutakse, et tagastatakse HTTP kood 400 ja veateade: "Parameter "unique" not applicable without "requestOnly" or "responseOnly".".

1. Sisestatakse URL

http://<TS2\_AADRESS>/asic?xRoadInstance=AA&memberClass=COM&memberCode=CLIENT1&subsystemCode=testservice&queryId=<päringu identifikaator>&force

mille päringu kirje on ajatembeldamata ja turvaserveris TS2 ei ole seadistatud ajatempliteenust, mis oleks võimeline ajatembeldust tegema ning veendutakse, et tagastatakse HTTP kood 500 ja veateade: "Failed to get time stamp from any time-stamping providers".

* Kuidas: turvaserveris TS2 failist /etc/xroad/conf.d/local.ini eemaldatakse [message-log] sektsioonist rida

timestamp-immediately=true

Muudatuste jõustumiseks restarditakse turvaserver TS2 (sisestades käsu: "sudo service xroad-proxy restart"). Keskserveris KS1 lisatakse uus mittetöötav ajatempliteenus (kasutatakse suvalist URLi ja sertfitikaati). Lisatud ajatempliteenus seadistatakse turvaserveri TS2 ainsaks kasutatavaks ajatempliteenuseks. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma. Seejuures salvestatakse päringu identifikaator ning küsitakse antud identifikaatoriga päringu kirjeid turvaserverist TS2.

### Abistsenaarium: Signeeritud päringu verifitseerimine

(Kasutatakse teststsenaariumite käigus.)

#### Verifitseerimiskonfiguratsiooni laadimine

1. Brauserisse sisestatakse URL

http://<TS2\_AADRESS>/verificationconf

ning salvestatakse pakutud fail verificationconf.zip kohalikku failisüsteemi ja pakitake lahti.

1. Tulemuseks peab olema järgmise sisuga kataloogistruktuur:

verificationconf

|-- AA

| `-- shared-params.xml

`-- instance-identifier

#### ASiC-konteineri verifitseerimine

1. ASiC-konteiner verifitseeritakse kasutades asicverifier utiliiti (levitatakse eraldi, eeldab Java 8 olemasolu süsteemis). Utiliit võtab käsurea argumendiks kausta nime, kus asub verifitseerimiskonfiguratsioon, ning ASiC-konteineri failinime, mida soovitakse verifitseerida:

java -jar asicverifier-1.0.jar verificationconf <failinimi.asice>

1. Verifitseerimine peab õnnestuma, signatuuri ja ajatempli andmed peavad olema korrektsed, konteinerist eraldatakse korrektne message.xml fail.

## Registreeritud objektide kustutamine

Selles peatükis testitakse olulisemate X-tee objektide kustutamist, sh

* X-tee liikme kustutamine,
* turvaserveri kustutamine,
* turvaserveri kliendi kustutamine,
* turvaserveri autentimissertifikaadi kustutamine.

### Teststsenaarium: X-tee liikme kustutamine keskserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Keskserverist **KS1** kustutatakse liige **CLIENT1** (Members -> Details -> Delete).
   * Keskserveris peab peamenüü "Management Requests" vaatesse ja turvaserverite TS1 ja TS2 "Management Requests" vaadetesse ilmuma taotlused tüübiga "Client deletion", mille "Comments" väljas on kirjas: "SUBSYSTEM:AA/COM/CLIENT1/sub deletion" ja "SUBSYSTEM:AA/COM/CLIENT1/testservice deletion".
   * Keskserveris peab turvaserverite TS1 ja TS2 detailvaate "Clients" tabi tabelist olema kadunud kliendid CLIENT1:sub ja CLIENT1:testservice.
   * Turvaserveris TS1 peab klient CLIENT1:sub olema olekus "global error", nimena kuvatakse "Client not found in global configuration".
   * Turvaserveris TS2 peab klient CLIENT1:testservice olema olekus "global error", nimena kuvatakse "Client not found in global configuration".
3. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega "Client 'SUBSYSTEM:AA/COM/CLIENT1/sub' not found".
4. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * CLIENT1 on liikmete nimekirjas ja tema alamsüsteemid on turvaserverite klientide nimistus,
   * turvaserverites on klientide CLIENT1\* nimed olemas ja olekuks "registered".
5. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Turvaserveri omaniku kustutamine keskserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Keskserverist **KS1** kustutatakse liige **TS2OWNER** (Members -> Details -> Delete).
   * keskserveris peab peamenüü "Management Requests" vaatesse ilmuma taotlused, mille "Comments" väljas on kirjas: "'SERVER:AA/GOV/TS2OWNER/TS2' deletion"
     + tüübiga "Client deletion" CLIENT1:testservice kohta,
     + tüübiga "Client deletion" TS2OWNER:sub kohta,
     + tüübiga "Certificate deletion" TS2 autentimissertifikaadi kohta,
   * keskserverist peab olema kustunud turvaserver TS2,
   * keskserveris CLIENT1 detailvaate "Subsystems" tab'is peab alamsüsteem "testservice" olema punases kirjas ja seda peab olema võimalik kustutada,
   * turvaserveris TS2 peavad turvaserveri omanik ja TS2OWNER:sub olema olekus "global error", nimena kuvatakse "Client not found in global configuration",
   * turvaserveris TS2 peab autentimissertifikaat olema olekus "global error".
3. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega: „Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1"“.
4. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * TS2OWNER on liikmete nimekirjas,
   * TS2 on turvaserverite nimekirjas,
   * CLIENT1:testservice ja TS2OWNER:sub on TS2 klientide nimekirjas,
   * TS2 on CLIENT1 "Used Servers" nimekirjas,
   * turvaserveris TS2 on omanik, TS2OWNER:sub ja autentimissertifikaat olekus "registered".
5. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Turvaserveri kustutamine keskserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Keskserverist **KS1** kustutatakse turvaserver **TS2** (Security Servers -> Details -> Delete).
   * keskserveris peab peamenüü "Management Requests" vaatesse ja TS2OWNER "Management Requests" tab'i ilmuma taotlused, mille "Comments" väljas on kirjas: "'SERVER:AA/GOV/TS2OWNER/TS2' deletion"
     + tüübiga "Certificate deletion" ja
     + tüübiga "Client deletion" (CLIENT1:testservice ja TS2OWNER:sub kohta)
   * keskserverist peab olema kustunud turvaserver TS2;
   * keskserveris CLIENT1 detailvaate "Subsystems" tab'is peab alamsüsteem "testservice" olema punases kirjas ja seda peab olema võimalik kustutada;
   * turvaserveris TS2 peab turvaserveri omanik olema olekus "global error", aga nimi peab alles olema;
   * turvaserveris TS2 peab autentimissertifikaat olema olekus "global error".
3. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1"".
4. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * TS2 on turvaserverite nimekirjas,
   * CLIENT1:testservice on TS2 klientide nimekirjas,
   * TS2 on CLIENT1 "Used Servers" nimekirjas,
   * turvaserveris TS2 on omanik ja autentimissertifikaat olekus "registered".
5. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Turvaserveri kliendi kustutamine keskserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Keskserverist **KS1** kustutatakse turvaserveri **TS2** klient **CLIENT1:testservice** (Security Servers -> Details -> Clients -> Delete)
3. Keskserverist KS1 kustutatakse turvaserveri **TS1** klient **CLIENT1:sub** (Members -> Details -> Used Servers -> Delete).
   * keskserveris peavad peamenüü "Management Requests" vaatesse ning TS1, TS2 ja CLIENT1 "Management Requests" tab'i ilmuma taotlused tüübiga "Client deletion", mille "Comments" väljas sisaldub "Client '<ID>' deletion";
   * keskserverist peavad turvaserverite TS1 ja TS2 "Clients" tab'ist olema kadunud kustutatud kliendid;
   * keskserveris CLIENT1 detailvaate "Subsystems" tab'is peavad alamsüsteemid "sub" ja "testservice" olema punases kirjas ja neid peab olema võimalik kustutada;
   * turvaserverites peavad kustutatud kliendid olema olekus "global error", kuid nimed peavad neil alles olema.
4. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1"“.
5. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * Turvaserverite "Clients" vaates on eelnevalt kustutatud kliendid olemas,
   * CLIENT1 "Used servers" vaates on olemas seosed turvaserveritega,
   * turvaserverites on kliendid olekus "registered".
6. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Turvaserveri kliendi kustutamine turvaserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Turvaserver TS2 varundatakse.
3. Turvaserverist **TS2** esitatakse kliendi **CLIENT1:testservice** registreerimise tühistamise taotlus (*unregister*). Kliendi andmeid ja sertifikaate ei kustutata.
   * Kliendi taotluse esitamisel küsitakse, kas kustutada ka kliendi andmed.
   * keskserveris peavad peamenüü "Management Requests" vaatesse, TS2 ja CLIENT1 "Management Requests" tab'i ilmuma taotlused tüübiga "Client deletion".
   * keskserverist peab turvaserveri TS2 "Clients" tab'ist olema kadunud CLIENT1:testservice.
   * keskserveris CLIENT1 detailvaate "Subsystems" tab'is peab alamsüsteem "testservice" olema punases kirjas ja seda peab olema võimalik kustutada;
   * turvaserveris TS2 peab CLIENT1:testservice olema olekus "deletion in progress", kliendi teenuste konfiguratsioon peab olema alles.
4. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1"“.
5. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * Turvaserveri TS2 "Clients" vaates on CLIENT1:testservice olemas,
   * CLIENT1 "Used servers" vaates on alamsüsteem "testservice" seotud TS2-ga,
   * turvaserveris TS2 jääb CLIENT1:testservice olekuks "deletion in progress".
6. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega: „Client 'SUBSYSTEM:AA/COM/CLIENT1/testservice' not found“.
7. **Turvaserver TS2 taastatakse** ja veendutakse, et konfiguratsioon on samasugune kui varundamise hetkel, st CLIENT1:testservice olekuks on "registered".
8. Turvaserverist **TS2** esitatakse kliendi **CLIENT1:testservice** kustutamise taotlus. Kustutatakse nii kliendi andmed kui seotud sertifikaadid.
9. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega: Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1" .
10. **Taastatakse turvaserver TS2**.
    * Turvaserveris TS2 peab CLIENT1:testservice olekuks olema "global error".
11. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Could not find addresses for service provider "SERVICE:AA/COM/CLIENT1/testservice/xroadGetRandom/v1"“.
12. **Taastatakse keskserver**.
    * turvaserveris TS2 peab CLIENT1:testservice olekuks olema "registered".
13. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Autentimissertifikaadi kustutamine keskserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt Abistsenaarium: Serveri varundamine ja taastamine)
2. Keskserveris **KS1** kustutatakse turvaserveri **TS2** autentimissertifikaat.
   * keskserveris peavad peamenüü "Management Requests" vaatesse ja TS2 "Management Requests" tab'i ilmuma taotlused tüübiga "Certificate deletion", mille "Comments" väljas sisaldub "Authentication certificate deletion",
   * keskserveris TS2 detailvaate "authentication certificates" tab'ist peab sertifikaat olema kustunud,
   * turvaserveris TS2 peab autentimissertifikaat olema olekus "global error".
3. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega: „Service provider did not send correct authentication certificate“.
4. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel:
   * TS2 detailvaate "authentication certificates" tab'i peab sertifikaat olema taastunud.
   * turvaserveris TS2 peab autentimissertifikaat olema olekus "registered".
5. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Teststsenaarium: Autentimissertifikaadi kustutamine turvaserverist

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Keskserver KS1 varundatakse (vt Abistsenaarium: Serveri varundamine ja taastamine).
2. Turvaserver TS2 varundatakse.
3. Turvaserverist **TS2** esitatakse autentimissertifikaadi registreerimise tühistamise taotlus (*unregister*). Sertifikaati ei kustutata.
   * keskserveris peavad peamenüü "Management Requests" vaatesse ja TS2 "Management Requests" tab'i ilmuma taotlused tüübiga "Certificate deletion".
   * keskserverist peab turvaserveri TS2 "Authentication certificates" tab'ist olema kadunud autentimissertifikaat.
   * turvaserveris TS2 peab autentimissertifikaat olema olekus "deletion in progress".
4. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Service provider did not send correct authentication certificate“. (Kui globalconfist kaob sertifikaat ära varem kui TLS cachest, siis kuni cache uuendamiseni on veateateks "Authentication certificate <DN> is not associated with any security server").
5. **Keskserver taastatakse** ja veendutakse, et keskserveri konfiguratsioon on samasugune kui varundamise hetkel, sh
   * keskserveris TS2 "Authentication certificates" vaates on autentimissertifikaat olemas,
   * turvaserveris TS2 on autentimissertifikaat olekus "deletion in progress".
6. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Service provider did not send correct authentication certificate“.
7. **Turvaserver TS2 taastatakse** ja veendutakse, et konfiguratsioon on samasugune kui varundamise hetkel, st autentimissertifikaadi olekuks on "registered".
8. Turvaserverist TS2 esitatakse autentimissertifikaadi registreerimise tühistamise taotlus (*unregister*). Sertifikaat kustutatakse.
   * Sertifikaadi kustutamisel peab serveri konfiguratsioonist kustuma ka autentimisvõti. Võtmeseadmele jääb võti alles ja seda kuvatakse UIs kollasel taustal.
9. Turvaserveris TS2 kustutatakse võtmeseadmelt autentimisvõti.
10. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Service provider did not send correct authentication certificate“.
11. **Taastatakse turvaserver TS2**.
    * autentimissertifikaadi olekuks peab saama "global error".
12. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab ebaõnnestuma veateatega „Service provider did not send correct authentication certificate“.
13. **Taastatakse keskserver**
    * autentimissertifikaadi olekuks peab saama "registered".
14. Turvaserverist TS1 tehakse kliendiga CLIENT1:sub päring testteenusele. Päring peab õnnestuma.

### Abistsenaarium: Serveri varundamine ja taastamine

(Kasutatakse teststsenaariumite käigus.)

#### Serveri varundamine

##### Serveri varundamine kasutajaliidese kaudu

1. Varundatakse serveri konfiguratsioon.
   * Veendutakse, et kuvatakse varundamise skripti väljund. Näide varundamise skripti väljundi alguse ja lõpu kohta keskserveri varundamisel:

CREATING DATABASE DUMP TO /var/lib/xroad/dbdump.dat\_backup\_Thu\_Nov\_\_5\_15\_31\_51\_EET\_2015

CREATING TAR ARCHIVE TO /var/lib/xroad/backup//conf\_backup\_20151105-153151.tar

central\_XROAD\_6.8\_AA

...

Backup file saved to /var/lib/xroad/backup//conf\_backup\_20151105-153151.tar

* + Näide varundamise skripti väljundi alguse ja lõpu kohta turvaserveri varundamisel:

CREATING DATABASE DUMP TO /var/lib/xroad/dbdump.dat\_backup\_Thu\_Nov\_\_5\_15\_40\_51\_EET\_2015

CREATING TAR ARCHIVE TO /var/lib/xroad/backup//conf\_backup\_20151105-154051.tar

security\_XROAD\_6.8\_AA/GOV/TS1OWNER/TS1

...

Backup file saved to /var/lib/xroad/backup//conf\_backup\_20151105-154051.tar

2. Kontrollitakse loodud varundusfaili tarball labelit (vt Varundusfaili tarball labeli kontrollimine).

##### Serveri varundamine käsureal

* Turvaserveri varundamiseks käivitatakse skript, mille argumentideks on turvaserveri ID ja loodava varundusfaili nimi (vt Veaolukorrad: serveri varundamise/taastamise skripti välja kutsumine puuduvate argumentidega).
* Näiteks turvaserveri TS1 varundamiseks tuleks varundamise skript käivitada nii:

/usr/share/xroad/scripts/backup\_xroad\_proxy\_configuration.sh -s "AA/GOV/TS1OWNER/TS1" -f backup.tar

* Veendutakse, et kuvatakse varundamise skripti väljund. Näide varundamise skripti väljundi alguse ja lõpu kohta turvaserveri varundamisel:

CREATING DATABASE DUMP TO /var/lib/xroad/dbdump.dat\_backup\_Fri\_Oct\_23\_08\_54\_40\_UTC\_2015

CREATING TAR ARCHIVE TO backup.tar

security\_XROAD\_6.8\_AA/GOV/TS1OWNER/TS1

...

Backup file saved to backup.tar

* Keskserveri varundamiseks käivitatakse skript, mille argumentideks on eksemplari identifikaator ja loodava varundusfaili nimi (vt Veaolukorrad: keskserveri varundamine). Näiteks keskserveri KS1 varundamiseks tuleks varundamise skript käivitada nii:

/usr/share/xroad/scripts/backup\_xroad\_center\_configuration.sh -i "AA" -f backup.tar

* Veendutakse, et kuvatakse varundamise skripti väljund. Näide varundamise skripti väljundi alguse ja lõpu kohta keskserveri varundamisel:

CREATING DATABASE DUMP TO /var/lib/xroad/dbdump.dat\_backup\_Tue\_Nov\_10\_14\_49\_12\_EET\_2015

CREATING TAR ARCHIVE TO backup.tar

central\_XROAD\_6.8\_AA

...

Backup file saved to backup.tar

* Kontrollitakse loodud varundusfaili tarball labelit (vt Varundusfaili tarball labeli kontrollimine).

##### Varundusfaili tarball labeli kontrollimine

Nii käsureal kui kasutajaliidese varundamisel tekitatakse tarballile label, mida saab kontrollida käsuga

tar tf <varundusfail> | head -1

1. Kontrollitakse loodud konfiguratsioonifaili tarball labelit. Veendutakse, et tarballi labeli väärtus on:
   * Keskserveri puhul: central\_XROAD\_<tarkvara versioon>\_<instantsi id>[\_<HA sõlme nimi>] (viimane sõltub HA toe olemasolust)
   * Turvaserveri puhul: security\_XROAD\_<tarkvara versioon>\_<turvaserveri id> (viimane kujul <instantsi id>/<omaniku liikmeklass>/<omaniku liikmekood>/<turvaserveri kood>)

##### Veaolukorrad: keskserveri varundamine

1. Varundamise skript käivitatakse koos HA sõlme nime argumendiga keskserveris, mis ei ole HA klastri liige. Näiteks:

/usr/share/xroad/scripts/backup\_xroad\_center\_configuration.sh -i "AA" -n "node\_0" -f backup.tar

1. Veendutakse, et keskserveri varundamine ebaõnnestub veateatega "Not expecting HA node name if postgresql-bdr-9.4 is not installed".

##### Veaolukorrad: serveri varundamise/taastamise skripti välja kutsumine puuduvate argumentidega

**Keskserveri varundamise skripti väljakutse ilma argumentideta:**

$ /usr/share/xroad/scripts/backup\_xroad\_center\_configuration.sh

Kuvatav veateade:

Missing value of instance ID

Usage: /usr/share/xroad/scripts/backup\_xroad\_center\_configuration.sh -i <instance ID> [-n <HA node name>] -f <path of tar archive>

Backup the configuration (files and database) of the X-Road central server to a tar archive.

OPTIONS:

-h Show this message and exit.

-b Treat all input values as encoded in base64.

-i Instance ID of the installation of X-Road.

-n Node name of the central server if deployed in HA setup.

-f Absolute path of the resulting tar archive.

**Keskserveri taastamise skripti väljakutse ilma argumentideta:**

$ /usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh

Kuvatav veateade:

Missing value of instance ID

Usage: /usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i <instance ID> [-n <HA node name>] -f <path of tar archive> [-F]

Restore the configuration (files and database) of the X-Road central server from a tar archive.

OPTIONS:

-h Show this message and exit.

-b Treat all input values as encoded in base64.

-i Instance ID of the installation of X-Road. Mandatory if -F is not used.

-n Node name of the central server if deployed in HA setup.

Mandatory if -F is not used.

-f Absolute path of the tar archive to be used for restoration. Mandatory.

-F Force restoration, taking only the type of server into account.

**Turvaserveri varundamise skripti väljakutse ilma argumentideta:**

$ /usr/share/xroad/scripts/backup\_xroad\_proxy\_configuration.sh

Kuvatav veateade:

Missing value of security server ID

Usage: /usr/share/xroad/scripts/backup\_xroad\_proxy\_configuration.sh -s <security server ID> -f <path of tar archive>

Backup the configuration (files and database) of the X-Road security server to a tar archive.

OPTIONS:

-h Show this message and exit.

-b Treat all input values as encoded in base64.

-s ID of the security server.

-f Absolute path of the resulting tar archive.

**Turvaserveri taastamise skripti väljakutse ilma argumentideta:**

$ /usr/share/xroad/scripts/restore\_xroad\_proxy\_configuration.sh

Kuvatav veateade:

Missing value of security server ID

Usage: /usr/share/xroad/scripts/restore\_xroad\_proxy\_configuration.sh -s <security server ID> -f <path of tar archive> [-F]

Restore the configuration (files and database) of the X-Road security server

from a tar archive.

OPTIONS:

-h Show this message and exit.

-b Treat all input values as encoded in base64.

-s ID of the security server. Mandatory if -F is not used.

-f Absolute path of the tar archive to be used for restoration. Mandatory.

-F Force restoration, taking only the type of server into account.

#### Serveri taastamine

##### Serveri taastamine kasutajaliidese kaudu

1. Vajadusel laetakse serverisse eelnevalt kohalikku failisüsteemi salvestatud varundusfail (vt Veaolukorrad: varundusfaili laadimine).
2. Taastatakse server varundusfailist (vt Veaolukorrad: serveri taastamine kasutajaliidese kaudu).
   * Veendutakse, et kuvatakse taastamise skripti väljund. Näide taastamise skripti väljundi alguse ja lõpu kohta keskserveri taastamisel:

CHECKING THE LABEL OF THE TAR ARCHIVE

central\_XROAD\_6.8\_AA

RESTORING CONFIGURATION FROM /var/lib/xroad/backup//conf\_backup\_20151023-073342.tar

CLEARING SHARED MEMORY

STOPPING ALL SERVICES EXCEPT JETTY

...

RESTORING DATABASE FROM /var/lib/xroad/dbdump.dat

RESTARTING SERVICES

xroad-signer start/running, process 3062

1. Veendutakse, et serverit saab taastada käsurealt loodud varukoopiast. Selleks viiakse nii turva- kui keskserveri puhul läbi järgmised sammud:
   * Luuakse varukoopia käsurealt valitud nimega (nt **/var/lib/xroad/backup/backup\_commandline.tar**). Vt ka Serveri varundamine käsureal
   * Taastatakse server nimetatud varukoopiast.
   * Veendutakse, et kuvatakse taastamise skripti väljund.

##### Veaolukorrad: varundusfaili laadimine

1. Proovitakse laadida faili, mis ei ole arhiivifail. Laadimine peab ebaõnnestuma.

##### Veaolukorrad: serveri taastamine kasutajaliidese kaudu

Kasutajaliidese kaudu taastamisel ollakse nõus taastama ainult sellisest tarballist, mille label on täpselt sama, mis antud serveri parameetritele vastavalt konstrueeritud string.

1. Proovitakse taastada server .tar failist, mis ei ole varundusfail. Taastamine peab ebaõnnestuma. Näide kuvatavast veateatest turvaserveris:

CHECKING THE LABEL OF THE TAR ARCHIVE

tar: Archive not labeled to match 'security\_XROAD\_6.8\_AA/GOV/TS1OWNER/TS1'

tar: Error is not recoverable: exiting now

The expected label (security\_XROAD\_6.8\_AA/GOV/TS1OWNER/TS1) and the actual label of the tarball <faili\_tarballi\_label> do not match. Aborting restore!

Failed to restore the configuration of the X-Road security server

1. Proovitakse taastada server varundusfailist, mille label ei vasta taastatava serveri parameetritele. Taastamine peab ebaõnnestuma.
   * Kuidas: keskserverisse laetakse üles mõne teise keskserveri varundusfail ning proovitakse UI kaudu konfiguratsioon sellest failist taastada. Näide kuvatavast veateatest:

CHECKING THE LABEL OF THE TAR ARCHIVE

tar: Volume 'central\_XROAD\_6.8\_AA\_node\_0' does not match 'central\_XROAD\_6.8\_BB'

tar: Error is not recoverable: exiting now

The expected label (central\_XROAD\_6.8\_BB) and the actual label of the tarball /var/lib/xroad/backup//conf\_backup\_20151106-113259\_FED0.tar do not match. Aborting restore!

Failed to restore the configuration of the X-Road central server

1. Proovitakse taastada server failist, mille laiend ei ole .tar. Taastamine peab ebaõnnestuma, kuvatav veateade peab algama reaga "tar: This does not look like a tar archive".
   * + Kuidas: kausta var/lib/xroad/backup pannakse suvaline fail ning proovitakse UI kaudu konfiguratsioon sellest failist taastada.
2. Proovitakse taastada keskserverit turvaserveri varundusfailist. Taastamine peab ebaõnnestuma.
   * Kuidas: laetakse turvaserveri varundusfail keskserverisse ja proovitakse UI kaudu konfiguratsioon sellest failist taastada. Taastamine peab ebaõnnestuma labelite mittesobivuse tõttu.

##### Serveri taastamine käsureal

1. Turvaserveri taastamiseks käsureal käivitatakse skript, mille argumentideks on eksemplari identifikaator, turvaserveri ID ja varundusfaili nimi (vt Veaolukorrad: serveri taastamine käsureal ja Veaolukorrad: serveri varundamise/taastamise skripti välja kutsumine puuduvate argumentidega). Näiteks turvaserveri TS1 taastamiseks tuleks taastamise skript käivitada nii:

/usr/share/xroad/scripts/restore\_xroad\_proxy\_configuration.sh -s "AA/GOV/TS1OWNER/TS1" -f backup.tar

1. Veendutakse, et kuvatakse taastamise skripti väljund. Näide taastamise skripti väljundi alguse ja lõpu kohta turvaserveri taastamisel:

CHECKING THE LABEL OF THE TAR ARCHIVE

security\_XROAD\_6.8\_AA/GOV/TS1OWNER/TS1

RESTORING CONFIGURATION FROM backup.tar

...

xroad-proxy start/running, process 10832

1. Keskserveri taastamiseks käsureal käivitatakse skript, mille argumentideks on eksemplari identifikaator ja varundusfaili nimi (vt Veaolukorrad: keskserveri taastamine). Näiteks keskserveri KS1 taastamiseks tuleks taastamise skript käivitada nii: /usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i "AA" -f backup.tar
   * Veendutakse, et kuvatakse taastamise skripti väljund. Näide taastamise skripti väljundi alguse ja lõpu kohta keskserveri taastamisel:

CHECKING THE LABEL OF THE TAR ARCHIVE

central\_XROAD\_6.8\_AA

RESTORING CONFIGURATION FROM backup.tar

...

RESTORING DATABASE FROM /var/lib/xroad/dbdump.dat

RESTARTING SERVICES

xroad-signer start/running, process 12374

1. Veendutakse, et serverit saab taastada kasutajaliidese kaudu loodud varukoopiast. Selleks viiakse nii kesk- kui turvaserveris läbi järgmised sammud:
   * Varundatakse server kasutajaliidesest (vt Serveri varundamine kasutajaliidese kaudu). Jäetakse meelde varukoopia failinimi (nt UI nimekirjast: **conf\_backup\_20151105-154051.tar**).
   * Taastatakse konfiguratsioon käsurealt, kasutades UI genereeritud failinime (nt failitee: **/var/lib/xroad/backup/conf\_backup\_20151105-154051.tar**).
   * Veendutakse, et kuvatakse taastamisskripti väljund.

##### Serveri taastamine käsureal forced mode võtmega

Käsurealt taastamisel on võimalik kasutada nn. forced mode'i võtmega -F, mispuhul kontrollitakse ainult serveri tüübi e. tarballi labeli esimese elemendi vastavust (võimalikud väärtused **security** ja **central**).

1. Taastatakse server forced mode võtmega (näide turvaserveri taastamise kohta) (vt Veaolukorrad: serveri taastamine käsureal):

/usr/share/xroad/scripts/restore\_xroad\_proxy\_configuration.sh -F -f /var/lib/xroad/backup/conf\_backup\_20151105-154051.tar

Näide taastamise skripti väljundi alguse ja lõpu kohta turvaserveri forced mode võtmega taastamisel:

CHECKING THE LABEL OF THE TAR ARCHIVE

RESTORING CONFIGURATION FROM conf\_backup\_20151023-081558.tar

...

xroad-proxy start/running, process 5552

##### Veaolukorrad: keskserveri taastamine

1. Taastamise skript käivitatakse koos HA sõlme nime argumendiga keskserveris, mis ei ole HA klastri liige. Näiteks:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i "AA" -n "node\_0" -f backup.tar

1. Veendutakse, et keskserveri taastamine ebaõnnestub veateatega "Not expecting HA node name if postgresql-bdr-9.4 is not installed".

##### Veaolukorrad: serveri taastamine käsureal

**Serveri taastamine forced mode võtit kasutades vale tüüpi serveri tarballist**

* Näide turvaserveri taastamisest, varundusfailiks on keskserveri varundusfail:

/usr/share/xroad/scripts/restore\_xroad\_proxy\_configuration.sh -F -f conf\_backup\_20151023-073342.tar

* Kuvatava veateate näide turvaserveri taastamisel keskserveri tarballist:

CHECKING THE LABEL OF THE TAR ARCHIVE

The beginning of the label does not contain the correct server type

Failed to restore the configuration of the X-Road security server

**Serveri taastamine varundusfailist tehnilistel põhjustel ebaõnnestub, aga pre-restore backup saab tehtud**

Keskserveri näitel, aga kehtib ka turvaserveri kohta:

1. Failis **/usr/share/xroad/scripts/\_restore\_xroad.sh** pannakse taastamine ebaõnnestuma kohe pärast pre-restore backupi ehitamist, nt:

...

stop\_services

create\_pre\_restore\_backup

# XXX

echo "Unexpected interruption"

exit 2

restore\_configuration\_files

restore\_database

...

1. Taastatakse keskserver mõnest varundusfailist, nt:

usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i "AA" -f /var/lib/xroad/backup/conf\_backup\_20151106-113259.tar

1. Tehakse fail **/usr/share/xroad/scripts/\_restore\_xroad.sh** jälle korda.
2. Taastatakse konfiguratsioon prerestore backupist:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i "AA" -f /var/lib/xroad/conf\_prerestore\_backup.tar

1. Veendutakse, et taastamine õnnestub, näide skripti väljundi lõpust:

...

etc/nginx/sites-enabled/

var/lib/xroad/dbdump.dat

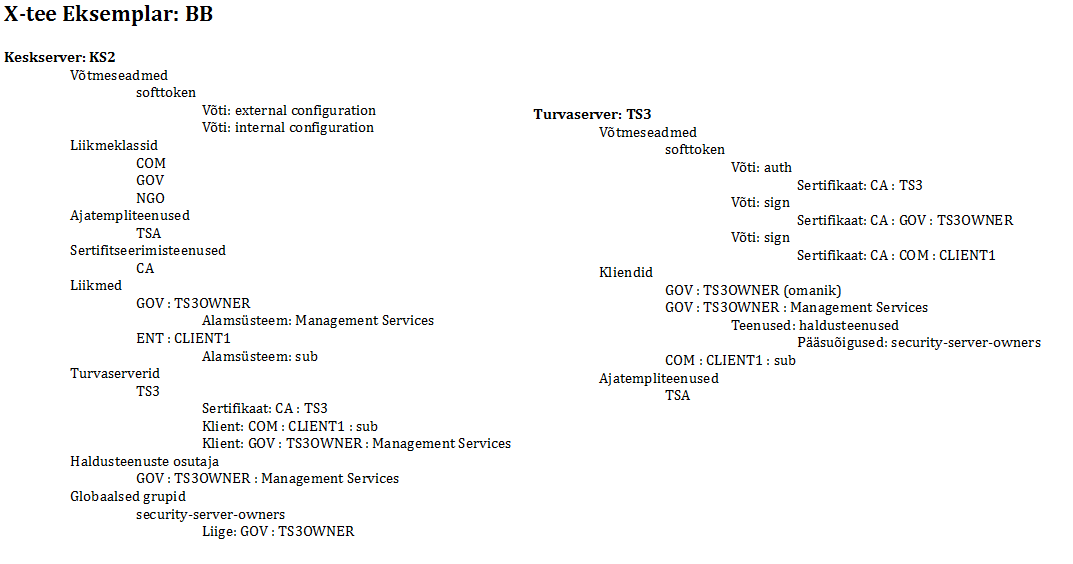
RESTORING DATABASE FROM /var/lib/xroad/dbdump.dat

RESTARTING SERVICES

xroad-signer start/pre-start, process 26945

## Föderatsiooni tugi

Siin testitakse kahe X-tee eksemplari födereerumist ja päringute vahendamist födereerunud keskkonnas. Ettevalmistusena testideks seadistatakse teine X-tee eksemplar (selle peatüki kolme esimese stsenaariumi käigus) järgmise ülesehitusega:



### Teststsenaarium: X-tee eksemplari BB keskserveri paigaldamine ja esialgne seadistamine

Testi käigus kasutatavad ressursid:

* Keskserver KS2

Teststsenaarium:

1. Paigaldatakse keskserveri pakid.
2. Initsialiseeritakse keskserver (vt Veaolukorrad: keskserveri initsialiseerimine):
   * seadistatakse keskserveri aadress ja eksemplari identifikaator: **BB**;
   * initsialiseeritakse tarkvaraline võtmeseade: **PIN = 1234**.
3. Seadistatakse liikmeklassid (vt Veaolukorrad: liikmeklasside seadistamine):
   * code: **GOV**, description: **Government organization**
   * code: **COM**, description: **Commercial enterprise**
   * code: **NGO**, description: **Non-governmental organization**
4. Seadistatakse sertifitseerimis- ja ajatempliteenused.
5. Konfiguratsiooniallikatele (nii sisemisele kui välimisele) genereeritakse võtmed:
   * **sisemise konfiguratsiooniallika** võti genereeritakse **tarkvaralisele** seadmele
   * **välise konfiguratsiooniallika** võti genereeritakse **tarkvaralisele** seadmele
6. Veendutakse, et:
   * allkirjavõti seatakse automaatselt aktiivseks, st kuvatakse tabelis rasvases kirjas
   * allkirjavõtme lisamisele järgnevalt genereeritakse automaatselt konfiguratsiooniallika ankur
7. Eksporditakse konfiguratsiooniallikate ankrud.
8. X-tee liikmeks lisatakse: Name: **TS3 Owner**, Class: **GOV**, Code: **TS3OWNER**
9. X-tee liikmele **TS3OWNER** lisatakse alamsüsteem **Management Services**.
10. Seadistatakse haldusteenused - haldusteenuste osutajaks määratakse alamsüsteem **TS3OWNER:Management Services.**

Testi lõpuks, keskserveris

* ei tohi UI kuvada ühtegi globaalset veateadet (ühe minuti jooksul peale haldusteenuste osutaja seadistamist võib UI veel globaalseid veateateid kuvada, kuna konfiguratsiooni genereerimine toimub kord minutis);
* seadistatud peab olema vähemalt üks sertifitseerimisteenus ja vähemalt üks ajatempliteenus;
* sisemine (internal) konfiguratsiooniankur peab olema alla laetud;
* **TS3OWNER** peab olema X-tee liikmete nimekirjas ja **TS3OWNER:Management Services** seadistatud haldusteenuste osutajaks;
* Haldusteenuste vaates „Management Services' Security Server” välja väärtusena kuvatakse nuppu „Register”, kuna **TS3OWNER:Management Services** pole ühegi turvaserveri omanik ega klient.

### Teststsenaarium: Haldusteenuste turvaserveri TS3 paigaldamine, seadistamine ja registreerimine

Testi käigus kasutatavad ressursid:

* Keskserver KS2
* Turvaserver TS3

Teststsenaarium:

1. Paigaldatakse turvaserveri pakid.
2. Laetakse üles keskserverist KS2 alla laetud sisemine konfiguratsiooniankur (vt Veaolukorrad: konfiguratsiooniankru üleslaadimine).
3. Initsialiseeritakse turvaserver (vt Veaolukorrad: Turvaserveri initsialiseerimine):
   * seadistatakse turvaserveri kood: **TS3**,
   * turvaserveri omanik: Class: **GOV**; Code: **TS3OWNER**,
     + Kuna TS3OWNER on KSis X-tee liikmeks registreeritud, peab klassi ja koodi täitumisel automaatselt täituma nime väli; lisaks peab koodi sisestamisel töötama autocomplete.
   * initsialiseeritakse tarkvaraline võtmeseade: PIN = **1234**.
4. Seadistatakse **ajatempliteenus**.
5. Seadistatakse omaniku allkirjasertifikaat, **allkirjavõti** genereeritakse **tarkvaralisele** seadmele (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
6. Seadistatakse (vt Abistsenaarium: Turvaserveri sertifitseerimine) ja aktiveeritakse autentimissertifikaat.
7. Autentimissertifikaat registreeritakse keskserveris, selleks:
   * saadetakse turvaserverist autentimissertifikaadi registreerimistaotlus ja
   * lisatakse keskserveris **KS2** liikmele **TS3OWNER** turvaserver **TS3**
8. Keskserveris KS2 lisatakse haldusteenuste osutaja **TS3OWNER:Management Services** turvaserveri TS3 kliendiks:
   * Haldusteenuste vaates klõpsatakse „Management Services' Security Server” välja väärtusena kuvatavat nuppu „Register”, sisestatakse turvaserveri TS3 andmed ja klõpsatakse "Submit".
   * Veendutakse, et keskserveris KS2 ilmub peamenüü "Management Requests" vaatesse, TS3 ja TS3OWNER "Management Requests" tab'i taotlus tüübiga "Client registration", mille "Comments" väljas sisaldub "Management service provider registration" ja status on "APPROVED".
9. Turvaserveris TS3 lisatakse **TS3OWNER:Management Services** turvaserveri kliendiks.
10. Turvaserveris TS3 seadistatakse alamsüsteemile **TS3OWNER:Management Services** haldusteenused (WSDL aadressi ja teenuste aadressi saab KS2 -> System settings -> management services):
    * lisatakse ja aktiveeritakse WSDL,
    * muudetakse teenuste aadress õigeks,
    * antakse teenuste pääsuõigused globaalsele grupile "**security-server-owners**".

Testi lõpuks, turvaserveris

* ei tohi turvaserveri UI kuvada ühtegi globaalset veateadet;
* turvaserveri omaniku (TS3OWNER) allkirjasertifikaat peab olema olekus: status = "registered", OCSP response = "good";
* autentimissertifikaat peab olema olekus: status = "registered", ocsp response = "good";
* System Parameters vaates peab olemas olema konfiguratsiooniankur ja ajatempliteenus;
* **TS3OWNER** peab klientide tabelis olema olekus "registered", vastav rida peab olema kuvatud rasvases kirjas;
* **TS3OWNER:Management Services** peab klientide tabelis olema olekus "registered".
* **TS3OWNER:Management Services** details -> services vaates peab olemas olema (mitte-"disabled"-olekus) haldusteenuste WSDL, milles sisalduvate teenuste aadress peab olema korrektselt seadistatud
* **TS3OWNER:Management Services** details -> service clients vaates peab olemas olema globaalne grupp "security-server-owners", kellele on antud pääsuõigused kõikidele haldusteenuste WSDLis sisalduvatele teenustele.

### Teststsenaarium: Kliendi registreerimine turvaserverisse TS3

Testi käigus kasutatavad ressursid:

* Keskserver KS2
* Turvaserver TS3

Teststsenaarium:

1. Keskserveris lisatakse liige: Name: **Client One**; Class: **COM**; Code: **CLIENT1**
2. Turvaserveris **TS3** lisatakse kliendiks **CLIENT1** **alamsüsteem "sub"**, otsides CLIENT1 globaalsest nimekirjast ja kirjutades alamsüsteemi koodi käsitsi juurde. Turvaserverist saadetakse keskserverisse kliendi registreerimistaotlus.
   * lisatud klient peab klientide nimekirja ilmuma olekus "registration in progress"
   * taotluse saatmisel hoiatatakse kasutajat, et liikmele CLIENT1 registreeritakse uus alamsüsteem "sub".
   * keskserveris peab lisatud taotlus ilmuma turvaserveri, liikme ja üldisesse haldustaotluste nimekirja olekus "waiting"
3. Turvaserveris **TS3** sertifitseeritakse **CLIENT1** (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
4. Keskserveris vormistatakse liikme **CLIENT1 alamsüsteemi "sub"** turvaserveri **TS3** kliendiks registreerimise taotlus.
   * keskserveris peavad kliendi registreerimise kaastaotlused olema turvaserveri, liikme ja üldises haldustaotluste nimekirja olekus "submitted for approval"
5. Keskserveris kinnitatakse lisatud registreerimistaotlused.

Testi lõpuks:

* Keskserveris peab liikmete nimekirjas olemas olema CLIENT1 ja tema detailandmete tabis "subsystems" peab kuvatama alamsüsteemi "sub" seotuna turvaserveriga TS3.
* Keskserveris peab turvaserveri TS3 detailandmete "Clients" tabis kuvatama klienti: CLIENT1:sub.
* Keskserveris peavad CLIENT1, TS3 ja üldises haldustaotluste nimekirjas olema kliendi registreerimistaotlused olekus "approved".
* Turvaserveris TS3 peab klientide nimekirjas olemas olema CLIENT1:sub, olekus "registered".
* Turvaserveris TS3 peab võtmete ja sertifikaatide tabelis peab olemas olema CLIENT1 sertifikaat olekus status: "registered", OCSP response: "good".

### Teststsenaarium: Föderatsiooni seadistamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS2

Teststsenaarium:

1. Keskserveritest KS1 ja KS2 laetakse alla välised konfiguratsiooniankrud.
2. Keskserverisse KS1 laetakse üles eksemplari BB väline konfiguratsiooniankur ja keskserverisse KS2 laetakse üles eksemplari AA väline konfiguratsiooniankur (vt Veaolukorrad: usaldatud ankru üleslaadimine).

Testi lõpus:

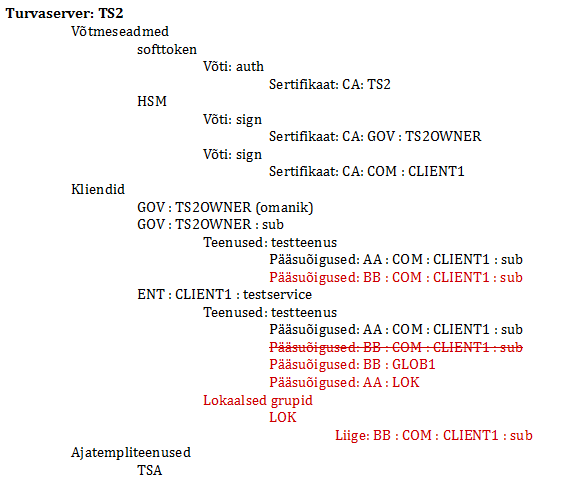
* Keskserveris KS1 kuvatakse usaldatud ankrute vaates instantsi BB ankru andmeid.
* Keskserveris KS2 kuvatakse usaldatud ankrute vaates instantsi AA ankru andmeid.

#### Veaolukorrad: usaldatud ankru üleslaadimine

* Proovitakse laadida üles faili, mis ei ole XML – veateade: „Failed to upload trusted anchor: incorrect file structure“.
* Proovitakse laadida üles XML faili, mis ei ole konfiguratsiooniankur – veateade: „Failed to upload trusted anchor: incorrect file structure".
* Proovitakse üles laadida oma instantsi ankrut – veateade: „Failed to upload trusted anchor: anchors originating from this instance are not supported as trusted anchors“.

### Teststsenaarium: Päringute vahendamine X-tee eksemplaride vahel

Testitakse teise eksemplari kuuluvale kliendile pääsuõiguste andmist ja eksemplaridevahelist teenuste kasutamist. Testi jooksul muutub turvaserveri TS2 konfiguratsioon järgmiselt (muutused punasega).



Testi käigus kasutatavad ressursid:

* Turvaserver TS2
* Keskserver KS2
* Testklient

Teststsenaarium:

1. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päringud **AA:COM:CLIENT1:testservice** ja **AA:GOV:TS2OWNER:sub** poolt osutatavatele testteenustele. Päringud peavad ebaõnnestuma.
2. Turvaserveris **AA:TS2** antakse klientide **AA:COM:CLIENT1:testservice** ja **AA:GOV:TS2OWNER:sub** poolt osutatavate testteenuse pääsuõigused kliendile **BB:COM:CLIENT1:sub**.
3. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päringud **AA:COM:CLIENT1:testservice** ja **AA:GOV:TS2OWNER:sub** poolt osutatavatele testteenustele. Päringud peavad õnnestuma.
4. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring kesksele teenusele **AA:random**. Päring peab õnnestuma.
5. Keskserveris KS2 lisatakse globaalne grupp **GLOB1**.
6. Keskserveris KS2 lisatakse **TS3OWNER:Management Services** globaalsesse gruppi **GLOB1**.
7. Turvaserveris **AA:TS2** antakse kliendi **AA:COM:CLIENT1:testservice** poolt osutatava testteenuse pääsuõigus globaalsele grupile **BB:GLOB1**
8. Turvaserverist **BB:TS3** tehakse kliendiga **BB:GOV:TS3OWNER:Management Services**  päring **AA:COM:CLIENT1:testservice** poolt osutatavale testteenusele. Päring peab õnnestuma.
9. Turvaserveris **AA:TS2** eemaldatakse kliendi **AA:COM:CLIENT1:testservice** poolt osutatava testteenuse pääsuõigus kliendilt **BB:COM:CLIENT1:sub**.
10. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab ebaõnnestuma.
11. Turvaserveris **AA:TS2** luuakse kliendile **AA:COM:CLIENT1:testservice** lokaalne grupp **LOK**, kuhu lisatakse klient **BB:COM:CLIENT1:sub**.
12. Turvaserveris **AA:TS2** antakse kliendi **AA:COM:CLIENT1:testservice** poolt osutatava testteenuse pääsuõigus lokaalsele grupile **AA:LOK**.
13. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.

### Teststsenaarium: Sisemise konfiguratsiooni signeerimisvõtme vahetamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS2
* Turvaserver TS1
* Testklient

Teststsenaarium:

1. Keskserveris **AA:KS1** genereeritakse sisemisele (internal) konfiguratsioonile **HSM'**i peale uus võti.
   * peale uue võtme genereerimist genereeritakse automaatselt uus sisemine konfiguratsiooniankur, mis sisaldab nii uue kui vana võtme avalikku võtit. Välimine konfiguratsiooniankur jääb samaks.
   * kuna aktiveeritud võti on olemas, siis äsja genereeritud võtit automaatselt ei aktiveerita.
2. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
3. Keskserveris **AA:KS1** laetakse alla sisemine konfiguratsiooniankur.
4. Turvaserverisse **AA:TS2** laetakse üles keskserverist alla laetud ankur.
   * turvaserverisse **AA:TS1** uut ankrut üles ei laeta (testime mis juhtub, kui turvaserveris ebaõnnestub alla laetava konfiguratsiooni verifitseerimine seni, kuni olemasolev konfiguratsioon aegub).
5. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
6. Keskserveris **AA:KS1** aktiveeritakse uus sisemise konfiguratsiooni allkirjastamisvõti.
7. Keskserveris **AA:KS1** kustutatakse vana sisemise konfiguratsiooni allkirjastamisvõti.
   * peale võtme kustutamist genereeritakse automaatselt sisemine konfiguratsiooniankur, mis sisaldab ainult uue võtme avalikku võtit.
8. Keskserveris **AA:KS1** laetakse alla sisemine konfiguratsiooniankur.
9. Turvaserverisse **AA:TS2** laetakse üles keskserverist alla laetud ankur.
10. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
11. Kui **AA:TS1** on konfiguratsioon aegunud (~10 minutit peale keskserveris uue võtme aktiveerimist, kasutajaliideses kuvatakse globaalset veateadet "Global configuration is expired"), tehakse turvaserverist **AA:TS1** kliendiga **AA:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab ebaõnnestuma.
    * Konfiguratsiooni kehtivus on määratud keskserveri süsteemse parameetriga "confExpireIntervalSeconds", mille vaikeväärtuseks on 600. Testimise kiirendamiseks võib vaikeväärtust muuta, sisestades keskserveri KS1 andmebaasi tabelisse "system\_parameters" võtme "confExpireIntervalSeconds" soovitud väärtusega.

### Teststsenaarium: Välimise konfiguratsiooni signeerimisvõtme vahetamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS2
* Testklient

Teststsenaarium:

1. Keskserveris **AA:KS1** genereeritakse välisele (external) konfiguratsioonile (tarkvaralisele võtmeseadmele) uus võti.
   * peale uue võtme genereerimist genereeritakse automaatselt uus väline konfiguratsiooniankur, mis sisaldab nii uue kui vana võtme avalikku võtit. Sisemine konfiguratsiooniankur jääb samaks.
   * kuna aktiveeritud võti on olemas, siis äsja genereeritud võtit automaatselt ei aktiveerita.
2. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
3. Keskserveris **AA:KS1** laetakse alla väline konfiguratsiooniankur.
4. Keskserverisse **BB:KS2** laetakse üles keskserverist **AA:KS1** alla laetud ankur.
5. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
6. Keskserveris **AA:KS1** aktiveeritakse uus välise konfiguratsiooni allkirjastamisvõti.
7. Keskserveris **AA:KS1** kustutatakse vana välise konfiguratsiooni allkirjastamisvõti.
   * peale võtme kustutamist genereeritakse automaatselt väline konfiguratsiooniankur, mis sisaldab ainult uue võtme avalikku võtit.
8. Keskserveris **AA:KS1** laetakse alla väline konfiguratsiooniankur.
9. Keskserverisse **BB:KS2** laetakse üles keskserverist **AA:KS1** alla laetud ankur.
10. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
    * Turvaserverist **BB:TS3** võib instantsi AA konfiguratsiooni allalaadimise ja verifitseerimise õnnestumist kontrollida logist /var/log/xroad/configuration\_client.log.

### Teststsenaarium: Föderatsiooni lõpetamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS2

Teststsenaarium:

1. Keskserverid KS1 ja KS2 varundatakse (vt Abistsenaarium: Serveri varundamine ja taastamine).
2. Keskserveris **AA:KS1** kustutatakse instantsi BB usaldatud ankur.
3. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab ebaõnnestuma.
4. Keskserver **AA:KS1** taastatakse.
5. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
6. Keskserveris **BB:KS2** kustutatakse instantsi AA usaldatud ankur.
7. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab ebaõnnestuma.
8. Keskserver **BB:KS2** taastatakse.
9. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.

### Teststsenaarium: Konfiguratsioonivahendaja kasutamine

Testi käigus kasutatavad ressursid:

* Konfiguratsioonivahendaja
* Keskserver KS1
* Keskserver KS2

Teststsenaarium:

1. Paigaldatakse konfiguratsioonivahendaja.
2. Initsialiseeritakse tarkvaraline võtmeseade (vt. Veaolukorrad: Initsialiseerimine ):

signer-console init-software-token, signer-console login-token 0

1. Seadistatakse üldised parameetrid (serveri aadress).
2. Luuakse kaks konfiguratsioonivahendaja eksemplari (vt. Veaolukorrad: Eksemplaride loomine): **AA-ext** ja **BB-ext** (confproxy-create-instance)
3. Konfiguratsioonivahendaja eksemplarides **AA-ext** ja **BB-ext** seadistatakse konfiguratsiooni vahendamine (vt. Veaolukorrad: Eksemplaride seadistamine).
   1. Genereeritakse konfiguratsiooni signeerimise võtmed (confproxy-add-signing-key).
      * Genereeritud võtmed võetakse automaatselt kasutusele.
   2. Laaditakse üles vastavate konfiguratsiooniallikate välised konfiguratsiooniankrud.
      * Konfiguratsiooni vaatamine (confproxy-view-conf) peab näitama, et kõik on OK.
   3. Eksporditakse konfiguratsioonivahendaja eksemplaride konfiguratsiooniankrud (confproxy-generate-anchor).
   4. Testitakse konfiguratsioonivahendajast konfiguratsiooni tõmbamist (download\_instance\_configuration.sh).
      * Konfiguratsiooni tõmbamine peab õnnestuma.
4. Keskserverisse **KS1** laetakse üles konfiguratsioonivahendaja eksemplari **BB-ext** konfiguratsiooniankur ja keskserverisse **KS2** laetakse üles konfiguratsioonivahendaja eksemplari **AA-ext** konfiguratsiooniankur
5. Testitakse päringute tegemist (vt Teststsenaarium: Päringute vahendamine X-tee eksemplaride vahel).
   * Päringute vahendamine peab töötama nii nagu enne konfiguratsioonivahendaja kasutusele võtmist.
6. Testitakse metateenuseid (vt Metateenuste kasutamine).
   * Metateenused peavad töötama nii nagu enne konfiguratsioonivahendaja kasutusele võtmist.

#### Veaolukorrad: Initsialiseerimine

1. Sisestatakse kaks erinevat PIN-koodi -- veateade.
2. Võtmeseadmesse sisselogimisel sisestatakse vale PIN -- veateade.

#### Veaolukorrad: Eksemplaride loomine

1. Üritatakse luua kaks korda järjest sama eksemplari -- veateade.

#### Veaolukorrad: Eksemplaride seadistamine

1. Võtme genereerimisel antakse ette vale võtmeseadme ID -- veateade.
2. Enne võtme genereerimist logitakse võtmeseadmest välja -- veateade.

## Teenusepakkuja turvaserveri dubleerimine

Testitakse päringu tegemist klastrisse ühendatud teenusepakkuja turvaserveritesse.

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1
* Turvaserver TS2
* Testklient

Teststsenaarium:

1. Turvaserverisse **TS1** registreeritakse klient **CLIENT1:testservice**, selleks

* lisatakse turvaserverisse klient CLIENT1:testservice,
* esitatakse turvaserverist kliendi registreerimistaotlus,
* vormistatakse keskserveris KS1 kliendi turvaserverisse lisamise taotlus,
* kinnitatakse keskserveris esitatud taotlused.

1. **TS1** kliendile **CLIENT1:testservice** seadistatakse testteenus ja anna testteenuse pääsuõigus kliendile **BB:COM:CLIENT1:sub.**
2. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
3. Turvaserveris **TS1** tekitatakse tõrge (nt sisesta käsk sudo service xroad-proxy stop).
4. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
5. Turvaserveris **TS1** taastatakse normaalne töö (nt sisesta käsk sudo service xroad-proxy start).
6. Turvaserveris **TS2** tekitatakse tõrge.
7. Turvaserverist **BB:TS3** tehakse kliendiga **BB:COM:CLIENT1:sub** päring **AA:COM:CLIENT1:testservice** poolt osutatavatele testteenustele. Päring peab õnnestuma.
8. Turvaserveris **TS2** taastatakse normaalne töö.

## Kasutajate haldus ning eri rollides kasutajate õigused turvaserveris ja keskserveris

Testitakse kasutajate haldust turvaserveris ja keskserveris.

* Keskserveri rollide kirjeldus: Cybernetica AS. X-tee keskserveri kasutajarollid. Dokumendi tähis Y-742-18.
* Turvaserveri rollide kirjeldus: Cybernetica AS. X-tee turvaserveri kasutajarollid. Dokumendi tähis Y-742-17.

Mõlemal juhul testimiseks:

1. Defineeritakse kasutajad, kellest igaühel on täpselt üks roll:

* KS-s: registreerimishaldur, süsteemiadministraator, turvahaldur.
* TS-s: turvahaldur, registreerimishaldur, teenusehaldur, süsteemiadministraator.

1. Logitakse erinevate kasutajate alt sisse kasutajaliidesesse ning kontrollitakse, et neile on kättesaadavad rollile vastavad toimingud.

## Metateenuste kasutamine

Testitakse kõikide metateenuste kasutamist turvaserveris TS1. Metateenuste päringud on kirjeldatud dokumendis: Cybernetica AS. X-Road: Service Metadata Protocol. Dokumendi tähis PR-META. Päringud esitatakse curl'iga.

1. Esitatakse metapäring potentsiaalsete teenusepakkujate nimekirja saamiseks:
   * Sama X-tee eksemplar: HTTP GET päring URLile <http://TS1/listClients>
   * Teine X-tee eksemplar: HTTP GET päring URLile [http://TS1/listClients?xRoadInstance=BB](http://TS1/listClients?instance=BB)
2. Esitatakse metapäring kesksete teenuste nimekirja saamiseks:
   * Sama X-tee eksemplar: HTTP GET päring URLile <http://TS1/listCentralServices>
   * Teine X-tee eksemplar: HTTP GET päring URLile [http://TS1/listCentralServices?xRoadInstance=BB](http://TS1/listCentralServices?instance=BB)
3. Esitatakse metapäring (listMethods) kõigi teenuste nimekirja saamiseks:
   * kliendilt AA:COM:CLIENT1:sub kliendile AA:COM:CLIENT1:testservice.
   * kliendilt BB:COM:CLIENT1:sub kliendile AA:COM:CLIENT1:testservice.
4. Esitatakse metapäring (allowedMethods) kõigi lubatud teenuste nimekirja saamiseks:
   * kliendilt AA:COM:CLIENT1:sub kliendile AA:COM:CLIENT1:testservice.
   * kliendilt BB:COM:CLIENT1:sub kliendile AA:COM:CLIENT1:testservice.
5. Esitatakse metapäring teenuse WSDLi saamiseks turvaserverist TS1 kliendile TS2OWNER:sub (HTTP GET päring URLile <http://TS1/wsdl?xRoadInstance=AA&memberClass=GOV&memberCode=TS2OWNER&subsystemCode=sub&serviceCode=xroadGetRandom&version=v1>).

## Keskserveri andmebaasi kirjete versioneerimine

Keskserveri andmebaasi centerui\_production tabelid (va distributed\_files ja schema\_migrations) on versioneeritud. Andmebaasi kirjete versioneerimiseks on lisatud andmebaasi juurde eraldi tabel **history**. See võimaldab hiljem tuvastada, milline kasutaja milliseid muudatusi tegi. Keskserveri UI kaudu ajaloo toega tabelitesse kirjete lisamisel, nende muutmisel ja kustutamisel peavad **history** tabelisse tekkima ootuspärased kirjed:

* INSERT korral lisatud kirje iga välja kohta üks rida;
* UPDATE korral muudetud kirje iga muutunud välja kohta üks rida;
* DELETE korral kustutatud tabeli iga välja kohta üks rida;
* Lisaks kui ühe tabeli muutmisest on mõjutatud teised tabelid, kajastuvad ka nendes toimunud muutused ajalootabelis.

Andmebaasiga centerui\_production ühendumiseks antakse keskserveris käsureal järgmine käsk:

psql -h 127.0.0.1 -U centerui centerui\_production

Parool: centerui

Testi käigus kasutatavad ressursid:

* Keskserver KS1

### Teststsenaarium: andmebaasikirjete muutmine kasutajaliidese kaudu

1. Keskserverisse lisatakse 3 uut kasutajat: user1, user2 ja user3 (adduser user1).
2. Kõigile lisatud kasutajatele antakse registreerimishalduri õigused (adduser user1 xroad-registration-officer).
3. Logitakse keskserveri kasutajaliidesesse sisse kasutajana user1.
4. X-tee liikmeks lisatakse: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2.**
5. Logitakse keskserveri kasutajaliidesest välja ning logitakse sisse kasutajana user2.
6. Muudetakse liikme **CLIENT2** nime Member name: **Client 2**.
7. Logitakse keskserveri kasutajaliidesest välja ning logitakse sisse kasutajana user3.
8. Kustutatakse keskserverist liige **CLIENT2**.
9. Ühendutakse andmebaasiga centerui\_production ning veendutakse, et tabelisse **history** on tekkinud korrektse ajatempliga järgmise kirjed:
   * Kirjed kasutajanimega **user1** tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names andmete lisamise ja muutmise kohta.
   * Kirjed kasutajanimega **user2** tabelites security\_server\_clients ja security\_server\_client\_names andmete muutmise kohta.
   * Kirjed kasutajanimega **user3** tabelitest security\_server\_clients, identifiers ja security\_server\_client\_names andmete kustutamise kohta.

### Teststsenaarium: andmebaasikirjete muutmine Postgresi käsurealt

1. Muudetakse Postgresi käsurealt andmeid ajalootoega tabelis, näiteks sisestatakse käsk "update system\_parameters set value = 600 where key ='ocspFreshnessSeconds';".
2. Veendutakse, et **history** tabelisse tekib tehtud muudatuse kohta kirje, mille kasutajanime väljas on nimi "centerui".

### Teststsenaarium: andmebaasikirjete muutmine ajalootoeta tabelites

Testitakse, et ajalookirjeid ei teki nende tabelitega seoses, mis on ajalootabeli toest välja jäetud (distributed\_files ja schema\_migrations).

1. Veendutakse, et distributed\_files tabelit uuendab süsteem iga kahe minuti tagant, kuid ajalootabelisse selle kohta kirjeid ei teki. Postgresi käsureal sisestatakse käsk "select file\_updated\_at from distributed\_files;", paari minuti pärast sisestatakse sama käsk uuesti ning veendutakse, et faili muutmise aeg on muutunud.
2. Veendutakse, et **history** tabelisse ei tekkinud distributed\_files tabelis tehtud muudatuse kohta kirjeid.

### Teststsenaarium: ajalootabeli toe säilimine peale keskserveri taastamist

1. Keskserver varundatakse ja taastatakse (vt Abistsenaarium: Serveri varundamine ja taastamine).
2. Logitakse keskserveri kasutajaliidesesse sisse kasutajana user1.
3. X-tee liikmeks lisatakse: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2**
4. Ühendutakse andmebaasiga centerui\_production ning veendutakse, et tabelisse **history** on tekkinud korrektse ajatempliga kirjed kasutajanimega **user1** tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names andmete lisamise ja muutmise kohta.

## Turvaserveri andmebaasi kirjete versioneerimine

Turvaserveri andmebaasi serverconf tabelid on versioneeritud. Andmebaasi kirjete versioneerimiseks on lisatud andmebaasi juurde eraldi tabel **history**. See võimaldab hiljem tuvastada, milline kasutaja milliseid muudatusi tegi. Turvaserveri UI kaudu ajaloo toega tabelitesse kirjete lisamisel, nende muutmisel ja kustutamisel peavad **history** tabelisse tekkima ootuspärased kirjed:

* INSERT korral lisatud kirje iga välja kohta üks rida;
* UPDATE korral muudetud kirje iga muutunud välja kohta üks rida;
* DELETE korral kustutatud tabeli iga välja kohta üks rida;
* Lisaks kui ühe tabeli muutmisest on mõjutatud teised tabelid, kajastuvad ka nendes toimunud muutused ajalootabelis.

Andmebaasiga serverconf ühendumiseks antakse turvaserveris käsureal järgmine käsk:

psql -h 127.0.0.1 -U serverconf serverconf

Parool: serverconf

Testi käigus kasutatavad ressursid:

* Turvaserver TS1

### Teststsenaarium: andmebaasikirjete muutmine kasutajaliidese kaudu

1. Turvaserverisse lisatakse 3 uut kasutajat: user1, user2 ja user3 (adduser user1).
2. Kõigile lisatud kasutajatele antakse registreerimishalduri õigused (adduser user1 xroad-registration-officer).
3. Logitakse turvaserveri kasutajaliidesesse sisse kasutajana user1.
4. Turvaserveris lisatakse kliendiks **CLIENT1 alamsüsteem "sub2"**. Turvaserverist keskserverisse kliendi registreerimistaotlust ei saadeta.
5. Logitakse turvaserveri kasutajaliidesest välja ning logitakse sisse kasutajana user2.
6. Kliendi CLIENT1:sub2 ühenduseks seadistatakse HTTPS (Security Server Clients -> Internal Servers).
7. Logitakse turvaserveri kasutajaliidesest välja ning logitakse sisse kasutajana user3.
8. Kustutatakse turvaserverist klient **CLIENT1:sub2**.
9. Ühendutakse andmebaasiga serverconf ning veendutakse et tabelisse **history** on tekkinud korrektse ajatempliga järgmise kirjed:
   * Kirjed kasutajanimega **user1** tabelitesse client ja identifier andmete lisamise kohta.
   * Kirje kasutajanimega **user2** tabelis client andmete muutmise kohta.
   * Kirjed kasutajanimega **user3** tabelist client andmete kustutamise kohta.

### Teststsenaarium: andmebaasikirjete muutmine Postgresi käsurealt

1. Muudetakse Postgresi käsurealt andmeid ajalootoega tabelis, näiteks sisestatakse käsk "update localgroup set updated = now() where id = 11;".
2. Veendutakse, et **history** tabelisse tekib tehtud muudatuse kohta kirje, mille kasutajanime väljas on nimi "serverconf".

### Teststsenaarium: ajalootabeli toe säilimine peale turvaserveri taastamist

1. Turvaserver varundatakse ja taastatakse (vt Abistsenaarium: Serveri varundamine ja taastamine).
2. Logitakse turvaserveri kasutajaliidesesse sisse kasutajana user1.
3. Turvaserveris lisatakse kliendiks **CLIENT1 alamsüsteem "sub2"**. Turvaserverist keskserverisse kliendi registreerimistaotlust ei saadeta.
4. Ühendutakse andmebaasiga serverconf ning veendutakse, et tabelisse **history** on tekkinud korrektse ajatempliga kirjed kasutajanimega **user1** tabelisse client andmete lisamise kohta.

## Halduslogimine

Testitakse haldustegevuste logimist. Haldustegevusena käsitletakse kasutajaliidese vahendusel tehtavaid andministreerimistegevusi, mis muudavad serveri olekut. Haldustegevusi logitakse turvaserveris ja keskserveris.

### Haldustegevuste logimine keskserveris

Testi käigus kasutatavad ressursid:

* Keskserver KS1

Teststsenaarium:

1. Logitakse keskserveri kasutajaliidesesse sisse kasutajana user1.
2. X-tee liikmeks lisatakse: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2**.
3. Liikmele **CLIENT2** lisatakse alamsüsteem **sub**.
4. Muudetakse liikme **CLIENT2** nime, Member name jäetakse tühjaks. Nime muutmine peab ebaõnnestuma veateatega: "Missing parameter: memberName".
5. Muudetakse liikme **CLIENT2** nime, Member name: **Client 2**.
6. Logitakse keskserveri kasutajaliidesest välja ning logitakse sisse kasutajana user2.
7. Proovitakse lisada uus globaalne grupp, grupi lisamisel jäetakse tühjaks "Code" ja/või "Description" väli. Grupi lisamine peab ebaõnnestuma.
8. Lisatakse uus globaalne grupp **GLOB1**.
9. **CLIENT2:sub** lisatakse grupi **GLOB1** liikmeks.
10. Vormistatakse alamsüsteemi **CLIENT2:sub** turvaserverisse TS1 registreerimise taotlus.
11. Logitakse keskserveri kasutajaliidesest välja ning logitakse sisse kasutajana user3.
12. Tühistatakse alamsüsteemi **CLIENT2:sub** turvaserverisse TS1 registreerimise taotlus.
13. Kustutatakse keskserverist liige **CLIENT2**.
14. Veendutakse, et halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Center UI* kirjed teostatud tegevuste kohta:
    * Kirjed kasutajanimega **user1** liikme CLIENT2 lisamise, alamsüsteemi lisamise ja nime muutmise kohta.
    * Kirje kasutajanimega **user1** liikme CLIENT2 nime muutmise nurjumise kohta.
    * Kirje kasutajanimega **user2** globaalse grupi lisamise nurjumise kohta.
    * Kirjed kasutajanimega **user2** globaalse grupi GLOB1 loomise ja CLIENT2:sub grupi liikmeks lisamise ning CLIENT2:sub turvaserveri TS1 kliendiks registreerimise taotluse esitamise kohta.
    * Kirjed kasutajanimega **user3** CLIENT2:sub turvaserveri TS1 kliendiks registreerimise taotluse tühistamise ja CLIENT2 kustutamise kohta.
    * Kirjed kasutajate **user1**, **user2** ja **user3** sisse- ja väljalogimise kohta.

### Haldustegevuste logimine turvaserveris

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1

Teststsenaarium:

1. Keskserveris lisatakse uus liige: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2**.
2. Kasutajatele user1, user2 ja user3 antakse turvaserveris TS1 teenusehalduri õigused (adduser user1 xroad-service-administrator).
3. Logitakse turvaserveri kasutajaliidesesse sisse kasutajana user1.
4. Turvaserveris TS1 lisatakse **CLIENT2** **alamsüsteem "sub"** turvaserveri kliendiks ja saadetakse kliendi registreerimistaotlus keskserverisse.
5. Kliendile **CLIENT2:sub** proovitakse lisada lokaalne grupp. Grupi lisamisel jäetakse tühjaks "Code" ja/või "Description" väli. Grupi lisamine peab ebaõnnestuma.
6. Logitakse turvaserveri kasutajaliidesest välja ning logitakse sisse kasutajana user2.
7. Seadistatakse **CLIENT2** allkirjasertifikaat (vt Abistsenaarium: Turvaserveri kliendi sertifitseerimine)
8. Logitakse turvaserveri kasutajaliidesest välja ning logitakse sisse kasutajana user3.
9. Kliendile **CLIENT2:sub** proovitakse lisada WSDL-i aadress, mis ei viita WSDLile. WSDL-i lisamine peab ebaõnnestuma.
10. Kliendile **CLIENT2:sub** lisatakse test-teenuse WSDL.
11. Seadistatakse test-teenuse parameetrid.
12. Seadistatakse test-teenuse pääsuõigused (vt Abistsenaarium: Pääsuõiguse andmine teenuse vaatest) - pääsuõigus antakse kliendile **CLIENT1:sub.**
13. Test-teenuse WSDL aktiveeritakse.
14. Veendutakse, et halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Proxy UI* kirjed teostatud tegevuste kohta:
    * Kirjed kasutajanimega **user1** liikme CLIENT2:sub turvaserveri kliendiks lisamise kohta.
    * Kirje kasutajanimega **user1** lokaalse grupi lisamise nurjumise kohta.
    * Kirjed kasutajanimega **user2** allkirjasertifikaadi seadistamise kohta.
    * Kirje kasutajanimega **user3** WSDL-i lisamise nurjumise kohta.
    * Kirjed kasutajanimega **user3** WSDL-i lisamise, test-teenuse seadistamise ja pääsuõiguste andmise kohta.
    * Kirjed kasutajate **user1**, **user2** ja **user3** sisse- ja väljalogimise kohta.

### Haldustegevuste logimine utiliidis signer-console

Testi käigus kasutatavad ressursid:

* Turvaserver TS1

Teststsenaarium:

Vastavalt utiliidi signer-console kasutusjuhendile (Cybernetica AS. Signer-console user`s guide. Dokumendi tähis UG-SC) tehakse turvaserveris TS1 utiliiti kasutades järgmised tegevused:

1. Võtmeseadmele genereeritakse võti.
2. Võtmele määratakse "friendly name".
3. Võtmele genereeritakse allkirjasertifikaadi taotlus. Sertifikaaditaotlus toimetatakse heakskiidetud sertifitseerimisteenuse osutajale ning võetakse vastu sertifikaaditaotluse alusel loodud allkirjasertifikaat.
4. Allkirjasertifikaat imporditakse turvaserverisse.
5. Kustutatakse allkirjasertifikaat.
6. Kustutatakse võti.
7. Veendutakse, et halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega **xroad** ja konteksti nimega *X-Road Signer Console* kirjed teostatud tegevuste kohta.

## Kasutaja sessiooni aegumine keskserveris ja turvaserveris

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1

Teststsenaarium:

1. Keskserveri KS1 kasutajaliideses on sisse loginud kasutaja 30 minutit passiivne.
2. Turvaserveri TS1 kasutajaliideses on sisse loginud kasutaja 30 minutit passiivne.
3. Veendutakse, et nii keskserveri kui turvaserveri kasutajaliideses kuvatakse teadet "Session timed out. Redirecting." ja kasutaja on välja logitud.

## Keskserveri kõrgkäideldavus

Selles peatükis testitakse kõrgkäideldavuse eesmärgil loodud keskserverite klastri kasutamist:

* kahest keskserverist koosneva keskserverite klastri paigaldamist;
* konfiguratsiooni varundamist ja taastamist;
* kõrgkäideldavuse seadistamist ühe keskserveriga X-tee instantsis;
* HA klastri tervisenäitajate vaatamist;
* keskserveri andmebaaside replikeerumist;
* keskserveri aadressi muutmist;
* konfiguratsiooni sisu sõlmele vastavuse kontrollimist;
* haldusteenuste kasutamist;
* mitme konfiguratsiooniallikaga ankrute genereerimist;
* konfiguratsiooniallika kaudu konfiguratsiooni levitamise ajutist katkestamist föderatsioonis;
* mitme konfiguratsiooniallika vahel valimist.

### Terminid ja lühendid

* **HA** - kõrgkäideldavus (*high availability*).
* **Sõlm** - kõrgkäideldavuse eesmärgil moodustatud keskserverite klastrisse kuuluv keskserver.
* **HA klaster** - kõrgkäideldavuse eesmärgil moodustatud keskserverite klaster.
* **Replikeerimine** - andmebaasimuudatuste dubleerimine klastri sõlmedesse.

### Testimise käigus vajalik info

#### Andmebaasiga ühendumine

Keskserveri andmebaasiga centerui\_production ühendumiseks antakse keskserveris käsureal järgmine käsk:

psql -h 127.0.0.1 -U centerui centerui\_production

Parool: centerui

#### Andmebaasiserveri töö peatamine ja taastamine

* Andmebaasiserveri töö peatamiseks antakse keskserveris käsk

service postgresql stop

* Andmebaasiserveri töö taastamiseks antakse keskserveris käsk

service postgresql start

#### iptables kasutamine konfiguratsiooni ligipääsmatuks muutmiseks

* Sõlme konfiguratsiooni ligipääsmatuks tegemiseks antakse serverites, mille jaoks konfiguratsioon ligipääsmatuks soovitakse teha käsk

sudo iptables -A INPUT -s <KS IP-aadress> -j DROP

* Sõlme konfiguratsiooni ligipääsu taastamiseks antakse serverites, mille jaoks konfiguratsiooni ligipääs taastada soovitakse käsk

sudo iptables -D INPUT -s <KS IP-aadress> -j DROP

### Abistsenaariumid

(Kasutatakse teststsenaariumite käigus.)

#### Allalaaditava faili ja baasikirje kokku viimine

Keskserveri UI-d kasutades laetakse alla sisemine ja väline konfiguratsiooniankur.

Ühendutakse KS andmebaasiga ja tehakse päringud, et näha andmebaasis olevaid andmeid konfiguratsiooniankrute kohta (näide sõlme 1 kohta):

**Sisemine konfiguratsiooniankur**:

SELECT anchor\_generated\_at, encode(anchor\_file, 'escape') FROM configuration\_sources WHERE source\_type='internal' AND ha\_node\_name='node\_1' AND anchor\_file\_hash='<UI-s olev ankrufaili räsi>';

**Väline konfiguratsiooniankur**:

SELECT anchor\_generated\_at, encode(anchor\_file, 'escape') FROM configuration\_sources WHERE source\_type='external' AND ha\_node\_name='node\_1' AND anchor\_file\_hash='<UI-s olev ankrufaili räsi>';

Veendutakse, et nii sisemise kui välise konfiguratsiooniankru korral ühtib kodeeritud anchor\_file väärtus UI-st alla laetud faili sisuga ning anchor\_generated\_at ühtib UI-s toodud ankru genereerimise ajaga.

Keskserveri UI-d kasutades laetakse alla failid private-params.xml ja shared-params.xml.

Tehakse päringud, et näha andmebaasis olevaid andmeid antud konfiguratsiooniosade kohta (näide sõlme 1 kohta):

**private-params.xml:**

SELECT file\_updated\_at, encode(file\_data, 'escape') FROM distributed\_files WHERE ha\_node\_name='node\_1' AND content\_identifier='PRIVATE-PARAMETERS';

**shared-params.xml:**

SELECT file\_updated\_at, encode(file\_data, 'escape') FROM distributed\_files WHERE ha\_node\_name='node\_1' AND content\_identifier='SHARED-PARAMETERS';

Veendutakse, et mõlema faili korral ühtib kodeeritud file\_data väärtus UI-st alla laetud faili sisuga ning file\_updated\_at ühtib UI-s toodud konfiguratsiooniosa genereerimise ajaga.

Veendutakse, et kataloogis /etc/xroad/globalconf/<instance identifier>/ asuvate failide private-params.xml ja shared-params.xml sisu ühtib UI-st alla laetud vastavate failide sisuga. Antud kataloogis asuvate failide sisu peab vastama ka /var/lib/xroad/public/<timestamped\_directory>/ asuvate vastava ajatempliga kataloogi failide sisule, st. failide viimase muutmise aeg peab vastama kataloogi nimes toodud ajatemplile (UTC-aeg).

#### Konfiguratsiooniallika verifitseerimissertifikaadi kontrollimine

Leitakse **sisemise konfiguratsiooniankru** allkirjastamisvõtme identifikaator:

SELECT key\_identifier FROM configuration\_signing\_keys

INNER JOIN configuration\_sources

ON configuration\_sources.active\_key\_id=configuration\_signing\_keys.id

WHERE configuration\_sources.source\_type='internal' AND configuration\_sources.ha\_node\_name='<uuritava sõlme nimi>';

Leitakse **välise konfiguratsiooniankru** allkirjastamisvõtme identifikaator:

SELECT key\_identifier FROM configuration\_signing\_keys

INNER JOIN configuration\_sources

ON configuration\_sources.active\_key\_id=configuration\_signing\_keys.id

WHERE configuration\_sources.source\_type='external' AND configuration\_sources.ha\_node\_name='<uuritava sõlme nimi>';

Veendutakse nii sisemise kui välise konfiguratsiooniankru kohta, et tulemuseks saadud allkirjastamisvõtme identifikaator leidub failis /etc/xroad/signer/keyconf.xml ning konfiguratsiooniankrus olev verificationCert väärtus ühtib vastava allkirjastamisvõtme contents väärtusega.

Näide vastavast keyconf.xml lõigust (väärtused lühendatult):

<key usage="SIGNING">

<keyId><allkirjastamisvõtme identifikaator></keyId>

<publicKey>MII...UjQIDAQAB</publicKey>

<cert active="true" id="D8832785A32AC3652839F0AFA86B0A2EC59F6B83">

<memberId ns2:objectType="MEMBER">

<ns2:xRoadInstance>AA</ns2:xRoadInstance>

<ns2:memberClass>selfsigned</ns2:memberClass>

<ns2:memberCode>3306e3ff-1a98-4db5-b732-17223e956511</ns2:memberCode>

</memberId>

<contents>MII...qG0T0fPVyWaA==</contents>

<status>registered</status>

</cert>

</key>

#### Haldusteenuse sertifikaadi väärtuse korrektsuse kontrollimine

Veendutakse, et uuritavas private\_params.xml failis olev authCertRegServiceCert väärtus on sama, mis konkreetses sõlmes asuva faili /etc/xroad/ssl/internal.crt sisu.

#### Konfiguratsiooni verifitseerimine

1. Laetakse konfiguratsioon alla ja salvestatakse kohalikku failisüsteemi.
   * Sisemine konfiguratsioon asub: http://<KS-i aadress>/internalconf.
   * Väline konfiguratsioon asub: http://<KS-i aadress>/externalconf.
2. Välise konfiguratsiooni korral veendutakse, et konfiguratsioon sisaldab täpselt üht konfiguratsiooniosa tüübiga Content-identifier: SHARED-PARAMETERS.
3. Sisemise konfiguratsiooni korral veendutakse, et konfiguratsioon sisaldab konfiguratsiooniosi tüüpidega Content-identifier: SHARED-PARAMETERS ja Content-identifier: PRIVATE-PARAMETERS, kumbagi täpselt üks.
4. Sisemise konfiguratsiooni korral veendutakse, et konfiguratsioon sisaldab konfiguratsiooniosi tüüpidega Content-identifier: CENTRALMONITORAGENTS ja Content-identifier: IDENTIFIERMAPPING, kumbagi täpselt üks.
5. Veendutakse, et Expire-date väljas sisalduv kellaaeg on hilisem konfiguratsiooni allalaadimise ajast (UTC-aeg).
6. Tehakse kindlaks, millisele konfiguratsiooniankrus olevale konfiguratsiooniallika verifitseerimissertifikaadile vastab konfiguratsioonis toodud verifitseerimissertifikaadi räsi.
   * Kuidas: konfiguratsiooniankrus olev kontrollitav verificationCert räsitakse kasutades konfiguratsioonis olevat räsialgoritmi infot, käivitades alltoodud Linuxi ja OpenSSl käsud.
   * verificationCert väärtus salvestatakse DER formaadis sertifikaadina, selleks salvestatakse verificationCert väärtus faili cert.b64 ja käivitatakse käsk:

base64 -d cert.b64 > certificate.der

Sertifikaat salvestatakse faili certificate.der.

* + Sertifikaat räsitakse vastavalt konfiguratsioonis toodud hash-algorithm-id väärtusele, juhul kui räsialgoritmiks on SHA-512:

openssl dgst -sha512 -hex certificate.der

Tulemuseks saadakse räsi HEX formaadis.

* + Eelmises punktis tulemuseks saadud räsi teisendatakse base64-kodeeritud kujule:

echo "<HEX formaadis räsi>" | xxd -r -p | base64

Kui tulemuseks saadud räsi vastab konfiguratsioonis olevale Verification-certificate-hash väärtusele, kasutatakse seda verifitseerimissertifikaati konfiguratsiooni allkirja verifitseerimiseks.

1. Allkiri asub konfiguratsiooni eelviimasel real ja on base64 kujul. Allkiri teisendatakse binaarkujule:

echo -n <allkiri\_base64\_kujul> | base64 --decode > signature.bin

1. Konfiguratsiooni sisu salvestatakse faili, milles **ei tohi olla viimast reavahetust**, selleks:
   * Tuvastatakse, milline väärtus vastab antud konfiguratsioonis innerboundary väärtusele, selleks uuritakse konfiguratsioonis sisalduva konfikataloogi päise boundary väärtust:

Content-Type: multipart/mixed; charset=UTF-8; boundary=xj0AtunSx7yjH97u4Rwckl7M8Nk=

* + Kopeeritakse allalaaditud konfiguratsiooni esimene osa, st. alates reast --<innerboundary> kuni viimase --<innerboundary> reani (kaasa arvatud) faili configuration\_data (innerboundary on asendatud eelmises punktis tuvastatud väärtusega).
  + Eemaldatakse failist viimane reavahetus:

truncate --size=-1 configuration\_data

1. Verifitseeritakse konfiguratsiooni sisu, selleks:
   * Eraldatakse sertifikaadist avalik võti:

openssl x509 -inform DER -in certificate.der -pubkey -noout > pubkey.pem

* + Tehakse kindlaks räsialgoritmi väärtus (konifguratsioonis toodud Signature-Algorithm-Id) ja kasutatakse avalikku võtit allkirja verifitseerimiseks, juhul kui räsialgoritmiks on SHA-512:

openssl dgst -sha512 -verify pubkey.pem -signature signature.bin configuration\_data

Verifitseerimine peab õnnestuma.

#### HA keskserveri varundamine ja taastamine

##### HA keskserveri varundamine

1. Keskserveri konfiguratsiooni varundamine kasutajaliidese kaudu
   * Varundatatakse serveri konfiguratsioon
2. Keskserveri konfiguratsiooni varundamine käsureal (vt Veaolukorrad: HA keskserveri varundamine).
   * Keskserveri varundamiseks käivitatakse skript, mille argumentideks on eksemplari identifikaator, sõlme nimi ja loodava varundusfaili nimi. Näiteks HA klastris oleva keskserveri KS1 varundamiseks tuleks varundamise skript käivitada nii:

/usr/share/xroad/scripts/backup\_xroad\_center\_configuration.sh -i "AA" -n "node\_0" -f backup.tar

1. Varundamisel tekitatakse tarballile label, mida saab kontrollida käsuga

tar tf <varundusfail> | head -1

1. Kontrollitakse nii käsureal kui kasutajaliidese kaudu loodud konfiguratsioonifaili tarball labelit. Veendutakse, et tarballi labeli väärtus on mõlema faili puhul:

central\_XROAD\_<tarkvara versioon>\_<instantsi id>\_<HA sõlme nimi>

##### Veaolukorrad: HA keskserveri varundamine

1. Varundamise skript käivitatakse ilma sõlme nime argumendita.
2. Veendutakse, et keskserveri varundamine ebaõnnestub veateatega "Missing value of HA node name but postgresql-bdr-9.4 is installed".

##### HA keskserveri taastamine

1. Keskserveri konfiguratsiooni taastamine kasutajaliidese kaudu
   * Taastatakse server varundusfailist.
2. Keskserveri konfiguratsiooni taastamine käsureal (vt Veaolukorrad: HA keskserveri taastamine).
   * Keskserveri taastamiseks käsureal käivitatakse skript, mille argumentideks on eksemplari identifikaator, sõlme nimi ja varundusfaili nimi. Näiteks HA klastris oleva keskserveri KS1 taastamiseks tuleks taastamise skript käivitada nii:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i "AA" -n "node\_0" -f backup.tar

##### Veaolukorrad: HA keskserveri taastamine

1. Taastamise skript käivitatakse ilma sõlme nime argumendita.
2. Veendutakse, et keskserveri taastamine ebaõnnestub veateatega "Missing value of HA node name but postgresql-bdr-9.4 is installed".

### X-tee eksemplari CC keskserverite paigaldamine ja esialgne seadistamine

Testitakse kahest keskserverist koosneva HA klastri paigaldamist.

#### Keskserveri KS4 paigaldamine

Testi käigus kasutatavad ressursid:

* Keskserver KS4

Teststsenaarium:

1. Keskserveris KS4 paigaldatakse kõrgkäideldavuse seadistamiseks pakk:

apt-get install xroad-center-clusterhelper

1. Keskserveris KS4 luuakse fail /etc/xroad/cluster/nodes sisuga:

<KS4 IP-aadress>

<KS5 IP-aadress>

1. Keskserveris KS4 käivitatakse klastri loomise skript:

sudo -i -u xroad /usr/share/xroad/scripts/xroad\_create\_cluster.sh

* + Kinnitatakse klastrisse kuuluvate sõlmede nimekiri;
  + SSH avaliku võtme lisamise käsk käivitatakse kõigis sõlmedes (keskserverites KS4 ja KS5) ja lubatakse skriptil töö lõpuni teha;
  + Veendutakse, et sõlmede nimedeks seadistatakse:
    - KS4 - node\_0
    - KS5 - node\_1
    - Skripti väljund sisaldab ridu: <KS4 IP aadress>: Configuring BDR node, using node ID 'node\_0' ja <KS5 IP aadress>: Configuring BDR node, using node ID 'node\_1'

1. Keskserverisse KS4 paigaldatakse keskserveri pakid.
2. Initsialiseeritakse keskserver KS4:
   * seadistatakse keskserveri aadress ja eksemplari identifikaator: **CC**;
   * initsialiseeritakse tarkvaraline võtmeseade: **PIN = 1234**.
3. Seadistatakse liikmeklassid:
   * code: **GOV**, description: **Government organization**
   * code: **COM**, description: **Commercial enterprise**
   * code**: NGO**, description: **Non-governmental organization**
4. Seadistatakse sertifitseerimis- ja ajatempliteenused.
5. Konfiguratsiooniallikatele (nii sisemisele kui välimisele) genereeritakse võtmed tarkvaralisele võtmeseadmele. Veendutakse, et:
   * allkirjavõti seatakse automaatselt aktiivseks, st kuvatakse tabelis rasvases kirjas.
   * allkirjavõtme lisamisele järgnevalt genereeritakse automaatselt konfiguratsiooniallika ankur.
6. X-tee liikmeks lisatakse: Name: **Client One**, Class: **COM**, Code: **CLIENT1**
7. X-tee liikmele **CLIENT1** lisatakse alamsüsteem **Management Services**.
8. Seadistatakse haldusteenused - haldusteenuste osutajaks määratakse alamsüsteem **CLIENT1:Management Services**

Testi lõpuks, keskserveris:

* ei tohi UI kuvada ühtegi globaalset veateadet (ühe minuti jooksul peale haldusteenuste osutaja seadistamist võib UI veel globaalseid veateateid kuvada, kuna konfiguratsiooni genereerimine toimub kord minutis);
* seadistatud peab olema vähemalt üks sertifitseerimisteenus ja vähemalt üks ajatempliteenus;
* CLIENT1 peab olema X-tee liikmete nimekirjas ja CLIENT1:Management Services seadistatud haldusteenuste osutajaks.
* Haldusteenuste vaates „Management Services' Security Server” välja väärtusena kuvatakse nuppu „Register”, kuna CLIENT1:Management Services pole ühegi turvaserveri omanik ega klient.
* Kasutajaliidese üleval vasakus nurgas kuvatakse lisaks instantsi nimele ka sõlme nime (CC (NODE\_0)).

#### Keskserveri KS5 paigaldamine

Testi käigus kasutatavad ressursid:

* Keskserver KS5

Teststsenaarium:

1. Keskserveris KS5 paigaldatakse keskserveri pakid.
2. Keskserveris KS5 paigaldatakse klastri terviseinfo vaatamise skripti kasutamiseks pakk:

apt-get install xroad-center-clusterhelper

1. Initsialiseeritakse keskserver KS5:
   * seadistatakse keskserveri aadress, eksemplari identifikaator: **CC** peab olema eeltäidetud;
   * initsialiseeritakse tarkvaraline võtmeseade: **PIN = 1234**.
2. Konfiguratsiooniallikatele (nii sisemisele kui välimisele) genereeritakse võtmed tarkvaralisele võtmeseadmele. Veendutakse, et:
   * allkirjavõti seatakse automaatselt aktiivseks, st kuvatakse tabelis rasvases kirjas.
   * allkirjavõtme lisamisele järgnevalt genereeritakse automaatselt konfiguratsiooniallika ankur.

Testi lõpuks, keskserveris:

* ei tohi UI kuvada ühtegi globaalset veateadet (ühe minuti jooksul peale ankrute genereerimist võib UI veel globaalseid veateateid kuvada, kuna konfiguratsiooni genereerimine toimub kord minutis);
* seadistatud on sama sertifitseerimisteenus, ajatempliteenus ja liikmeklassid nagu keskserveris KS4;
* CLIENT1 peab olema X-tee liikmete nimekirjas ja CLIENT1:Management Services seadistatud haldusteenuste osutajaks;
* Kasutajaliidese üleval vasakus nurgas kuvatakse lisaks instantsi nimele ka sõlme nime (CC (NODE\_1)).

### Kõrgkäideldava süsteemi varundamine ja taaste

#### Olemasoleva kõrgkäideldava süsteemi varundamine ja taastamine kasutajaliidese kaudu

Testi käigus kasutatavad ressursid:

* Keskserver KS4
* Keskserver KS5

Teststsenaarium:

1. Keskserveris KS4 varundadakse süsteemi konfiguratsioon selliselt, nagu ta jäi KS4 ja KS5 initsialiseerimise lõpuks. Varundusfail salvestatakse väljapoole testitavat süsteemi, et seda saaks hiljem kasutada tühja süsteemi taastamisel.
2. Korratakse eelmist punkti keskserveris KS5.
3. Keskserveris KS5 lisatakse globaalne grupp koodiga "TEMP" ja kirjeldusega "Temporary". Veendutakse, et kirje tekib ka keskserverisse KS4.
4. Kirjutatakse üles mõlemas keskserveris aktiivsete sisemise ja välise konfi allkirjastamise võtmete identifikaatorid.
5. Keskserverites KS4 ja KS5 genereeritakse mõlemas lisaks üks välise konfiguratsiooni allkirjastamise võti ja aktiveeritakse uus võti mõlemas keskserveris.
6. Keskserveris KS4 eemaldatakse initsialiseerimise käigus lisatud ajatempliteenus. Veendutakse, et see kaob ka keskserveris KS5.
7. Keskserveris KS5 valitakse taastamiseks eelnevalt loodud varundusfail ja käivitatakse taastamine.
8. Veendutakse, et pärast taastamist on mõlemas keskserveris nii globaalsete gruppide, võtmete kui ajatempliteenuse osas taastunud initsialiseerimise järgne seis (globaalset gruppi "TEMP" ei ole; lisatud võtmed on kadunud, endised võtmed, mis enne muudatusi kirja pandi, on aktiivsed; ajatempliteenuse kirje on jälle olemas).
9. Korratakse andmete muutmise samme 3-6.
10. Korratakse taastamise samme 7-9, algatades seekord taastamise keskserveris KS4, seal eelnevalt loodud varundusfailiga.

#### Varundatud süsteemi taastamine tühjale süsteemile käsurealt

Testi käigus kasutatavad ressursid:

* Keskserver KS4a
* Keskserver KS5a

Teststsenaarium:

1. Tühjas süsteemis paigaldatakse keskserverite klaster ja keskserveri pakid masinatesse KS4a ja KS5a (vt "Keskserveri KS4 paigaldamine" ja "Keskserveri KS5 paigaldamine"), aga keskservereid ei initsialiseerita.
2. Keskserveritesse KS4a ja KS5a kopeeritakse eelmises testis loodud varundusfailid vastavalt masinale.
3. Taastatakse keskserver KS4a, näiteks kui varundusfail on /tmp/conf\_backup\_20151216-125301.tar:

sudo -i -u xroad /usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i CC -n node\_0 -f /tmp/conf\_backup\_20151216-125301.tar

1. Logitakse sisse keskserveri KS4a kasutajaliidestesse ja sisestatakse tokeni PIN kood.
2. Veendutakse, et minuti jooksul õnnestub keskserveris KS4a konfiguratsiooni genereerimine.
3. Taastatakse keskserveri KS5a konfiguratsioonifailid ilma andmebaasita (võti -S), näiteks kui varundusfail on /tmp/conf\_backup\_20151216-125451.tar:

sudo -i -u xroad /usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh -i CC -n node\_0 -f /tmp/conf\_backup\_20151216-125451.tar -S

1. Veendutakse, et taastamiskäsu väljundi üks viimaseid ridu on "SKIPPING DB RESTORE AS REQUESTED".
2. Logitakse sisse keskserveri KS5a kasutajaliidesesse ja sisestatakse tokeni PIN kood.
3. Veendutakse, et minuti jooksul õnnestub keskserveris KS5a konfiguratsiooni genereerimine.
4. Veendutakse vabalt valitud kirjete abil, et kirjete lisamine, muutmine ja kustutamine toimivad ja muudatused replikeeruvad.

### Konfiguratsiooniankrute genereerimine kõrgkäideldavas süsteemis

#### Konfiguratsiooniankrute automaatne genereerimine eksemplaris CC

Testi käigus kasutatavad ressursid:

* Keskserver KS4
* Keskserver KS5

Teststsenaarium:

1. Veendutakse, et keskserveri KS4 UI-s kuvatav konfiguratsiooniankru räsi ja ankru genereerimise ajatempel ühtib keskserveri KS5 UI-s kuvatava ankrufaili räsi ja ankru genereerimise ajatempliga nii sisemise kui välise konfiguratsiooniankru puhul.
2. Laaditakse keskserveritest KS4 ja KS5 sisemine konfiguratsiooniankur alla ning veendutakse, et ankrufailide sisu on sama.
3. Laaditakse keskserveritest KS4 ja KS5 väline konfiguratsiooniankur alla ning veendutakse, et ankrufailide sisu on sama.
4. Ühendutakse keskserverite KS4 ja KS5 andmebaasidega ja veendutakse nii sisemise kui välise konfiguratsiooniankru kohta, et andmebaasis olev ankru aktiivse allkirjastamisvõtme identifikaator ühtib vastava keskserveri UI-s kuvatava aktiivse allkirjastamisvõtme identifikaatoriga (vt Konfiguratsiooniallika verifitseerimissertifikaadi kontrollimine).
5. Keskserveris KS4 genereeritakse uus sisemine konfiguratsiooniankur. Veendutakse, et keskserveri KS5 UI-s kuvatav sisemise konfiguratsiooniankru genereerimise ajatempel ühtib keskserveri KS4 UI-s kuvatava uue ajatempliga.
6. Veendutakse, et keskserverite KS4 ja KS5 andmebaasis olev sisemise konfiguratsiooniankru genereerimise ajatempel (anchor\_generated\_at) ühtib samuti keskserverite UI-s kuvatava uue ajatempliga (vt Allalaaditava faili ja baasikirje kokku viimine).

### Halduslogimine kõrgkäideldavas süsteemis

#### Halduslogimine X-tee eksemplaris CC

Testitakse, et puhtale süsteemile HA klastri installi käigus loodud kataloogid on syslogile kirjutatavad.

Testi käigus kasutatavad ressursid:

* Keskserver KS4
* Keskserver KS5

Teststsenaarium:

1. Keskserveris KS4 genereeritakse sisemisele konfiguratsioonile tarkvaralisele võtmeseadmele uus võti.
2. Keskserveris KS4 aktiveeritakse uus sisemise konfiguratsiooni allkirjastamisvõti.
3. Keskserveris KS4 kustutatakse vana sisemise konfiguratsiooni allkirjastamisvõti.
4. Keskserveris KS5 proovitakse lisada uus liikmeklass, liikmeklassi lisamisel jäetakse tühjaks "Code" ja/või "Description" väli. Liikmeklassi lisamine peab ebaõnnestuma.
5. Keskserveris KS5 lisatakse uus liikmeklass.
6. Keskserveris KS5 kustutatakse lisatud liikmeklass.
7. Veendutakse, et keskserveris KS4 halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Center UI* kirjed teostatud tegevuste kohta:
   * Kirje sisemisele konfiguratsioonile allkirjastamisvõtme genereerimise kohta.
   * Kirje sisemise konfiguratsiooni allkirjastamisvõtme aktiveerimise kohta.
   * Kirje sisemise konfiguratsiooni allkirjastamisvõtme kustutamise kohta.
8. Veendutakse, et keskserveris KS5 halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Center UI* kirjed teostatud tegevuste kohta:
   * Kirje liikmeklassi lisamise nurjumise kohta.
   * Kirje liikmeklassi lisamise kohta.
   * Kirje liikmeklassi kustutamise kohta.

### X-tee eksemplari AA kõrgkäideldava keskserverite klastri seadistamine

Testitakse kõrgkäideldavuse seadistamist ühe keskserveriga X-tee instantsis.

#### Keskserverite klastri seadistamine ja keskserveri KS3 paigaldamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Keskserveris KS1 paigaldatakse kõrgkäideldavuse seadistamiseks pakk:

apt-get install xroad-center-clusterhelper

1. Keskserveris KS1 luuakse fail /etc/xroad/cluster/nodes sisuga:

<KS1 IP-aadress>

<KS3 IP-aadress>

1. Keskserveris KS1 käivitatakse klastri loomise skript:

sudo -i -u xroad /usr/share/xroad/scripts/xroad\_create\_cluster.sh

* + Kinnitatakse klastrisse kuuluvate sõlmede nimekiri;
  + SSH avaliku võtme lisamise käsk käivitatakse kõigis sõlmedes (keskserverites KS1 ja KS3) ja lubatakse skriptil tööga jätkata;
  + Veendutakse, et sõlmede nimedeks seadistatakse:
    - KS1 - node\_0
    - KS3 - node\_1
    - Skripti väljund sisaldab ridu: <KS1 IP aadress>: Configuring BDR node, using node ID 'node\_0' ja <KS3 IP aadress>: Configuring BDR node, using node ID 'node\_1'

1. Keskserveris KS3 paigaldatakse keskserveri pakid.
2. Keskserveris KS3 paigaldatakse klastri terviseinfo vaatamise skripti kasutamiseks pakk:

apt-get install xroad-center-clusterhelper

1. Initsialiseeritakse keskserver KS3:
   * seadistatakse keskserveri aadress, eksemplari identifikaator: **AA** peab olema eeltäidetud;
   * initsialiseeritakse tarkvaraline võtmeseade: **PIN = 1234**.
2. Konfiguratsiooniallikatele (nii sisemisele kui välimisele) genereeritakse võtmed tarkvaralisele võtmeseadmele. Veendutakse, et:
   * allkirjavõti seatakse automaatselt aktiivseks, st kuvatakse tabelis rasvases kirjas.
   * allkirjavõtme lisamisele järgnevalt genereeritakse automaatselt konfiguratsiooniallika ankur.

Testi lõpuks, keskserveris KS3:

* ei tohi UI kuvada ühtegi globaalset veateadet (ühe minuti jooksul peale ankrute genereerimist võib UI veel globaalseid veateateid kuvada, kuna konfiguratsiooni genereerimine toimub kord minutis);
* seadistatud on sama sertifitseerimisteenus, ajatempliteenus, liikmeklassid ja haldusteenuste osutaja nagu keskserveris KS1;
* Kasutajaliidese üleval vasakus nurgas kuvatakse lisaks instantsi nimele ka sõlme nime (AA (NODE\_1)).

Testi lõpuks, keskserveris KS1:

* ei tohi UI kuvada ühtegi globaalset veateadet;
* Kasutajaliidese üleval vasakus nurgas kuvatakse lisaks instantsi nimele ka sõlme nime (AA (NODE\_0)).

#### Konfiguratsiooniankrute automaatne genereerimine eksemplaris AA

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Veendutakse, et keskserveri KS1 UI-s kuvatav konfiguratsiooniankru räsi ja ankru genereerimise ajatempel ühtib keskserveri KS3 UI-s kuvatava ankrufaili räsi ja ankru genereerimise ajatempliga nii sisemise kui välise konfiguratsiooniankru puhul.
2. Laaditakse keskserveritest KS1 ja KS3 sisemine konfiguratsiooniankur alla ning veendutakse, et ankrufailide sisu on sama.
3. Laaditakse keskserveritest KS1 ja KS3 väline konfiguratsiooniankur alla ning veendutakse, et ankrufailide sisu on sama.
4. Ühendutakse keskserverite KS1 ja KS3 andmebaasidega ja veendutakse nii sisemise kui välise konfiguratsiooniankru kohta, et andmebaasis olev ankru aktiivse allkirjastamisvõtme identifikaator ühtib vastava keskserveri UI-s kuvatava aktiivse allkirjastamisvõtme identifikaatoriga (vt Konfiguratsiooniallika verifitseerimissertifikaadi kontrollimine).
5. Keskserveris KS1 genereeritakse uus väline konfiguratsiooniankur. Veendutakse, et keskserveri KS3 UI-s kuvatav välise konfiguratsiooniankru genereerimise ajatempel ühtib keskserveri KS1 UI-s kuvatava uue ajatempliga.
6. Veendutakse, et keskserverite KS1 ja KS3 andmebaasis olev välise konfiguratsiooniankru genereerimise ajatempel (anchor\_generated\_at) ühtib samuti keskserverite UI-s kuvatava uue ajatempliga (vt Allalaaditava faili ja baasikirje kokku viimine).

#### Halduslogimine X-tee eksemplaris AA

Testitakse, et olemasolevale süsteemile HA klastri seadistamise käigus loodud/muudetud kataloogid on syslogile endiselt kirjutatavad.

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Keskserver KS1 varundatakse. (vt HA keskserveri varundamine)
2. Keskserveris KS1 muudetakse keskse teenuse **random** osutajat.
3. Keskserver KS1 taastatakse. (vt HA keskserveri taastamine)
4. Keskserver KS3 varundatakse. (vt HA keskserveri varundamine)
5. Keskserveris KS3 proovitakse muuta keskserveri aadressi, kuid aadressi väli jäetakse tühjaks. Keskserveri aadressi muutmine peab ebaõnnestuma.
6. Keskserveris KS3 muudetakse keskserveri aadressi.
7. Keskserveris KS3 muudetakse haldusteenuste osutajat.
8. Keskserver KS3 taastatakse. (vt HA keskserveri taastamine)
9. Veendutakse, et keskserveris KS1 halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Center UI* kirjed teostatud tegevuste kohta:
   * Kirje serveri varundamise kohta.
   * Kirje keskse teenuse osutaja muutmise kohta.
   * Kirje serveri taastamise kohta.
10. Veendutakse, et keskserveris KS3 halduslogis (*/var/log/xroad/audit.log*) on korrektse ajatempliga, kasutajanimega ja konteksti nimega *X-Road Center UI* kirjed teostatud tegevuste kohta:
    * Kirje serveri varundamise kohta.
    * Kirje keskserveri aadressi muutmise nurjumise kohta.
    * Kirje keskserveri aadressi muutmise kohta.
    * Kirje haldusteenuste osutaja muutmise kohta.
    * Kirje serveri taastamise kohta.

### HA klastri tervisenäitajate vaatamine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. HA klastri terviseinfo vaatamiseks käivitatakse keskserveris KS3 skript /usr/share/xroad/scripts/check\_ha\_cluster\_status.py
2. Veendutakse, et skripti väljundi "SUMMARY OF CLUSTER STATUS" alajaotuses on read
   * All nodes: OK
   * Configuration: OK
3. Veendutakse, et alajaotuses "DETAILED CLUSTER STATUS INFORMATION" kajastuvad kõigi sõlmede andmed ning kõigi sõlmede node\_status väärtus on ready.
4. Veendutakse, et N-1 node'i infos on väärtustatud replikeerimisinfo elemendid (replication\_client\_address, replication\_lag\_bytes, replication\_state), kus N == sõlmede arv klastris.
5. Veendutakse, et iga sõlme kohta toodud genereeritud failide (sisemine ja väline konfiguratsiooniankur, private-params ja shared-params) viimase muutuse ajatemplid ühtivad keskserverite KS1 ja KS3 UI-s toodud failide genereerimise ajatemplitega (UTC-aeg).
6. Peatatakse sõlme node\_0 andmebaasiserveri töö ja käivitatakse skript uuesti.
7. Keskserveris KS3 veendutakse, et skripti väljundi "SUMMARY OF CLUSTER STATUS" alajaotuses on read
   * **All nodes: NOK**
   * Configuration: OK
8. Taastatakse sõlme node\_0 andmebaasiserveri töö ja käivitatakse skript uuesti suvalisel sõlmel.
9. Veendutakse, et tulemus vastab punktidele 2-4.

### Andmebaaside replikeerumine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Keskserveris KS1 lisatakse X-tee liikmeks: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2**.
2. Veendutakse, et keskserveri KS3 andmebaasi tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names on samad andmed lisatud.
3. Veendutakse, et keskserveri KS3 andmebaasi tabelisse history on tekkinud kirjed tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names kliendi **CLIENT2** andmete lisamise ja muutmise kohta, mille ha\_node\_name väärtus on node\_0.
4. Keskserveris KS1 muudetakse liikme **CLIENT2** nime Member name: **Client 2**.
5. Veendutakse, et keskserveri KS3 andmebaasi tabelites security\_server\_clients ja security\_server\_client\_names on liikme **CLIENT2** nimi muutunud.
6. Veendutakse, et keskserveri KS3 andmebaasi tabelisse history on tekkinud kirjed tabelites security\_server\_clients ja security\_server\_client\_names andmete muutmise kohta, mille ha\_node\_name väärtus on node\_0.
7. Keskserveris KS1 kustutatakse liige **CLIENT2**.
8. Veendutakse, et keskserveri KS3 andmebaasi tabelitest security\_server\_clients, identifiers ja security\_server\_client\_names on liikme **CLIENT2** andmed kustutatud.
9. Veendutakse, et keskserveri KS3 andmebaasi tabelisse history on tekkinud kirjed tabelitest security\_server\_clients, identifiers ja security\_server\_client\_names andmete kustutamise kohta, mille ha\_node\_name väärtus on node\_0.
10. Peatatakse keskserveri KS1 andmebaasiserveri töö.
11. Keskserveris KS3 lisatakse X-tee liikmeks: Name: **Client Two**, Class: **GOV**, Code: **CLIENT2**.
12. Taastatakse keskserveri KS1 andmebaasiserveri töö.
13. Veendutakse, et keskserveri KS1 andmebaasi tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names on kliendi **CLIENT2** andmed lisatud.
14. Veendutakse, et keskserveri KS1 tabelisse history on tekkinud kirjed tabelitesse security\_server\_clients, identifiers ja security\_server\_client\_names kliendi **CLIENT2** andmete lisamise ja muutmise kohta, mille ha\_node\_name väärtus on node\_1.

### Keskserveri aadressi muutmine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Keskserveris KS1 muudetakse System Settings vaates keskserveri aadressi. Veendutakse, et andmebaasides muutus õige sõlme vastava süsteemiparameetri väärtus.

**Kuidas**: Keskserverite KS1 ja KS3 andmebaasis tehakse päring

SELECT value FROM system\_parameters WHERE key='centralServerAddress' AND ha\_node\_name='node\_0';

1. Veendutakse, et keskserveri KS1 UI-s kuvatavad keskserveri aadressist sõltuvad väärtused on muutunud:

* System Settings - WSDL Address
* System Settings - Services Address
* Configuration Management - Internal Configuration - Download URL
* Configuration Management - External Configuration - Download URL

1. Veendutakse, et keskserverites KS1 ja KS3 genereeriti uued sisemise ja välise konfiguratsiooni ankrud ning uute ankrufailide keskserveri KS1 UI-s kuvatav genereerimise ajatempel ja räsi ühtivad keskserveri KS3 UI-s kuvatavate vastavate andmetega.
2. Laetakse alla nii keskserveri KS1 kui KS3 sisemine ja väline konfiguratsiooniankur ning veendutakse, et igas ankrus kajastub uus KS1 aadress.

### Konfiguratsiooni sisu sõlmele vastavuse kontrollimine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Keskserverites KS1 ja KS3 kontrollitakse, kas haldusteenuse sertifikaadi väärtus private-params.xml failis vastab antud sõlme sertifikaadile (vt Haldusteenuse sertifikaadi väärtuse korrektsuse kontrollimine).
2. Keskserveris KS1 lülitatakse konfiguratsiooni genereerimine cronist välja.

Kuidas: failis /etc/cron.d/xroad-center kommenteeritakse välja rida

\* \* \* \* \* xroad curl http://127.0.0.1:8084/managementservice/gen\_conf 2>&1 >/dev/null;

1. Sõlm KS3 tehakse keskserveri KS1 jaoks ligipääsmatuks.
2. Keskserverisse KS1 lisatakse uus liige. Lisatud liikmele lisatakse alamsüsteem.
3. Keskserveris KS1 muudetakse haldusteenuste osutajaks lisatud liikme alamüsteem.
4. Keskserveris KS1 kutsutakse käsitsi välja konfigenereerija:

curl http://127.0.0.1:8084/managementservice/gen\_conf

1. Keskserveri KS1 UI kaudu laetakse alla failid private-params.xml ja shared-params.xml ning veendutakse, et failides kajastuvad punktides 4 ja 5 tehtud muudatused.
2. Keskserveri KS3 UI kaudu laetakse alla failid private-params.xml ja shared-params.xml ning veendutakse, et failides ei kajastu punktides 4 ja 5 tehtud muudatused.
3. Taastatakse ligipääs sõlmele KS3 keskserveri KS1 jaoks.
4. Keskserveris KS1 lülitatakse konfiguratsiooni genereerimine cronist tagasi sisse.

### Haldusteenuste kasutamine

Veendutakse, et katkestus andmebaasi töös ei mõjuta edasist haldusteenuste kasutamist.

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3
* Turvaserver TS1

Teststsenaarium:

1. Peatatakse sõlmede KS1 ja KS3 andmebaasiserveri töö.
2. Proovitakse turvaserveri TS1 kliendiks registreerida **CLIENT1** **alamsüsteem "sub2"**. Kliendi registreerimise taotluse saatmine ebaõnnestub.
3. Tehakse turvaserveris TS1 uus autentimisvõti ja -sertifikaat. Saadetakse turvaserverist sertifikaadi registreerimistaotlus, taotluse saatmine ebaõnnestub.
4. Taastatakse sõlmede KS1 ja KS3 andmebaasiserveri töö.
5. Proovitakse turvaserveri TS1 kliendiks registreerida **CLIENT1** **alamsüsteem "sub2"**. Kliendi registreerimistaotluse saatmine õnnestub.
6. Saadetakse turvaserverist TS1 autentimissertifikaadi registreerimistaotlus, taotluse saatmine õnnestub.

### Mitme konfiguratsiooniallikaga ankrute genereerimine

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS3

Teststsenaarium:

1. Veendutakse, et HA klastri terviseinfos olevad konfiguratsiooniankrute viimase muutmise ajatemplid vastavad UI-s ja andmebaasis leiduvatele ajatemplitele (vt Allalaaditava faili ja baasikirje kokku viimine).
2. Veendutakse, et keskserverites KS1 ja KS3 genereeritud sisemistes ja välistes konfiguratsiooniankrutes on kaks konfiguratsiooniallikat: KS1 ja KS3.
3. Veendutakse, et keskserverites KS1 ja KS3 genereeritud sisemistes ja välistes konfiguratsiooniankrutes olevate konfiguratsiooniallikate verifitseerimissertifikaadid vastavad konfiguratsiooniallikat sisaldavas keskserveris genereeritud vastavale võtmele (vt Konfiguratsiooniallika verifitseerimissertifikaadi kontrollimine).
4. Keskserverites KS1 ja KS3 genereeritakse uued sisemise ja välise konfiguratsiooni allkirjastamise võtmed ja aktiveeritakse uued võtmed.
5. Veendutakse, et keskserverites KS1 ja KS3 kajastuvad tehtud muutused andmebaasis korrektselt: tehakse kindlaks, et tabelis configuration\_sources on iga sõlme puhul aktiivseks märgitud sama võti nagu keskserveri UI-s (võtme identifikaator, mis peab ühtima UI-s toodud identifikaatoriga asub tabelis configuration\_signing\_keys veerus key\_identifier).
6. Veendutakse, et uued automaatselt genereeritud konfiguratsiooniankrud sisaldavad konfiguratsiooniallikate verifitseerimissertifikaate, mis vastavad uutele aktiivsetele võtmetele (vt Konfiguratsiooniallika verifitseerimissertifikaadi kontrollimine).
7. Veendutakse, et HA klastri terviseinfos olevad konfiguratsiooniankrute viimase muutmise ajatemplid vastavad UI-s ja andmebaasis leiduvatele ajatemplitele (vt Allalaaditava faili ja baasikirje kokku viimine).
8. Laetakse alla ja verifitseeritakse KS1 ja KS3 sisemine ja väline konfiguratsioon (vt Konfiguratsiooni verifitseerimine).

### Konfiguratsiooniallika kaudu konfiguratsiooni levitamise ajutine katkestamine föderatsioonis

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS2
* Keskserver KS3
* Konfiguratsioonivahendaja
* Turvaserver TS3

Teststsenaarium:

1. Konfiguratsioonivahendaja eksemplaris AA-ext laetakse üles eksemplari AA väline konfiguratsiooniankur, mis sisaldab konfiguratsiooniallikaid KS1 ja KS3.
2. Sõlme KS1 kaudu tehakse konfiguratsioon ligipääsmatuks keskserverile KS2, turvaserverile TS3 ja konfiguratsioonivahendajale.
3. Keskkonna BB keskserveris KS2 laetakse üles eksemplari AA väline konfiguratsiooniankur, mis sisaldab konfiguratsiooniallikaid KS1 ja KS3 ning veendutakse, et see õnnestub.
4. Keskserverist KS2 laetakse alla private\_params.xml fail ning veendutakse, et seal on olemas usaldatud ankrus sisalduv info keskkonna AA konfiguratsiooniallikate kohta.
5. Veendutakse, et turvaserveris TS3 on fail /etc/xroad/globalconf/AA/shared-params.xml, mis sisaldab keskkonna AA konfiguratsiooni ja fail /etc/xroad/globalconf/AA/shared-params.xml.metadata, mis uueneb iga minuti tagant.
6. Veendutakse, et konfiguratsioonivahendajas on kataloog /var/lib/xroad/public/AA-ext/, kuhu kopeeritakse iga minuti tagant eksemplari AA konfiguratsioon (shared-params.xml).
7. Ka sõlme KS3 konfiguratsioon tehakse keskserverile KS2, turvaserverile TS3 ja konfiguratsioonivahendajale ligipääsmatuks.
8. Veendutakse, et turvaserver TS3 logib, et ei saa ühestki keskkonna AA sõlmest konfiguratsiooni: logis /var/log/xroad/configuration\_client.log logitakse:

Failed to download configuration from any configuration location:

location: http://<KS1 aadress>/externalconf; error: HttpError: Connection timed out

location: http://<KS3 aadress>/externalconf; error: HttpError: Connection timed out

1. Veendutakse, et konfiguratsioonivahendaja logib, et ei saa ühestki keskkonna AA sõlmest konfiguratsiooni: logis /var/log/xroad/confproxy.log logitakse:

Error when executing configuration-proxy 'AA-ext': java.lang.Exception: configuration-client error (exit code 122), download failed

1. Keskserveris KS2 laaditakse üles eksemplari AA väline konfiguratsiooniankur, mis sisaldab konfiguratsiooniallikaid KS1 ja KS3 ning veendutakse, et see ebaõnnestub.
2. Sõlme KS3 konfiguratsioon tehakse keskserverile KS2, turvaserverile TS3 ja konfiguratsioonivahendajale ligipääsetavaks.
3. Veendutakse, et turvaserver TS3 saab keskkonna AA konfiguratsiooni kätte (/var/log/xroad/configuration\_client.log logitakse konfiguratsiooni allalaadimine sõlmest KS3).
4. Veendutakse, et konfiguratsioonivahendaja saab keskkonna AA konfiguratsiooni kätte (/var/log/xroad/confproxy.log logitakse eksemplari AA-ext konfiguratsiooni allalaadimine).
5. Keskserveris KS2 laaditakse üles eksemplari AA väline konfiguratsiooniankur, mis sisaldab konfiguratsiooniallikaid KS1 ja KS3 ning veendutakse, et see õnnestub.
6. Sõlme KS1 kaudu tehakse konfiguratsioon keskserverile KS2, turvaserverile TS3 ja konfiguratsioonivahendajale ligipääsetavaks.

### Mitme konfiguratsiooniallika vahel valimine

#### Konfiguratsiooniallika kleepuvus olukorras, kus konfiguratsiooniklient valib mitme konfiguratsiooniallika vahel

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Turvaserver TS1

Teststsenaarium:

1. Turvaserveris TS1 imporditakse keskserveri KS1 sisemine konfiguratsiooniankur. Tehakse kindlaks, millisest konfiguratsiooniallikast (kas KS1 või KS3) konfiguratsioon alla laeti (turvaserveris TS1 /var/log/xroad/configuration\_client.log).
2. Veendutakse, et turvaserver TS1 laeb iga minuti tagant konfiguratsiooni alla samast konfiguratsiooniallikast.
3. Tehakse antud konfiguratsiooniallikas turvaserveri TS1 jaoks ligipääsmatuks.
4. Veendutakse, et turvaserver TS1 hakkab konfiguratsiooni teisest allikast alla laadima.
5. Ligipääsmatuks tehtud konfiguratsiooniallikas tehakse taas turvaserveri TS1 jaoks ligipääsetavaks.
6. Veendutakse, et konfiguratsiooniallikas, kust turvaserver TS1 konfiguratsiooni alla laeb, ei muutu.

#### Konfiguratsiooniallika kleepuvus föderatsioonis, HA toega usaldatud süsteemidest konfiguratsiooni allalaadimisel

Testi käigus kasutatavad ressursid:

* Keskserver KS1
* Keskserver KS4
* Turvaserver TS1

Teststsenaarium:

1. Veendutakse, et keskserveri KS4 väline konfiguratsiooniankur sisaldab kahte konfiguratsiooniallikat: KS4 ja KS5.
2. Keskserveris KS1 imporditakse keskserveri KS4 väline konfiguratsiooniankur.
3. Turvaserveris TS1 veendutakse, et sisemisest konfiguratsiooniallikast allalaaditud konfiguratsioonist saadi ka usaldatud ankru info ja et sealt omakorda võetakse üks allikatest, kust konfiguratsioon lisaks alla laadida: turvaserveris TS1 /var/log/xroad/configuration\_client.log logitakse:

Downloading configuration from http://<CC keskkonna KS aadress>/externalconf

1. Veendutakse, et turvaserver TS1 laeb iga minuti tagant konfiguratsiooni alla samast välisest konfiguratsiooniallikast.
2. Tehakse antud konfiguratsiooniallikas turvaserveri TS1 jaoks ligipääsmatuks.
3. Veendutakse, et turvaserver TS1 hakkab konfiguratsiooni teisest CC keskkonna keskserverist alla laadima.
4. Ligipääsmatuks tehtud konfiguratsiooniallikas tehakse taas turvaserveri TS1 jaoks ligipääsetavaks.
5. Veendutakse, et konfiguratsiooniallikas, kust turvaserver TS1 konfiguratsiooni alla laeb, ei muutu.