13. Turvaserveri esialgne konfigureerimine

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 13. Turvaserveri esialgne konfigureerimine
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.32

Sisukord

13.1. Sissejuhatus

Selles õppetükis antakse juhiseid X-tee turvaserveri esialgse konfigureerimise kohta. Pärast õppetüki läbimist oskad

- laadida turvaserverisse üles konfiguratsiooniankru;
- määrata X-tee liikme liikmeklassi ja -koodi, turvaserveri koodi ja tarkvaralise võtmeseadme PIN-i.

Turvaserveri initsialiseerimiseks vajate 10–15 minutit.

13.2. X-tee globaalne konfiguratsioon

Globaalne konfiguratsioon koosneb XML-failidest, mida turvaserverid regulaarselt X-tee keskserverist alla laadivad. Globaalne konfiguratsioon sisaldab muu hulgas järgmiseid andmeid:

- usaldusankrute (CA-d ja ajatempliteenused) aadressid ja avalikud võtmed;
- vahepealsete CA-de avalikud võtmed;
- OCSP-teenuste aadressid ja avalikud võtmed (kui ei ole juba kättesaadavad sertifikaatide Authority Information Access laienduse kaudu);
- X-tee liikmete ja nende alamsüsteemide andmed;
- liikmete X-tee süsteemis registreeritud turvaserverite aadressid;
- turvaserverite X-tee süsteemis registreeritud autentimissertifikaatide andmed;
- turvaserverite X-tee süsteemis registreeritud klientide andmed;
- globaalsete pääsuõiguste gruppide andmed ja
- X-tee süsteemi parameetrid.

13.3. Konfiguratsiooniankur

Konfiguratsiooniankur on andmehulk, mida saab kasutada konfiguratsiooni pakkujalt (nt Eesti X-teed haldav asutus) saadava teabe allalaadimiseks ja kontrollimiseks. Konfiguratsiooniankur sisaldab iga allika kohta URL-i ja avaliku võtme sertifikaati, mida kasutatakse allalaaditud konfiguratsiooni tervikluse kontrollimiseks. Konfiguratsiooniankur on XML-fail.

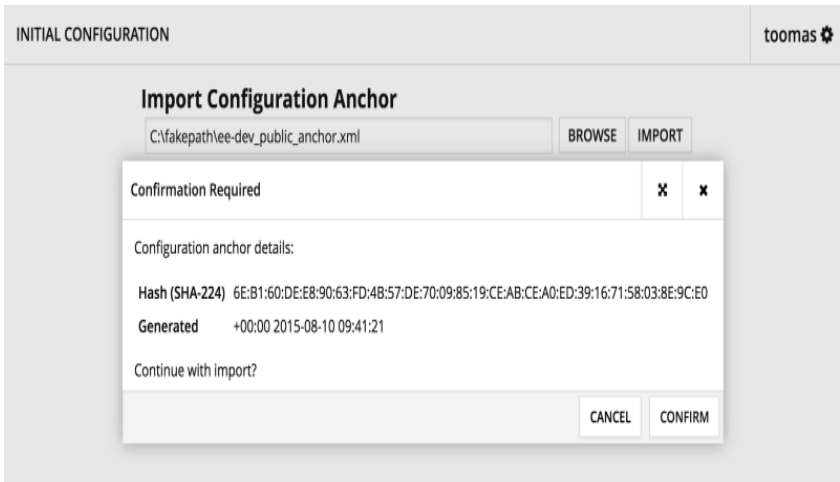
Igal X-tee keskkonnal on eri konfiguratsioon. Kasuta selle X-tee keskkonna konfiguratsiooniankrut, mida sa kasutad.

Kolme keskkonna konfiguratsiooniankrud on järgmised:

- Arenduskeskkond: https://x-tee.ee/anchors/ee-dev_public_anchor.xml
- Testkeskkond: https://x-tee.ee/anchors/ee-test_public_anchor.xml
- Toodangukeskkond: https://x-tee.ee/anchors/EE_public-anchor.xml

Esmakordselt veebiliidesest https://<SECURITYSERVER IP ADDRESS>:4000/ turvaserverisse sisse logides pead laadima üles konfiguratsiooniankru, mis määrab serveri keskkonna alatiseks.

NB! Seda ei saa hiljem muuta! Muu keskkonna määramiseks peate tegema uue installi.



13.4. Liikmeklass, liikmekood, turvaserveri kood ja tarkvaralise võtmeseadme PIN

Pärast konfiguratsiooniankru üleslaadimist tuleb määrata:

Liikmeklass
Liikmeklass rühmitab sarnaste omadustega X-tee liikmed üheks üksuseks. Näiteks rühmitatakse riigiasutused liikmeklassi „GOV“ alla, eraettevõtted „COM“ alla jne.

Liikmekood
Liikmekood on X-tee liikmega seotud ja oma liikmeklassi piires unikaalne märgikombinatsioon. Liikmekood peab jääma samaks kogu X-tee liikme eluea jooksul. Näiteks on Eesti ettevõtete ja riigiasutuste puhul liikmekoodiks äriregistrikood.

Turvaserveri kood
Turvaserveri kood on turvaserveri tähis, mis peab olema organisatsiooni piires kordumatu. Turvaserveri koodi näide on arenduskeskkonnas oleva turvaserveri kood ORGANISATION-UNIT-DEV. See on arenduskeskkonnas registreerimisvormil kohustuslik.

Tarkvaralise võtmeseadme PIN
Tarkvaralise võtmeseadme PIN on turvakood, mis on keskkonnast sõltumata kohustuslik. Veendu, et see on turvaline ja seda talletatakse turvaliselt.

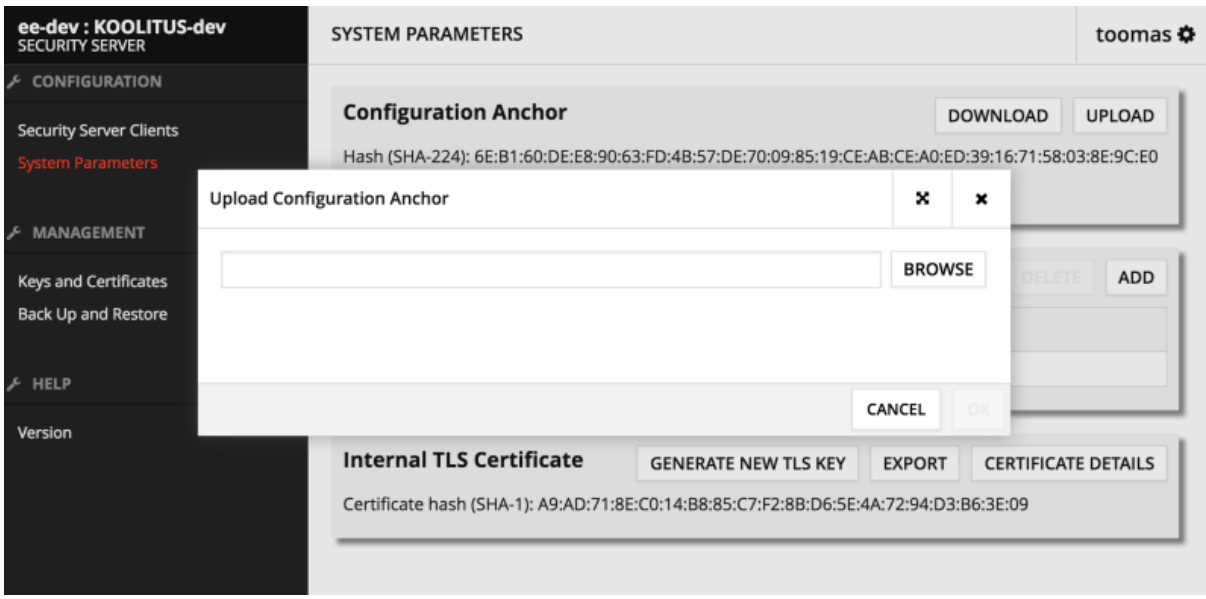
Kui konfigureerimine on lõpule viidud, X-tee turvaserver initsialiseeritakse ja seda saab seadistada usaldusteenuste kasutamiseks.

13.5. Konfiguratsiooniankru haldus

Juurdepääsuõigused:
konfiguratsiooniankru üleslaadimiseks: turvahaldur;
konfiguratsiooniankru allalaadimiseks: turvahaldur, süsteemiadministraator.

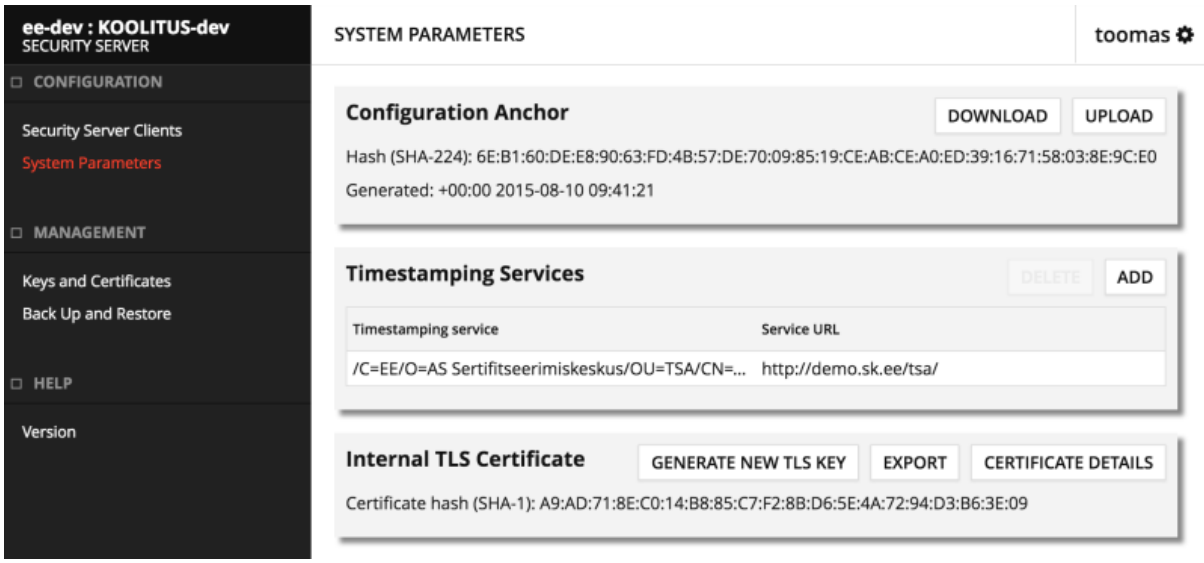
Konfiguratsiooniankru üleslaadimiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Klõpsa jaotises **„Configuration Anchor“** nuppu **„Upload“**.
3. Otsi kohalikust failisüsteemist üles ankrufail ja klõpsa nuppu „**Upload**“.
4. Veendu, et laed üles korrektse ankrufaili. Selleks võrdle üleslaaditud faili räsi X-teed haldava asutuse poolt avalikustatud kehtiva ankrufaili räsiga (vaata siit). Räside ühtimisel kinnita üleslaadimine, klõpsates „**Confirm**“.



Konfiguratsiooniankru allalaadimiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Klõpsa jaotises **„Configuration Anchor“** nuppu **„Download“** ja salvesta pakutav fail.


ee-dev : KOOLITUS-dev
SECURITY SERVER
SYSTEM PARAMETERS
toomas
CONFIGURATION
Security Server Clients
System Parameters
MANAGEMENT
Keys and Certificates
Back Up and Restore
HELP
Version
Configuration Anchor
DOWNLOAD
UPLOAD
Hash (SHA-224): 6E:B1:60:DE:E8:90:63:FD:4B:57:DE:70:09:85:19:CE:AB:CE:A0:ED:39:16:71:58:03:8E:9C:E0
Generated: +00:00 2015-08-10 09:41:21
Timestamping Services
DELETE
ADD
Timestamping service
Service URL
/C=EE/O=AS Sertifitseerimiskeskus/OU=TSA/CN=...
http://demo.sk.ee/tsa/
Internal TLS Certificate
GENERATE NEW TLS KEY
EXPORT
CERTIFICATE DETAILS
Certificate hash (SHA-1): A9:AD:71:8E:C0:14:B8:85:C7:F2:8B:D6:5E:4A:72:94:D3:B6:3E:09

13.6. Küsimused

Selle õppetüki läbimiseks otsusta, kas järgmised väited on tõesed või mitte.

A. Arendus-, test- ja toodangukeskkonna puhul saab kasutada sama konfiguratsiooniankrut.
B. Kui X-tee testkeskkonna konfiguratsiooniankur on laaditud turvaserverisse, ei ole seda võimalik toodangukeskkonna konfiguratsiooniankru üles laadimisega asendada.

Õigeid vastuseid vaata siit (avanevad uues aknas).

13.7. Kokkuvõte

Selle õppetüki lõpetuseks vaata alltoodud videot.