20. Suhtlus kliendi infosüsteemiga; turvaserveri paigaldamise valideerimine

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 20. Suhtlus kliendi infosüsteemiga; turvaserveri paigaldamise valideerimine
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.38

Sisukord

20.1. Sissejuhatus

Selles õppetükis antakse juhiseid turvaserveri ühendumise kohta kliendi infosüsteemiga. Õppetüki lõpus arutatakse lühidalt X-tee turvaserveri paigaldamise valideerimist. Pärast õppetüki läbimist oskad

- valida turvaserveri jaoks kliendi infosüsteemiga ühenduse loomiseks õige protokolli;
- ühendada turvaserveri nii teenuse kasutaja kui ka teenuse osutaja rollis oleva sisevõrgu serveriga;
- hallata sisevõrgu TLS-sertifikaati;
- muuta sisevõrgu TLS-võtit ja sertifikaati ning
- kontrollida, kas X-tee turvaserveri paigaldamine õnnestus.

Õppetüki läbimiseks kulub aega umbes 20 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

X-TEE

RIIGI INFOSÜSTEEMI AMET

20.2. Kliendi infosüsteemiga suhtlemise protokollid

Juurdepääsuõigused: registreerimishaldur, teenusehaldur.

Turvaserver saab teenuseid osutavate või kasutavate infosüsteemiserveritega suhelda protokolli HTTP, HTTPS või HTTPS NOAUTH kaudu.

- **Protokolli HTTP** tuleb kasutada juhul, kui infosüsteemi server ja turvaserver kasutavad omavaheliseks suhtluseks privaatset võrgusegmenti, millesse ei ole ühendatud ühtegi muud arvutit. Samuti ei tohi infosüsteemi server pakkuda interaktiivse sisselogimise võimalust.
- **Protokolli HTTPS** tuleb kasutada juhul, kui infosüsteemi serveri ja turvaserveri vaheliseks suhtluseks pole võimalik eraldi võrgusegmenti eraldada. Sellisel juhul kaitstakse nendevahelist sidet võimaliku jälgimise ja sekkumise eest krüptograafiliste meetoditega. Protokolli HTTPS kasutamisel tuleb infosüsteemi serveri(te) jaoks genereerida sisevõrgu TLS-sertifikaadid, mis laaditakse turvaserverisse.
- **Protokolli HTTPS NOAUTH** tuleks kasutada, kui soovite, et turvaserver jätaks infosüsteemi TLS-sertifikaadi verifitseerimise vahele.

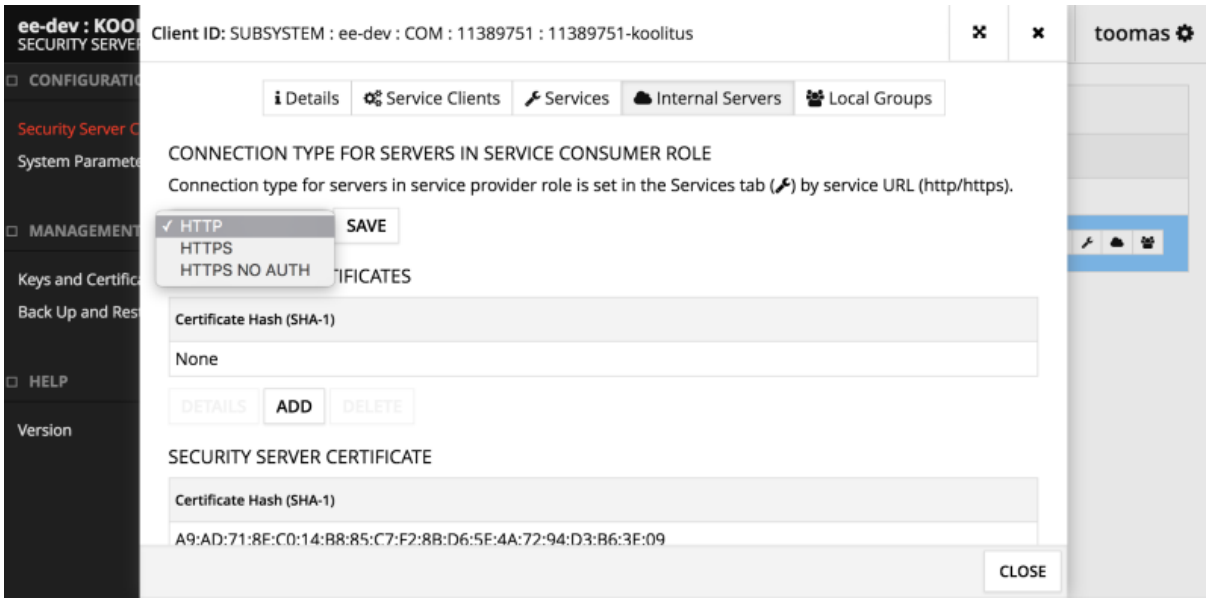
Kui ühendusviisiks on valitud HTTP, kuid infosüsteem ühendub turvaserveriga üle protokolli HTTPS või HTTPS NOAUTH, siis võetakse ühendus vastu, kuid kliendi sisevõrgu TLS-sertifikaati ei verifitseerita.

20.3. Teenuse kasutaja rollis oleva sisevõrgu serveri ühendamine

Juurdepääsuõigused: registreerimishaldur, teenusehaldur.

Teenuse kasutaja rollis oleva sisevõrguserveri ühendusviisi määramiseks tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“ ja klõpsa kliendi real ikoonil „**Internal Servers**“.
2. Vali rippmenüüs „**Connection Type**“ ühendusviis ja klõpsa „**Save**“



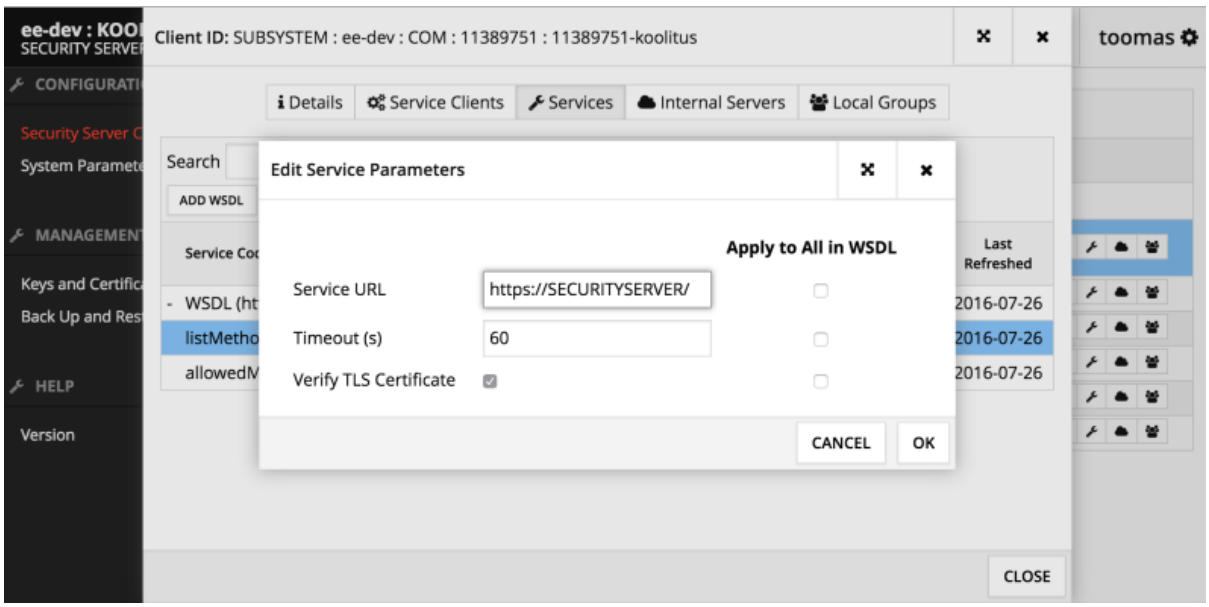
Sõltuvalt valitud ühendusviisist on infosüsteemi päringu URL kas **http://SECURITYSERVER/** või **https://SECURITYSERVER/**. Päringu tegemisel tuleb aadress SECURITYSERVER asendada turvaserveri tegeliku aadressiga.

20.4. Teenuse osutaja rollis oleva sisevõrgu serveri ühendamine

Juurdepääsuõigused: registreerimishaldur, teenusehaldur.

Teenuste osutaja rollis oleva sisevõrgu serveri ühendusviisi määrab teenuse URL-is sisalduv protokoll. Ühendusviisi muutmiseks tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“, vali tabelist klient ja klõpsa kliendi real ikoonil „**Services**“.
2. Vali tabelist teenus ja klõpsa „**Edit**“.
3. Määra teenuse URL-is protokolliks HTTP või HTTPS. HTTPS-protokolli puhul märgi vajadusel lahter „**Verify TLS certificate**“.



20.5. Sisevõrgu TLS-sertifikaadi lisamine

Turvaserveri kliendile sisevõrgu TLS-sertifikaadi lisamiseks (ühendusviisi HTTPS puhul) tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“ ja klõpsa kliendi real ikoonil „**Internal Servers**“.
2. Sertifikaadi lisamiseks klõpsa „**Internal TLS Certificates**” menüüs nuppu „**Add**“, vali kohalikust failisüsteemist sertifikaadi fail ja klõpsa „**OK**“. Sertifikaadi sõrmejälg kuvatakse tabelis „Internal TLS Certificates“.

Vajalik sertifikaat tuleks hankida kohaliku infosüsteemi arendajalt või klienditoe esindajalt. Vajadusel tuleks see sertifitseerimiskeskusest osta või käsitsi genereerida. Näiteks saate OpenSSL-i abil luua serveri enda allkirjastatud võtme ja sertifikaadi paari üheainsa käsuga:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyo
ut certificate.key -out certificate.crt
```

- `req` määrab, et sertifikaaditaotluse haldus vastab standardile X.509. X.509 on avaliku võtme infrastruktuuri standard, mida SSL ja TLS võtme- ja sertifikaadihalduses kasutavad.
- `-x509` muudab eelmist alamkäsku, andes süsteemile käsu luua enda poolt allkirjastatud sertifikaat.
- `-nodes` määrab, et OpenSSL ei kasuta võimalust sertifikaati parooliga turvata. Nii ei ole teenuse käivitamisel vaja kasutaja sekkumist.
- `-days 365` määrab sertifikaadi kehtivusaja.
- `-newkey rsa:2048` määrab, kas soovime samal ajal genereerida nii uut sertifikaati kui ka uut võtit. `rsa:2048` määrab, et RSA-võtme pikkus on 2048 bitti.
- `-keyout` ütleb OpenSSL-ile, kuhu genereeritud privaatvõtme fail paigutada.
- `-out` ütleb OpenSSL-ile, kuhu loodav sertifikaat paigutada.

Sertifikaadi genereerimise jooksul peab väärtus „Common Name“ olema infosüsteemi täielik domeeninimi või IP.

Turvaserverisse laaditud sisemine TLS-sertifikaat peab olema sama, mida kasutab kohalik infosüsteem.

20.7. Sisevõrgu TLS-võtme ja -sertifikaadi muutmine

Juurdepääsuõigused: turvahaldur, süsteemiadministraator.

Turvaserveri sisemise TLS-võtme ja -sertifikaadi muutmiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Klõpsa jaotises „**Internal TLS Certificate**“ nuppu „**Generate New TLS Key**“ ja avanevas aknas klõpsa „**Confirm**“.

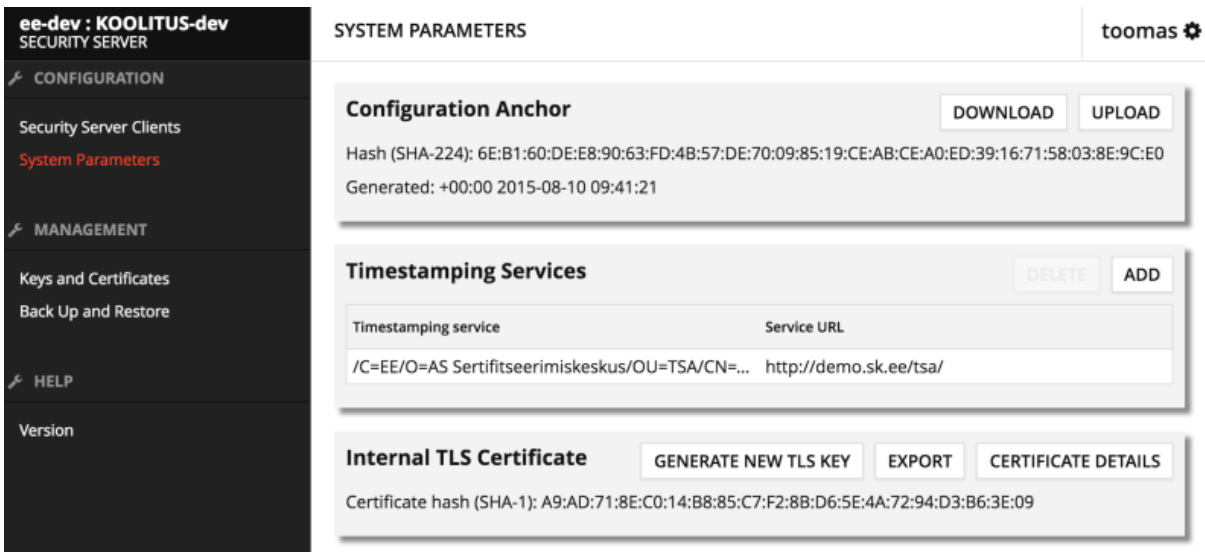
Turvaserver loob võtme, mida kasutatakse kliendi infosüsteemidega suhtlemiseks, ning sellele vastava enda poolt allkirjastatud sertifikaadi. Muutub ka turvaserveri sertifikaadi sõrmejälg. Turvaserveri domeeninimi salvestatakse sertifikaadi väljale „Common Name“ ning sisemine IP-aadress laiendusväljale „subjectAltName“.

Turvaserveri sisemise TLS-sertifikaadi eksportimiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Klõpsa jaotises „**Internal TLS Certificate**“ nuppu „**Export**“ ja salvesta pakutav fail kohalikku failisüsteemi.

Turvaserveri sisemise TLS-sertifikaadi andmete vaatamiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Klõpsa jaotises „**Internal TLS Certificate**“ nuppu „**Certificate Details**“.



20.8. Küsimus

Selle õppetüki läbimiseks otsusta, kas järgmine väide on tõene või mitte.

Protokolli HTTPS kasutamisel tuleb infosüsteemi serveri jaoks genereerida sisevõrgu TLS-sertifikaadid, mis laaditakse turvaserverisse.

Õiget vastust vaata siit (avaneb uues aknas).

20.9. Paigaldamise valideerimine

Saad kontrollida, kas X-tee turvaserveri paigaldamine on õnnestunud, tehes päringu kõigi X-tee eksemplari potentsiaalsete teenuseosutajate (st liikmed ja alamsüsteemid) kohta. Selleks tuleb teha turvaserverile GTTP GET päring.

Päringu URL on http://SECURITYSERVER/listClients või https://SECURITYSERVER/listClients, sõltuvalt sellest, kas HTTPS-protokoll on konfigureeritud turvaserveri ja infosüsteemi vaheliseks suhtluseks. Päringu tegemisel tuleb aadress SECURITYSERVER asendada turvaserveri tegeliku aadressiga.

Turvaserveri vastus peab olema content-type text/xml ja vastus PEAB sisaldama allpool määratletud clientList XML elementi:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<ns2:clientList xmlns:ns1="http://x-road.eu/xsd/identifiers" xmlns:ns2="http://x-road.eu/xsd/xroad.xsd">
  ▼<ns2:member>
    ▼<ns2:id ns1:objectType="MEMBER">
       <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
       <ns1:memberClass>GOV</ns1:memberClass>
       <ns1:memberCode>70006317</ns1:memberCode>
     </ns2:id>
     <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  ▼<ns2:member>
    ▼<ns2:id ns1:objectType="SUBSYSTEM">
       <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
       <ns1:memberClass>GOV</ns1:memberClass>
       <ns1:memberCode>70006317</ns1:memberCode>
       <ns1:subsystemCode>testservice</ns1:subsystemCode>
     </ns2:id>
     <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  ▼<ns2:member>
    ▼<ns2:id ns1:objectType="SUBSYSTEM">
       <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
       <ns1:memberClass>GOV</ns1:memberClass>
       <ns1:memberCode>70006317</ns1:memberCode>
       <ns1:subsystemCode>aar</ns1:subsystemCode>
     </ns2:id>
     <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  ▼<ns2:member>
    ▼<ns2:id ns1:objectType="SUBSYSTEM">
       <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
       <ns1:memberClass>GOV</ns1:memberClass>
```

Lisateavet teenuse metaandmete protokolli kohta leiad siit.

20.6. Sisevõrgu TLS-sertifikaadi haldus

Turvaserveri sisemise TLS-sertifikaadi andmete vaatamiseks tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“ ja klõpsa kliendi real ikoonil „**Internal Servers**“.
2. Vali tabelist „Internal TLS Certificates“ sertifikaat ja klõpsa „**Details**“**.**

Sisevõrgu TLS-sertifikaadi kustutamiseks tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“ ja klõpsa kliendi real ikoonil „**Internal Servers**“.
2. Vali tabelist „**Internal TLS Certificates**“ sertifikaat ja klõpsa „**Delete**“.
3. Kinnita kustutamist, klõpsates avanenud aknas „**Confirm**“.

Turvaserveri sisemise TLS-sertifikaadi eksportimiseks tee järgmist.

1. Menüüs „**Configuration**“ vali „**Security Server Clients**“ ja klõpsa kliendi real ikoonil „**Internal Servers**“.
2. Klõpsa „**Export**“ ja salvesta pakutav fail kohalikku failisüsteemi.