14. Ajatempliteenuste haldus; võtmete ja sertifikaaditaotluste genereerimine

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 14. Ajatempliteenuste haldus; võtmete ja sertifikaaditaotluste genereerimine
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.32

Sisukord

14.1. Sissejuhatus

Selles õppetükis räägitakse X-tee turvaserveri konfigureerimisest usaldusteenuste kasutamiseks. Pärast õppetüki läbimist oskad

- hallata ajatempliteenuseid turvaserveris;
- genereerida allkirjavõtme ja allkirjavõtme sertifikaaditaotluse ning
- genereerida autentimisvõtme ja autentimisvõtme sertifikaaditaotluse.

Selleks kõigeks kulub aega umbes 15 minutit.

Arenduskeskkonnas saab turvaserverile sertifikaate taotleda meili teel, saates meiliaadressil (help@ria.ee) sertifikaaditaotluse, organisatsiooni nime, organisatsiooni registreerimisnumbri ja serveri koodi.

Arenduskeskkonnas saab turvaserverile sertifikaate taotleda meili teel, saates meiliaadressil (help@ria.ee) sertifikaaditaotluse, organisatsiooni nime, organisatsiooni registreerimisnumbri ja serveri koodi.

14.7. Kokkuvõte

Esiteks genereeri allkirja (SIGN)-/autentimisvõti (AUTH).

Teiseks genereeri allkirja (SIGN)-/autentimisvõtmele (AUTH) sertifikaaditaotlus.

Kolmandaks edasta sertifikaaditaotlus tunnustatud sertifitseerimisteenuse osutajale. Teenuseosutaja loob sertifikaadi.

Ajatempliteenuse saab lisada otse turvaserveri kasutajaliidese kaudu.

14.2. Ajatempliteenuste haldus

Juurdepääsuõigused: turvahaldur.

Ajatempliteenuse lisamiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Jaotises „**Timestamping Services**“ klõpsa käsku **„Add“**.
3. Vali avanevas aknas vastav teenus ja klõpsa nuppu **„OK“**.

Ajatempliteenuse kustutamiseks tee järgmist.

1. Tee menüüs „**Configuration**“ valik **„System Parameters“.** Avatakse süsteemi parameetrite vaade.
2. Vali jaotises **Ajatempliteenused** teenus, mille soovid kustutada, ja klõpsa käsku **Kustuta**.

Kui konfigureeritakse mitu ajatempliteenust, proovib turvaserver saada ajatempli tabelis kõige ülemiselt teenuselt ja kui katse ei õnnestu, liigub allapoole järgmise teenuse juurde.

14.3. Allkirjavõtme genereerimine

Juurdepääsuõigused:
kõik toimingud: turvahaldur;
kõik toimingud, v.a võtmeseadmesse sisse logimine: registreerimishaldur;
võtmeseadmesse sisse logimine: süsteemiadministraator.

Enne allkirjavõtme genereerimist **veendu, et turvaserveri kellaaeg oleks õige**. Seejärel tee järgmist.

1. Menüüs „**Management**“ vali „**Keys and Certificates**“.
2. Kui kasutad riistvaralist võtmeseadet, kontrolli, et seade on turvaserveriga ühendatud. Seade peab olema kuvatud „**Keys and Certificates**” tabelis.
3. Võtmeseadmesse sisse logimiseks klõpsa tabelis seadme real nupule „**Enter PIN**“ ja sisesta PIN-kood. Kui sisestatakse õige PIN-kood, kuvatakse nupu „**Enter PIN**“ nupu asemel nupp „**Logout**“.
4. Allkirjavõtme genereerimiseks vali tabelis seade, klõpsates selle reale, ja klõpsa nupule „**Generate key**“. Sisesta võtmele silt ja vajuta „**OK**”. Genereeritud võti kuvatakse tabelis seadme rea all. Sildi väärtuseks kuvatakse võtme nimi.

14.4. Allkirjavõtmele sertifikaaditaotluse genereerimine

Juurdepääsuõigused: turvahaldur, registreerimishaldur.

Allkirjavõtmele sertifikaaditaotluse genereerimiseks tee järgmist.

1. Menüüs „**Management**“ vali „**Keys and Certificates**“.
2. Vali tabelist võti ja klõpsa nuppu „**Generate CSR**“. Avanenud dialoogiboksis:
   - vali rippmenüüst „**Usage**” sertifikaadi kasutusviis (allkirjasertifikaadi jaoks väärtus „SIGN”);
   - vali rippmenüüst „**Client**” X-tee liige, kellele sertifikaat välja antakse;
   - vali rippmenüüst „**Certification Service**” sertifikaadi väljaandja;
   - vali rippmenüüst sertifikaaditaotluse formaat (vastavalt valitud sertifitseerimisteenuse nõuetele kas PEM või DER);
   - klõpsa „**OK**“.
3. Vaata avanenud vormil üle sertifikaadi omaniku andmed, mis lisatakse CSR-i, ja täida vajaduse korral tühjad väljad.
4. CSR-i genereerimise lõpuleviimiseks klõpsa „OK“ ja salvesta pakutav fail kohalikku failisüsteemi.

Pärast CSR-i genereerimist lisatakse tabelisse võtme rea alla kirje „Request“, mis näitab, et sellele võtmele on loodud sertifikaaditaotlus. Kirje lisatakse ka siis, kui taotlust kohalikku failisüsteemi ei salvestatud.

Allkirjavõtme sertifitseerimiseks toimeta sertifikaaditaotlus tunnustatud sertifitseerimisteenuse osutajale ning võta vastu sertifikaaditaotluse alusel loodud allkirjasertifikaat.

14.5. Autentimisvõtme genereerimine

Juurdepääsuõigused:
kõik toimingud: turvahaldur;
võtmeseadmesse sisse logimine: süsteemiadministraator.

Turvaserveri autentimisvõtmeid saab genereerida ainult tarkvaraliste võtmeseadmetega. Tee järgmist.

1. Menüüs „**Management**“ vali „**Keys and Certificates**“.
2. Tarkvaralisse võtmeseadmesse sisse logimiseks klõpsa tabelis seadme real nupule „**Enter PIN**“ ja sisesta PIN-kood. Kui sisestatakse õige PIN-kood, kuvatakse nupu „**Enter PIN**“ nupu asemel nupp „**Logout**“.
3. Autentimisvõtme genereerimiseks vali tabelis seade, klõpsates selle reale, ja klõpsa nupule „**Generate key**“. Sisesta võtmele silt ja vajuta „**OK**”. Genereeritud võti kuvatakse tabelis seadme rea all. Sildi väärtuseks kuvatakse võtme nimi.

14.6. Autentimisvõtmele sertifikaaditaotluse genereerimine

Juurdepääsuõigused: turvahaldur.

Autentimisvõtmele sertifikaaditaotluse genereerimiseks tee järgmist.

1. Menüüs „**Management**“ vali „**Keys and Certificates**“.
2. Vali tabelist autentimisvõti ja klõpsa nuppu „**Generate CSR**“. Avanenud dialoogiboksis:
   - vali rippmenüüst „**Usage**” sertifikaadi kasutusviis (autentimissertifikaadi jaoks väärtus „AUTH”);
   - vali rippmenüüst „**Certification Service**” sertifikaadi väljaandja;
   - vali rippmenüüst sertifikaaditaotluse formaat (vastavalt valitud sertifitseerimisteenuse nõuetele kas PEM või DER);
   - klõpsa „**OK**“.
3. Vaata avanenud vormil üle teave, mis lisatakse CSR-i, ja täitke vajaduse korral tühjad väljad.
4. CSR-i genereerimise lõpuleviimiseks klõpsa „OK“ ja salvesta pakutav fail kohalikku failisüsteemi.

Pärast CSR-i genereerimist lisatakse tabelisse võtme rea alla kirje „Request“, mis näitab, et sellele võtmele on loodud sertifikaaditaotlus. Kirje lisatakse ka siis, kui taotlust kohalikku failisüsteemi ei salvestatud.

Autentimisvõtme sertifitseerimiseks toimeta sertifikaaditaotlus tunnustatud sertifitseerimisteenuse osutajale ning võta vastu sertifikaaditaotluse alusel loodud autentimissertifikaat.