16. Sertifikaadi olekud

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 16. Sertifikaadi olekud
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.36

Sisukord

16.1. Sissejuhatus

Selles õppetükis selgitatakse, kuidas turvaserveris kuvatakse teavet sertifikaatide, võtmete ja/või võtmeseadmete kättesaadavuse, registreeritusoleku ja kehtivuse kohta. Juttu tuleb järgmistest sertifikaatide olekutest:

- võtmeseadmete, võtmete ja sertifikaatide kättesaadavusolekud (hall, kollane ja valge);
- allkirjasertifikaadi registreeritusolekud (registreeritud või kustutatud);
- autentimissertifikaadi registreeritusolekud (salvestatud, registreerimisel, registreeritud, globaalne viga, kustutamisel või kustutatud) ja
- sertifikaatide kehtivusolekud (kehtivusinfo puudub, peatatud, kehtiv, aegunud, tühistatud või inaktiveeritud).

Pärast selle õppetunni läbimist saad aru teabest, mida turvaserver sertifikaatide oleku kohta kuvab.

Õppetüki läbimiseks kulub sul 10-15 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

X-TEE

RIIGI INFOSÜSTEEMI AMET

16.2. Võtmeseadmete, võtmete ja sertifikaatide kättesaadavusolekud

Võtmeseadmete, võtmete ja sertifikaatide kättesaadavuse kohta kasutatakse vaates „Keys and Certificates“ järgmisi taustavärvusi.

Hall taust
Objekt ei ole turvaserverile kättesaadav. Halli taustaga sertifikaate ei saa sõnumite vahendamiseks kasutada.

Kollane taust
Objekt on turvaserverile kättesaadav, kuid objekti andmed ei ole salvestatud turvaserveri konfiguratsioonis. Näiteks võib kiipkaart olla serveriga ühendatud, kuid kiipkaardil olevad sertifikaadid ei ole serverisse imporditud. Kollase taustaga sertifikaate ei saa sõnumite vahendamiseks kasutada.

Valge taust
Objekt on turvaserverile kättesaadav ja objekti andmed on salvestatud turvaserveri konfiguratsioonis. Valge taustaga sertifikaate saab sõnumite vahendamiseks kasutada.

Võtmeseadme ja võtme andmed salvestatakse automaatselt konfiguratsiooni nendega seotud sertifikaadi turvaserverisse importimisel või võtmele sertifikaaditaotluse genereerimisel. Sarnaselt kustutatakse võtmeseadme ja võtme andmed turvaserveri konfiguratsioonist automaatselt viimase nendega seotud sertifikaadi ja/või sertifikaaditaotluse kustutamisel.

16.3. Sertifikaatide registreeritusolekud

Registreeritusolekud väljendavad seda, kas ja kuidas saab sertifikaati X-tee süsteemis kasutada.

Vaates „Keys and Certificates“ kuvatakse sertifikaadi registreeritusolekud (välja arvatud olek „Deleted“) tabeli tulbas „**Status**“ (Olek).

Sertifikaadid tuleb X-tee keskserveris valideerida. Seda tehakse käsitsi tööajal. Seepärast võib sertifikaadi oleku muutmine võtta veidi aega.

16.4. Allkirjasertifikaadi registreeritusolekud

Turvaserveri allkirjasertifikaat saab olla ühes järgmistest registreeritusolekutest.

Registered (Registreeritud)
Sertifikaat on turvaserverisse imporditud ja salvestatud turvaserveri konfiguratsiooni. Registreeritud olekus allkirjasertifikaati saab kasutada X-tee sõnumite allkirjastamiseks.

Deleted (Kustutatud)
Sertifikaat on serveri konfiguratsioonist kustutatud. Juhul, kui kustutatud olekus sertifikaat asub turvaserveriga ühendatud riistvaralisel võtmeseadmel, kuvatakse sertifikaat kollase taustvärvusega.

16.5. Autentimissertifikaadi registreeritusolekud

Turvaserveri autentimissertifikaat saab olla ühes järgmistest registreeritusolekutest.

Saved (Salvestatud)
Sertifikaat on turvaserverisse imporditud ja salvestatud turvaserveri konfiguratsiooni, aga sertifikaati pole registreerimiseks esitatud.

Registration in progress (Registreerimisel)
Autentimissertifikaadi registreerimistaotlus on loodud ja saadetud keskserverisse, aga seos sertifikaadi ja turvaserveri vahel ei ole veel kinnitatud.

Registered (Registreeritud)
Seos autentimissertifikaadi ja turvaserveri vahel on keskserveris kinnitatud. Registreeritud olekus autentimissertifikaati saab kasutada X-tee sõnumite vahetamiseks tarviliku turvalise andmevahetuskanali loomiseks.

Global error (Globaalne viga)
Seos autentimissertifikaadi ja turvaserveri vahel on keskserveris tühistatud.

Deletion in progress (Kustutamisel)
Autentimissertifikaadi kustutamise taotlus on saadetud keskserverisse. Sellest olekust on võimalik üleminek, isegi kui autentimissertifikaadi kustutamise taotluse saatmine nurjub.

Deleted (Kustutatud)
Sertifikaat on turvaserveri konfiguratsioonist kustutatud.

16.6. Sertifikaatide kehtivusolekud

Kehtivusolek näitab, kas sertifikaadil on kehtiv OCSP (Online Certificate Status Protocol) vastus.

Vaates „Keys and certificates“ kuvatakse sertifikaadi kehtivusolekud tulbas **„OCSP response“**. Kehtivusolekuid (välja arvatud olekut „Disabled“) kuvatakse sertifikaatidele, mille registreeritusolekuks on „Registered“.

Turvaserveri sertifikaat saab olla ühes järgmistest kehtivusolekutest.

Unknown (Kehtivusinfo puudub)
Sertifikaadil puudub kehtiv OCSP vastus (OCSP vastuse kehtivuse periood on määratud X-teed haldava asutuse poolt) või viimaseks OCSP vastuseks on saadud „Unknown“ (teave taotletava sertifikaadi kohta puudub) või veateade.

Suspended (Peatatud)
Viimaseks OCSP vastuseks on saadud „Suspended“ (Peatatud).

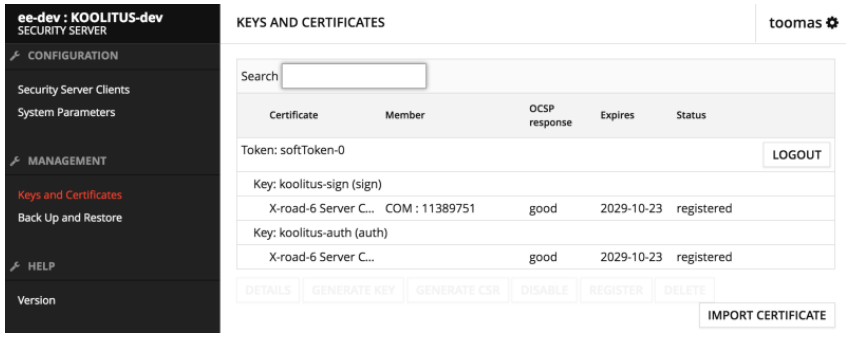
Good (Kehtiv)
Viimaseks OCSP vastuseks on saadud „Good“ (Kehtiv). Vaid kehtivas olekus olevaid sertifikaate saab kasutada päringute allkirjastamiseks või turvaserverite vahel ühenduse loomiseks.

Expired (Aegunud)
Sertifikaadi aegumistähtaeg on möödunud. Sertifikaat ei ole aktiivne ja selle kohta ei tehta OCSP päringuid.

Revoked (Tühistatud)
Viimaseks OCSP vastuseks on saadud „Revoked“ (Tühistatud). Sertifikaat ei ole aktiivne ja selle kohta ei tehta OCSP päringuid.

Disabled (Inaktiveeritud)
Kasutaja on märkinud sertifikaadi inaktiveerituks. Sertifikaat ei ole aktiivne ja selle kohta ei tehta OCSP päringuid.

16.7. Kokkuvõte



X-tee turvaserveris saab sertifikaate kasutada sõnumite vahendamiseks üksnes siis, kui need on (vaates „Keys and Certificates“

- **valgel taustal, mis tähendab, et sertifikaat on turvaserverile kättesaadav;**
- **olekus „Registered“ (veerus „Status“), mis tähendab, et sertifikaat on registreeritud ja**
- **olekus „Good“ (veerus „OCSP response“), mis tähendab, et sertifikaat on kehtiv.**