8. Usaldusteenused X-teel

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 8. Usaldusteenused X-teel
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.29

Sisukord

8.1. Sissejuhatus

Käesolev õppetükk annab ülevaate usaldusteenustest X-teel. Õppetüki lõpetamise järel oskad Sa:

- defineerida usaldusteenused ja selgitada, mida nende kasutamine annab,
- kirjeldada e-templi sertifikaadi, turvaserveri autentimissertifikaadi, sertifikaadi kehtivuskinnituse teenuse ja ajatempli teenuse tähtsust ja tähendust,
- selgitada, kuidas usaldusteenused tagavad andmevahetuse turvalisuse X-teel,
- planeerida usaldusteenustega seotud tegevusi X-tee kasutuselevõtu protsessis ning
- valida kvalifitseeritud usaldusteenuste pakkujalt endale sobivad nõuetekohased usaldus-teenused.

Õppetüki läbimiseks kulub Sul umbes 15 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

X-TEE

RIIGI INFOSÜSTEEMI AMET

8.2. Usaldusteenused

Usaldusteenused on standardiseeritud ja reguleeritud teenused, mis on infotehnoloogilistes lahendustes põhiteenuste aluseks.

Kvalifitseeritud usaldusteenuste kasutamine on oluline tõendusväärtuse seisukohast. Need aitavad tagada, et kasutatavad sertifikaadid on seotud õigete osapooltega (autentsus). Samuti tagavad need e-templi mehhanismide abil vahetatud andmete allika ja muutumatuse teistele osapooltele.

Usaldusteenuseid osutavad kolmandad osapooled, kes vastavad kindlaks määratud nõuetele (kvalifitseeritud usaldusteenuste osutajad).

Usaldusteenused on reguleeritud Euroopa Parlamendi ja Nõukogu 23. juuli 2014. a määruses (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (nr 910/2014, **eIDAS määrus**). See on kõigile Euroopa Liidu liikmetele otsekohalduv regulatsioon, mis määratleb ühesugused tingimused kõigile digitaalsetele usaldusteenustele ning elektroonilise identiteedi ja allkirjastamise/tembeldamise aspektidele. eIDAS määrus on kättesaadav siit.

8.3. Usaldusteenused Eesti X-teel

Andmevahetuse tervikluse ning X-teel vahetatud sõnumi ja X-tee liikme seotuse näitamiseks kasutatakse **e-templit** (eIDAS määruse mõttes täiustatud e-templit kvalifitseeritud sertifikaadiga).

E-templi loomiseks kasutatakse järgmisi usaldusteenuseid:

- sertifitseerimise teenus, mille kaudu väljastatakse **e-templi sertifikaat** (kvalifitseeritud e-templi sertifikaat täiustatud e-templi loomiseks) ja **turvaserveri autentimissertifikaat**,
- **sertifikaadi kehtivuskinnituse teenus** ning
- **ajatempliteenus**.

Nimetatud usaldusteenused on vajalikud kõikide X-teel vahetatavate sõnumite tembeldamiseks. Liikmel on keelatud töödelda X-teel vahetatud andmeid, mida ei ole e-tembeldatud või mida ei ole võimalik aegtembeldada.

X-tee turvaserver jälgib usaldusteenuste toimivust automaatselt ning tagab teenuste lühiajaliste katkestuste ajaks süsteemi toimivuse.

Järgnevalt käsitletakse nimetatud usaldusteenuseid ükshaaval.

8.4. E-templi sertifikaat

X-tee e-tempel on eIDAS määruse mõttes **täiustatud e-tempel kvalifitseeritud sertifikaadiga**.

Täiustatud e-tempel on eIDAS määruse järgi e-tempel,

- mis on seotud ainuüksi allkirja andjaga,
- mida saab kasutada üksnes allkirja andja,
- mille abil on võimalik allkirja andjat tuvastada ning
- mis on seotud allkirjastatud andmetega selliselt, et kõik hilisemad andmete muudatused on tuvastatavad.

E-templi kvalifitseeritud sertifikaat on e-templi sertifikaat, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab eIDAS määruse lisas III sätestatud nõuetele.

X-tee liikme e-templi sertifikaat on niisiis kvalifitseeritud usaldusteenuse osutaja poolt väljastatud sertifikaat e-templi moodustamiseks. E-tempel **esindab organisatsiooni**. E-templi sertifikaati kasutatakse vahetatavate sõnumite autentsuse, tervikluse ning salgamatuse tagamiseks. Sellega tagatakse universaalne kõrge turvalisus kogu vahetatavale andmestikule.

Sõnumi keha, allkirju ja ajatemplit (ehk allkirjastatud ja ajatembeldatud teavet) hoitakse **ASiC konteineris** (*Associated Signature Container*) **XAdES** (*XML Advanced Electronic Signature*) **vormingus**.

Kui turvaserver on majutuses (seda kasutab mitu liiget), siis peab e-templi sertifikaate olema ühes turvaserveris mitu: turvaserveri omaniku e-templi sertifikaat ja lisaks iga majutatava liikme kohta üks e-templi sertifikaat. E-templi sertifikaatide tellimine ja turvaserverisse lisamine võib toimuda igal tarvilikul ajahetkel.

.

8.5. Turvaserveri autentimissertifikaat

Turvaserveri autentimissertifikaat on kvalifitseeritud usaldusteenuse osutaja poolt väljastatud ja turvaserveriga seotud sertifikaat. Seda kasutatakse turvaserverite autentimiseks nendevahelise krüpteeritud ühenduse loomisel.

Turvaserveri autentimissertifikaadi abil määratakse niisiis pääsuõigusi X-teel ning luuakse turvaline andmekanal kahe turvaserveri vahel. Seda peab olema iga turvaserveri kohta üks.

Turvaserveri autentimissertifikaat peab vastama Internet Engineering Task Force (IETF) standardile RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*).

8.6. Sertifikaadi kehtivuskinnitus

Koos e-templi sertifikaadi ja turvaserveri autentimissertifikaadiga on liikmel vaja hankida ka kehtivuskinnituse teenus.

> **Sertifikaadi kehtivuskinnituse teenus (*Online Certificate Status Protocol, OCSP*) on usaldusteenuse osutaja garantii, et kasutatav sertifikaat kehtib ning X-tee liige on see, kes ta väidab enda olevat. OCSP vastuse aeg määrab ära varaseima absoluutse aja, mil iga konkreetne sõnum X-teel vahetatud sai.**

OCSP vastused saadetakse koos sõnumiga alati teisele X-tee osapoolele. See võimaldab X-tee liikmel iga teise suvalise liikme autentsuses veenduda, tegemata selleks täiendavaid päringuid kehtivuskinnituse teenuse osutajale. Turvaserver realiseerib seda osa sõnumivahetuse protokollistikust automaatselt. Liige on seotud vaid selle kehtivuskinnituse teenuse osutajaga, kelle käest ta saab kinnituse oma sertifikaatide kehtivuse kohta.

Iga liige kasutab oma sertifitseerimisteenuse osutaja kehtivuskinnituse teenust vastavalt oma sertifikaatide arvule (e-templi ja autentimissertifikaatide summa). Sõnumid tembeldatakse saatmisel pakikaupa. Need jõuavad partneriteni räsidega, mis võimaldavad kontrollida sõnumi tembeldatust pakis. Nii on X-tee liige kaitstud kehtivuskinnituse teenuse mahu kasvamise eest, kui X-teed kasutatakse paljude partneritega ning andmevahetuse maht (sõnumite ja teenuste arv) kasvavad. Teisisõnu, täiendavate partnerite kaasamine suhtlusesse ei too juurde lisakeerukust ega tõsta usaldusteenuste kulusid.

Kasutatav kehtivuskinnituse teenus peab vastama IETF standarditele RFC 6960 või RFC 2560.

Sertifikaadi kehtivuskinnituse teenuse lubatud järjestikulise katkestuse maksimaalne kestus on 4 tundi ning summaarne seisak ööpäevas ei tohi ületada 12 tundi.

8.7. Ajatempel

Ajatempliteenuse abil lisatakse vahetatud sõnumitele digitaalne ajatempel. Ajatempel määrab ära hilisema absoluutse aja, millal andmevahetus kahe osapoole vahel konkreetse sõnumi näol võis toimuda, ning annab seeläbi vahetatud andmetele pikaajalise tervikluse garantii.

Ajatembeldatakse kõik X-teel vahetatavad sõnumid ja päringulogid.

X-teel kasutatav ajatempliteenus peab olema kvalifitseeritud eIDAS määruse tähenduses ja vastama IETF standardile RFC 3161.

Turvaserver peab olema ühendatud võrguaja protokolli (*Network Time Protocol*, NTP) 1. või 2. kihi ajaserveriga. Ajatempliteenus tohib erineda UTC-ajast kuni 1 sekund. Teenus ei tohi olla järjestikuliselt katkenud (planeeritult või planeerimata) rohkem kui neli tundi.

8.8. X-tee turvalisuse garantii

X-tee ülesanne on tagada vahetatavate andmete turvalisus. Kui tervikluse ja konfidentsiaalsuse tagamiseks kasutatakse sertifikaate ning OCSP ja ajatempli teenust, siis käideldavust tagab see, et andmevahetuse stsenaariumid ei ole oma käideldavuse tingimuste suhtes usaldusteenustest sõltuvad.

Kasutades pakksigneerimist ja aegtembeldamist, tagab X-tee, et andmevahetus osapoolte vahel toimub mitte suurema kui teatud 8-tunnise perioodi jooksul. Turvaserveris uuendatakse regulaarselt kasutatava sertifikaadi kohta OCSP vastust, mida kasutatakse korduvalt. OCSP vastus tagab andmevahetuse toimumise aja alumise raja. Aegtembeldamine see-eest annab sündmuse toimumise ülemise raja.

X-tee tagab vahetatud andmete turvalisuse, kui andmete vahetamisel on nende signeerimiseks kasutatud OCSP ja ajatempli ajaline erinevus mitte suurem kui 8 tundi. Sellest tulenevalt küsib X-tee turvaserver sertifikaatide kehtivusekinnitusi 48-minutilise (1/10 kaheksast tunnist) intervalliga.

See omakorda tähendab, et ühe sertifikaadi kohta tehakse ühes kalendrikuus kuni 930 kehtivuskinnituse päringut (30 päringut päevas), ja seda sõltumata X-tee partnerite, teenuste või päringute arvust.

Sama kehtib ajatempli puhul. Igas päevaks teeb üks turvaserver, sõltumata andmevahetuse mahust, partnerite arvust ja turvaserveri klientide arvust, kuni 30 ajatembelduspäringut. Kui mingil ajahetkel sõnumeid päringulogisse ei teki, siis tühja logi ei aegtembeldata.

8.9. Usaldusteenuste valimine

Sobivad usaldusteenused valib X-tee liige ise.

Usaldusteenused peavad olema väljastatud kvalifitseeritud usaldusteenuse osutaja poolt ja vastama X-tee keskuse poolt kehtestatud miinimumnõutele.

Kõik usaldusteenuste osutajad on leitavad Euroopa usaldusnimekirjast, mis on kättesaadav siit.

Eesti test- ja toodangukeskkonnas on hetkel teadaolev usaldusteenuse pakkuja SK ID Solutions AS. Arenduskeskkonnas osutab usaldusteenuseid Riigi Infosüsteemi Amet (RIA) (pole kvalifitseeritud usaldusteenuse pakkuja eIDAS määruse mõttes). SK ID Solutions AS osutab arenduskeskkonnas vaid ajatempliteenust.

Keskuse nõuded usaldusteenustele on kättesaadavad siit.

Soovitame teil küsida võimalikult usaldusteenuse osutajalt nende nõuete alusel omale pakkumist.

8.10. Usaldusteenuste valimine (jätkub)

Usaldusteenuste osutajad on mõistlik välja valida või neile alternatiivid leida enne turvaserveri paigaldamist kulude planeerimise etapis. Usaldusteenuste seadistamine toimub turvaserveri tarkvara installeerimise järel. Sertifikaatide taotlusi saab siis genereerida vastavalt valitud teenusepakkuja formaadile. Seejärel sertifikaadid väljastatakse ning need paigaldatakse turvaserverisse.

Testkeskkonnas ei tohi kasutada legitiimseid kvalifitseeritud sertifikaate. Testkeskkonda tuleb tuua selle teenusepakkuja testsertifikaat, kelle sertifikaati plaanitakse kasutada toodangukeskkonnas. See tagab, et toodangukeskkonnas ei ilmneks sertifitseerimise ega kehtivuskinnituse teenusega seoses mingeid üllatusi.

E-templi ja turvaserveri autentimissertifikaadid võivad olla hangitud erinevatelt teenusepakkujatelt.

Uue usaldusteenuse osutaja lisandumisel kontrollib X-tee keskus täiendavalt tarvilike nõuete täidetust ning vajadusel täiendab X-tee tehnoloogilist platvormi, et nõuetekohased usaldusteenuse pakkujad ja sertifikaadid oleksid kasutatavad.

8.11. Usaldusteenuste kasutamisega seotud kulud

Usaldusteenuste kasutamisega seotud kulud katab X-tee liige ise. All on toodud AS Sertifitseerimiskeskuse usaldusteenuste hinnad.

- E-templi sertifikaat (ühele organisatsioonile) ja turvaserveri autentimissertifikaat maksavad paketina 240 eurot aastase kehtivuse korral, 400 eurot kaheaastase kehtivuse korral ja 600 eurot kolmeaastase kehtivuse korral. E-templi sertifikaat maksab eraldi ostes 150 eurot üheaastase kehtivuse korral, 275 eurot kaheaastase kehtivuse korral ja 375 eurot kolmeaastase kehtivuse korral.
- Sertifikaadi kehtivuskinnituse teenusemaht oleneb X-tee keskkonna tingimustest. Ühe autentimis- ja ühe e-templi sertifikaadi teenindamiseks mõeldud kehtivuskinnituse teenuse hind on 76 eurot (toodangukeskkonnas).
- Ajatempli teenuse maht on kuni 1000 päringut kuus ühe turvaserveri kohta. Ajatempli teenuse hinnakiri on siin.

Teiste pakkujate usaldusteenuste hinnad võivad olla erinevad.

8.12. Küsimused

Õppetüki lõpetamiseks vasta palun järgmistele küsimustele.

1. Milline alltoodud fraasidest kirjeldab millist usaldusteenust?

A. Seotud liikmega, tõendab liikme seost sõnumiga
B. Seotud turvaserveriga, kasutatakse turvaserverite autentimiseks
C. Kinnitab kasutatavate sertifikaatide kehtivust
D. Võimaldab kontrollida, millal mingi operatsioon toimus

2. Milline alltoodud väidetest on väär?

A. Turvaserveri autentimissertifikaati peab iga turvaserveri kohta olema üks.
B. Kui turvaserver on majutuses, siis on vaja nii turvaserveri omaniku kui ka iga majutatava liikme e-templi sertifikaate.
C. E-templi ja turvaserveri autentimissertifikaadid peavad olema hangitud samalt usaldusteenuste osutajalt.

Õigeid vastuseid vaata siit (avanevad uues aknas).

8.13. Kokkuvõte

Usaldusteenused (e-templi sertifikaat, turvaserveri autentimissertifikaat, sertifikaadi kehtivuskinnitus ja ajatempel) on standardsed andmete turvalisust tõstvad operatsioonid. Nende kasutamine on oluline eeskätt tõendusväärtuse seisukohast.

Usaldusteenuste kasutamine on Eesti X-teel kohustuslik.

Sobivad usaldusteenused valib ja nende eest tasub X-teega liituja ise.

Usaldusteenuste osutajad tuleks välja valida enne turvaserveri paigaldamist, ent nende seadistamine toimub turvaserveri tarkvara installeerimise järel.