5. Turvaserver, liidestuskomponent ja MISP

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 5. Turvaserver, liidestuskomponent ja MISP
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.28

Sisukord

5.1. Sissejuhatus

Selles õppetükis tutvud Sa turvaserveri, liidestuskomponendi ja MISPiga (*mini information service portal*). Õppetüki lõpus suudad Sa:

- kirjeldada turvaserveri tähtsust ja tööpõhimõtteid,
- selgitada, kuidas turvaserver tagab X-teel vahetatavate andmete tervikluse,
- kirjeldada turvaserverite liiaskonfiguratsiooni toimimist,
- selgitada liidestuskomponendi olemust ja vajalikkust ning
- selgitada MISPi olemust.

Õppetüki läbimiseks kulub Sul umbes 15 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

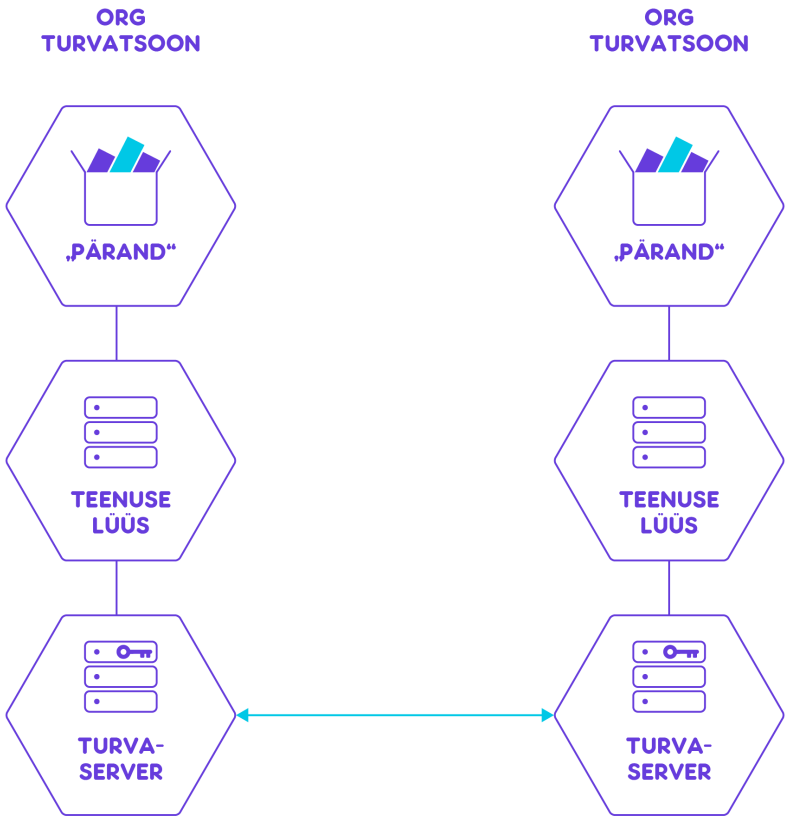
Eesti
tuleviku heaks

X-TEE

RIIGI INFOSÜSTEEMI AMET

5.2. Päringu liikumine X-teel

Päringu liikumist X-teel illustreerib alljärgnev joonis.



Nagu jooniselt näha, mängivad infosüsteemide omavahelises suhtluses olulist rolli turvaserver ja teenuse lüüs ehk liidestuskomponent. Mis need on?

5.3. Turvaserver

Turvaserver teisendab turvalises seesmises võrgus vahetatavad sõnumid selliselt, et neid oleks võimalik ebaturvalises avalikus võrgus teistega vahetada. Turvaserver rakendab juurdepääsu kontrolli sissetulevatele sõnumitele ja tagab seega, et andmetele pääsevad juurde ainult need kasutajad, kes on teenusepakkujaga sõlminud vastava kokkuleppe.

Turvaserver tagab turvalise andmevahetuse infosüsteemide vahel. See suunab liikme infosüsteemist saadetud X-tee-keelsed päringud X-teele ning pakendab need selliselt, et need jõuaksid vaid õigete adressaatideni ning oleksid ühtlasi kaitstud vahelthaaramise, muutmise ja kaotsimineku või korduvkasutuse eest. Selle peamine funktsioon on vahendada taotlusi viisil, mis säilitab nende tõendusväärtuse. Turvaserver peab arvet võimalike sihtkohtade üle, tõlgib infosüsteemide nimetusi IP-aadressideks, tembeldab andmeid, rakendab andmevahetuskanalile krüptograafiat, toodab päringustatistikat jms.

Turvaserver on ühelt poolt ühendatud avaliku Internetiga ja teiselt poolt ühendatud organisatsiooni sisevõrgu infosüsteemidega. Teatud mõttes võib turvaserverit vaadelda kui spetsiaalset **rakenduse tasandil tulemüüri**, mis toetab SOAP-protokolli ning allkirjastab ja verifitseerib allkirja vahetavatel sõnumitel. Seega tuleks see seadistada paralleelselt organisatsiooni tulemüüriga, mis vahendab protokolle.

5.4. Turvaserveri pidamine

Turvaserver on vaba tarkvara, mille igaüks saab ise alla laadida ja paigaldada. Selle haldamise kulud tuleb liikmel endal katta.

Selleks, et turvaserver X-teega ühendust saaks, on vaja keskuse heakskiidetud sertifikaate. Turvaserveri pidamiseks on vajalikud turvaserveri autentimise sertifikaat ning selle kehtivuse tagamiseks kehtivuskinnituse teenus. Samuti tuleb kasutada ajatempliteenust.

Turvaserver on X-tee protokollistikku järgiv näidislahendus. See on **parim moodus X-teel andmete vahetamiseks**. Kui aga nii sertifikaatide, sõnumivahetuse protokolli kui ka keskusega suhtlemise osas järgitakse samu kriteeriume ja nõudeid, siis on turvaserveri asemel võimalik välja arendada hoopis oma lahendus.

5.5. Turvaserver ja terviklus

Turvaserver tagab andmete terviklust kahel moel:

- kõigi päringu- ja vastussõnumite **digitembeldamine**,
- kõikide laekunud sõnumite **aegtembeldamine** mõistliku aja möödudes.

Iga turvaserver talletab laekunud signeeritud sõnumid **sõnumilogisse**. Iga logi sisaldab vastavalt X-tee protokollile sõnumit ja sõnumi tembeldamiseks kasutatud atribuute.

Iga sõnumi digitembeldamine ja aegtembeldamine võimaldab juriidilise tõestusväärtusega väita, kas andmevahetus toimus või ei toimunud. Samuti ei saa hiljem keegi sõnumilogis muuta päringu asjaolusid.

Kvalifitseeritud usaldusteenustest tulenevalt kasutatakse X-teel riistvaralisi turvalise allkirjastamise vahendeid. Keskus ega ükski usaldusteenuse pakkuja ei ole andmevahetuse hetkel kriitiliselt tarvilikud.

5.6. Turvaserverite liiaskonfiguratsioon

Kogu süsteemi saadavuse suurendamiseks ja teenuse jõudluse ja töökindluse tõhustamiseks saab turvaservereid seadistada **liiaskonfiguratsioonis.**

Selleks on kaks võimalust.

- Mitme üksiku turvaserveri seadistamine ja alamsüsteemi registreerimine neist igaühes (vaata siit). Teenusekasutaja valib kiiremini vastava teenusepakkuja turvaserveri ja kasutab seda seni, kuni see mingil põhjusel pole enam saadaval. Koormuse tasakaalustamise tulemused poleks optimaalsed. See pigem pakub tõrkesiirde järgmisele saadaolevale serverile.
- Mitme identse turvaserveri seadistamine TCP (*Transmission Control Protocol*) vookoormuse tasakaalustamisfunktsiooni taha ja koormuse tasakaalustamisfunktsiooni registreerimine X-tee avalikus IP-s. See annaks paremaid tulemusi koormuse tasakaalustamiseseisukohalt, kuid SSL-i (*Secure Sockets Layer*) kätluse seisukohalt tooks see lisakulusid. Konfiguratsioonihaldus pole keskne. Identse serverikonfiguratsiooni saab saavutada varundus- ja taastevalikute abil, mis on saadaval turvaserveri tarkvaras.

Lisaks koormuse hajutamisele võib organisatsioon omada mitut turvaserverit eesmärgiga pakkuda mõnda neist väiksematele organisatsioonidele renditeenusena.

5.7. Liidestuskomponent

Liige saab X-teed kasutada automaatseks infotöötluseks, kui ta teostab oma infosüsteemis liidestuskomponendiks nimetatava osa.

Liidestuskomponent paikneb piltlikult turvaserveri ja seesmise infosüsteemi vahel. Selle roll on tõlkida infosüsteemi sisemine äriloogika ja tehnoloogiline keel koosvõimeliseks X-tee keeleks. See võib olla terve eraldiseisev keskse andmevahetussiini (ESB) lahendus või lihtne teek, mis oskab kohalikku tehnoloogilist keelt X-tee protokollile vastavaks tõlkida.

Liidestuskomponendi ja turvaserveri erinevus seisneb selles, et esimene tagab kohaliku infosüsteemi loogika ja tehnoloogia vastavuse X-tee protokolliga, samas kui teine täidab andmeturbe tagamisega seotud funktsioone.

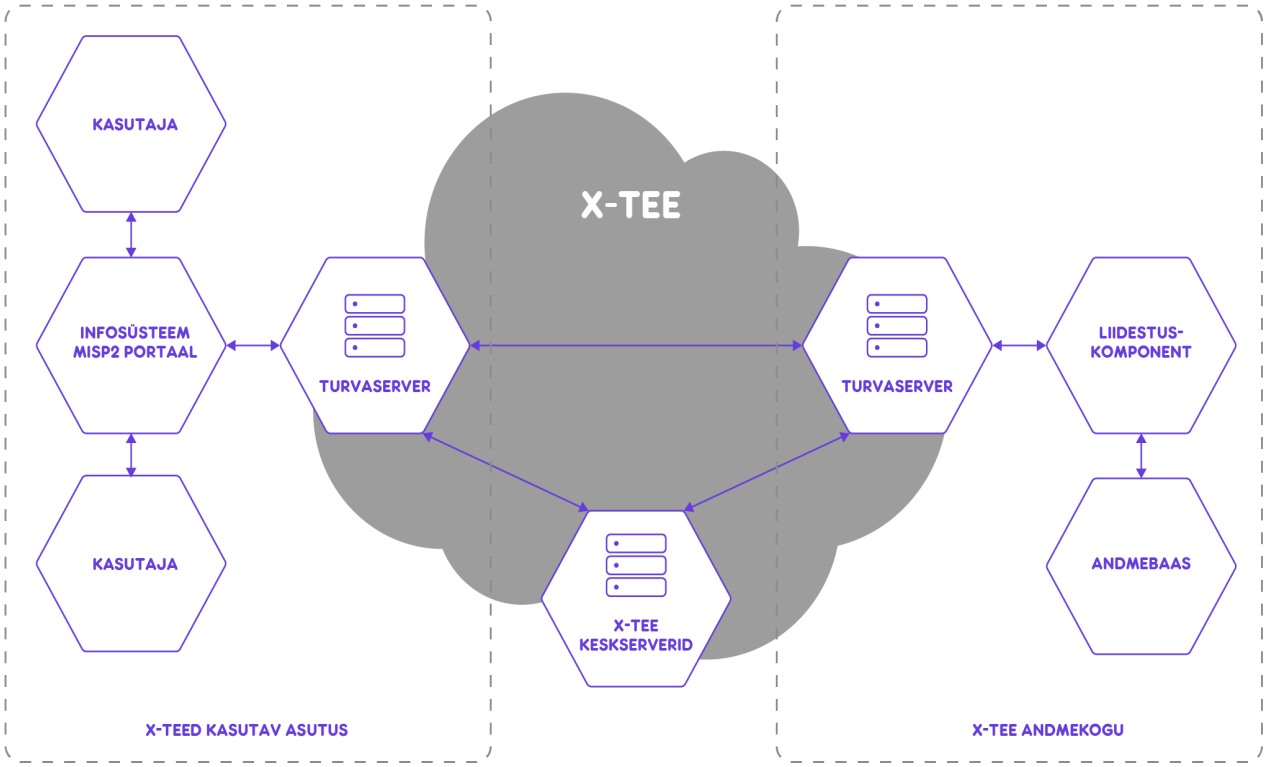
Varem on liidestuskomponenti nimetatud ka adapterserveriks.

Liidestuskomponent ei ole standardne lahendus, mille asutus saaks endale lihtsasti alla laadida ja paigaldada. See tuleb asutusel endal juurde arendada. Mõned soovitused liidestuskomponendi arendamisega seoses on toodud siin.

5.8. MISP

MISP (*mini information service portal*) on standardne veebiportaal, mis on kui liidestuskomponent X-tee ja inimkasutaja vahel. MISPi muudab atraktiivseks tõsiasi, et see suudab teenuseid kirjeldava WSDL faili automaatselt tõlkida kasutajale sobivaks veebivormiks. Sel moel saab kasutaja teenust tarbida tavalise veebilehitseja abil.

MISPi kasutamiseks peab kasutaja end eelnevalt autentima. Ka MISP vajab kontaktpunkti X-teega (turvaserverit). On ettevõtteid, mis pakuvad turvaserveri ja MISPi lahendust näiteks väiksematele omavalitsustele. See säästab omavalitsust vajadusest omada oma serverit ja serveriruumi. MISP kõlbab niisiis tarvitamiseks neile asutustele, kel on tarvidus X-tee kaudu andmeid vahetada, kuid puuduvad võimalused oma infosüsteemi liidestamiseks sellega.



MISPi on lisaks võimalik kasutada keerukamate andmete kogumise ülesannete juures, näiteks siis, kui andmeid kogutakse mitmest andmekogust või kui kasutatakse mitut andmeteenust. Sellisel juhul on MISPi tööd täpsemalt võimalik korraldada XForms tehnoloogiat kasutades. X-tee XForms-kompleksteenuse koostamise lühijuhend on kättesaadav siin.

Lisaks võimaldab MISP X-teega ühenduda ka muudel rakendustel. Selleks pakub see n-ö programmiliste päringute liidest.

MISPi juhendid on leitavad siit.

5.9. Küsimused

Enne õppetüki kokkuvõtte lugemist vasta palun järgmistele küsimustele.

1. Selle, et andmepakkuja infosüsteemile pääseksid ligi vaid andmepakkujaga kokkuleppe sõlminud kasutajad, tagab...

A. Autentimissertifikaat
B. Liidestuskomponent
C. MISP

2. Kohaliku infosüsteemi loogika ja tehnoloogia vastavuse X-tee protokolliga tagab…

A. Turvaserver
B. Liidestuskomponent
C. MISP

3. Kuidas tagab turvaserver vahetatavate andmete terviklust?

A. Päringusõnumite digitembeldamine
B. Vastussõnumite digitembeldamine
C. Kõigi laekunud sõnumite aegtembeldamine mõistliku aja möödudes
D. Kõigi päringu- ja vastussõnumite vahetamine läbi X-tee keskuse

Õigeid vastuseid vaata siit (avanevad uues aknas).

5.10. Kokkuvõte

Turvaserver on “vahemees” X-tee liikme infosüsteemi ja avaliku Interneti vahel. See suunab liikme infosüsteemist saadetud X-tee-keelsed päringud X-teele ning pakendab need selliselt, et need jõuaksid vaid õigete adressaatideni.

Liidestuskomponent tõlgib infosüsteemi sisemise äriloogika ja tehnoloogilise keele koosvõimeliseks X-tee keeleks.

MISP paneb andmeteenuseid kirjeldavad WSDL failid kasutajale sobivasse veebivormi, et too saaks teenuseid tarbida tavalise veebilehitseja abil.