

## 2. Kaalutlused X-tee väljatöötamisel ja X-tee ülesehitus

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid

Kursus: X-tee turvaserveri administraatori õppematerjal

Raamat: 2. Kaalutlused X-tee väljatöötamisel ja X-tee ülesehitus

Printija: Jan Raik

Kuupäev: kolmapäev, 26. august 2020, 11.27

# Sisukord

2.1. Sissejuhatus

2.2. Kahepoolne lahendus

2.3. Keskne infosüsteem

2.4. Teenussiin

2.5. Usaldatud vahendajad

2.6. Terviklusohud ja koosvõime

2.7. X-tee ülesehitus

2.8. Küsimused

2.9. Kokkuvõte

## 2.1. Sissejuhatus

Käesolevas õppetükis tutvustatakse X-tee ülesehitust ja kaalutlusi selle väljatöötamisel.

Pärast õppetüki läbimist suudad Sa kirjeldada X-tee arhitektuuri, selle loomisaegseid alternatiive ning seda, kuidas X-tee arhitektuur lahendab nende alternatiivide puudujäägid.

Õppetüki läbimiseks kulub Sul 10-12 minutit.



Euroopa Liit  
Euroopa  
Regionaalarengu Fond



Eesti  
tuleviku heaks

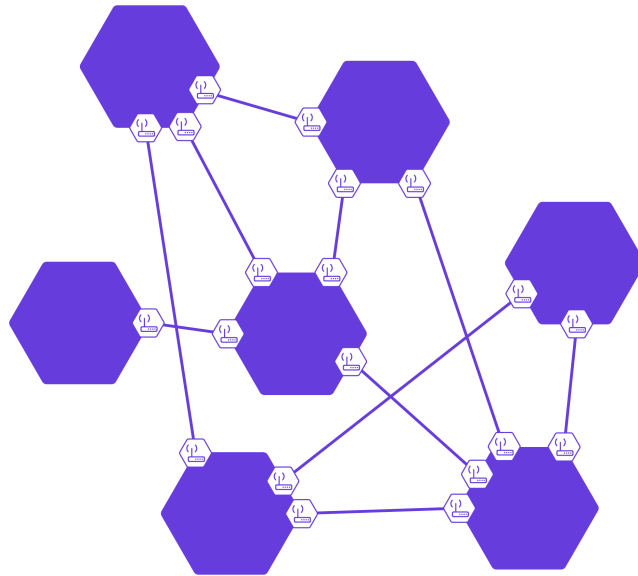


RIIGI INFOSÜSTEEMI AMET

## 2.2. Kahepoolne lahendus

X-tee ülesehitusest ja tööpõhimõtetest arusaamiseks tuleb mõista võimalusi ja kaalutlusi, millest lähtudes X-tee välja töötati.

1990ndate aastate lõpus tekkis vajadus võimaldada suhtlus erinevate infosüsteemide vahel Eestis. Piiratud eelarve tõttu polnud **kahepoolne lahendus**, mille abil iga süsteem suhtleks otse teise süsteemiga võimalik. Kui oht andmete terviklusele ja süsteemi haavatavusele oleks olnud väike, oleks sellise lahenduse ülalpidamine ja tugi olnud **liiga kulukas**. Lisaks oleks edasiste arenduste keerukust arvesse võttes sellest saanud pärandlahendus.



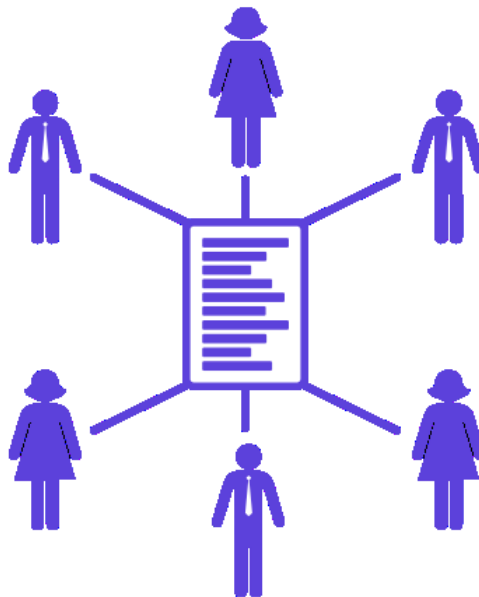
Kahepoolne lahendus

## 2.3. Keskne infosüsteem

Teine võimalus, **keskne infosüsteem**, oleks olnud veelgi problemaatilisem. Keskset suurt infosüsteemi on küll kerge kasutada, ent see on ühtlasi ka kergesti kuritarvitatav.

Lähiajaloo on küllalt näiteid selle kohta, millist ohtu kujutab riiklusele andmete kontrollimatu kogunemine ühte kesksesse infosüsteemi. Keskse infosüsteemi oht ilmnisid esmakordselt 1930-ndate Saksamaal, kus imporditud kartoteegisüsteemid (sisuliselt infotehnoloogia) leidsid kasutust teatud rahvastikugruppide selekteerimisel ja hävitamisel. Eestis realiseerus keskse infosüsteemi oht 1996. aasta septembris, mil demonstreeriti häkker Imre Perli loodud avalikku superinfosüsteemi. See süsteem sisaldas andmeid inimeste elukoha, laenude, telefonikõnede, suhtlusringkonna jms kohta.

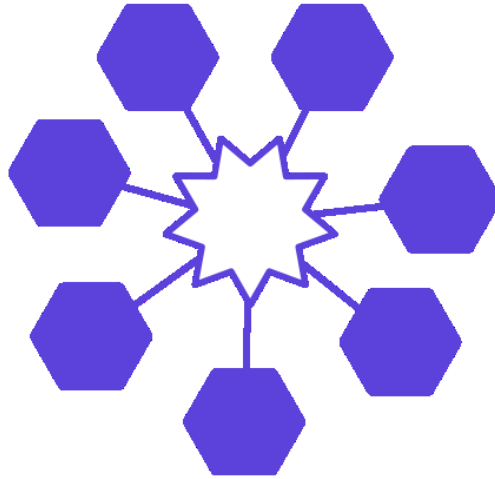
Kokkuvõtteks võib öelda, et keskne infosüsteem oleks **kriitilise tõrkepunkti korral ohustanud andmete konfidentsiaalsust**. Kuigi seda oleks olnud hõlbus hallata ja kulud oleksid olnud väiksed, poleks seda saanud demokraatliku riigi avaliku halduses kasutada. Kui kesksest infosüsteemist oleksid aga kõik võimalused kuritarvitusteks ennetavalt kõrvaldatud, muutunuks see praktiliselt kasutamatuks (Andersoni reegel).



Keskne infosüsteem

## 2.4. Teenussiin

Võimalik oli kasutada ka tarkvara arhitektuurist tuntud keskse andmevahetussiini (ESB) lahendust, mis lisaks klienditaotluse vastuvõtmisele, transleerimisele ja marsruutimisele sobivaks vastusteenuseks teenindab ka tarbeteenuseid. See oleks aga olnud haldamise mõttes keerukas ja kallis lahendus, sest iga ESB-ga ühendatud infosüsteemi oleks tulnud testida iga muu ESB-ga ühendatud süsteemi vastu. See oleks loonud ka kasutaja/juurdepääsu hierarhia ning see on vastuvõtlik inimlikele eksimustele.

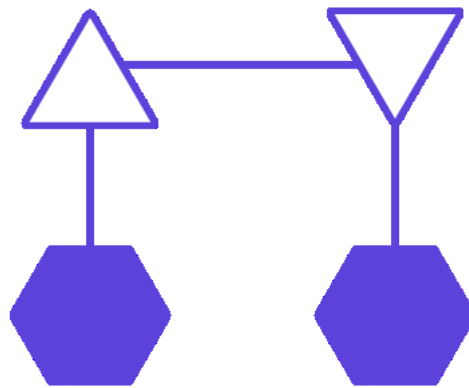


Keskne andmevahetussiin

## 2.5. Usaldatud vahendajad

Põhimõtteliselt saanuks kasutada ka usaldusväärseid teenuse vahendajaid, nagu seda on tehtud finantssektoris *Four-Corner-Model* tüüpi lahenduste abil. Seal on iga äripartner sõlminud lepingu ühe või mitme eraldi teenusepakkujaga, kes tagavad dokumentide õige vahetuse äripartnerite vahel. Tavaliselt pakub avatud standarditel põhinev võrk ühenduvust ja vahendeid äridokumentide turvaliseks ja usaldusväärseks vahetuseks.

Selle lahenduse eesmärk on sõnumi edastamise turvalisus, aga mitte sõnumi standardiseerimine, mistõttu jääks alles sõnumi tõlgendamise probleem erinevate osapoolte vahel. Mida rohkem on osapooli, seda kallim oleks usaldatud vahendusteenuse arendus. Kuigi rünnatavuse risk on siin madal, tõuseks halduskeerukus iga uue liikme lisandumisel.



Usaldatud vahendajad

## 2.6. Terviklusohud ja koosvõime

Arvestada tuli ka terviklusohutudega, st sellega, kas keegi saab infot märkamatult muuta või kas andmed saavad ise „rikneda“. Kui iga asutus säilitaks oma keldris kõiki andmeid, siis juhtuks paratamatult, et ühes asutuses isiku andmeid uuendatakse, teises aga mitte. Nii tekiks ühest isikust mitu erinevate andmetega teisikut ning pärast poleks võimalik öelda, milline neist on õige ja täpsem. Mõned riigid on duplikaate üritanud vältida baaside sünkroniseerimise abil, kuid siin tuleb sisse ajaline nihe, sest pole nii lihtne gigabaite turvaliselt ühest linnast teise toimetada.



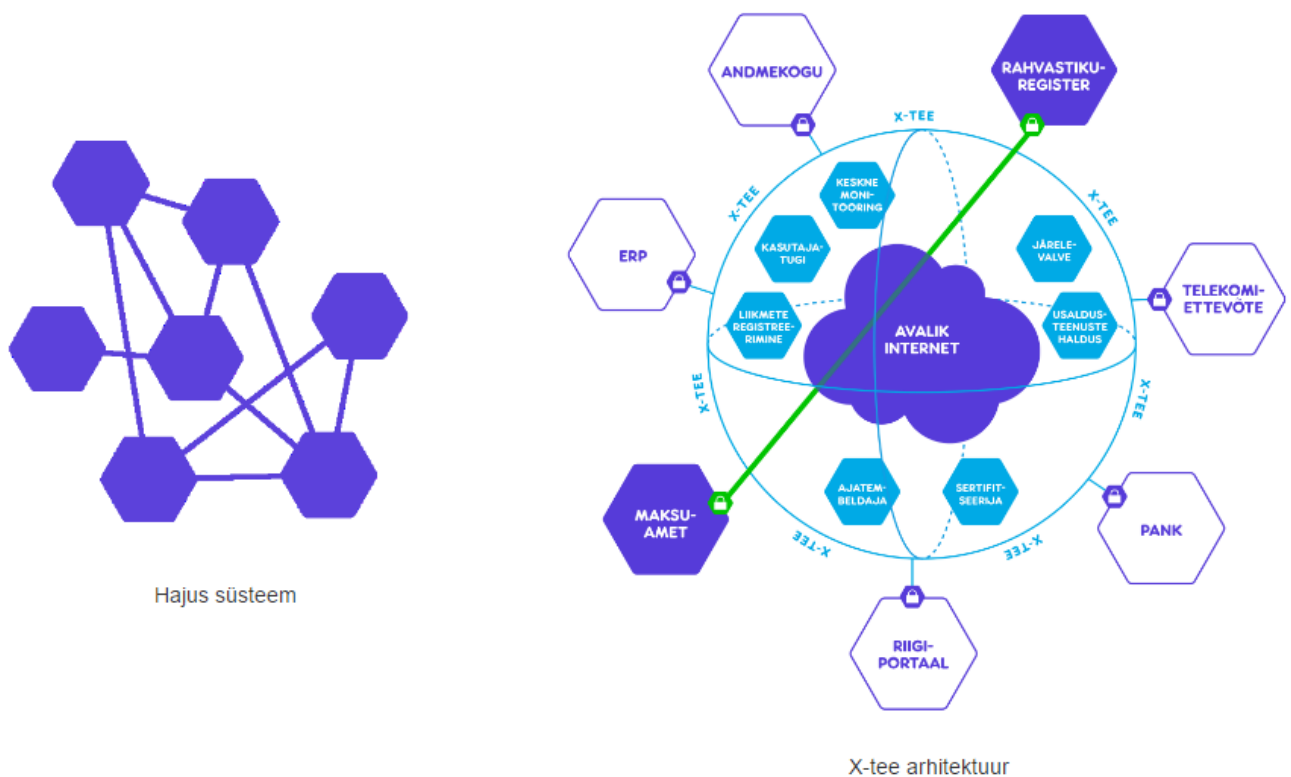
**Niisiis tuli X-tee väljatöötamise käigus tagada, et infosüsteemid, mis olid loodud eri aegadel ning asusid eri tehnoloogilistel platvormidel, suhtleksid üksteisega ühises keeles (standardiseeritus ehk koosvõime).**





## 2.7. X-tee ülesehitus

Ülalkirjeldatud kaalutlustest lähtudes jõuti X-tee **hajusa arhitektuurini**.



X-tee abil saavad liitunud osapooled omavahel turvaliselt suhelda üle avaliku Interneti. Maksu- ja Tolliamet saab teha päringuid Rahvastikuregistrisse. Telekomiettevõtte saab esitada e-arve panka. Kodanik saab riigiportaali kaudu kontrollida andmeid Maksu- ja Tolliameti ning Rahvastiku-registris. Tänu hajusale ülesehitusele ei ole kesket punkti, mille töö lakkamine peataks X-teel andmete vahetuse. Andmeid vahetavad osapooled omavahel otse. Suhtlemine toimub läbi turvaserveri.

X-teel on sõnumiprotokoll kõigile osapooltele sama. Teenust saab osutada ja teiste teenuseid kasutada sarnastel tingimustel ja sarnase tehnoloogiaga. Ei pea iga erineva osapoolega suhtlemiseks oma infosüsteemi lisama uut tehnoloogilist lahendust ega tuge uutele protokollidele.

X-tee kasutamise kulud on võrreldes muude lahendustega madalad, ilma et tõuseks risk andmete turvalisusele.

X-tee hajusa arhitektuuri turvalisust tõestab fakt, et seni pole olnud ühtegi seda seiskavat juhtumit.

## 2.8. Küsimused

**Enne õppetüki lõpetamist otsusta palun, milline alltoodud väidetest on väär.**



- A. X-tee hajus ülesehitus tagab turvalisuse, sest andmeid vahetavad osapooled omavahel otse ning pole keskset punkti, mille töö lakkamine peataks andmevahetuse.
- B. Keskne infosüsteem oleks kriitilise tõrkepunkti korral ohustanud andmete konfidentsiaalsust.
- C. Usaldatud vahendajate kasutamine oleks lahendanud sõnumi standardiseerituse, ent mitte turvalisuse probleemi.
- D. Keskse andmevahetussiooni lahendus oleks olnud kallis ja raske hallata.
- E. X-teel ei pea uute osapooltega suhtlemiseks oma infosüsteemi uut arendust lisama, vaid suhtlemine toimub üle avaliku Interneti.

Õiget vastust vaata siit (avaneb uues aknas).

## 2.9. Kokkuvõte

Käesoleva õppetüki võtab kokku ülalkäsitletud arhitektuuritüüpide põhiomaduste võrdlustabel.

	<b>Kahepoolne lahendus</b>	<b>Keskne infosüsteem</b>	<b>Teenussiin</b>	<b>Usaldatud vahendajad</b>	<b>X-tee</b>
<b>Halduskeerukus</b>	kõrge	madal	kõrge	kõrge	madal
<b>Suhete keerukus</b>	keskmine	keskmine	kõrge	kõrge	madal
<b>Ökosüsteemi kulu</b>	kõrge	madal	kõrge	kõrge	madal
<b>Usaldusväarsuse risk</b>	madal	kõrge	keskmine	madal	madal