4. X-tee tööpõhimõtted ja osalised X-teel

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 4. X-tee tööpõhimõtted ja osalised X-teel
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.28

Sisukord

4.1. Sissejuhatus

Käesolevas õppetükis tutvustatakse X-tee tööpõhimõtteid (eriti turvalisust puudutavat) ning osalisi X-teel. Õppetüki lõpus suudad Sa:

- seletada lahti X-tee tööpõhimõtted,
- kirjeldada, kuidas toimub andmevahetus X-teel,
- selgitada, kuidas saavad liikmed X-teed kasutada,
- loetleda X-tee keskuse ülesandeid ja põhjendada keskuse vajalikkust ning
- defineerida usaldusteenused.

Õppetüki läbimiseks kulub Sul umbes 15 minutit.

4.2. X-tee tööpõhimõtted

X-tee haldamisel järgitakse järgmisi põhimõtteid:

Sõltumatus platvormist ja arhitektuurist
X-tee võimaldab mis tahes tarkvaraplatvormil oleval infosüsteemil suhelda mis tahes tarkvaraplatvormil oleva andmeteenuse osutaja infosüsteemiga.

Mitmepoolsus (multilateraalsus)
X-tee liikmel on võimalus taotleda juurdepääsu kõigile X-tee kaudu osutatavatele andmeteenustele, sõltumata tehnoloogiast või äriloogikast.

Turvalisus
X-tee kaudu andmete vahetamisel ei muutu andmete käideldavus, terviklus ja konfidentsiaalsus. X-tee säilitab liikmetevahelises andmevahetuses andmete omandi ja vastutuse. X-tee tagab, et liikmetest sõltumatuid käideldavust mõjutavaid faktoreid on minimaalselt.

Avatus ja standardiseeritus
X-tee haldamisel ja arendamisel kasutatakse võimalusel rahvusvahelisi standardeid ja protokolle.

4.3. X-tee põhipostulaadid

Iga ametkond X-teel peab omaenda infosüsteemi, kuid ei oma koopiat kõigest muust. Pole asutusi ega inimesi, kel oleks õigus siseneda igasse infosüsteemi. Andmed X-tee keskusest läbi ei käi. Isegi juhul, kui X-tee keskuse turvalisus on ohustatud, on andmete säilimine liidestatud infosüsteemides tagatud, ning vastupidi – rünnak ühe infosüsteemi vastu ei mõjuta teisi infosüsteeme või X-teed.

X-teel vahetatavatele andmetele pääsevad ligi vaid volitatud isikud asutustest või organisatsioonidest, kellega on sõlmitud andmekasutuskokkulepe (**konfidentsiaalsuse** põhimõte). X-tee liige defineerib ise, milliseid andmeteenuseid ta soovib pakkuda ja kellele teenuste kasutamise pääsuõigusi anda (**autonoomsuse** põhimõte). Iga ühendatud asutus on **tuvastatav** (krüptograafilise e-templi sertifikaadi abil). Andmevaldaja võib klientidelt nõuda, et iga päringut tegev isik tuvastataks (näiteks ID kaardiga). X-tee tagab niisiis **liikmete autentsuse** üksteise suhtes.

Samuti garanteerib X-tee, et andmeteenuste abil vahetatavad andmed jõuaksid asjakohaste liikmeteni leketeta ja terviklikult (moondumata ja tõendusväärtuslikult). Andmete moondumine liikmete vahel on tuvastatav (**tervikluse põhimõte**).

Igast liigutusest X-teel jääb jälg. On võimalik **tõendada**, kas ja millal mingi konkreetne andmevahetus toimus. Tõendusvõimet tagavad sõnumite logid tekivad sõnumi saajaks oleva X-tee liikme juurde. Sõnumi õigsuse tõendamiseks tagantjärele ei ole liikmel vaja ühegi kolmanda osapoole kinnitust.

Samuti võimaldab X-tee isoleerida liikmeid, kelle tegevusest või tegevusetusest tekib teistele liikmetele kahju.

4.4. Andmevahetus X-teel

Andmevahetus X-teel toimub üle üldotstarbelise avaliku Interneti. Liikluse muudab turvaliseks **krüpteeritud sidekanal**. Krüpteeritud tunnelid luuakse ajutiselt, st vaid hetkedeks, kui neid tegelikult vaja läheb (*Transport Layer Security / Secure Sockets Layer, TLS/SSL*). TLS ja selle eellane SSL on krüptograafilised protokollid, mis tagavad suhtluse turvalisuse arvutivõrgus. Lisateavet nende kohta leiad siit.

Andmevahetus X-teel toimub üksnes **eelnevalt defineeritud andmeteenuste piires**. Andmete vorming on andmeteenusega üheselt määratud. Vabu päringuid teha ei saa. Kõik päringumallid on eelnevalt ette valmistatud.

Isikuandmete päring isikukoodi alusel (rr.RR72_isik.wsdl)

```
<definitions xmlns:xrd="http://x-road.ee/xsd/x-road.xsd" xmlns:
tns="http://rr-v5.x-road.ee/producer"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-ENC="ht
tp://schemas.xmlsoap.org/soap/encoding/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl
="http://www.w3.org/ns/wsdl"
xmlns="http://schemas.xmlsoap.org/wsdl/"targetNamespace="htt
p://rr-v5.x-road.ee/producer">
<types>
<schema xmlns="http://www.w3.org/2001/XMLSchema" targetNamespac
e="http://rr-v5.x-road.ee/producer">
<import namespace="http://x-road.ee/xsd/x-road.xsd" schemaLocat
ion="http://x-road.ee/xsd/x-road.xsd"/>
<complexType name="XRoadResponseBaseType" abstract="true">...</
complexType>
<complexType name="adsTase">...</complexType>
<simpleType name="year">...</simpleType>
<simpleType name="date">...</simpleType>
<simpleType name="time">...</simpleType>
<simpleType name="PersonalCode">
<restriction base="string">
<pattern value="[1,2,3,4,5,6][0-9]{2}((0[0-9])|(1[0-2]))(([0-2]
[0-9])|(3[0,1]))[0-9]{4}"/>
</restriction>
</simpleType>
<simpleType name="RiigiKood">
<annotation>
<documentation>
Standard ISO 3166 – International Standard Codes for the Repres
entation of the Names of Countries
</documentation>
</annotation>
<restriction base="string">
<pattern value="[0-9][0-9][0-9]"/>
</restriction>
</simpleType>
```

Vajalik WSDL (*Web Services Description Language*) fail tuleb küsida infosüsteemi arendajalt. Loe WSDL-i kohta lähemalt siit.

Andmeteenuste kasutamiseks peab olema sõlmitud leping andmeteenuse osutajaga.

4.5. X-tee liikmed: andmeteenuse osutajad, kasutajad ja vahendajad

X-tee kõige tähtsamad liikmed on **andmeteenuse osutajad**. Nemad jagavad teistele andmeid välja või vastupidi, koguvad neid. Kõik riiklikud registrid on ühtlasi andmeteenuse osutajad.

Enamik liikmeid X-teel on **passiivsed kasutajad**. Nad küsivad andmebaasidest andmeid, kuid ise omaenda andmebaasi ei pea või kui peavadki, siis ei jaga sealseid andmeid teistele X-tee liikmetele. Enamasti toimub see mitte käsitsi ega otse veebilehitsejast, vaid vastav funktsionaalsus on programmeeritud asutuse või ettevõtte infosüsteemi.

Võimalik on ka kombineeritud kasutus ehk siis andmeküsimine ja -jagamine vaheldumisi või suisa samaaegselt. Ise küsime andmeid infosüsteemist A ja B, kodanik teenindusletis annab meile killu lisainfot, mille salvestame omaenda infosüsteemi C, ning viimast infosüsteemi pakume kasutamiseks välja kõigile teistele, muuhulgas infosüsteeme A ja B teenindavatele asutustele. Kolme infosüsteemi (A, B, C) ühendab asjaolu, et andmesubjekti isikukoodi järgi on võimalik edaspidi teha päring kasvõi kolme infosüsteemi korraga (komplekspäring).

X-teel on tõeliselt keerukaid komplekspäringuid, mille tulemusi kuvatakse näiteks alles pärast 37st erinevast infosüsteemist vastuste saamist. Kiiruseületaja isiku, lubade ja kindlustuse kontroll on üks säärastest. Üht lõpuleviidud küsimise-vastuse akti nimetatakse **interaktsiooniks**.

X-tee liikmeteks võivad olla ka **andmeteenuse vahendajad**. Andmeteenuse vahenduse puhul paigaldab X-tee kasutamiseks vajaliku turvaserveri kolmas osapool. Kliendi infosüsteem on X-teega liidestatud selle kolmanda osapoole turvaserveri kaudu. Andmeteenuse vahendus võib olla vajalik nendele asutustele, kelle jaoks on turvaserveri omamine ja haldamine liiga kulukas või kellel ei ole selleks vajalikku IT kompetentsi. Andmevahetuse teenust pakkuvaid ettevõtteid on turul mitmeid.

4.6. X-tee keskus

Ehkki X-tee järgib hajusat arhitektuuri, on sel ometi olemas ka keskus. Miks ei saa ilma selleta?

Tulenevalt tõsiasjast, et X-teel liiguvad krüpteeritud andmed otse ühest infosüsteemist teise või lausa mitmesse korraga, võib keskus esmapilgul näida tõesti üleliigsena.

> **Keskus pole andmevahetuses vajalik. Andmed sealt läbi ei käi. Nii on tagatud, et vahetatavad andmed on kättesaadavad vaid andmevahetuse osapooltele.**

X-tee keskuse olulisus ilmneb, kui vaadelda selle ülesandeid.

- Keskus **väljastab andmevahetuseks vajalikud sertifikaadid** (arenduskeskkonnas) või **tunnustab sobiva sertifitseerimisteenuse pakkuja** (test- ja tootmiskeskkonnas).
- Keskus **võtab vastu uusi liikmeid**. Keda keskuse levitatud „telefoniraamatus“ ei sisaldu, see jääb teistele X-tee liikmetele nähtamatuks. Ilma keskuseta poleks niisiis teada, kellega saab üldse andmeid vahetada.
- Keskus **levitab globaalset konfiguratsiooni** X-tee liikmetele (usaldusahelate aadressid ja avalikud võtmed, teave X-tee liikmete ja nende alamasüsteemide kohta, X-teel registreeritud liikmete turvaserverite aadressid), teave globaalsete juurdepääsuõigustega rühmade kohta, X-tee süsteemiparameetrid, jne).
- Keskus kontrollib, et X-teel järgitaks kehtestatud reegleid (**kasutuse monitooring**), ja **käsitleb turvaintsidente**.
- Keskus **kogub statistikat**, mida liikmete turvaserverid sinna saadavad. Sel moel on teada, millised liikmed omavahel seotud on. Nii on võimalik ökosüsteemi põhiseid riske hallata.
- Lisaks nõustab ja koolitab keskus asutusi ja isikuid X-teega seotud küsimustes.

X-tee keskus Eestis on Riigi Infosüsteemi Amet (RIA). Soomes on keskuseks Rahvastikuregistri keskus (Väestörekisterikeskus, VRK).

4.8. Küsimused

Õppetüki lõpetamiseks otsusta palun, millised alltoodud väidetest on tõesed.

A. X-tee võimaldab mis tahes tarkvaraplatvormil olevatel infosüsteemidel omavahel suhelda.
B. X-teel on tsentraliseeritud ülesehitus, sest andmevahetus käib läbi keskuse.
C. Andmevahetus X-teel toimub üle avaliku Interneti, ent läbi krüpteeritud sidekanali.
D. X-tee liikmel on õigus ise määrata, kellele ta andmeid välja jagab.
E. Tervikluse põhimõte X-teel tähendab seda, et liige defineerib ise, milliseid andmeteenuseid ta teistele pakub.
F. Seda, milliste sertifikaatidega pääseb X-teel andmeid vahetama, määravad usaldus-teenuste osutajad.

Õiget vastust vaata siit (avanevad uues aknas).

4.9. Kokkuvõte

X-tee hajus arhitektuur tagab andmevahetuse käideldavuse, tervikluse ja konfidentsiaalsuse. See võimaldab eri aegadel loodud ja eri tehnoloogilistel platvormidel eksisteerivatel infosüsteemidel üksteisega ühises keeles suhelda (standardiseeritus ehk koosvõime).

Andmevahetus X-teel toimub üle avaliku Interneti, krüpteeritud sidekanalit kasutades ning eelnevalt defineeritud andmeteenuste piires.

X-teel on kolme tüüpi osalisi: X-tee liikmed, X-tee keskus ja usaldusteenuste osutajad.

Andmeteenuseid võib X-tee liige nii osutada, kasutada kui ka vahendada.

X-tee keskus võtab vastu uusi liikmeid, levitab liikmetele globaalset konfiguratsiooni, väljastab andmevahetuseks vajalikke sertifikaate ja tunnustab sobivad sertifitseerimisteenuse pakkujad, teostab X-tee kasutuse monitooringut, käsitleb turvaintsidente, kogub statistikat ning nõustab asutusi ja isikuid X-teega seotud küsimustes.

Usaldusteenused aitavad tõendada nii andmevahetuse osapoole autentsust kui ka seda, millal andmeid päriti või muudeti.

4.7. Usaldusteenused

Oluline tüüp osalisi X-teel on **usaldusteenuste osutajad**.

> **Usaldusteenuste kasutamine on oluline tõendusväärtuse seisukohast. Usaldusteenused aitavad tõendada, et andmeteenuse osapool on tõepoolest see, kes ta väidab end olevat. Samuti võimaldavad need tõendada, millal andmeid päriti või muudeti.**

Andmevahetuse tervikluse ning X-teel vahetatud sõnumi ja X-tee liikme seose tuvastamise tagamiseks on X-tee liige kohustatud turvaserveris kasutama järgmisi usaldusteenuseid:

- **sertifitseerimise teenus**, mille kaudu väljastatakse e-templi sertifikaat ja turvaserveri autentimissertifikaat,
- **sertifikaadi kehtivuskinnituse teenus** ja
- **ajatembeldamise teenus.**

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

Vaata alltoodud videot usaldusteenuste kohta.