TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Informaatika instituut

Liis Mironova 152935IABM

X-TEE PLATVORMI KRIITILISTE KESKSETE TEENUSTE TESTIMINE

Magistritöö

Juhendaja: Gunnar Piho
Doktorikraad
Infosüsteemide
dotsent
Kaasjuhendaja: Heiko Vainsalu
Magistrikraad
Valdkonnajuht

Tallinn 2017

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Liis Mironova

08.05.2017

Annotatsioon

Infosüsteemide andmevahetuskiht X-tee on tehniline ja organisatsiooniline keskkond, mis korraldab turvalist internetipõhist andmevahetust avaliku ja erasektori infosüsteemide vahel. Alates 2015. aasta 2. novembrist algas üleminek X-tee versioonile 6, mis on kohustuslik kõigile X-teega liitunud organisatsioonidele.

Käesolev magistritöö käsitleb uuele X-tee versioonile üleminekuga kaasnenud muudatusi, tarkvara testimise korraldamist, ärianalüüsi planeerimist ja riskianalüüsi tulemusi.

Magistritöö käigus on välja selgitatud olulisemad kriitilised kesksed teenused, millest sõltub X-tee platvormi terviklik toimimine. Töö raames koostatakse testilood iga kriitilise keskse teenuse kohta ning viiakse läbi tarkvara testimine.

Tehtud töö tulemusena on analüüsitud kriitiliste kesksete teenuste toimivust kriisiolukorras. Lisaks on välja toodud meetmed intsidentide ennetamiseks, riskide maandamiseks ja kahjude vähendamiseks katastroofiolukorras. Koostatud testilugusid on tulevikus võimalik kasutada arenduste testimisel ning anda sisendiks automaattestide loomisel.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 82 leheküljel, 4 peatükki, 14 joonist.

Abstract

Testing of critical central services of the X-Road

X-Road, the data exchange layer for information systems, is a technological and organizational environment enabling secure Internet-based data exchange between public and private sector information systems. On 2 November 2015 transition to X-Road version 6 began which is mandatory for all organizations that have joined X-Road.

This thesis deals with the changes that came with the transition to the new version of X-Road, the management of software testing, the planning of business analysis and the results of risk analysis.

The most critical central services on which the consistent functioning of the X-Road platform depends on have been determined during this thesis. Test cases for every critical central service are created and software testing is carried out.

As a result of this thesis, the functioning of critical central services in a crisis situation has been analysed. Furthermore, means to pre-empt incidents, mitigate risks and reduce damage in the case of a catastrophe are introduced. The aforementioned test cases can be used in the future when testing software development and can be used as input for test automation.

The thesis is in Estonian language and contains 82 pages of text, 4 chapters, 14 figures.

Lühendite ja mõistete sõnastik

Alamsüsteem	"Tehnoloogiliselt ja organisatoorselt piiritletud X-tee liikme infosüsteemi osa andmeteenuse osutamiseks või kasutamiseks." [1]
Andmeteenus	"X-tee liikme teenus, mille kaudu toimub internetipõhine andmevahetus." [1]
E-tempel	*Electronic seal.* "Elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mis tagavad viimatinimetatud andmete päritolu ja tervikluse. X-teel kasutatav täiustatud e-tempel vastab eIDASe artiklis 36 sätestatud nõuetele." [18]
HTTP	*HyperText Transfer Protocol.* Andmevahetusprotokoll, mida kasutatakse Internetis dokumentide vahetamiseks, täpsemalt TCP/IP klient-server protokoll HTML-dokumentide vahetamiseks veebis. [19]
Intsident	*Incident*. Ootamatu rike (mis ei ole standardse teenuse osa), mis põhjustab või võib põhjustada IT teenuse planeerimata katkestuse või teenuse kvaliteedi olulise languse. Kaasa arvatud konfiguratsioonielemendi tõrge, mis ei ole veel teenusele mõju avaldanud. [8]
Kehtivuskinnituse teenus	*Online Certificate Status Protocol (OCSP)*. "Elektrooniline teenus, mida tavaliselt osutatakse tasu eest ja mis seisneb e-allkirjade, e-templite või e-ajatemplite, registreeritud e-andmevahetusteenuste ning nende teenustega seotud sertifikaatide kontrollimises." [18]

Konfidentsiaalsus	*Data confidentiality.* "Andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile." [7]
Kvalifitseeritud usaldusteenuse osutaja	*Qualified trust service provider*. "Usaldusteenuse osutaja, kes osutab üht või mitut kvalifitseeritud usaldusteenust ning kellele järelevalveasutus on andnud kvalifitseeritud staatuse." [18]
Käideldavus	*Data availability*. "Eelnevalt kokku lepitud vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (vajalikul ja nõutaval ajahetkel ja vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile." [7]
MIME	*Multipurpose Internet Mail Extensions*. Universaalsed internetiposti laiendused. Eeskiri sõnumite vormindamiseks, mis ei ole ASCII tekstid viisil, et neid saaks edastada üle Interneti. MIME kodeerimissüsteemil põhinev MIME tüüp on Internetis edastatavate andmete kodeerimisel *de facto* standard. [22]
RFC3161	Interneti X.509 standardi avaliku võtme infrastruktuuri ajatempli protokoll, mis kirjeldab päringu saatmise formaati ajatempliteenuse pakkujale ja tagastatava vastuse. [25]
RFC6960	Interneti X.509 standardi avaliku võtme infrastruktuuri sertifikaadi protokoll, mis täpsustab digitaalse sertifikaadi staatuse nõudmata sertifikaadi tühistusnimistut. [26]
RIA	Riigi Infosüsteemi Amet. [15]
RPC	*Remote Procedure Call.* Kaugprotseduurikutse protokoll, mis võimaldab ühes arvutis asuval programmil täita teises arvutis asuvat programmi. Klient saadab serverile vajalikke argumente sisaldava sõnumi ning server tagastab programmi täitmise tulemused. [43]

SOAP	*Simple Object Access Protocol.* "Arvutivõrkudes kasutatav protokoll, millega veebiteenused vahetavad omavahel struktuurseid andmeid, kasutades XML formaati." [20]
Sõnum	"Vormindatud andmete kogum, mida vahetatakse andmeteenuse osutaja ja kasutaja vahel X-tee kaudu." [1]
Teenustaseme lepe	*Service Level Agreement* (*SLA*). Teenustaseme lepe kirjeldab IT teenuse, dokumenteerib teenuse parameetrid ja spetsifitseerib IT teenuse osutaja ja kliendi vastutused. Teenustaseme lepe määratleb maksimaalse mittetöötamise aja või maksimaalse kõrvalekalde teenuse kvaliteedist. Teenustaseme lepe sõlmitakse IT teenuse pakkuja ja kliendi vahel. [8]
Terviklus	*Data integrity*. "Andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine." [7]
TLS	*Transport Layer Security protocol.* "Transpordikihi turbeprotokoll, mis võimaldab klient-server rakendustel omavahel turvaliselt üle Interneti suhelda, olles kaitstud pealtkuulamise või sõnumite rikkumise ja võltsimise eest." [24]
Turvaserver	"Tarkvaraline lahendus, mis järgib X-tee baasprotokollistikku." [1]
Turvaserveri autentimissertifikaat	"Kvalifitseeritud usaldusteenuse osutaja poolt väljastatud ja turvaserveriga seotud sertifikaat, mis tõendab turvaserveri autentsust ja mida kasutatakse turvaserverite autentimiseks turvaserverite vahelise ühenduse loomisel." [32]
WSDL	*Web Services Description Language*. "Protokoll veebiteenuste kirjeldamiseks ja juurdepääsu võimaldamiseks." [21]

X-tee	Infosüsteemide andmevahetuskiht. [1]
X-tee keskus	“Riigi Infosüsteemi Amet, kes vastutab X-tee haldamise ja arendamise eest.” [1]
X-tee liige	“Asutus või isik, kes on liitunud X-teega.” [1]
X-tee sõnumiprotokoll	“X-tee baasprotokollistiku osa, mis võimaldab X-tee liikmetel sõnumeid töödelda.” [1]
X.509	Rahvusvahelise Elekterside Liidu standard, mis määrab avaliku võtme sertifikaatide, äravõetud sertifikaatide nimestike ja volitamissertifikaatide vormingud ning sertifitseerimisradade valideerimisalgoritmi. [23]
XML	*Extensible Markup Language.* Laiendatav märgistuskeel, mille abil jagatakse Interneti veebirakendustes infosüsteemide vahel struktureeritud andmeid. [44]

Sisukord

Jooniste loetelu

1 Sissejuhatus

Vabariigi Valitsuse poolt välja antud "Infosüsteemide andmevahetuskihi" määruse § 2 punkti 1 [1] kohaselt on X-tee tehniline taristu ja keskkond X-tee liikmete vahel, mis võimaldab turvalist ja tõestusväärtust tagavat internetipõhist andmevahetust. X-tee eesmärk on pakkuda Eesti riigi kodanikele ja riigiametnikele juurdepääs riigi andmekogudele kui ühtsele tervikule seitse päeva nädalas ja kakskümmend neli tundi ööpäevas [2]. Riigi infosüsteemi kuuluvatel andmekogudel on kohustus omavahel andmevahetust teostada läbi infosüsteemide andmevahetuskihi [3]. X-teel on tuhandeid andmeteenuseid [4], millest kodanikele mõeldud päringud on kasutatavad kõigile Eesti isikutunnistust omavatele inimestele. Infosüsteemide andmevahetuskiht ei ole suhtlemiseks ainult riigi- ja kohalikele omavalitsusasutustele. Teenuseid osutavad ja omavahelist infovahetust korraldavad ka eraõiguslikud ettevõtted [2]. X-tee tulevikuvisiooniks on pakkuda laialt kasutatavat platvormi. Sealhulgas võimaldada turvalist piiriülest andmevahetust sarnastel alustel kui riigisiseselt [2].

Infoturbeekspert Anto Veldre on Riigi Infosüsteemi Ameti ajaveebis [5] X-teed iseloomustanud järgmiselt: "Tuleb aru saada, et eestlased mingit seniolematult uut infotehnoloogiat siiski kokku ei leiutanud, pigem leiutati olemasolevate infotehnoloogiate baasil uus riigipidamise viis (e-riigi tehnoloogia). Lahendus ise aga sai nimeks X-tee." Tänaseks on X-tee standardne moodus andmevahetuse teostamiseks Eesti avalikus sektoris [6]. Hetkel on X-teel ligi 230 infosüsteemi, umbes 1200 organisatsiooni ja üle 1500 andmeteenuse. See tähendab, et X-tee korrapärane funktsioneerimine on oluline paljudele osapooltele – alates politseiametnikust, kes teostab tööpostil sõiduki üle taustakontrolli kuni kodanikuni, kes soovib näha talle arsti poolt välja kirjutatud retseptiravimeid. Kui arvesse võtta statistikat [4], mille kohaselt sooritatakse ainuüksi ühes kuus X-teel kümneid miljoneid päringuid, siis ka mõned tunnid kestev käideldavust puudutav intsident ei ole X-tee-suguse süsteemi jaoks aktsepteeritav. X-tee keskus peab tagama, et süsteem toimib vastavalt teenustaseme leppes kokkulepitule [9] ja suudab kriisiolukorras säilitada X-tee ökosüsteemi nõuetekohase töötamise ning liikmetevahelise andmevahetuse tõrgeteta funktsioneerimise.

1.1 Probleem

Seoses uue X-tee versiooni 6 kasutuselevõtuga on vaja veenduda, et infosüsteemide andmevahetuskiht on tõrkekindel. X-tee platvormina ei tohi negatiivselt mõjutada liikmetevahelist päringute vahetamise käideldavust ka situatsioonides, kus andmevahetuse toimumiseks vajalikes kriitilistes funktsioonides esineb tõrkeid. Selleks peab tarkvara olema suuteline toimima ja vastama X-tee keskkondadele määratud tehnilistele omadustele [10]. X-teel on kolm erinevat keskkonda:

- andmeteenuste arendamisel kasutatakse arenduskeskkonda, kus liikmeteks ei pea olema päris organisatsioonid ega andmeteks tegelikud andmed;
- andmeteenuste testimisel toimetatakse testkeskkonnas, kus liikmeteks on juriidilised isikud ja kasutusel testandmed;
- andmeteenuste testimisega lõpule jõudmisel liitutakse toodangukeskkonnaga, kus liikmeteks on reaalsed organisatsioonid ja andmeteks reaalsed andmed.

Organisatsiooniga, kes soovib X-tee toodangukeskkonnaga liituda, sõlmib X-tee keskus teenustaseme leppe. Selles määratletakse kui kiiresti eri olukordades tõrked kõrvaldatakse. Arendus- ja testkeskkondade puhul teenustaseme lepet ei sõlmita. Nendes keskkondades toimub tõrgete kõrvaldamine esimesel võimalusel olenevalt vabade ressursside olemasolust [11]. Magistritöös keskendub autor eelkõige toodangukeskkonnale, kuna selle toimimine on reaalsete organisatsioonide ja andmete vahetamise tõttu kõige kriitilisem. Ühtlasi on tegemist ainsa X-tee keskkonnaga, mis on kaetud teenustaseme leppega. Kui toodangukeskkonna tõrketaluvus on tõestatud, siis on seda võimalik tulevikus rakendada ka test- ja arenduskeskkondadele.

Kui X-tee platvorm ei vasta tõrketaluvuse ootustele, siis on intsidentide toimumisel mõjutatud sajad infosüsteemid ja organisatsioonid, kelle igapäevane andmevahetus võib olla häiritud. Arvesse võttes asjaolu, et üleminek uuele X-tee versioonile 6 (vt peatükk 2.3) on juba toimumas, siis on oluline võimalikult varakult kindlaks teha, kas X-tee süsteemi komponendid (vt peatükk 3.1) ja kriitilised kesksed teenused (vt peatükk 3.3) ka reaalsuses töötavad ettenähtud tingimustel. Kui selgub, et mitte, siis tuleb määratleda ja kõrvaldada puudused.

Ajahetkel, mil magistritöö kirjutamisega alustati, oli X-tee versioon 6 toimimiseks vajalike komponentide ja kesksete teenuste katkestuste üleelatavus testimata tehnilisel ja organisatoorsel kujul. See ei võimalda olla kindel süsteemi probleemideta toimimises vastavalt keskkonna tehnilistele omadustele ja pärsib X-tee keskuse valmisolekut katastroofiolukordades reageerimiseks. X-tee on viisteist aastat olnud kõiki liikmeid puudutavate tõrgeteta [4] kasutusel Eesti riigi infotehnoloogilise selgroona – on oluline, et nii see ka jääks.

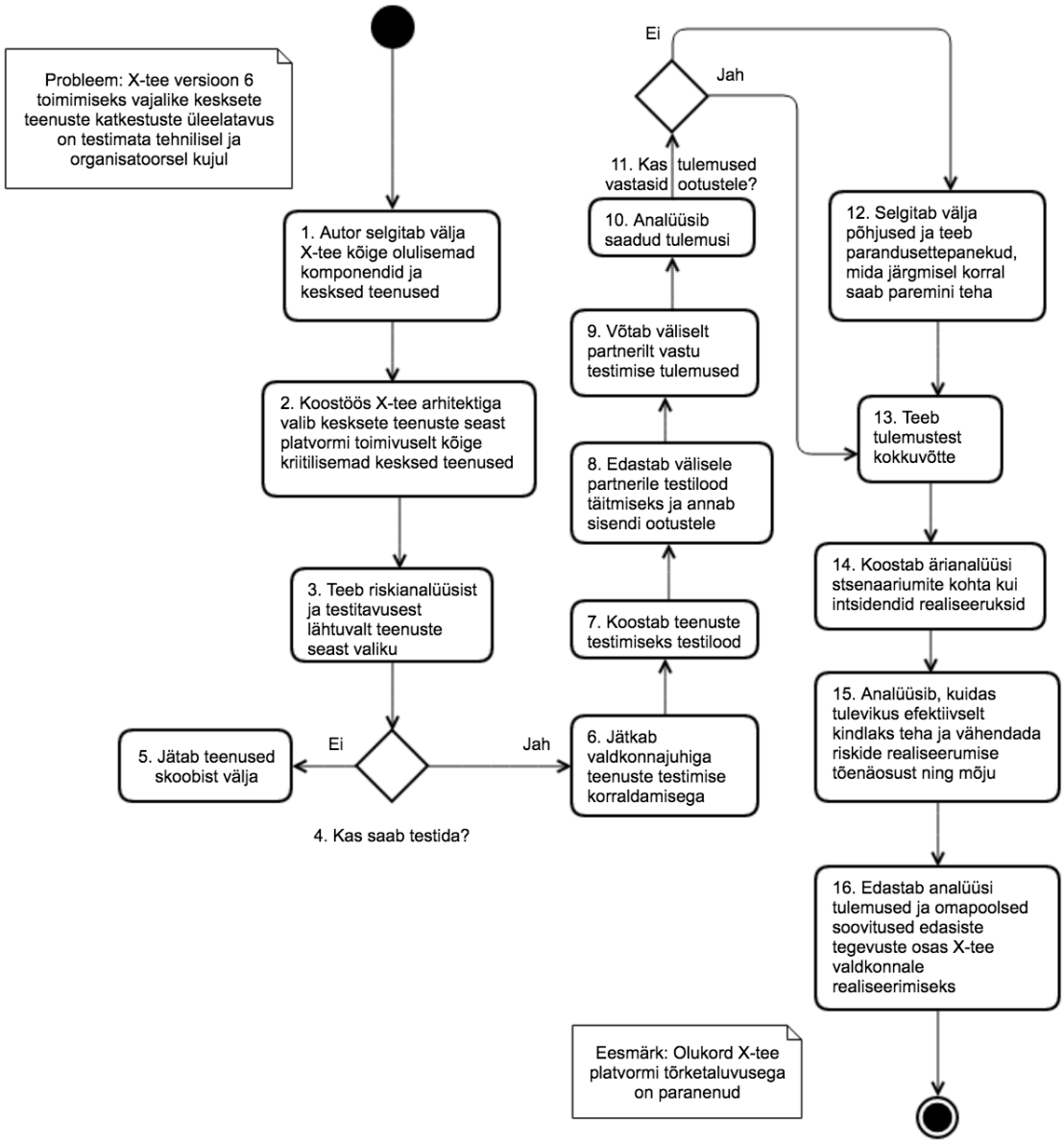
1.2 Eesmärk

Käesoleva magistritöö eesmärgiks on analüüsida ja välja selgitada, kas X-tee versioon 6 toimimiseks vajalikud komponendid ja teenused töötavad vastavalt tehnilistele omadustele või mitte. Selleks vaatleb autor X-teel eduka andmevahetuse seisukohalt kõige olulisemaid komponente ja keskseid teenuseid ning teeb nende seast valiku. Seejärel koostab kriitilisemate kesksete teenuste testimiseks testilood, mis näitavad, kuidas situatsiooni muutus mõjutab andmevahetust X-teel ja süsteemi üldist toimimist. Testide läbiviimise tulemusena selgub, kas seni paikapidanud oletused on tõesed ja kehtivad X-tee versioon 6 puhul. Lisaks koostab autor ärianalüüsi, mis võimaldab hinnata tagajärgi juhul, kui intsidendid realiseeruvad ja kaardistada edasisi tegevusi. Töö tulemusena tekib sisend, kuidas tulevikus efektiivsemalt kindlaks teha, et ka pärast järgmisi X-tee tarkvara arendusi ei kannata kriitilised funktsioonid.

Magistritöö on aktuaalne, kuna X-tee tõrketaluvuses selgusele jõudmine annab X-tee keskusele veendumuse, et kriisiolukorras suudetakse probleemid lahendada enne kui need jõuavad mõjutada lõppkasutajaid. Infosüsteemide andmevahetuskihi haldamise üks põhimõtetest on turvalisus, mille kohaselt ei muutu X-tee kaudu andmete vahetamisel andmete käideldavus, terviklus ega konfidentsiaalsus [1]. Antud magistritöö käsitleb eelkõige käideldavuse parameetrit. Varasemalt on kindlustunne platvormi käideldavuse tagamisel baseerunud paljuski arhitektuursele lahendusele ja X-tee kui platvormi toimimise loogikale. Reaalselt ei ole keerukamaid piirsituatsioone testitud, mis pärsib ka nende ennetamist ja valmisolekut ekstreemsetes olukordades adekvaatselt reageerida. Eelnevalt väljatoodud tegevuste täitmine võimaldab veenduda X-tee versioon 6 tarkvara korrapärases toimivuses, aitab välja tuua süsteemi nõrkused, juhtida tähelepanu lahenduste otsimisele ja leida võimalused riskide maandamiseks.

1.3 Töö protsess

Magistritöös seatud eesmärgi täitmiseks järgib autor töö protsessi, mis on kujutatud Joonisel 1.



Joonis 1. Töö protsessi tegevusdiagramm autori vaatest

Esmalt selgitab autor välja X-tee kui terviku toimimise seisukohalt kõige olulisemad komponendid ja kesksed teenused (vt Joonis 1 punkt 1). Seejärel valib koostöös X-tee arhitektiga kesksete teenuste seast välja eduka andmevahetuse vaatest kõige kriitilisemad kesksed teenused. Järgmise sammuna teeb nende seast valiku testitavusest lähtuvalt (vt Joonis 1 punkt 4). See tähendab, et kui mõnda teenust ei ole võimalik

teatud põhjustel mõistlikul viisil testida, siis sellised teenused jäetakse teadlikult skoobist välja. Need võetakse vaatluse alla hiljem käesoleva töö väliselt.

Teisalt otsustab autor koos valdkonnajuhiga lähtudes eelnevalt välja valitud kriitilistest kesksetest teenustest testimise tehnikate üle (vt Joonis 1 punkt 6). Pärast seda koostab teenuste testimiseks testilood, mille alusel on võimalik veenduda, kuidas keskkonnale määratud parameetrite ületamine mõjutab andmevahetust X-teel. Testimiseks kasutatakse välise partneri kaasabi. Autor annab testilood täitmiseks testijatele, kes realiseerivad testilugudes olevad sammud. Testilugudes on välja toodud oodatud tulemused, mis testide läbimise järel peavad tekkima.

Magistritöö skoobis on lisaks ka analüüsida, kas testilood on õigesti koostatud ja aitavad veenduda teenustele määratud tehniliste omaduste paikapidavuses. Samuti annab testimine vastuse küsimusele, kas tulevikus tuleks antud probleemile teistmoodi läheneda. Testimise tulemuste põhjal saab X-tee keskus veenduda, kas testilood läbitakse vastavalt oodatule. Kui testilugude põhjal käivitatavad testid ei anna oodatud väljundeid, siis selgitab autor välja põhjused ja teeb parandusettepanekud, millega järgmisel korral täiendavalt arvestada (vt Joonis 1 punkt 12). Kui selgub, et testilood on täitnud oma eesmärgi ja testimise tulemused vastavad ootustele, siis teeb autor järgmise tegevusena testimisest kokkuvõtte (vt Joonis 1 punkt 13).

Ühtlasi on plaanis koostada ka ärianalüüs (vt Joonis 1 punkt 14). Lisaks püüab autor leida võimalused, kuidas tulevikus vähendada ohtude realiseerumise tõenäosust ja mõju. Eelneva põhjal tekib sisend, kuidas edaspidi efektiivsemalt kindlaks teha, et X-tee tõrketaluvus on säilinud ning meetodid, kuidas taastada võimalikult tõhusalt X-tee töövõime intsidentide toimumisel. Kogu Joonisel 1 näidatud protsessi täitmise tulemusena jõuab autor lahenduseni ja olukord X-tee tõrketaluvuse osas paraneb.

1.4 Töö struktuur

Magistritöö teises osas annab autor ülevaate X-teest ja tarkvara testimisest. Kolmandas osas esitab peamised ja olulised tulemused ehk kriitiliste kesksete teenuste valiku ja testide koostamisel arvesse võetu. Lisaks toob autor välja X-tee süsteemi komponendid ja protokollid. Neljandas osas analüüsib töö tulemusi ehk läbiviidud testimist ja teeb järeldused. Lõpuks põhjendab võimalikke riskide maandamise meetodeid ja annab

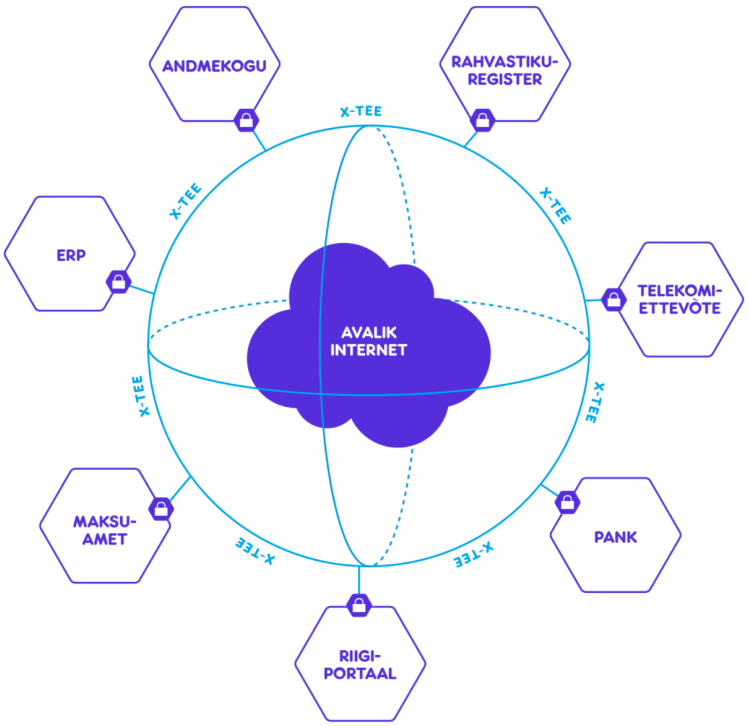
soovitused edasiseks. Töös kasutatud lühendid ja mõisted on defineeritud ning nende pärinemise allikatele on viidatud peatükis “Lühendite ja mõistete sõnastik”. Lühendite ja mõistete kasutamisel neile töö peatükkides rohkem ei viidata.

2 Ülevaade X-teest ja tarkvara testimisest

Peatüki eesmärgiks on anda ülevaade X-teest ja tarkvara testimisest, et kolmandas osas selgitatud X-tee komponendid, protokollid, kriitilised kesksed teenused ja testid ning neljandas osas põhjendatud analüüs, järeldused ja soovitused oleksid arusaadavad.

2.1 X-tee taust

X-tee loomist koordineeris Majandusministeeriumi riigi infosüsteemide osakond ja riiklikult hakati seda juurutama 2001. aastal [12]. Joonisel 2 [13] on kujutatud X-tee olemus, mis vastab algsele visioonile ja kehtib tänaseni.



Joonis 2. X-tee olemus

Jooniselt 2 on näha, et andmevahetus liikmete vahel toimub üle avaliku Interneti turvalise X-tee andmevahetuskihi kaudu. Andmeid vahetavateks osapoolteks on X-teega liidestunud infosüsteemid ja erinevad organisatsioonid nii avalikust kui ka erasektorist.

X-teest on välja kujunenud platvorm, mis tagab liikmetele andmevahetuses:

- autonoomsuse – X-tee liige defineerib ise, milliseid andmeteenuseid soovib pakkuda ning kellele teenuste kasutamise pääsuõigusi anda;
- käideldavuse – andmevahetus toimub otse liikmete vahel ega sõltu kesksetest komponentidest;
- konfidentsiaalsuse – info jõuab X-tee vahendusel vaid nende osapoolteni, kellele on selleks õigus antud;
- tõestusväärtuse – e-templi kasutamine võimaldab tõestada, kellelt laekunud andmed pärinevad;
- koosvõime – sõltumata liikme poolt kasutatavast tehnoloogiast või arhitektuurist räägivad kõik X-tee liikmed üksteisega ühises keeles. [14]

X-tee võimaldab liikmetel säästa aega ja vahendeid, mis kuluksid organisatsioonidel turvaliste süsteemide väljatöötamisele, kahepoolsete kokkulepete sõlmimisele ja töös hoidmisele. Infosüsteemide andmevahetuskihiga liitumisel tekib võimekus vahetada andmeid kõigi X-tee liikmetega. [14]

Käesoleval ajal vastutab X-tee platvormi haldamise ja arendamise eest keskus ehk Riigi Infosüsteemi Amet (edaspidi RIA) [1]. RIA koordineerib riigi infosüsteemi arendamist ja haldamist, korraldab infoturbega seotud tegevusi ja käsitleb Eesti arvutivõrkudes toimuvaid turvaintsidente [15]. RIA nõustab riigi infosüsteemi osalisi, kuidas oma infosüsteeme nõuetekohaselt hallata ja teostab nende üle järelevalvet [16]. RIA missiooniks on koordineerida riigi infosüsteemi arendamist ja haldamist nii, et riik saaks rahvast teenindada parimal võimalikul moel, rakendades targalt IT võimalusi.

Riigi infosüsteemi valdkondade hulka kuuluvad lisaks infosüsteemide andmevahetuskihile (X-tee valdkond) ka riigi infosüsteemi haldussüsteem ja kataloog RIHA, riigiportaal eesti.ee, avaliku võtme infrastruktuur PKI ning dokumendivahetuskiht DHX [16]. Magistritöö autor töötab RIA-s teenuste halduse osakonnas X-tee teenusehaldurina.

2.2 X-tee arhitektuur

Peatükk sisaldab X-tee tuumtehnoloogia tehnilist arhitektuuri, et anda ülevaade süsteemi toimimis- ja tööpõhimõtetest. Järgnev loetelu koosneb arhitektuursetest eesmärkidest ja otsustest, mis võeti vastu X-teed kujundades ja arendades [17].

- X-tee on hajus ja detsentraliseeritud ehk andmed liiguvad andmevahetuse käigus otse ühelt liikmelt teisele, ilma vahendajateta. Vahetatud sõnumid on krüpteeritud. Seega ei ole andmed kolmandatele osapooltele nähtavad.

- X-tee ühendab erinevaid infosüsteeme vaatamata nende poolt kasutusel olevatele platvormidele. Keskselt ei määrata tööriistu ega tehnoloogiaid, mida osapooled organisatsioonisiseselt peavad kasutama.

- X-teel andmete vahetamisel ei muutu nende omanik. Andmete omanikuks on teenuse pakkuja, kes otsustab, kellele anda juurdepääs konkreetsele andmeteenusele.

- Andmete omanik määratakse kõigile X-teel töödeldavatele sõnumitele elektroonilise allkirjastamisega, mis muudab kõik sõnumid digitaalse tõendina kasutatavaks. Tehniline lahendus järgib e-templi nõudeid vastavalt eIDASele [18]. Kõik sõnumid, nii saadetud päringud kui ka vastuvõetud vastused allkirjastatakse kvalifitseeritud sertifikaadiga. Tulenevalt sertifitseerija nõuetest kasutatakse allkirjastamise käigus turvalist allkirja andmise vahendit. Allkirjastatud sõnumid on ajatembeldatud ja logitud, mis võimaldab hiljem kontrollida allkirjade kehtivust ehk universaalselt tõestada, kas ja milliseid andmeid ning millisel ajahetkel liikmed vahetasid.

- Protokollid (vt peatükk 3.2) on disainitud viisil, et X-tee platvormis ei oleks ühtegi “pudelikaela” (ingl k *bottleneck*). Komponendid on loodud põhimõttel, mille kohaselt ühe komponendi rike ei mõjuta ülejäänud süsteemi tööd (ingl k *a single point of failure*).

X-tee baseerub avalikel standarditel – HTTP, SOAP, WSDL, MIME, X.509, TLS, RFC3161, RFC6960.

2.3 Üleminek X-tee versioonile 6

RIA algatas liikmete X-tee versioonile 6 ülemineku 2015. aasta lõpus [27]. X-tee versioon 6 eesmärk on muuta selgemaks senist turvaskeemi ja tagada infosüsteemide andmevahetuskihi kaudu vahetatavate sõnumite terviklus kasutades selleks täiustatud e-templit kvalifitseeritud sertifikaadiga [18]. Sellest tulenevalt võivad sertifikaate väljastada kõik kvalifitseeritud usaldusteenuste osutajad Euroopas. Varasemalt on sertifikaate väljastanud RIA, kuid uue versiooni puhul on võimeline seda teenust hetkel Eestis ainsana pakkuma SK ID Solutions AS [28]. Kõigi liikmete poolt uue versiooniga kohanemine ja pärandvarast (ingl k *legacy*) vabanemine võtab aega vähemalt paar aastat, kuna tegemist on suurte muudatustega.

Võrreldes X-tee versiooni 5 versiooniga 6 kajastuvad põhilised erinevused nende vahel metoodikas, kuidas turvaserverid sõnumeid töötlevad, samuti X-tee sõnumiprotokollis ehk millise struktuuriga sõnumeid turvaserverid vahetavad [29]. Kogu X-tee ajaloo jooksul on kasutusel olevat sõnumiprotokolli muudetud neli korda [4] ning tehnoloogilisele lahendusele tehtud suuremaid uuendusi viiel korral. Hetkel on käimas neljas protokollistiku muudatus, millega kaasnebki uue X-tee versioon 6 tarkvara kasutuselevõtt. Kui X-tee versioon 5 toetas sõnumiprotokolli versioone 2.0, 3.0 ja 3.1, siis X-tee versioon 6 toetab vaid sõnumiprotokolli versiooni 4.0 [30]. See muudatus puudutab lisaks keskusele ka kõiki liikmeid, kes peavad oma teenused uuele versioonile vastavaks arendama.

Muudatused on ka liikmelisuses ja pääsuõigustes. X-tee versioonis 5 eristati teenuse tarbijaid ja pakkujaid sertifikaatide tasemel – esimesi organisatsioonina ning teisi infosüsteemina. X-tee versioonis 6 on liikmeteks organisatsioonid, kellega on seotud alamsüsteem(id). Alamsüsteem on X-tee liikme infosüsteem või selle osa. Alamsüsteem kasutab eelnevalt mainitud X-tee liikme täiustatud e-templi kvalifitseeritud sertifikaati [28]. Ühel organisatsioonil võib olla mitu alamsüsteemi, mis on teineteisest sõltumatud. Varasemalt andis infosüsteemi haldaja pääsuõigused asutusele, nüüd hallatakse pääsuõiguseid alamsüsteemi tasandil. Kui ühele alamsüsteemile antakse teatud andmeteenuste kasutamiseks pääsuõigused, siis ei mõjuta need sama liikme teiste alamsüsteemide pääsuõigusi [31].

X-tee versioonis 5 ei olnud turvaserverid peale IP aadressi kuidagi identifitseeritud, kuid versioonis 6 omavad nad sertifikaadist sõltumatut identifikaatorit. Igal turvaserveril peab ka olema kehtiv autentimissertifikaat, mida kasutatakse turvaserverite autentimiseks ja nendevahelise krüpteeritud ühenduse loomiseks. Muutunud on ka usaldusteenuste tarbimine. Varasemalt ei teinud turvaserver kehtivuskinnituse ega e-ajatempli päringuid, kuid versioonis 6 teostab [28].

Kaugemale ulatuvaks, uue X-tee versiooni 6 loomise põhjuseks, oli vajadus tagada rahvusvaheline andmevahetus ja X-tee kooskõla E-identimise ja e-tehingute usaldusteenuste seadusega [33]. Tegemist ei ole pelgalt tarkvara versiooni uuendusega. Kaasnevad muudatused on paljuski organisatoorsed. Võrdluseks võib tuua, et eelnevad suuremad protokollistiku muutustega seotud üleminekud on aega võtnud aastaid. Seega tegemist on mastaapse uuendusega.

Eelnevalt kirjeldatud võrdlused versioonide vahel näitavad selgelt, et keerukaid muudatusi on palju. Sellest tulenevalt on X-tee keskus pidanud modelleerima uued haldusprotsessid ja korraldama senisest veelgi rohkem arutelusid koostööpartneritega. Vaatamata sellele, et X-tee versioon 6 tugineb algsele X-tee arhitektuurile ja põhimõtetele, sisaldab see ka funktsioone, mida X-tee varem ei teostanud või täitis teistmoodi. Seetõttu tuleb keskusel tarkvara testimise abil kindlaks teha, et andmevahetuse toimimine vastab nõuetele.

2.4 Ülevaade tarkvara testimisest

Tarkvara testimise eesmärk ISO/IEC/IEEE 29119-1:2013 [34] standardi kohaselt on tarkvara kvaliteedi kontroll, mille käigus veendutakse toote vastavuses soovitule. Testimine ei ole üks ainus tegevus, vaid terviklik protsess. Testimise protsessi käigus selgub, kas arendatud lahendus vastab nõuetele, eeldatavatele funktsionaalsustele ja kasutajate vajadustele. Nõuded on vahend tulemi kvaliteedi defineerimiseks erinevatest vaatepunktidest [35]. Tarkvara mittevastavus nõuetele on viga ja testimine on vajalik vigade leidmiseks. Veaks loetakse ka tarkvara mittevastavust vajadustele, teisisõnu sobimatust probleemi lahendamiseks. Mõned vigadest võivad olla vähem olulised, kuid teised seevastu kriitilised [36]. Käesolevas töös keskendutakse kriitilistele vigadele.

Tarkvaratoote kvaliteedi hindamiseks kasutatakse tarkvara kvaliteediatribuute. Selleks on palju erinevaid skeeme, kuid üks levinumaid rahvusvahelisi standardeid on üle võetud ka Eesti standardiks – EVS–ISO/IEC 25010:2011 [37]. Selle alusel peab tarkvara kasutamisel olema töökindel, efektiivne ja kasutajasõbralik ning täitma vajalikke funktsioone ka pärast hooldamist ning erinevatele riist- ja tarkvaraplatvormidele üle viimist [38]. Eelnevast lähtudes on defineeritud kvaliteedifaktorid: funktsionaalne sobivus, töökindlus, kasutatavus, hooldatavus, tõhusus, ühilduvus, turvalisus ja porditavus. Igal kvaliteedifaktoril on talle omased atribuudid, mida toote hindamisel jälgitakse. Antud töö skoobis on töökindluse faktor, mille atribuutideks on [38]:

- käideldavus - tarkvaratoote suutlikkus olla seisundis, kus ta saab antud ajahetkel täita deklareeritud kasutamistingimustel nõutavat funktsiooni;
- tõrketaluvus - tarkvaratoote suutlikkus säilitada spetsifitseeritud sooritusvõime tase tarkvara defektide puhul või tootele spetsifitseeritud liidese rikkumise puhul;
- küpsus - tarkvaratoote suutlikkus vältida tarkvara defektidest tulenevaid tõrkeid;
- taastuvus - tarkvaratoote suutlikkus tõrke korral ennistada spetsifitseeritud sooritusvõimetase ja taastada andmed, mida tõrge otseselt mõjutas.

Testimist planeerides tuleb arvestada nii aja- kui ka rahakuluga, mis seab piirangud testimise ulatusele. Seetõttu on praktikas võimalik realiseerida ainult osa testidest. On selge, et vigade tekkimist ei ole võimalik täielikult vältida, kuid efektiivne testimisprotsess võimaldab suure osa olulistest vigadest leida. Mida varasemas tarkvara elutsükli faasis vead leitakse, seda odavam on nende parandamine [39]. See on ka üheks argumendiks, miks on X-tee tõrketaluvuses veendumine valdkonnale antud etapis prioriteediks.

Lisaks peab arvestama asjaoluga, et kõrvaltvaataja võib suurema tõenäosusega vigu leida kui näiteks arendaja, kes toote arendamisega pidevalt tegeleb. Põhjuseks on valed eeldused ja harjumused ning korduvad vead, mida tarkvaraga kursis olev inimene teeb [36]. Seetõttu on kasulik lasta tarkvara testida neil, kelle jaoks on testitav objekt võõras.

Esimese testimise printsiibi kohaselt näitab testimine vigade olemasolu. See tuleneb teaduslikust eksperimendist ja on testijate poolt omaks võetud. Testimine aitab välja tuua vigade olemasolu, kuid ei suuda tõestada, et vigu ei eksisteeri. Testimine vähendab tarkvaras avastamata vigade esinemise tõenäosust, kuid isegi siis kui vigu ei leita, ei saa kindel olla, et ühtegi viga ei ole [36]. Järelikult ei olegi kõige olulisem tõestada, et tarkvaras ei esine ühtegi viga, vaid veenduda, et see vastab oodatule.

Kokkuvõttes on esmatähtis, et tarkvara aitaks kasutajal teatud funktsioone efektiivselt täita. Isegi kui tarkvarast suudetaks leida kõik vead ja need ka parandataks, kuid sellegipoolest ei vastaks see soovitule, siis kasutajad lõpetaksid ikkagi selle kasutamise. Sel põhjusel tuleb tarkvara testimise eesmärgiks pidada mitte pelgalt vigade leidmist, vaid kvaliteedi kontrolli. Testimine annab informatsiooni otsuste langetamiseks. Kvaliteetne info aitab vastu võtta õigeid otsuseid, mis omakorda soodustab riskide maandamist [35].

2.5 Testimise tehnikad

Vastavalt testimise täpsemale eesmärgile eristatakse mitmeid testimise liike. Peamiselt kategoriseeritakse Rahvusvahelise Tarkvara Testimise Kvalifikatsiooniliidu (ingl k *International Software Testing Qualifications Board, ISTQB*) järgi staatilist ja dünaamilist testimist. Staatilise testimise puhul ei käivitata programmikoodi, vaid vaadatakse üle ja analüüsitakse kogu tarkvaraga kooskäivat dokumentatsiooni, sealhulgas tarkvara lähtekoodi [36]. Antud juhul lähtutakse testimise klassifikatsiooni valikul meetodist ja lähenemisest. Käesolevas töös kasutatakse dünaamilist testimist, mille käigus käivitatakse testitav objekt ehk programm ja uuritakse selle käitumist [39].

X-tee tõrketaluvuses veendumiseks otsustas X-tee valdkond manuaalse testimise kasuks, mille kohaselt viiakse testilood läbi käsitsi. Manuaalset testimist eelistades võeti arvesse asjaolu, et tegemist on testimisega, mida varem ei ole nii suures mahus ühe korraga läbi viidud ja see sisaldab testilugusid, mida ei ole veel kordagi reaalselt testimisel kasutatud. Seega ei oleks mõistlik sellistele testilugudele koheselt läbi proovimata automaatteste luua. Manuaalselt testimiselt saadud tulemustest saab sisendi tulevikus automaattestide kirjutamiseks, et edaspidi anda need täitmiseks arvutile. Testide automatiseerimisel lähtutakse üldjuhul ärikriitilistest, korduvatest ja aeganõudvatest testilugudest. Lisaks ka stsenaariumitest, mida on keeruline manuaalselt

testida [40]. Valdkond on juba vastu võtnud otsuse, et automaattestid luuakse, kuid need teostatakse tulevikus ega mahu antud töö skoopi.

Manuaalse testimise käigus vaatleb testija tarkvara kui "musta kasti", teadmata midagi selle sisemisest struktuurist. Musta kasti testimist kasutatakse enamasti funktsionaalse testimise puhul, kuid välistatud ei ole ka mittefunktsionaalne testimine. Musta kasti testimist samastatakse testilugudel põhineva testimistehnikaga. Mõlema meetodi puhul on sisuliselt tegemist sisend-väljund testidega, milles testija keskendub küsimusele "mida" tarkvara teeb, mitte eriti "kuidas" ta seda teeb. Kasutuslugudepõhist testimist võib rakendada kõigil testimise tasemetel. Süsteemitestimisel on see eriti abiks, kuna nõuded ja funktsionaalsused on testide aluseks [36].

Süsteemitestimise käigus testitakse kogu süsteemi vastavust tootele esitatud nõuetele. Süsteemitestimine on ühtlasi ka musta kasti testimise alaliik [39]. Selles võib katta testid, mille aluseks on riskid, nõuded, äriprotsessid, kasutuslood või teised dokumendid, mis selgitavad süsteemi käitumist kõrgemal tasemel. Süsteemitestimist viiakse üldjuhul läbi viimaste testimiste seas tarkvara valmimise lõppfaasis. Seeläbi soovitakse enne toote üleandmist veenduda, et see vastab nõuetele ja eesmärgile. Süsteemitestimist teostavad tavaliselt spetsialiseerunud testijad arendusmeeskonnast, kuid olenevalt olukorrast mõnikord ka kolmanda osapoole meeskond või ärianalüütikud. Süsteemitestimine võiks katta nii funktsionaalseid kui ka mittefunktsionaalseid nõudeid. Funktsionaalsete nõuete testimist alustatakse tavapäraselt eelnevalt mainitud kasutuslugudepõhise testimisega. Süsteemitestimise puhul on väga oluline, et testkeskkond, kus testid teostatakse, oleks võimalikult lähedane reaalsele toodangukeskkonnale. Seeläbi vähendatakse keskkondade erinevustest tulenevate vigade avaldumise riski toodangukeskkonas [36].

Lisaks kasutatakse integratsioonitestimist, millega testitakse erinevate komponentide liidestumist ja koostööd teiste süsteemiosadega. Integratsioonitestimist võib läbi viia pärast komponentide testimist, et mõista, kuidas komponendid omavahel suhestuvad või pärast süsteemitestimist, et proovida kõikide komponentide koostoimimist korraga. Viimane variant on keerulisem, kuna kõike testitakse koos ja see on aeganõudev ning vigade korral on keeruline leida, milles täpselt viga seisnes. Samas võimaldab see varakult näha kogu süsteemi töötamist ja eeldab, et kõik komponendid on valmis. Vastasel juhul oleks vaja valmimata komponente simuleerida ja hiljem tuleks testimist

korrata. Parim praktika integratsioonitestimisel on alustada süsteemi integreerimist komponentidest, mis võivad põhjustada enim probleeme. Seeläbi saab varakult vead parandada ning tõenäosus, et edaspidi lisatavad komponendid omavahel tõrgeteta töötavad, on suurem [36].

Vähesel määral rakendatakse ka uurivat testimist, mille käigus kasutavad testijad enim loovust. Alati ei suudeta testilugude kirjutamisel kõiki sisendeid ja oodatavaid väljundeid täpselt kirja panna, kuid testijatel võib testimise käigus tekkida ideid, mida nad saavad katsetada ja seeläbi samuti vigu leida. Kõik testijad praktiseerivad mingil määral uurivat testimist, sest üldjuhul viivad nad lisaks dokumenteeritule läbi ka täiendavaid testilugusid [39].

Magistritöö raames kombineeritakse püstitatud eesmärkide täitmiseks antud peatükis tutvustatud testimise tehnikaid rohkemal või vähesemal määral. Testimisel on veel palju teisigi liike, kuid autor otsustas anda ülevaate vaid sellistest metoodikatest, mida antud töös rakendatakse. Kasutatavad tehnikad valiti probleemi ja eesmärki teades, X-tee platvormi toimimisloogikale ning kogenud testijuhi arvamusele ja hinnangule tuginedes.

2.6 Testimise tegevused

Kuigi testide käivitamine tundub olevat testimise juures kõige olulisem, siis sellegipoolest vajatakse lisaks testilugudele ka näiteks testiplaani ja raportit testide läbiviimise kohta. Tulemuste dokumenteerimine on üks testimise võtmetegevusi, mis on tellijale abiks lõpliku otsuse langetamisel ja aitab selgusele jõuda tarkvara vastavuses oodatule. Testimise tase võib varieeruda väga algelistest testidest kõrgtasemeliste testideni, kuid vaatamata sellele lähtutakse seejuures alati fundamentaalsetest tegevustest [36]:

- planeerimine ja kontrollimine – sõnastatakse erinevate osapoolte huvid ja eesmärgid testimisele ning jälgitakse ja mõõdetakse testimise reaalset kulgemist vastavalt paikapandud plaanile;
- analüüs ja disain – planeerimise käigus sõnastatud eesmärgid tõlgendatakse reaalseteks tingimusteks ja testimise protseduuriteks, disainitakse testid ning hinnatakse nõuete ja süsteemi testitavust, lisaks kirjeldatakse testimiseks vajalik keskkond, infrastruktuur ja tööriistad;

- juurutamine ja käivitamine – testi tingimustest kujundatakse testilood ja paigaldatakse testkeskkond, seejärel testilood käivitatakse, logitakse testide tulemuste väljundid ning võrreldakse neid oodatud tulemustega;

- testimise tulemuste hindamine ja raporteerimine – analüüsitakse testide tulemusi ja võrreldakse neid algselt püstitatud eesmärkidega, hinnatakse süsteemi testidega kaetust ja vajadusel teostatakse täiendavad testid, lisaks koostatakse kokkuvõte läbiviidud testimisest;

- testimise lõppemisega seotud tegevused – kogutakse kokku info läbitud testimise tegevuste kohta, kontrollitakse tulemusi, tehtud tööd antakse üle tulevasele haldajale ja analüüsitakse kordaminekuid ja möödalaskmisi kõigi testimise tegevuste vältel.

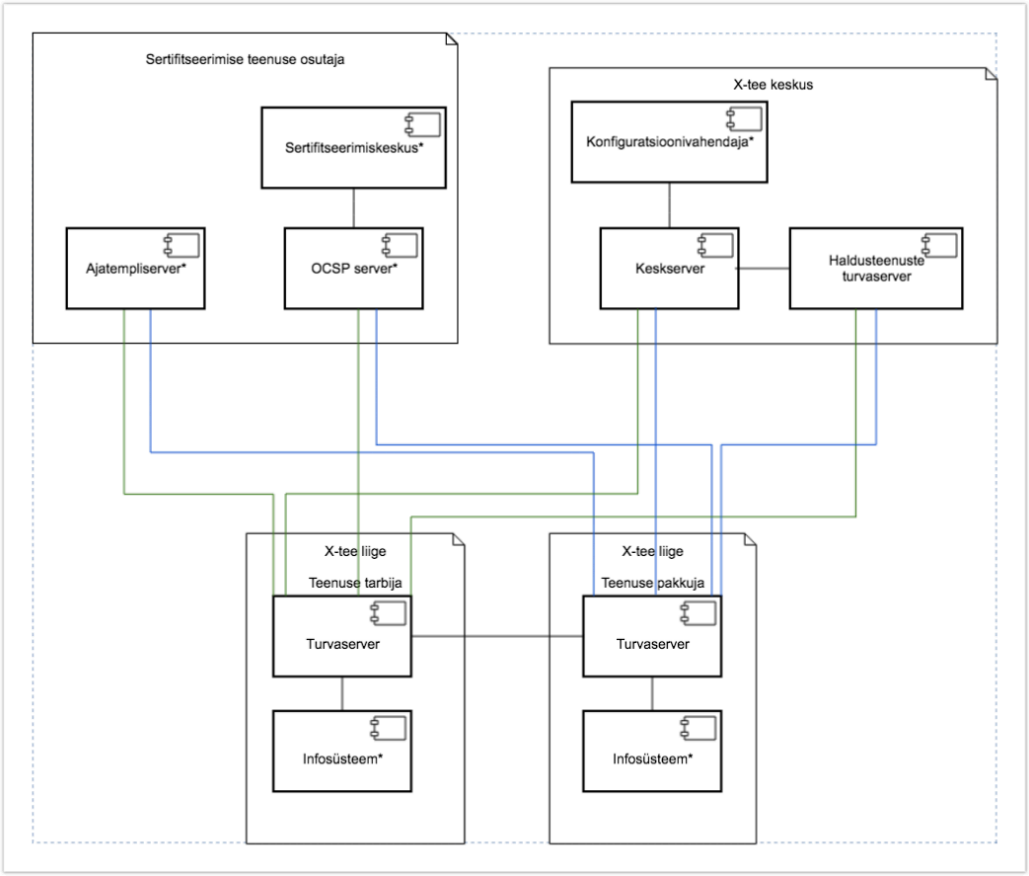
Loetelus välja toodud tegevused on loogilises järjestuses, kuid teatud projektide puhul sooritatakse mõnda neist üheaegselt ning teist sootuks mitmeid kordi [36]. Taolist testimise protsessi kasutatakse eelkõige dünaamilise testimise puhul, mida rakendatakse ka antud magistritöös.

3 X-tee komponendid, protokollid ja kriitiliste kesksete teenuste testide koostamine

Peatüki eesmärgiks on anda ülevaade X-tee süsteemi komponentidest, protokollidest, kriitilistest kesksetest teenustest ja testidest, millega tehakse kindlaks X-tee versioon 6 tõrketaluvus.

3.1 X-tee süsteemi komponendid

Joonisel 3 on kujutatud X-tee süsteemi komponendid. Tegemist on minimaalse komplektiga, mis on vajalik ühe X-tee keskkonna edukaks toimimiseks.



Joonis 3. X-tee komponentide skeem

Komponendid, mis ei ole X-tee tuumtehnoloogia osad, on märgitud tärniga (*).

Komponente on võimalik süsteemi töökindluse tõstmiseks klasterdada. Teenuse tarbija turvaserveri seosed komponentidega on arusaamise lihtsustamiseks kujutatud rohelise tooniga ja teenuse pakkuja turvaserveri seosed sinise tooniga. Komponentide detailsem ülevaade on leitav järgnevatest alapeatükkidest, mille välja toomisel on autor tuginenud X-tee arhitektuuridokumendile [17].

3.1.1 X-tee keskus

X-tee keskus (vt Joonis 3) haldab keskserverit ja haldusteenuste turvaserverit. Haldusteenuste turvaserver on oma olemuselt tavaline turvaserver, mis on defineeritud keskserveris haldusteenuseid pakkuma. Konfiguratsioonivahendaja on valikuline komponent, mida kasutatakse födereerunud X-tee keskkondade konfiguratsiooni jagamiseks.

Keskserver haldab andmebaasi, milles hoitakse kirjeid X-tee liikmete ja turvaserverite kohta. Lisaks sisaldab keskserver X-tee keskkonna turvapoliitikat, mis koosneb:

- kvalifitseeritud sertifitseerimise teenuse osutajate nimekirjast,
- kvalifitseeritud ajatempliteenuse osutajate nimekirjast,
- seadistatavatest parameetritest.

Kogu eelnev info moodustab globaalse konfiguratsiooni, mis on turvaserveritele kättesaadav HTTP protokolli kaudu. Lisaks konfiguratsiooni levitamisele omab keskserver liidest haldustegevuste, nagu näiteks turvaserveri klientide lisamine ja eemaldamine, läbiviimiseks.

Konfiguratsioonivahendaja töötab konfiguratsiooni allalaadimise protokolli alusel. Konfiguratsioonivahendaja laeb keskserverist konfiguratsiooni alla, salvestab ja teeb vastavalt keskkonnale seatud nõuetele konfiguratsiooni kättesaadavaks turvaserveritele, keskserveritele või teistele konfiguratsioonivahendajatele. See võimaldab suurendada süsteemi kättesaadavust luues lisaallika konfiguratsiooni allalaadimiseks ja aidates seeläbi vähendada keskserveri koormust. Konfiguratsioonivahendajat kasutatakse usaldusföderatsiooni puhul, mil erinevad X-tee instantsid omavahel ühendatakse ja globaalse konfiguratsiooni levitamine vajab suuremat paindlikkust. Hetkel X-tee toodangukeskkond konfiguratsioonivahendajat ei kasuta.

Haldusteenuste turvaserverisse on lisatud teenused, mida kasutavad X-tee liikmed kui neil on vaja oma liikmelisuses muudatusi teha. Turvaserverid pöörduvad teenuste poole kui soovitakse keskserveris:

- registreerida X-tee alamsüsteem turvaserveri kliendina,
- eemaldada klient turvaserverist,
- lisada autentimissertifikaat turvaserverisse,
- eemaldada autentimissertifikaat turvaserverist.

Haldusteenused [41] on standardsed X-tee teenused, mida keskserver pakub haldusteenuste turvaserveri kaudu ja mis kutsutakse esile turvaserveri kasutajaliidesest. Haldusteenuste kohta on täpsem ülevaade peatükis 3.2.

3.1.2 X-tee liige ehk teenuse tarbija ja pakkuja

Teenuse tarbijad ja teenuse pakkujad (vt Joonis 3) haldavad ise oma infosüsteeme ja turvaservereid. Infosüsteemid ühendatakse turvaserveritega, mille tulemusena tekib liikmetel võimekus X-teel andmeid vahetada.

Turvaserver vahendab infosüsteemide vahel sissetulevaid päringuid ja väljaminevaid vastuseid. Turvaserver koondab X-tee infrastruktuuri turvalisust puudutavad aspektid:

- haldab nii autentimiseks kui ka allkirjastamiseks vajalikke võtmeid,
- teostab pääsuõiguste kontrolli,
- saadab sõnumeid üle turvalise kanali,
- loob tõestusväärtust omavaid e-templitega sõnumeid,
- varustab vahetatud päringuid ajatempliga,
- logib turvaserveris sooritatud tegevusi ja päringuid.

Turvaserver on võimeline majutama mitmeid kliente. Turvaserverit haldav organisatsioon on turvaserveri omanik, majutatavad on turvaserveri kliendid. Turvaserverit haldav organisatsioon võib omada mitut turvaserverit.

Turvaserveris hallatakse kahte tüüpi võtmeid. Autentimisvõtmeid kasutatakse turvaserveritevahelise krüptograafiliselt turvalise kanali loomiseks. Kliendi e-templi võtmeid kasutatakse vahetatavate sõnumite allkirjastamiseks. Autentimisvõtmeid hoitakse alati tarkvaralisel allkirjastamise moodulil (ingl k *software token*) ning e-templi võtmeid võib olenevalt X-tee keskkonnast, organisatoorsetest ja sertifitseerimispoliitikast tulenevatest nõuetest hoida tarkvaralisel allkirjastamise moodulil või riistvaralisel allkirjastamise vahendil.

Turvaserver laeb keskserverist alla ja hoiab vahemälus ajakohast globaalset konfiguratsiooni. Lisaks ka oma sertifikaatide väljastajalt saadud sertifikaadi kehtivuse infot. Vahemälus hoidmise funktsionaalsus võimaldab turvaserveril tegutseda ka, siis kui primaarsed allikad ei ole kättesaadavad. Puhverdatud konfiguratsioon ja sertifikaadi kehtivuse info on kasutatavad fikseeritud aja jooksul, tagamaks nende teenuste vastu sooritatud rünnakutest tekkivat tervikluse kadu platvormis.

Infosüsteem võib kasutada või pakkuda teenuseid X-tee kaudu. Teenuse tarbija infosüsteemi jaoks on turvaserver lüüs teiste X-tee liikmeteni. Infosüsteemi suhtlus turvaserveriga põhineb SOAP protokollil. Infosüsteemis on mehhanism turvaserveri haldaja autentimise ja juurdepääsuõiguste haldamiseks, mis on kooskõlas vastava X-tee keskkonna nõuetega. Lõppkasutaja identiteet saab teenuse pakkujale selgeks SOAP sõnumi päises, mis on seotud sõnumile antud allkirjaga. Teenuse tarbija näeb X-tee liikmete ja saadaval olevate teenuste loetelu X-tee metaandmete protokolli vahendusel.

Teenuse pakkuja infosüsteem teostab SOAP päringuid, mis peavad vastama X-tee sõnumiprotokollile. Teenused peavad olema üle X-tee kättesaadavad ja kirjeldatud WSDL-is. Selle tagamiseks on turvaserveris realiseeritud metateenused [41], mis moodustavad X-tee platvormisisese hajusa teenuste kataloogi.

3.1.3 Sertifitseerimise teenuse osutaja

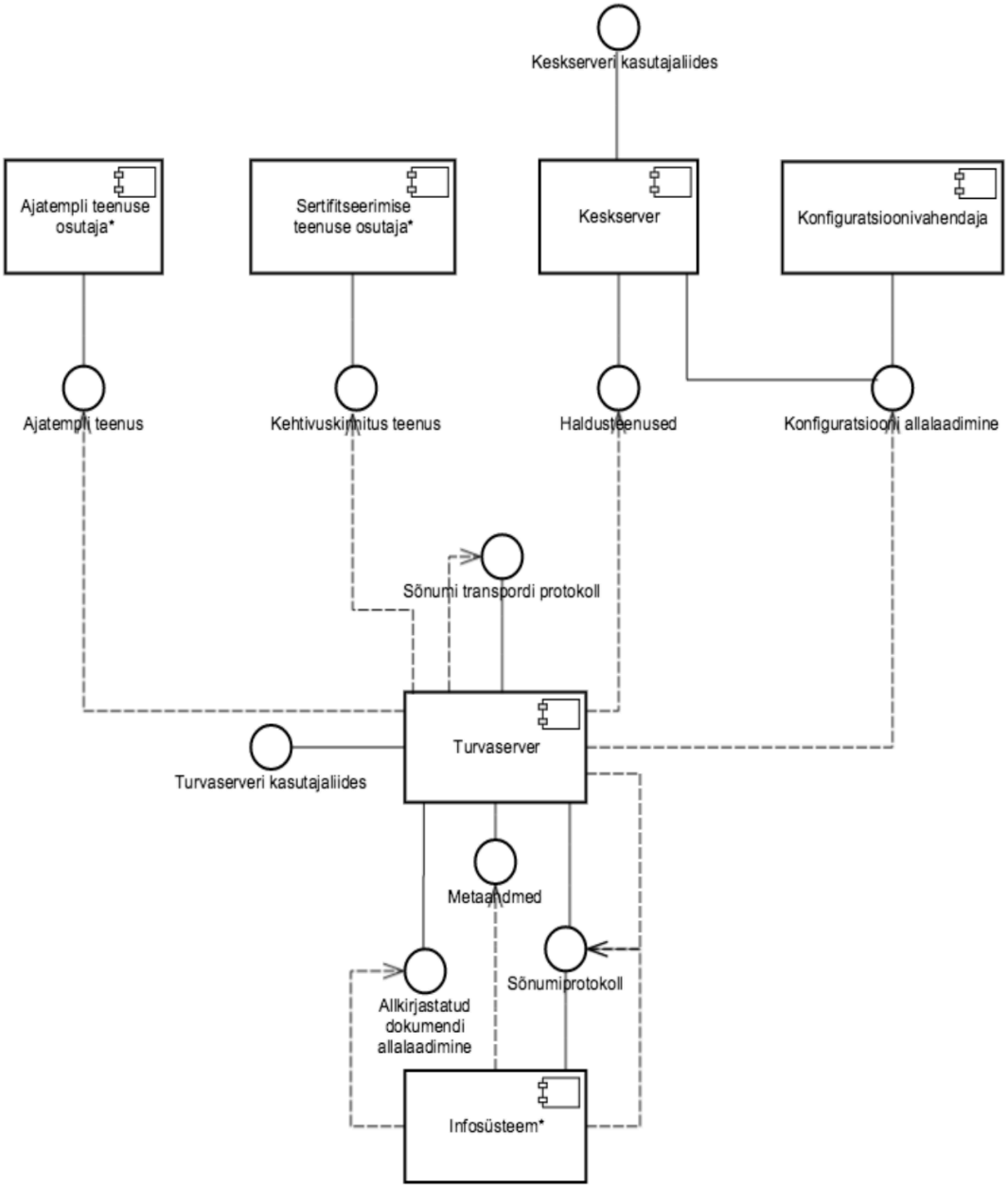
Sertifitseerimise teenuse osutaja (vt Joonis 3) alla kuuluvad ajatempliserver ja OCSP server. Tegemist on usaldusteenustega, mida X-tee liikmed võivad tarbida erinevatelt teenuse pakkujatelt. Usaldusteenuste osutajad jagunevad vastavalt oma ülesandele ajatempliteenuse pakkujaks ja sertifitseerimise teenuse osutajaks.

Ajatempliteenuse pakkuja väljastab ajatempleid, mis sertifitseerivad andmete olemasolu kindlal ajahetkel. Ajatempliteenuse pakkuja rakendab ajatempliteenuse protokolli. X-teel kasutatakse pakkajatembeldust, kuna see vähendab ajatempliteenusele kuluvat rahalist ressurssi, parandab turvaserveri jõudlust ning töökindlust juhul, kui ajatempliteenuse pakkuja ei ole mingil põhjusel stabiilselt kättesaadav. Määravaks koormuse juures ei ole X-teel saadetavate sõnumite arv, vaid turvaserverite koguarv süsteemis.

Sertifitseerimise teenuse osutaja väljastab X-tee liikmeteks olevatele organisatsioonidele e-templi kvalifitseeritud sertifikaate ja turvaserveritele autentimissertifikaate. Sertifikaate hoitakse turvaserverites. Sertifitseerimise teenuse pakkuja töötleb e-templi kvalifitseeritud sertifikaate, mis kohanduvad PKCS [42] protokollile. Sertifitseerimise teenuse pakkuja levitab sertifikaadi kehtivuse staatust kehtivuskinnituse (OCSP) protokolli kaudu. Turvaserver hoiab vahemälus saadud OCSP vastuseid, et vähendada OCSP teenusele kuluvat rahalist ressurssi ja suurendada töövõimet.

3.2 X-tee protokollid

Selleks, et süsteemi komponendid omavahel suhelda saaksid, on tarvis kindlalt paika pandud protokolle ehk reeglistikke, kuidas komponentidevaheline suhtlus toimub. Joonisel 4 on kujutatud peamised X-tee süsteemi komponendid, liidesed ja protokollid.



Joonis 4. X-tee loogiline struktuur

Komponendid, mis ei ole X-tee tuumtehnoloogia osad, on märgitud tärniga (*).

Järgmistes lõikudes selgitab autor tuginedes X-tee arhitektuuridokumendile [17] infosüsteemide andmevahetuskihis kasutatavate protokollide eesmärke ja seoseid eelnevalt tutvustatud komponentidega.

X-tee sõnumiprotokolli (vt Joonis 4) kasutavad teenuse tarbija- ja pakkujate infosüsteemid X-tee turvaserveriga suhtlemiseks. Sõnumiprotokolli kasutab nii teenuse tarbija infosüsteem kui ka teenuse pakkuja turvaserver. X-tee sõnumiprotokoll põhineb üle HTTP(S)-i protokolli liikuvatel SOAP sõnumitel. Saadetud sõnumi päises olevad väljad võimaldavad kindlaks teha teenuse tarbija ja väljakutsutud teenuse. Sõnumiprotokoll ja sõnumi transpordi protokoll moodustavad alustala X-tee andmevahetusele.

Globaalse konfiguratsiooni allalaadimise protokoll on keskserveri poolt pakutav sünkroonne protokoll, mida kasutavad turvaserverid ja konfiguratsioonivahendajad. Protokoll põhineb HTTP ja MIME mitmepoolsel sõnumi saatmisel (ingl k *MIME multipart messaging*). Konfiguratsiooni allkirjastab keskserver, et tagada selle terviklus. Protokoll võimaldab turvaserveritel ja konfiguratsioonivahendajatel kontrollida, kas konfiguratsioon on vahepeal muutunud ja allalaadida vaid muutunud osasid. X-tee turvaserverid hoiavad alles lokaalset koopiat globaalsest konfiguratsioonist, mida perioodiliselt usaldusväärsest konfiguratsiooni allikast uuendatakse. Vahemälus hoitaval globaalsel konfiguratsioonil on kehtivusaeg, mis peab alati olema pikem perioodist, mille tagant turvaserver globaalset konfiguratsiooni värskendab. Turvaserverid töötavad tõrgeteta kuni vahemälus hoitav globaalne konfiguratsioon on kehtiv. Seevastu kehtetu globaalne konfiguratsioon piirab osaliselt turvaserveri administraatori poolt sooritatavaid haldustegevusi ja keelab turvaserveril sissetulevate päringute töötlemise. Lühiajaline liidese katkestus on talutav globaalse konfiguratsiooni kehtivuse piires.

Sõnumi transpordi protokolli kasutavad turvaserverid päringute ja nende vastuste töötlemiseks. Protokolli võib esile kutsuda nii teenuse tarbija infosüsteem kui ka teenuse pakkuja turvaserver. Protokoll põhineb HTTPS-il ja kasutab vastastikust sertifikaatidel põhinevat TLS autentimist. SOAP sõnumid, mis teenuse tarbija ja teenuse pakkuja infosüsteemidelt vastu võetakse, on kokku pakitud MIME sõnumisse koos allkirjade ja OCSP vastustega.

Sõnumi metaandmete protokolli (vt Joonis 4) kasutavad teenuse tarbija infosüsteemid X-tee keskkonna kohta informatsiooni kogumiseks. Täpsemalt X-tee liikmete, nende poolt pakutavate teenuste ja teenuste WSDL kirjelduste leidmiseks. Protokolli kutsub esile teenuse tarbija infosüsteem. Teenuseid päritakse sarnaselt standardsete X-tee andmeteenustega või implementeeritakse HTTP(S) GET päringutena, et lihtsustada kliendi infosüsteemi rakendust.

Allkirjastatud dokumendi allalaadimise protokolli kasutavad infosüsteemid turvaserveri sõnumilogist allkirjastatud konteinerite allalaadimiseks. Lisaks pakub teenus käepärast meetodit globaalse konfiguratsiooni allalaadimiseks, mida kasutatakse allkirjastatud konteinerite kontrollimiseks. Protokolli kutsub esile infosüsteem. Teenus on implementeeritud HTTP(S) GET päringutena.

Haldusteenuseid kasutavad turvaserverid haldustegevuste, näiteks turvaserveri kliendi registreerimine või autentimissertifikaadi kustutamine, sooritamiseks. Haldusteenuste protokolli pakub keskserver. Teenus kutsutakse välja turvaserverite poolt. Haldusteenused on realiseeritud kui standardsed X-tee teenused, mida pakub X-tee keskkonda haldav organisatsioon haldusteenuste turvaserveri kaudu. Erandiks on autentimissertifikaadi registreerimise teenus, mis tehnilistel põhjustel implementeeritakse otse keskserverist. Haldusteenuste toimimine ei ole X-tee andmevahetuse seisukohalt kriitiline tegevus ja seetõttu ei ole haldusteenuste kättesaadavus kõige olulisem. Kui haldusteenused ei ole kättesaadavad, siis ei saa turvaserverid hallata oma kliente ja autentimissertifikaate. Mõnda tegevust, näiteks klientide ja sertifikaatide eemaldamist, saab keskserveri administraator manuaalselt haldusteenuseid kasutamata sooritada. Haldusteenuste tegevused ei ole ajakriitilised.

Kehtivuskinnituse teenuse protokolli kasutavad turvaserverid allkirjastamise ja autentimise sertifikaatide kehtivuse informatsiooni pärimiseks. OCSP protokoll on sünkroonne protokoll, mida pakub OCSP vastaja (ingl k *OCSP responder*), mis kuulub sertifitseerimiskeskusele. X-teel on iga turvaserver vastutav oma sertifikaatide kehtivuse info allalaadimise ja vahemälus hoidmise eest. OCSP vastused saadetakse turvaserveritele sõnumi transpordi protokolli osana. Tänu sellele ei pea turvaserverid tundma OCSP teenust, mida kasutab teine osapool. Lisaks toetab selline kokkulepe olukorda, kus ligipääs OCSP teenusele võib olla sertifikaatide omanikele piiratud või tasuline. OCSP teenused omavad erinevaid optimiseerimisstrateegiaid, nagu näiteks eel-

loodud OCSP vastused. OCSP vastuseid kasutatakse sertifikaadi valideerimise protsessis, seega OCSP teenuse tõrge blokeerib X-tee sõnumivahetuse. Kui vahemälus hoitavaid OCSP vastuseid ei ole võimalik värskendada, siis ei ole turvaserverid võimelised sõnumeid välja saatma. Seetõttu määrab OCSP vastuste eluiga maksimaalse aja, mil OCSP teenused võivad olla kättesaamatud. Eluiga on defineeritud keskserveri omaniku poolt ja võib erineda erinevate X-tee keskkondade vahel.

Ajatempliteenuse protokolli (vt Joonis 4) kasutavad turvaserverid vahetatud sõnumite pikaajalise tõestusväärtuse kindlustamiseks. Logisid ajatembeldatakse perioodiliselt. Ajatempliteenuse sünkroonset protokolli pakub ajatempliteenuse pakkuja. Sellegipoolest kasutavad turvaserverid ajatempli protokolli asünkroonsel viisil kasutades pakkajatembeldamist. Turvaserverid logivad kõiki sõnumeid, mis on jõudnud teise osapoole turvaserverisse. Seda tehakse selleks, et eraldada sõnumivahetuse kättesaadavus ajatempliteenuse pakkuja kättesaadavusest, mis aitab vähendada sõnumivahetuse latentsust. Kuna ajatembeldamist kasutatakse asünkroonsel viisil, siis ei mõjuta ajatempliteenuse ajutine mittekättesaadavus otseselt X-tee sõnumivahetust. Sellegipoolest, kui turvaserver ei saa ajatembeldada kogunenud sõnumeid kindla ajaperioodi vältel, siis muutub keeruliseks kindlal ajahetkel toimunud sõnumivahetuse tõestamine. Selleks, et minimeerida võimalikku riski, lõpetavad turvaserverid sõnumite edastamise kui ajatempliteenuses esinevad mõnda aega tõrked. Maksimaalne lubatud ajaperiood sõnumi logimise ja sõnumi ajatembeldamise vahel on defineeritud turvaserveris, kuid paika pandud keskuse poolt ja võib erineda X-tee keskkondade vahel.

Lisaks ülaltoodud protokollidele, mis põhinevad sünkroonsel RPC stiilil, on olulisel kohal ka turvaserveri ja keskserveri kasutajaliidesed, mida kasutavad selleks volitatud administraatorid vastavalt turvaserveri või keskserveri konfigureerimiseks ja haldamiseks.

3.3 Kriitilised kesksed teenused

Selleks, et X-tee tõrketaluvuses veenduda, on enne testimise tegevuste (vt peatükk 2.6) alustamist vaja välja selgitada X-tee toimimise kontekstis kriitilised kesksed teenused. Eelnevates peatükkides välja toodud X-tee süsteemi komponentide ja protokollide ülevaade kinnitab, et turvaliseks andmevahetuseks on vajalik mitmete funktsioonide koostoimimine. Teatud teenused on X-tee korrapärase töötamise seisukohalt kriitilise tähtsusega. Käesolev peatükk keskendub kriitilistele kesksetele teenustele, mille nõuetekohasus testimise käigus selgub.

Kesksete teenuste all mõeldakse teenuseid, mis on vajalikud platvormi toimimiseks, et liikmetel oleks võimalik andmeid vahetada. Oluline on mõista, et kesksete teenuste all ei käsitleta keskselt keskserverisse lisatavaid andmeteenuseid.

X-tee kesksеteks teenusteks on (vt peatükk 3.2):

- globaalse konfiguratsiooni jagamine,
- haldusteenused,
- ajatempliteenus,
- kehtivuskinnituse teenus,
- NTP.

Kesksed teenused selgitas autor välja X-tee arhitektuuridokumentide alusel ja arutas teemat RIA-s X-tee valdkonna siseselt. Arutelu käigus selgus, et mitte kõik kesksetest teenustest ei ole kriitilised. Kriitiline on teenus, siis kui selle mittetoimimine mõjutab otseselt andmevahetust X-teel. Näiteks haldusteenused võimaldavad hallata turvaservereid ja X-tee liikmeid. Taolised tegevused ei ole ajakriitilised, mis tähendab, et kui tekib intsident, mille tulemusena haldustegevused ei toimi ja liige ei saa neid tegevusi mõnda aega sooritada, siis X-tee andmevahetus ei lakka töötamast. Seetõttu ei peeta haldusteenuseid kriitiliseks ega testita antud töös nende teenuste tõrketaluvust.

Teine oluline aspekt, milles tuli enne testide läbiviimist veenduda, oli testitavus. Näiteks selgus, et võrguaja protokoll (NTP) on X-tee andmevahetuse seisukohalt oluline, kuna kellade erinevus võib põhjustada seisakut andmevahetuses. Kui kehtivuskinnituse

teenus kehtib teatud piirides ja turvaserverite kellad ei ole sünkroonis, siis võivad turvaserverid sattuda aega, mil hakatakse valesti hindama usaldusteenuste tõestatavust. Turvaserveritele näib, et kehtivuskinnitus on kaotanud oma kehtivuse, kuid tegelikkuses ei ole. Tegemist on kahtlemata kriitilise olukorraga, kuid käesoleva töö käigus ei olnud võimalik seda teostada. Põhjusena tõi RIA süsteemiadministraator välja, et kasutatav virtuaalserverite platvorm keelab NTP teenuse sünkroniseerimise välja lülitamist ning manuaalselt kella seadistamist. Ainus võimalus oleks olnud virtuaalsed serverid internetiühendusest eemaldada, kuid siis poleks saanud kehtivuskinnitust, mis oli antud testi üheks eelduseks.

X-tee valdkonnas peetud arutelus tulid välja veel mõned tegurid, mis võivad samuti turvaserverite töös tõrkeid põhjustada. Näiteks internetiühenduse kadumine tervikuna, tõrked andmebaasi kättesaadavusega, probleemid riistvaralise allkirjastamisvahendi ja turvaserveri vahelises ühenduses või Linuxi Ubuntu distributsiooni pakenduse eripärad, kuid need ei ole X-tee spetsiifilised ja jäid seega testimise skoobist välja.

Järgnevates alapeatükkides annab autor ülevaate iga kriitilise keskse teenuse kohta, mis selekteeriti kesksete teenuste hulgast ja mille mõju andmevahetusele antud töös selgub.

3.3.1 Globaalne konfiguratsioon

Globaalsest konfiguratsioonist saab turvaserver info teise liikme turvaserveri ja alamsüsteemi kohta, kuhu on vaja päring saata. Lisaks info usaldusteenuste toimivuse ja süsteemsete parameetrite kohta. Globaalset konfiguratsiooni võib lihtsustatult mõista kui aadressiraamatut, millest leiab vajaliku osapoole kontaktid. Globaalne konfiguratsioon koosneb XML-failidest, mida turvaserverid perioodiliselt (toodangukeskkonnas umbes iga ühe minuti tagant) X-tee keskserverist allalaevad. Turvaserverite jaoks globaalse konfiguratsiooni allalaadimiseks ja verifitseerimiseks vajalik info asub konfiguratsiooniankrutes.

Selleks, et keskserver hakkaks globaalset konfiguratsiooni genereerima, tuleb pärast keskserveri esmast initsialiseerimist luua võtmed globaalse konfiguratsiooni allkirjastamiseks. Pärast seda tekitatakse keskserveris sisemine ja väline konfiguratsiooniankur, mis on samuti XML failid.

Järgnevalt on Joonisel 5 välja toodud X-tee toodangukeskkonnas kasutusel oleva sisemise konfiguratsiooniankru osa, mis on täismahus leitav Lisast 1.

```
<ns3:configurationAnchor xmlns:ns2="http://x-
road.eu/xsd/identifiers" xmlns:ns3="http://x-road.eu/xsd/xroad.xsd">
<generatedAt>2015-10-30T12:45:29.925Z</generatedAt>
<instanceIdentifier>EE</instanceIdentifier>
<source>
<downloadURL>http://213.184.41.186/internalconf</downloadURL>
<verificationCert>
MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwW
hcNMzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
CspebxrUlGPGTbjkv+tihZ2s0F7inWvPm2apDM8o5qjFDXHTnAT2vUkAqG4RJvTA5F2jdxFsQ2yHE3+xojSP5
U3s58G3MjehLCPP8o4mOrXWuWMS5QKOeSuwDQgxiHS0SdD4nugfsrAAIdZCB24eyLokNrmDmvDllYN4xuH30I
Dltw2R4Y8KWkCvcR/2aiB53XNDD3FCC1SqfqSVj2JemLKRVnGQOZDMhF3S2lqHhK9/4adsDORGuYTgsboN60Z
jHoCWNT9MzUHk3y2ravH16RCCGh05coUslgpjcYqXigm0z4BeAqyfg2dy12QzL8op1nQZ889T+vDdDC6myP84
OjAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAMZdq9VTf57RWMc0Zkqayvad
ZNDFtO7k9q8xohztUr0BAprU+UgvTe8tu4JqfPwx0e10WULugYOR20IUGxVRm6wVmCDr5SVzVuYlV1f/gTxZx
7ZuEPHkB1AbnMWCa9qKmD+F9i0X1Erp6T62e6Y2x2hriGQMJDnA81nq4EEQYdLQQaiEodU3VMpJD7kDX0jPIN
E5JpMoMhhFM+wrL5q995C/oR76S5elQnGbwJExPArv4HaznLJ9di9MLaLb5nHNFZTrJMXG5vr8Lv5fHwNuC91
hlQZVQ+BE5eOHUI8f5Uu00KBqxPTJCHlHbhx+OTeuI0d2DVNEEFUn2YQ7uSaKp+A==
</verificationCert>
</source>
```

Joonis 5. Osa sisemise konfiguratsiooniankru XML faili sisust

Konfiguratsiooniankrus (vt Joonis 5) sisalduvad kasutatavad nimeruumid, ankru genereerimise aeg, keskkonna instantsi identifikaator, allalaadimise URL-id kolmest erinevast keskserverist ja sertifikaatide räsid. X-tee versioon 6 toodangukeskkonnas on kolm klasterdatud keskserverit. Sisemist konfiguratsiooniankrut kasutavad turvaserverid globaalse konfiguratsiooni allalaadimiseks. Välist konfiguratsiooniankrut kasutatakse erinevate X-tee instantside födereerimiseks [45].

Kui konfiguratsiooni ankrud on genereeritud, siis tuleb keskserveris konfigureerida liikmeklassid, haldusteenuseid pakkuv alamsüsteem, sertifitseerimisteenuse pakkuja ja ajatempliteenuse pakkuja. Kui eelnev on tehtud, siis hakkab keskserver globaalset konfiguratsiooni genereerima. Konfiguratsiooni terviklus tagatakse keskserveri poolt konfiguratsiooni kausta allkirjastamisega. Kui see peaks mingil põhjusel nurjuma ja allkirja ei teki, siis globaalse konfiguratsiooni loomine ebaõnnestub [45]. Allkirjastamisel kasutatakse vaikimisi SHA-512 räsifunktsiooni [46].

Globaalse konfiguratsiooni genereerimine ei ole ühekordne tegevus, kuna andmebaas muutub pidevalt ja liikmed peavad uuenenud infoga kursis olema. Keskserveris on defineeritud globaalse konfiguratsiooni kehtivuse parameeter (*confExpireIntervalSeconds*), mis defineerib kui kaua globaalne konfiguratsioon kehtib.

Eraldi on seadistatav parameeter globaalse konfiguratsiooni uuendamise sageduse määramiseks. Globaalse konfiguratsiooni genereerimise intervall peab olema lühem kui globaalse konfiguratsiooni aegumise intervall, vastasel juhul kaotab turvaserverite poolt allalaetav konfiguratsioon alati kehtivuse enne kui kehtiv konfiguratsioon muutub kättesaadavaks [47]. Sellises olukorras ei oleks andmevahetus X-teel võimalik.

Liige peab globaalse konfiguratsiooni saamiseks vastava X-tee keskkonna konfiguratsiooniankru oma turvaserverisse laadima. Vastasel juhul ei tea turvaserver, milliselt URL-ilt globaalset konfiguratsiooni küsida. Kui turvaserveril ei ole globaalset konfiguratsiooni, siis on ta justkui välismaailmast eraldatud ega tea midagi sellest, mis vastavas keskkonnas toimub. Turvaserveris on defineeritud globaalse konfiguratsiooni allalaadimise intervalli parameeter (*update-interval*), mis defineerib kui tihti turvaserver globaalset konfiguratsiooni alla laeb [47]. Kui turvaserver küsib globaalset konfiguratsiooni liiga harva, siis võib tekkida olukord, kus turvaserveris on aegunud info või ta saab keskserverilt konfiguratsiooni, mis on juba vahepeal jõudnud aeguda. Kui paljud turvaserverid küsiksid globaalset konfiguratsiooni liiga tihti, siis võib keskserver ülekoormatud olla. Kui mingi hetk peaks tekkima olukord, kus turvaserver ei küsi globaalset konfiguratsiooni, siis on andmevahetus edukas kuni viimati saadud globaalne konfiguratsioon kehtib.

3.3.2 Kehtivuskinnituse teenus

Kehtivuskinnituse teenuse abil saavad X-tee liikmed info sertifikaadi kehtivuse ja kehtivuskinnituse väljastamise aja kohta. Sisuliselt on tegemist usaldusteenuse pakkuja kinnitusega, et sertifikaat kehtib ja X-tee liige vastab väidetavale. Teenus põhineb OCSP-protokollil [26]. Kehtivuskinnituse teenus on tavaline klient-server süsteem, kus OCSP klient saadab OCSP vastajale ehk serverile päringu sertifikaadi kohta ning server saadab vastuse, mis sisaldab sertifikaadi kehtivust või mittekehtivust ja kinnituse andmise aega. Serveri vastus on digitaalselt signeeritud. OCSP vastaja vastused sertifikaadi kohta võivad olla kolmelaadsed:

- sertifikaat kehtib,
- sertifikaat ei kehti,

- informatsioon küsitava sertifikaadi kohta puudub, mis tähendab, et OCSP vastaja ei saada infot teatud usaldusteenuse osutajate poolt välja antud sertifikaatide kohta.

Olenevalt sertifitseerimispoliitikast võivad OCSP vastuste tähendused erineda. Näiteks standardikohane OCSP positiivne vastus sertifikaadi kohta ei tähenda ilmtingimata, et küsitav sertifikaat üldse kunagi väljastatud on. SK ID Solutions AS-i OCSP positiivne vastus tähendab aga, et sertifikaat on välja antud ning ta oli kinnituse väljastamise hetkel kehtiv. SK ID Solutions AS OCSP server saab sertifikaatide kehtivuse info otse sertifikaatide andmebaasist, kuhu laekuvad operatiivselt ka kõik sertifikaatide oleku muutused. See tagab, et OCSP vastused näitavad võimalikult ajakohast sertifikaatide staatust [48]. Iga X-tee liige on seotud vaid talle teenust pakkuva sertifitseerimise ja kehtivuskinnituse teenuse osutaja(te)ga. Keskserveri haldusliideses defineeritakse vastava X-tee keskkonna jaoks sertifitseerimisteenuse osutaja.

OCSP vastuse aeg määrab varaseima absoluutse aja, mil konkreetne sõnum X-teel vahetati. E-templi sertifikaadi OCSP vastus saadetakse koos päringuga teisele X-tee osapoolele. See on osa sõnumivahetusest, mida turvaserver realiseerib automaatselt. Sõnumid tembeldatakse pakikaupa, mis aitab suurendada läbilaskevõimet juhul, kui allkirjastamisel kasutatakse mõnda vähem võimekat riistvaralist allkirjastamise vahendit [49]. Usaldusteenuse osutajalt saadud OCSP vastuste kehtivuse periood defineeritakse keskserveri andmebaasis eraldi parameetrina (*ocspFreshnessSeconds*) ja jagatakse turvaserveritele globaalse konfiguratsiooni kaudu [47]. Saadud OCSP vastuste kehtivus salvestatakse vahemällu ja teatud ajaperioodi tagant kontrollitakse vahemälust, kas järgmise perioodi jooksul OCSP vastus aegub. Aegumise korral küsitakse OCSP serverilt uus kehtivusaeg. Iga turvaserver küsib usaldusteenuse osutajalt kehtivuse infot ainult enda sertifikaadi kohta.

X-teel päringute vahetamiseks peavad osapooled omavahel looma turvalise TLS kanali. Selle käigus kontrollitakse esmalt, kas kehtiv turvaserveri autentimissertifikaadi OCSP vastus on vahemälus olemas või mitte. Kui kehtivat OCSP vastust vahemälus ei ole, siis laetakse autentimissertifikaadi OCSP vastused alla teiselt osapoolelt, kellega andmeid vahetatakse ja hoitakse neid lokaalselt vahemälus. Seejärel kontrollib teenuse tarbija turvaserver teise osapoole turvaserveri autentimissertifikaati ja loob sertifitseerimisahela. Kui verifitseerimine on edukas, siis saadab teenuse tarbija päringu

teenuse pakkuja turvaserverisse. Kui kontrollimine ebaõnnestub, siis saadetakse veateade ja soovitud päringu saatmine nurjub [50].

3.3.3 Ajatempliteenus

Ajatempliteenuse abil lisatakse vahetatud sõnumilogile digitaalne ajatempel. Ajatemplid kinnitavad, et teatud andmed eksisteerisid vastaval ajahetkel. Ajatempel määrab hilisema absoluutse aja, millal andmevahetus kahe osapoole vahel konkreetse sõnumi näol toimus ning annab seeläbi vahetatud andmetele pikaajalise tervikluse garantii. X-teel kasutatav SK ID Solutions AS ajatempliteenus on kvalifitseeritud eIDAS määruse [18] kohaselt ja vastab IETF standardile RFC-3161 [51].

Ajatempliteenus on sisuliselt klient-server süsteem, milles ajatempli klient saadab serverile ajatemplipäringu andmekogumi olemasolu tõestamiseks teatud ajahetkel. Ajatempliteenus tagastab andmekogumi olemasolu kinnitava digitaalselt allkirjastatud tõendi. Ajatempliteenus on HTTP teenus, ajatemplipäring esitatakse HTTP POST päringuna [52].

Ajatembeldatakse kõik X-teel vahetatavad sõnumid ja päringulogid. Seejuures on oluline turvaserveri ühendamine võrguaja protokolli NTP piisavalt usaldusväärse (stratum-1, stratum-2) ajaserveriga, vastasel juhul võivad tekkida ebakõlad [51]. Ajatembeldamise intervall defineeritakse keskserveri andmebaasis eraldi parameetrina (*timeStampingIntervalSeconds*) ja jagatakse turvaserveritele globaalse konfiguratsiooni kaudu. Tegemist on näitajaga, mis defineerib kui tihti peab sõnumilogi ajatembeldama. Selleks, et hiljem oleks võimalik allkirja kehtivust tõestada, peab parameeter *timeStampingIntervalSeconds* olema alati väiksem kui parameeter *ocspFreshnessSeconds*. Kui parameeter *timeStampingIntervalSeconds* on suurem, siis võib tekkida olukord, kus ajatembeldamisel ei ole OCSP vastus enam kehtiv, kuna ajatembeldamine toimub asünkroonselt.

Turvaserveris on võimalik konfigureerida ka ajaperioodi mil ajatembeldamine võib ebaõnnestuda (*acceptable-timestamp-failure-period*) enne kui turvaserver lõpetab päringute vastuvõtmise [47]. Sisuliselt saab seeläbi ajaperioodi lõpmatuks seadistada, kuid sel juhul pole hiljem võimalik tagada saadetud päringute tõestusväärtust. Seega on rangelt mittesoovitatav vastavat parameetrit oma äranägemise järgi konfigureerida. Ajatembeldamise ebaõnnestumise parameeter on pigem kaitsemehhanism, mida saab

kasutada olukorras, kus ajatempliteenuse osutaja teenuses esineb katkestus, mida ei suudeta lubatud aja jooksul lahendada ning seega on võimalik andmevahetust X-teel siiski jätkata.

3.4 Testide koostamine

Eduka testimise aluseks on vajaduspõhiselt koostatud testilood, milles on välja toodud testitav objekt, sisendid, tingimused ja oodatavad tulemused. Testilugude dokumenteerimise detailsus sõltub organisatsioonist, testitavast lahendusest ja testimise eesmärgist. Kõigepealt tuleb selgeks teha testimise tingimused, mille tulemusena saab kokku koguda testide koostamiseks vajaliku info. Selleks kasutatakse näiteks süsteemi nõudeid, tehnilist kirjeldust, programmikoodi, ettevõtte äriprotsesse või töötajate kogemusi [36]. Testi tingimuste identifitseerimine aitab luua detailseid teste.

Konkreetsete testilugude koostamisel on tähtsaim võimalikult täpselt kirja panna oodatud testi tulemus. Testimise edukus sõltub otseselt testilugude loomise kvaliteedist. Vastasel juhul võib tekkida olukord, kus kõige olulisemad ja kriitilisemad funktsionaalsused jäävad testimata ja võimalikud vead avastatakse alles, siis kui kasutajad toodet juba aktiivselt kasutavad.

Antud töös on testilugude loomisel lähtutud IEEE 829 standardist [53], mille näol on tegemist dokumendiga, milles selgitatakse, kuidas koostada testi dokumentatsiooni ja teste omavahel seostada. Testilugu sisaldab infot testiloo identifikaatori, testitava toote, sisend- ja väljundparameetrite, keskkonna eelduste, spetsiaalsete protseduuriliste eelduste ja teiste süsteemidega seotud sõltuvuste kohta.

Järgnevates alapeatükkides välja toodud testilood on koostatud kriitiliste kesksete teenuste tõrketaluvuse testimiseks. Teenuseid selgitati eelmistes peatükkides 3.3.1, 3.3.2 ja 3.3.3. Testilugude kirjutamisel on lähtutud olemasolevast arendaja poolt loodud testplaanist, IEEE 829 standardist, süsteemi tehnilisest kirjeldusest ja parameetritest, äriprotsessidest ning arhitekti ja teenusehaldurite töökogemusest. Testimise eesmärk on testida teenuseid, mitte seadistatud konfiguratsiooni. Seetõttu on testilugude puhul vähendatud parameetrite väärtusi, et hoida kokku testimisele kuluvat aega. Testilood antakse testijatele täitmiseks lisaks testplaanile täiendavate testilugudena ja edastatakse käesolevas töös oleval kujul (vt Lisa 2-4).

3.4.1 Globaalse konfiguratsiooni test

Testi eesmärk on veenduda, kas globaalse konfiguratsiooni kehtivuse aegumise korral on andmevahetus X-tee liikmete vahel mõjutatud. Nagu käesolevas töös varasemalt mainitud, siis kogu X-tee kasutamise aja jooksul ei ole kordagi reaalselt olnud intsidenti, kus globaalse konfiguratsiooni genereerimise ja edastamisega oleks probleeme ning konfiguratsiooni kehtivuse aeg ületataks. Vastavat olukorda pole ka ametlikult testitud. Arhitektuuriliselt ja süsteemi parameetrite kohaselt on teada, et kui keskserver ei suuda globaalset konfiguratsiooni genereerida ja liikmetele jagada ning viimase õnnestunud globaalse konfiguratsiooni kehtivus turvaserverites aegub, siis ei suuda turvaserverid enam omavahel päringuid vahetada.

Toodangukeskkonnas on globaalse konfiguratsiooni kehtivuseks määratud kuus tundi [10]. Kui probleem lahendatakse kuue tunni jooksul, siis turvaserverid sellest mõjutatud ei saa, kuna neil on olemas konfiguratsioon, mis kehtib kuus tundi. Kui lahendust ei leita kuue tunni jooksul, siis lõppevad päringud turvaserverite vahel veateadetega alates hetkest, mil turvaserveris hoitav globaalne konfiguratsioon oma kehtivuse kaotab ega saa uuesti globaalset konfiguratsiooni küsides uut kehtivat konfiguratsiooi kätte. Niipea kui keskserver suudab uuesti globaalset konfiguratsiooni jagada, taastub ka olukord liikmete andmevahetuses.

Koostatud testiloos identifikaatoriga TS01 (vt Lisa 2) võrdsustati globaalse konfiguratsiooni kehtivus kuue tunni (21600 sekundit) asemel kümne minutiga (600 sekundit). Vastasel juhul peaks ootama kuus tundi, et näha, kas testi läbiviimise tulemus vastab oodatule. Kümme minutit on globaalse konfiguratsiooni kehtivuse vaikimisi väärtus uue installatsiooni korral [47]. Seetõttu otsustas autor kuue tunni asemel kasutada kümmet minutit.

Testiloo identifikaatoriga TS01 punktis 6 tekitati olukord, mille tagajärjel ei ole võimalik keskserveril enam globaalset konfiguratsiooni tekitada. Seejärel tehti punktis 7 testpäring, mis peab õnnestuma, kuna konfiguratsioon pole sel hetkel veel jõudnud aeguda. Seejärel oodati punktis 8 kümme minutit, sest see oli konfiguratsiooni kehtivuse aeg ja pärast seda sooritati punktis 10 uuesti testpäring, mis peab ebaõnnestuma, kuna globaalne konfiguratsioon on selleks hetkeks aegunud.

3.4.2 Kehtivuskinnituse teenuse test

Testi eesmärk on veenduda, kas kehtivuskinnituse teenuse kehtivuse aegumise korral on andmevahetus X-tee liikmete vahel mõjutatud. Tegemist on X-tee platvormi jaoks senitundmatu teenusega, mida rakendatakse esmakordselt X-tee versioonis 6. Seega on teenuse kasutamine X-teel veel mõnevõrra uus ning selle tõrketaluvuses ei ole varasemalt testimise käigus veendutud. Kehtivuskinnituse teenust tarbitakse toodangu- ja testkeskkonnas SK ID Solutions AS-ilt. Seega teenuse toimimine sõltub otseselt X-tee keskuse välisest osapoolest ja osati ka X-tee-poolsest liidestusest vastava teenusega.

Kui turvaserveril puudub info piisavalt värske OCSP vastuse kohta ja tal ei õnnestu saada õiget staatust teiselt turvaserverilt ning eelneva tulemusena sertifitseerimisahela verifitseerimine ebaõnnestub, siis lõppevad ka päringud osapoolte vahel veateadetega. Põhjusel, et turvaserver ei vaheta sõnumeid tundmatu osapoolega, kelle õigsuses tal ei ole võimalik veenduda. See on vajalik selleks, et andmed, mida X-teel vahendatakse ei satuks tuvastamata osapoolte kätte ja andmete konfidentsiaalsus oleks tagatud.

Toodangukeskkonnas on OCSP kehtivuse aeg kaheksa tundi [10]. Koostatud testiloos identifikaatoriga TS02 (vt Lisa 3) võrdsustati OCSP vastuse kehtivuse parameeter *ocspFreshnessSeconds* kaheksa tunni (28800 sekundit) asemel kümne minutiga (600 sekundit). Testiloo identifikaatoriga TS02 punktis 2 tekitati olukord, mille tagajärjel ei ole võimalik OCSP vastajalt vastuseid saada. Seega peavad ka päringud veateadetega lõppema. Punktis 4 fikseeriti globaalse konfiguratsiooni kehtivuse lõppemise aeg selleks, et punktis 6 oleks võimalik veenduda, et turvaserver sai uue globaalse konfiguratsiooni ja arvestab tehtud muudatust. Punktis 7 tehti päring, mis peab õnnestuma, kuna OCSP vastused peavad olema sel hetkel veel kehtivad. Seejärel oodati 10 minutit ja punktis 9 tehti uus päring, mis peab ebaõnnestuma, kuna selleks ajaks on OCSP vastused kehtetud.

3.4.3 Ajatempliteenuse test

Testi eesmärk on veenduda, kas ajatempliteenuse mittetöötamise korral on andmevahetus X-tee liikmete vahel mõjutatud. Sarnaselt kehtivuskinnituse teenusega, on ka ajatempliteenus esmakordselt X-teel kasutusel ning selle tõrketaluvuses ei ole varasemalt testimise käigus veendutud. Ajatempliteenust tarbitakse kõigis X-tee keskkondades samuti väliselt usaldusteenuse pakkujalt SK ID Solutions AS-ilt.

Selleks, et saadetud sõnumite tõestusväärtuses oleks võimalik hiljem veenduda, tegeleb turvaserver sõnumilogi ajatembeldamisega. Ajatembeldatakse nii päringud kui ka vastused, mis turvaserverist väljuvad. Ajatembeldamine ei toimu kohe kui sõnum saadetakse, vaid perioodiliselt teatud aja tagant. Näiteks toodangukeskkonnas toimub see kolmkümmend korda ööpäevas [10]. Eelnevalt on peatükis 3.3.3 välja toodud, et turvaserver töötaks põhimõtteliselt ka ilma ajatempliteenuseta, kui ta on vastavalt seadistatud. Praktikas ei ole soovitav seda rakendada, kuna sel juhul oleks keeruline hiljem allkirja kehtivust tõestada.

Testiloo identifikaatoriga TS03 (vt Lisa 4) koostamisel ei olnud eesmärgiks leida võimalusi, kuidas ajatembeldamise kasutamisest loobuda, vaid püüda tekitada olukord, kui ajatempliteenust ei ole ja veenduda, et sel juhul on mõjutatud ka andmevahetus. Testimise lihtsustamiseks asendati turvaserveri konfiguratsioonifailis parameetri *acceptable-timestamp-failure-period* toodangukeskkonnas kasutatav ja ühtlasi ka vaikimisi väärtus neli tundi (14400 sekundit) kümne minutiga (600 sekundit). Seejärel tehti testiloo identifikaatoriga TS03 punktis 3 päring, mis peab õnnestuma, kuna turvaserver saab päringut ajatembeldada. Pärast seda tekitati punktis 4 olukord, mille tagajärjel ei ole turvaserveril võimalik saadetavaid päringuid ja vastuseid ajatembeldada. Punktis 7 tehti taaskord päring, mis ei pea õnnestuma, kuna turvaserver ei saa päringuid ajatembeldada ja seetõttu ei tohi ta ka rohkem päringuid teenindada.

4 Tulemuste analüüs, järeldused ja edasised plaanid

Peatüki eesmärgiks on anda ülevaade testimise korraldusest ja kokkuvõttest, testide tulemustest ning tehtud analüüsist ja järeldustest.

4.1 Testimise läbiviimine

Magistritöö kirjutamise perioodil korraldas RIA Euroopa Liidu struktuurifondide investeeringute kava projektist "X-tee piirideülene koostöö" riigihanke "Ühisarendatud koodi manuaalne testimine nr 2" [54]. Hanke käigus testiti X-tee versioon 6 tuumtarkvara versiooni 6.9.4, mis oli testimise alustamisel värskeim versioon. Varasemas peatükis 2.3 tõi autor välja X-tee versioon 6 peamised erinevused võrreldes versioon 5-ga. Ühtlasi selgitas mitmeid erinevaid funktsioone, mida X-tee komponendid uues versioonis täidavad. Seoses eelneva, rahvusvaheliseks muutumise ja X-tee E-identimise ja e-tehingute usaldusteenuste seadusega [33] kooskõlla viimisega, on X-teele lisandunud usaldusväärtust tagavaid teenuseid, mille mõju X-tee platvormile oli vaja testida. Sel põhjusel peeti lisaks värskeima tarne testimisele vajalikuks hankes katta ka tõrketaluvuses veendumiseks tarvilikud täiendavad testid.

RIA ei korralda põhjalikku majasisest X-tee testimist tarkvara tarne loomise eesmärgil, kuna selleks napib ressurssi ja valdkonna peamine rõhk on hetkel ülemineku korraldamisel uuele X-tee versioonile 6. Testimise muudab mahukaks asjaolu, et lisaks Eestis tehtavatele arendustele, toimub aktiivne koostöö ka Soomega. See teeb toodangukeskkonna jaoks vajaliku tarne moodustamise väga keeruliseks, kuna Soome arendajad lisavad X-tee tuumtarkvarasse muudatusi Soome rahvastikuregistrikeskuse (soome k *Väestörekisterikeskus, VRK*) tellimusel. Kokkupandavas tarnes võib olla näiteks poole aasta jooksul tehtud soomlaste arendusi, mille tootestamise kõlblikkust ei saa testimata eeldada. Seetõttu ei olnud autori eesmärgiks testkeskkonna paigaldamine ja seadistamine ning testide iseseisev täitmine. Testimine viidi läbi testimise teostaja

taristus. X-tee tuumtehnoloogia töökindluse ja kvaliteedi tagamiseks telliti hanke käigus manuaalse testimise läbiviimist nii testilugude põhiselt kui ka uurivat meetodit kasutades. Testimist tehti integratsiooni- ja süsteemitesti tasemel. Testilood põhinesid X-tee üleandmise testplaanil, mida RIA on varasemalt ka ise vastuvõtutestimisel kasutanud. Lisaks koostas autor kriitiliste kesksete teenuste testimiseks täiendavad testilood (vt Lisa 2-4), mille loomiseks arvessevõetud tegurid on selgitatud peatükkides 3.4.1, 3.4.2 ja 3.4.3.

Testimist teostati testijate poolt riigihankes ettenähtud ajaperioodil alates 21. veebruarist kuni 16. märtsini 2017. aastal. Testijad jõudsid töödega valmis planeeritud aja jooksul ega vajanud täiendavat aega. RIA ehk tellija poolt olid etteantud testid, mis pidid täidetud saama. Testijad said ise otsustada testide läbiviimise järjestust. Teatud testid sõltusid teineteisest ehk olid eelduseks teiste testide täitmisel.

Testimise tulemused dokumenteeriti RIA JIRA Xray keskkonnas ja need olid tellijale kogu projekti jooksul nähtavad. Vajadusel konsulteeris töö teostaja jooksvalt tellijaga. Tekkinud küsimusi arutati Skype'i vahendusel. Küsimused puudutasid nii testide läbiviimist, tehnilist konsultatsiooni kui ka täpsustusi dokumentatsiooni kirjutamise osas. Lisaks kohtuti testijatega projekti jooksul kolm korda, et saada ülevaade tööde teostamise kohta ja vajadusel rääkida pikemat arutelu nõudvatest teemadest. See andis tellijale kogu projekti vältel kindluse, et töid teostatakse vastavalt ajakavale ning töödega jõutakse valmis ettenähtud ajaks.

Aja kokkuhoidmiseks oli partner valmis kasutama tellija poolt pakutavat sertifitseerimiskeskust. See tähendas, et kui mõne testi teostamiseks oli vajalik kasutada sertifitseerimisteenust, näiteks sertifikaate väljastada või tühistada, siis RIA teenusehaldurid võimaldasid seda. See tekitas testijate töös küll mõningaid väiksemaid viivitusi, mis ei mõjutanud projekti ajakava, kuid panid testijad tellijast teatud määral sõltuma.

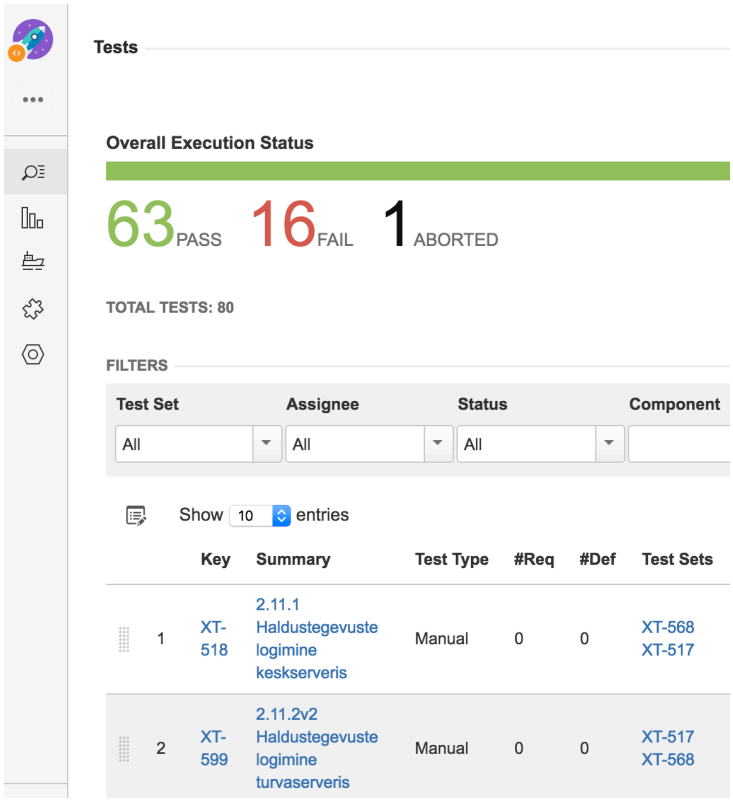
Kui umbes kolmveerand testimisest oli lõpule viidud, selgus juhuslikult vestluse käigus, et testijad olid ekslikult testinud vale versiooni (vanemat, mis oli juba varasemalt testitud). Tellijana oldi koheselt mures, et tööde üleandmine võib viibida. Testijad kinnitasid, et kuna enamus ettenähtud ajast kulus neil süsteemiga tutvumiseks ja

dokumenteerimiseks, siis teistkordne testimine võtab kordades vähem aega ja projekti tähtajad sellest tulenevalt ei muutu.

Küll aga otsustas partner õige versiooni testimisel ise sertifitseerimiskeskuse paigaldada, et kiirendada testimise protsessi. Testijad varustati tellija abil vajaliku dokumentatsiooni ja juhistega ning nad said täiendava komponendi paigaldatud ja seadistatud. Testijad alustasid õige versiooni testimist ja jõudsid tööd üleantud vaatamata kõigele algselt kokkulepitud tähtajaks.

4.2 Testimise kokkuvõte

Testimisel lähtuti X-tee üleandmise testplaanist ja täiendavatest testilugudest, mis kokku moodustasid kaheksakümmend testi. Edukalt läbiti kuuskümmend kolm testi, üks test jäi osapoolte kokkuleppel täitmata ning kuusteist testi ebaõnnestusid (vt Joonis 6).



Joonis 6. Testide tulemuste kokkuvõte

Edukalt läbitud testide hulka loeti testid, mille tulemused vastasid oodatule ja mille testilood ei vajanud täiendamist ning olid arusaadavad. Täitmata jäänud test jäi tegemata, kuna testijate poolt paigaldatud ja seadistatud sertifitseerimiskeskusel

puudusid teatud funktsionaalsused, mis olid vajalikud testi läbimiseks. Ebaõnnestunud testideks peeti teste, mis ei vastanud oodatule või mille testilood olid kirja pandud kujul, mis ei võimaldanud saavutada oodatud tulemust esimesel katsel. Sellistest testilugudest loodi kloonid ja parandati koostöös tellijaga kujule, mis võimaldab saavutada testide eesmärke.

Testimise teostaja hinnangul oli kõige keerulisem testimiseks vajaliku keskkonna ülesseadmine. See võttis ebaproportsionaalselt palju aega võrreldes ajaga, mis kulus reaalse testimise peale. Nende ettepaneku kohaselt võiks tellija järgmisel korral pakkuda valmis testkeskkonda, et testijad saaksid koheselt testima hakata. Tellijale ei tulnud see üllatusena, kuna varasemalt läbiviidud manuaalse testimise tagasiside, küll teise partneri poolt, oli sama. Seda teades oli tööde teostamiseks määratud aega lisatud aeg (umbes kaks nädalat), mis kulub sisseelamiseks ja tarkvarast arusaamiseks. Tegemist oli teadliku otsusega, kuna koheselt testima asudes puudub partneril täielikult arusaam tarkvara toimimisloogikast, mis pärsib testimist. Sel juhul tekiks partneril rohkelt küsimusi, millele vastamine võtaks tellijal palju aega ja kaoks ka manuaalse testimise läbiviimise väljast tellimise kasu. Lisaks oskavad partneri testijad tähelepanu pöörata asjaoludele, mida tarkvara tundvad inimesed ei pruugi märgata. Tellijal puuduv ajaline ressurss oli peamiseks hanke korraldamise põhjuseks. Küll aga on tellija nõus, et testimisel kasutatud dokumentatsioon on kohati puudulik ja vajab kindlasti täiendamist. Tõenäoliselt vähendaksid täpsed ja detailsed juhised keskkonna paigaldamisele kuluvat aega.

Kokkuvõttes leiti testimise käigus kolm tarkvara viga, mis dokumenteeriti ja edastati tellijale edasiseks uurimiseks. Nendel vigadel autor töös rohkem ei peatu, kuna ükski neist ei olnud tõsine ega seotud kriitiliste kesksete teenuste või X-tee platvormi tõrketaluvusega. Üldjoontes oli testimine edukas, sest üheski olulises funktsionaalsuses vigu ei olnud ja testimine kulges ootuspäraselt. See tähendab, et tarkvara tarne avalikustamisel ei esine eeldatavalt takistusi testitud funktsionaalsuse osas ja suuremad riskid on maandatud. Väljatoodud puudused seisnesid peamiselt juhendites ja aegunud dokumentatsioonis.

Järgnevates alapeatükkides toob autor detailselt välja kriitilisi keskseid teenuseid puudutavate testide tulemused, mille põhjal teeb järeldused X-tee platvormi tõrketaluvuse kohta.

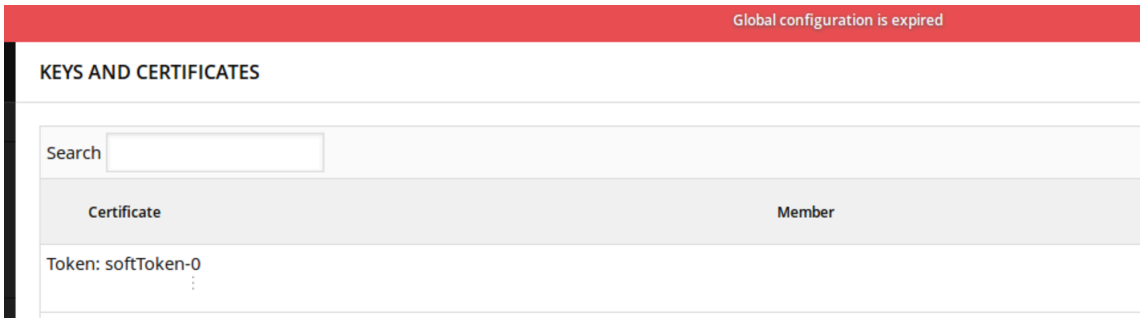
4.2.1 Globaalse konfiguratsiooni testi tulemused

Testi tulemused vastasid oodatule ehk turvaserveris ei õnnestunud päringute töötlemine pärast globaalse konfiguratsiooni aegumist. Test sooritati vastavalt Lisas 2 näidatud testiloole. Testimiseks kasutati testteenust, mille sisu on leitav Lisast 5. Testi õnnestumist tõestab veateade (vt Joonis 7), mis saadi pärast globaalse konfiguratsiooni kehtivuse lõppemist päringut tehes.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
    <faultcode>Server.ClientProxy.OutdatedGlobalConf</faultcode>
    <faultstring>Global configuration is expired</faultstring>
    <faultactor></faultactor>
    <detail>
      <faultDetail xmlns="">6625i47c-a8dd-4a4c-baa1-0179fb634590</faultDetail>
    </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Joonis 7. Globaalse konfiguratsiooni testi SOAP vastus

Testiloo identifikaatoriga TS01 punkti 9 kohaselt peab ka turvaserveri haldusliideses olema näha punasel taustal veateateid globaalse konfiguratsiooni aegumise kohta. Testimine kinnitas, et haldusliidese kõigis vaadetes olid vastavad veateated. Joonisel 8 on kujutatud ühe näitena kuvatõmmis turvaserveri haldusliidese “Keys and Certificates” vaatest, kus on näha punasel taustal veateadet “Global configuration is expired” globaalse konfiguratsiooni aegumise kohta.



Joonis 8. Globaalse konfiguratsiooni aegumise veateade

Kõik testiloo sammud olid korrektsed ja täitsid eesmärki. Küll aga oli testi näol tegemist ühest kuueteistkümnest testist, mis loeti ebaõnnestunuks, kuna testiloos oli puudu üks eeldus. Testiloo kirjutamisel lähtus autor juba olemasolevast töötavast keskkonnast

mitte uuest paigaldusest. Selgus, et testiloo esimeses punktis olev parameeter *confExpireIntervalSeconds* oli andmebaasist puudu ja selle muutmiseks oli parameeter vaja esmalt andmebaasi lisada. Testijad lõid vastavast testiloost klooni ja lisasid testiloole vajaliku eelduse ja viite juhendile.

4.2.2 Kehtivuskinnituse teenuse testi tulemused

Testi tulemused vastasid oodatule ehk turvaserveris ei õnnestunud päringute töötlemine pärast OCSP vastuse kehtivuse lõppemist. Test sooritati vastavalt Lisas 3 välja toodud testiloole. Testimiseks kasutati testteenust, mille sisu on leitav Lisast 5. Testi õnnestumist tõestab veateade (vt Joonis 9), mis saadi pärast OCSP vastuse kehtivuse lõppemist päringut tehes.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
    <faultcode>Server.ClientProxy.SslAuthenticationFailed</faultcode>
    <faultstring>Security server has no valid authentication certificate</faultstring>
    <faultactor></faultactor>
    <detail>
      <faultDetail xmlns="">9285i47c-a8dd-4a4c-baa1-0179fb634590</faultDetail>
    </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Joonis 9. Kehtivuskinnituse teenuse testi SOAP vastus

Kõik testiloo sammud olid korrektsed ja täitsid eesmärki. Sarnaselt eelmise testiga oli ka selle testi näol tegemist ühest kuueteistkümnest testist, mis loeti ebaõnnestunuks, kuna testiloos oli samuti puudu üks eeldus. Testiloo kirjutamisel lähtus autor taaskord olemasolevast töötavast keskkonnast mitte uuest paigaldusest. Selgus, et testiloo esimeses punktis olev parameeter *ocspFreshnessSeconds* oli andmebaasist puudu ja selle muutmiseks oli parameeter vaja esmalt andmebaasi lisada. Lisaks täiendasid testijad testiloo identifikaatoriga TS02 punkti 2, milles oli ununenud täpsustus, et OCSP vastaja URL-i muutmisel tuleb kindlasti lisada ka uuesti korrektne sertifikaat, kuna URL-i vahetamisega läheb kaduma juba varasemalt imporditud sertifikaat. Testijad tegid vastavast testiloost klooni, lisasid testiloole vajaliku eelduse ja viite juhendile ning täpsustasid testiloo teist sammu.

4.2.3 Ajatempliteenuse testi tulemused

Testi tulemused vastasid oodatule ehk turvaserveris ei õnnestunud päringute töötlemine pärast ajatempliteenuse katkemist. Test sooritati vastavalt Lisas 4 välja toodud testiloole. Testimiseks kasutati testteenust, mille sisu on leitav Lisast 5. Testi õnnestumist tõestab veateade (vt Joonis 10), mis saadi pärast ajatempliteenuse katkemist päringut tehes.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
       <faultcode>Server.ClientProxy.LoggingFailed.TimestamperFailed</faultcode>
       <faultstring>Cannot time-stamp messages: no timestamping services
       configured</faultstring>
       <faultactor></faultactor>
       <detail>
         <faultDetail xmlns="">2215i47c-a8dd-4a4c-baa1-0179fb634590</faultDetail>
       </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Joonis 10. Ajatempliteenuse testi SOAP vastus

Vaatamata sellele, et test iseenesest õnnestus ja oodatud tulemus saavutati, viitasid testijad asjaolule, et testiloos identifikaatoriga TS03 sisalduvad sammud 1, 2 ja 5 on tarbetud, kuna tegelikkuses ei arvestatud parameetris *acceptable-timestamp-failure-period* määratud väärtusega, milleks oli 600 sekundit. See tähendab, et turvaserver keeldus päringuid töötlemast kohe kui ajatempliteenus kustutati, mitte pärast 600 sekundit. Tellija otsustas, et antud test iseenesest töötas, kuid ei täitnud sellele osutatud eesmärki. Eeldati, et ajatempliteenuse kustutamisel testiloo sammus 4 arvestatakse sammus 1 seadistatud aega, kuid oletus ei pidanud paika. Seega tehti otsus, et testilugu vajab muutmist. Koheselt tekkis kaks varianti, kuidas saavutada soovitud olukord. Esimene variant eeldas turvaserveri tulemüüris ajatempliteenuse piiramist ja teine veelgi lihtsam variant tähendas ajatempliteenuse peatamist sertifitseerimiskeskuse serveris. Otsustati teise variandi kasuks, kuna seda oli kergem teostada ja see sarnanes ka rohkem reaalsele olukorrale, mis võib tekkida.

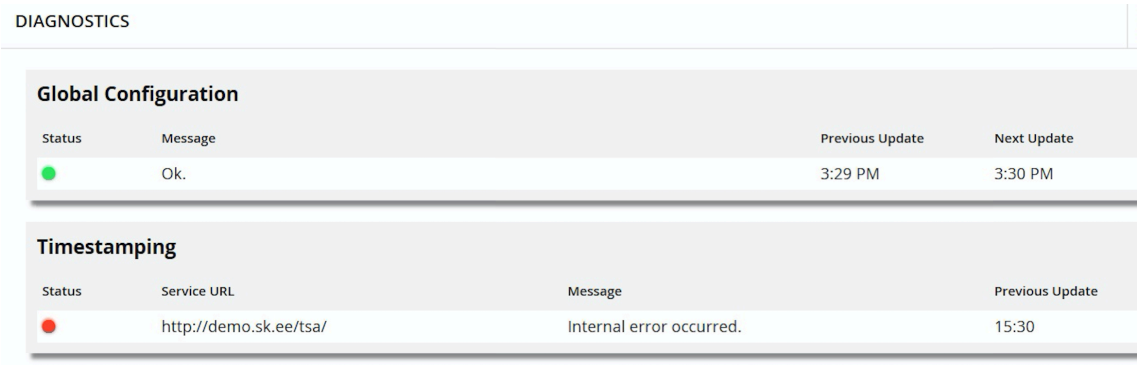
Testijad lõid vastavast testiloost klooni, muutsid testiloos identifikaatoriga TS03 sammu 4 vastavalt kokkulepitule ja sooritasid testi. Testijad kinnitasid, et testilugu vastab nüüd algsetele ootustele ja testis arvestatakse esimeses sammus konfigureeritud ajaga.

Selle kinnituseks dokumenteerisid nad ka veateate (vt Joonis 11), mis päringu sooritamisel saadi.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
       <faultcode>Server.ClientProxy.LoggingFailed.TimestamperFailed</faultcode>
       <faultstring>Cannot time-stamp messages</faultstring>
       <faultactor></faultactor>
       <detail>
         <faultDetail xmlns="">2215i47c-a8dd-4a4c-baa1-0179fb634590</faultDetail>
       </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Joonis 11. Ajatempliteenuse teise testi SOAP vastus

Samal ajal oli turvaserveri haldusliidese "Diagnostics" vaates näha viga ajatempliteenuses esineva vea "Internal error occured." kohta (vt Joonis 12).



Joonis 12. Ajatempliteenuse veateade

Testi tulemusi oodates arutas tellija valdkonnasiseselt detailsemalt ajatempliteenuse toimimist ja arutelu käigus selgusid veel kaks lisatingimust, mille toimimist sooviti testida. Nende realiseerimiseks oli sisuliselt vaja läbida samasugused sammud, mis on testiloos identifikaatoriga TS03, kuid esimeses sammus olev *acceptable-timestamp-failure-period* parameeter erines testiloos olevast ja ajatempliteenus pidi olema sertifitseerimiskeskuses peatatud. Testijatel ei olnud otsest kohustust kahte täiendavat testi sooritada, kuna kõik testid, mida partner pidi läbi viima, olid fikseeritud algses lähteülesandes. Vaatamata sellele otsustas autor siiski pöörduda testijate poole kahe täiendava testiloo läbimiseks, põhjendades seda asjaoluga, et testijatel on veel töötav

testkeskkond olemas ja ka kogemus vastavate testide läbimiseks. Testijad olid nõus abistama ja täiendavad testilood läbima.

Vajadus lisatestide järele tekkis olukorra kirjeldusest, mis on välja toodud peatükis 3.3.3. Põhimõtteliselt on turvaserveri administraatoril võimalik konfigureerida ajatempliteenust talle sobivalt, kuid see on rangelt mittesoovitatav. Tegemist on pigem kaitsemehhanismiga, mida tuleks kasutada ainult äärmisel vajadusel. Tellija soovis saada kinnitust kahele kasutusloole:

1) kas turvaserveris parameetri *acceptable-timestamp-failure-period* väärtuse 0 korral on ajatempliteenus väljalülitatud (ingl k *disabled*) ja turvaserver töötleb päringuid edasi või tähendab see, et ajatempliteenuses ei tohi esineda katkestust ja turvaserver ei töötle päringuid;

2) kas turvaserveris parameetri *acceptable-timestamp-failure-period* väärtuse INT_MAX korral töötleb turvaserver päringuid edasi ka juhul, kui ajatempliteenus on turvaserveris seadistamata või mitte.

Testijad läbisid mõlemad testid vastavalt kokkulepitule ja saatsid testimise ajal sooritatud sammude ja tulemuste kohta täpsustused.

Esimese täiendava testi tulemusena selgus, et kui parameetri *acceptable-timestamp-failure-period* väärtus on 0 ja ajatempliteenus on sertifitseerimiskeskuses väljalülitatud, siis turvaserver töötleb päringuid edukalt. Tulemust ei muuda ka asjaolu, kas ajatempliteenus on turvaserveris konfigureeritud või mitte, mis sisuliselt tähendab, et sel juhul ei sõltu turvaserveri päringute töötlemine ajatempliteenuse olemasolust ega toimimisest. Sellise konfiguratsiooni puhul tagatakse andmete terviklus andmevahetuses vaid osaliselt.

Teise täiendava testi tulemusena selgus, et kui parameetri *acceptable-timestamp-failure-period* väärtus on INT_MAX ja ajatempliteenus on sertifitseerimiskeskuses väljalülitatud, siis turvaserver töötleb päringuid edukalt ainult juhul, kui ajatempliteenus on turvaserveris konfigureeritud. INT_MAX on sisuliselt väga pikk aeg ja nii kaua kuni see pole kätte jõudnud lastakse päringud läbi. Kui ajatempliteenus on turvaserveris konfigureerimata, siis päringute töötlemine ebaõnnestub, mis tähendab, et turvaserveri päringute töötlemine sõltub ajatempliteenuse konfiguratsioonist.

4.3 Järeldused testide tulemuste kohta

Vaatamata sellele, et kõigis kriitiliste kesksete teenuste testimiseks koostatud testilugudes esines mõningaid puudusi, vastasid testide tulemused oodatule. X-tee liikmetevaheline andmevahetus sõltub kriitiliste kesksete teenuste (globaalse konfiguratsiooni jagamine ja usaldusteenused) toimivusest. Kui teenustes esineb tõrkeid, konfigureeritud kehtivuse parameetrid ületatakse ning teenused ei saa taastatud ettenähtud ajaks, siis tekivad probleemid ka X-tee liikmetel omavahel päringuid edastades.

Mis puudutab testilugude kirjutamist, siis on autor arvamusel, et see oli kindlasti üks olulisemaid tegevusi mõistmaks, kas kesksed teenused toimivad vastavalt seni arvatule või mitte. Testilugude koostamine nõudis head süsteemi tundmist, kuna igas testiloos oli omavahel seotud erinevate komponentide koostoimimine ja arvesse tuli võtta mitmeid parameetreid. Nagu näitasid ka peatükis 4.2.3 ajatempliteenuse testide tulemused, siis tegelikult on ilma tervikut nägemata üsna keeruline kirjutada testilugu, et testida just seda, mida on vaja. Tegelikud tulemused selguvad alles hetkel, mil testid läbi viiakse.

Eelnevast tulenevalt arvab autor, et kui ajaline ressurss ja magistritöö maht ei oleks sedavõrd piiratud, siis oleks kindlasti võimalik veel koostada erinevaid testilugusid, mille abil saaks süsteemi toimimist täpsemalt määratleda. Seda kinnitas ka arutelu, mis tekkis ajatempliteenuse testimise käigus. Kui varem polnud niivõrd detailselt kriitiliste kesksete teenuste toimimist kunagi arutatud, siis meeskonnasiseselt mõtteid vahetades, tekkis üha enam stsenaariume, mida võiks kindlasti veel testida. Esialgsed mõtted said tänu vastutulelikule partnerile kaetud, kuid kindlasti on neid veel.

Kui autor hakkas testide tulemusi analüüsima ja kokkuvõtteid tegema, selgus, et testimise käik ei ole testijate poolt piisavalt dokumenteeritud. Selle võrra oli rohkem vaja testijatega suhelda ja paljud tegevused üle küsida. Antud testide juures olid testimise sammud ja vahetulemused isegi olulisemad kui lõpptulemused. Oluline oli mõista, kas oodatud tulemuseni jõuti nii nagu testiloos on ettenähtud. Testilugude kirjutamine ja täitmine ei olnud triviaalsed, sest kui mingi samm vahelt ära unustada, siis võib lõpptulemus küll vastata oodatule, kuid selle tähendus ei ole sama. Koheselt oli selge, et kui tulevikus tehakse veel kriitilisi funktsionaalsusi või teenuseid puudutavaid teste, siis peaks kindlasti olema väga detailselt määratletud, missugust

dokumentatsiooni lõpptulemusena testijatelt oodatakse. Hetkeolukorras oleks lähteülesandes pidanud välja tooma, et täiendavate testilugude puhul soovitakse lisaks testi tulemustele ka detailset raportit või logi testipõhiselt läbiviidud tegevuste kohta. See annab tellijale kindluse, et testitakse õiget omadust või funktsionaalsust õigesti.

Kohati tekkis autoril soov testilood ise läbi testida, et oleks täielik kindlus tehtu osas. Õnneks oli tegemist väga vastutuleliku partneriga, kes oli valmis tellijat varustama kogu vajaliku infoga ja isegi mõnda testi uuesti sooritama, et anda ülevaade, kuidas täpselt tulemuseni jõuti ja vajalik läbi rääkida. Ideaalolukorras oleks parimaks variandiks kõige kriitilisem analüüsida ja arutada arendajatega ning koostööna vajalik testimine läbi viia. Ei ole välistatud, et seda ka tulevikus tehakse. Kokkuvõtvalt oli tegemist esimese sammuga. Tõenäoliselt on võimalik tõrketaluvuse testimiseks kirjutada veel projekte, mille eesmärk oleks vastava teemaga täies mahus tegeleda. Hetkel oli see vaid osa korraldatud hankest, mis näitas, et X-tee platvormi tõrketaluvuse teema on aktuaalne ja sellega peab kindlasti edasi tegelema.

4.4 Ärianalüüs

X-tee keskus ei ole võimeline ainuüksi omal jõul täpselt mõõtma kui suurt mõju ja kahjusid tekitaks X-tee kriitiliste kesksete teenuste tõrgete realiseerumine. Selleks tuleks kaasata ka X-tee liikmeid ja kolmandaid osapooli. Teada on, et kriisiolukorras peatuksid kõik X-tee teenused, kuid pole teada kui suure osa moodustavad X-tee andmeteenused kõigist e-riigis olevatest teenustest. Valdkonnajuhi arvamusel tekiks kahes kolmandikus kõigist avalikest teenustest häireid ja katkestusi kõigis eluvaldkondades ja elualades, kuid keda täpselt ja kui palju mõjutab teenuste seiskumine tegelikult, pole suudetud hinnata. See nõuaks veel vähemalt ühe väga mahuka uurimistöö tegemist.

Selleks, et teada saada missugused avalikud teenused oleksid kindlasti häiritud kui puuduks võimalus X-teed kasutada, peaks esmalt vaatama teenuste kasutusstatistikast olulisemaid osapooli. Seejärel tuleks iga liikmega eraldi suhelda ja neilt välja selgitada, missugused ja kui suur osa teenustest sõltub otseselt X-tee toimimisest. Sisuliselt tehakse samasugust analüüsi ka elutähtsate teenuste osutajate uuringutes. See info on teada teenuseid pakkuvatel ja tarbivatel organisatsioonidel majasiseselt. Oluliselt keerukam on aga välja selgitada tegelikku mõju, mille hindamiseks tuleks esmalt tekitada metoodikad, kuidas mõõta:

1) X-tee platvormist tulenevat otsest mõju asutuste toimimisele,

2) igast andmeteenusest tulenevat mõju andmeteenuste kasutajatele ja pakkujatele.

Eelneva info kogumiseks oleks kindlasti vaja ka X-tee liikmete enda initsiatiivi ja huvi selle vastu. Vastavalt saadud tulemustele saaks X-tee keskus teha edasised järeldused ja otsused oma tegevustes platvormi haldamisel.

4.5 Riskianalüüs

Testimine täies mahus on võimalik ainult väga triviaalsetel juhtudel, kuid tarkvara puhul ei ole see enamasti teostatav. Esiteks tähendaks see tohutut testide arvu ja ajakulu ning teiseks oleks see kokkuvõttes kulukam kui vigade tegelikkuses realiseerumise maksumus. Seetõttu hinnatakse olulisemate testide väljaselgitamiseks riske. Risk on miski, mis ei ole veel juhtunud ega pruugi kunagi juhtuda, kuid on sellele vaatamata potentsiaalne probleem. Riskide hindamine aitab määrata ka tarkvara testidega kaetust. Igal tarkvara süsteemil on oma riskitase ja igal intsidendil on oma mõju [36]. Näiteks mõne e-poe veebilehekülje ajutine tõrge ei põhjustaks tõenäoliselt sama suurt kahju kui X-tee andmevahetuse seisak. Riskianalüüsi eesmärgiks on:

- kaardistada riskid,
- selgitada välja võimalikud ohud ja nõrkused,
- hinnata ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid ning
- valida sobivad turvameetmed ohtude realiseerumise mõju vähendamiseks.

Riskianalüüs on testimise planeerimisel üheks olulisemaks sisendiks [35]. IT valdkonna riskianalüüsiks ei ole Eestis ega rahvusvaheliselt kasutuses ühtset metoodikat. Seega kombineeris RIA vajalikud juhised mitmetest Eesti õigusaktidest, EVS-ISO/IEC 27005:2014 “Infotehnoloogia turbemeetodid. Infoturvariski haldus” standardist [55] ja küberturvalisuse juhisest [56].

X-tee riskianalüüs on koostatud valdkonnajuhi ja arhitekti poolt ning tegemist on asutusesisese dokumendiga, mida pole töös võimalik täies mahus avaldada. Küll aga

saab sealt sisendi, mis on suurimateks ohtudeks ja nõrkusteks andmevahetuses ja kui suur on nende realiseerumise tõenäosus.

Riskianalüüsi koostades jaotati X-tee kui platvorm osadeks, mida oli võimalik hinnata. Riskianalüüsi kohaselt on kaks teenust, mille katkestuste puhul on raskeimaks tagajärjeks andmevahetuse seiskumine: globaalse konfiguratsiooni jagamine ja usaldusteenused. Need on ühtlasi ainsad teenused, mille riskiklass on hinnatud väga kõrgeks. Globaalse konfiguratsiooni jagamise katkestuse esinemise tõenäosus on väga suur ja usaldusteenuste katkemise tõenäosus on suur [57]. Teenuste puhul hinnati mõju ja katkestuse esinemise tõenäosust. Kui mõlemad parameetrid olid kõrged, siis hinnati ka riskiklassi kõrgelt. Riskianalüüsis sisalduv info aitab kindlasti ka edaspidi rõhutada antud teema olulisust ning tõsta selle prioriteeti valdkonna tegevuste hulgas.

4.6 Riskide maandamine

X-tee keskus ei suuda küll iseseisvalt täpselt hinnata mõju ulatust kui X-tee platvormi töös tervikuna esineks tõrkeid, kuid on teada, et need puudutaksid väga suurt osa liikmetest. Kriitiliste kesksete teenuste puhul jälgitakse teenustaseme leppes olevaid ekspluatatsiooninõudeid [9]. Ühe planeerimata või planeeritud katkestuse maksimaalne kestus võib tavaolukorras olla kuus tundi. See tähendab, et alla kuuetunnise katkestuse korral püsitakse lubatud ajavahemikus ja X-tee liikmed mõjutatud ei ole. Kui katkestus kestab üle kuue tunni, siis on andmevahetus häiritud erinevatest hetkedest alates, mil turvaserveri vahemälus hoitav globaalne konfiguratsioon kaotab kehtivuse. Seetõttu tuleb leida vahendid ning välja töötada meetodid ja tegevusplaanid, et katastroofiolukorras oleks katkestustest mõjutatud osapooli võimalikult vähe.

4.6.1 Globaalne konfiguratsioon

Globaalse konfiguratsiooni genereerimises ja jagamises esinevad probleemid võivad olla tingitud erinevatest asjaoludest:

- võrguprobleemidest,
- keskserveri hävinemisest,
- pikaajalisest elektrikatkestusest,

- riistvaralise allkirjastamisseadme ja turvaserverivahelise ühenduse katkemisest,
- administreerimisveast.

X-tee kasutab riigiasutuste andmesidevõrku ASOnet [58], mida RIA pakub ka teistele riigiasutustele ja kohalikele omavalitsustele. Kui globaalse konfiguratsiooni genereerimine ebaõnnestub näiteks ASOnet-ist tulenevate võrguprobleemide tõttu ja on teada, et lahendust ei suudeta leida järgneva kuue tunni jooksul, siis peab RIA kontakteeruma mõne teise andmesidevõrgu teenuse pakkujaga. Kui leitakse alternatiiv, siis tuleb X-tee keskserver üle viia uue teenuse pakkuja juurde ning luua uus konfiguratsiooniankur liikmetele väljasaatmiseks. Kõik need tegevused võtavad aga oma aja, mis peab mahtuma kuue tunni sisse. Selleks, et ajalised hinnangud oleksid objektiivsed, tuleb kõik vastavad tegevused eelnevalt läbi teha ja dokumenteerida.

Kui realiseeruks teine variant ehk turvaserverid ei saa globaalset konfiguratsiooni kätte keskserveri hävinemise tõttu, siis tuleb taastada kõik vajalikud komponendid, mida keskusel on vaja uue konfiguratsiooni tekitamiseks (vt peatükk 3.3.1). X-tee versiooni 6 taastamiseks viidi läbi mitmeid katseid. Tulemused näitasid, et kui taastada on vaja minimaalne komponentide komplekt, et keskserver saaks globaalset konfiguratsiooni jagada, siis kulub selleks umbes tund aega. Planeeritud on korraldada taastetest, milles taastatakse kõik komponendid vastavalt hetkel olemasolevale toodangukeskkonnale. See võtab kindlasti rohkem aega, kuna väga suur roll selles on ka infrastruktuuri osakonnal, kes tegeleb vajalike serverite paigaldamise, seadistamise ja administreerimisega. Pärast seda saavad X-tee teenusehaldurid tegeleda X-tee-spetsiifilise osa seadistamisega. Varasemalt ei ole sellist stsenaariumit testitud.

Lisaks on plaanis luua ja testida talitluspidevuse plaan, mis lisaks tehnilistele tegevustele sisaldab ka kommunikatsiooni kriisiolukorras, mida ei tohi alahinnata. Talitluspidevuse plaan aitab tagada äri toimivuse erinevate ohustsenaariumite realiseerumise korral. Kui kommunikatsioon on tõhus ja läbi proovitud, siis suudetakse kiiremini vajalikke otsuseid vastu võtta. Intsidentidele õigeaegne reageerimine ja eskaleerimine aitavad pidurdada olukorra halvenemist [59]. Kui talitluspidevuse plaani testimisest selgub, et kuus tundi ei ole piisav aeg, mille jooksul X-tee keskkond suudetakse taastada, siis peab globaalse konfiguratsiooni kehtivust pikendama. Seeläbi on keskusel rohkem aega tegutsemiseks, et intsident ei jõuaks mõjutada X-tee liikmeid,

kuna globaalne konfiguratsioon kehtib. Kui X-tee keskus võtab vastu otsuse globaalse konfiguratsiooni kehtivuse pikendamise osas, siis tehakse konfiguratsioonis muudatus, mis jõuab kõigi liikmeteni ja hakkab neile kehtima.

Kõigi eelnevalt põhjendatud riskide maandamise meetmete kohta peab teadma ajakulu. Vastasel juhul ei saa vastu võtta otsuseid, milliseid meetmeid rakendada. Intsidendi korral peab kuuetunnine lubatud katkestus olema jagatud nn kontrollpunktideks, kus võetakse vastu otsused. Kui on teada, et minimaalse komplekti taastamine võtab näiteks tund aega ja katkestus on kestnud juba üle nelja tunni, siis viienda tunni alguses on viimane aeg alustada taastamistegevustega. Kontrollpunktide paika panemisel peab olema arvestatud kui palju aega võtab teatud tegevus ja vastavalt sellele järjestama edasisi etappe.

Kõige olulisem on õigesti planeerida kommunikatsiooni X-tee liikmetele. Kui tekitatakse uus konfiguratsiooni ankur, siis see tähendab, et liikmed peavad selle kasutusele võtma. Kui kommunikatsiooniga viivitatakse, siis ei jõua liikmed uut ankrut kasutusele võtta. Seega on nad siiski mõjutatud ning X-tee keskus ei saa omalt poolt rohkem midagi teha. Seetõttu peab lisaks tõenäoliselt läbi mõtlema kõige kiirema ja tõhusama info liikumise mehhanismi, mille abil jõuaksid ajakriitilise sisuga teated koheselt turvaserverite administraatoriteni.

Kokkuvõtvalt leidub globaalse konfiguratsiooni riskide maandamiseks erinevaid võimalusi, kuid seejuures on väga oluline, et võimalikud olukorrad on läbi testitud ja dokumenteeritud ajalise täpsusega. Siis on võimalik paika panna kontrollpunktid valikuvariantidega ja kommunikatsiooniplaanid.

4.6.2 Usaldusteenused

Usaldusteenuste võimalike intsidentide korral on keskusel oluliselt keerulisem riske maandada, kuna tegemist ei ole RIA poolt pakutavate teenustega, vaid majavälise teenuse pakkujaga. Globaalses konfiguratsioonis on defineeritud usaldusteenuseid puudutavad parameetrid. Kui katkestus suudetakse elimineerida lubatud aja jooksul, siis ei juhtu midagi ja kliendid mõjutatud ei ole. Kui usaldusteenuste osutaja teavitab ametlikult, et intsidenti ei suudeta lahendada õigeagselt, siis on X-tee keskusel võimalus muuta globaalses konfiguratsioonis usaldusteenuste parameetrite kehtivust ajutiselt

pikemaks. Turvaserverid saavad globaalse konfiguratsiooni kaudu uuendatud info ega ole intsidendist mõjutatud.

Seejuures on veel oluline katkestuse põhjus. Kui katkestus on tingitud küberründest (millega võib olla mõjutatud andmete terviklus või konfidentsiaalsus), siis on esimesena vaja välja selgitada, kas viimane usaldusteenuse pakkujalt saadud vastus on usaldusväärne. Kui jah, siis saab keskus taaskord uuendada globaalset konfiguratsiooni ja käideldavuse huvides lõdvendada piire. Siinkohal on tähtsal kohal liikmetele info edastamine, et nad oleksid teadlikud muudatuste põhjustest ja mõistaksid, et võimalikud riskid on analüüsitud ja langetatud otsused põhjendatud. Kui usaldusteenuse osutajalt viimasena saadud vastus ei ole usaldusväärne, siis peab RIA peadirektor tegema otsuse platvormi sulgemise kohta. Kui selgub, et intsidendi tagajärjed ei ole katastroofilised ja süsteem jääb töösse, siis on võimalik taaskord pikendada globaalset konfiguratsiooni kuni usaldusteenuste töö taastub. Kui võetakse vastu otsus platvormi sulgemise kohta, siis on kõige kiiremaks variandiks levitada liikmetele vigast globaalset konfiguratsiooni või X-tee keskuse komponentide seiskamine. Igal juhul on ka selliste stsenaariumite korral kõige olulisem kiire infovahetus X-tee keskuse ja liikmete vahel.

Lisaks eelnevale on SK ID Solutions AS näol tegemist Eestis ainsa kvalifitseeritud usaldusteenuste osutajaga, mis tähendab, et eriolukorras pole hetkel teist teenuse pakkujat, kes suudaks X-tee usaldusteenuste tingimustele vastavat teenust tagada. Infovahetus SK ID Solutions AS ja RIA vahel on seni toiminud efektiivselt, kuid raske on hinnata, kuidas see kriisiolukorras töötaks ja kas see oleks ka piisav. Seetõttu korraldati kohtumine SK ID Solutions AS-iga, kus arutati kriisiolukorras reageerimist. Usaldusteenuste osutaja kinnitas, et neil on olemas töötavad protsessid eriolukordades tegutsemiseks ja varasem kogemus on näidanud, et intsidentidega on suudetud tegeleda operatiivselt hoides ära suuremad kahjud.

X-tee platvormi toimimise seisukohalt on ajal väga suur tähtsus. Kui näiteks usaldusteenuste toimimises esineb tõrkeid, siis on kõige olulisem sellest võimalikult kiiresti teada saada, et saaks planeerida edasisi tegevusi. Olenevalt sellest kui kaua on teenus juba maas olnud, otsustatakse mida edasi teha, et katkestuse mõju ulatus oleks võimalikult väike. Sel põhjusel tegi autor kohtumisel usaldusteenuste osutajaga ettepaneku tekitada RIA-sse võimekus reaalajas jälgida SK ID Solutions AS X-teel kasutatavate teenuste olekuinfot. Täpsemalt soovitakse, et ka RIA monitooringus oleks

näha teenuste kohta info, mis võimaldab kriisiolukorras ka RIA töötajaid kiiresti teavitada, näiteks SMS-i teel. SK ID Solutions AS sai RIA vajadusest aru ja pidas ettepanekut mõistlikuks ning realiseeritavaks. Teemaga tegeletakse edasi ja antakse esimesel võimalusel tagasisidet, kuidas ja millal saaks lahenduse teostada.

Monitooringu lahendus ei tähenda, et RIA ainult sellele tugineb ja kommunikatsioon kaob täielikult ära. Pigem annab see teadmise, valmisoleku reageerimiseks ja lisaaega tegevuste planeerimiseks. RIA saab omalt poolt koostada tegevuste kogumi, mis oleks osa talitluspidevuse plaanist. Kui SK ID Solutions AS teavitab RIA-t ka ametlikult, et nad ei suuda oma teenuseid lubatud ajaks taastada, siis peab RIA-l olema varuplaan. Näiteks on RIA-l ajutiselt võimalik paigaldada ja seadistada sertifitseerimisserver ja pakkuda teenuseid seni kuni SK ID Solutions AS oma teenused taastab. X-tee versioonis 5 pakkus RIA ise X-tee liikmetele vajalikku sertifitseerimiskeskust, seega kogemus selle teenuse pakkumiseks on olemas. Selline lahendus võimaldab X-tee liikmetele tekkivat kahju ära hoida või oluliselt vähendada. Loomulikult nõuab see eraldi analüüsi ja täpset tegevuskava, kuid see oleks kõige tõenäolisem ja realistlikum variant, mida eriolukorras rakendada.

Mitme usaldusteenuse osutaja olemasolu väga suur eelis oleks ka see, et kui ühe usaldusteenuse osutaja teenustes esineb tõrkeid, siis mõjutatud on ainult temaga seotud liikmed, mitte terve platvorm. Pole välistatud, et tulevikus tekib veel kvalifitseeritud usaldusteenuste osutajaid, kes hakkavad oma teenuseid pakkuma ka X-tee liikmetele. Sel juhul peab RIA uute teenusepakkujatega kokkulepped sõlmima ja tekib lisavõimalusi riskide maandamiseks eriolukorras.

4.7 Autoripoolsed soovitused edasiste tegevuste osas

Antud peatükis esitab autor omapoolsed soovitused koos põhjendustega, mis võimaldavad efektiivsemalt ennetada ja parandada valmisolekut juhul, kui X-tee kriitilistes kesksetes teenustes peaks esinema intsidente, mis võivad mõjutada X-tee liikmetevahelist andmevahetust.

- X-tee valdkonnale tuleks kasuks majasisene kompetents testimistegevuste korraldamiseks. Läbiviidud projekti tagasisidena selgus, et kõige keerulisem ja aeganõudvam oli süsteemi tundma õppimine ja testkeskkonna paigaldamine.

Sama tagasiside andsid ka eelmisel hankel osalenud partnerid. Kui majasisesed X-tee testijad tunnevad hästi X-tee tarkvara, siis võidab valdkond testimisel palju aega. X-teel on hetkel kaks arenduspartnerit, mis tähendab rohkem muudatusi loodavates tarnetes, mida on vaja kontrollida. Seega täiendav ressurss testijate näol on õigustatud. Kogenud testijad annavad parema tulemuse, kuna süsteemi tundes oskavad nad rakendada rohkem uurivat testimist ja mõelda "kastist välja". Lisaks oleks nende ülesandeks luua ja hallata testkeskkondi, milles saab koheselt teste läbi viia ja vajadusel korrata. Majasisesed testijad tegeleksid X-tee tarkvara tarnete testimisega ja saaksid panustada teemadesse, mis nõuavad detailsemat analüüsi. Kui vastav kompetents oleks magistritöö kirjutamise hetkel olemas olnud, siis oleks autoril olnud tunduvalt parem ülevaade testimise käigust. Testimise maht oleks võinud suurem olla ja kokkuvõtte tegemine lihtsam, sest vajalik info oleks koheselt kättesaadav olnud.

- Jooksva tegevusena soovitab autor jätkata X-tee komponentide ja kesksete teenuste analüüsimist tõrketaluvuse osas. Testide tulemused näitasid, et kõik uurimise alguses olnud oletused pidasid paika ehk testitud teenuste tõrgete korral on mõjutatud andmevahetus X-teel. Selgus, et kui valdkonnas panustatakse antud teemale veel aega, siis on tõenäoliselt võimalik koostada veel erinevaid testilugusid, mille täitmine annab kindluse süsteemi toimimise osas ja võimaldab saada sisendi, et välja töötada juhised rikete korral reageerimiseks.

- Töö käigus selgus, et X-tee keskus ei saa iseseisvalt ärianalüüsi koostada. Seega teeb autor ettepaneku esmalt vaadata X-tee kasutusstatistikat ja koguda kokku info suurimate andmeteenuste tarbijate ja pakkujate kohta. Teisalt uurida neilt, kui suures osas sõltuvad neile vajalikud teenused X-tee platvormi toimimisest. Seejärel saab RIA analüüsida saadud infot ja teha otsused ning tegevusplaanid, kuidas kriisiolukorras taastada andmevahetus, et mõju osapooltele oleks minimaalne.

- Globaalse konfiguratsiooni kehtivuse objektiivseks hindamiseks tuleb läbi viia talitluspidevuse plaani testimine. Kaasatud peavad olema kõik RIA töötajad, kelle tegevused on vajalikud intsidendi ilmnemise korral. Kaasaarvatud

operatiivse info edastamise eest vastutavad inimesed, kes peavad tekkinud situatsioonist kommunikeerima mõjutatud osapooli. Seni kehtiv nõue on pigem subjektiive hinnang, mis ei põhine analüüsil. Esiteks annab talitluspidevuse plaani läbi tegemine kindluse töötajatele, et nad teavad, mida teha kui tekib eriolukord. Teiseks saab valdkond teada kui palju aega kulub kogu süsteemi taastamisele algusest lõpuni kõigi vajalike tegevustega. Selle tulemusena saab selguse, kas hetkel seadistatud globaalse konfiguratsiooni kehtivus on piisav. Kui jah, siis on teada, mis on viimane ajaline piir, millal on veel võimalik taastamist alustada ja jõuda töötava süsteemini. Sellest tulenevalt saab ka RIA juhtkond võtta vastu õigeid ja läbimõeldud otsuseid, kui sündmused peaksid eskaleeruma.

- Läbiviidud testimisel sai kinnitust ka usaldusteenuste kriitiline tähtsus X-tee andmevahetuses. Hetkel on SK ID Solutions AS X-teel kvalifitseeritud usaldusteenuste osutajaks. Praegu puudub X-tee keskusel mehhanism, mis võimaldab reaalajas näha X-teel kasutatavate usaldusteenuste olekuinfot. Autor rääkis SK ID Solutions AS-ga toimunud kohtumisel RIA vajadustest. Pärast seda lubas partner omalt poolt vastava võimekuse tekitamiseks RIA-le välja uurida vajaliku info. Autor loodab, et valdkond ka edaspidi panustab antud teemasse ja töötav lahendus realiseeritakse võimalikult kiiresti. Üleminek X-tee versioonile 6 toimub aktiivselt. Üha enam liikmeid jõuab arenduste ja testimisega valmis ning liitub toodangukeskkonnaga. Seega on väga tähtis, et X-tee keskusel on vahendid võimalikult kiiresti tuvastamaks kui kriitilistes teenustes esineb tõrkeid.

- X-tee versioon 6 loomise üheks suurimaks eesmärgiks oli andmevahetuse muutmine rahvusvaheliseks. See tähendab, et sisuliselt vahetatakse erinevate X-tee instantside vahel konfiguratsiooniankrud, mille tagajärjel saavad vastavates instantsides olevad liikmed omavahel andmeid vahetada ehk tekib usaldusföderatsioon. See tähendab, et kriisiolukorras võib mõjutatud osapoolte arv veelgi suureneda. Sel põhjusel soovitab autor valdkonnal analüüsida, kuidas mõjutavad tõrked kriitilistes kesksetes teenustes X-tee liikmete andmevahetust usaldusföderatsioonis. Näiteks X-tee versioon 6 arenduskeskkondade ankrud

said Soomega hiljuti vahetatud. Seega on võimalik juba vastavaid olukordi testida esialgu isegi autori poolt loodud testilugude abil.

- Mis puudutab veel usaldusteenuseid, siis peab kindlasti leidma X-teele sobivaid kvalifitseeritud usaldusteenuste osutajaid. Seeläbi tekib X-tee liikmetele suurem valikuvõimalus ja keskus saab kriisiolukorras kasutada teisi usaldusteenuste pakkujaid. Võimalik, et platvormile on võimalik luua funktsionaalsus, kus turvaserverid aktsepteerivad mitmeid sertifitseerimiskeskusi korraga ja kui ühel neist tekib intsident, siis on võimalik pöörduda teiste poole ning andmevahetus X-teel ei ole mõjutatud.

Üldisem nõuanne on jätkata tegevusi X-tee platvormi tõrketaluvuse suurendamiseks järgides eelnevalt välja toodud soovitusi.

Kokkuvõte

Aastaid Eesti e-riigi alustalaks olev infosüsteemide turvaline andmevahetuskiht X-tee on muutumas rahvusvaheliseks. Sel põhjusel muudeti sõnumiprotokolli ja loodi uus X-tee versioon 6. On esmatähtis, et liikmetele pakutav platvorm säilitaks kõigi toimunud muudatuste ja uuenduste juures töökindluse ja teenustaseme leppes lubatu. Vastasel juhul võib olla mõjutatud andmete konfidentsiaalsus, terviklus või käideldavus, mis ei ole lubatav eriti isikuandmeid töötlevate süsteemide puhul.

Magistritöö eesmärgiks oli analüüsida ja välja selgitada, kas X-tee versioon 6 toimimiseks vajalikud komponendid ja teenused töötavad vastavalt keskkonnale määratud tehnilistele omadustele. Töö tulemusena selgusid X-tee kui terviku toimimise seisukohalt kõige kriitilisemad kesksed teenused, mille testimiseks koostas autor testilood ja andis need sisendiks tarkvara manuaalse testimise projekti. Loodud stsenaariumite eesmärgiks oli teada saada, kuidas situatsiooni muutus mõjutab andmevahetust X-tee liikmete vahel.

Autor tegi partnerilt saadud tulemustest kokkuvõtte, millest selgus, et seni paikapidanud oletused olid tõesed. Testid kinnitasid, et globaalse konfiguratsiooni jagamises ja usaldusteenustes esinevate intsidentide korral esinevad tõrked liikmetevahelises andmevahetuses. Lisaks said parandatud testilugude puudused, mille tulemusena saab loodud stsenaariume kasutada edaspidises testimises. Testitud kesksete teenuste kriitilisust kinnitas riskianalüüs, milles oli samade teenuste riskiklassi hinnatud väga kõrgeks. Tehtud analüüsi ja järelduste tulemusena otsustati testida talitluspidevuse plaani, et välja selgitada vajadus globaalse konfiguratsiooni kehtivuse pikendamise osas ja alustati usaldusteenuste osutajaga läbirääkimisi, et täiendada X-tee keskuses olevat monitooringut, mille abil saab kriisiolukorras operatiivselt vajaliku info.

Magistritöös seatud eesmärkide täitmine aitas veenduda X-tee versioon 6 tarkvara korrapärases toimivuses ja suurendas valmisolekut ekstreemses olukorras adekvaatselt reageerida.

Summary

X-Road, the secure data exchange layer for information systems that has been the foundation of Estonia's e-government is becoming international. For this reason, the message protocol was changed and a new version 6 of X-Road was created. It is crucial that the platform offered to X-Road members retained it's reliability and the agreed upon service levels throughout all the changes and updates. Otherwise the confidentiality, integrity or availability of data might be negatively affected which is unacceptable, especially within systems that process personal data.

The goal of this thesis was to analyse and determine whether the components necessary for the functioning of X-Road version 6 were working in accordance with the technical parameters of the X-Road environment. As a result of this thesis, the most critical central services for the functioning of X-Road as a whole were determined. The author created test cases for these central services and used them as an input for a manual software testing project. The goal of these scenarios was to find out how a changed situation would affect data exchange between X-Road members.

The author made a summary of the results received from the testing partner, which confirmed previous assumptions. The tests confirmed that when incidents occur with trust services or with the sharing of global configuration, data exchange between members also fails. The deficiencies in the test cases were resolved which allows them to be used in future testing. The criticality of the tested central services was also confirmed by a risk analysis, in which the risk class of these services was concluded to be very high. As a result of the analysis and the conclusions, it was decided that the contingency plan should be tested to determine the possible need for a longer global configuration validity period. Negotiations with the trust service provider were also started to improve the monitoring at the X-Road centre, which would provide necessary operational data in the event of a crisis.

The fulfilment of the goals set in this thesis helped confirm the consistent operation of X-Road version 6 software and increased readiness to react adequately in the case of an extreme situation.

Kasutatud kirjandus

[1] Vabariigi Valitsus. (27. september 2016. a.). *Infosüsteemide andmevahetuskiht.* Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/127092016004

[2] Cybernetica AS. *X-tee*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Cybernetica AS kodulehekülg: https://cyber.ee/e-riik/x-tee/

[3] Vabariigi Valitsus. (6. jaanuar 2016. a.). *Avaliku teabe seadus*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/106012016007

[4] Riigi Infosüsteemi Amet. (1. oktoober 2016. a.). *X-tee faktileht*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Infosüsteemi Ameti kodulehekülg: https://ria.ee/x-tee/fact/

[5] Veldre, A. (28. august 2015. a.). *Sissejuhatus X-teesse (osa 1)*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Infosüsteemi Ameti ajaveeb: https://blog.ria.ee/tag/x-tee/

[6] Riigi Infosüsteemi Amet. *3.3. X-tee tähtsus*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas X-tee turvaserveri administraatori õppematerjal Riigi Infosüsteemi Ameti Moodle-s: https://moodle.ria.ee/mod/book/view.php?id=320&chapterid=30

[7] Vabariigi Valitsus. (25. jaanuar 2009. a.). *Infosüsteemide turvameetmete süsteem.* Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/13125331

[8] Bernard, P. (2012). *Foundations of ITIL 2011 Edition*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Van Haren Publishing, Zaltbommel kodulehekülg: https://www.vanharen.net/

[9] Riigi Infosüsteemi Amet. (21. oktoober 2015. a.). *Teenustaseme ekspluatatsiooninõuded*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Infosüsteemi Ameti kodulehekülg: https://www.ria.ee/public/x_tee/Teenustaseme_ekspluatatsiooninouded.pdf

[10] Riigi Infosüsteemi Amet. (12. detsember 2011. a.). *X-tee v6 keskkonnad*. Kasutamise kuupäev: 1. detsember 2016. a., allikas Riigi Infosüsteemi Ameti kodulehekülg: https://www.ria.ee/ee/x-tee-keskkonnad.html#v6

[11] Riigi Infosüsteemi Amet. *6.3. Keskkondade erinevused*. Kasutamise kuupäev: 4. veebruar 2017. a., allikas X-tee turvaserveri administraatori õppematerjal Riigi Infosüsteemi Ameti Moodle-s: https://moodle.ria.ee/mod/book/view.php?id=323&chapterid=54

[12] Riigi Infosüsteemi Amet. (14. detsember 2016. a.). *Tallinnas tähistatakse X-tee 15. sünnipäeva*. Kasutamise kuupäev: 4. veebruar 2017. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/ee/tallinnas-tahistatakse-x-tee-15-sunnipaeva.html

[13] D/V/S/ON OÜ. (2015). *X-tee turundusmaterjalid. Valminud Euroopa Liidu struktuurifondide toetusskeemist "Infoühiskonna teadlikkuse tõstmine" Riigi Infosüsteemi Ameti tellimusel.* Kasutamise kuupäev: 24. oktoober 2016. a., allikas Asutusesiseseks kasutamiseks

[14] Riigi Infosüsteemi Amet. (28. detsember 2015. a.). *X-tee tutvustus*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/ee/x-tee-tutvustus.html

[15] Majandus- ja Kommunikatsiooniminister. (26. veebruar 2016. a.). *Riigi Infosüsteemi Ameti põhimäärus*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/126022016002

[16] Riigi Infosüsteemi Amet. (27. juuni 2007. a.). *Riigi Infosüsteemi Amet*. Kasutamise kuupäev: 24. oktoober 2016. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/ee/ria.html

[17] Cybernetica AS. (20. detsember 2016. a.) *X-road Architecture Technical Specification*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas Riigi Infosüsteemi Ameti Github: https://github.com/ria-ee/X-Road/blob/develop/doc/Architecture/arc-g_x-road_arhitecture.md

[18] Euroopa Parlament ja Nõukogu. (28. august 2014. a.) *Euroopa Parlamendi ja Nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas Euroopa Liidu Teataja: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910&from=ET

[19] World Wide Web Consortium (W3C). (2014). *HTTP – Hypertext Transfer Protocol*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas W3C koduleheküg: https://www.w3.org/Protocols/

[20] World Wide Web Consortium (W3C). (2007). *Simple Object Access Protocol (SOAP) Version 1.2 Part 1: Messaging Framework (Second Edition)*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas W3C koduleheküg: https://www.w3.org/TR/soap12-part1/

[21] World Wide Web Consortium (W3C). (2001). *Web Services Description Language (WSDL) 1.1*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas W3C koduleheküg: https://www.w3.org/TR/wsdl

[22] Internet Engineering Task Force (IETF). (1998). *The MIME Multipart/Related Content-type. Request for Comments 2387*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://www.ietf.org/rfc/rfc2387.txt

[23] Internet Engineering Task Force (IETF). (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Request for Comments 5280*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://tools.ietf.org/html/rfc5280

[24] Internet Engineering Task Force (IETF). (2008). *The Transport Layer Security (TLS) Protocol Version 1.2. Request for Comments 5246*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://tools.ietf.org/html/rfc5246

[25] Internet Engineering Task Force (IETF). (2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Request for Comments 3161*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: http://www.rfc-base.org/txt/rfc-3161.txt

[26] Internet Engineering Task Force (IETF). (2013). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Request for Comments 6960*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://tools.ietf.org/html/rfc6960

[27] Riigi Infosüsteemi Amet. (01. november 2016. a.). *Käskkiri X-tee versiooni 6 juurutamise ajakava kinnitamise kohta*. Kasutamise kuupäev: 8. veebruar 2017. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/public/x_tee/kaskkiri-X-tee-versiooni-6-juurutamine.pdf

[28] Riigi Infosüsteemi Amet. (15. jaanuar 2015. a.). *Lühiülevaade peamistest erinevustest X-tee versioonide 5 ja 6 vahel*. Kasutamise kuupäev: 8. veebruar 2017. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/public/x_tee/X-tee_v5_ja_v6_erisused.pdf

[29] Riigi Infosüsteemi Amet. (15. jaanuar 2015. a.). *Üleminek X-tee versioonile 6*. Kasutamise kuupäev: 8. veebruar 2017. a., allikas Riigi Infosüsteemi Ameti koduleheküg: https://www.ria.ee/ee/uleminek-x-tee-versioonile-6.html

[30] Cybernetica AS. (16. mai 2016. a.) *X-road*: Message *Protocol v4.0*. Kasutamise kuupäev: 9. veebruar 2017. a., allikas X-tee versioon 6 repositoorium: http://x-road.eu/docs/x-road_message_protocol_v4.0.pdf

[31] Riigi Infosüsteemi Amet. *10.4. X-tee alamsüsteem*. Kasutamise kuupäev: 9. veebruar 2017. a., allikas X-tee turvaserveri administraatori õppematerjal Riigi Infosüsteemi Ameti Moodle-s: https://moodle.ria.ee/mod/book/view.php?id=327&chapterid=92

[32] Riigi Infosüsteemi Amet. (02. juuni 2016. a.). *Infosüsteemide andmevahetuskihi usaldusteenuste tingimused*. Kasutamise kuupäev: 14. veebruar 2016. a., allikas Riigi Infosüsteemi Ameti koduleheküIg: https://www.ria.ee/public/x_tee/usaldusteenuste_tingimused.pdf

[33] Riigikogu. (25. oktoober 2016. a.). *E-identimise ja e-tehingute usaldusteenuste seadus*. Kasutamise kuupäev: 8. veebruar 2017. a., allikas Riigi Teataja: https://www.riigiteataja.ee/akt/125102016001

[34] IEEE Computer Society. (1. september 2013. a.). *29119-1-2013 – Software and systems engineering Software testing Part 1: Concepts and definitions*. Kasutamise kuupäev: 01. märts 2017. a., allikas IEEE Xplore Digital Library koduleheküIg: http://ieeexplore.ieee.org/document/6588537/

[35] ASA Quality Services. (24. jaanuar 2017. a.). *Testijuhtimise ABC ehk kuidas panna testimine "juhtuma"?*. Kasutamise kuupäev: 01. märts 2017. a., allikas ASA Quality Academy koolitus: http://www.aka.ee/koolitused.html#TJABC

[36] Graham, D. Veenendaal, E. Evans, I. Black, R. (7. aprill 2014. a.). *Foundations of Software Testing ISTQB Certification.* Kasutamise kuupäev: 01. märts 2017. a., allikas Technical University of Cluj-Napoca koduleheküIg: https://www.utcluj.ro/media/page_document/78/Foundations%20of%20software%20testing%20-%20ISTQB%20Certification.pdf

[37] Eesti Standardikeskus. (2012). *EVS-ISO/IEC 25010:2011 – Süsteemi- ja tarkvaratehnika. Süsteemide ja tarkvara kvaliteedinõuded ja kvaliteedi hindamine. Süsteemide ja tarkvara kvaliteedimudelid.* Kasutamise kuupäev: 01. märts 2017. a., allikas Eesti Standardikeskuse koduleheküIg: https://www.evs.ee/tooted/evs-iso-iec-25010-2011

[38] Tepandi, J. (21. detsember 2016. a.). *Tarkvara protsessid, kvaliteet ja standardid.* Kasutamise kuupäev: 01. märts 2017. a., allikas "Software quality (Tarkvara kvaliteet)" kursus: http://tepandi.ee/tks-loeng.pdf

[39] Markvardt, M. (2006). *Tarkvara testimist käsitlev juhendmaterjal.* Kasutamise kuupäev: 01. märts 2017. a., allikas Majandus- ja Kommunikatsiooniministeeriumi koduleheküIg: https://www.mkm.ee/sites/default/files/tarkvara_testimise_juhis_-_koopia.doc

[40] Guru99. (2017). *Automation Testing Tutorial: Process, Planning & Tools.* Kasutamise kuupäev: 08. märts 2017. a., allikas Guru99 koduleheküIg: http://www.guru99.com/automation-testing.html

[41] Cybernetica AS. (9. november 2015. a.) *X-road: Service Metadata Protocol*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas X-tee versioon 6 repositoorium: http://x-road.eu/docs/x-road_service_metadata_protocol.pdf

[42] Internet Engineering Task Force (IETF). (2003). *Public-Key Cryptography Standards (PKCS). #1: RSA Cryptography Specifications Version 2.1. Request for Comments 3447*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://tools.ietf.org/html/rfc3447#page-70

[43] Internet Engineering Task Force (IETF). (2009). *RPC: Remote Procedure Call Protocol Specification Version 2. Request for Comments 5531*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas IETF koduleheküg: https://tools.ietf.org/html/rfc5531

[44] W3Schools. *Introduction to XML*. Kasutamise kuupäev: 14. veebruar 2017. a., allikas W3Schools koduleheküg: https://www.w3schools.com/xml/xml_whatis.asp

[45] Cybernetica AS. (20. jaanuar 2017. a.) *X-Road: Central Server Installation Guide*. Kasutamise kuupäev: 20. märts 2017. a., allikas Riigi Infosüsteemi Ameti Github: https://github.com/ria-ee/X-Road/blob/develop/doc/Manuals/ig-cs_x-road_6_central_server_installation_guide.md

[46] Internet Engineering Task Force (IETF). (2006). *US Secure Hash Algorithms (SHA and HMAC-SHA). Request for Comments 4634*. Kasutamise kuupäev: 20. märts 2017. a., allikas: https://tools.ietf.org/html/rfc4634

[47] Cybernetica AS. (23. veebruar 2017. a.) *X-Road: System Parameters User Guide*. Kasutamise kuupäev: 20. märts 2017. a., allikas Riigi Infosüsteemi Ameti Github: https://github.com/ria-ee/X-Road/blob/develop/doc/Manuals/ug-syspar_x-road_v6_system_parameters.md

[48] SK ID Solutions AS. *Sertifitseerimiskeskuse OCSP-teenus SK-OCSP*. Kasutamise kuupäev: 20. märts 2017. a., allikas SK ID Solutions AS koduleheküg: http://sk.ee/upload/files/kehtivuskinnituse_tech_kirjeldus.pdf

[49] Riigi Infosüsteemi Amet. *8.6. Sertifikaadi kehtivuskinnitus*. Kasutamise kuupäev: 20. märts 2017. a., allikas X-tee turvaserveri administraatori õppematerjal Riigi Infosüsteemi Ameti Moodle-s: https://moodle.ria.ee/mod/book/view.php?id=323&chapterid=54

[50] Cybernetica AS. (17. oktoober 2015. a.) *X-Road: Message Transport Protocol*. Kasutamise kuupäev: 21. märts 2017. a., allikas Riigi Infosüsteemi Ameti Github: https://github.com/ria-ee/X-Road/blob/develop/doc/Protocols/pr-messtransp_x-road_message_transport_protocol_2.2_Y-743-4.docx

[51] Riigi Infosüsteemi Amet. *8.7. Ajatempel*. Kasutamise kuupäev: 20. märts 2017. a., allikas X-tee turvaserveri administraatori õppematerjal Riigi Infosüsteemi Ameti Moodle-s: https://moodle.ria.ee/mod/book/view.php?id=325&chapterid=70

[52] SK ID Solutions AS. *Ajatempliteenuse tehniline lisainfo*. Kasutamise kuupäev: 20. märts 2017. a., allikas SK ID Solutions AS koduleheküg: https://www.sk.ee/teenused/ajatempliteenus/tehniline-lisainfo/

[53] IEEE Computer Society. (2008). *829-2008 – IEEE Standard for Software and System Test Documentation.* Kasutamise kuupäev: 21. märts 2017. a., allikas IEEE Xplore Digital Library kodulehekülg: http://standards.ieee.org/findstds/standard/829-2008.html

[54] Riigi Infosüsteemi Amet. (01. juuni 2016. a.). *Riigi infosüsteemi baaskomponentide kvaliteedijuhtimise ja testimise raamleping. (Viitenumber 173287).* Kasutamise kuupäev: 27. veebruar 2017. a., allikas Rahandusministeeriumi E-riigihangete keskkond: https://riigihanked.riik.ee/register/

[55] Eesti Standardikeskus. (2014). *EVS-ISO/IEC 27005:2014 – Infotehnoloogia. Turbemeetodid. Infoturvariski haldus.* Kasutamise kuupäev: 15. märts 2017. a., allikas Eesti Standardikeskuse kodulehekülg: https://www.evs.ee/tooted/evs-iso-iec-27005-2014

[56] Riigi Infosüsteemi Amet. (2016). *Riskianalüüsi koostamise juhend.* Kasutamise kuupäev: 15. märts 2017. a., allikas Asutusesiseseks kasutamiseks

[57] Riigi Infosüsteemi Amet. (21. november 2016. a.). *X-tee riskianalüüs.* Kasutamise kuupäev: 15. märts 2017. a., allikas Asutusesiseseks kasutamiseks

[58] Riigi Infosüsteemi Amet. (10. jaanuar 2012. a.) *Riigiasutuste andmesidevõrk ASOnet*. Kasutamise kuupäev: 22. aprill 2017. a., allikas Riigi Infosüsteemi Ameti kodulehekülg: https://www.ria.ee/ee/aso.html

[59] Akkermann, K. *Talitluspidevusplaan*. Kasutamise kuupäev: 22. aprill 2017. a., allikas ASA Quality Services OÜ kodulehekülg: https://www.asaquality.ee/images/euro2010/4_Talitluspidevus_Kristjan_Akkermann.pdf

Lisa 1 – X-tee toodangukeskkonna sisemine konfiguratsiooniankur

```
<ns3:configurationAnchor xmlns:ns2="http://x-road.eu/xsd/identifiers" xmlns:ns3="http://x-
road.eu/xsd/xroad.xsd">
    <generatedAt>2015-10-30T12:45:29.925Z</generatedAt>
    <instanceIdentifier>EE</instanceIdentifier>
    <source>
      <downloadURL>http://213.184.41.186/internalconf</downloadURL>
      <verificationCert>
        MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwWhcN
        MzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCspebx
        rUlGPGTbjkv+tihZ2s0F7inWvPm2apDM8o5qjFDXHTnAT2vUkAqG4RJvTA5F2jdxFsQ2yHE3+xojSP5U3s58G3Mj
        ehLCPP8o4mOrXWuWMS5QKOeSuwDQgxiHS0SdD4nugfsrAAIdZCB24eyLokNrmDmvDllYN4xuH30IDltw2R4Y8KWk
        CvcR/2aiB53XNDD3FCC1SqfqSVj2JemLKRVnGQOZDMhF3S2lqHhK9/4adsDORGuYTgsboN60ZjHoCWNT9MzUHk3y
        2ravH16RCCGh05coUslgpjcYqXigm0z4BeAqyfg2dy12QzL8op1nQZ889T+vDdDC6myP84OjAgMBAAGjEjAQMA4G
        A1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAMZdq9VTf57RWMc0ZkqayvadZNDFtO7k9q8xohztUr0BA
        prU+UgvTe8tu4JqfPwx0e10WULugYOR20IUGxVRm6wVmCDr5SVzVuYlV1f/gTxZx7ZuEPHkB1AbnMWCa9qKmD+F9
        i0X1Erp6T62e6Y2x2hriGQMJDnA81nq4EEQYdLQQaiEodU3VMpJD7kDX0jPINE5JpMoMhhFM+wrL5q995C/oR76S
        5elQnGbwJExPArv4HaznLJ9di9MLaLb5nHNFZTrJMXG5vr8Lv5fHwNuC91hlQZVQ+BE5eOHUI8f5Uu00KBqxPTJC
        HlHbhx+OTeuI0d2DVNEEFUn2YQ7uSaKp+A==
      </verificationCert>
    </source>
    <source>
      <downloadURL>http://213.184.41.190/internalconf</downloadURL>
      <verificationCert>
        MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwWhcN
        MzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCelmcJ
        CFxutulUGk1Hx6Lzo3YtYYjSEi1NpTqxcqo2k+baiyOjAiQyT9HJoNZ5KAFw8JsYQzzY8NdJK6HcvQr6Uv4brG36
        lX9S8vI+bkQLPTvtxMgYLAq6TazkPGOq2mdwVsxF4c9u2OHf6E179pokdD7c9cQ9VHCfUqZ/Uu1hLiv9PQ/kWlF6
        JUeyAdFiq5bb/X5VJsptfCFyj8iqwjlXqR57YeGWi6JYGJtpkPyLOc5c/+s6me4cnW9ZkZYrq9Rrlh0oDyqTyajZ
        HW5Cp/GoOYUzfuy+ZGxc988AOsKxs2miFtQbkspCyW7AypYeeZX+SSlhGQj9f6M2TLKJBu+jAgMBAAGjEjAQMA4G
        A1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAEu6tRns1iW3c+qRCEpBfOyify3UMHPH1nkn55pZlWuYh
        Vi6a+/fyMie+URfrA2V6GdgZKNBCt7j0uZ5sAzJSjZEgSu0ts98CUxMoR4IuE7wCAKLPfosFJBMF8IFsg6igbGEK
        4F0VcIf3K8KpdS2tyzluetgP1MTQze4oJs3VHqxrSEso/2ykg2k2sYGazEhPDx+Z3dWukLixl9MPdf6fajEu/2Pd
        zQPQzDyT52M2N4vNlyEem7LGi4xqBcB636l9yhE8eTTHaSgaErV4LGjaxxgLyMt/svPL6fSFBAtwMMmmM07D9H+7
        j+zS5JUSA7EA2TDiz9UndyGH2hTUOmj3yw==
      </verificationCert>
    </source>
    <source>
      <downloadURL>http://213.184.41.178/internalconf</downloadURL>
      <verificationCert>
        MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwWhcN
        MzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9i1X8
        c3a7CSXoHXKXVPnUcqaplqRiMGa/z+gj35+/YxisA8KgAiHmuAr54AD6AUvZZrfbYqaC6g0fKB14b0xMTc2dtS3c
        i7TCDU1EPO1mxm08n2o0F/SZUOC/8kLFE4wIxCuaqdLzA6LgSI18tQJrXtnki/W4ixjgGPvVQ8s2jP9jMeXI+wWG
        DY79YKF4vHTkWp3KMv2VAgys3XVunIhTNtEaXU8Vnn6SEsyN1Xq3csTY4h/2iIHOpbFeZKLxBFe3piF68l1RwtPa
        1id7BS/IwSl4toa+ipm5w1EoqtcIV/1Mxj+4SF2u844AKsimoVQIiAeJmJWf+LDpe2pwQj7NAgMBAAGjEjAQMA4G
        A1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAvUGy2pkLhlpH3e70YTJ08AVp/FsM5pudyuOjLz7YfPXp
        keHGqjTKd//piQEcLqE6s5CEg5Wnbz7lHNAJeway6uQoAzJ67HEHK1v1Lwb1fnxQA83WszPidRp6+SRMenbTlDdF
        tguYB3s7c6wUf4a0YhZ+TPHsImw3+ZAHtfBaOhErUkLSoG7vUcIixN7TNhpKPaBYuwmBMgANDLLIkoeIIUlKmbjc
        VVPCpTUZ3aGetd3aVF/jl6pu1KyoRIRKnTwCRQhuqRMyh1NiCbbQC0DPRnFlb7DUlw6n4T4jjKcSZ4TcTl918fBF
        +oHvQI7KfhMtSVG73nCb/yC1i31dEfsc1A==
      </verificationCert>
    </source>
</ns3:configurationAnchor>
```

Joonis 13. Sisemise konfiguratsiooniankru XML faili sisu

Lisa 2 – Testilugu globaalse konfiguratsiooni kehtivuse aegumise kohta

ID	**TS01**
Kirjeldus	Globaalse konfiguratsiooni kehtivus kaob 10 minuti möödudes.
Eeltingimused	Paigaldatud ja seadistatud X-tee keskkond, kus andmevahetus toimib edukalt.
Teststsenaarium	1. Muuda keskserveris andmebaasi parameetri confExpireIntervalSeconds väärtuseks 600. 2. Tee keskserverile taaskäivitus muudatuse jõustumiseks ja uue globaalse konfiguratsiooni loomiseks. 3. Fikseeri globaalse konfiguratsiooni kehtivuse lõppemise aeg (expirationDate väärtus) turvaserveris asuvast /etc/xroad/globalconf/<instance>/shared-params.xml.metadata failist. 4. Oota paar minutit. 5. Veendu, et turvaserver on saanud uue globaalse konfiguratsiooni. Selleks vaata turvaserveris asuvat shared-params.xml.metadata faili. 6. Logi keskserveri haldusliidesesse ja vali “Management > Global Configuration > Signing Keys” ning vajuta nupule “LOGOUT”. 7. Tee turvaserverist päring teenusele. Päring peab õnnestuma. 8. Oota 10 minutit. 9. Logi sisse turvaserveri haldusliidesesse. Veendu, et punasel taustal kuvatakse veateadet globaalse konfiguratsiooni

	aegumise kohta. 10. Tee turvaserverist päring teenusele. Päring peab ebaõnnestuma. 11. Taastada testi läbiviimise eelne konfiguratsioon.
Oodatud tulemus	Turvaserverist tehtav päring peab ebaõnnestuma.
Erinõudmised keskkonnale	Testimise lihtsustamiseks ja ajakulu vähendamiseks võib globaalse konfiguratsiooni aegumise parameetri võrdsustada kuue tunni asemel kümne minutiga, mis on vaikimisi väärtus uue paigalduse korral.

Lisa 3 – Testilugu kehtivuskinnituse teenuse kehtivuse aegumise kohta

ID	TS02
Kirjeldus	Kehtivuskinnituse teenuse kehtivus kaob 10 minuti möödudes.
Eeltingimused	Paigaldatud ja seadistatud X-tee keskkond, kus andmevahetus toimib edukalt.
Teststsenaarium	1. Muuda keskserveris andmebaasi parameetri ocspFreshnessSeconds väärtuseks 600. 2. Muuda keskserveri haldusliideses OCSP Responderi URL valeks, selleks vali "Configuration > Certification Services", vajuta Approved Certification Service loetelus olevale teenusepakkujale ning nupule "Edit". Avanenud aknas vali vaheleht "OCSP Responders", vajuta "Edit", muuda URL ära nt "https://www.ria.ee" ja vajuta "OK". 3. Tee keskserverile taaskäivitus muudatuse jõustumiseks. 4. Fikseeri globaalse konfiguratsiooni kehtivuse lõppemise aeg (expirationDate väärtus) turvaserveris asuvast /etc/xroad/globalconf/<instance>/shared-params.xml.metadata failist. 5. Oota paar minutit. 6. Veendu, et turvaserver on saanud uue globaalse konfiguratsiooni. Selleks vaata turvaserveris asuvat shared-params.xml.metadata faili. 7. Tee turvaserverist päring teenusele. Päring peab õnnestuma. 8. Oota 10 minutit.

	9. Tee turvaserverist päring teenusele. Päring peab ebaõnnestuma. 10. Taastada testi läbimise eelne konfiguratsioon.
Oodatud tulemus	Turvaserverist tehtav päring peab ebaõnnestuma.
Erinõudmised keskkonnale	Testimise lihtsustamiseks ja ajakulu vähendamiseks võib kehtivuskinnituse teenuse värskendamise parameetri võrdsustada kaheksa tunni asemel kümne minutiga. Tegelikkuses on toodangukeskkonna parameetriks määratud 28800 sekundit ehk kaheksa tundi.

Lisa 4 – Testilugu ajatempliteenuse katkemise kohta

ID	**TS03**
Kirjeldus	Ajatembeldamist ei toimu.
Eeltingimused	Paigaldatud ja seadistatud X-tee keskkond, kus andmevahetus toimib edukalt.
Teststsenaarium	1. Muuda /etc/xroad/conf.d/local.ini konfiguratsioonifailis parameetri acceptable-timestamp-failure-period väärtuseks 600. 2. Tee turvaserveri käsurealt protsessidele xroad-proxy ja xroad-signer taaskäivitus. 3. Tee turvaserverist päring teenusele. Päring peab õnnestuma. 4. Logi turvaserveri haldusliidesesse ja vali “Configuration > System Parameters > Timestamping Services”, vajuta seadistatud ajatempliteenuse osutajale ning nupule “DELETE”. 5. Oota vastavalt turvaserveri /etc/xroad/conf.d/addons/message-log.ini konfiguratsioonifaili parameetris acceptable-timestamp-failure-period määratud väärtusele. 6. Ajatembeldamine lakkab töötamast. 7. Tee turvaserverist päring teenusele. Päring peab ebaõnnestuma ja saama veateate, et turvaserveri ajatempliteenus on seadistamata. 8. Taastada testi läbiviimise eelne konfiguratsioon.
Oodatud tulemus	Turvaserverist tehtav päring peab ebaõnnestuma.
Erinõudmised keskkonnale	Testimise lihtsustamiseks ja ajakulu vähendamiseks võib parameetri acceptable-timestamp-failure-period vaikimisi väärtuse 14400 asendada 600-ga.

Lisa 5 – Testimisel kasutatud teenus

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:ns1="http://producer.x-road.eu"
    xmlns:xrd="http://x-road.eu/xsd/xroad.xsd"
    xmlns:id="http://x-road.eu/xsd/identifiers">
  <SOAP-ENV:Header>
    <xrd:client id:objectType="SUBSYSTEM">
      <id:xRoadInstance>AA</id:xRoadInstance>
      <id:memberClass>COM</id:memberClass>
      <id:memberCode>CLIENT1</id:memberCode>
      <id:subsystemCode>sub</id:subsystemCode>
    </xrd:client>
    <xrd:service id:objectType="SERVICE">
      <id:xRoadInstance>AA</id:xRoadInstance>
      <id:memberClass>COM</id:memberClass>
      <id:memberCode>CLIENT1</id:memberCode>
      <id:subsystemCode>testservice</id:subsystemCode>
      <id:serviceCode>mock</id:serviceCode>
      <id:serviceVersion>v1</id:serviceVersion>
    </xrd:service>
    <xrd:id>8c09ff0e-9365-45f0-9eea-04a87f64e8ad</xrd:id>
    <xrd:userId>EE12345678901</xrd:userId>
    <xrd:issue>12345</xrd:issue>
    <xrd:protocolVersion>4.0</xrd:protocolVersion>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <ns1:mock>
      <desiredResponse>bodyData_10KB</desiredResponse>
    </ns1:mock>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Joonis 14. Testteenuse mock SOAP päring