X-tee haldus ja töökindlus

Kas X-tee töökindluse tagamiseks rakendatakse vajalikke meetmeid?

Riigikontrolli aruanne Riigikogule
Tallinn, 23. veebruar 2021

X-tee haldus ja töökindlus

Kas X-tee töökindluse tagamiseks rakendatakse vajalikke meetmeid?

Kokkuvõte auditeerimise tulemustest

Riigi ülesannete täitmine, sealhulgas info vahetamine asutuste vahel või teenuste osutamine, on paratamatult muutunud suurel määral digitaalseks. See tähendab, et vajadus vahetada suurt hulka elektroonseid andmeid on iga aastaga üha suurem.

2000. aastate algul loodud infosüsteemide turvalise andmevahetuskihi X-tee kasutajate arv ja selle vahendusel sooritatavate päringute arv kasvab endiselt. Samal ajal on alustatud X-tee tööks vajaliku tarkvara ja tööpõhimõtete eksporti välisriikidesse, samuti tarkvara üheskoos arendamist Soome kolleegidega.

Mida me auditeerisime?

Riigikontroll auditeeris, kas X-tee keskuse haldamise eest vastutav Riigi Infosüsteemi Amet on silmas pidanud olulisemaid X-teed ohustavaid riske ja nende maandamiseks abinõud tarvitusele võtnud. Samuti vaadati, kas amet koos X-tee kasutajatega on kinni pidanud nõuetest, mis on riik X-tee haldamiseks kehtestanud, et turvaline andmevahetus toimiks jätkusuutlikult.

Miks on see maksumaksjatele oluline?

2020. aasta 1. detsembri seisuga oli X-teega liitunud 200 avaliku sektori asutust (sh kohaliku omavalitsuse asutused) ja 525 erasektori asutust ning kaudselt kasutas X-tee teenuseid ligikaudu 52 000 ettevõtet ja asutust. Turvalise andmevahetuskihiga oli liidestatud 1263 infosüsteemi. X-teed kasutavad asutused ehk X-tee liikmed olid paigaldanud 164 turvaserverit. Teenuste arv, mida sai kasutada X-tee vahendusel, oli 2741.

Auditi ajal sooritati X-tee vahendusel ühes kalendrikuus kokku ligi 133 miljonit päringut. X-tee kaudu tehtavad päringud võimaldavad märkimisväärselt hoida kokku elanike, ettevõtjate ja ametnike aega ning lihtsustada osapoolte vahel asjaajamist. Arvestades X-tee kaudu tehtavate päringute hulka, muutuks X-tee mittetoimimisel enamiku avalike teenuste osutamine võimatuks või vähemalt oleks olulisel määral raskendatud. X-tee kaudu toimuva andmevahetuse asendamine mitteelektroonilise andmevahetusega oleks praktiliselt võimatu või vähemalt väga kulukas.

Mida me auditi tulemusel leidsime ja järeldasime?

Auditi tulemusena selgus, et Riigi Infosüsteemi Amet ja auditis vaadeldud X-tee liikmed on rakendanud üldjuhul X-tee töökindluse tagamiseks vajalikke meetmeid. Samas tuvastas Riigikontroll X-teega liidestatud andmekogude tervikluse ja konfidentsiaalsuse puhul maandamata riske, mis tulenevad sellest, et mitmetel juhtudel ei ole X-tee liikmed sõlminud andmeteenuse kasutamise kokkuleppeid ega kontrollinud eraõiguslike asutuste infoturbe taset nende liitumisel X-teega.

Riigikontrolli olulisemad tähelepanekud turvalise andmevahetus-kanali X-tee kohta on järgmised:

- **Riigi Infosüsteemi Amet on selgitanud välja X-tee töökindlust ohustavad olulisemad riskid ja hinnanud neid. Riskide maandamiseks on välja töötatud meetmed, millest mitmeid ka rakendatakse.** X-tee taristu kesksed teenused on olnud seni võrdlemisi töökindlad: X-tee teenustes on viimase kolme aasta jooksul olnud X-tee kesksetest komponentidest tingituna üks olulise mõjuga katkestus.

- **Mitmed Vabariigi Valitsuse määrusega „Infosüsteemide andmevahetuskiht“ X-teele kehtestatud nõuetest on jäänud üldsõnaliseks ning võimaldavad X-tee liikmetel neid rakendamisel erinevalt tõlgendada.** Näiteks peavad X-teed kasutusele võtvad asutused rakendama infoturbega seotud riskide maandamiseks vajalikke meetmeid, kuid selgitamata on jäetud, milliseid turvameetmeid ja millisel tasemel tuleks rakendada.

- **Auditi käigus leidis Riigikontroll mõned riskid, mis võivad ohustada X-teega liidestatud andmekogude terviklust ja konfidentsiaalsust ning luua võimalused volitamata ligipääsuks andmetele või volitamata muudatuste tegemiseks. Nende riskide tekkimise kaks olulisemat põhjust on järgmised:**

  - Andmeteenuse kasutamise kokkulepete sõlmimisel puudub ühtne praktika, mõned asutused ei sõlmi neid üldse. Andmeteenuse kasutamise kokkulepete täitmist kontrollivad vaid üksikud X-tee liikmed. Need asutused uurivad andmete kasutamise põhjuseid päringuid teinud X-tee liikmetelt eelkõige andmekaitse seisukohast, s.t hinnatakse, kas X-tee kaudu kättesaadavaks tehtud andmeid (iseäranis isikuandmeid) töödeldakse ainult seaduses ettenähtud eesmärkidel.

  - Ükski auditeeritud riigiasutustest ei veendu andmeteenuse kasutajaga kokkuleppe sõlmimise eel, kas eraõiguslikust juriidilisest isikust ettevõtja rakendab turvalisusega seotud riskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. Eraõiguslikud X-tee liikmed kinnitavad küll andmeteenuse kasutamise lepingut sõlmides, et nad rakendavad vajalikke meetmeid, kuid kontrolli selle üle andmeteenuse osutajad ei tee.

- **Ehkki eraldi talitluspidevuse plaani X-tee kohta Riigi Infosüsteemi Amet koostanud ei ole, on turvalise andmevahetuse püsivaks toimimiseks kasutusele võetud meetmeid ning muudes dokumentides sätestatud nõudeid talitluspidevuse tagamiseks.** Puudusteks võib pidada taastetestide tegemise ebaregulaarsust ja nende dokumenteerimata jätmist. Samuti seda, et X-teega seotud infovarade elutähtsust ja tundlikkust ei ole eraldi hinnatud.

Mida me auditi tulemusel soovitasime?

Riigikontroll soovitused Riigi Infosüsteemi Ameti peadirektorile:

- Algatada X-tee toimimist korraldava määruse „Infosüsteemide andmevahetuskiht“ muudatus, mis teeks X-tee liikmetele kehtestatud nõuded täpsemaks ja üheselt arusaadavamaks, nii et andmeteenuse

osutajatel oleks võimalik neid nõudeid rakendada ja Riigi Infosüsteemi Ametil nende rakendamist kontrollida. Samuti tuleks töötada välja vajalikud juhendid määrusest tulenevate nõuete rakendamiseks ja korraldada X-tee liikmetele vastavad koolitused.

- Hinnata andmeteenuse kasutamise lepingute sõlmimata jätmisest tulenevaid riske andmekogude turvalisusele ja võtta kasutusele neid riske maandavad tegevused. Samuti kaaluda andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsuse lisamist, et muuta X-tee portaali andmeteenuste avamine ja kasutamine senisest vähem bürokraatlikuks.

- Töötada välja eraõiguslikust juriidilisest isikust ettevõtjast X-tee liikmete kontrolli süsteem, et oleks tagatud määruses „Infosüsteemide andmevahetuskiht“ nõutavate terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendamise kontroll ja järelevalve.

- Korraldada regulaarselt X-tee kesksete komponentide taastetestimisi ning dokumenteerida need. Puuduste esinemise korral võtta ette vajalikud parendustegevused.

Riigi Infosüsteemi Ameti peadirektori vastus: Amet tutvus Riigikontrolli aruandega ja esitas oma seisukohad soovituste suhtes.

Amet on seisukohal, et tulenevalt vajadusest tagada X-tee tarkvara jätkusuutlik arendamine, haldamine ja kasutamine ei ole otstarbekas Vabariigi Valitsuse määruse tasemel kõiki üksikasju reguleerida. Ameti hinnangul tuleks X-tee liikmetele kehtivad täpsed nõuded kindlaks määrata pigem liitumislepinguga. Amet nõustus aga Riigikontrolli järeldusega, et juhendmaterjali piisavust ja arusaadavust võib olla vaja analüüsida ning juhendeid tuleb vajaduse korral täiendada ja hoida ajakohasena.

Kui X-tee tarkvara ja Riigi Infosüsteemi Amet loovad eeldused andmeteenuste loomiseks, osutamiseks ja kasutamiseks, saab andmeteenuste praktiline kasutus tugineda üksnes X-tee liikmete omavahelisele kokkuleppele. Ametil on plaanis tulevikus välja arendada X-tee iseteeninduskeskkonnas andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsus.

Riigi Infosüsteemi Amet peab oluliseks kontrollida, et X-teed kasutatakse määruses ja lepingus esitatud nõuete kohaselt, olenemata X-tee liikme õiguslikust vormist. Amet tunnistas, et tõhusa kontrolli tegemiseks eraõiguslike juriidiliste isikute üle on vaja hinnata olemasolevate õiguste ja sekkumismeetmete piisavust ning välja töötada toimiv kontrollisüsteem.

Riigi Infosüsteemi Amet hakkab korraldama regulaarseid taasteteste koos nende dokumenteerimisega ning viib ellu vajalikud parendustegevused.

Sisukord

Valdkonna ülevaade **5**
X-tee toimimise põhimõtted 5
X-tee haldamine 7
X-tee liikmed ja teised seotud osapooled 8
X-tee töökindlus ja selle tagamine Riigi Infosüsteemi Ametis **9**
X-tee olulisus asutustes teenuste osutamisel ja kasutamisel on erinev 9
X-tee haldamisel kasutatakse Riigi Infosüsteemi Ametis parimat praktikat 11
Riskide juhtimine ja regulaarne läbivaatus on süsteemne 13
Talitluspidevuse tagamiseks on X-tee kesksed komponendid dubleeritud ja sõltuvust nendest vähendatud 14
X-tee keskses taristus on toimunud viimase kolme aasta jooksul üks olulise mõjuga intsident 15
X-tee töökindluse tagamine liikmete poolt **16**
Mitmed X-tee liikmetele määrusega kehtestatud nõuded on üldsõnalised ning nende täitmist ei kontrollita 16
X-teega liitumine ning andmeteenuste avamine ja kasutamine vajab korrastamist 17
Infosüsteemide toimivuse tagamiseks kasutatakse erinevaid standardeid ja rakendatakse erinevat praktikat 19
X-tee liikmete infoturbega seotud nõuded ja nende auditeerimine on eraõiguslike asutuste puhul puudulik 19
X-tee päringutega seotud intsidente lahendavad enamasti andmeid vahetavad X-tee liikmed 20
Riigikontrolli soovitused ja auditeeritute vastused **28**
Auditi iseloomustus **32**
Auditi eesmärk 32
Hinnangu andmise kriteeriumid 32
Riigikontrolli varasemaid auditeid infotehnoloogia valdkonnas **35**
Lisa A. Auditi käigus korraldatud küsitluse küsimused **36**

Valdkonna ülevaade

Riigi infosüsteemi andmevahetuskiht X-tee – tehniline lahendus, mis võimaldab korraldada andmevahetust riigi infosüsteemide vahel ning hõlbustab igaühe juurdepääsu riigi andmekogude andmetele.

1. Riigi infosüsteemi andmevahetuskihti X-tee hakati juurutama 17. detsembril 2001. aastal. Selle loomist koordineeris sel ajal Teede- ja Sideministeeriumi riigi infosüsteemide osakond. X-tee loomise visioonis oli luua juurdepääs andmekogudele 7 päeva nädalas ja 24 tundi ööpäevas.[1]

2. Tolleaegse Teede- ja Sideministeeriumi asekantsleri sõnul sooviti toona tõsta kodanik jooksupoisi rollist kõrgemale ning kinnistada ka riigi jaoks arusaam, et klient/kodanik on kuningas. Selleks käivitati X-tee ehk risttee nimeline arendusprojekt. See pidi looma võimaluse kodanikule, ettevõtjale ja ametnikule kasutada oma volituste piires eri ametkondades ja eri andmekogudes sisalduvaid andmeid ning pakkuda elektroonselt teenuseid, mis ei ole piiratud ainult ühe ametkonna infosüsteemiga.[2]

3. Esimesed omavahel ühendatud andmekogud olid äriregister ja kinnistusraamat, hiljem lisandusid rahvastiku-, hoone- ja ehitusregister. Plaani järgi pidid Eesti inimesed saama võimaluse interneti kaudu vaadata ja parandada oma andmeid rahvastikuregistris ning ametnikel pidi tekkima võimalus oma tööd kiirendada ja täpsemaks muuta, esitades päringuid viie registri andmebaasidesse.

4. X-tee väljatöötamise käigus tuli tagada, et infosüsteemid, mis olid loodud eri ajal ning asusid eri tehnoloogilistel platvormidel, suhtleksid üksteisega ühises keeles, s.t oleks standardiseeritud ja põhineks koosvõimel. Riigi infosüsteemi loomiseks otsustati valida hajus arhitektuur, s.t lahendus, kus andmed jäävad asutuste endi andmekogudesse ja andmekogudest päringute tegemiseks kasutatakse infosüsteemide andmevahetuskihti X-teed.[3]

X-tee toimimise põhimõtted

X-tee liige – turvalise andmevahetuskihiga liidestunud asutus, kes jagab välja oma andmeid, vahendab või kasutab teiste andmeid.

5. X-tee abil saavad sellega liitunud osapooled (edaspidi X-tee liikmed) omavahel turvaliselt suhelda interneti kaudu. Tänu X-tee ülesehitusele ei ole keskset punkti, mille töö lakkamine peataks X-teel kohe andmevahetuse. Mitmeid tunde kestev X-tee kesksete komponentide mittefunktsioneerimine avaldaks mõju X-tee andmevahetustele. Andmeid vahetavad osapooled omavahel otse, suhtlemine toimub turvaserverite kaudu (vt joonis 1).

X-tee sõnumiprotokoll – X-tee baasprotokollistiku osa, mis võimaldab X-tee liikmetel sõnumeid töödelda.
Allikas: https://www.riigiteataja.ee/akt/106082019017

6. X-teel on sõnumiprotokoll kõigile osapooltele sama ning see võimaldab X-tee teenuseid osutada ning kasutada sarnastel tingimustel ja sarnase tehnoloogiaga. X-tee liikmed ei pea iga osapoolega suhtlemiseks oma infosüsteemi lisama uut tehnoloogilist lahendust ega tuge uutele protokollidele. Samuti olid X-tee loomisel sõnumiprotokolli kasutamise kulud võrreldes muude lahendustega madalad, ilma et oleks kasvanud oht andmete turvalisusele.[4]

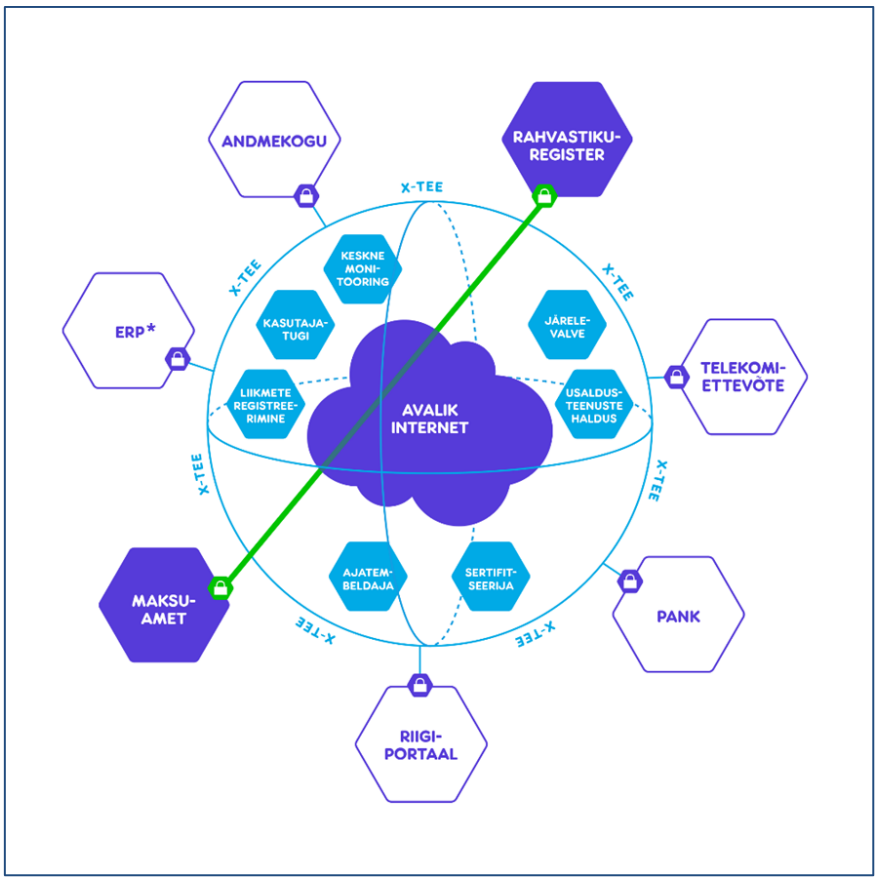
[1] https://www.ria.ee/et/uudised/tallinnas-tahistatakse-x-tee-15-sunnipaeva.html

[2] https://arvamus.postimees.ee/1871481/e-riik-on-joudmas-ristteele

[3] Kasutatud RIA X-tee ja riigi infosüsteemi haldussüsteemi RIHA abikeskuse materjale (https://abi.ria.ee/xtee/et).

[4] Kasutatud Riigi Infosüsteemi Ameti juhendeid ehk RIA X-tee ja riigi infosüsteemi haldussüsteemi RIHA abikeskuse materjale (https://abi.ria.ee/xtee/et).

Joonis 1. X-tee üldine arhitektuur



* ERP – *Enterprise Resource Planning* ehk ettevõtte ressursside planeerimise tarkvara, nt tööjõu-, seadme-, hoone-, materjali- ja rahaarvestus.

Allikas: Riigi Infosüsteemi Amet

7. Asutusel tuleb X-teega liitumiseks soetada ja kasutusele võtta turvaserver, arendada ja registreerida andmeteenused ning sõlmida andmeteenuse kasutamise kokkulepped.

8. X-tee haldamisel on Riigi Infosüsteemi Amet (RIA) endale eesmärgiks võtnud järgida järgmisi tööpõhimõtteid[5]:

- **Sõltumatus platvormist ja arhitektuurist**: X-tee peab võimaldama mis tahes tarkvaraplatvormil oleval infosüsteemil suhelda mis tahes tarkvaraplatvormil oleva andmeteenuse osutaja infosüsteemiga.
- **Multilateraalsus**: X-tee liikmel peab olema võimalus taotleda juurdepääsu kõigile X-tee kaudu osutatavatele andmeteenustele, sõltumata tehnoloogiast või äriloogikast.
- **Turvalisus**: X-tee kaudu andmete vahetamisel ei tohi muutuda andmete käideldavus, terviklus ega konfidentsiaalsus. X-tee säilitab liikmete andmevahetuses andmete omandi ja vastutuse.

[5] https://www.ria.ee/et/riigi-infosusteem/andmevahetuskiht-x-tee.html

- **Avatus ja standardiseeritus**: X-tee haldamisel ja arendamisel tuleb kasutada võimaluse korral rahvusvahelisi standardeid ja protokolle.

9. X-tee on üles ehitatud põhimõttel, et X-teel vahetatavatele andmetele võiksid ligi pääseda vaid volitatud isikud asutustest või organisatsioonidest, kellega on sõlmitud andmeteenuse kasutamise kokkulepped (**konfidentsiaalsuse põhimõte**). X-tee liige määrab ise, milliseid andmeteenuseid ta soovib pakkuda ja kellele teenuste kasutamise pääsuõigusi anda (**autonoomsuse põhimõte**).

10. Iga ühendatud asutus on tuvastatav krüptograafilise e-templi sertifikaadi abil. Andmevaldaja võib klientidelt nõuda, et iga päringut tegev isik end tuvastaks (näiteks ID-kaardiga). X-tee tagab sellega liikmete **autentsuse** üksteise suhtes.

11. Samuti peab X-tee tagama, et andmeteenuste abil vahetatavad andmed jõuaksid asjakohaste liikmeteni leketeta ja terviklikult, s.t muutmata ja tõendusväärtuslikult. Andmete moondumine liikmete vahel on tuvastatav, s.t tagatud on **tervikluse põhimõte**. Igast tegevusest X-teel jääb jälg. Samuti on võimalik tõendada, kas ja millal andmevahetus toimus.

12. Andmevahetus X-teel toimub interneti kaudu. Andmevahetuse muudab turvaliseks krüpteeritud sidekanal. Krüpteeritud side luuakse ajutiselt, s.t vaid hetkedeks, kui seda tegelikult vaja läheb. Andmevahetus X-teel toimub üksnes eelnevalt määratud andmeteenuste piires. Andmete vorming on andmeteenusega üheselt määratud. Vabu päringuid teha ei saa, kõik päringumallid on eelnevalt ette valmistatud.[3]

X-tee haldamine

13. X-teel on kolme tüüpi osapooli: X-tee keskus, X-tee liikmed ja usaldusteenuste osutajad. X-tee keskuse ülesandeid täidab RIA, kes vastutab ka X-tee haldamise ja arendamise eest.[6] Auditi kontekstis on RIA kui X-tee keskse juhi olulisemate ülesannete hulgas

- hallata X-tee keskkondasid;
- korraldada liikmelisust;
- tagada X-tee kasutamise võimalus;
- seirata X-tee kasutamist ja käsitleda turvaintsidente;
- koguda statistikat, mida liikmete turvaserverid sinna saadavad (nt millised liikmed omavahel seotud on);
- nõustada X-tee liikmeid X-teega seotud küsimustes.

[6] Vabariigi Valitsuse 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ § 4.

X-Road – avatud lähtekoodiga tarkvara ja ökosüsteemilahendus, mis tagab organisatsioonide ühtse ja turvalise andmevahetuse. Tarkvara on juba kasutusel rahvusvaheliselt, sest Eesti X-tee kõrval kasutavad seda ka Soome, Fääri saared, Island, Taani, Jaapan jt.

14. Alates 2018. aastast arendab MTÜ Nordic Institute for Interoperability Solutions (edaspidi NIIS) tarkvara X-Road, mille komponente kasutatakse ka X-teel. RIA enam ise X-tee tarkvara arendusi ei telli, vaid osaleb arendusprotsessis pigem NIISile uute arendussoovide sisendi andjana.

15. NIIS on Eesti-Soome ühisettevõtmine, mille kõrgem juhtorgan on üldkoosolek, kus Soome poolt esindab nende Rahandusministeerium ning Eestit Majandus- ja Kommunikatsiooniministeerium. NIISi nõuandva töörühma üks neljast liikmest on RIA andmevahetuse osakonna juhataja.

16. RIA esindajad annavad oma sisendi NIISile X-teel avastatud vigade, turvaintsidentide ja uute arendussoovide kohta. Vajaduse korral osutab NIIS RIA-le teise taseme tuge keerulisemate X-tee juhtumite lahendamisel. NIISi üheks ülesandeks on ka arendatava tarkvara turvalisuse hindamine ja selleks korraldatakse läbistustestimisi.

X-tee liikmed ja teised seotud osapooled

17. X-tee liikmed on andmeteenuse osutajad ja -kasutajad. Nad jagavad teistele oma andmeid välja või vastupidi, kasutavad neid oma tegevuses. Samuti on nad kohustatud rakendama turvalisusega seotud riskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid ning korraldama rakendatavate meetmete sõltumatu auditeerimise vähemalt iga nelja aasta järel.

18. Enamik X-tee liikmetest on passiivsed kasutajad, s.t nemad küsivad andmebaasidest andmeid, kuid omaenda andmebaasides olevaid andmeid teistele X-tee liikmetele ei jaga või ise andmebaase ei pea.

Teadmiseks, et

RIAs on X-teega seotud kolm osakonda, kelle peamised X-teega seonduvad ülesanded on järgmised:

- andmevahetuse osakond tegeleb infosüsteemide andmevahetuskihi arendamise, haldamise ja majutamise korraldamisega ning on X-tee keskuse rollis;
- intsidentide käsitlemise osakond tegeleb X-teega seotud turvaintsidentide analüüsimisega;
- standardi- ja järelevalveosakond tegeleb riskianalüüside hindamisega ja järelevalvega.

19. X-teel on võimalik ka andmete kombineeritud kasutus ehk andmeküsimine ja -jagamine vaheldumisi või suisa samal ajal. Lisaks on võimalik teha päringuid mitmesse infosüsteemi korraga, näiteks kodaniku isikukoodi järgi, ning sellist andmevahetust nimetatakse komplekspäringuks.

20. X-tee liikmeks võivad olla ka andmeteenuse vahendajad. Andmeteenuse vahendaja on X-tee liige, kes võimaldab enda organisatsiooni välisele füüsilisele või juriidilisele isikule juurdepääsu andmeteenusele oma infosüsteemi vahendusel. Andmeteenuse vahendus võib olla vajalik nendele asutustele, kelle jaoks on turvaserveri omamine ja haldamine liiga kulukas või kellel ei ole selleks vajalikku IT-kompetentsust.

21. Samuti on olulised X-tee osapooled **usaldusteenuste osutajad** (praegu X-teel SK ID Solutions AS). Andmevahetuse tervikluse ning X-teel vahetatud sõnumi ja X-tee liikme seose tuvastamise tagamiseks on X-tee liige kohustatud turvaserveris kasutama järgmisi usaldusteenuseid:

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

22. Lisaks toimimisele X-tee keskse juhina (vt p-d 13–16) on RIA-l ka muid rolle. Üks nendest on järelevalve roll, näiteks saab RIA rikkumise ja vale- või puudulike andmete esitamise avastamisel X-tee liikmelisuse lõpetada või piirata liikmelisusest tulenevaid õigusi või anda tähtaeg puuduse kõrvaldamiseks.

23. Auditis vaadeldi RIA-poolset X-tee keskset töökorraldust ja X-tee arendamise reegleid ning X-tee liikmete töökorraldust järgmistes asutustes: Haridus- ja Teadusministeerium, Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium (MKM), Kultuuriministeerium, Keskkonnaministeerium, Maaeluministeerium, Välisministeerium, Maksu- ja Tolliamet, Maanteeamet, Tervise ja Heaolu Infosüsteemide Keskus, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Rahandusministeeriumi Infotehnoloogiakeskus, Registrite ja Infosüsteemide Keskus. Lisaks sellele vaadeldi kolme kohalikku omavalitsust – Pärnu, Tartu ja Tallinna linnavalitsust – ning kolme riigile kuuluvat ühingut – Elering ASi, OÜd TS Laevad ning Riigimetsa Majandamise Keskust.

X-tee töökindlus ja selle tagamine Riigi Infosüsteemi Ametis

24. RIA on määruse[7] järgi kohustatud tagama X-tee toimimise mitmete erinevate tegevuste, näiteks X-tee tarkvara uuendamise, selle liikmeteni toimetamise, intsidentide lahendamise, X-tee taristu arendusprojektide elluviimise, X-tee arhitektuurse tervikluse tagamise jm kaudu.

25. Auditi käigus vaadati, kas ja kuidas on RIA selgitanud välja X-tee töökindlust ohustavad riskid. Samuti analüüsiti, kas neid riske on hinnatud, kas on välja töötanud riskide maandamiseks meetmed ja kas neid meetmeid rakendatakse.

Töökindlus – IT-teenuse või muu konfiguratsioonielemendi võime tõrkele vastu seista või pärast tõrget õigel ajal taastuda.

Allikas: infotehnoloogia haldamise tavade ja protsesside standardite kogu (ITIL) sõnastik

X-tee olulisus asutustes teenuste osutamisel ja kasutamisel on erinev

26. Enamasti soovivad kõik X-tee kasutusele võtnud asutused ja ettevõtted turvalise andmevahetuse abil toetada oma olulisemaid põhitegevuse protsesse ja avalike teenuste osutamist. X-tee teenuste olulisus võib iga liikme jaoks olla tema põhitegevusest või konkreetse protsessi kriitilisusest lähtuvalt erinev.

27. Paljudel X-tee liikmetel ei ole võimalik avalikke teenuseid osutada või nende osutamine on oluliselt häiritud, kui X-tee kaudu andmevahetus ei toimi. Arvestades mõnede asutuste poolt X-tee kaudu tehtavate päringute hulka ja päringute keerukust, ei ole sageli võimalik kasutada ka alternatiivseid ITst mittesõltuvaid lahendusi. Suhteliselt vähestel juhtudel on võimalik kasutada teistsuguseid, s.t X-teele mittetuginevaid IT-lahendusi, näiteks tehes päringuid otse veebiliidese kaudu mõnest andmekogust.

[7] Vabariigi Valitsuse 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ § 4 lg 1.

28. Viis kõige enam teenuseid osutavat X-tee süsteemi teevad umbes 44% kõigist X-tee päringutest (vt tabel 1), mida 2020. aasta juulikuus oli kokku 133 miljonit.

Tabel 1. Enim X-tee päringuid tegevad infosüsteemid (juulis 2020)

Infosüsteem	Päringute arv	Osakaal kõigist päringutest, %
Töötamise registri (TÖR) X-tee alamsüsteem	17 266 818	13,0
Retseptikeskuse X-tee alamsüsteem	12 188 030	9,1
Rahvastikuregistri X-tee alamsüsteem	10 398 705	7,8
Piirikontrolli andmekogu PIKO X-tee alamsüsteem	10 015 764	7,5
Tervise infosüsteemi X-tee alamsüsteem	8 666 816	6,5

Allikas: X-tee faktileht (https://www.x-tee.ee/factsheets/EE/)

29. Juhul, kui X-tee mittefunktsioneerimine põhjustaks olukorra, kus teenused lakkaksid kas täielikult või osaliselt toimimast, ei funktsioneeriks auditis vaadeldud asutuste teenustest maksuvõlgade kontroll ja mitmed tervise infosüsteemi teenused. Samuti ei saaks osa andmekogusid (näiteks rahvastikuregister ja isikut tõendavate dokumentide andmekogu) oma tegevuseks vajalikke andmeid.

30. ASil TS Laevad oleks teenuste katkemisest tekkiv kahju pigem teoreetiline. X-tee mittetoimimise korral ei saa nad registritest kontrollida sõidusoodustusõigust ja seetõttu peavad piletite müümisel lähtuma eelmise müügi andmetest.

31. Auditi käigus vaatas Riigikontroll, kas X-tee mittetoimimise puhuks on X-tee liikmel olemas alternatiivne IT-lahendus või mõni muu (mitte IT-põhine) lahendus teenuse osutamiseks. See tähendab, et kui X-tee kaudu katkeb andmevahetus teiste andmekogude või infosüsteemidega, siis asutusel on varuplaan vajalike andmete saamiseks või teenuse osutamiseks ilma nende andmeteta.

32. Alternatiivsed IT-lahendused olid olemas vähestes auditeeritud asutustes. Mõnel asutusel töötaksid X-tee häirete korral teenused eelsalvestatud info põhjal, mõni saaks teatud osas korraldada infovahetust e-kirja teel. Vähesed tõid välja, et neil on partneritega olemas selged kokkulepped, mida saab näiteks kriisiolukorras kasutusele võtta.

33. Enim X-tee päringuid tegevatest alamsüsteemidest (vt tabel 1) on digiretsepti teenuse esimeseks alternatiiviks ühenduse võtmine digiretsepti operaatoriga. Seesuguse tegevuse võimekus ei ole aga kuigi suur (iga päev ostetakse välja ligi 35 000 retsepti ravimeid), kuna (telefoni-) operaatorite arv on piiratud. Kui retseptikeskuse teenused ei ole kättesaadavad 24 tunni jooksul, on teiseks alternatiiviks paberretseptid, mida aga ei pruugi tervishoiuteenuse osutajatel vajalikus mahus olemas olla ja mis tuleb sel juhul kulleritega laiali saata.

34. Ravikindlustuse kontrollimiseks (umbes 1 miljon päringut kuus) alternatiivi ei ole. Kui ravikindlustuse andmekogu ei ole kättesaadav, siis osutatakse tervishoiuteenus tasulisena või kontrollitakse kindlustuse

olemasolu hiljem ning selle puudumise korral esitab teenuseosutaja inimesele või Eesti Haigekassa teenuseosutajale hiljem nõude.

35. Audit näitas, et paljud auditis vaadeldud asutused X-tee pikemaaegseteks katkestusteks valmistunud ei ole. X-tee kesksed teenused on seni olnud küllaltki töökindlad ja keskseid komponente puudutavaid intsidente on juhtunud harva.

36. Mitme auditeeritu ja RIA andmevahetuse osakonna sõnul on X-tee mittetoimimisel võimalik luua andmekogude vahel ka alternatiivne ühendus, näiteks VPN (*virtual private network*) ühenduse abil. Samas võtab see sõltuvalt asutusest, andmekogust ja päringust üldjuhul aega mitmeid tunde või päevi ning see võiks olla eelkõige ajutine alternatiivne lahendus vaid mõne andmekogu vahel andmete edastamiseks.

X-tee haldamisel kasutatakse Riigi Infosüsteemi Ametis parimat praktikat

37. X-tee haldamisel ei ole RIA võtnud eesmärgiks ühegi üldtunnustatud IT juhtimise standardi rakendamist. Samas on protseduurid asutusesisestes dokumentides kokku lepitud.

ITIL – infotehnoloogia haldamise tavade ja protsesside standardite kogu (*Information Technology Infrastructure Library*), mis on üle maailma tunnustatud infotehnoloogia haldamise protsesside raamistik ning mida on kasutatud ja arendatud juba 20 aastat.

38. Auditit alustades eeldati, et RIA kasutab X-tee haldamiseks IT juhtimise parimat praktikat. Aluseks võeti infotehnoloogia haldamise tavade ja protsesside standardite kogu ITIL.

39. Riigikontroll valis kõigist ITILi protsessidest ja teemadest need, mis X-tee haldamisel ja töökindluse tagamisel on olulisemad. Need on

- käideldavuse juhtimine;
- muudatuste juhtimine;
- infoturbe juhtimine ja
- intsidentide haldus.

40. Auditi käigus leidis Riigikontroll, et X-tee halduseks kasutatavad protsessid on dokumenteeritud ja neist on osapooli teavitatud, neid seiratakse ja optimeeritakse RIAs, lähtudes parimast praktikast.

Käideldavuse juhtimine

41. Käideldavuse tagamisel eeldas Riigikontroll, et X-tee käideldavuse juhtimiseks on paika pandud käideldavuse nõuded ja käideldavuse taset seiratakse.[8]

Teenustaseme lepe ehk SLA (*service level agreement*) – teenuseid ja teenusesihte piiritlev dokumenteeritud kokkulepe teenuseandja ja kliendi vahel. SLAs võidakse sätestada nõuded pakutavate teenuste ja nende muudatuste kvaliteedile, teenusega seotud nõuded teenusepakkujale (nt lubatav planeerimata katkestuste kestus mingil ajaperioodil) ning muud poolte õigused ja kohustused.

42. Selgus, et käideldavuse nõuded on fikseeritud RIA ja MKMi sõlmitud teenustaseme leppes. RIA jälgib X-teel toimuvat tegevust, sh käideldavuse näitajaid. Taristu komponentide seireks kasutatakse tarkvara, mis jälgib X-tee keskse taristu ja selle komponentide toimimist. Tõrgete korral saadab tarkvara X-tee administraatoritele teate e-postiga või sõnumiga, et oleks võimalik kiiresti intsidentidele reageerida.

43. X-tee andmeteenuse osutamisel ja kasutamisel peavad osapooled leppima omavahel kokku käideldavuse teenustaseme tingimused, lähtudes teenuste kriitilisusest ja olulisusest. RIA asutustevahelist

[8] ITIL Foundation, 5.2.1. Availability Management.

andmeteenuse osutamise ja kasutamise käideldavust ei seira ega kontrolli vastavate kokkulepete täitmist (vt ka p-d 79–81).

Muudatuste juhtimine

44. Muudatuste juhtimise korraldamisel on kõige olulisem kirja panna muudatuste juhtimise põhimõtted, sh rollid ja vastutus. Samuti on vaja tagada, et muudatused oleks selgelt fikseeritud ja kohustuslikud kõigile olulisetele huvirühmadele. Olulistest X-tee muudatustest (nt suured tarkvarauuendused) tuleb kõigile X-tee liikmetele teada anda.[9]

45. Audit näitas, et RIA-l on kasutusel üldine muudatuste haldamise protsess. Selles on olulises osas paika pandud muudatuste juhtimise rollid ja vastutus. Olulisi muudatusi tehakse plaaniliste muudatuste skeemi järgi, millest annab kõige olulisemale osapoolele ehk X-tee liikmetele teada RIA andmevahetuse osakond.

Infoturbe juhtimine

46. Infoturbe juhtimise korraldamisel eeldati, et RIA-l on olemas üldine infoturbepoliitika, juurutatud intsidendihalduse protseduurid, toimiv riskide hindamise süsteem ja kord, kasutusele võetud sisekontrollide hindamise ja auditeerimise protseduurid. Samuti pääsuõiguste jagamise protseduurid, läbistustestimise põhimõtted ning protseduurid infoturbe muudatuste haldamiseks (nt tulemüüri konfiguratsiooni muutmiseks).[10]

ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem.

47. RIA on mitmete andmekogude vastutava või volitatud töötlejana kohustatud rakendama riigi ühtset infoturbe raamistikku ISKEt. Selle rakendamise kontrollimiseks peavad asutused tellima ISKE-auditeid. Viimati auditeeriti ISKE rakendamist 2016. aastal ja 2018. aastal.

48. 2016. aasta auditis anti hinnang vaid infosüsteemide andmevahetuskihile X-tee. 2018. aasta auditis vaadati aga X-teed juba koos teiste RIA andmekogudega (nt RIHA, eesti.ee portaal, TARA (riigi autentimisteenus), AAR (pääsuõiguste haldussüsteem) jt). Auditite tulemusel X-tee kohta olulisi märkusi ei olnud, välja oli toodud vaid madala riskitasemega märkus selle kohta, et turvaklassi analüüsi dokumente oli viimati muudetud liiga pikka aega tagasi (14.12.2016).

49. Ka Riigikontroll ei leidnud oma auditi käigus kontrollitud infoturbe juhtimise aspektide puhul, s.t infoturbepoliitika, intsidendihalduse protseduuride, riskihindamise süsteemi, sisekontrollide hindamise ning auditiprotseduuride olemasolu kohta olulisi puudusi. Olemas oli intsidendihalduse kord ja juurutatud intsidentide toimumise korral rakendatavad protseduurid, samuti riskijuhtimise protseduurid (vt järgmine alampeatükk).

50. Samuti on mõned auditid tellinud NIIS tarkvara X-Road hindamiseks. Läbistustestimise korda ega protseduure eraldi RIAs kehtestatud ei ole. Samas on NIIS X-tee tarkvarale mitmeid läbistustestimisi tellinud, sama on RIA teinud X-tee iseteeninduskeskkonnale.

Intsidendihaldus

51. Intsidentide haldamisel eeldas Riigikontroll, et RIA tegeleb X-teega seotud turvaintsidentide käsitlemisega ning selleks on olemas intsidentide haldamise kord ja protseduurid. Samuti kontrollisid audiitorid, kas infot intsidentide kohta kogutakse ja analüüsitakse ning kas see on riskide hindamise üks aluseid. Samuti on ITILi raamistikus eeldatud, et

[9] ITIL Foundation, 5.1.6. Organizational Change Management.
[10] ITIL Foundation, 5.1.3. Information Security Management.

intsidentidest teavitatakse kasutajatuge, personali, kliente (X-tee puhul selle liikmeid) ning et intsidendihalduse protsess on olemas ka arendus- ja testkeskkondadele.[11]

52. RIAs käsitletakse X-teega seotud turvaintsidente üldise intsidendihalduse protsessi kaudu. Selleks on RIA kehtestanud intsidendihalduse põhimõtted. Need aga intsidentidest saadud info kogumist ega analüüsimist ei käsitle. RIA andmevahetuse osakond X-teega seotud turvaintsidente ei analüüsi, vaid sellega tegeleb intsidentide käsitlemise osakond CERT (*Computer Emergency Response Team*). RIA intsidendihalduse protsessi kohaselt on intsidente puudutav info ka kasutajatoe tegevuse üheks aluseks.

53. Andmevahetuse osakond kinnitas näiteks, et nende teada tegeleb just standardi- ja järelevalveosakond X-tee liikmete riskianalüüside hindamisega; küsib välja turvaserveri turvalisuse hindamiseks vajaliku teabe, turvaeeskirjad ning info rakendatud meetmete kohta; selgitab välja, kas X-teega liitumiseks esitatud andmed on tõesed.

54. Auditi käigus leidis Riigikontroll, et esineb mitmeid X-tee valdkondi või tegevusi, mille puhul ei ole üheselt kokku lepitud, kas nende eest vastutab RIA järelevalveosakond või andmevahetuse osakond. Intervjuudest selgus et mitmete teemade kohta arvavad mõlemad pooled, et asjaga tegeleb teine pool.

55. Järelevalveosakonna sõnul tegelevad nad aga riskianalüüsiga ainult selles ulatuses või sel määral, mida nimetatud üldiste riskide analüüsides on käsitletud, X-tee spetsiifilisi analüüse tehtud ei ole. Samuti ei tegele järelevalveosakond X-tee liikmete turvaserveri turvalisuse hindamiseks vajaliku teabe hankimisega ega X-teega liitumiseks esitatud andmete õigsuse kontrolliga. Olukorras, kus vastutust nimetatud tegevuste eest ei ole kindlaks määratud, dubleeritakse osa tegevuste sooritamist või siis ei tee neid tegevusi üldse keegi (vt p-d 49–51).

Riskide juhtimine ja regulaarne läbivaatus on süsteemne

56. IT juhtimise parima praktika rakendamine loob eeldused vältida infotehnoloogiliste süsteemide haldamisel suuremaid probleeme, kuid tegelikku olukorda, näiteks tegevusala spetsiifilisi riske hindamata ei suudeta vältida kõiki X-teed varitsevaid ohte. ITILi kohaselt on riskijuhtimine vajalik, et tajuda kõiki organisatsiooni põhitegevust ähvardavaid ohte ja nendega toime tulla. Riskijuhtimine on vajalik, et tagada organisatsiooni jätkusuutlikkus ja luua klientidele väärtust.[12]

X-tee riskide juhtimine

57. Riigikontroll eeldas auditit tehes, et olulisemad X-teega seotud riskid on hinnatud, nende maandamiseks on välja töötatud vajalikud meetmed ja neid meetmeid rakendatakse. Samuti eeldati, et X-tee riskianalüüs on koostatud ja seda on uuendatud mõistliku aja tagant.

58. Auditi käigus selgus, et riskide hindamine on RIAs üldine tava ja seda tehakse regulaarselt kord aastas. X-tee riske käsitletakse koos kõigi teiste RIA pakutavate teenuste riskidega.

[11] ITIL Foundation, 5.2.5. Incident Management.
[12] ITIL Foundation, 5.1.10. Risk Management.

59. Peale selle on 2019. aasta aprillis koostatud eraldi ka X-tee IT-riskianalüüs. Selles analüüsis oli eristatud erinevaid riske, mis on seotud

- usaldusteenuse pakkumisega,
- X-tee kesksete komponentidega ning
- X-tee liikmete teadlikkusega.

60. Selle analüüsi kokkuvõttena on välja toodud mõned olulisemad abinõud leitud riskide maandamiseks. Näiteks alustas RIA ettevalmistusi, et luua SK ID Solutions ASi sertifitseerimisteenustele alternatiivne võimalus pakkuda sertifikaate ja ajatempliteenust. Samuti on RIA teadvustanud riski, et praegu kasutusel olevad krüptoalgoritmid on tulevikus lahti murtavad ja RIA peab kvantarvutite arenedes sellele kiiresti reageerima. Riigikontrolli hinnangul ei puudu sellest analüüsist olulisi riske, mis oleks seotud X-tee arendamise ja haldusega.

61. Audit näitas, et üldist RIA riskianalüüsi uuendatakse kord aastas. X-tee olulisemad riskid on leidnud käsitlemist, nende maandamiseks on töötatud välja meetmed ja neid meetmeid rakendatakse.

Talitluspidevuse tagamiseks on X-tee kesksed komponendid dubleeritud ja sõltuvust nendest vähendatud

62. X-tee kesksed teenused peavad RIA ja MKMi sõlmitud teenustaseme leppe kohaselt olema igapäevaselt kättesaadavad ja toimima. RIA peab selle leppe järgi tagama X-tee talitluspidevuse, s.t andma kindlustunde, et X-tee turvaline andmevahetuskiht on võimeline ka pärast tõsist intsidenti jätkama teenuste osutamist ettemääratud vastuvõetaval tasemel, s.t lepingutes fikseeritud teenustasemel.[13]

Talitluspidevuse tagamine

63. Riigikontroll eeldas, et RIA on koostanud talitluspidevuse plaani ning on selles kajastanud minimaalselt nõutavad tingimused. Samuti eeldati, et nimetatud plaani on testitud. Talitluspidevuse tagamiseks on oluline hinnata X-tee toimimiseks vajalike infovarade kriitilisust X-tee teenuste toimimisel. Talitluspidevus- ja taasteplaane tuleb samuti testida ja personali nende kasutamiseks treenida.[14]

64. Audit näitas, et RIA on kasutusele võtnud mitmed meetmed talituspidevuse tagamiseks ja parandamiseks. Näiteks on dubleeritud X-tee toimimiseks vajalikud kesksed komponendid. Lisaks hoitakse X-tee keskseid komponente eri asukohas. Teatud määral on vähendatud sõltuvust kesksetest RIA hallatavatest X-tee komponentidest, s.t tõrgete korral RIA kesksete serverite või SK ID Solutions ASi teenuste kättesaamisel kasutatakse puhveraega.

65. RIA ei ole eraldi dokumendina talitluspidevuse plaani koostanud, ent on sätestanud nõuded talitluspidevuse tagamiseks muudes dokumentides. Näiteks on hädaolukorra riskianalüüsis kirjeldatud ühe X-teega seotud ohustsenaariumina riigi toimimiseks oluliste andmete tervikluse rikkumist. Samuti sisaldab X-tee IT-riskide hindamine mitmeid

[13] ISO 22300, ISO/IEC 19086, 22318.

[14] ITIL Foundation, 5.2.12. Service Continuity Management ja Cobit (raamistik infotehnoloogia haldamiseks ja juhtimiseks) DSS04 - Managed Continuity.

võimalikke ohustsenaariumeid ja lahendusi. Siiski ei ole eelnimetatud talitluspidevust tagavates dokumentides omavahelised seosed selgelt välja toodud.

Infovara – informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.

66. X-teega seotud infovarade elutähtsust ja tundlikkust, s.t nende mõju X-tee teenustele, ei ole RIA eraldi hinnanud ega analüüsinud. Samas selgus auditi käigus, et nõudeid X-tee püsivaks toimimiseks ja toimepidevuse tagamiseks oli RIA kehtestanud teistes kordades ja juhendites.

67. Kuigi RIA sõnul on X-tee taastamist küll testitud, ei ole testimisi dokumenteeritud. Taasteplaanide testimise dokumenteerimine on vajalik testiandmete hilisemaks tõestamiseks ja analüüsimiseks, et saada väärtuslikke võrdlusandmeid talitluspidevuse plaani parendamiseks ja uuendamiseks.

68. Audit näitas, et ehkki eraldi talitluspidevuse plaani X-tee kohta koostatud ei ole, on RIA kasutusele võtnud meetmeid turvalise andmevahetuse püsivaks toimimiseks ning sätestanud talitluspidevuse nõudeid erinevates muudes dokumentides. Puudusteks võib pidada taastetestide ebaregulaarsust ja dokumenteerimata jätmist.

X-tee keskses taristus on toimunud viimase kolme aasta jooksul üks olulise mõjuga intsident

69. Probleemid ja intsidendid, mida riskide hindamisest ja maandamisest hoolimata ei õnnestu vältida, tuleb aegsasti avastada ning nende lahendamiseks peavad organisatsioonis olema kokku lepitud protseduurid ja vastutajad. Riigikontroll eeldas, et RIA-l on olemas intsidentidega toimetulemiseks protseduurid, mille alusel käsitletakse X-teega seotud turvaintsidente. Samuti eeldati, et RIA seirab X-tee kasutamist, püüdes avastada kõik ebakõlad ja anomaaliad, enne kui need andmevahetusele suuremaid probleeme põhjustavad.[15]

X-tee intsidendihaldus

70. X-tee intsidentidega tegeletakse intsidendihalduse protsessi kohaselt: esmakontaktiks on andmevahetuse osakond, kes lahendab juhtumid ise või vajaduse korral suunab keerukamate ja arendusi puudutavate juhtumite käsitlemise edasi (nt NIISile).

71. Nagu eespool (vt p 42) öeldud, kasutatakse X-tee toimimise jälgimiseks seiretarkvara. S.t andmevahetuse osakond seirab X-tee kasutamist ja kogub selle kohta statistikat, et saada ülevaade teenuse kasutamisest. Lisaks teeb intsidentide käsitlemise osakond CERT pidevalt riigiasutuste andmesidevõrgu turvaseiret, mille üheks osaks on ka X-tee komponendid. Järelevalveosakond ei tee X-tee seiret, vaid riiklikku ja haldusjärelevalvet[16] ning samuti järelevalvet korrakaitseseaduse ja Vabariigi Valitsuse seaduses sätestatud piirides.

72. Intsidentide analüüsimisel ja kokkuvõtete tegemisel on oluline anda sisend riskide hindamisse. Riigikontroll eeldas, et X-tee keskses taristus või liikmete juures toimunud infoturbe intsidendid ei ole põhjustatud riskidest, mida ei ole riskianalüüsides käsitletud või mida ei ole piisavalt maandatud. Samuti, et ei ole toimunud intsidente, mis tulenevad

[15] ITIL Foundation, 5.2.5. Incident Management.

[16] Avaliku teabe seaduse § 531 alusel.

asjaoludest (probleemidest), millega ei ole vajalikul määral tegeletud või mida ei ole suudetud lahendada.

73. Enamik viimasel kolmel aastal toimunud intsidentidest on RIA sõnul tekkinud tarkvara vigadest või konfiguratsiooniprobleemidest, mis on enamasti lahendatud mõistliku aja jooksul. Olulise mõjuga intsidente on X-tee kesksetes teenustes 2017. aasta aprillist kuni 2020. aasta aprillini olnud üks ja see toimus 2017. aastal. Toimunud intsidentide kohta koostatud aruannete põhjal ei tuvastanud Riigikontroll probleeme, mida riskianalüüsis ei oleks kajastatud.

74. Seni toimunud intsidentide põhjuseid analüüsides ei saa öelda, et eksisteeriks riske, mida ei oleks riskianalüüsides käsitletud. Ka enamiku auditeeritute sõnul on X-tee seni olnud väga töökindel.

75. Audit näitas, et RIA on selgitanud välja olulisemad X-tee töökindlust ohustavad riskid ja hinnanud neid. Nende riskide maandamiseks on RIA loonud meetmed ja mitmeid nendest meetmetest ka rakendatakse. X-tee teenustes on 2017. aasta aprillist 2020. aasta aprillini olnud X-tee kesksetest komponentidest tingituna üks olulise mõjuga katkestus, s.t X-tee taristu kesksed teenused on olnud seni võrdlemisi töökindlad. Siiski võib öelda, et auditis vaadeldud asutused ei ole valmistunud pikemateks X-tee katkestusteks, s.t neil puuduvad enamasti alternatiivsed võimalused osutada X-teel põhinevaid teenuseid.

X-tee töökindluse tagamine liikmete poolt

76. X-tee üldisema haldamisega, sealhulgas näiteks arvestusega liikmete üle, tarkvara kättesaadavuse tagamisega, turvaintsidentide keskse käsitlemisega, X-tee kasutamise seiramise ja kasutusstatistika kogumisega, tegeleb RIA. Hajusa süsteemi puhul on aga oluline, kuidas on tagatud erinevate X-tee liikmete juures andmete terviklus, konfidentsiaalsus ja käideldavus. RIA-le kehtestatud nõuete ja kohustuste kõrval on Vabariigi Valitsuse määrusega „Infosüsteemide andmevahetuskiht“ (edaspidi X-tee määrus) määratud nõuded ka X-tee liikmetele.

Mitmed X-tee liikmetele määrusega kehtestatud nõuded on üldsõnalised ning nende täitmist ei kontrollita

Nõuded X-tee liikmetele

77. X-tee määrus[17] sisaldab X-tee liikme kohustusi, millest olulisemad on järgmised:

- X-tee andmeteenuse osutamiseks ja kasutamiseks peavad X-tee liikmed omavahel sõlmima andmeteenuse kasutamise kokkulepped.
- X-tee liikmed tagavad oma X-teega ühendatava infosüsteemi järjepideva toimimise, haldamise, arendamise ning turvalise ja häireteta töö.
- X-tee liikmed peavad rakendama turvalisusega seotud riskide maandamiseks andmete terviklust, konfidentsiaalsust ja

[17] Vabariigi Valitsuse 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ § 5.

käideldavust tagavaid meetmeid ning tagama rakendatavate meetmete sõltumatu auditeerimise vähemalt iga nelja aasta järel.

- X-teed kasutavad asutused rakendavad turvalise ja standardiseeritud andmevahetuse tagamise elemendid.
- X-tee liikmed teavitavad RIAt X-tee kasutamisega seotud probleemidest.

78. Auditi käigus selgus, et mitmed X-teele kehtestatud nõuetest on jäänud üldsõnaliseks. Näiteks võimaldavad eeltoodud loetelus teise ja kolmandana nimetatud kohustused X-tee liikmetel neid rakendamisel erinevalt tõlgendada.

79. X-tee liikmed tagavad oma X-teega ühendatava infosüsteemi järjepideva toimimise, haldamise, arendamise ning turvalise ja häireteta töö. X-tee liikmed peavad rakendama turvalisusega seotud riskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid ning tagama rakendatavate meetmete sõltumatu auditeerimise vähemalt iga nelja aasta järel

80. Riigikontrolli hinnangul tuleks täpsemalt kindlaks määrata minimaalselt nõutav andmete terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete komplekt. See võimaldaks X-tee liikmetel üheselt mõista, mis turvalisuse tase on X-teega liitumisel ja kasutamisel vajalik.

81. Samuti ei ole RIA X-tee liikmetele kehtestanud detailsemaid juhendeid, kuidas neid meetmeid ellu viia. See aga võimaldab X-tee liikmetel käituda määruse nõuete rakendamisel loominguliselt ning tõlgendada neid leebemalt ja vähem koormavana. Auditi käigus tehtud intervjuudel selgus, et enamasti deklareerivad X-teega liituvad ja X-tee kaudu andmeteenuseid kasutama hakkavad asutused, et nad vastavad määruse nõuetele, kuid üldjuhul määruses olevate nõuete täitmise üle kontrolli ega järelevalvet ei tehta.

X-teega liitumine ning andmeteenuste avamine ja kasutamine vajab korrastamist

Teadmiseks, et

X-teega liitumist ja X-tee haldamist on reguleerinud erinevad õigusaktid:

- 2004–2008 kehtis Vabariigi Valitsuse 19.12.2003. a määrus nr 331 „Infosüsteemide andmevahetuskihi rakendamine“;
- 2008–2016 kehtis Vabariigi Valitsuse 24.04.2008. a määrus nr 78 „Infosüsteemide andmevahetuskiht“ ning
- alates 2016. aasta sügisest kehtib Vabariigi Valitsuse 23.09.2016. a määrus nr 105 „Infosüsteemide andmevahetuskiht“.

82. X-teega liitumiseks on vaja sõlmida RIAga liitumiskokkulepe, kus fikseeritakse poolte õigused, kohustused ja vastutus. Andmeteenuse osutamiseks ja kasutamiseks peavad osapooled sõlmima andmeteenuse kasutamise kokkuleppe.

83. Auditi käigus kontrolliti RIA ja X-tee liikmete vaheliste liitumiskokkulepete olemasolu juhusliku valimi abil, mis hõlmas 10% liikmeid.

84. Kontrolli tulemusena selgus, et ligi 83%-l valimis olnud asutustest on X-teega liitumise dokumendid olemas, ülejäänute liitumise kokkuleppeid ei suutnud RIA auditi käigus esitada. X-teega liitumise dokumente puudus aastatest 2004, 2007, 2009, 2010, 2012 ja 2014. Liitumisega seotud dokumentideks võisid olla näiteks nõuetele vastavuse kinnitus või liitumiskokkulepe. RIA selgituste kohaselt on X-teega seotud õigusaktid aja jooksul muutunud ja seetõttu on X-tee liitumise kokkuleppeid sõlmitud eri alusel ja viisil.

Andmeteenuse kasutamise kokkulepete sõlmimine

85. Riigikontroll eeldas, et X-tee andmeteenuse osutamisel ja kasutamisel on sõlmitud andmeteenuse kasutamise kokkulepped ja andmeteenuse osutajad kontrollivad andmeteenuse kasutamise kokkulepete olemasolu ja täitmist.

86. Selgus, et mitmetel juhtudel ei ole asutused sõlminud eelnimetatud kokkuleppeid. Vähemalt pooled Riigikontrolli küsitluses (vt "Auditi iseloomustus") osalenud asutustest on sõlminud andmeteenuse kasutamise kokkuleppeid. Neljandik vastanutest märkis, et kõikidel juhtudel kokkuleppeid ei sõlmita.

87. Kokkulepete sõlmimata jätmise kohta toodi erinevad põhjendusi. Näiteks arvati, et kehtivad õigusaktid reguleerivad poolte suhteid piisavalt ja eraldi andmekasutuse kokkuleppeid ei ole vaja sõlmida, või eelistati vähem bürokraatlikke lahendusi andmeteenuste avamiseks ja kasutamiseks, näiteks saadetakse e-kiri palvega avada andmeteenus. Tallinna linn ei sõlmi andmevahetuse kokkuleppeid. Tallinn ei pea seda vajalikuks, sest pakutavaid teenuseid on vähe.

88. Andmeteenust pakkuvad asutused lähenevad leppe sõlmimisele erinevalt. Näiteks nõuavad Maksu- ja Tolliamet ning Maanteeamet andmevahetuslepingut. Samas on aga asutusi, kes on andmeteenused toimima pannud e-kirjaga saadetud päringu peale. Samuti ei sõlmi lepinguid AS TS Laevad, kellel on andmete kasutamine võimaldatud kirjaliku taotluse esitamisel registripidajale.

89. Riigikontrolli korraldatud küsitluse tulemusena saab öelda, et ainult 38% vastanutest on sõlminud eraõiguslike asutustega andmeteenuse kasutamise kokkuleppeid. Samuti selgus, et X-tee kaudu teenust avades ei kontrollita andmete terviklust, konfidentsiaalsust ega käideldavust tagavate meetmete olemasolu teenusega liituvates eraõiguslikes asutustes. Üks vastanud asutustest eeldas, et liituv asutus on läbinud ISKE-auditi, teine aga seda, et meetmete rakendamist kontrollib ja hindab andmete omanik ise.

90. Lisaks puudub ühtne lähenemine sellele, millised asjaolud või tingimused reguleeritakse andmeteenuse kasutamise kokkulepetes. Mõnel asutusel on välja töötatud teenustaseme tingimused ja osapoolte ülesanded, mõni lähtub X-tee määruse §-s 12 (andmeteenuse osutamise ja kasutamise põhimõtted, sh kohustused) toodud nõuetest ning mõnel asutusel on põhjalikult fikseeritud õiguslik alus, teenuse kirjeldus, andmevahetuse eesmärk ja poolte kohustused.

91. Auditeeritud asutustest kontrollivad andmeteenuse kasutamise kokkulepete täitmist vaid üksikud andmeteenuse osutajad. Need asutused uurivad andmete kasutamise põhjuseid päringuid teinud X-tee liikmetelt eelkõige andmekaitse seisukohast, s.t kas X-tee kaudu kättesaadavaks tehtud andmeid (iseäranis isikuandmeid) töödeldakse ainult seaduses ettenähtud eesmärkidel. Kõige enam on auditeeritute sõnul kontrollinud päringute põhjendatust Siseministeeriumi infotehnoloogia- ja arenduskeskus. Andmeteenuse kasutamise kokkulepete mittesõlmimine ja kontrolli puudumine andmete kasutamise üle võib viia andmete väärkasutuseni.

Infosüsteemide toimivuse tagamiseks kasutatakse erinevaid standardeid ja rakendatakse erinevat praktikat

92. Andmekogude ja infosüsteemide vaheline andmevahetus on igapäevaselt vajalik erinevate avalike teenuste osutamiseks. Seetõttu on iga pakutava teenuse seisukohalt oluline, et vajalike andmete allikaks olevad andmekogud toimivad jätkusuutlikult. Selleks peaks iga X-tee liige tagama oma andmekogu püsiva ülalpidamise, vajaduse korral uuendamise, neis sisalduvate andmete õigsuse, andmete vajalikul tasemel kättesaadavuse vaid selleks volitatud osapooltele.

Infosüsteemide toimepidevus

93. Riigikontroll eeldas, et asutused ehk X-tee liikmed tagavad oma tegevusega, lähtudes X-tee määruses paika pandud nõuetest, X-teega liidestatud andmekogu või infosüsteemi järjepideva toimimise, haldamise, arendamise ning turvalise ja häireteta töö.

94. Vaadeldud asutustest on riigiasutused ja kohalikud omavalitsused kohustatud rakendama ISKEt. Selle rakendamise abil püütakse tagada infosüsteemi järjepidev toimimine, haldamine, arendamine ning turvaline ja häireteta töö.

95. Mõneti erinev olukord on eraõiguslikes asutustes, kes on X-tee liikmed. Neil ei ole otsest kohustust kasutusele võtta IT juhtimise või infoturbe standardeid, ent mõned neist rakendavad parimat praktikat. AS Elering rakendab infoturbe standardit ISO/IEC 27001 ning OÜ TS Laevad kasutab lisaks standardit ISO/IEC 277002 ja lähtub ISKEst. Vaadeldud asutustest ei rakendanud Riigimetsa Majandamise Keskus ühtegi infoturbestandardit ega -raamistikku.

96. X-tee liikmed kasutavad ISKE rakendusjuhendit andmekogu või infosüsteemi järjepideva toimimise, haldamise, arendamise ning turvalise ja häireteta töö tagamiseks. Samuti on nad kohustatud ISKE rakendamise kohta tellima auditi, kuid neis auditites X-tee komponente sageli auditeeritud. Milles aga seisneb andmekogu või infosüsteemi järjepideva toimimise, haldamise, arendamise ning turvalise ja häireteta töö tagamine, see tuleks detailsemate juhistega täpsemalt kindlaks määrata.

X-tee liikmete infoturbega seotud nõuded ja nende auditeerimine on eraõiguslike asutuste puhul puudulik

97. Asutustes, mis oma andmekogude toimimiseks ja teenuste pakkumiseks vajavad turvalist andmevahetust teiste andmeandjatega, on infoturbe tagamine esmatähtis. Kõige kindlamalt tagab vajalikul tasemel infoturbe riiklikult või rahvusvaheliselt tunnustatud IT- jm raamistike rakendamine. Samas tuleks seda teha nii, et kõigi vajalike infoturbemeetmete olemasolu kontrollitakse regulaarselt.

Infoturbe tagamine

98. Riigikontroll eeldas auditit tehes, et asutused on rakendanud turvalisusega seotud riskide maandamiseks vajalikud infoturbe meetmed ning X-teed kasutatavates asutustes on regulaarselt korraldatud infoturbe standardi rakendamise (näiteks ISKE) auditeid. Samuti eeldati, et infoturbe meetmed on rakendatud sellisel määral, et nimetatud auditites ei ole leitud olulisi puudusi.

99. Enamik X-tee liikmetest ja auditis vaadeldud asutustest on riigi- ja omavalitsusasutused. Seega on nad andmekogude vastutava või volitatud

töötlejana kohustatud rakendama riiklikku infoturbe raamistikku ISKEt ning nende peamised riskihindamised ja riskide maandamise meetmed on seotud ISKEga. Mõnevõrra erinev olukord on riigi äriühingutes, kus rakendatakse mitmeid erinevaid infoturbe standardeid (vt p 95).

100. Auditis vaadeldud riigiasutustel olid ISKE-auditid tellitud ja läbi viidud. Vaadeldud KOVides ei olnud viimastel aastatel ISKE-auditeid tehtud. KOVidele ISKE-auditite tellimise kohustus on MKMil.

101. ISKE-auditite puhul täheldas Riigikontroll, et ISKE-auditi juhendis ei ole kohustust auditi valimisse võtta andmekogude X-teega seotud komponente. Seega auditeeritakse X-tee komponente vaid juhul, kui mõni X-tee komponent satub ISKE-auditi juhuvalimisse, s.t läbiviidud ISKE-auditites on X-teega seotud teemasid harva käsitletud.

102. Ükski auditeeritud asutus ei ole eraldi hinnanud seda, mis infoturbe standardit või raamistikku eraõiguslikud asutused rakendavad. Samas tuleb märkida, et teatud juhtudel on asutustel olnud eraõiguslike juriidiliste isikute päringutega probleeme, näiteks on küsitud liiga suurt hulka andmeid korraga.

103. Riigikontroll eeldas auditis, et andmeteenuse osutaja veendub eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjast andmeteenuse kasutajaga kokkuleppe sõlmimise eel, et andmeteenuse kasutaja rakendab turvalisusega seotud riskide maandamiseks piisavaid meetmeid, et tagada andmete terviklus, konfidentsiaalsus ja käideldavus.

104. Audit näitas, et auditeeritud riigiasutustest mitmed (nt Tervise ja Heaolu Infosüsteemide Keskus, Maanteeamet, Maksu- ja Tolliamet) ei veendu andmeteenuse kasutajaga kokkuleppe sõlmimise eel, kas eraõiguslikust juriidilisest isikust ettevõtja rakendab turvalisusega seotud riskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. Eraõiguslikud X-tee liikmed küll kinnitavad X-tee liitumislepingut (ja andmeteenuse kasutamise lepingut) sõlmides, et nad rakendavad vajalikke meetmeid, kuid seda auditis vaadeldud andmeteenuse osutajad ei kontrolli ja sellisel kujul jääb vastavus pigem deklaratiivseks. Selline meetmete kontrolli puudumine ei võimalda veenduda, et turvalisuse tagamiseks on rakendatud minimaalselt vajalikud meetmed, mistõttu võib omakorda tekkida võimalus volitamata ligipääsuks andmetele või volitamata muudatuste tegemiseks.

X-tee päringutega seotud intsidente lahendavad enamasti andmeid vahetavad X-tee liikmed

105. X-tee jätkusuutliku toimimise üheks tagatiseks on see, kui X-tee liikmed suudavad kiirelt ja tõhusalt toime tulla probleemidega, mis andmevahetuse korraldamisel ette tulevad. Kindlasti on oluline ka seesuguste probleemide kiire avastamine ja kõigi seotud osapoolte teavitamine.

X-tee liikmete intsidendihaldus

106. Teenuste toimepidevuse tagamiseks, probleemide kiireks kõrvaldamiseks ja riskide maandamiseks on vajalik kvaliteetse intsidendihalduse olemasolu. Seetõttu oli vaja veenduda, et asutused teavitavad RIAt X-tee keskset taristut puudutavatest probleemidest ja neil on ülevaade, missuguste probleemidega on tegemist.

107. Audit näitas, et enamik intsidentidest tekib kahe X-tee liikme vaheliste tehniliste või organisatsiooniliste tõrgete tõttu. Sel juhul on otstarbekas, et neid intsidente lahendavad pigem need osapooled ise.

108. Selliste tõrgete tekkimise põhjused võivad olla erinevad. Sageli on probleemide allikaks puudulik infovahetus andmekogude ja infosüsteemide arendamisel, s.t uuenduste planeerimisel jäetakse teise poolega arvestamata või arendusse tekib tehnilisi vigu, mis võivad muuta näiteks päringu parameetreid.

109. Riigikontrolli küsitlusele vastanud asutused pigem ei ole kogenud X-tee või X-teega seotud teenuste olulisi katkestusi.

110. Kokkuvõtteks võib öelda, et mõningaid õigusaktides RIA-le ja X-tee liikmetele kehtestatud nõudeid ei täideta. Andmeteenuse kasutamise kokkuleppeid X-tee liikmete vahel mitmetel juhtudel ei sõlmita ning ei kontrollita eraõiguslike asutuste infoturbe taset nende liitumisel X-teega. Kokkulepete puudumine ja nõuete eiramine võib tuua endaga kaasa volitamata ligipääsu andmetele ning andmete väärkasutamise.

111. Riigikontrolli soovitused Riigi Infosüsteemi Ameti peadirektorile:

- Algatada Vabariigi Valitsuse 23.09.2016. aasta määruse nr 105 „Infosüsteemide andmevahetuskiht“ muudatus, mis teeks X-tee liikmetele kehtestatud nõuded täpsemaks ja üheselt arusaadavaks, nii et X-tee liikmetel oleks võimalik neid nõudeid rakendada ja andmeteenuse osutajatel nende rakendamist kontrollida. Näiteks kindlaks määrata, millised nõuded peavad olema täidetud, et
  - X-tee liikmetel oleks rakendatud turvariskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavad meetmed ning
  - X-teega ühendatavatel infosüsteemidel oleks tagatud nende järjepidev toimimine, haldamine, arendamine ning turvaline ja häireteta töö.

  Samuti tuleks töötada välja vajalikud juhendid määrusest tulenevate nõuete rakendamiseks ja viia läbi vastavad X-tee liikmete koolitused.
- Sõlmida X-teega liitumisel kõigi asutustega liitumiskokkulepped ja tagada nende lepete säilimine.
- Hinnata riske, mis tulenevad asjaolust, et mõned X-tee liikmed ei pea andmeteenuse kasutamise kokkulepete sõlmimist vajalikuks ja mõistlikuks ega sõlmi neid; ning võtta ette vastavaid riske maandavad tegevused. Kaaluda andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsuse lisamist X-tee portaali, et andmeteenuste avamine ja kasutamine oleks senisest vähem bürokraatlik.
- Töötada välja eraõiguslikust juriidilisest isikust ja füüsilisest isikust ettevõtjast X-tee liikmete kontrolli süsteem, et oleks tagatud X-tee määruses nõutavate terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendamise kontroll ja järelevalve.

- Kehtestada nõuded X-tee komponentide kontrollimiseks ISKE-auditites ja muuta vastavalt sellele ISKE-auditi juhendit.
- Korraldada regulaarselt läbi X-tee kesksete komponentide taastetestimisi ning dokumenteerida need protsessid. Puuduste esinemise korral võtta ette vajalikud parendustegevused.
- Täpsustada X-tee arendamise, haldamise ja järelevalvega seotud osakondade ülesandeid selliselt, et oleks tagatud kõigi vajalike ülesannete täitmine ja nende ülesannete jaotus oleks osapooltele arusaadav.

Riigi Infosüsteemi Ameti peadirektori vastused:

- RIA on seisukohal, et tulenevalt vajadusest tagada X-tee tarkvara jätkusuutlik arendamine, haldamine ja kasutamine ei ole otstarbekas Vabariigi Valitsuse määruse tasemel kõiki üksikasju reguleerida. Vastavalt X-tee määruse § 5 lõikele 2 sõlmitakse liitumiseks X-teega RIA ja taotleja vahel liitumiskokkulepe, milles fikseeritakse poolte õigused, kohustused ja vastutus. RIA hinnangul tuleks X-tee liikmetele kehtivad täpsed nõuded kindlaks määrata pigem liitumislepinguga. RIA on käesolevaks ajaks välja töötanud ka varasemaga võrreldes selgema liitumisprotsessi, mille keskmes on liitumislepingu sõlmimine. Uus liitumislepinguvorm kinnitati RIA peadirektori poolt 26.08.2020 ning on kättesaadav RIA veebilehelt https://www.ria.ee/et/riigi-infosusteem/x-tee/liitumine.html. Samal veebilehel on avaldatud ka juhendmaterjal ja tehnilised kirjeldused liitumisprotsessi läbimise hõlbustamiseks. Nõustume aga Riigikontrolli järeldustega selles osas, et juhendmaterjali piisavust ja arusaadavust võib olla vajalik täiendavalt analüüsida ning neid tuleb vajadusel täiendada ning hoida ajakohasena. Samuti oleme arvestanud, et X-tee liitumisleping peab hõlmama pooltele kehtivaid nõudeid arusaadavas võtmes ning praegune liitumislepinguvorm võib vajada aja jooksul täpsustamist.
- Nõustume soovitusega sõlmida X-teega liitumisel kõigi asutustega liitumiskokkulepped ning liigume selles suunas, et RIA-l oleksid kõikide X-tee liikmetega liitumiskokkulepped sõlmitud ning kohaselt säilitatud.
- Siinkohal peame vajalikuks selgitada, et X-tee haldamise üheks põhimõtteks on multilateraalsus, mis kätkeb X-tee liikme võimalust taotleda juurdepääsu kõigile X-tee kaudu osutatavatele andmeteenustele. Multilateraalsuse põhimõtte eesmärk ei ole üksnes X-tee liikmete vaheliste suhete paljususele osutamine, vaid peale partneri vaba valimise peab liikmetel olema võimalik reguleerida ka pooltevahelise kokkuleppe sisu. X-tee määruse § 12 lõike 1 kohaselt on lubatud andmeteenust osutada ja kasutada vastavalt X-tee liikmete vahelisele andmeteenuse kasutamise kokkuleppele. Järelikult on andmeteenuse osutamine ja kasutamine ilma X-tee liikmete vahelise kokkuleppeta vastuolus X-tee määruse nõuetega. Samas on kokkulepet vaja eeskätt X-tee liikmetele endile, et fikseerida andmevahetuse üksikasjad ning tagada tegevuse kooskõla ka andmevahetust laiemalt reguleerivate õigusaktidega (näiteks isikuandmete kaitse üldmääruse ja avaliku teabe seadusega). Kui X-tee tarkvara ja RIA loovad eeldused andmeteenuste loomiseks,

osutamiseks ja kasutamiseks, saab andmeteenuste praktiline kasutus tugineda üksnes X-tee liikmete omavahelisele kokkuleppele.

X-tee liikmete vaheline kokkulepe andmeteenuse osutamiseks ja kasutamiseks võib olla nii kliendipõhine kui ka teenusepõhine (näiteks SLA (*service level agreement*) või teenuse kasutamise tingimused). Teenusepõhine lähenemine sobib, kui andmeteenuse kasutamise tingimused on standardsed või pakutav teenus on näiteks osa liikme osutatavast avalikust teenusest. Kliendipõhine andmeteenuse kasutamise kokkulepe sobib juhtudel, kus andmeteenuse osutamine ja kasutamine on spetsiifiline ning X-tee osapoolte sõltuvus teineteisest suurem. Igal juhul tuleb andmeteenuse kasutamise kokkuleppes kindlaks määrata andmeteenuse kasutamiseks vajalikud infoturbemeetmed ning andmeteenuse kasutaja alamsüsteemilt nõutavad organisatsioonilised, füüsilised ja infotehnilised turvameetmed ja andmeteenuse kolmandale isikule vahendamise luba ning teenustaseme tingimused (X-tee määruse § 12 lg 1 p 1–3).

Märgime, et RIA-l on plaanis tulevikus välja arendada X-tee iseteeninduskeskkonnas andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsus.

Täiendavalt peame vajalikuks rõhutada, et riigi ja kohaliku omavalitsuse üksuse andmekogu ja infosüsteemi (sh X-tee alamsüsteemi) pidamisel on X-tee liige kohustatud turvameetmete valikul rakendama Vabariigi Valitsuse 20.12.2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ sätestatud kohustusi. RIA teostab infosüsteemide turvameetmete süsteemi rakendamise üle järelevalvet vastavalt avaliku teabe seaduse (edaspidi AvTS) § 531 lõikele 1.

- RIA peab oluliseks kontrollida X-tee kasutamist määruses ja lepingus esitatud nõuetele olenemata X-tee liikme õiguslikust vormist. Mööname, et seni on RIA keskendunud eelkõige avaliku sektori asutustele, kuivõrd AvTS § 439 lõike 5 kohaselt peab andmevahetus riigi infosüsteemi kuuluvate andmekogude vahel toimuma üle X-tee. Eraõiguslikele juriidilistele isikutele võimaldatakse X-tee kasutamist soovi korral vastavalt AvTS § 439 lõikele 6. Tunnistame, et tõhusa kontrolli teostamiseks on vaja hinnata olemasolevate õiguste ja sekkumismeetmete piisavust ning välja töötada toimiv kontrolli süsteem.

- X-tee keskseid komponente auditeeritakse RIAs regulaarselt vastavalt kehtestatud ISKE klassile. X-tee liikmete poolseid X-tee komponente auditeeritakse vastavalt sellele, kuidas vastav moodul valimisse satub. Nõustume, et X-tee komponentide turvaline käitamine on oluline ning tegelik kontrollivajadus on suurem. Küll aga ei ole meie hinnangul otstarbekas seda probleemi lahendada ISKE auditeerimisjuhendi muutmise kaudu, kuivõrd ISKE asendub lähiajal uue Eesti infoturbe standardiga. Seetõttu peame mõistlikuks arvestada Riigikontrolli ettepanekuga uue standardiga kehtestatava auditeerimise korraldamise juures.

- RIA nõustub siinkohal Riigikontrolli soovitusega ning hakkame korraldama regulaarseid taasteteste koos nende dokumenteerimisega ning viime ellu vajalikud parendustegevused.

- Soovitusega täpsustada X-tee arendamise, haldamise ja järelevalvega seotud osakondade ülesandeid nõustume ning algatame arutelu ülesannete ja vastutuste täpsemaks kirjeldamiseks.

112. **Riigikontrolli soovitused andmeteenuseid osutavatele X-tee liikmetele** (Haridus- ja Teadusministeerium, Majandus- ja Kommunikatsiooniministeerium, Keskkonnaministeerium, Tervise ja Heaolu Infosüsteemide Keskus, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Rahandusministeeriumi Infotehnoloogiakeskus, Registrite ja Infosüsteemide Keskus):

- Hinnata eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjale andmeteenuse avamisel ja osutamisel sellega seonduvaid riske ning rakendada riskide minimeerimiseks vajalikke meetmeid, sh kontrollida, kas andmeteenuse kasutaja on rakendanud turvariskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid.

- Töötada koostöös Riigi Infosüsteemi Ametiga välja eraõiguslikust juriidilisest isikust ja füüsilisest isikust ettevõtjast X-tee liikmete kontrolli süsteem, et oleks tagatud X-tee määruses nõutavate terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendamise kontroll.

Siseministeeriumi infotehnoloogia- ja arenduskeskuse platvormiteenuste osakonna juhataja vastus:

- Teeme ettepaneku luua RIA eestvedamisel piisav õigusraamistik, et maandada andmeteenuse avamise ja osutamisega seotud riske tervikuna. Sealhulgas luua selgus, kuidas teostada eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjate poolt kohaldatud riskide minimeerimise meetmete kontrolli. Erinevad asutused peaksid kohaldama sarnaseid meetodeid, et riskide minimeerimise meetmetele kohandatavad nõuded oluliselt ei erineks. Täna puudub praktika ja juriidiline alus eraõiguslikust juriidiliste või füüsilistest isikute poolt hallatavatele süsteemidele kontrolli teostamiseks.

- SMIT on valmis panustama RIA eestvedamisel toimuvasse kontrollisüsteemi loomisesse. Teeme ettepaneku luua süsteem, mis oleks kulutõhus ja ei tekitaks olulisel määral juurde bürokraatiat. Samuti, et oleks lihtsasti kohaldatav ja ei oleks nii keeruline, et takistaks IT-teenuste arendamist.

Tervise ja Heaolu Infosüsteemide Keskuse direktori vastus: Vabariigi Valituses 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ § 12 lg 2 punkti 2 alusel peab andmeteenuse osutaja eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjast andmeteenuse kasutajaga kokkuleppe sõlmimise eel veenduma, et andmeteenuse kasutaja rakendab turvalisusega seotud riskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid.

Määrus viitab küll veendumiskohustusele, kuid ei määrus ega selle seletuskiri too selgelt esile, mida on „veendumisena“ silmas peetud ja millised kohustused sellest täpselt tekivad. Meie hinnangul ei tulene sellest igale asutusele kohustust ega pädevust teostada sisulist kontrolli (nt nõuda eraettevõtetel vastavust kinnitavaid turvaauditeid, sertifikaate või veenduda asutuses kohapeal turvanõuete täitmises) kõigi asutuste osas, kellele andmeteenuse kasutamist vahendatakse. Andmeteenuse vahendamisel veendume täna, sõlmides andmeteenuse kasutajaga liidestuslepingu, millega kinnitab liidestuv asutus selgelt, kas tingimused, sh nõutud turvalisuse tagamise kohustus, on tema poolt täidetud ja võtab endale teadlikult kohustuse turvameetmeid rakendada. Seeläbi on täidetud ka nõue veenduda turvanõuete täitmises. Volitust täiendavate aktiivsete kontrollide teostamiseks ette nähtud ei ole, samuti ei ole selliste võimalike kontrollide sisu määratud, mistõttu ei ole kehtiva määruse pinnalt võimalik täiendavaid kontrolle teostada.

Kui määruse täiendamise kaudu luuakse andmeteenust vahendavatele asutustele täiendavaid kohustusi, tuleks sellised muudatused kokku leppida koostöös vastavate asutustega. Uute kohustuste sisu peaks olema selgelt fikseeritud ja üheselt mõistetav, koostatud nende täitmiseks selged juhised. Samuti tuleks enne kehtiva regulatsiooni muutmist veenduda, et asutustel on piisavad ressursid ja võimekus tekkivate kohustuste täitmiseks. Tagada tuleks mõistlik aeg uute kohustuste täitmisega alustamiseks.

Rahandusministeeriumi Infotehnoloogiakeskuse direktori vastus: See küsimus on suunatud andmeomanikele. Samas on ebaselge, mil moel nad üldse niisugust kontrolli täna teha võivad või saavad ja kas niisuguse kontrolli läbiviimine on üldse nende pädevuses.

Kui seda vajalikuks peetakse, tuleb õigusaktidega kehtestada eraõiguslikele X-tee liikmetele infoturbesüsteemi rakendamise ning auditeerimise kohustus. Sel juhul on võimalik lepingu sõlmimisel tugineda eraõigusliku X-tee liikme kinnituse asemel audiitori hinnangule.

Registrite ja Infosüsteemide Keskuse direktori vastus: Eraõiguslike isikute puhul vastava kontrollimehhanismi rakendamine, mille käigus RIK peaks vastavat kontrolli teostama, andmeteenuse kokkuleppe sõlmimise faasis ei tundu mõistlik. Nimelt saavad andmeteenuse kokkulepet sõlmida vaid X-tee liikmed omavahel ja X-tee liikmelisuse saamisele eelnevalt on taotlejal kohustus tagada, et tema süsteemi puhul oleks rakendatud turvalisusega seotud riskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmed ning tagatud rakendatavate meetmete sõltumatu auditeerimise vähemalt iga nelja aasta järel (määruse § 5 lg 4 p 3). Juhul, kui nõue ei ole täidetud, siis on RIA-l õigus keelduda X-tee liikmelisuse väljastamisest määruse § 6 p 4 alusel. Seega, sisuliselt peaks juba X-tee liikmelisus meie jaoks näitama, et kokkulepet sõlmida sooviva isiku süsteemi puhul on rakendatud turvariskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmed ning täiendav kontrollivajadus ei tundu proportsionaalne saavutatava eesmärgi suhtes.

Topeltkontrolli vajadus võib turvalisuse kaalutlustel isegi mõistlik olla, kuid oleme seisukohal, et kontrolli kohustus peaks olema keskselt lahendatud ja paigutatud vaid ühe pädeva asutuse kohustuseks. Meie hinnangul taoliseks pädevaks asutuseks peaks olema RIA, kellele on juba

antud õigus järelevalve teostamiseks. Juhul, kui järelevalve teostamise õigust on vajalik laiendada, siis on kindlasti lihtsam teha seda järelevalve teostamise õigust konkreetses valdkonnas juba omava asutuse suhtes. Kui kontrolli teostamise kohustus lasub tulevikus ka RIKiga sarnastel asutustel, siis võivad sellega kaasneda mitmed täiendavad murekohad, peamiselt halduskoormuse tõus keeldumisotsuste vormistamisel ja võimalike vaidluste lahendamisel. Järelevalve käigus kontrolli teostamise kohustusega asutuste paljususe olukorras kerkib esile veel täiendav murekoht, nimelt samaväärsete kontrollimeetmete kehtestamine. Mida rohkem on kontrolli teostajaid, seda enam võib tekkida olukordi, kus meetmed on asutuste lõikes erinevad. Taolise olukorra vältimiseks ongi vajalik, et meetmed kehtestab ja kontrolli teostab vaid üks asutus (RIA).

Keskkonnaministeeriumi asekantsleri vastus: Peamiselt puudutavad soovitused aadressiandmete süsteemi, mis vastavalt avaliku teabe seaduse § 439 lg 1 p 3 on üks riigi infosüsteemi kindlustavatest süsteemidest. Tulenevalt Vabariigi Valitsuse 08.10.2015. a määrusest nr 103 „Aadressiandmete süsteem“ (edaspidi ADS) on aadressiandmeid töötleva andmekogu pidaja ja koha-aadressi määraja kohustatud aadressiandmete määramiseks ja töötlemiseks kasutama ADSi infosüsteemi aadressiandmeid, samas võib riigi infosüsteemi mittekuuluva andmekogu liidestada ADSi infosüsteemiga ka teiste ADSi infosüsteemi pakutavate teenuste kaudu. Aadressiandmed kuuluvad oma olemuselt avaandmete hulka ja neile ei ole seatud juurdepääsupiiranguid, näiteks on aadressiandmed kättesaadavad https://xgis.maaamet.ee/adsavalik/. Avaandmed on vastavalt avaliku teabe seaduse § 31 lg 1 selline avalik teave, mille üldist kasutamist ei ole seadusega või seadusega kehtestatud korras piiratud, sealhulgas taaskasutatakse sellist teavet „ärilisel või mitteärilisel eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi“. Seetõttu ei pea Keskkonnaministeerium Riigikontrolli soovitusi aadressiandmete süsteemi suhtes rakendatavateks.

Metsaregistri andmeteenuse eraõiguslikust juriidilisest isikust kasutajaga on teatud riskide maandamise meetmed kokku lepitud. Metsaregistri põhimääruse muutmise eelnõuga täpsustatakse metsaregistrile juurdepääsu tingimusi, mis võimaldab edaspidi seada metsaregistri andmete kasutamisele veel konkreetsemaid nõudeid. Kontrollisüsteemi loomine koostöös Riigi Infosüsteemi Ametiga aitaks nende nõuete täitmist tagada.

Haridus- ja teadusministri vastus: Haridus ja Teadusministeerium on sõlminud kõikide X-tee teenuste kasutamiste ja pakkumiste osas andmeedastusteenuse kokkulepped nii X-tee teenuste kasutajate kui ka X-tee teenuste pakkujatega, kuid tõesti ei viida läbi kontrolle, kas eraõiguslikust juriidilisest isikust ettevõtja rakendab turvalisusega seotud riskide maandamiseks piisavalt andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. Oleme selles osas usaldanud eraõiguslikust juriidilisest isikust ettevõtja lepingulisi kinnitusi.

Oleme seisukohal, et teise osapoole poolt andmete terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete kontrolli kohustus ei peaks lasuma teenuse osutajal teenuse avamisel, vaid see peaks toimuma RIA poolt asutuse liitumisel X-tee toodangukeskkonnaga ning hiljem kindlaks määratud perioodilisusega.

Vastava kohustuse asetamine teenuse osutajale suurendab märgatavalt teenuse osutajate ja teenuse kasutajate halduskoormust. Erinevad teenuse osutajad ei suuda tagada ühtset kontrolli taset. Antud kohustuse seadmine teenuse osutajale võib põhjustada olukorra, et ühte teenuse kasutajat kontrollivad lühikese aja jooksul mitu erinevat teenuse osutajat. Ainult teenuse avamise käigus läbi viidav kontroll ei ole piisav, vaid vastavat kontrolli peaks läbi viima perioodiliselt.

Majandus- ja Kommunikatsiooniministeeriumi kantsleri vastus:
Riigikontrolli soovitus tugineb Vabariigi Valitsuse 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ (X-tee määrus) § 12 lg 2 p 2 sätestatule. MKM püüab andmeteenuse osutamise eel edaspidi senisest suurema hoolsusega X-tee määrusega pandud kohustusi täita. Sh kontrollida, kas andmeteenuse kasutaja on rakendanud turvariskide maandamise meetmeid. MKM on valmis osalema eraõiguslike X-tee liikmete, kes ei täida avalikku ülesannet, kontrolli süsteemi väljatöötamises.

/allkirjastatud digitaalselt/

Ines Metsalu-Nurminen
auditiosakonna peakontrolör

Riigikontrolli soovitused ja auditeeritute vastused

Riigikontroll andis auditi põhjal Riigi Infosüsteemi Ametile ja X-tee liikmetele mitmeid soovitusi. RIA peadirektor ja X-tee liikmed (Siseministeeriumi infotehnoloogia- ja arenduskeskus, Tervise ja Heaolu Infosüsteemide Keskus, Rahandusministeeriumi Infotehnoloogiakeskus, Registrite ja Infosüsteemide Keskus, Keskkonnaministeerium, Haridus- ja teadusministeerium, Majandus- ja Kommunikatsiooniministeerium) saatsid ajavahemikul 16.12.2020–20.01.2021 oma vastused Riigikontrolli soovitustele.

Riigikontrolli soovitused	Auditeeritute vastused
X-tee töökindluse tagamine **111. Riigikontrolli soovitused Riigi Infosüsteemi Ameti peadirektorile:** ▪ Algatada Vabariigi Valitsuse 23.09.2016. aasta määruse nr 105 „Infosüsteemide andmevahetuskiht“ muudatus, mis teeks X-tee liikmetele kehtestatud nõuded täpsemaks ja üheselt arusaadavaks, nii et X-tee liikmetel oleks võimalik neid nõudeid rakendada ja andmeteenuse osutajatel nende rakendamist kontrollida. Näiteks kindlaks määrata, millised nõuded peavad olema täidetud, et ▪ X-tee liikmetel oleks rakendatud turvariskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavad meetmed ning ▪ X-teega ühendatavatel infosüsteemidel oleks tagatud nende järjepidev toimimine, haldamine, arendamine ning turvaline ja häireteta töö. Samuti tuleks töötada välja vajalikud juhendid määrusest tulenevate nõuete rakendamiseks ja viia läbi vastavad X-tee liikmete koolitused.	**RIA peadirektori vastus:** RIA on seisukohal, et tulenevalt vajadusest tagada X-tee tarkvara jätkusuutlik arendamine, haldamine ja kasutamine ei ole otstarbekas Vabariigi Valitsuse määruse tasemel kõiki üksikasju reguleerida. Vastavalt X-tee määruse § 5 lõikele 2 sõlmitakse liitumiseks X-teega RIA ja taotleja vahel liitumiskokkulepe, milles fikseeritakse poolte õigused, kohustused ja vastutus. RIA hinnangul tuleks X-tee liikmetele kehtivad täpsed nõuded kindlaks määrata pigem liitumislepinguga. RIA on käesolevaks ajaks välja töötanud ka varasemaga võrreldes selgema liitumisprotsessi, mille keskmes on liitumislepingu sõlmimine. Uus liitumislepinguvorm kinnitati RIA peadirektori poolt 26.08.2020 ning on kättesaadav RIA veebilehelt https://www.ria.ee/et/riigi-infosusteem/x-tee/liitumine.html. Samal veebilehel on avaldatud ka juhendmaterjal ja tehnilised kirjeldused liitumisprotsessi läbimise hõlbustamiseks. Nõustume aga Riigikontrolli järeldustega selles osas, et juhendmaterjali piisavust ja arusaadavust võib olla vajalik täiendavalt analüüsida ning neid tuleb vajadusel täiendada ning hoida ajakohasena. Samuti oleme arvestanud, et X-tee liitumisleping peab hõlmama pooltele kehtivaid nõudeid arusaadavas võtmes ning praegune liitumislepinguvorm võib vajada aja jooksul täpsustamist.
▪ Sõlmida X-teega liitumisel kõigi asutustega liitumiskokkulepped ja tagada nende lepete säilimine.	Nõustume soovitusega ning liigume selles suunas, et RIA-l oleksid kõikide X-tee liikmetega liitumiskokkulepped sõlmitud ning kohaselt säilitatud.
▪ Hinnata riske, mis tulenevad asjaolust, et mõned X-tee liikmed ei pea andmeteenuse kasutamise kokkulepete sõlmimist vajalikuks ja mõistlikuks ega sõlmi neid; ning võtta ette vastavaid riske maandavad tegevused. Kaaluda andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsuse lisamist X-tee portaali, et andmeteenuste avamine ja kasutamine oleks senisest vähem bürokraatlik. **p-d 77–81 ja 84–91**	Siinkohal peame vajalikuks selgitada, et X-tee haldamise üheks põhimõtteks on multilateraalsus, mis kätkeb X-tee liikme võimalust taotleda juurdepääsu kõigile X-tee kaudu osutatavatele andmeteenustele. Multilateraalsuse põhimõtte eesmärk ei ole üksnes X-tee liikmete vaheliste suhete paljususele osutamine, vaid peale partneri vaba valimise peab liikmetel olema võimalik reguleerida ka pooltevahelise kokkuleppe sisu. X-tee määruse § 12 lõike 1 kohaselt on lubatud andmeteenust osutada ja kasutada vastavalt X-tee liikmete vahelisele andmeteenuse kasutamise kokkuleppele. Järelikult on andmeteenuse osutamine ja kasutamine ilma X-tee liikmete vahelise kokkuleppeta vastuolus X-tee määruse nõuetega. Samas on kokkulepet vaja eeskätt X-tee liikmetele endile, et fikseerida andmevahetuse üksikasjad ning tagada tegevuse kooskõla ka andmevahetust laiemalt reguleerivate õigusaktidega (näiteks isikuandmete kaitse üldmääruse ja avaliku teabe seadusega). Kui X-tee tarkvara ja RIA loovad eeldused andmeteenuste loomiseks, osutamiseks ja kasutamiseks, saab andmeteenuste praktiline kasutus tugineda üksnes X-tee liikmete omavahelisele kokkuleppele. X-tee liikmete vaheline kokkulepe andmeteenuse osutamiseks ja kasutamiseks võib olla nii kliendipõhine kui ka teenusepõhine (näiteks SLA (*service level agreement*) või teenuse kasutamise tingimused). Teenusepõhine lähenemine sobib, kui andmeteenuse kasutamise tingimused on standardsed või pakutav teenus on näiteks osa liikme osutatavast avalikust teenusest. Kliendipõhine andmeteenuse kasutamise kokkulepe sobib juhtudel, kus andmeteenuse osutamine ja kasutamine on spetsiifiline ning X-tee osapoolte sõltuvus teineteisest suurem. Igal juhul tuleb andmeteenuse kasutamise kokkuleppes kindlaks määrata andmeteenuse

Riigikontrolli soovitused	Auditeeritute vastused
	kasutamiseks vajalikud infoturbemeetmed ning andmeteenuse kasutaja alamsüsteemilt nõutavad organisatsioonilised, füüsilised ja infotehnilised turvameetmed ja andmeteenuse kolmandale isikule vahendamise luba ning teenustaseme tingimused (X-tee määruse § 12 lg 1 p 1–3). Märgime, et RIA-l on plaanis tulevikus välja arendada X-tee iseteeninduskeskkonnas andmeteenuse kasutamise kokkulepete sõlmimise ja taotluste halduse funktsionaalsus. Täiendavalt peame vajalikuks rõhutada, et riigi ja kohaliku omavalitsuse üksuse andmekogu ja infosüsteemi (sh X-tee alamsüsteemi) pidamisel on X-tee liige kohustatud turvameetmete valikul rakendama Vabariigi Valitsuse 20.12.2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ sätestatud kohustusi. RIA teostab infosüsteemide turvameetmete süsteemi rakendamise üle järelevalvet vastavalt avaliku teabe seaduse (edaspidi AvTS) § 531 lõikele 1.
X-tee töökindluse tagamine ▪ Töötada välja eraõiguslikust juriidilisest isikust ja füüsilisest isikust ettevõtjast X-tee liikmete kontrolli süsteem, et oleks tagatud X-tee määruses nõutavate terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendamise kontroll ja järelevalve.	RIA peab oluliseks kontrollida X-tee kasutamist määruses ja lepingus esitatud nõuetele olenemata X-tee liikme õiguslikust vormist. Mööname, et seni on RIA keskendunud eelkõige avaliku sektori asutustele, kuivõrd AvTS § 439 lõike 5 kohaselt peab andmevahetus riigi infosüsteemi kuuluvate andmekogude vahel toimuma üle X-tee. Eraõiguslikele juriidilistele isikutele võimaldatakse X-tee kasutamist soovi korral vastavalt AvTS § 439 lõikele 6. Tunnistame, et tõhusa kontrolli teostamiseks on vaja hinnata olemasolevate õiguste ja sekkumismeetmete piisavust ning välja töötada toimiv kontrolli süsteem.
▪ Kehtestada nõuded X-tee komponentide kontrollimiseks ISKE-auditites ja muuta vastavalt sellele ISKE-auditi juhendit.	X-tee keskseid komponente auditeeritakse RIAs regulaarselt vastavalt kehtestatud ISKE klassile. X-tee liikmete poolseid X-tee komponente auditeeritakse vastavalt sellele, kuidas vastav moodul valimisse satub. Nõustume, et X-tee komponentide turvaline käitamine on oluline ning tegelik kontrollivajadus on suurem. Küll aga ei ole meie hinnangul otstarbekas seda probleemi lahendada ISKE auditeerimisjuhendi muutmise kaudu, kuivõrd ISKE asendub lähiajal uue Eesti infoturbe standardiga. Seetõttu peame mõistlikuks arvestada Riigikontrolli ettepanekuga uue standardiga kehtestatava auditeerimise korraldamise juures.
▪ Korraldada regulaarselt läbi X-tee keskse komponentide taastetestimisi ning dokumenteerida need protsessid. Puuduste esinemise korral võtta ette vajalikud parendustegevused. **p-d 66–67 ja 98–104**	RIA nõustub siinkohal Riigikontrolli soovitusega ning hakkame korraldama regulaarseid taasteteste koos nende dokumenteerimisega ning viime ellu vajalikud parendustegevused.
X-tee keskse juhtimise tõhustamine ▪ Täpsustada X-tee arendamise, haldamise ja järelevalvega seotud osakondade ülesandeid selliselt, et oleks tagatud kõigi vajalike ülesannete täitmine ja nende ülesannete jaotus oleks osapooltele arusaadav. **p-d 52–55**	Nõustume soovitusega ning algatame arutelu ülesannete ja vastutuste täpsemaks kirjeldamiseks.
X-tee töökindluse tagamine liikmete poolt **112. Riigikontrolli soovitused andmeteenuseid osutavatele X-tee liikmetele** (Haridus- ja Teadusministeerium, Majandus- ja Kommunikatsiooniministeerium, Keskkonnaministeerium, Tervise ja Heaolu Infosüsteemide Keskus, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Rahandusministeeriumi Infotehnoloogiakeskus, Registrite ja Infosüsteemide Keskus):	**Siseministeeriumi infotehnoloogia- ja arenduskeskuse vastus:** Teeme ettepaneku luua RIA eestvedamisel piisav õigusraamistik, et maandada andmeteenuse avamise ja osutamisega seotud riske tervikuna. Sealhulgas luua selgus, kuidas teostada eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjate poolt kohaldatud riskide minimeerimise meetmete kontrolli. Erinevad asutused peaksid kohaldama sarnaseid meetodeid, et riskide minimeerimise meetmetele kohandatavad nõuded oluliselt ei erineks. Täna puudub praktika ja juriidiline alus eraõiguslikust juriidiliste või füüsilistest isikute poolt hallatavatele süsteemidele kontrolli teostamiseks.

Riigikontrolli soovitused	Auditeeritute vastused
▪ Hinnata eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjale andmeteenuse avamisel ja osutamisel sellega seonduvaid riske ning rakendada riskide minimeerimiseks vajalikke meetmeid, sh kontrollida, kas andmeteenuse kasutaja on rakendanud turvariskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. ▪ Töötada koostöös Riigi Infosüsteemi Ametiga välja eraõiguslikust juriidilisest isikust ja füüsilisest isikust ettevõtjast X-tee liikmete kontrolli süsteem, et oleks tagatud X-tee määruses nõutavate terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendamise kontroll. **p-d 102–104**	SMIT on valmis panustama RIA eestvedamisel toimuvasse kontrollisüsteemi loomisesse. Teeme ettepaneku luua süsteem, mis oleks kulutõhus ja ei tekitaks olulisel määral juurde bürokraatiat. Samuti, et oleks lihtsasti kohaldatav ja ei oleks nii keeruline, et takistaks IT-teenuste arendamist. **Tervise ja Heaolu Infosüsteemide Keskuse direktori vastus:** Vabariigi Valituses 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ § 12 lg 2 punkti 2 alusel peab andmeteenuse osutaja eraõiguslikust juriidilisest isikust või füüsilisest isikust ettevõtjast andmeteenuse kasutajaga kokkuleppe sõlmimise eel veenduma, et andmeteenuse kasutaja rakendab turvalisusega seotud riskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. Määrus viitab küll veendumiskohustusele, kuid ei määrus ega selle seletuskiri too selgelt esile, mida on „veendumisena“ silmas peetud ja millised kohustused sellest täpselt tekivad. Meie hinnangul ei tulene sellest igale asutusele kohustust ega pädevust teostada sisulist kontrolli (nt nõuda eraettevõtetel vastavust kinnitavaid turvaauditeid, sertifikaate või veenduda asutuses kohapeal turvanõuete täitmises) kõigi asutuste osas, kellele andmeteenuse kasutamist vahendatakse. Andmeteenuse vahendamisel veendume täna, sõlmides andmeteenuse kasutajaga liidestuslepingu, millega kinnitab liidestuv asutus selgelt, kas tingimused, sh nõutud turvalisuse tagamise kohustus, on tema poolt täidetud ja võtab endale teadlikult kohustuse turvameetmeid rakendada. Seeläbi on täidetud ka nõue veenduda turvanõuete täitmises. Volitust täiendavate aktiivsete kontrollide teostamiseks ette nähtud ei ole, samuti ei ole selliste võimalike kontrollide sisu määratud, mistõttu ei ole kehtiva määruse pinnalt võimalik täiendavaid kontrolle teostada. Kui määruse täiendamise kaudu luuakse andmeteenust vahendavatele asutustele täiendavaid kohustusi, tuleks sellised muudatused kokku leppida koostöös vastavate asutustega. Uute kohustuste sisu peaks olema selgelt fikseeritud ja üheselt mõistetav, koostatud nende täitmiseks selged juhised. Samuti tuleks enne kehtiva regulatsiooni muutmist veenduda, et asutustel on piisavad ressursid ja võimekus tekkivate kohustuste täitmiseks. Tagada tuleks mõistlik aeg uute kohustuste täitmisega alustamiseks. **Rahandusministeeriumi Infotehnoloogiakeskuse direktori vastus:** See küsimus on suunatud andmeomanikele. Samas on ebaselge, mil moel nad üldse niisugust kontrolli täna teha võivad või saavad ja kas niisuguse kontrolli läbiviimine on üldse nende pädevuses. Kui seda vajalikuks peetakse, tuleb õigusaktidega kehtestada eraõiguslikele X-tee liikmetele infoturbesüsteemi rakendamise ning auditeerimise kohustus. Sel juhul on võimalik lepingu sõlmimisel tugineda eraõigusliku X-tee liikme kinnituse asemel audiitori hinnangule. **Registrite ja Infosüsteemide Keskuse direktori vastus:** Eraõiguslike isikute puhul vastava kontrollimehhanismi rakendamine, mille käigus RIK peaks vastavat kontrolli teostama, andmeteenuse kokkuleppe sõlmimise faasis ei tundu mõistlik. Nimelt saavad andmeteenuse kokkulepet sõlmida vaid X-tee liikmed omavahel ja X-tee liikmelisuse saamisele eelnevalt on taotlejal kohustus tagada, et tema süsteemi puhul oleks rakendatud turvalisusega seotud riskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmed ning tagatud rakendatavate meetmete sõltumatu auditeerimise vähemalt iga nelja aasta järel (määruse § 5 lg 4 p 3). Juhul, kui nõue ei ole täidetud, siis on RIA-l õigus keelduda X-tee liikmelisuse väljastamisest määruse § 6 p 4 alusel. Seega, sisuliselt peaks juba X-tee liikmelisus meie jaoks näitama, et kokkulepet sõlmida sooviva isiku süsteemi puhul on rakendatud turvariskide maandamiseks piisavaid andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmed ning täiendav kontrollivajadus ei tundu proportsionaalne saavutatava eesmärgi suhtes. Topeltkontrolli vajadus võib turvalisuse kaalutlustel isegi mõistlik olla, kuid oleme seisukohal, et kontrolli kohustus peaks olema keskselt lahendatud ja paigutatud vaid ühe pädeva asutuse kohustuseks. Meie hinnangul taoliseks pädevaks asutuseks peaks olema RIA, kellele on juba antud õigus järelevalve teostamiseks. Juhul, kui järelevalve teostamise õigust on vajalik laiendada, siis on kindlasti lihtsam teha seda järelevalve teostamise õigust konkreetses valdkonnas juba omava asutuse suhtes. Kui kontrolli teostamise kohustus lasub tulevikus ka RIKiga sarnastel asutustel, siis võivad sellega kaasneda mitmed täiendavad murekohad, peamiselt halduskoormuse tõus

Riigikontrolli soovitused	Auditeeritute vastused
	keeldumisotsuste vormistamisel ja võimalike vaidluste lahendamisel. Järelevalve käigus kontrolli teostamise kohustusega asutuste paljususe olukorras kerkib esile veel täiendav murekoht, nimelt samaväärsete kontrollimeetmete kehtestamine. Mida rohkem on kontrolli teostajaid, seda enam võib tekkida olukordi, kus meetmed on asutuste lõikes erinevad. Taolise olukorra vältimiseks ongi vajalik, et meetmed kehtestab ja kontrolli teostab vaid üks asutus (RIA). **Keskkonnaministeeriumi asekantsleri vastus:** Peamiselt puudutavad soovitused aadressiandmete süsteemi, mis vastavalt avaliku teabe seaduse § 439 lg 1 p 3 on üks riigi infosüsteemi kindlustavatest süsteemidest. Tulenevalt Vabariigi Valitsuse 08.10.2015. a määrusest nr 103 „Aadressiandmete süsteem“ (edaspidi ADS) on aadressiandmeid töötleva andmekogu pidaja ja koha-aadressi määraja kohustatud aadressiandmete määramiseks ja töötlemiseks kasutama ADSi infosüsteemi aadressiandmeid, samas võib riigi infosüsteemi mittekuuluva andmekogu liidestada ADSi infosüsteemiga ka teiste ADSi infosüsteemi pakutavate teenuste kaudu. Aadressiandmed kuuluvad oma olemuselt avaandmete hulka ja neile ei ole seatud juurdepääsupiiranguid, näiteks on aadressiandmed kättesaadavad https://xgis.maaamet.ee/adsavalik/. Avaandmed on vastavalt avaliku teabe seaduse § 31 lg 1 selline avalik teave, mille üldist kasutamist ei ole seadusega või seadusega kehtestatud korras piiratud, sealhulgas taaskasutatakse sellist teavet „ärilisel või mitteärilisel eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi“. Seetõttu ei pea Keskkonnaministeerium Riigikontrolli soovitusi aadressiandmete süsteemi suhtes rakendatavateks. Metsaregistri andmeteenuse eraõiguslikust juriidilisest isikust kasutajaga on teatud riskide maandamise meetmed kokku lepitud. Metsaregistri põhimääruse muutmise eelnõuga täpsustatakse metsaregistrile juurdepääsu tingimusi, mis võimaldab edaspidi seada metsaregistri andmete kasutamisele veel konkreetsemaid nõudeid. Kontrollisüsteemi loomine koostöös Riigi Infosüsteemi Ametiga aitaks nende nõuete täitmist tagada. **Haridus- ja teadusministri vastus:** Haridus- ja Teadusministeerium on sõlminud kõikide X-tee teenuste kasutamiste ja pakkumiste osas andmeedastusteenuse kokkulepped nii X-tee teenuste kasutajate kui ka X-tee teenuste pakkujatega, kuid tõesti ei viida läbi kontrolle, kas eraõiguslikust juriidilisest isikust ettevõtja rakendab turvalisusega seotud riskide maandamiseks piisavalt andmete terviklust, konfidentsiaalsust ja käideldavust tagavaid meetmeid. Oleme selles osas usaldanud eraõiguslikust juriidilisest isikust ettevõtja lepingulisi kinnitusi. Oleme seisukohal, et teise osapoole poolt andmete terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete kontrolli kohustus ei peaks lasuma teenuse osutajal teenuse avamisel, vaid see peaks toimuma RIA poolt asutuse liitumisel X-tee toodangukeskkonnaga ning hiljem kindlaks määratud perioodilisusega. Vastava kohustuse asetamine teenuse osutajale suurendab märgatavalt teenuse osutajate ja teenuse kasutajate halduskoormust. Erinevad teenuse osutajad ei suuda tagada ühtset kontrolli taset. Antud kohustuse seadmine teenuse osutajale võib põhjustada olukorra, et ühte teenuse kasutajat kontrollivad lühikese aja jooksul mitu erinevat teenuse osutajat. Ainult teenuse avamise käigus läbi viidav kontroll ei ole piisav, vaid vastavat kontrolli peaks läbi viima perioodiliselt. **Majandus- ja Kommunikatsiooniministeeriumi kantsleri vastus:** Riigikontrolli soovitus tugineb Vabariigi Valitsuse 23.09.2016. a määruse nr 105 „Infosüsteemide andmevahetuskiht“ (X-tee määrus) § 12 lg 2 p 2 sätestatule. MKM püüab andmeteenuse osutamise eel edaspidi senisest suurema hoolsusega X-tee määrusega pandud kohustusi täita. Sh kontrollida, kas andmeteenuse kasutaja on rakendanud turvariskide maandamise meetmeid. MKM on valmis osalema eraõiguslike X-tee liikmete, kes ei täida avalikku ülesannet, kontrolli süsteemi väljatöötamises.

Auditi iseloomustus

Auditi eesmärk

Auditi eesmärk oli anda hinnang selle kohta, kas X-tee töökindluse tagamiseks on planeeritud vajalikud meetmed ja kas neid meetmeid rakendatakse.

Hinnangu andmise kriteeriumid

Auditi peamised kriteeriumid olid järgmised:

- Riigi Infosüsteemi Amet on teinud kindlaks X-tee töökindlust ohustavad riskid ja töötanud välja riskide maandamise meetmed ning rakendab neid meetmeid.
- Õigusaktides jm dokumentides RIA-le ja X-tee liikmetele kehtestatud nõudeid täidetakse.
- Eraõiguslike juriidiliste isikute X-teega liitumisel on tagatud X-tee määruses kehtestatud nõuete täitmine.

Auditi ulatus ja käsitlusviis

Auditeeritud periood oli aeg alates 2020. aasta algusest, mil oli võimalik kasutada ainult X-tee versiooni 6, sh selle lahendusi, õigusakte, juhendeid, rakendatud meetmeid jm.

Auditeerimisel lähtuti X-tee määruse kehtivast versioonist (Vabariigi Valitsuse 23.09.2016. a määrus nr 105 „Infosüsteemide andmevahetuskiht“).

Auditis vaadeldi X-teega seotud töökorraldust ja X-tee arendamise reegleid Riigi Infosüsteemi Ametis.

Peale selle auditeeriti X-tee liikmete töökorraldust järgmistes asutustes: Haridus- ja Teadusministeerium, Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium, Kultuuriministeerium, Keskkonnaministeerium, Maaeluministeerium, Välisministeerium, Maksu- ja Tolliamet, Maanteeamet, Tervise ja Heaolu Infosüsteemide Keskus, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Rahandusministeeriumi Infotehnoloogiakeskus ning Registrite ja Infosüsteemide Keskus.

Lisaks sellele vaadeldi kolme kohalikku omavalitsust ning kolme riigile kuuluvat ühingut: vastavalt Pärnu, Tartu ja Tallinna linnavalitsust ning Elering ASi, OÜd TS Laevad ning Riigimetsa Majandamise Keskust.

Auditis on kasutatud erinevaid analüüsimeetodeid, peamiselt dokumendianalüüsi, mille käigus on vaadeldud turva- jm intsidentidega seotud dokumentatsiooni, ISKE-auditite aruandeid, RIA ja X-tee liikmete sisemisi dokumente, X-tee liikmete liitumiskokkuleppeid ning andmeteenuse kasutamise kokkuleppeid. Analüüsitud on Riigikontrolli korraldatud intervjuude ja küsitluse tulemusi. Küsitluse käigus esitatud küsimused on toodud aruande lisas A.

Lisaks sellele võrreldi, kas RIA-l on haldamiseks ja töökindluse tagamiseks kasutusel IT juhtimise parim praktika, lähtudes raamistikest nagu infotehnoloogia haldamise tavade ja protsesside standardite kogu ITIL (*Information Technology Infrastructure Library*), infosüsteemide kolmeastmeline etalonturbe süsteem ISKE ja COBIT (*Control Objectives for Information and Related Technologies*).

Auditi käigus korraldatud intervjuud

Asutus	Kuupäev	Nimi ja ametikoht
Riigi Infosüsteemi Ameti andmevahetuse osakond	07.04.2020 ja 14.04.2020	Joonas Heiter – juhataja
		Jürgen Šuvalov – (X-tee) tootejuht
		Vitali Stupin – arhitekt
Riigi Infosüsteemi Ameti standardi- ja järelevalveosakond	20.04.2020	Ilmar Toom – juhataja
		Raul Volter – juhtiveekspert
Pärnu Linnavalitus	28.04.2020	Sander Blehner – infotehnoloogiateenistuse juht, arendusjuht
		Annemarii Hunt – infotehnoloogiateenistuse analüütik
		Siret Lilleleht – infotehnoloogiateenistuse andmekaitsespetsialist
Tartu Linnavalitus	06.05.2020	Kalev Pullonen – avalike teenuiste arendamise meeskonna teabehaldussüsteemide juhtivarendaja
Tallinna Linnavalitus	13.05.2020	Mari Roots – linnakantselei avalike teenuste infosüsteemide arendamise osakonna juhataja
		Gert Väli – linnakantselei arvutisüsteemide osakonna juhataja
Maanteeamet	20.05.2020	Taavi Sepp – infotehnoloogia osakonna juhataja
		Juhan Kaarpalu – infotehnoloogia osakonna teenusehaldur
		Tea Tanner – liiklusregistri rakendusadministraator
		Oliver Karjane – süsteemiadministraator
Tervise ja Heaolu Infosüsteemide Keskus	21.05.2020	Tanel Tera – e-teenuste osakonna juhataja
		Anneli Arula – kvaliteedijuht
		Kerli Lubja – õigustalituse juhataja
Riigimetsa Majandamise Keskus	07.05.2020	Jaan Schults – IT-osakonna juhataja
		Leho Jõgi – IT-osakonna süsteemiadministraator
Elering AS	09.06.2020	Urve Aavik – IT-osakonna juhataja
TS Laevad OÜ	10.06.2020	Hanno Hussar – IT-juht
		Reimo Salumets – IT-infrastruktuuri arhitekt
MTÜ Nordic Institute for Interoperability Solutions (NIIS)	11.06.2020	Ville Sirviö – juhatuse esimees
		Petteri Kivimäki – tehnoloogiate juht
Maksu- ja Tolliamet (MTA) ning Rahandusministeeriumi Infotehnoloogiakeskus (RMIT)	12.06.2020	Anne Leisner – MTA teenuste osakonna e-büroo juht
		Tõnis Kuuse – MTA sisekontrolli osakonna juhataja
		Ingrid Tänav – MTA teenuste osakonna e-büroo teenusejuht
		Evar Ojasaar – MTA teabeosakonna andmehalduse ja arenduse valdkonna juht
		Andrus Põldpere – RMITi peaspetsialist
		Andres Klemm – RMITi infoturbe osakonna juhataja
SK ID Solutions AS	26.06.2020	Kalev Pihl – juhatuse esimees

Auditis kontrolliti RIA ja X-tee liikmete liitumiskokkulepete olemasolu. Selleks koostas Riigikontroll valimi, mis moodustas 10% X-teega liitunud asutuste üldarvust (08.09.2020. a seisuga oli X-tee liikmete üldarv 700). Välja valitud 70 asutuse ja ettevõtte puhul kontrolliti lepingute olemasolu. RIA edastas 58 asutuse ja ettevõtte liitumise kohta käivad dokumendid koos selgitustega.

Riigikontrolli järeldused eraõiguslike juriidiliste isikute kohta (nt turvameetmete rakendamine) tuginevad nii intervjuudele kui ka küsitlusele X-tee liikmete seas. Peamiselt tegelevad eraõiguslike juriidiliste isikutega andmeteenuse osutajad, kes peavad nendega sõlmima andmeteenuse kasutamise kokkulepped.

Enamiku asutustega korraldati intervjuud, osa asutusi vastas küsimustikule. Küsimustikele vastasid Keskkonnaministeerium, Kaitseministeerium, Välisministeerium, Registrite ja Infosüsteemide Keskus, Maaeluministeerium, Kultuuriministeerium, Siseministeeriumi infotehnoloogia- ja arenduskeskus ning Haridus- ja Teadusministeerium. Lisaks viidi läbi intervjuud MTÜga Nordic Institute for Interoperability Solutions (NIIS) ja ASiga SK ID Solutions.

Auditi lõpetamise aeg

Auditi toimingud lõpetati oktoobris 2020.

Auditi meeskond

Auditi meeskonda kuulusid auditijuht Toomas Viira, vanemaudiitor Alo Lääne ja audiitor Jevgeni Lazartšuk.

Kontaktandmed

Auditi kohta saab lisainfot Riigikontrolli kommunikatsiooniüksusest
tel +372 640 0704 või +372 640 0777, e-post riigikontroll@riigikontroll.ee

Auditiaruande elektrooniline koopia (pdf) on saadaval koduleheküljel www.riigikontroll.ee.

Auditiaruande kokkuvõte on saadaval ka inglise keeles.

Auditiaruande number Riigikontrolli asjaajamissüsteemis on 2-1/80053/5.

Riigikontrolli postiaadress on:

Kiriku 2/4
15013 TALLINN
Tel +372 640 0700
Faks +372 661 6012
riigikontroll@riigikontroll.ee

Riigikontrolli varasemaid auditeid infotehnoloogia valdkonnas

11.09.2019 – **Avaliku sektori tarkvaraarenduse projektide juhtimine**

14.05.2018 – **Eesti riigi kriitiliste andmekogude turvalisuse ja säilitamise tagamine**

Kõik aruanded on kättesaadavad Riigikontrolli koduleheküljelt www.riigikontroll.ee

Lisa A. Auditi käigus korraldatud küsitluse küsimused

Küsimused
1. Kas X-tee teenuste avamiseks ja kasutamiseks sõlmitakse alati andmeteenuse kasutamise kokkulepe?
2. Juhul kui kokkulepped ei ole sõlmitud, siis mis oli selle põhjuseks?
3. Kelle vahel sõlmitakse tavaliselt andmeteenuse kasutamise kokkulepped?
4. Missugused asjaolud või tingimused reguleeritakse teie andmeteenuse kasutamise kokkulepetes?
5. Millised on Teie hinnangul kõige olulisemad valitsemisala X-teed kasutavad teenused (või e-teenused)? Palun tooge kolm näidet.
6. Millist mõju avaldaks X-tee või selle komponentide mittefunktsioneerimine nimetatud teenustele?
7. Kas X-tee mittetoimimise korral on Teil olemas alternatiivne IT-lahendus? Palun tooge näide eelnevalt nimetatud näidete põhjal!
8. Kas X-tee mittetoimimisel on Teil olemas muu alternatiivne, s.t IT-st mittesõltuv lahendus (eelnevalt toodud näidete põhjal)?
9. Kas X-tee mittetoimimine on põhjustanud Teie X-teega seotud teenuste või e-teenuste kasutamisel olulisi katkestusi? Kui jah, siis palun kirjeldage, milles need seisnesid.
10. Kas olete RIAt teavitanud sellistest katkestustest?
11. Kuidas on Teie haldusalas korraldatud eraõiguslike juriidiliste isikutele teenuste avamine üle x-tee?
12. Kas Teie haldusalas sõlmitakse eraõiguslike asutustega andmeteenuse kasutamise lepingud?
13. Kas ja kuidas hindate riskide maandamiseks andmete terviklust, konfidentsiaalsust ja käideldavust tagavate meetmete rakendatust eraõiguslikes asutustes enne X-tee kaudu neile andmeteenust avades?
14. Kuidas andmeteenuse kasutamise kokkulepetes on määratud, kuidas on tagatud eraõiguslike asutuste infosüsteemi(de) järjepidev toimimine, haldamine, arendamine ning turvaline ja häireteta töö?
15. Kas ja kuidas olete kontrollinud, millist infoturbe standardit või -raamistikku eraõiguslikud asutused rakendavad?
16. Kas eraõiguslikud asutused, kellega te andmeid vahetate, on tellinud turvameetmete (infoturbe raamistike, standardite) rakendamise kohta auditeid?
17. Kas auditites on tehtud olulisi puudustele viitavaid tähelepanekuid, mis võivad ohustada X-tee teenuste kasutamist? Kui jah, siis kas Teie poolt on järgnenud sellest tingituna mingeid tegevusi?
18. Kas Teie haldusala andmeteenuseid kasutavatel eraõiguslikel asutustel on viimaste aastate jooksul esinenud probleeme X-teega või teiste X-tee osalistega andmeid vahetades? Kui jah, siis milliseid?
19. Kuidas ja millal eraõiguslikud asutused teavitavad Teid või RIAt (sh intsidentide käsitlemise osakonda) X-tee kasutamisega seonduvatest probleemidest ja asjaoludest, mis võivad mõjutada RIA või X-tee liikme kohustuste täitmist?
20. Kas Teil on X-tee arendamise ja kasutamise kohta märkusi?
21. Kas Teil on muid küsimusi või kommentaare X-tee kohta?