



TALLINNA  
TEHNIKAÜLIKOOL

# Eelanalüüs Eesti riigiasutuste turvalisele e-kirjavahetussüsteemile optimaalseima lahenduse leidmiseks

Koostanud:  
Toomas Lepik  
Jaan Priisalu  
Anna-Maria Osula  
Sten Mäses



Euroopa Liit  
Euroopa  
Regionaalarengu Fond



Eesti  
tuleviku heaks

# Sisukord

Sisukord .....	2
Kasutatud lühendid .....	4
Lühiülevaade .....	6
Sissejuhatus .....	7
1. Projekti ulatus ja meetodikad.....	8
Ulatus .....	8
Metoodikad .....	9
2. Intervjuude ülevaade .....	10
3. Hetkeolukord.....	12
Tehnilised eksperimendid .....	12
Muljed katsetustest.....	13
4. Rahvusvahelised parimad praktikad ja lahendused .....	15
Tehnilised parimad praktikad.....	15
Krüpteerimine USAs.....	17
Krüpteerimine Euroopa Liidu andmekaitstes.....	19
eIDAS määrus.....	21
5. Identifitseeritud probleemid ja probleemi täpsem püstitus .....	23
6. Võimalikud lahendused krüpteeritud sõnumite saatmiseks lõppkasutajalt lõppkasutajale .....	25
Õiguslikud aspektid.....	25
Tehnoloogilised aspektid .....	25
Idee 1 – Ühtne meiliserver.....	28
Idee 2 – S/MIME kasutamine ID-kaardi ja DNSSEC abil kui läbiva krüpteerimise lahendus .....	38
Idee 3 – DigiDoc plugin meilikliendi ja brauseri jaoks .....	45
7. Soovitavad nõuded praeguste süsteemide turvalisuse aspektide parandamiseks.....	47
SMTP TLS .....	47
IPSec kasutus .....	48
VPN organisatsioonide vahel.....	48
Must Fiiber.....	48
DNS-i turvalisuse suurendamine .....	48
Usalduse suurendamine sõnumi allika ja saaja vahel .....	49
Riigisaladuse töötlemine .....	50
Muud märkused.....	51
Lõppjärelused.....	52

Tehnilised soovitused.....	52
Mugavus.....	52
Mobiilid.....	53
Õiguslik pool.....	53
Poliitika.....	55
Lisa 1 – Intervjuude kokkuvõte .....	56
Lisa 2 – Vastused hankes esitatud küsimustele .....	60
Lisa 3 – TLS, SPF, DNSSEC analüüsi tabelid .....	62
Lisa 4 – Lahenduste võrdlustabel.....	68
Hinnang lahenduse turvalisusele.....	69
Turvalise sõnumi saatmise suunad.....	70
Haldamine .....	71
Operatsioonisüsteemid / populaarsete meiliklientide tugi .....	72

# Kasutatud lühendid

Alljärgnevalt on ära toodud valik uurimuses kasutatud olulisematest tehnilistest lühenditest.

- CA – Sertifitseerimiskeskus (ingl. k. *certification authority*); usaldatav kolmas pool avaliku võtme taristus (PKI), kes volitatud kasutajaile või süsteemidele annab välja digitaalsertifikaate, kinnitades neid digitaalsignatuuriga, ja tühistab neid<sup>1</sup>
- DNSSEC – Domain Name System Security Extensions, "domeeninimesüsteemi turvalaiendid", IETF spetsifikatsioonid (RFC 4033, RFC 4034, RFC 4035 jt), mis tagavad DNS-andmete allika autentimise, andmetervikluse ja autenditud puudumise; kaitsevad näiteks DNS-pette eest<sup>2</sup>
- DKIM – DomainKeys Identified Mail, "domeenivõtmega identifitseeritud meil"; teesklust, kalastust ja spämmi tõrjuv krüptograafiline meili autentimise meetod<sup>3</sup>
- DLP – lekketõrje, ingl. k. *data leak prevention*
- DMARC – Domain-based Message Authentication, Reporting and Conformance
- HSM – füüsiline turvamoodul<sup>4</sup>
- MDA – *mail delivery agent*
- MSA – *mail submission agent*
- MTA – *mail transfer agent*
- MUA – *mail user agent*
- Otspunktkrüpteerimine – andmete krüpteerimine lähtepunktis ja dekrüpteerimine kavatsetud sihtpunktis, ilma vahepealse krüpteerimiseta<sup>5</sup>; lõppkasutajast lõppkasutajani krüpteerimine; ingl. k. *end-to-end encryption*
- RA – Registreerimiskeskus<sup>6</sup> avaliku võtme taristus, ingl. k. *registration authority*
- SPF – ("saatjapoliitika karkass") elektronposti protokollis SMTP standardlaiend (RFC 7208, <https://tools.ietf.org/html/rfc7208>), võimaldab kontrollida saatedomeeni ehtsust<sup>7</sup>
- TLS – (Transport Layer Security, "transpordikihi turve") protokollis SSL variant, milles RSA krüptosüsteemi asemel kasutatakse Diffie-Hellmani avaliku võtmega krüptograafilist

---

<sup>1</sup> <http://akit.cyber.ee/term/560>

<sup>2</sup> <http://akit.cyber.ee/term/1061-dnssec>

<sup>3</sup> <http://akit.cyber.ee/term/9120-dkim>

<sup>4</sup> <http://akit.cyber.ee/term/1902>

<sup>5</sup> <http://akit.cyber.ee/term/693-end-to-end-encryption>

<sup>6</sup> <http://akit.cyber.ee/term/1116>

<sup>7</sup> <http://akit.cyber.ee/term/6538-spf>

süsteemi; IETFi standard (RFC 5246); võimaldab enne andmevahetust kliendi ja serveri vastastikku autentimist ning leppida kokku krüpteerimisalgoritmi ja võtmed<sup>8</sup>

---

<sup>8</sup> <http://akit.cyber.ee/term/547-tls>

# Lühiülevaade

Eelanalüüs on valminud Riigi Infosüsteemi Ameti (RIA) tellimusena. Tööd on teostatud hankelepingu nr 4.2-3/15-0677-001 alusel tellitud Euroopa Liidu (EL) struktuurifondide programmi „Nutika teenuste taristu arendamine“ raames.

Antud eelanalüüs uurib erinevaid võimalusi sõnumivahetuse turvalisemaks muutmiseks. Uurimuse käigus viidi läbi ka intervjuud riigiasutuste esindajatega. Põhirõhk on e-kirja teel saadetava info turbel, kuid lisaks uuritakse ka muid võimalusi sõnumite ja failide turvaliseks saatmiseks.

Eelanalüüsi tulemusena soovitame taristu kaitsmiseks kasutada teadaolevaid parimaid praktikaid, s.h. korrektselt rakendada TLS, SPF, DNSSEC, DKIM, DMARC. Parimatest praktikatest on täpsemalt juttu peatükis „4. Rahvusvahelised parimad praktikad ja lahendused“ (lk 15).

Lähtudes potentsiaalsest mõjuulatusest, osutusid erinevaid lahendusi analüüsid eelistatumateks kaks varianti:

- 1) S/MIME rakendamine, kasutades avaliku võtme hoidmiseks DNSSEC-iga kaitstud DNS taristut ja salajase võtmena ID-kaardil paiknevat salajast võtit.
- 2) Meiliklientidele DigiDoc Krüpto liidestuse loomine (*plugin*).

Lisaks mainitud variantidele on antud dokumendis vaadeldud ka muid lahendusi ning erinevaid teemakohaseid õiguslikke aspekte.

# Sissejuhatus

Kõrgendatud tundlikkusega dokumentide loomise käigus vahetavad riigiteenistujad omavahel suure osa infost meilidega<sup>9</sup> ja erinevates sõnumivahetus-keskkondades. Sageli ei ole selline info üksikult vaadates tundlik ega vasta asutusesiseseks kasutamiseks (AK) tunnistamiseks vajalikele tunnustele. Kui aga vaadata sellist infot üheskoos muu infovooga, siis võib tekkida olukord, kus erinevate mittetundlike infokildude kogunemine kolmandate osapoolte kätte ei ole soovitatav ning terviklikult konteksti arvestades oleks õigustatud selle klassifitseerimine piiratud juurdepääsuga teabeks. Samas on vastava olukorra õigeaegne tuvastamine raskendatud või võimatu.

Sellises olukorras on mõistlik, et võimalikult suur osa riigiasutuste vahel saadetakse infost oleks vaikumisi krüpteeritud. Paraku kasutatakse peamise sõnumiedastusvahendina meilisüsteeme, mis vaikumisi seadetes ei saada infot krüpteeritud kujul. On küll loodud erinevaid viise e-kirja teel saadatava info krüpteerimiseks, kuid neil kõigil on omad puudused. E-kirjavahetussüsteemi täies mahus asendamine spetsiaalselt turvaliseks sõnumivahetuseks loodud platvormiga on samuti keeruline, sest see on kujunenud peamiseks sõnumiedastusvahendiks asutuseväliste kontaktidega. Lisaks on meilikonto tihedalt seotud grupitöövahenditega, mis teeb omakorda keerulisemaks lõppkasutajate ümberharjutamise täiesti uutmoodi lahendusega.

Eelnevat silmas pidades on antud eelanalüüsis pakutud välja ja analüüsitud ideid olemasolevate meilisüsteemide turvalisemaks tegemiseks või turvalise sõnumivahetuse süsteemi loomiseks.

Antud dokument kirjeldab hetkeolukorda ning pakub välja kolm erinevat lahendusvarianti, samuti annab soovitusi praeguse olukorra ja süsteemi kiireks parendamiseks.

Krüpteerimine on keeruline. Seetõttu tuleb olenemata valitud lahendusest kasutajale õpetada, mis on krüpteerimine ja kuidas see töötab konkreetse lahenduse puhul. Samuti tuleks rakenduse haldaja ja lõppkasutaja õpetada lahendama võtmehaldusega seotud probleeme.

Sissejuhatavalt on veel oluline märkida, et meilisüsteemi turvalisuse tagamiseks on vaja vaadelda süsteeme tervikuna. Ükski programm üksikult ei lahenda meilivahetusega seonduvaid turvaprobleeme lõplikult.

*“Email communications cannot be made trustworthy with a single package or application. It involves incremental additions to basic subsystems, with each technology adapted to a particular task.”<sup>10</sup>*

---

<sup>9</sup> Antud töös kasutatakse mõisteid “e-kiri” ja “meil” sünonüümideks.

<sup>10</sup> NIST - SECOND DRAFT NIST Special Publication 800-177 - Trustworthy e-mail - [http://csrc.nist.gov/publications/drafts/800-177/sp800-177\\_second-draft.pdf](http://csrc.nist.gov/publications/drafts/800-177/sp800-177_second-draft.pdf)

# 1. Projekti ulatus ja metoodikad

Projekti eesmärgiks oli analüüsida erinevaid võimalusi sõnumivahetuse turvalisemaks muutmiseks.

## Ulatus

Tehnilise uurimuse esmane prioriteet on e-kirjavahetus (*e-mail*). Olulisteks teemadeks olid serverite vahelise liikluse krüpteerimine, võtmete haldus ning vaadeldi ka ligipääsu mobiilsete seadmetega.

Meilivahetuse uurimisel vaadeldakse eri suhtlussuundi ja -ulatusi:

- Riigiasutused omavahel
- Riigiasutused omavahel ja oma lepinguliste partneritega
- Riigiasutused ja residendid (s.h. kodanikud)
- Riigiasutused ja Euroopa institutsioonid
- Riigiasutused, Euroopa institutsioonid ja välised partnerid

Teine prioriteet oli lisaks meilidele muu sõnumiside uurimine – mis on kasutusel ja mida soovitada.

Kolmas prioriteet oli turvalise dokumendivahetuse uurimine.

Lisaks käsitleb käesolev eelanalüüs krüpteeritud sõnumite saatmiseks väljapakutud tehniliste lahendustega seotud õiguslikke piiranguid. Analüüs teeb ettepanekuid, millised muudatused oleksid vajalikud kehtivas regulatsioonis, et pakutud lahendusi rakendada.

RIA esindajate poolt anti viide 57 riigiasutuse domeenile. TTÜ poolt laiendati nimekirja 65 domeenini. Lisaks viidi läbi intervjuud järgnevate riigiasutuste turbeala esindajatega:

1. Siseministeeriumi infotehnoloogia- ja arenduskeskus
2. Sotsiaalministeerium
3. Keskkonnaministeerium
4. Rahandusministeeriumi infotehnoloogiakeskus
5. Justiitsministeerium
6. Politsei- ja piirivalveamet
7. Kaitseministeerium
8. Välisministeerium

Vaatluse alla kuulusid:

- Operatsioonisüsteemid: Windows, OS X, Linux, iOS, Android
- Meilikliendid: MS Outlook, Thunderbird, iOS Native Mail App

Eelanalüüsi käigus uuriti täpsemalt lahenduste kasutuselevõtu sobilikkust järgmiste piirangutega:

- Operatsioonisüsteemid: MS Windows alates versioonist 7, Linux vaatega Debian'il põhinevatele distrodele alates Debian'i versioonist 7
- Meilikliendid: MS Outlook alates versioonist 2007, iOS Native Mail App, Thunderbird alates versioonist 38.0

- Mobiilide operatsioonisüsteemid: iOS, Android

Põhjalikum testimine viidi läbi järgmiste operatsioonisüsteemidega: Windows 10, Windows Server 2008 R2, Ubuntu 15.04. Põhifookus oli meiliklientide uurimisel. Operatsioonisüsteemide eripärad antud kontekstis määravat rolli ei omanud.

Lisaks vaadeldi kolmandate osapoolte tehtud uurimusi<sup>11</sup> süsteemidega, kuhu olid paigaldatud Outlook, Thunderbird, iOS Native Mail App või Mail Reader on Android.

Vaatluse alla ei kuulunud:

- SMS ja mobiilsete täislahenduste temaatika
- Mõjuhinnangud (sh rakendamise mahud ja maksumused) planeeritud ja/või välja pakutud lahendustele
- Krüptograafiliste algoritmide süva-uuring<sup>12</sup>

Vaatluse alla ei kuulunud otseselt ka teave, mille turbetase on kõrgem kui AK, näiteks riigisaladuse ja salastatud välisteabe seaduses sätestatu, kuid kuivõrd tegu on olulise teemaga riigisutustevahelise turvalise e-kirjavahetussüsteemi kontekstis, oleme sellest tulenevaid nõuded põgusalt käsitletud.

## Metoodikad

Antud uurimuses kasutatakse järgnevaid metoodikaid analüüsi sooritamiseks:

- Struktureeritud intervjuud erinevate riigiasutuste esindajatega
- Süsteemide tehniline kaardistus
- Teadusartiklite ning õigusaktide analüüs
- Tehnilised eksperimendid (s.h. TLS, SPF ja DNSSEC implementatsiooni kontrollimine, mille tulemused on kirjeldatud Lisas 1).

Käsitluse all asuvate küsimuste uurimiseks tehti järgnevat:

- Sooritati süsteemide tehniline kaardistamine
- Kaardistati ja analüüsiti asjassepuutuvaid õigusakte ning rahvusvahelisi praktikaid
- Toodi välja võimalikud lahendused

---

<sup>11</sup> The Joys of Importing & Using an S/MIME Certificate

- [http://ccit.mines.edu/UserFiles/File/ccit/security/importing\\_and\\_using\\_smime\\_certificate-web.pdf](http://ccit.mines.edu/UserFiles/File/ccit/security/importing_and_using_smime_certificate-web.pdf)

<sup>12</sup> Sellega tegelevad ja on tegelenud teised uurimused. Näiteks:

[https://www.ria.ee/public/RIA/Krptograafiliste\\_algoritmide\\_uuring\\_2015.pdf](https://www.ria.ee/public/RIA/Krptograafiliste_algoritmide_uuring_2015.pdf)

## 2. Intervjuude ülevaade

Eelanalüüsi käigus viidi läbi 8 intervjuud erinevate riigiasutuste IT-turbe spetsialistidega. Intervjuude struktuur ja kogutud info on täpsemalt ära toodud peatükis Lisa 1 – Intervjuude kokkuvõte.

Eraldi välja toomist vääriksid järgmised punktid:

- Kasutajamugavus on äärmiselt kõrgelt hinnatud. Kasutajamugavust defineeriti üldiselt kui lõppkasutaja lisategevuste hulka, mis teatud lahendusega kaasneksid. Eelistatakse lahendusi, mis toimiksid tavakasutajale nähtamatult või minimaalset lisategevust nõudvana.
- Asutustel on probleemiks konfidentsiaalsete andmete saatmine ja vastu võtmine, kui teiseks pooleks on ilma ID-kaardita isik. Kui mõlemal osapoolel on ID-kaart, siis kasutatakse laialdaselt CDOC krüpteerimislahendust.
- ID-kaardil põhinevat autentimist kasutatakse ka sageli VPN-ühenduse loomisel.
- Mobiilsete seadmetega on mitmeid probleeme. Mitmed intervjuueeritud asutused uurivad aktiivselt lahendusi mobiilsete seadmete haldamiseks, aga keegi veel kesket haldust loonud pole.

Intervjuude käigus asutuste poolt tõstatatud probleemsed kohad, millele oodatakse lahendust, on pikemalt ära toodud peatükis „Lisa 1 – Intervjuude kokkuvõte“, punktis 9 (lk 56).

Eesti riigiasutustes enam kasutatavad meilikliendid ning meilisisu krüpteerimisega seotud teemadest on rohkem juttu peatükis “3. Hetkeolukord”.

Intervjuus osalenutele saadeti ka küsimus intsidentide arvu kohta järgnevates valdkondades:

- 1) Võlts-meili saatmine
  - Meili päise võltsimine
  - Saatja võltsimine ja vastuste teisele meilile küsimine (seda nii kirja sisus kui ka „reply-to“ abil)
  - Sarnase domeeni nime kasutamine
  - Läbi "avatud" serverite saates (kogu kiri on ise võlts, aga usaldus saavutatakse kirja sisus oleva teksti abil)
- 2) Vahendusrünne
  - DNS-i nime hõive teel
  - DNS-i MX kirje manipuleerimine DNS-pette ründe teel
  - Kirjavigade ära kasutamise teel
- 3) Vahetu võrgu pealt kuulamine / vahendusrünne
  - BGP mürgitamise abil
  - Füüsilise ligipääsu abil
- 4) Tulemüüri ära kasutamine / vahendusrünne
  - Privilegeeritud ligipääs
  - Sissemurdmine, ülevõtmine
- 5) Meililüüsi / lüüsi ära kasutamine / vahendusrünne
  - Privilegeeritud ligipääs
  - Sissemurdmine, ülevõtmine
- 6) Meiliserveri ära kasutamine

- Privilegeeritud ligipääs
  - Sissemurdmine, ülevõtmine
- 7) Ligipääs kasutaja töölauale (*desktop*)
- Privilegeeritud ligipääs
  - Sissemurdmine, ülevõtmine
- 8) Veebimeilile ligipääs/ebaturvaline kasutamine
- Sissemurdmine, ülevõtmine (k.a. suisa <http://> kasutamine)
- 9) Teenuse tõkestusrünne (DoS/DDoS)

Intsidentide arvu osas vastust üheltki asutuselt ei tulnud.

CERT-EE andmetel oli registreeritud meilidega seonduvaid juhtumeid 2015. aastal 64 ja 2016. aastal esimeses kvartalis 65 korda. CERT-EE ei kategoriseeri intsidente sedavõrd täpselt, kui antud uurimuse käigus küsiti. CERT-EE antud numbrid ei sisalda teenust tõkestavaid ummistusründeid meilisüsteemidele (DDoS). Samuti ei ole CERT-EE-le otseselt teada „*desktop*’i ligipääse“.

Lisaks tuleks mainida, et me räägime tervikluse, konfidentsiaalsuse ja käideldavuse võimalikest kadudest. Sealjuures tuleb konfidentsiaalsuse kao õigeaegseks avastamiseks teha suuremaid jõupingutusi ning muuta organisatsioonide tööd. See omakorda loob täiendava vajaduse korraliku logihalduse olemasolule ning infosüsteemi arhitektuuri heale disainile.

### 3. Hetkeolukord

Intervjuudest selgus, et käesolevas uuringus vaadeldud organisatsioonides kasutatakse järgnevad meilikliente:

- MS Outlook – kasutusel hinnanguliselt üle 78 % keskvalitsuse asutuste arvutitest
- MS Outlook Web Application
- GroupWise klient
- Apple Native Mail App
- Android Email App
- Android Gmail App
- Thunderbird
- Apple Mail

Tarkvara tegelikku kasutust ja litsentse tuleb täpsustada tarkvara auditiga.

Otspunktkrüpteerimiseks ehk lõppkasutajalt lõppkasutajale krüpteerimiseks (*end-to-end encryption*) kasutatakse e-posti sõnumisisu krüpteerimist.

#### **Sõnumisisu krüpteerimise lahendustest on kasutatavad järgmised:**

- CDOC konteiner
- GnuPGP – välisel suhtlusel vähesel määral
- ACID – Suhtlus EL suunal<sup>13</sup> (saadetakse sõnumeid kuni tasemega EL Piiratud)
- Väliste osapooltega on kasutusel ka parooliga ZIP konteiner koos AES krüpteerimisega, kusjuures parooli edastatakse kas varem või hiljem ja eelistatult muud kanalit mööda.

### Tehnilised eksperimendid

Tehniliste eksperimentide käigus uuriti skoobis olevate asutustega seotud domeenide ja meiliserverite seadistusi.

Meiliserverites jookseb suuremal enamusel MS Exchange, versioonid 2007-2013.

Tervikluse tõenäosuse suurendamiseks ja rämpsposti vähendamiseks ettenähtud SPF kirjed on rakendatud 26 domeenil 65-st 24. märtsi (2016. a) seisuga.

Tervikluse ja konfidentsiaalsuse parandamiseks kasutatav DNSSEC on rakendatud 7 domeenil 65-st 24. märtsi (2016. a) seisuga.

---

<sup>13</sup> <http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/eu-restricted/offline-file-encryptor/acid-cryptofiler-v7/>

Vaadeldud domeenidel oli kirjeldatud 42 erinevat MX ehk meiliserveri kirjet, millele vastas 39 unikaalset IP-d ja millest täiesti korrektselt vastas STARTTLS-ile 13 otspunkti ning 10 teavitas, et TLS-i ei toetata.

Täpsem info on toodud välja peatükis Lisa 3 – TLS, SPF, DNSSEC analüüsi tabelid.

Hetkel kasutusel olevate meiliklientide ja tehnoloogiate kasutamisest paremaks arusaamiseks teostasime järgmisi katsetusi:

- OpenPGP kasutamine Thunderbird'iga
- OpenPGP kasutamine Outlook'iga
- Sertifikaadi taotlemine kolmanda osapoole CA-lt (<https://www.startssl.com/>)
- Krüpteeritud sõnumi saatmise ja saamise testimine soft-sertifikaadiga Outlooki'iga
- Krüpteeritud sõnumi saatmise ja saamise testimine soft-sertifikaadiga Thunderbird'iga
- Kataloogi kasutamine Active Directory keskkonnas sertifikaadi leidmiseks Outlook'iga
- Outlooki testimine ID-kaardiga
- Thunderbird'i testimine ID-kaardiga
- SK halduses oleva LDAP kataloogi kasutamise testimine<sup>14</sup>

OS X ning iOS platvormide osas piirdusid eksperimendid kolmandate osapoolte uurimuste ja materjalide läbi töötamisega.

Testis kasutati järgmisi tarkvara versioone: Windows 8.1, Windows 10, Windows 2012 server, Exchange 2013, Office 365, Office 2013, Office 2016, Linux Ubuntu 15.10, Thunderbird 3.8, Enigmail 1.9.2, Gpgwin 2.3.0.

## Muljed katsetustest

OpenPGP sertifikaatide genereerimine on tehnilise spetsialisti jaoks lihtne pärast vastava lisatarkvara paigaldamist.<sup>15</sup>

Thunderbird'ile piisab pistikprogrammist ning Thunderbird'i laiendamine ei eelda haldusülesannetega eeliskasutaja õigusi.

Vabavaralistest vahenditest sai katsetatud Windowsi keskkonnas suuremahulist tarkvarakomplekti Gpg4win<sup>16</sup>, mille paigaldamine eeldab kasutajalt arvuti haldusõigusi. Antud tarkvarakomplekti valmisversioonil tuvastati probleem 64-bitise Outlooki toega. Automaatne krüpteerimine ja dekrüpteerimine läbi Outlook'i ei ole võimalik. Küll aga on võimalik saadetud sõnumi sisu lahti krüpteerida vastavat installeeritud programmi kasutades.

Tehniline spetsialist saab sertifikaadi taotlemisega hakkama, kuid tavakasutaja jaoks võib

---

<sup>14</sup> <https://sk.ee/repositoorium/ldap/ldap-kataloogi-kasutamine/ldap-kataloogi-kasutamine>

<sup>15</sup> <https://courses.cs.ut.ee/2016/infoturve/spring/Et/PGP>

<sup>16</sup> <https://www.gpg4win.org/download.html>

sertifikaatide konteinerite vaheline tegutsemine ilma õpetusteta osutada probleemseks. Samas on Active Directory keskkonnas võimalik automaatselt väljastada lokaalseid tarkvaralisi sertifikaate.

Outlooki häälestamine sertifikaadi kasutuseks on tehnilisele spetsialistile lihtne ja seda saab teha ka keskselt administratiivseid malle kasutades.<sup>17</sup>

Sõnumi saatmine Outlookiga kulges probleemideta. Saatmiseks tuleb kas Outlook häälestada automaatse krüpteerimise peale või teha minimaalselt kolm hiireklõpsu lisaks.

Thunderbirdi häälestamine sertifikaadiga sõnumi saatmiseks oli tehnilisele spetsialistile lihtne.

AD kasutamine kataloogina (kui sinna publitseeritakse sertifikaat) on lihtne ja toimub kasutaja jaoks automaatselt.

Välise LDAP-i kasutus nõuab häälestust, kuid on tehnilise spetsialisti jaoks lihtne. LDAP eeldab tavaotsingu terminina kas kasutajanime või meiliaadressi otsingut.

ID-kaardi ühendamise Outlooki oli lihtne, kuid siin tuleb mainida vajadust lisada @eesti.ee konto ja lubada SMTP-serveril selle konto nimelt saatmine selleks, et krüpteerimine tavaolukorras töötaks.

Kui me soovime @eesti.ee aadressi sisaldavat sertifikaati kasutada mõne teise meiliaadressi alt, siis lõhub see tervikluse, kuid lubab andmeid krüpteerida. Selleks tuleb muuta Outlooki käitumist läbi Windowsi registri.<sup>18</sup>

Thunderbirdi häälestamine ID-kaarti kasutamiseks oli [www.id.ee](http://www.id.ee) portaalis antud juhiste abil<sup>19</sup> spetsialistile jõukohane. Tuli arvestada ainult 64-bitise süsteemi eripäradega ja sellest tingitud failiasukoha muutusega.

Krüpteeritud sõnumi saatmisel tuleb arvestada @eesti.ee e-posti aadressi piirangut ja SMTP-serveri poolsete võimalike piirangutega saatja ja saadetava sõnumi suhtes.

---

<sup>17</sup> <https://technet.microsoft.com/en-us/library/cc179061.aspx>

<sup>18</sup> <https://support.microsoft.com/en-us/kb/2497165>

<sup>19</sup> <http://www.id.ee/?id=34232>

## 4. Rahvusvahelised parimad praktikad ja lahendused

### Tehnilised parimad praktikad

Seoses Snowden'i paljastustega NSA tegevuse kohta on teadmine e-kirjade krüpteerimisvajadusest jõudnud suurema hulga inimesteni. Sellest tulenevad ka uued teenused nagu ProtonMail ja Lavabit, millest viimase loojad arendasid välja DIME (Dark Mail<sup>20</sup>), mis on huvitav kontseptsioon, kuid antud kontekstis liiga toores, et seda lahendusena välja pakkuda. Tulevikus võiks kaaluda nimetatud kontseptsiooni arendusse investeerimist.

Meilivahetuseks vajaliku taristu arhitektuur on kompleksne ja krüpteerimise korrektne rakendamine on keeruline. Seetõttu keskenduvad enamik uuritud parimatest praktikatest soovitudele ja nõuetele olemasoleva meilitaristu ja taristu arhitektuuri parandamiseks ja serveritevahelise liikluse krüpteerimiseks (ISKE<sup>21</sup>, BSI<sup>22</sup>, NIST<sup>23,24</sup>, CTS<sup>25</sup>), tuues välja otspunktkrüpteerimise vajaduse ja võimaluse.

Olemasoleva arhitektuuri parandamisel soovitatakse vähendada ohtu, et organisatsiooni kasutuses olev domeen oleks soovimatult seotud spämmikampaaniatega. Soovitatakse kasutada SPF, DKIM ja DMARC teenuseid, et võimaldada soovi korral sõnumi saatja tuvastamine ning sõnumi terviklus.

Serveritevahelise krüpteerimise lahenduseks pakutakse välja TLS-i kasutamist (SMTP protokoll transpordikihi tasemel turvamine) ning sama organisatsiooni piires VPN ja/või IPsec kasutamist.

Tasub ära märkida, et SMTP jaoks TLS-i rakendamine sõltub paljustki organisatsioonidevahelistest kokkulepetest. Kokkulepete puudumisel on võimalik kasutada süsteemi vastu madaldusrünnet (krüpteeritud ühenduse asemel lepitakse tavalise SMTP-ga).<sup>26</sup> Organisatsioonidevaheliste kokkulepete olemasolul võib kasutada ka IPsec-i, mis aitab turvata kogu organisatsioonidevahelist kommunikatsiooni.

Serveritevahelise liikluse krüpteerimise ja saatja serveri tuvastamise praktikad on selgelt hakanud toetama ka Google ning serveritevahelise andmevahetuse krüpteerimise puudumisest on hakatud teavitama ka tavakasutajaid.<sup>27</sup>

Otspunktkrüpteerimise juures räägitakse enamjaolt kahest lahendusest:

---

<sup>20</sup> <https://darkmail.info/spec>

<sup>21</sup> <https://www.ria.ee/iske>

<sup>22</sup> <https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html>

<sup>23</sup> Guidelines on Electronic Mail Security - <http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf>

<sup>24</sup> Guidelines on Electronic Mail Security (Second Draft) - [http://csrc.nist.gov/publications/drafts/800-177/sp800-177\\_second-draft.pdf](http://csrc.nist.gov/publications/drafts/800-177/sp800-177_second-draft.pdf)

<sup>25</sup> <https://www.gov.uk/guidance/common-technology-services-cts-secure-email-blueprint>

<sup>26</sup> Redirecting and modifying SMTP mail with TLS session renegotiation attacks - <http://www.porcupine.org/postfix-mirror/smtp-renegotiate.pdf>

<sup>27</sup> <https://support.google.com/mail/answer/6330403>

1) S/MIME, mis versioonina 3.2 on staatuses PROPOSED STANDARD<sup>28</sup>

2) OpenPGP, mis on samuti staatuses PROPOSED STANDARD<sup>29</sup>

Mõlemad lahendused keskenduvad meilisõnumi sisu kaitsele, jättes täielikult välja sõnumi metaandmed ehk saatja, saaja ja sõnumi pealkirja – arvestades, et seda infot kaitstakse serveritevahelist liiklust krüpteerides.

Tegevus	S/MIME	OpenPGP
Võtme loomine	Kasutaja saab tööandja või CA käest X.509 sertifikaadi.	Kasutajad loovad ise oma avalike ja privaatvõtmete paarid ning lasevad need teistel kasutajatel kinnitada.
Sertifikaadi verifitseerimine	PKI: Sertifikaadid verifitseeritakse usaldatud juursertifikaatide abil, mis on paigaldatud kasutaja arvutisse.	Usaldusvõrgustik: Suvaline hulk kasutajaid saab võtmeid verifitseerida. Kasutajad teevad turvaotsuseid vastavalt sellele, kas nad usaldavad võtmete allkirjastamiseks kasutatud võtmeid.
Sertifikaadi tühistamine	Sertifikaate tühistamine käib nende väljastaja või CA kaudu.	Sertifikaate saab tühistada ainult avaliku võtme omanik.
Avalike võtmete turvaline omandamine meilikliendi poolt	Kaks erinevat võimalust:  1) Meiliklient saadab vastava päringu sertifikaatide kataloogi suunas (LDAP või DNS).  2) Kasutaja saab teiselt osapoolelt allkirjastatud (Eesti seaduse kohaselt ei ole antud juhul tegu digiallkirjaga) meili, milles sisaldub teise osapoolse sertifikaat.  Meilisüsteem saab automaatselt kontrollida sertifitseerimisteenuse pakkuvalt sertifikaadi usaldusväarsust.	Kaks erinevat võimalust:  1) PGP avalike võtmete serveri või lisakanali kaudu (nt avaliku võtme veebilehel avaldamine).  2) Kasutaja saab teiselt osapoolelt allkirjastatud (Eesti seaduse kohaselt ei ole antud juhul tegu digiallkirjaga) meili, milles sisaldub teise osapoolse sertifikaat.
Meilikliendipoolne tugi E-kirja kliendi poolne tugi	Enamikes Eesti riigiasutustes kasutusel olevates meiliklientides on S/MIME funktsionaalsus sisse ehitatud.	Funktsionaalsus tuleb enamusele Eesti riigiasutustes kasutusel olevatele meiliklientidele eraldi installeeritava tarkvara abil lisada.

<sup>28</sup> <https://tools.ietf.org/html/rfc5751>

<sup>29</sup> <https://tools.ietf.org/html/rfc4880>

DNSSEC-i tugi	Draft <sup>30</sup> Using Secure DNS to Associate Certificates with Domain Names For S/MIME	Draft <sup>31</sup> Using DANE to Associate OpenPGP public keys with email addresses
---------------	---	--

Nimetatud krüpteerimislahenduste juures ei vaadelda, kuidas kasutajat krüpteerimisest selgelt teavitada. Pigem jäetakse see meilikliendi ülesandeks, esitades samas meilikliendile tehnilisi nõudeid selle kohta, kuidas töödelda sõnumeid.

Meilisüsteemi turvalisuse rakendamisel ja lõppkasutajalt lõppkasutajale krüpteerimist rakendades tuuakse välja korduvalt samad probleemsed kohad:

- DNS
- süsteemi keerukus
- võtmehaldus
- kasutaja võime krüptosüsteemi kasutada
- selge süsteemipoolne kommunikatsioon

DNS ei ole turvaline ilma DNSSEC-ta. DNS-i ohustab näiteks nimehõiverünne.

Süsteemi loetakse keerukaks, sest meilisüsteem koosneb rohkematest osapooltest kui pelgalt klient ja server.

Selge süsteemipoolne kommunikatsioon kasutaja suunal on vajalik, et selgitada kasutajale, kas süsteem tegeleb või ei tegele vastava e-kirja krüpteerimisega („Why Johnny Can’t encrypt“<sup>32</sup> ja „Limitations of S/MIME“<sup>33</sup>).

Tuuakse välja, et subjektiivsele turvalisusele ja vigade vähendamisele töödeldavate andmete kategoriseerimisel aitab pigem kaasa krüpto-operatsioonide tegemine väljaspool sõnumivahetuskeskkonda.<sup>34</sup>

## Krüpteerimine USAs

Lisaks parimatele praktikatele uuriti käesolevas uurimuses ka erinevate asutuste praktilisi krüpteerimisnõudeid. Näiteks USA tervishoiuasutustele on esitatud kindlad nõuded patsiendiga seotud info vahendamiseks ja käitlemiseks. Räägitakse ka vajadusest andmeid krüpteerida. Erinevad asutused on lähenenud sellele probleemile erinevalt. Mõned näiteks on toonud informatsiooni sõnumivahetus-kanalist välja ning saadavad vajadusel kasutajale veebilinki, millele kasutaja saab

<sup>30</sup> <https://datatracker.ietf.org/doc/draft-ietf-dane-smime>

<sup>31</sup> <https://tools.ietf.org/html/draft-ietf-dane-openpgpkey-12>

<sup>32</sup> [http://www.cs.berkeley.edu/~tygar/papers/Why\\_Johnny\\_Cant\\_Encrypt/OREilly.pdf](http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OREilly.pdf)

<sup>33</sup> A. Levi and C. B. Güder, “Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach,” *Computers & Security*, vol. 28, no. 3–4, pp. 105–120, May 2009.

<sup>34</sup> Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes  
[http://cups.cs.cmu.edu/soups/2013/proceedings/a5\\_Ruoti.pdf](http://cups.cs.cmu.edu/soups/2013/proceedings/a5_Ruoti.pdf)

ligi eelnevalt jagatud parooli abil. Samuti jagavad mõned asutused kasutajale ühe- või mitmekordseks kasutamiseks vajalikke krüptovõtmeid.

Rahvusvahelisi praktikaid uurides tuleb tõdeda, et olukord Eestis on ainulaadne, sest kõiki residente hõlmav PKI on väga laialdaselt kasutusel. Teistes riikides nii laialdast sektoriteülest kasutust ei ole või ei peeta seda isegi võimalikuks. Nt USA NIST raport turvalisest meilivahetusest<sup>35</sup> keskendub olukorrale, kus kõiki residente hõlmav PKI ei ole realistlik.

USA meditsiiniliste isikuandmete käitlemist reguleerib HIPAA<sup>36</sup>. Meili teel jagatava info konfidentsiaalsust on USA kontekstis raske tagada, seega kasutatakse HIPAA sätestatud karmide nõuetega toime tulekuks järgnevaid meetodeid.

- Kasutajale antakse ligipääs veebiportaale temaga eelnevalt kohtudes.
- Kasutajale antakse krüpto-võtmed temaga eelnevalt kohtudes.
- Kasutajale jagatakse infot läbi spetsiaalse rakenduse (nt mobiiliäpp).
- Parool saadetakse läbi teise kanali (nt SMS).

Kasutajaga delikaatsete andmete jagamine toimub sageli läbi kolmandate osapoolte ehk läbi vastavat teenust pakkuvate organisatsioonide.<sup>37</sup>

USA sõjaväes on kasutusel Common Access Card (CNC)<sup>38,39</sup>, millel asuvaid võtmeid muuhulgas kasutatakse ka krüpteeritud meilide saatmiseks. CNC antakse välja ainult lepingulise koostöö korral USA sõjaväega. Vastavad meiliaadressid on @mail.mil lõpuga. CNC ümber loodud arhitektuur võimaldab otspunktkrüpteerimist. CNC jaoks kasutatav CA ei ole meilientide ja brauserite usaldusväärses CA listides.

CNC-le on paigutatud kolm krüpto võtit autentimise, allkirjastamise ja meili krüpto jaoks, kusjuures meili krüpto jaoks kasutatav võtmepaar on arhiveeritud kaardist väljas pikaajalise e-postile ligipääsu tarbeks.

Meilide krüpteerimiseks kasutatakse S/MIME standardset lahendust ning arvestada tuleb sellega, et sõjaväe (sh USA sõjaväe) eripäraks on võimalus muudatusi jõuga läbi suruda ning seda ei saa seetõttu otseselt võrrelda teiste riigiasutustega.

Kui USA õiguslikuks eripäraks on sektorialne regulatsioon, siis Euroopa riikide õiguskord eelistab valdkondadeülest lähenemist.

---

<sup>35</sup> [http://csrc.nist.gov/publications/drafts/800-177/sp800-177\\_second-draft.pdf](http://csrc.nist.gov/publications/drafts/800-177/sp800-177_second-draft.pdf)

<sup>36</sup> <http://whatishipaa.org/>

<sup>37</sup> Nt CryptnSend - <https://cryptnsend.com/howitworks.html>

<sup>38</sup> <http://www.cac.mil/common-access-card/>

<sup>39</sup> <http://www.gemalto.com/brochures/download/dod.pdf>

## Krüpteerimine Euroopa Liidu andmekaitstes

EL õigus ei maini otsesõnu riikliku e-kirjavahetussüsteemi või üldise krüpteerimise kohustuslikkust.<sup>40</sup> Laiem kohustus isikuandmeid kaitsta (sealhulgas nende terviklikkust) tuleneb EL andmekaitseraamistikust, mille põhimõtted peegelduvad siseriiklikes isikuandmete kaitse seadustest ning sisaldavad kohustust kaitsta andmesubjekti õigusi isikuandmete töötlemisel.

Laiulatusliku andmekaitse reformi tulemusena on vastsetl jõustunud “*Euroopa Parlamendi ja Nõukogu Direktiiv 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK*” (edaspidi direktiiv).<sup>41</sup> Kuivõrd direktiiv keskendub pädevate asutuste poolt isikuandmete töötlemisele süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, siis detailsemat analüüsi instrument käesoleva eelanalüüsi kontekstis ei leia. Küll aga tasub välja tuua direktiivist nähtuvad sätted, kus käsitletakse direktiivi reguleerimisalas krüpteerimist isikuandmete töötlemisel.

Direktiiv selgitab:

“Turvalisuse tagamiseks ja käesolevat direktiivi rikkuva töötlemise vältimiseks peaks vastutav töötleja või volitatud töötleja hindama töötlemisega seotud ohtusid ja rakendama asjaomaste ohtude leevendamiseks meetmeid, näiteks krüpteerimist. Selliste meetmetega tuleks tagada vajalik turvalisuse tase, sealhulgas konfidentsiaalsus, ja võtta arvesse teaduse ja tehnoloogia viimast arengut, ohule vastavaid rakenduskulusid ja kaitstavate isikuandmete laadi. Andmeturbeohtusid hinnates tuleks kaaluda isikuandmete töötlemisest tulenevaid ohtusid, nagu edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhuslik või ebaseaduslik hävitamine, kaotsimine, muutmine või loata avalikustamine või neile juurdepääs, mille tagajärjel võib eelkõige tekkida füüsiline, varaline või mittevaraline kahju. Vastutav töötleja ja volitatud töötleja peaksid tagama, et isikuandmeid ei töötle volitamata isikud.” (direktiivi p 60)

Sellest lähtuvalt paneb direktiiv liikmesriikidele kohustuse direktiivi reguleerimisalas isikuandmeid töödelda viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid (direktiivi artikkel 4 lg 1 f). Kuigi nimetatud norm krüpteerimise kohustuslikkust ei sätesta, on selge, et krüpteerimist peetakse üheks vahendiks,

---

<sup>40</sup> Siseriiklikus õiguses on näiteid, kus teatud piiratud tingimustel on krüpteerimine kohustuslik. Näiteks Itaalia andmekaitse seaduses sisaldub põhimõte, mille alusel on delikaatsete isikuandmete töötlemisel kohustus need krüpteerida või kasutada muid lähenemisi, mis lubaksid andmesubjekti isikustamise ainult konkreetse vajaduse korral. Data Protection Code - Legislative Decree no. 196/2003, <http://www.garanteprivacy.it/garante/document?ID=4814258>, seksioon 22 (6)

<sup>41</sup> Direktiiv sätestab artiklis 63 lg 1, et: “Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid hiljemalt 6. mail 2018. /.../”. Euroopa Parlamendi ja Nõukogu Direktiiv 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, <http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016L0680&from=EN>

millega direktiivi rikkuvat töötlemist vältida.

Lisaks eelnevale mainitakse direktiivis krüpteerimist vaid andmesubjekti teavitamise kohustuse kontekstis. Nimelt lisab direktiivi artikkel 31 kohustuse vastutavale töötlejale teavitada andmesubjekti põhjendamatu viivitusega seotud rikkumisest, kui isikuandmetega seotud rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele, välja arvatud juhul, kui vastutav töötleja on rakendanud asjakohaseid tehnoloogilisi ja korralduslikke kaitsemeetmeid ning neid kohaldati isikuandmetega seotud rikkumisest mõjutatud isikuandmetele, kasutades eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsuõigusega isikutele loetamatuks (näiteks krüpteerimine) (direktiivi artikkel 31 lg 3 a).

Lisaks uuele direktiivile on jõustunud ka “*Euroopa Parlamendi ja Nõukogu Määrus 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta*”<sup>42</sup> ehk isikuandmete kaitse üldmäärus (edaspidi üldmäärus), mis kohaldatakse alates 25. maist 2018 (üldmääruse artikkel 99 lg 2). Käesolevas eelanalüüsi läbiviimisel lähtutakse küll eelkõige kehtivast riiklikust isikuandmete kaitse seadusest, kuid käsitletakse ka 2018. aastal kohaldatava üldmääruse asjakohaseid norme.

Üldmäärus tunnistab krüpteerimist kui ühte meetet üldmääruses kehtestatud isikuandmete töötlemise rikkumise vältimiseks. Üldmäärus selgitab:

“Turvalisuse tagamiseks ja käesolevat määrust rikkudes sooritatava töötlemise vältimiseks peaks vastutav töötleja või volitatud töötleja hindama töötlemisega seotud ohtusid ja rakendama asjaomaste ohtude leevendamiseks meetmeid, näiteks krüpteerimist. Võttes arvesse teaduse ja tehnoloogia viimast arengut ja meetmete rakenduskulusid, tuleks kõnealuste meetmetega tagada vajalik turvalisuse tase, sealhulgas konfidentsiaalsus, mis vastaks ohtudele ja kaitstavate isikuandmete laadile. Andmeturbeohtu hinnates tuleks kaaluda isikuandmete töötlemisest tulenevaid ohte, nagu edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhuslik või ebaseaduslik hävitamine, kaotamine, muutmine ja loata avalikustamine või neile juurdepääs, mille tagajärjel võib eelkõige tekkida füüsiline, materiaalne või mittemateriaalne kahju.” (üldmäärus p 83)

Asjakohaste kaitsemeetmete olemasolu (sh krüpteerimist) võetakse arvesse teatud juhtudel ka siis, kui vastutav töötleja peab kindlaks tegema, kas muul eesmärgil töötlemine on kooskõlas eesmärgiga, mille jaoks isikuandmeid algselt koguti (üldmääruse artikkel 4 e). Üldmäärus märgib eelpool nimetatud direktiiviga sarnaselt krüpteerimise ära ka olukorras, kui andmesubjekti tuleb teavitada isikuandmetega seotud rikkumisest (üldmäärus artikkel 34 lg 3 a).

Kui nimetatud kaks üldmääruses krüpteerimise mainimist ei pruugi antud konteksti olla esmase tähtsusega, siis üldmääruse artikkel 32 sätestab selgelt krüpteerimise rolli EL isikuandmete kaitses. Üldmääruse artikkel 32 lg 1 selgitab, et “võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmarke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele”, võivad vastutav töötleja ja volitatud töötleja ohule vastava turvalisuse taseme tagamiseks rakendada

---

<sup>42</sup> Euroopa Parlamendi ja Nõukogu Määrus 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta, <http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

asjakohaseid tehnilisi ja korralduslikke meetmeid. Üheks loetletud meetmeks, mille abil tagada isikuandmete töötlemise turvalisus, on ka krüpteerimine (üldmääruse artikkel 32 lg 1 a). Artikkel ei muuda krüpteerimise kasutamist kohustuslikuks, vaid nimetab seda ühe võimaliku meetmena, mida võib kasutada vastavalt vajadusele.

Uue andmekaitseraamistiku mõju krüpteerimise rollile andmete kaitse ja terviklikkuse tagamiseks siseriiklikus õiguses näeme reaalsuses ilmselt kahe aasta pärast, kui nimetatud normid kohaldatakse.

## eIDAS määrus

Märkimisväärselt on EL astunud ka konkreetseid samme turvalise e-identimise (sealhulgas elektrooniliste andmete päritolu ja tervikluse kinnitamist võimaldavate lahenduste) riikideülese reguleerimise vallas. Selle parimaks näiteks on Euroopa Parlamendi ja Nõukogu määrus nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (nn eIDAS määrus).<sup>43</sup> Hetkel on Eestis arutusel juba Euroopa Parlamendi ja nõukogu määruse nr 910/2014 „e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul“ rakendamise seaduse eelnõu.<sup>44</sup>

Määruse eesmärgiks on saavutada e-identimise vahendite ja usaldusteenuste asjakohane turvalisuse tase ning selle tagamiseks luuakse õigusraamistik e-allkirja, e-templi, e-ajatempli, e-dokumentide, registreeritud e-andmevahetusteenuste ja veebisaitide autentimise sertifitseerimisteenuste jaoks.

Kuigi määrus otsesõnu e-kirjavahetussüsteemide krüpteerimist ei maini, tuleb antud eelanalüüsi kontekstis vaadelda määruse üldist eesmärki, milleks on e-autentimine ehk elektrooniline protsess, mis võimaldab füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja tervikluse kinnitamist. Samuti võib olla huvipakkuv määruses sisalduv termin „registreeritud e-andmevahetusteenus“, mis märgib teenust, mille abil saab kolmandate isikute vahel edastada elektrooniliselt andmeid, tõendada edastatud andmete käitamist, sealhulgas andmete saatmist ja kättesaamist, ning kaitsta edastatud andmeid kadumise, varguse, kahjustamise või lubamatu muutmise eest”.<sup>45</sup>

Antud kontekstis on oluline rõhutada, et määrus ei sekku riikide õigusesse korraldada siseriiklikku isikutuvastamist vaid reguleerib nimetatud teenuste piiriülest toimimist.

Ka Euroopa Komisjoni siseregulatsioon on 2008. aastal pakkunud välja suunised turvaliseks sõnumivahetuseks väliste osapooltega<sup>46</sup>. Vastaval juhul pidas Komisjon põhimõtteliselt ise oma CA-d üleval ning jagas kolmandatele osapooltele tehnilist nõu, kuidas võtta S/MIME-t kasutusele. Lisaks kasutatakse ACID dokumendi konteineri standardit<sup>47</sup> sellise suhtluse tarbeks, kus eelnevalt

---

<sup>43</sup> Euroopa Parlamendi ja Nõukogu määrus nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul, <http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910&from=ET>

<sup>44</sup> Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 „e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul“ rakendamise seaduse eelnõu, 27.04.2016. Leitav eelnõude andmebaasist.

<sup>45</sup> Euroopa Parlamendi ja Nõukogu määrus nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul, artikkel 3, p 36

<sup>46</sup> <http://ec.europa.eu/competition/contacts/encryption.pdf>

<sup>47</sup> <http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/eu-restricted/offline-file-encryptor/acid-cryptofiler-v7/>

on teise osapoole usaldusväärsus kontrollitud.

## 5. Identifitseeritud probleemid ja probleemi täpsem püstitus

Peamise probleemina on RIA tõstatanud sõnumivahetuse konfidentsiaalsuse tagamise vajaduse, mis eelistatult toimuks tavakasutaja jaoks võimalikult lihtsalt.

Intervjuudest tuli välja vajadus tagada sõnumites ja sõnumi manustes lisaks terviklus ja salgamatus<sup>48</sup>.

Tuleks vaadelda sõnumisaladuse tagamist kahel tasemel: esmalt serverite vahel ja siis lõppkasutajalt lõppkasutajale tasemel.

Serveritevahelise ühenduse turvalisuse tagamiseks eeldatakse lisaks serverite ja võrgu häälestamisele ka organisatsioonilisi kokkuleppeid.

Lõppkasutajalt lõppkasutajale krüpteerimise puhul on kasutajal vaja tarkvara (nt meiliklient), millega krüpteeritud sõnumit saata ja vastu võtta. Krüpteeritud sõnumi saatmiseks on lisaks krüpteerimisvõimelisele meilikliendile tarvis võtmehaldust.

Standardolukorras võib kasutada avaliku ja salajase võtmega krüptosüsteemi. Selles süsteemis peab krüpteerija kuskilt saama teise osapoole võtme krüpteerimisoperatsiooni teostamiseks.

Krüpteeritud sõnumi saatjal peab olema võimalus veenduda saatja võtme autentsuses.

Sertifikaadid, mis sisaldavad avalikku võtit, võivad sisaldada isiklikku informatsiooni. Näiteks korrektselt X.509 vormingus välja antud sertifikaadid sisaldavad isikuandmeid. Sellega võivad kaasneda õiguslikud piirangud sertifikaatide töötlemisel.

Lisaks võib tehniliste lahenduste rakendamine kaasa tuua ka kehtiva regulatsiooni täiendamist.

Tuleb ka nentida, et praegune alternatiiv sõnumi krüpteerimiseks, milleks on CryptoDoci kasutamine, ei ole sobilik. Hetkel on CryptoDociga krüpteeritud sõnumi saatmiseks vajalik minimaalselt 17 hiire klõpsu.

Hoolimata lahendusest, vajavad tähelapanu järgmised üldisemad küsimused:

- 1) Kust saavad kasutajad võtmed krüpteerimiseks ja lahti krüpteerimiseks ja kuidas neid hoitakse?
- 2) Kuidas paigaldatakse kasutaja seadmesse (arvuti, mobiil) meiliklient (või muu sõnumite saatmiseks mõeldud tarkvara), millel on krüpteerimise ja lahti krüpteerimise ning võtmete kontrollimise oskus?
- 3) Kuidas tagada tavakasutajale kasutajasõbralik tarkvaralahendus?

---

<sup>48</sup> ITU-T X.1252: Salgamatus – kaitstus selle eest, et üks mingis toimingus osalenud olemist eitab enda osalemist toimingus või selle mingis osas

Kasutatava turvalisuse juures on ühes uurimuses<sup>49</sup> kõige olulisemate aspektidena välja toodud järgmised punktid:

- 1) Käivituskulud – teenuse ülespanek ja alustamine peaks olema kasutajale lihtne.
- 2) Adekvaatsed metafoorid – turbefunktsioonid (nt krüpteerimine, allkirjastamine ja sertifikaadid) peaksid olema kasutajale tavamõistetega arusaadavalt ning adekvaatselt ära seletatud.
- 3) Lihtsad usaldusküsimused – tavakasutaja käest tohib küsida vähe ning ainult kergesti langetatavate otsuste kohta.
- 4) Nähtamatu PKI (avaliku võtme taristu) – tavakasutaja saab süsteemi usaldusotsuste tegemiseks kasutada ka ilma PKI kontseptsioonidest aru saamata.
- 5) Hoidumine piiritlemata verifitseerimisest – kasutaja ei peaks olema sunnitud kasutama informatsiooni väljastpoolt kehtestatud tegevusala (näiteks räside võrdlemine).

---

<sup>49</sup> Cristian Thiago Moecke and Melanie Volkamer, “Usable secure email communications: criteria and evaluation of existing approaches,” *Info Mngmnt & Comp Security*, vol. 21, no. 1, pp. 41–52, Mar. 2013.

## 6. Võimalikud lahendused krüpteeritud sõnumite saatmiseks lõppkasutajalt lõppkasutajale

Võimalikud lahendused krüpteeritud sõnumite saatmiseks lõppkasutajalt lõppkasutajale (otspunktkrüpteerimine) võtavad arvesse nii õiguslikke kui tehnoloogilisi aspekte.

Olemasoleva süsteemide võrgu- ja meiliserveri tasemel turvamist käsitleme põhjalikumalt peatükis „7. Soovitavad nõuded praeguste süsteemide turvalisuse aspektide parandamiseks“ (lk. 47).

### Õiguslikud aspektid

Õiguse vallas tuleb turvalise e-kirjavahetussüsteemi loomisel arvestada õigusaktidest tulenevate kohustuste ja piirangutega. Eelkõige tuleb iga lahenduse juures analüüsida kehtivate õigusaktide kohaldavust ning vajadusel olemasoleva regulatsiooni muutmist ja täpsustamist. Kuna hetkel puudub Eestis krüpteeritud e-kirjavahetussüsteemi reguleeriv eriseadus, saab kehtivatest piirangutest aimu erinevate õigusaktide analüüsist kogumina. Analüüsitud on nii siseriiklikku õigust kui ka relevantseid EL norme.

Õiguskorra täiendamise osas käesolevas analüüsis tehtavaid ettepanekuid tuleb kindlasti uuesti läbi vaadata, kui tehnilise lahenduse detailid on selgunud. Rõhutame mistahes tehnilise lahenduse edasisel arendamisel nn *privacy by design* lähenemise järgimise olulisust. Samuti tuleb iga üksiku ettepaneku juures kaaluda tasakaalu ülereguleerimise (nt normatiivaktide muudatused, mis toovad selguse asemel endaga kaasa uusi kitsendusi) ning *laissez faire* (nt regulatsiooni üldine puudumine, mis annab küll rohkem tegutsemisvabadust, kuid ei ole läbipaistev ega paku õiguskindlust) lähenemise vahel. Arvestades usaldusteenuste ja infoühiskonna kiiret arengut ei pruugi olla otstarbekas krüpteeritud e-kirjavahetussüsteemi eriregulatsiooni loomine seaduse tasemel. Selle asemel tuleks lähtuda üldistest eesmärkidest nagu e-riigi operatiivne toimimine, läbipaistvus, õiguskindlus, põhiõiguste kaitse ning nende valguses olemasolevat õiguskorda täiendada. Vajadusel võib kaaluda uute võimalikult madala taseme õigusaktide tutvustamist, näiteks Vabariigi Valitsuse seaduse § 26 alusel Vabariigi Valitsuse määruste loomist või olemasolevate määruste täiendamist. Konkreetset ettepanekuid on toodud iga tehnilise lahenduse juures eraldi.

Analüüsist nähtuvate ettepanekute valguses võiksid seadusandluse korrastamise või selle tõlgendamise juhiste andmisesse olla kaasatud eelkõige Majandus- ja Kommunikatsiooniministeerium, Andmekaitse Inspeksioon, Riigi Infosüsteemi Amet, Riigikantselei, Õiguskantsler ning Justiitsministeerium.

### Tehnoloogilised aspektid

Krüpteeritud sõnumite saatmiseks on mõistlik kasutada avaliku võtme taristu mudelit (PKI). PGP-laadne võrkusalduusel põhinev mudel ei ole suuremas mastaabis antud kontekstis otstarbekas.

PKI kasutamisel on järgmised variandid:

- 1) Iga organisatsioon peab oma PKI-d.

Sel juhul on vaja asutustevahelist ristusaldust ehk asutustevahelisi kokkuleppeid. See on

Eesti riigi mastaabis liiga kulukas, sest nõuab palju erialaste (tehniliste ja organisatoorsete) teadmistega spetsialiste.

- 2) Riigiasutuste ülene PKI-d (mõni suurem IT-asutus, nt SMIT, RMIT)  
Sel juhul tuleb arvestada piiratud ulatust – seda saab kehtestada ainult riigiasutustes ning nende lepingulistele partneritele.
- 3) Riigiülene PKI (hetkel Eestis CA rollis on SK, RA rollis on PPA).  
Sel juhul on sertifikaadi andmete kuju ja sertifikaadi välja andmise protseduurid vähese paindlikkusega. Hetkel on probleemiks sertifikaatide leidmine meilikliendi abil.

PKI-na vaadeldakse ka DNS-Based Authentication of Named Entities (DANE).<sup>50</sup> DANE on võimalik siduda meiliaadressi sisaldavate sertifikaatidega.<sup>51</sup> Lisaks on Verisign'i uurimisrühm leidnud, et DANE kasutamine lahendab osad CA-de paljususega seonduvad probleemid, vähendades mõningal määral ründepinda.<sup>52</sup>

Kõikide loetletud süsteemide puhul tõstatub küsimus, kust kasutaja saab salajase ja avaliku võtme komplekti ja kus seda võtmete komplekti hoitakse.

Salajase ja avaliku võtme saamiseks on järgmised variandid:

- a) Genereeritakse ja hoitakse lokaalses süsteemis tarkvaraliselt ja antakse avalik võti PKI-le allkirjastamiseks.
- b) Genereeritakse ja hoitakse arvuti/mobiili riistvaras ja avalik võti antakse PKI-le allkirjastamiseks.
- c) Genereeritakse ja hoitakse spetsiaalses riistvaras nagu näiteks ID-kaart ja avalik võti antakse PKI-le allkirjastamiseks.
- d) Genereeritakse keskses riistvara seadmes füüsilises turvamoodulis (HSM), antakse PKI-le allkirjastamiseks ja väljastatakse kasutajale hoiustamiseks eelpool (punktides a, b ja c) mainitud viisidel.

Kindlasti peab krüpteerimiseks vajalike võtmete hoiustamises osalema kasutaja. Viimase meetodi korral (punkt d) on võimalik võtmete arhiveerimine väljastaja poolt.

PKI on kasutusel kasutaja ja avaliku võtme seotuse ja võtme kehtimise tõendamiseks.

Meiliklientidega on põhiküsimus selles, kuidas jõuavad tavakasutaja meilikliendi konfiguratsiooni meili krüpteerimisega seonduvad võtmed.

Lisaks on vaja teada, kust leida teise osapoole avalikku võtit. Hetkel on meilikliendiga SK hallatavast LDAP-ist<sup>53</sup> avalikke võtmeid sisaldavate sertifikaatide otsimine raskendatud. Järgneval pildil (Pilt 1) on näide hetkel võimalikust päringust.

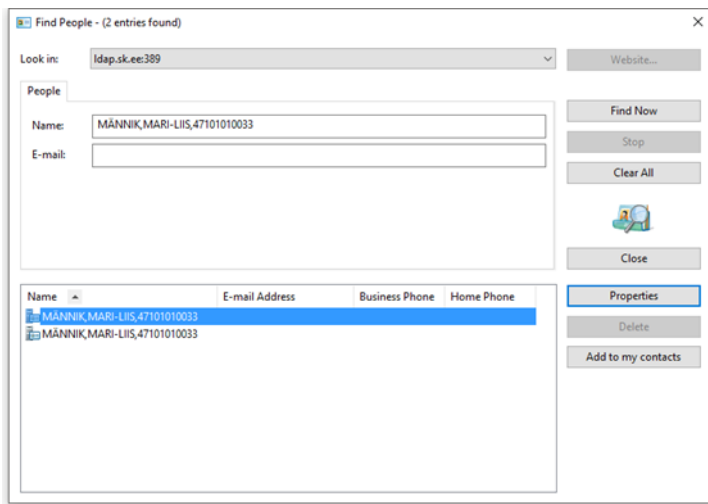
---

<sup>50</sup> <https://tools.ietf.org/html/rfc6698>

<sup>51</sup> <https://tools.ietf.org/html/draft-ietf-dane-smime-07>

<sup>52</sup> Reducing the X.509 Attack Surface with DNSSEC's DANE <http://conferences.npl.co.uk/satin/papers/satin2012-Osterweil.pdf>

<sup>53</sup> LDAP-i kataloogi kasutamine on hetkel kirjeldatud aadressil <https://www.sk.ee/repositoorium/ldap/ldap-kataloogi-kasutamine>. LDAP kataloog on hetkel ligipääsetav aadressilt [ldap.sk.ee:389](https://ldap.sk.ee:389)



Pilt 1-LDAP päringu näide.

Kasutusmugavuse parandamiseks on vaja minimeerida klõpsude arvu krüpteeritud sõnumi saatmiseks.<sup>54</sup> Hetkel on CryptoDoc'iga krüpteeritud sõnumi saatmiseks vajalik minimaalselt 17 hiireklõpsu.

Krüpteeritud sõnumite juures on oluline lahendada olukord, kus krüpteeritud sõnum saadetakse mitmele osapoolle korraga ja osad adressaadid ei ole võimelised krüpteeritud sõnumist aru saama. Praegu olemasolevate lahenduste korral tekib mainitud juhul n-ö „hard fail“, kus sõnum saadetakse kõigile adressaatidele ühte moodi (olenevalt süsteemi seadetest kas krüpteeritult või krüpteerimata). Lisaks võiks süsteemis olla n-ö „soft fail“ võimalus, mis tähendab seda, et sõnum saadetakse võimaluse korral krüpteerituna. Kui mõni osapool ei ole krüpteerimisvõimeline, siis „soft fail“ korral on võimalik konfidentsiaalsusele eelistada käideldavust (kasutajat sellest valikust selgelt informeerides).

Lahendustena pakume seega ideid, mis eeldavad järgnevat:

- 1) Tervikuna on asutustel ebaotstarbekas hallata iseseisvaid PKI struktuure, mis on omavahel ristusalduses.
- 2) Asutused ei soovi ise tegeleda krüptograafiliste privaatvõtmete kasutajatele kätte toimetamisega.
- 3) Kasutaja ei soovi aktiivselt osaleda täiendavate avalike sertifikaatide loomisel.

Järgnevalt on erinevad ideed põhjalikumalt lahti kirjutatud. Kõigis arvestustes on hinnatud skooopi kuuluvateks riigitöötajate arvuks ligikaudu 31 435 inimest.<sup>55</sup>

<sup>54</sup> Klõpsude arvu mõõtmine ei ole kaugeltki ainuke viis kasutusmugavuse mõõtmiseks, kuid see aitab hinnata, kui keeruline ja aeganõudev on mingi kindel protsess.

<sup>55</sup> <http://riigiraha.fin.ee/geoqlik/proxy/QvAJAXZfc/opendoc.htm?document=Riigiraha.qvw&host=local&anonymous=true>

## **Idee 1 – Ühtne meiliserver**

Meiliserveritele esitatakse üldjoontes järgmised nõudmised:

- veebimeili olemasolu
- mobiilseadmete tugi
- IMAP/POP3 tugi
- võimekus integreeruda kaasaegsete spämmi- ja viirustõrjevahenditega
- elementaarne kõrgkäideldavuse tugi
- kalendri ja grupitöövahendite tugi
- vajaliku halduskompetentsi olemasolu

Ühtne meiliserver võiks lisaks lihtsalt meili vahendamisele võimaldada ka laiemaid turvafunktsioone, nt määrata, kes klientidest ja kui kaua saab sõnumeid lugeda; ära hoida sõnumi loata edastamist ja/või modifitseerimist; lubada sõnumi aegumist – see tähendab anda kasutajale võimalus paremini kontrollida sõnumivoogu vastava lahenduse piires. Seadusest (näiteks isikuandmete kaitse seadusest) tulenevad nõudmised on loetletud allpool kehtiva regulatsiooni alla.

Eesti riigiasutustes on valdavalt kasutusel Microsoft Exchange lahendused, mis täidavad eelpool loetletud nõudmisi. Seega põhineb käesolev idee just Microsoft Exchange lahendusel.

**Idee mõju ulatus:** Keskvalitsuse riigieelarvelised asutused kuni ligikaudu 31 435 inimest.

Ettepanek on võtta riigis kasutusele üks Exchange’l põhinev grupitöö serveri lahendus, pannes üles vähemalt 4 meiliserveri klastrit koos Active Directory CA ja IMS lahendusega.

Hetkel pole tehnilises lahenduses määratud, mil viisil toimuks meiliserveri kasutajate registri loomine ning haldamine või kas selleks oleks vajalik X-teega liidestamine kasutajate tekitamiseks personali andmete põhjal (näiteks Microsoft Active Directory kontekstis) isegi juhul, kui see võib olla arhitektuuri osa.

### **Kehtiv regulatsioon ja selle muutmise vajadus**

Järgnev analüüs selgitab kehtivat regulatsiooni ning sellest tulenevaid piiranguid ning analüüsib selle muutmise vajadust käesoleva tehnilise lahenduse valguses. Õigusanalüüsi aluseks on piiratud info tehnilise lahenduse omaduste ja arhitektuuri kohta.

### **Avaliku teabe seadus**

Kehtiva regulatsiooni alusel tuleb hinnata, mil viisil reguleerib ühtse e-kirjavahetussüsteemi loomist, rakendamist ja juurutamist avaliku teabe seadus (AvTS). Kõigepealt vaatleb analüüs, kas ühtses e-kirjavahetussüsteemis töödeldavad andmed kuuluvad avaliku teabe alla. Seejärel hinnatakse, millised oleksid nõuded ühtsele e-kirjavahetussüsteemi loomisele, kui see hõlmaks enda all andmekogu asutamist või X-teega liidestamist. Viimaks vaadeldakse nõudeid, mis kehtivad asutusesiseseks kasutuseks tunnistatud teabe töötlemisele.

AvTS § 3 lg 1 alusel on avalik teave “mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja

dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites.” AKI täpsustab, et avalikuks teabeks (või teisisõnu avaliku sektori teabeks) on kogu avaliku sektori valduses olev teave, olenemata sellest, kas seda tuleb dokumendiregistris registreerida või mitte.<sup>56</sup> Näiteks ei tule dokumendiregistris registreerida asutusesiselt adresseeritud dokumente nagu arvamused, teated, memod, õiendid, nõuanded jm (AvTS § 35 lg 2 p 3), mis tänapäeval peaaegu eranditult saadetakse elektrooniliselt. Seadus ei nimeta otseselt, kas asutusesisene või asutustevaheline igapäevane e-kirjavahetus kuulub avaliku teabe alla. Kui aga eeldada, et asutusesisene või asutustevaheline igapäevane e-kirjavahetus teenib valdavalt riigiasutuste avaliku ülesande täitmise eesmärki, saab seda lugeda avalikuks teabeks.

Järgmisena küsime, millised on AvTS-i alusel nõuded avaliku teabe töötlemisele. Esmalt analüüsimme, kas meiliserveri loomise mõnes etapis tuleb asutada andmekogu AvTS tähenduses. AvTS § 43<sup>1</sup> lg 1 sätestab, et “andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.” Praeguse praktika kohaselt käsitletakse asutuste meiliservereid kui ainult organisatsiooni sisemise töökorralduse vajadusteks või asutustevaheliseks dokumentide menetlemiseks peetavat ja riigi infosüsteemi mittekuuluvat andmekogu AvTS § 43<sup>3</sup> lg 4 mõistes. Lähtuvalt praktikast saab seega ka riigiasutustevahelist ühtset e-kirjavahetussüsteemi pidada andmekoguks AvTS § 43<sup>3</sup> lg 4 mõistes. AvTS § 43<sup>3</sup> lg-st 4 tuleneb ka, et ainult organisatsiooni sisemise töökorralduse vajadusteks või asutustevaheliseks dokumentide menetlemiseks peetavat ja riigi infosüsteemi mittekuuluvat andmekogu ei pea AvTS § 43<sup>3</sup> lg 3 alusel kooskõlastama ning samuti ei ole riigi infosüsteemi haldussüsteemi määruse (nn RIHA määrus)<sup>57</sup> § 7 lg 2 alusel vaja kooskõlastamist RIHA-ga. Küll aga tuleb kõik andmekogud ja riigi infosüsteemi kuuluvad andmekogudega seotud infosüsteemid RIHA-s registreerida (RIHA määrus § 9 lg 1, AvTS § 43<sup>2</sup> lg 1). Lisaks andmekogudele kantakse RIHA-sse ka näiteks andmekogu staatusega infosüsteeme, infosüsteemide standardlahendusi ning teenuseid.<sup>58</sup>

Lisaks ühtsele meiliserverile tuleb hinnata ka meiliserveri administreerimiseks vajaminevate erinevate andmete korrastatud kogumite õiguslikku tähendust. Näiteks tuleb administreerimiseks pidada andmebaasi, milles sisalduvad kõikide kasutajate nimed, meiliaadressid, asutus, ametikoht, isikukood ja vajadusel muu info. Kuna seadus keelab asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid (AvTS § 43<sup>3</sup> lg 2), tuleb tehnilise lahenduse arendamisel kontrollida, milliseid andmeid meiliserveri administreerimiseks täpselt vajatakse.<sup>59</sup> Kui on olemas samu andmeid koguv andmekogu (antud juhul võiks kõne alla tulla näiteks “Riigi personali arvestuse andmekogu”<sup>60</sup>), tuleb eraldi vaadelda sellele juurdepääsu küsimust. Näiteks “Riigi personali arvestuse andmekogu” puhul on sellesse sisestatud andmetele juurdepääs sätestatud “Riigi

<sup>56</sup> AKI AvTS üldjuhend lk 7,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)

<sup>57</sup> Riigi infosüsteemi haldussüsteem, RT I, 29.03.2016, 6, <https://www.riigiteataja.ee/akt/129032016006?leiaKehtiv>

<sup>58</sup> AKI andmekogude juhend lk 4,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Andmekogude%20juhend\\_1.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Andmekogude%20juhend_1.pdf)

<sup>59</sup> Juhul, kui selgub, et ühtse meiliserveri administreerimiseks on vaja luua siiski eraldi andmekogu, siis tuleb jälgida AvTS-s esitatud nõudeid andmekogude loomise kohta (AvTS peatükk 5<sup>1</sup>). Nii kohalduks sellisel juhul ilmselt AvTS § 43<sup>3</sup> lg 4, mille alusel ainult organisatsiooni sisemise töökorralduse vajadusteks või asutustevaheliseks dokumentide menetlemiseks peetavat ja riigi infosüsteemi mittekuuluvat andmekogu ei pea AvTS § 43<sup>3</sup> (3)-s sätestatud korras kooskõlastama.

<sup>60</sup> Riigi personali- ja palgaarvestuse andmekogu asutamine ja selle põhimäärus, RT I, 31.03.2015, 24, <https://www.riigiteataja.ee/akt/121052013006?leiaKehtiv>

personali- ja palgaarvestuse andmekogu asutamine ja selle põhimääruse” § 10-s. Olenevalt sellest, milline asutus hakkab meiliserverit administreerima, võib olla vaja andmekogu põhimäärust täiendada, et lisada tingimused, mille alusel meiliserverit administreeriv asutus saab sellised andmekogu kasutusõigused, mida tema töötajad vajavad oma tööülesannete täitmiseks.

AvTS § 43<sup>9</sup> lg 3 alusel on AvTS § 43<sup>9</sup>-s loetletud riigi infosüsteemi kindlustavate süsteemide kasutamine kohustuslik kõigi riigi ja kohaliku omavalitsuse andmekogude pidamisel. Näiteks on riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemise puhul töötlemiseks kasutatavate infosüsteemidele ning nendega seotud infovaradele kehtestatud turvameetmete süsteem (infosüsteemide turvameetmete süsteemi ehk nn ISKE määrus).<sup>61</sup> AvTS § 43<sup>3</sup> lõikes 4 nimetatud andmekogule tuleneb ISKE rakendamise kohustus § 43<sup>9</sup> lg 3 teisest lausest. Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kirjeldustest (ISKE määruse § 1 lg 2). ISKE määruse § 2 täpsustab, et turvameetmete süsteemi rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises, nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etaloniturbesüsteemi rakendamisjuhendile ja nende rakendamises ning rakendamise auditeerimises.

Kui e-kirjavahetussüsteemi toimimiseks on vajalik see liidestada X-teega (näiteks tehnilises osas mainitud Microsoft Active Directory-ga seotult), tuleb lisaks eelnevale järgida ka X-teega liitumise korra ja selle kasutamise nõudeid, mis tulenevad infosüsteemide andmevahetuskihi määrusest (nn X-tee määrus).<sup>62</sup> Sellest järeldub, et kuigi ISKE määrus sätestab, et selle reguleerimisalaks on “riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem” (ISKE määrus § 1 lg 1), tuleneb X-tee määruse § 19 lg 1-st, et kõigile X-teega liidetavatele infosüsteemidele (olenemata sellest, kas seal töödeldakse andmekogudes sisalduvaid andmekoosseisusid või mitte), määratakse turvaklass ja turvaklassile vastavad turvameetmed võetakse kasutusele vastavalt ISKE määrusele. X-tee määrus ega ka AvTS sellist terminit nagu “infosüsteemi” ei defineeri.

Lisaks eelnevale reguleerib AvTS eraldi veel ka asutusesiseseks tunnistatud teabe kaitset (AvTS § 43). Selle lg 1 alusel peab teabevaldaja rakendama organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, et kaitsta asutusesisese teabe terviklikkust, käideldavust ning konfidentsiaalsust. Seaduse tekstist ei nähtu, mil määral need turvameetmed erinevad ISKE määruses sätestatud turvameetmete süsteemist. Seadus selgitab, et organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid tuleb rakendada asutusesisese teabe kaitseks olenemata teabe vormingust nii digitaalkujul kui ka paberkandjal teabe osas (AvTS § 43 lg 2). Seega kehtivad nimetatud nõuded kindlasti ka elektroonilisel teel saadetud asutusesiseseks kasutamiseks tunnistatud teabele.

Erinevalt AvTS-st on AKI oma üldjuhendis osundanud, et asutus peab kaitsma enda valduses olevat avalikku teavet sõltumata sellest, kas teave on piiranguga või piiranguta, paberil või elektrooniline, isikuandmetega või isikuandmeteta, andmekogusse kuuluv või andmekogu-väline. Üldjuhendi järgi tuleb mistahes avaliku teabe puhul garanteerida selle käideldavus, terviklikkus ja konfidentsiaalsus, mida teabevaldaja peab tagama rakendades organisatsioonilisi, füüsilisi ja infotehnilisi kaitsemeetmeid. Üldjuhend viitab, et sellise kohustuse paneb asutustele AvTS § 43 lg

---

<sup>61</sup> Infosüsteemide turvameetmete süsteem, RT I 2009, 6, 39, <https://www.riigiteataja.ee/akt/13125331?leiaKehtiv>

<sup>62</sup> Infosüsteemide andmevahetuskiht, RT I, 15.09.2015, 11, <https://www.riigiteataja.ee/akt/115092015011?leiaKehtiv>

Kuigi AKI üldjuhendi tõlgendus justkui laiendaks AvTS § 43 asutusesisese teabe kaitseks ette nähtud sätteid kogu avalikule teabele, tuleb pigem lähtuda seaduses sätestatud kitsamast vaatest. Ühtlasi saab kehtivast AvTS-st ning selle põhjal kehtestatud määrustest järeldada, et kohustus on kaitsta riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteeme ning nendega seotud infovarasid ning juurdepääsupiiranguga andmeid, samuti tuleb turvameetmed rakendada X-teega liidestatud infosüsteemides, kuid ülejäänud avaliku teabe kaitseks me seadusest konkreetseid sätteid ei leia.<sup>64</sup>

## Isikuandmete kaitse seadusest tulenevad nõuded

Ühtsele e-kirjavahetussüsteemile kehtiva regulatsiooni vältimatuks osaks on isikuandmete kaitse seadusest (IKS)<sup>65</sup> tulenevad nõuded, millele lisaks kohaldatakse alates 2018. aastast EL andmekaitse üldmäärust.

Enne isikuandmete töötlemisega seotud nõudmisteni jõudmist paar märkust isikuandmete kaitsega seotud definitsioonide ja nende kohaldamise kohta antud tehnilise lahenduse puhul. Kehtiva IKS-i järgi on isikuandmed “mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on” (IKS § 4 lg 1). Üldregulatsiooni poolt sätestatav definitsioon on veelgi täpsem: isikuandmed on “igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekt“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal” (üldmääruse artikkel 4). Isikuandmete töötlemine on IKS-i järgi “iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, riskasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest” (IKS § 5).<sup>66</sup> On selge, et ühtses riigiasutustevahelises e-kirjavahetussüsteemis töödeldakse muuhulgas ka isikuandmeid.

Isikuandmete töötleja on füüsiline või juriidiline isik, välismaa äriühingu filiaal või riigi- või kohaliku omavalitsuse asutus, kes töötleb või kelle ülesandel töödeldakse isikuandmeid (IKS § 7 lg

<sup>63</sup> AKI AvTS üldjuhend lk 38,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)

<sup>64</sup> Mingil määral võib kaitsmise alla lugeda ka AvTS § 3<sup>1</sup>, mis sätestab avaliku teabe taaskasutamisest tulenevad piirangud.

<sup>65</sup> Isikuandmete kaitse seadus, RT I, 06.01.2016, 10, <https://www.riigiteataja.ee/akt/130122010011?leiaKehtiv>

<sup>66</sup> Üldmääruse isikuandmete töötlemise definitsioon: “isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamine, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine”. Üldmäärus artikkel 4 lg 2.

1). IKS § 7 eristab vastutavat<sup>67</sup> ja volitatud töötletajat<sup>68</sup>, üldmäärus lisab siia juurde veel kaasvastutava töötletaja mõiste. Viimane tähistab juhtu, kui kaks või enam vastutavat töötletajat määravad ühiselt kindlaks isikuandmete töötlemise eesmärgid ja vahendid (üldmääruse artikkel 26). Antud tehnilise lahenduse arendamisel ning selle praktilisel rakendamisel tuleb seega defineerida, milline asutus või asutused täidavad vastutava töötletaja rolli määrates kindlaks isikuandmete töötlemise eesmärgid ja vahendid ning milline asutus või asutused täidavad volitatud töötletaja rolli. Kuivõrd pole teada, kes ja kuidas süsteemi haldama hakkab, ei saa hetkel sellele küsimusele lõplikku õiguslikku hinnangut anda. Kuid võib eeldada, et ilmselt on vastutava töötletaja rollis keskne IT-asutus, kes ühtset e-kirjavahetussüsteemi haldab ning volitatud töötletajateks erinevate riigiasutuste enda IT-tugiüksused.

Isikuandmete töötlemisel tuleb lähtuda mitmetest seaduse poolt sätestatud põhimõtetest. Näiteks tuleb järgida IKS § 6 sisalduvaid isikuandmete töötlemise põhimõtteid: seaduslikkuse põhimõte (isikuandmeid tohib töödelda vaid seadusest tulenevatel alustel ning määratletud ja õiguspäraste eesmärkide saavutamiseks), eesmärgikohasuse põhimõte (isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötlemise eesmärkidega kooskõlas), minimaalsuse põhimõte (isikuandmeid võib koguda ja töödelda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks), kasutuse piiramise põhimõte (kui seaduses ei ole alust isikuandmete töötlemisele, võib neid muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal), andmete kvaliteedi põhimõte (isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötlemise eesmärgi saavutamiseks), turvalisuse põhimõte (isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest) ning individuaalse osaluse põhimõte (andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääsu tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist). Sarnased isikuandmete töötlemise põhimõtted on loetletud ka üldmääruse artiklis 5: seaduslikkus, õiglus ja läbipaistvus; eesmärgi piirang; võimalikult väheste andmete kogumine; õigsus; säilitamise piirang; usaldusväärsus ja konfidentsiaalsus. Nimetatud põhimõtete täitmise eest vastutab ning on võimeline selle täitmist tõestama vastutav töötletaja (üldmäärus artikkel 5 lg 2).

IKS § 24 sätestab konkreetsemad isikuandmete kaitsest tulenevad nõuded isikuandmete töötlemisele. Näiteks on isikuandmete töötletaja kohustatud eesmärkide saavutamiseks mittevajalikud isikuandmed viivitamata kustutama või sulgema, kui seadus ei näe ette teisiti. Samuti peab töötletaja tagama, et töödeldavad isikuandmed on õiged ja, kui see on eesmärkide saavutamiseks vajalik, viimases seisus ning vajadusel neid täiendama ja parandama. Samuti tuleb isikuandmete parandamise korral viivitamata teavitada sellest kolmandaid isikuid, kellelt isikuandmed saadi või kellele isikuandmeid edastati, kui see on tehniliselt võimalik ega too kaasa ebaproportsionaalselt suuri kulutusi. Üldmäärus lisab, et: “Arvestades töötlemise laadi, ulatust, konteksti ja eesmarke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte,

---

<sup>67</sup> Üldmääruse vastutava töötletaja definitsioon: “füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid”. Üldmääruse artikkel 4 lg 7.

<sup>68</sup> Üldmääruse vastutava töötletaja definitsioon: “füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötletaja nimel”. Üldmääruse artikkel 4 lg 8.

rakendab vastutav töötleja asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete töötlemist kooskõlas käesoleva määrusega. Vajaduse korral vaadatakse need meetmed läbi ja ajakohastatakse neid” (üldmäärus artikkel 24 lg 1). Uuendusena julgustab 2018. aastal kohalduv üldmäärus vastutavat töötlejat oma kohustuste järgmise tõendamise elemendina kasutama üldmääruse artiklis 40 osutatud heakskiidetud toimumisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist. Üldmääruse artikkel 25 kehtestab nõuded lõimitud ja vaikimisi andmekaitsele ning artikkel 28 sätestab volitatud töötleja kohustused.

Eraldi käsitletakse ka isikuandmete töötlemise turvalisust. IKS § 25 kehtestab, et isikuandmete töötleja peab kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed, et kaitsta isikuandmete terviklikkust, tagada õiguspärane käideldavus ja konfidentsiaalsus. Näiteks on isikuandmete töötleja isikuandmete töötlemisel kohustatud vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele; ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis, samuti andmekandjate omavolilist teisaldamist ning ära hoidma isikuandmete omavolilist salvestamist, muutmist ja kustutamist ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal ning kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi. Oluline on, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks ning et oleks võimalik kontrollida millal, kellele ja millised isikuandmed edastati. Üldmääruse artikkel 32 täpsustab IKS § 25 nimetatud kohustusi ning nimetab ühe meetmena turvalisuse tagamiseks ka krüpteerimist (üldmääruse artikkel 32 lg 1 a).

Nimetatud nõuded on seda olulisemad, et kõigi riigiasutuste e-kirju hakkab haldama üks IT-asutus ning seega on õigustatud kõrgendatud tähelepanu sellele, mil viisil ja määral isikuandmete töötlemise turvalisus tagatud on. Siinkohal tuleb üle korrata üldmääruses sisalduv soovitus nimetatud meetmete järgimiseks ning selle järgmise tõendamiseks koostada üldmääruse artiklis 40 osutatud heakskiidetud toimumisjuhendid või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismid.

Antud kontekstis tuleb erilist tähelepanu pöörata ka isikuandmete töötlemise lubatavuse alustele. IKS § 10 kohaselt on isikuandmete töötlemine lubatud üksnes andmesubjekti nõusolekul, seaduse alusel või kui haldusorganipoolne töötlemine on vajalik avaliku ülesande täitmise käigus seaduse, välislepingu või EL Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud kohustuse täitmiseks. Avaliku ülesandega on tegemist juhul, kui nimetatud ülesanne on pandud riigi- või kohaliku omavalitsuse asutusele või juriidilisele või füüsilisele isikule täitmiseks seadusega või seaduse alusel antud mõne muu õigusaktiga.

Andmesubjekti nõusoleku küsimine isikuandmete töötlemiseks on kõige levinum viis isikuandmete töötlemiseks õigusliku aluse saamiseks. Andmesubjekti nõusolek kehtib üksnes juhul, kui see tugineb andmesubjekti vabal tahtel. Seadus näeb ette, et nõusolekus peavad olema selgelt määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud, samuti andmete kolmandatele isikutele edastamise tingimused ning andmesubjekti õigused tema isikuandmete edasise töötlemise osas. Vaikimist või tegevusetust nõusolekuks ei loeta. Reeglina peab nõusolek olema kirjalikku taasesitamist võimaldavas vormis ning teistest samal ajal esitatud tahteavaldustest selgesti eristatav. Oluline on, et andmesubjektil on õigus igal ajal oma nõusolek tagasi võtta ning et vaidluse korral eeldatakse, et andmesubjekt ei ole oma isikuandmete töötlemiseks nõusolekut andnud (IKS § 12, täpsustatakse muuhulgas üldmääruse artiklites 7, 12, seotud ka artiklid 13, 15-20).

Kui isikuandmete töötlemise lubatavus ei tulene seadusest, võib antud tehnilise lahenduse puhul andmesubjekti nõusolekut küsida mitmeti. Näiteks võib nõusoleku küsimise aluseks olla töösuhte aluseks olev dokument või e-kirjavahetussüsteemi programmi kasutustingimused. Lisaks on soovitatav isikuandmete töötlemise põhimõtted täiendavalt selgitada eraldi dokumendis. Analoogse näitena võib siinkohal tuua Sertifitseerimiskeskuse 'Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused', milles sisalduvad ka sätted andmesubjekti nõusoleku kinnitamiseks.<sup>69</sup> Isikuandmete töötlemise lubatavuse aluse täpne määratlus sõltub tehnilise lahenduse üksikasjadest ning selle rakendamisest.

Eraldi tasub mainida ka Andmekaitse Inspeksiooni (AKI) rolli, kes teostab seaduses ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle riiklikku ja haldusjärelevalvet (IKS § 32).<sup>70</sup> Riigiasutustevahelise ühtse e-kirjavahetussüsteemi loomisel on tugevalt soovituslik kaasata AKI-t näiteks soovituslikke juhiste tarbeks või konsulteerida konkreetsemate üksikküsimuste osas. Lisaks kehtestab üldmääruse artikkel 37 lg 1 a, et kui isikuandmeid töötleb avaliku sektori asutus või organ, määravad vastutav ja volitatud töötleja andmekaitseametniku, kelle ülesanneteks on muuhulgas teavitada ja nõustada vastutavat töötlejat või volitatud töötlejat ning isikuandmeid töötlevaid töötajaid seoses nende kohustustega ning järgida üldmääruse ja muude asjakohaste normide ja vastutava töötleja või volitatud töötleja isikuandmete kaitse põhimõtete järgimist, sealhulgas vastutusvaldkondade jaotamist, isikuandmete töötlemises osaleva personali teadlikkuse suurendamist ja koolitamist, ning seonduvat auditeerimist (üldmääruse artikkel 39).

## eIDAS määrus

Eraldi tasub täpsustada eIDAS määruse kohaldumist. Nimelt sätestab määruse artikkel 2 lg 2, et õigusakti ei kohaldata selliste usaldusteenuste osutamise suhtes, mida kasutatakse eranditult suletud süsteemides, mis tulenevad siseriiklikust õigusest või määratletud osalejate kogumi vahelistest kokkulepetest.

Küll aga tuleneb määrusest kohustus avalikule sektorile piiriüleselt tunnustada teiste liikmesriikide omadustelt samaväärseid ning teavitatud elektroonse identiteedi skeeme, mille detailsem analüüs jääb käesolevast probleemipüstitusest välja.<sup>71</sup>

---

<sup>69</sup> kasutustingimused, 25.01.2016,

[https://www.sk.ee/upload/files/ESTEID\\_Kasutustingimused\\_20160125.pdf](https://www.sk.ee/upload/files/ESTEID_Kasutustingimused_20160125.pdf)[https://www.sk.ee/upload/files/ESTEID\\_Kasutustingimused\\_20160125.pdf](https://www.sk.ee/upload/files/ESTEID_Kasutustingimused_20160125.pdf)

<sup>70</sup> AKI võib IKS § 33 alusel muuhulgas rakendada seadustes ettenähtud alustel, ulatuses ja korras haldussundi, algatada vajaduse korral vääртеomenetluse ja kohaldab karistust, anda soovituslikke juhiseid; tal on õigus peatada või keelata isikuandmete töötlemine, nõuda ebaõigete isikuandmete parandamist, isikuandmete sulgemist või töötlemise lõpetamist, sealhulgas hävitamist või edastamist arhiivi ning rakendada isiku õiguste ja vabaduste kahjustamise ärahoidmiseks vajaduse korral asendustäitmise ja sunniraha seaduses sätestatud korras viivitamata isikuandmete kaitseks organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, välja arvatud juhul, kui isikuandmeid töötleb riigiasutus. Osad nimetatud õigustest on riigiasutustele kohaldatavad üksnes juhul, kui kohaldamata jätmine tooks kaasa andmesubjekti õiguste olulise kahjustamise. AKI võib järelevalvemenetluse algatada kaebuse alusel või omal algatusel. Lisaks on IKS-i täitmise tagamiseks AKI ametiisikul õigus teha isikuandmete töötlejale ettekirjutusi ja vastu võtta otsuseid. Kui riigiasutusest isikuandmete töötleja ei ole AKI ettekirjutust selles määratud tähtaja jooksul täitnud, võib AKI pöörduda halduskohtumenetluse seadustikus sätestatud korras protestiga halduskohtusse. (§ IKS 40)

<sup>71</sup> Rohkem infot leitav: Mark Erlich, e-Allkirjad Euroopas ja nende käsitlemine Eestis, RIA 2016,

## Kehtiva õiguse muutmise vajadus

Tuleb kaaluda, mil viisil reguleerida antud tehnilise lahenduse kasutamist riigiasutuste poolt. Seaduse tasandil reguleerimine ei pruugi olla antud juhul otstarbekas. Eelistada tuleks üleriigilisele riigiasutustele kohaldatava e-kirjasüsteemi kehtestamiseks näiteks Vabariigi Valitsuse seaduse<sup>72</sup> § 26 alusel loodud Vabariigi Valitsuse määrust ning vajadusel juhiste andmist. Analoogset lahendust järgib juba ka määrus “Asjaajamiskorra ühtsed alused” (AÜA)<sup>73</sup>, mis reguleerib muuhulgas riigi- ja kohaliku omavalitsuse asutuste ning avalik-õiguslike juriidiliste isikute asjaajamisele ja dokumendihaldusele esitatavaid nõudeid (AÜA § 1).

Tulenevalt eelpool koostatud analüüsist, võiks riigiasutustevahelise ühtse e-kirjasüsteemi loomise rakendamiseks kaaluda AvTS § 43 lg 3 alusel antud volitusnormi<sup>74</sup> kasutamist, mille järgi võib Vabariigi Valitsus määrusega kehtestada asutusesisese teabe terviklikkuse, käideldavuse ja konfidentsiaalsuse kaitseks rakendatavate organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete loetelu. Kuigi nimetatud määruse eesmärgiks võib seaduse sõnastuse järgi pidada asutusesiseseks kasutamiseks tunnistatud teavet, on ühtses e-kirjavahetussüsteemis ilmselt keeruline rakendada meetmeid, mis asutusesiseseks kasutuseks tunnistatud teabele eraldi turvameetmeid pakuksid ning seega tuleks eelistada e-kirjavahetussüsteemi kaitset tervikuna. Seega pakub käesolev analüüs välja, et AvTS § 43 lg-s 1 sätestatud organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamise kohustuse täitmise üheks osaks oleks riigiasutuste kohustus kasutada käesolevas tehnilises lahenduses pakutud ühtset e-kirjavahetussüsteemi, mis omakorda peab olema üles ehitatud ja rakendatud viisil, mis tagab elektrooniliselt saadetavate asutusesiseseks kasutamiseks tunnistatud teabe kaitse.

AvTS § 43 lg 3 alusel välja antud määrus võiks lisaks riigiasutustele ühtse e-kirjasüsteemi kohustuslikuks muutmisele sisaldada ka täiendavat regulatsiooni ühtse e-kirjasüsteemi ülesehituse ja rakendamise osas, sealhulgas sätteid, kuidas on e-kirjasüsteemis salvestatud teave kaitstud juhusliku või tahtliku volitamata muutmise eest; kuidas kaitstakse teavet juhusliku hävimise ja tahtliku hävitamise eest või olukorras, kui on takistatud õigustatud isikule andmete kättesaadavuse takistamise eest ning kuidas on teave kaitstud juhusliku või tahtliku volitamata juurdepääsu eest (loetletud ka § AvTS 43 lg-s 1). Kasutades taaskord AÜA määruse analoogiat, võib AvTS § 43 lg 3 alusel antud määruses sisalduda ka normatiivne alus täiendavate juhiste andmiseks, mida peavad järgima kõik avalikke ülesandeid täitvad asutused ja isikud (AÜA § 54<sup>2</sup> lg 1).<sup>75</sup> Nimetatud juhistes või muudes toetavates dokumentides (nt kasutajatele suunatud eeskirjad või e-kirjavahetussüsteemis isikuandmete töötlemise põhimõtted) saab täiendavalt reguleerida ka järgnevad teemad: e-kirjade ja muude andmete säilitamine, volitused e-kirjadele ja muudele andmetele ligipääsuks ja nende töötlemiseks ning e-kirjavahetussüsteemi haldaja kohustused ja õigused.

AvTS § 43 lg 3 alusel loodav määrus võib sisaldada ka täpsustusi muude vajalike

---

[https://www.ria.ee/public/PKI/EL\\_e-allkirjade\\_kasitlemine.pdf](https://www.ria.ee/public/PKI/EL_e-allkirjade_kasitlemine.pdf)

<sup>72</sup> Vabariigi Valitsuse seadus, RT I, 30.12.2015, 72, <https://www.riigiteataja.ee/akt/111062013007?leiaKehtiv>

<sup>73</sup> Asjaajamiskorra ühtsed alused, RT I, 26.08.2015, 6, <https://www.riigiteataja.ee/akt/130122011062?leiaKehtiv>

<sup>74</sup> Volitusnormi näol on tegemist õigust andva, mitte kohustava volitusnormiga, Avaliku teabe seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, 27/04/2015, lk 21.

<sup>75</sup> Näiteks AÜA § 54<sup>2</sup> lg 1 sätestab, et Majandus- ja Kommunikatsiooniministeerium kavandab ja koordineerib asjaajamise arengut ja elektroonilisele dokumendihaldusele üleminekut avalikus sektoris ning annab dokumendihalduse alaseid juhiseid.

organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamise kohta, arvestades, et nimetatud nõuded kehtivad ka paber kandjal asutusesiseseks kasutamiseks tunnistatud teabele.

Alternatiivse lahendusena võib täiendavalt analüüsida ka AÜA määruse sisulise uuendamise otstarbekust. Põhimõtteliselt saaks määrust uuendada viisil, et määruse reguleerimisalasse lisanduks riigiasutustevaheline e-kirjavahetus ning määruses kehtestada nii e-kirjavahetussüsteemi kasutamise kohustuslikkus kui ka viited e-kirjavahetussüsteemile kehtivatele infoturbealastele nõuetele, sh krüpteerimisele.

Kolmanda võimaliku lahendusena võib kaaluda ISKE määruse uuendamist viisil, et sinna lisada riigiasutustele kohustus kasutada käesolevas lahendusidees pakutud ühtset (krüpteeritud) e-kirjavahetussüsteemi ning samasisuline täiendav meede ISKE meetmete hulka lisada.

Lisaks tuleb mainida, et käesoleva lahenduse puhul täpsustatakse tehnilise lahenduse üksikasjad ning ühtse e-kirjavahetussüsteemi kasutamisega seotud detailid muuhulgas ka tarnijaga sõlmitavas lepingus.

Olenevalt sellest, kuidas lahendatakse e-kirjavahetussüsteemi haldamine ja koordineerimine, võib osutada vajalikuks ka vastavalt uuendada koordineeriva ja haldava asutuse põhimäärust<sup>76</sup> ning muid seotud normatiivdokumente. Näiteks võib nii käesolevas lahenduses pakutud ühtse e-kirjavahetussüsteemi kohustuslikkuse riigiasutuste infoturbesüsteemi osana kui ka selle haldamisega seotu kehtestada Vabariigi Valitsuse määrusega "Infoturbe juhtimise süsteem".<sup>77</sup>

## Tugevused

- + Lahendab Eesti ametnikult Eesti ametnikule turvalise e-kirjavahetuse probleemi
- + Võimaldab kasutusele võtta IRM-i ehk Information Rights Management'i riigi sees, mis omakorda võimaldaks järgnevat:
  - o Määrata, kes klientidest ja kui kaua saab sõnumeid lugeda
  - o Ära hoida sõnumi loata edastamist ja/või modifitseerimist, näiteks ära hoida salvestamist, lõikamist ning kleepimist MS Office vahenditega
  - o Sõnumi aegumist
  - o Sõnumitega analoogselt käsitleda MS Office dokumente
- + Võimaldab garanteeritud 24/7 teenust ja vähendab isikute hulka, kes saavad seadmetele ligi
- + Tekitab haldamise sünergiat
- + Lahendab osaliselt probleemi Ametnik - isik krüptovõimeta, sh. välispartnerid. Microsofti pilvepõhised autentimisteenused kasutavad lahendused lahendavad probleemi juhul, kui sõnumi saajal on MS Office 365 või Windows Live konto

## Puudused

- Antud valik tekitab sõltuvuse tarnijast
- Krüpto väljavahetamine ja tugi sõltub tootjast

---

<sup>76</sup> Riigi Infosüsteemi Ameti põhimäärus RT I, 26.02.2016, 2 § 15 (11), <https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv>

<sup>77</sup> Infoturbe juhtimise süsteem, RT I, 19.03.2012, 4, <https://www.riigiteataja.ee/akt/119032012004>

- Vaikimisi krüpteerimist ei kasutata
- Üks ühtne platvorm teeb ründamise lihtsamaks
- Suurendab hajutatud teenusetõkestusründe (DDoS) ohtu
- Keskne lahendus põhjustaks asutuste poolt suure tõenäosusega rohkem vastuseisu, kui mõni teine alternatiivne lahendus
- Probleemid asutuste põhiste lisapoliitikate rakendamisega (lisanõudmised turvalisusele)
- Kindlasti tuleks taolise süsteemi rakendamise korral arvestada asutuste ja organisatsioonide vastuseisuga, kuna organisatsioonid on erineva turvavajadusega ja kõik organisatsioonid ei soovi töötajate informatsiooni vabalt ühises kataloogipuus jagada (osad ei saa seda teha julgeolekukaalutlustel)
- Lahendab välise osapoolega suhtluse probleemida ainult födereeritusse korral.

Probleemi väliste osapooltega krüpteerimisel saab osaliselt lahendada kasutades teisi antud dokumendis välja pakutud ideid.

## **Ressursivajadus**

- Kõikidele kasutajatele ja/või seadmetele Microsoft Exchange ja serveri kliendi litsentsid
- Serveri litsentsid MS Windows Enterprise serveritele
- Olemasolevate süsteemide migratsioon ja süsteemide paralleelne käitamine

Esialgssed süsteemi haldus- ja käitluskulud on hinnanguliselt 3 miljonit eurot (koos koolitustega ligikaudu 4,4 miljonit eurot). Sealjuures võivad kulud olla osaliselt kaetud asutuste litsentseerimise mudelitega. Täpsema lisakulu välja selgitamiseks tuleks teha asutuste litsentside audit.

## **Haldamine ja selle koordineerimine**

Lõppkasutaja seadme tarkvara paigaldus, häälestamine ja laiendamine on asutust teenindava IT-üksuse ülesanne. Ka kasutajate loomine võib olla asutust teenindava IT-üksuse ülesanne.

Toimub serverihalduse konsolideerimine ühe IT-asutuse kätte.

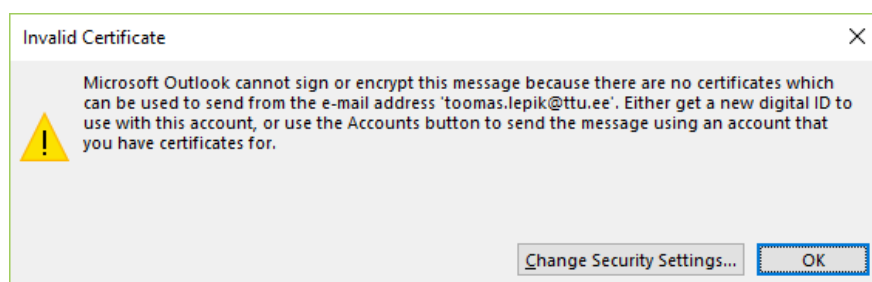
Koordineerimine ja järelvalve funktsioon võiks jääda RIA-le.

## Idee 2 – S/MIME kasutamine ID-kaardi ja DNSSEC abil kui läbiva krüpteerimise lahendus

### Idee mõju ulatus: Potentsiaalselt kogu maailm

S/MIME on populaarne turvalise meiliedastuse protokoll, mis võimaldab turvalist meili saata ka osapooltele, kellel Eesti ID-kaarti ei ole, aga kes kasutavad teisi tunnustatud sertifikaate väljastavaid CA-sid. S/MIME protokolliga seotud rakendamise peamiseks probleemiks on meilikliendi soov siduda sõnumi saatmine sertifikaadis määratletud meiliaadressiga.

Hetkel nõuavad kõik enamkasutatavad meilikliendid, et kasutaja poolt esitatav sertifikaat sisaldaks meiliaadressi, millelt toimub meili saatmine.



Pilt 2- MS Outlook veateade, kui ei leita meiliaadressile sobilikku sertifikaat

Eesti ID-kaarti kasutades peaksid nii saaja kui ka saatja olema @eesti.ee aadressiga. Teistsuguste meiliaadresside korral (nt juhan@asutus.ee) tuleks seega kasutaja ID-kaardiga seotud avalik võti siduda ka tema vastava meiliaadressiga (nt [juhan@asutus.ee](mailto:juhan@asutus.ee)).

Seda sidumist saaks tehniliselt teha SK kaudu. Hinnanguline kulu riigisektorile oleks sel juhul ligikaudu 2 miljonit eurot aastas (summa võib muutuda olenevalt läbirääkimiste tulemusest) ning on kaheldav, et väljaspool riigisektorit oleksid kõik tavakasutajad nõus antud teenuse eest maksma.

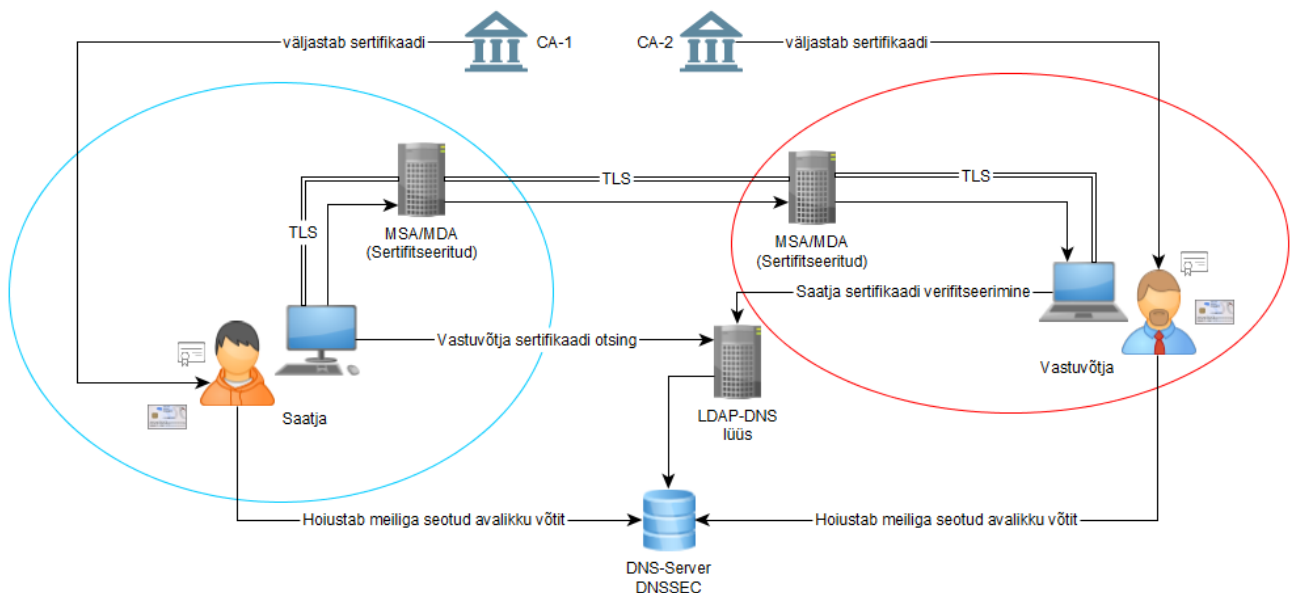
Kui on jõutud DNSSEC-i rakendamiseni, võib meili jaoks kasutatava PKI puhul CA struktuurist loobuda.

Tasuks ära mainida, et praegune Mobiil-ID arhitektuur ei võimalda seda krüpteerimiseks kasutusele võtta. Mobiilsete seadmete kaudu turvaliselt meilide lugemine võiks olla võimalik kasutades selleks uue põlvkonna NFC tehnoloogiat toetavat ID-kaarti.<sup>78</sup>

Antud idee on mõeldud eraldi lahendusena praegusele süsteemile või ka keskse serveri lahenduse laiendamiseks.

---

<sup>78</sup> <http://nelenkov.blogspot.com/2013/10/signing-email-with-nfc-smart-card.html>



Skeem S/MIME kasutamisest koos DNSSEC-iga

Kuidas seda teha:

- 1) Tuleb laiendada ID-kaardi ajurit (draiverit), et see võimaldaks ID-kaardi avaliku võtme vastu välja anda digitaalset sertifikaati, mida on võimalik hoida ID-kaardist väljas olevas sertifikaatide hoidlas.
- 2) Antud protsess tuleb teha skriptitavaks võimaldades organisatsioonile automaatset digitaalset sertifikaadi genereerimist ja meilikliendi konfiguratsiooni.
- 3) Avalikustada sertifikaadid, mis on seotud avalike meiliaadressidega. Ettepanek teha seda DNS-i kaudu, kasutades DNSSEC vahendeid.<sup>79</sup> Selle protsessi automatiseerimiseks tuleks luua eraldi tööriist. DNS protokolliga kasutamine kataloogi pidamiseks LDAP-i asemel on X-tees juba väljakujunenud praktika.
- 4) Tuleb luua riiklik LDAP-DNS lüüs<sup>80</sup> (*gateway*).
- 5) Tuleb häälestada meiliklient seda lüüsi kasutama meiliaadressiga seotud avalike võtmete leidmiseks.
- 6) Tuleb õpetada tavakasutajale, kuidas luua ja kasutada meiliaadressiga seotud lisertifikaati. Tavakasutajal on kaks võimalust:
  - a. Kasutada @eesti.ee meiliaadressi
  - b. Genereerida või hankida sertifikaat oma meiliaadressile või kasutada selleks vastavat tööriista (mida hetkel ei eksisteeri), mille korral oleks kasutajal vaja oma meiliaadressiga seotud lisertifikaadiga seoses täiendavaid oskusi
- 7) Soovituslik on õpetada süstemaatiliselt kõigile kasutajatele uue süsteemi kasutamist ning selle tugevaid ja nõrku kohti.

LDAP DNS lüüsi loomine on vajalik, kuna hetkel kasutuses olevatel meiliklientidel toimub krüpteerimise tarbeks teise osapoole leidmine kas läbi eelnevalt vahetatud sertifikaatide või LDAP-tüüpi kataloogist.

<sup>79</sup> Using Secure DNS to Associate Certificates with Domain Names For S/MIME

<https://tools.ietf.org/html/draft-ietf-dane-smime-00>

<sup>80</sup> <https://meetings.icann.org/en/dublin54/schedule/wed-dnssec/presentation-outlook-smimea-21oct15-en.pdf>

## Kehtiv regulatsioon ja selle muutmise vajadus

Esmalt kontrollime, kas ja mil määral kehtiv õigus reguleerib käesolevas tehnilises lahenduses välja pakutud täiendavate sertifikaatide loomist. Seejärel vaatleme sertifikaadil asuvate isikuandmete töötlemise (taaskasutamise) aluseid ning teeme ettepanekud kehtiva regulatsiooni täiendamiseks.

## Sertifikaat ning isikuandmete töötlemine

Vaatleme esmalt kehtivat regulatsiooni, mis puudutab sertifikaate. Sertifikaat „Digitaalallkirja seaduse“ mõistes on dokument, mis on välja antud, võimaldamaks digitaalallkirja või digitaalse templi andmist ja kontrollimist ning milles avalik võti seotakse üheselt sertifikaadi omanikuga (DAS § 5 lg 1). Isikut tõendavate dokumentide seadus (ITDS)<sup>81</sup> § 9<sup>4</sup> lg 1 selgitab, et ID-kaardile kantakse tavapärast kaks sertifikaati: digitaalset tuvastamist võimaldav sertifikaat ja digitaalset allkirjastamist võimaldav sertifikaat, mille väljastab dokumendi väljaandja. ITDS § 9<sup>4</sup> lg 3 alusel võib dokumendi väljaandja dokumenti kantava digitaalset allkirjastamist võimaldava sertifikaadi väljaandmiseks anda lepingu alusel üle kohustusi digitaalallkirja seaduse § 18 lg-s 1 nimetatud sertifitseerimisteenuse osutajale<sup>82</sup> või ITDS § 9<sup>4</sup> lg 4 alusel dokumenti kantava digitaalset tuvastamist võimaldava sertifikaadi tehnilise moodustamise anda lepingu alusel üle sellealast pädevust omavale teenuse osutajale.<sup>83</sup> Kuivõrd käesolev tehniline lahendus keskendub sertifikaadile, mis ei võimalda digitaalse allkirja või templi andmist, siis ei ole antud kontekstis sertifikaat käsitletav “Digitaalallkirja seaduse” mõistes.

Tehniline lahendus näeb ette, et riigiasutuse IT-üksus loob asutuse töötajatele nende avaliku võtme alusel täiendava sertifikaadi. Avalikustatakse sertifikaadid, mis on seotud avalike meiliaadressidega.

Kuivõrd tehniline lahendus näeb ette, et sertifikaat sisaldab riigiasutuses töötava isiku isikuandmeid (nimi ja emailiaadress), tuleb analüüsida isikuandmete kaitse seadusest tulenevaid nõudeid. Isikuandmete vastutavad ja volitavad töötajad peavad arvesse võtma isikuandmete töötlemise põhimõtteid (näiteks minimaalsuse põhimõtet, mille alusel isikuandmeid võib koguda ja töödelda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks) (IKS § 6). Samuti tuleb jälgida teisi isikuandmete kaitsest tulenevaid nõudeid, mis on detailsemalt lahti kirjutatud esimese lahenduse all.

Nagu eelpool selgitatud, on IKS § 10 kohaselt isikuandmete töötlemine lubatud üksnes andmesubjekti nõusolekul, seaduse alusel või kui haldusorganipoolne töötlemine on vajalik avaliku ülesande täitmise käigus seaduse, välislepingu või EL Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud kohustuse täitmiseks.

---

<sup>81</sup> Isikut tõendavate dokumentide seadus, RT I, 06.04.2016, 5, <https://www.riigiteataja.ee/akt/106042016005?leiaKehtiv>

<sup>82</sup> Vt ka ERS eelnõu § 25. Isikut tõendavate dokumentide seaduse muutmise, mille alusel isikut tõendavate dokumentide seaduse § 9<sup>4</sup> lõige 3 muudetakse ja sõnastatakse järgmiselt: „(3) Dokumendi väljaandja võib dokumenti kantava digitaalset allkirjastamist võimaldava sertifikaadi väljaandmiseks anda lepingu alusel üle kohustusi Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 „e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul“ rakendamise seaduse nõuete kohasesse usaldusnimekirja kantud kvalifitseeritud usaldusteenuse osutajale.“

<sup>83</sup> Vt ka Digitaalse isikutunnistuse vorm, tehniline kirjeldus ja digitaalsele isikutunnistusele kantavate andmete loetelu, RT I, 03.12.2015, 19, <https://www.riigiteataja.ee/akt/103122015019>

Riigiasutustes töötavate ametnike ja töötajate nime ja meiliaadressi veebis avalikustamise ning selle taaskasutamise seaduslikkuse üldise aluse leiame AvTS-st. AvTS § 28 lg 1 p 6 sätestab, et teabevaldajal on kohustus avalikustada riigi- ja kohaliku omavalitsuse asutuste koosseisud ja neis asutustes ettenähtud ametikohti täitvate ametnike ees- ja perekonnanimed, hariduse ja eriala, telefoninumbrid ning emailiaadress. Need andmed tuleb AvTS §-s 31 nimetatud teabevaldajal AvTS § 29 lg 1 alusel avalikustada veebilehel. AKI üldjuhend täpsustab, et mitte kõikide ametnike ja töötajate kontaktandmed ei kuulu võrgulehel avalikustamisele. AvTS § 35 lg 1 punkti 3<sup>1</sup> piirangu alla kuuluvad näiteks sisejulgeoleku tagamise, riigikaitsepoliitika kujundamise, riigikaitse korraldamise sh riigi sõjalise kaitse planeerimise, ettevalmistamise ja juhtimise või riigisaladuse ja salastatud välisteabe kaitse korraldamisega tegelevad ametnike ja töötajate kontaktandmed.<sup>84</sup> AKI selgitab ka olukordi, kus ametniku või töötaja otsekontaktide avalikustamine veebilehel ei pruugi olla otstarbekas.<sup>85</sup>

Kui avalikku teavet, mille üldist kasutamist ei ole seadusega või seadusega kehtestatud korras piiratud, kasutatakse eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi, on tegu avaliku teabe taaskasutamisega AvTS § 3<sup>1</sup> lg 1 mõistes. AvTS § 3<sup>1</sup> lg 7 näeb ette, et kui seaduse alusel avalikustatav teave sisaldab isikuandmeid, võib sellise teabe üldist kasutamist piirata, kui selle üldiseks kasutamiseks andmine kahjustab oluliselt isiku eraelu puutumatust. Enne teabe üldiseks kasutamiseks andmist peab teabevaldaja hindama teabe üldisele kasutamisele piirangute kehtestamise vajadust (AvTS § 3<sup>1</sup> lg 3).<sup>86</sup> Seega, v.a. seaduses loetletud erandite korral, ei keela AvTS riigiasutustes töötavate ametnike ja töötajate nimede ja meiliaadresside taaskasutamist käesoleva tehnilise lahenduse tarbeks loodavates sertifikaatides ja nende avalikustamisel. Ka riigil endal võiks olla huvi oma asutustes töötavate ametnike ja töötajate käesoleva tehnilise lahenduse kontekstis käsitletavate sertifikaatide avalikustamise osas, sest see võimaldaks kodanikul soovi korral riigiesindajatega turvaliselt suhelda.

## Sertifikaatide kehtivuse kontrolli regulatsioon

LDAP-i kasutamise osas tuleb analüüsida LDAP-i kataloogi kasutamisele hetkel kehtivat regulatsiooni.<sup>87</sup> ITDS § 9<sup>4</sup> lg 6 sätestab, et “digitaalset tuvastamist võimaldav sertifikaat ja

---

<sup>84</sup> AKI AvTS Üldjuhend lk 21,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)

<sup>85</sup> AKI AvTS Üldjuhend lk 23,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)

<sup>86</sup> Vt ka AKI AvTS üldjuhend lk 34-35,

[http://www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTS%20%C3%BCldjuhend%2030.03.2016.pdf)

<sup>87</sup> LDAPi kataloogi kättesaadavuse regulatsioon on kehtivas õiguskorras hägune. Algselt loodi LDAP-kataloog selliselt, et otsingut sai läbi viia ainult ühte elementi teades: kas eesnime, perekonnanime või isikukoodi. Selline funktsionaalsus võimaldas lisaks olemasolevate andmete kontrollimisele, mis on sertifikaadi kehtivuse kontrollimise peamine eesmärk, tegeleda ka konkreetse inimese ja temaga sugulus- või hõimlussuhete mõttes seotud inimeste otsimisega. Endise õiguskantsleri Allar Jõksi arvamus leidis 2006. aastal, et sellisel viisil isikukoodi igapäevase kättesaadavus suurendab ohtu kuritarvitusteks ja identiteedivargusteks. Lisaks saab isikukoodist teada isiku sünniaja, mis ei ole sertifikaadi kontrollimise saavutamiseks vältimatult vajalik. Seoses sellega, et taoliseks isikuandmete töötlemiseks puudus seaduslik alus ning et see oli vastuolus IKS § 12-ga, mille alusel on isikuandmete avalikustamiseks vajalik andmesubjekti

digitaalset allkirjastamist võimaldav sertifikaat on seotud dokumendi kasutaja isikuandmetega ja avalikult kontrollitavad isikukoodi kaudu”. Praeguses sõnastuses on võimalik sätet tõlgendada mitmel viisil. Üks tõlgendus on, et säte lubab isikukoodi alusel kontrollida vaid sertifikaadi kehtimist (seega järgides minimaalsuse põhimõtet). Samal ajal on võimalik sätet tõlgendada nii, et isikukoodi alusel saab kontrollida nii sertifikaadi kehtimist kui ka sertifikaadi sisu (s.t. näiteks isikukoodile vastava isiku ees- ja perekonnanime). Viimane tõlgendus on ka hetkel praktikas kasutusel. Kehtiva seaduse kohaselt ei saa sertifikaati kontrollida vaid ees- ja perekonnanime abil.

Kuivõrd kodanikel on õigustatud ootused turvaliste suhtluskanalite osas ning seda eriti suhtluses riigiga, võiks seadusandja kaaluda teatud tingimustel isikukoodide hõlpsama kasutatavuse krüpteerimise eesmärgil. Teeme ettepaneku sertifitseerimisteenuse osutaja poolt pakutav sertifikaadi kontrollimise võimaluse protsessi (hetkel LDAP kataloogi kaudu) kasutusloogikale määratud tingimused uuesti läbi vaadata ning sertifikaadi kontrollimise teenuse pakkumise sisu ITDS-s täpsustada. Lisaks võiks sertifitseerimisteenuse osutaja täiendavalt avaldada sertifikaatide kehtivuse kontrollimisel isikuandmete töötlemise põhimõtted. Soovitame küsida ka õiguskantsleri arvamust, kes oma hiljutises sõnavõtus väljendas selget poolehoidu krüpteerimise eesmärgil isikukoodide vaba kättesaadavuse osas.<sup>88</sup>

Kui sertifitseerimisteenuse osutaja poolt sertifikaatide kehtivuse kontrollimiseks vajalike isikuandmete töötlemise alused leiduvad seaduses, pole andmesubjektidelt eraldi nõusolekut küsida vaja. Kui siiski eraldi andmesubjekti nõusolekut on vaja, võib andmete töötlemiseks andmesubjekti nõusoleku küsida ning isikuandmete töötlemise aluseid selgitada ID-kaardi väljastamisel (hetkel tehakse seda dokumendis “Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused”<sup>89</sup>).

## Kehtiva õiguse muutmise vajadus

Lahendusidee näeb ette, et tehnilise lahenduse kasutamine ei ole kogu riigiasutustevahelise e- kirjavahetusele kohustuslik vaid rangelt soovitatav. Võib kaaluda tehnilise lahenduse kasutamise loetlemist ühe asutusesisese teabe terviklikkuse, käideldavuse ja konfidentsiaalsuse kaitseks rakendatavate organisatsiooniliste, füüsiliste ja infotehniliste turvameetmetena, mida saab täpsustada AvTS § 43 lg 3 alusel Vabariigi Valitsuse poolt välja antavas määruses. Soovi korral võib nimetatud määruses selle lahenduse kasutamise asutusesiseseks tunnistatud teabe töötlemisel muuta kohustuslikuks. Samas määruses võib viidata ka täiendavalt välja antavatele juhiste, mis käesolevas lahenduses välja pakutud krüpteerimise lahenduse kasutamist ja rakendamist

---

nõusolek, soovitas Jõks LDAP kataloogi toimimismehhanisme muuta. Sellest lähtuvalt muudeti 2006. aastal LDAP-kataloogis isikute sertifikaatide otsingut. Seega saab kehtiva LDAP-kataloogi kasutamiskohaselt esmane adresseerimine toimuda otse isikukoodi või registrikoodi kasutades. Edaspidi saab rakendada kasutatud sertifikaatide loetelu selleks, et vajalikku nime isikukoodiga kokku viia. Vt Aasta Tegevuse Ülevaade' (2007) 269–272 <[http://oiguskantsler.ee/sites/default/files/õiguskantsleri\\_2006.\\_aasta\\_tegevuse\\_ulevaade.pdf](http://oiguskantsler.ee/sites/default/files/õiguskantsleri_2006._aasta_tegevuse_ulevaade.pdf)>.

<sup>88</sup> Interneti 2016 Päev, Ülle Madise sõnavõtt paneelis, <http://video.postimees.ee/3637167/postimehe-ulekanne-mida-eestlane-internetis-teeb>

<sup>89</sup> Sertifitseerimiskeskus, Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused, 25.01.2016,

[https://www.sk.ee/upload/files/ESTEID\\_Kasutustingimused\\_20160125.pdf](https://www.sk.ee/upload/files/ESTEID_Kasutustingimused_20160125.pdf)

detailsemalt kirjeldavad. Lisaks võib AKI anda soovituslikke juhiseid AvTS-i rakendamiseks (AvTS § 45 lg 4).

Sarnaselt eelmises lahenduses väljapakutavale võib alternatiivse lahendusena täiendavalt analüüsida ka AÜA määruse sisulise uuendamise otstarbekust. Põhimõtteliselt saaks määrust uuendada viisil, et määruse reguleerimisalasse lisanduks riigiasutustevaheline e-kirjavahetus ning määruses kehtestada nõuded e-kirjavahetussüsteemile kehtivatele infoturbealastele meetetele sh krüpteerimisele.

## Tugevused

- + S/MIME toetav laiendus on integreeritud enamustesse meili-süsteemidesse, sh veebimeil ja mobiililahendused
- + S/MIME ja DNSSEC on rahvusvaheliselt tunnustatud standardid
- + Meile saab saata ja vastu võtta turvaliselt ka ilma spetsiaalse tarkvaralaiendusega (kuigi see eeldab kasutajalt natuke põhjalikumaid oskuseid)
- + DNSSEC-i paigutatavad avalikud võtmed ei pea olema tingimata ID-kaardiga seotud
- + Krüpto-võimelisele välispartnerile saab edastada ka selliselt, et väline partner ei pea omama ID-kaarti

## Puudused

- Ei lahenda probleemi ametniku suhtlusel krüpto-võimekuseta kodanikuga
- Lahendab ainult osaliselt probleemi ametniku suhtlusel välisametnikuga
- Ei lahenda listide probleemi
- Loob juurde uued ohud seoses sellega, et DLP võimalus jääb ainult lõppseadmesse
- Serverites ei oleks enam võimalik sõnumite sisu analüüs
- Kirjale antav allkiri ei oleks Digitaalallkirja seaduse<sup>90</sup> kohaselt digitaalallkiri (samaväärne omakäelise allkirjaga)

## Ressursivajadus

- Arenduskulu ID-kaardi tarkvara draiver - 2 kuud (4 inimtöökuud)
- Arenduskulu sertifikaadi väljalaskeks ja DNS-i puusse DNSSEC-le sobival kujul automaatseks lisamiseks - 1 kuu
- Keskse LDAP protokolliga DNSSEC-ist otsimise lahenduse loomine - 2 kuud
- Asutusepõhised kulud
- Arenduskulud, et luua meilikliendi plugin, mis võimaldaks kasutajal teha lihtsamalt turvaotsuseid - ligikaudu 4 kuud. See plugin ei ole otseselt vajalik, kuid samas suurendaks tõenäosust, et krüpteerimine on tõestatud õigesti ning annaks võimaluse saata mitmele osapoolle kirju nii, et ainult osad kirjad on krüpteeritud.

---

<sup>90</sup> Digitaalallkirja seadus, RT I, 14.03.2014, 12, <https://www.riigiteataja.ee/akt/694375?leiaKehtiv>

- Sertifikaadi väljalase - mõni minut kasutaja kohta - kui draiveri ja ID-kaardi tarkvara laiendus on õigesti tehtud
- Automaatne kliendi arvutite häälestamine näidiste olemasolul. Aega kulub mõni minut arvuti kohta

Ülejäänud haldust võib pidada tavapärase halduse osaks.

Hinnanguline kogumaksumus koos koolitustega oleks ligikaudu 580 tuhat eurot.

Pilootprojekti hinnanguline maksumus oleks 145 tuhat eurot.

Ilma meilikliendi pluginat arendamata ca 109 tuhat eurot.

## **Haldamine ja selle koordineerimine**

Lõppkasutaja seadme tarkvara paigaldus, häälestamine ja laiendamine on asutust teenindava IT-üksuse ülesanne ja nende tegevuste lihtsustamiseks tuleb IT-üksusele anda vastavad abivahendid.

Antud lahendusidees on IT-üksuse ülesandeks ka kasutajapõhiste avalike võtmete sidumine meiliaadressidega ja selle info avaldamine DNS-i väljatöötatud abivahendeid kasutades.

Olenevalt sellest, kuidas lahendatakse tehnilise lahenduse haldamine ja koordineerimine, võib osutada vajalikuks ka vastavalt uuendada koordineeriva ja haldava asutuse põhimäärust<sup>91</sup> ning muid seotud normatiivdokumente. Eelpool nimetatud IT-üksuste ülesanded võib vajadusel täpsemalt määratleda ka määruses “Infoturbe juhtimise süsteem”<sup>92</sup>, milles muuhulgas sätestatakse terviklik juhtimismeetmete kompleks, mis võimaldab tagada asutuse põhitegevuse jätkusuutlikkuse ja infovarade kaitstuse (määruse § 2 (3)).

Meiliserverite halduslahendusi ei muudeta, kuid peame heaks ideeks meiliserverite haldamise konsolideerimist, sest see aitaks parandada süsteemide käideldavust ning haldusteenuse kvaliteeti.

ID-kaardi tarkvara arendamis- ja uuendustegevused jäävad RIA ülesandeks.

---

<sup>91</sup> Riigi Infosüsteemi Ameti põhimäärus RT I, 26.02.2016, 2 § 15 (11), <https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv>

<sup>92</sup> Infoturbe juhtimise süsteem, RT I, 19.03.2012, 4, <https://www.riigiteataja.ee/akt/119032012004>

## **Idee 3 – DigiDoc plugin meilikliendi ja brauseri jaoks**

### **Idee mõju ulatus: Potentsiaalselt kõik Eesti vabariigi residendid**

Idee aluseks on kasutada olemasolevat Eesti Vabariigi võtmehalduse süsteemi ilma täiendavaid sertifikaate välja andmata ja ilma lisanduvat kesket sõnumivahetuse süsteemi loomata.

Tüüpiliselt on x.509 sertifikaat seotud meiliaadressiga. Samas teisele osapoolle krüpteerimist ei pea otseselt meiliaadressiga siduma.

Selleks, et parandada ja kiirendada krüpteerimise protsessi, soovitame kasutusele võtta plugina, mis sobib riigi jaoks rohkem kasutatud meilisüsteemidesse ja kiirendab DigiDoc-i allkirjastamise ja DigiDoc Krüpto kasutamist.

Plugin võimaldaks meili sisu krüpteerida sellisel moel, et seda oleks võimalik lugeda ka tavalise DigiDoc Krüpto programmiga (vastavat pluginat omamata). Plugin võimaldaks ka meili sisu allkirjastada sellisel kombel, et allkirja on võimalik näha ja kontrollida DigiDoc tarkvaraga.

### **Kehtiv regulatsioon ja selle muutmise vajadus**

Hetkel reguleerib digitaalset allkirjastamist juba mainitud DAS, mille asendab tulevikus eIDAS määrus. Hetkel on arutusel juba viidatud Euroopa Parlamendi ja nõukogu määruse nr 910/2014 „e identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul“ rakendamise seaduse eelnõu. Digiallkirjastamiseks vajalike sertifikaatide dokumendile kandmist ning nende väljaandmist reguleerib ITDS. Sertifikaatidel sisalduvat infot sätestab määrus “Digitaalse isikutunnistuse vorm, tehniline kirjeldus ja digitaalsele isikutunnistusele kantavate andmete loetelu”.<sup>93</sup> Sertifitseerimisteenuse pakkuja on omalt poolt täpsustanud sertifikaatide kasutustingimusi<sup>94</sup> ning sertifitseerimispõhimõtted.<sup>95</sup> Loetletud aktides analüüs muudatuste vajadust käesoleva tehnilise lahenduse kontekstis ette ei näe.

Sarnaselt eelmises lahenduses leitule tuleb korrata, et krüpteerimise teeks kasutaja jaoks lihtsamaks eelmise tehnilise lahenduse juures analüüsitud sertifikaatide kehtivuse kontrollimise teenuse parem kättesaadavus. Selleks tuleks täpsustada sertifikaadi kontrollimise teenuse pakkumise õiguslikke aluseid ITDS-s viisil, mis võimaldaks sertifikaadi kontrollimise ning isikukoodi kättesaadavuse ka isiku nime alusel. Lisaks võiks sertifitseerimisteenuse osutaja täiendavalt avaldada sertifikaatide kehtivuse kontrollimisel isikuandmete töötlemise põhimõtted.

Sarnaselt eelmisele lahendusele näeb ka see lahendusidee ette, et tehnilise lahenduse kasutamine ei ole kogu riigiasutustevahelise e-kirjavahetusele kohustuslik vaid rangelt soovitatav. Võib kaaluda tehnilise lahenduse kasutamise loetlemist ühe asutusesisese teabe terviklikkuse, käideldavuse ja konfidentsiaalsuse kaitseks rakendatavate organisatsiooniliste, füüsiliste ja infotehniliste

---

<sup>93</sup> Digitaalse isikutunnistuse vorm, tehniline kirjeldus ja digitaalsele isikutunnistusele kantavate andmete loetelu, RT I, 03.12.2015, 19, <https://www.riigiteataja.ee/akt/103122015019>

<sup>94</sup> Sertifitseerimiskeskus, Sertifikaatide kasutustingimused, <https://www.sk.ee/repositoorium/kasutustingimused/>

<sup>95</sup> Sertifitseerimiskeskus, Sertifitseerimispõhimõtted, <https://www.sk.ee/repositoorium/CPS/>

turvameetmetena, mida saab täpsustada AvTS § 43 lg 3 alusel Vabariigi Valitsuse poolt välja antavas määruses. Soovi korral võib nimetatud määruses selle lahenduse kasutamise asutusesiseseks tunnustatud teabe töötlemisel muuta kohustuslikuks. Samas määruses võib viidata ka täiendavalt välja antavatele juhistele, mis käesolevas lahenduses välja pakutud krüpteerimise lahenduse kasutamist ja rakendamist detailsemalt kirjeldavad.

Sarnaselt eelmistes lahendustes väljapakutavale võib alternatiivse lahendusena täiendavalt analüüsida ka AÜA määruse sisulise uuendamise otstarbekust ning eelnevalt viidatud "Infoturbe juhtimise süsteemi" määruse täendamist.

### **Tugevused**

- + Kui kaasneb ID-kaardi tarkvaraga, siis on sees pidevas uuendus-tsükklis
- + Riigiasutustel on välja kujunenud poliitika antud tarkvara uuendamiseks
- + RIA-l on kogemusi, kuidas krüpto-tarkvara välja vahetada
- + Ei lisandu litsentsikulused asutustele

### **Puudused**

- Tuleb nullist arendada
- Erinevate meiliklientide ja brauserite liidestused lisavad keerukust
- Kolmandate osapooltega suhtluseks (kellel ID-kaarti pole) ei paku lahendust
- Tavakasutajate käitumisharjumisi tuleb muuta
- Püsikulud tarkvara arendamisele ja hooldamisele
- Võimalik mainekahju tehniliste probleemide korral

### **Ressursivajadus**

Hinnanguliselt kuni 4 kuud tööd (ca. 16 inimtöökuud) täpsemaks disainimiseks, arenduseks. Koguinvesteeringu maksumuseks (koos koolitustega) oleks ligikaudu 560 tuhat eurot. Pilootprojekti maksumus oleks ligikaudu 31 tuhat eurot.

### **Haldamine ja selle koordineerimine**

Lõppkasutaja seadmesse tarkvara paigaldus, tarkvara häälestamine ja laiendamine on asutust teenindava IT-üksuse ülesanne.

Enamasti oleks haldamine teostatav keskselt sarnaselt DigiDoc tarkvara arenduse ja uuendamisega. Haldamist ja uuendamist koordineeriks RIA, kus on selle jaoks juba vastav töögrupp.

Haldamise lisakulud on RIAle hinnanguliselt 28 tuhat eurot iga suurema operatsioonisüsteemi või meilikliendi muudatuse kohta.

## 7. Soovitavad nõuded praeguste süsteemide turvalisuse aspektide parandamiseks

Lihtsaim viis ennetada sõnumisaladuse rikkumisega seonduvaid probleeme on rakendada infoturvet sõnumi transpordil serverite vahel. Eesti ja rahvusvahelistest parimatest praktikatest tulenevalt on selleks järgnevad alternatiivid:

- a) SMTP TLS kasutuselevõtt
- b) Laiem krüpteeritus organisatsioonide vahel IPsec-i kasutades
- c) VPN organisatsioonide vahel
- d) Täielikult organisatsiooni(de) kontrolli all olevad ühendusliinid (n-ö „must fiiber“)

Kõik krüpteerimise meetodid suurendavad riski kasutaja poolt kõrgelt hinnatud käideldavusele ja eeldavad käideldavuse tagamiseks korraliku monitooringu ja muudatuste planeerimise olemasolu. Järgnevalt on iga mainitud alternatiivi pikemalt lahti seletatud.

### SMTP TLS

SMTP TLS-i kasutuselevõtt on kõige lihtsam. Hetkel on TLS-i implementeerimine kohati puudulik. Enamuses olukordades eelistatakse käideldavust sõnumi saatmisel turvalisusele, mis võib anda võimaluse vahendusründeks.

Riigiasututele kuuluvad meiliserverid peaks häälestama selliselt, et nad vahetaksid infot ainult krüpteeritult. See eeldab nii riigiasutuse enda kui teiste osapoolte krüpteerimise võimekuse seiret tuvastamiseks sertifikaatide aegumist ja võimaliku rünnet.

Samuti eeldab see riigiasutuste omavahelisi kokkuleppeid turvalise meilikommunikatsiooni nõudmiseks. Samas saab TLS-i võimekust kasutusel võtta ilma selliseid kokkuleppeid omamata.

Sertifikaatide valik TLS kasutamiseks ei tohiks olla problemaatiline ka rahalistes kitsikustes.<sup>96</sup> TLS sertifikaadi puhul on kindlasti alternatiiviks DANE<sup>97</sup> kasutuselevõtt. Lisaks on Eestis võimalik kasutada näiteks SK sertifikaate, mille aastane hind serveri kohta on ligikaudu 90€ (lisandub käibemaks) aastas<sup>98</sup> või mõne teise sertifitseerimisteenuse pakkuja sertifikaate (nt startssl.com). Loomulikult ei tohi ära unustada julgeolekuküsimust.

Peidetud lisakulud võivad olla MTA uuendamise vajadus krüpto toetamiseks, seiresüsteemi implementeerimine (seda võib teha ka mitme asutusega ühiselt) ja süsteemi halduri harimine. Esmane juurutamine ei tohiks võtta üle ühe tööpäeva.

Kõige ajamahukamaks ja ennustatumaks võib olla sertifikaadi ostmisega seotud hange.

---

<sup>96</sup> Tasuta jagavad sertifikaate näiteks <https://letsencrypt.org> ja <https://startssl.com>

<sup>97</sup> The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA <https://tools.ietf.org/html/rfc6698>

<sup>98</sup> <https://www.sk.ee/teenused/hinnakiri/asutuse-sertifikaadid/>

## IPSec kasutus

IPSec-i kasutuselevõtmine annab võimaluse krüpteerida laiemat hulka kommunikatsiooni organisatsioonide vahel tehes seda võrgu kihil. IPSec võimaldab toimida kui *multipoint* arhitektuur.

Samas on IPSec protokoll keerukam kui TLS ja seega tõenäoliselt ka vigade suhtes tundlikum.<sup>99</sup>

Enamus tänapäevaseid võrguseadmeid peaks IPSeci-i toetama. Samas võib probleemiks saada protsessori jõudlus. Lisaks eeldab IPSec kasutuselevõtt organisatsioonide vahel koheseid kokkuleppeid.

IPSeci võib teatud juhtudel vaadelda kui VPN-i alaliiki.

Tulenevalt nimetatud aspektidest soovitame IPSeci implementeerimist kaaluda.

## VPN organisatsioonide vahel

Võrkude omavaheline ühendamine transpordi tasandil või kõrgemal eesmärgiga meilivahetus ja teiste organisatsioonide sisemistele ressurssidele juurdepääs eeldab mõlemal pool sarnase tehnoloogilise koosluse kasutuselevõttu. VPN-ide loomiseks on mitmeid alternatiive.

VPN-i ühenduse loomisel eeldatakse tavaliselt punktist punkti arhitektuuri, mis võib mitme organisatsiooni vahelise kommunikatsiooni teha väga keeruliseks.

## Must Fiiber

Siin kehtib eeldus, et organisatsioonide vahel on privaatne sisevõrguna kasutatav võrk. Must fiiber on väga hea võimalik lahendus positiivsete mõjudega käideldavusele eeldusel, et organisatsioon omab füüsilist kontrolli ruumide ja kaablikaevude üle, mida see kaabeldus läbib. Muudel juhtudel tuleb selle kihi peal rakendada omale sobilikku eelmainitud krüptograafia lahendust.

## DNS-i turvalisuse suurendamine

Üheks võimalikuks ründevektoriks on DNS nimede hõive valetades DNS-i vastuseid; selle ründe tõenäosuse vähendamiseks soovitame implementeerida DNSEC-i.

DNSSEC-i implementeerimine annab võimalus DANE kasutamiseks nii TLS-i kui S/MIME tarbeks.

DNSSEC-i esialgene implementeerimine võib olla väga madala kuluga. Näiteks hetkel Zone pakub seda 0 euro eest aastas juhul, kui nimed osta nende juurest.<sup>100</sup>

---

<sup>99</sup> <https://www.schneier.com/cryptography/paperfiles/paper-ipsec.pdf>

<sup>100</sup> <https://www.zone.ee/blogi/2014/09/01/zone-varskendus-ja-tasuta-dnssec-taisteenus/>

## Usalduse suurendamine sõnumi allika ja saaja vahel

Saaja meiliserveri jaoks saatja autentsuse kontrollimise lihtsustamiseks tuleb kasutusele võtta SPF (Sender Policy Framework).

Kasutuselevõtt on lihtne ning eeldab kirje tekitamist DNS-i.

Soovituslik oleks kasutada ka DKIM (Domain Keys Identified Mail) lahendust, mis tagab ka serveri poolt saadetud sõnumi tervikluse.<sup>101</sup> Selle kasutuselevõtt on keerulisem ning võib eeldada meiliserveri uuendamist.

Lisaks võtta kasutusele DMARC (Domain-based Message Authentication, Reporting and Conformance) lahendus, mis SPF-i ja DKIM-i omavahel kokku seob tuues välja organisatsiooni poliitikad selles osas, kuidas SPF-i ja DKIM lahendust pakutakse. Samal ajal tuleb silmas pidada, et säärane rakendamine võib kaasa tuua ka mõned probleemid (toodud välja järgnevas tabelis).<sup>102</sup>

	Tavalised kasutused	Mida mõjutab negatiivselt
Aliased	Edasi suunamisel, mitu ühele konsolideerimine, edevuse aadressid	SPF
Edasi saatja	Meiliprogrammi tasemel edasisuunamine	SPF & DKIM
Meililist	Listisõnumi saatmine saatja nimel ja postitamine listi modifikatsioonidega (nagu näiteks jalus, mis identifitseerib maili listi)	SPF & DKIM resultaadid võivad viia DMARC poliitika tagasilükkamiseni ja listist välja langemiseni
Lüüs	Piiramatu sõnumite ümber kirjutamine ja edastamine	SPF & DKIM
Perimeetri filtrid	Spämm või kurivara filtrid, mis muudavad või kustutavad sõnumisisu	DKIM

---

<sup>101</sup> <http://dkim.org/>

<sup>102</sup> [http://csrc.nist.gov/publications/drafts/800-177/sp800-177\\_second-draft.pdf](http://csrc.nist.gov/publications/drafts/800-177/sp800-177_second-draft.pdf)

## Riigisaladuse töötlemine

Järgnevalt anname põgusa ülevaate riigisaladuse töötlemisele kehtivatest normatiivaktidest ning viitame riigisaladuse elektroonilisele töötlemisele kehtestatud peamistele nõuetele. Kuivõrd täpsemad nõuded elektroonilise teabeturbe tagamiseks on sätestatud “piiratud” tasemega riigisaladuseks tunnistatud dokumentides, siis piirub allolev ülevaade avalikult kättesaadavate normatiivaktidega.<sup>103</sup>

Riigisaladuse ja salastatud välisteabe seadus (RSVS)<sup>104</sup> kaitseb riigisaladust ja salastatud välisteavet avalikuks tuleku ja juurdepääsuõigusetu isikule teatavaks saamise eest (RSVS § 1) ning Vabariigi Valitsuse määrus “Riigisaladuse ja salastatud välisteabe kaitse kord” (RSVKK)<sup>105</sup> kehtestab riigisaladuse ja salastatud teabekandjate töötlemise täpsemad nõuded.

Teabevaldaja<sup>106</sup> on kohustatud kasutusele võtma nõuetekohased organisatsioonilised, füüsilised ja elektroonilise teabeturbe meetmed riigisaladuse kaitseks (RSKS § 20 lg 1).<sup>107</sup> Olulise põhimõttena hinnatakse salastatud teabekandjat<sup>108</sup> tervikuna tema eri osade kõrgeima riigisaladuse tasemega (RSKS § 17 lg 1).

Riigisaladuse edastamine on üks riigisaladuse töötlemise vorme, mida reguleerib täpsemalt RSKS § 35, kusjuures nõuded edastamisele võivad erineda olenevalt sellest, kes kellele riigisaladust edastab. RSVKK § 102 järgi on salastatud teabe edastamine tehnilise sidekanali kaudu lubatud ainult juhul, kui kasutatakse asjakohasel tasemel teabe edastamiseks akrediteeritud süsteemi.<sup>109</sup>

Elektrooniline teabeturbe tähistab riigisaladuse või salastatud välisteabe käideldavuse, salajasuse ja terviklikkuse tagamist töötlussüsteemis (RSKS § 3 p 10). Selleks kehtestatud nõuete täitmist kontrollib Teabeamet (RSKS § 23 lg 1 p 1). RSVKK § 105 loetleb elektroonilise teabeturbe nõuded salastatud teabe kaitseks selle elektroonilisel töötlemisel. Näiteks võib salastatud teavet elektrooniliselt töödelda ainult salastatud teabe töötlussüsteemis, mis vastab elektroonilise teabeturbe nõuetele ning millel on Teabeameti<sup>110</sup> antud kehtiv vastavussertifikaat või ajutine

---

<sup>103</sup> Riigisaladuse töötlemisele kehtivad eelnevalt analüüsitud kehtivast regulatsioonist erinevad normatiivaktid. Näiteks AvTS ei kohaldu riigisaladuseks või salastatud välisteabeks oleva teabe suhtes (AvTS § 2 lg 2 p 1). Samuti ei kohaldu ISKE määrus riigisaladust töötlevate infosüsteemide turbeks (ISKE määrus § 1 lg 3).

<sup>104</sup> Riigisaladuse ja salastatud välisteabe seadus, RT I, 12.03.2015, 46,

<https://www.riigiteataja.ee/akt/112032015046?leiaKehtiv>

<sup>105</sup> Riigisaladuse ja salastatud välisteabe kaitse kord, RT I, 19.08.2014, 22,

<https://www.riigiteataja.ee/akt/119082014022?leiaKehtiv>

<sup>106</sup> Asutus, põhiseaduslik institutsioon või juriidiline või füüsiline isik, kelle valduses on riigisaladus või salastatud välisteave (RSKS § 3 p 4).

<sup>107</sup> RSVKK § 22 sätestab nõuded riigisaladust valdava asutuse, põhiseadusliku institutsiooni ja juriidilise isiku riigisaladuse kaitse juhendile, kus võib muuhulgas sätestada ka riigisaladuse töötlussüsteemi turvanõuete rakendamise juhendi (RSVKK § 22 lg 2 p 7).

<sup>108</sup> Mistahes objekt, millele on jäädvustatud riigisaladus või salastatud välisteave (RSKS § 3 p 3).

<sup>109</sup> Vt ka Tehnilise sidekanali kaudu edastamise erandid, RSVKK § 102.

<sup>110</sup> Muuhulgas algatab Teabeamet teabevaldaja taotlusel või omal algatusel töötlussüsteemi akrediteerimise, korraldab ja kontrollib riigisaladuse kaitseks kasutatavate krüptomaterjalide töötlemist ning annab nende töötlemiseks juhiseid ja teavet, ja rakendab turvarikke või selle tekkimise ohu korral töötlussüsteemi kaitseks turvameetmeid (RSKS § 23 lk 2 p 3, 6, 7).

kasutusluba.<sup>111</sup> RSVKK § 105 lg 6 loetleb elektroonilise teabeturbe tagamise peamised põhimõtted: minimaalsus, turvariskide pideva haldamise põhimõtte ja süsteemi turvalisuse regulaarne kontrollimine, privileegide piiratus, isekaitsvate sõlmede kasutamise põhimõtte ning sügavuti kaitse põhimõtte. RSVKK § 106 täpsustab töötlussüsteemile esitatavad nõuded. Näiteks peab salastatud teabe töötlussüsteem võimaldama “tuvastada ja registreerida isikud, kes omasid või võisid omada juurdepääsu salastatud teabele ja selle kaitsmist toetavatele süsteemitoimingutele ja -vahenditele; eristada süsteemi kasutajaid salastatud teabele juurdepääsu õiguse põhjal; juurdepääsu teabele ja selle kaitsmist toetavatele süsteemitoimingutele ja -vahenditele üksnes juurdepääsuõiguse ja põhjendatud teadmismajaduse olemasolul; kontrollida teabe ning selle kaitsmist toetavate süsteemitoimingute ja -vahendite salajasust, terviklikkust, käideldavust, samuti nende päritolu, usaldatavust ja ühendusi” jne. RSVKK § 107 paneb töötlevale üksusele kohustuse välja arendada süsteemi turvanõuete loetelu, milles esitatakse süsteemi tehniline kirjeldus, ülevaade süsteemi riskianalüüsi tulemustest, süsteemile esitatavate turvanõuete kirjeldus, süsteemis rakendatavate turvameetmete loetelu, süsteemi turvalisuse korraldamise kirjeldus. Enne salastatud teabe töötlemiseks uue süsteemi ehitamist või kasutusele võtmist kooskõlastab töötlev üksus loetelu Teabeametiga (RSVKK § 107 lg 2).

Täiendavad nõuded elektroonilise teabeturbe tagamiseks on kehtestatud RSVS § 39 lg 2 alusel kolme määrusega. Määrustes “Krüptomaterjalide ning nende töötlemise ja kaitse nõuded”<sup>112</sup> ning “Kiirgusturbe tagamise nõuded”<sup>113</sup> kehtestatu on märgitud “piiratud” tasemel riigisaladuseks. Määrus “Arvutite ja kohtvõrkude kaitse nõuded”<sup>114</sup> kehtestatakse arvutite ja kohtvõrkude kaitse nõuded elektroonilise teabeturbe tagamiseks töötlussüsteemides (määruse § 1).

## Muud märkused

Sõnumivahetuse vahendina toodi välja ka tihe Skype kasutus. Enamikel juhtudel kasutatakse organisatsioonisiselt Skype for Business lahendust. Sellest tulenevalt võiks kaaluda Skype for Business instantside födereerimist, et parandada riigisiseste sõnumivoogude turvalisust.

---

<sup>111</sup> Vt ka RSKS § 46.

<sup>112</sup> Krüptomaterjalide ning nende töötlemise ja kaitse nõuded, RT I, 30.10.2015, 6, <https://www.riigiteataja.ee/akt/130102015006>

<sup>113</sup> Kiirgusturbe tagamise nõuded, RTL 2008, 21, 311, <https://www.riigiteataja.ee/akt/12937569>

<sup>114</sup> Arvutite ja kohtvõrkude kaitse nõuded, RTL 2007, 102, 1702, <https://www.riigiteataja.ee/akt/12905091>

# Lõppjärelused

## Tehnilised soovitusused

Antud eelanalüüsi käigus leiti, et mitmed riigiasutused ei kasuta mitmeid rahvusvahelisi parimaid praktikaid meilivahetuse turvalisuse tagamiseks. Järgnevate parimate praktikate järgimine võiks olla rangelt soovituslik: TLS, SPF, DNSSEC, DKIM, DMARC. Lisaks on soovitatav kaaluda IPsec kasutuselevõtmist organisatsioonidevahelise kommunikatsiooni turvalisuse parandamiseks.

- Serverite vahel tuleb rakendada SMTP protokollile TLS ning juurutada monitooring, mis seda kontrolliks.
- Otspunktkrüpteerimise (lõppkasutajalt lõppkasutajale krüpteerimise) korral on kõige mõistlikum DLP tegemine lõppseadmes.
- Soovitame kasutada aadresside reputatsiooni, kus kontrollitakse, kas antud aadressilt ollakse varem krüpteeritud meili saanud. Tekitada ja jagada organisatsioonide vahel krüpteeritud meilisaatjate "*whitelist*".
- Teha krüpteerivad meililistid, kus spetsiifiliselt välja töötatud list-server tegeleks võtmete ja erandite haldamisega.
- Rahvusvahelistest standarditest soovitame eelistada S/MIME koos X.509 standardile vastavate sertifikaatidega.
- Tavaliselt on *end-to-end* krüptograafia mõeldud ainult sõnumi edastamiseks, mitte selle pikaajaliseks salvestamiseks. Seega pakutud lahendustes pole võimalik võtmete taastamine. Tuleb laiendada meilisüsteemi ja kasutada asutuse digitemplit, et tagada saadetud/saadud sõnumite pikaajaline säilitamine.
- On tarvis rakendada seiresüsteeme, mis kontrollivad krüpteerimise rakendamist sõnumivahetuses.
- Konsolideerida võimalikult palju, sest krüpteerimisega seotud kesksete süsteemide haldus- ja disainivõimekuse saavutamine on üksikutel asutustel keerulisem.

## Mugavus

Lõppkasutaja koolitamine on vältimatu. Kuigi on väga oluline, et lõppkasutaja jaoks toimuksid turvalisust tagavad protsessid võimalikult lihtsalt, on kindlasti tarvis koolitada kõik tavakasutajad korrektselt turvaotsuseid tegema.

- PGP kasutamine jätkub, aga PGP ei pea olema tsentraalselt toetatud lahendus, sest seda kasutatakse suhteliselt vähe ning see on sageli tavakasutaja jaoks liiga keeruline.
- Exchange, Domino, GroupWise'i kalendrid on rakendused, mille funktsioonid kasutajaid nende kasutusharjumuste tõttu ühe või teise tootja tarkvara eelistama motiveerivad. Kasutajate harjumuste ega meiliklientide muutmine ei ole lihtne.
- Mitme erineva kiipkaardi kasutamine on lõppkasutajale ebamugav (nt asutusepõhise kiipkaardi ja Eesti ID-kaardi).

## Mobiilid

Mobiilsete seadmete kasutamisega seonduvalt toodi igas küsitletud asutuses välja vajadus põhjalikumalt uurida mobiilsete seadmetega seonduvaid turvaküsimusi, sh turvalist sõnumivahetust.

- Kui me võimaldame mobiilis meili lugemist, siis peavad ka viiruseotsija/-tõrje ning DLP mobiilis asuma.
- Mobiiliplatvormidele on vaja luua soovitud turvaeesmärkide saavutamiseks sobiva konfiguratsiooniga profiilid. Juhul kui see ei ole võimalik, siis tuleb valida teine mobiiliplatvorm.
- Turvaliseks sõnumivahetuseks mobiilsete seadmete abil on järgnevad võimalused:
  - o mobiilil (tahvelarvutil) on eraldi aadress digitaalse sertifikaadiga,
  - o uue põlvkonna ID-kaart NFC-ga, mida saaks mobiiliga kasutada,
  - o uue põlvkonna SIM-kaart (või e-SIM<sup>115</sup>), millel on laiendusvõimalused.

## Õiguslik pool

- Krüpteerimise roll andmete terviklikkuse ja konfidentsiaalsuse tagamisel on Euroopa Liidu andmekaitseraamistikus selgelt välja toodud.
- Eestis puudub kehtivast õigusest tulenev nõue riigiasutustevaheline e-kirjavahetus krüpteerida. Küll aga toetab riigiasutustevahelise e-kirjavahetussüsteemi krüpteerimise vajadust AvTS-st ning selle põhjal kehtestatud määrustest tulenev nõue kaitsta riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavaid infosüsteeme ning nendega seotud infovarasid ning juurdepääsupiiranguga andmeid.
- AvTS § 43 kehtestab asutusesisese teabeks tunnistatud teabe kaitse tagamiseks kohustuse, mille alusel peab teabevaldaja rakendama organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, et kaitsta asutusesisese teabe terviklikkust, käideldavust ning konfidentsiaalsust. Arvestades elektroonilisel teel saadetud asutusesiseseks tunnistatud teabe hulka, on oluline, et toimivad e-kirjavahetussüsteemid nimetatud nõuetele vastaksid.
- Kuna e-kirjavahetussüsteemis ei ole mõistlik eraldi turvameetmeid rakendada juurdepääsupiiranguga ja -piiranguta teabele, on otstarbekas võtta kasutusele lahend, mis tagaks kogu e-kirjavahetussüsteemi kaitse tervikuna.
- Samuti tulenevad IKS-st konkreetsed nõuded isikuandmete töötlemisele. Näiteks IKS § 25 kehtestab, et isikuandmete töötleja peab kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed, et kaitsta isikuandmete terviklikkust, tagada õiguspärane käideldavus ja konfidentsiaalsus. Üldmääruse artikkel 32 täpsustab IKS § 25 nimetatud kohustusi ning nimetab ühe meetmena turvalisuse tagamiseks ka krüpteerimist (üldmääruse artikkel 32 lg 1 a). Lisaks julgustab üldmääruse vastutavat töötlejat oma kohustuste järgmise tõendamise elemendina kasutama üldmääruse artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist.

---

<sup>115</sup> Sisseehitatud SIM-kaart, ingl. k. *embedded SIM*

- Nimetatud nõuded on eriti olulised ühtse meilisüsteemi pakkuva lahenduse puhul, kus kõigi riigiasutuste e-kirju hakkab potentsiaalselt haldama üks IT-asutus ning seega on õigustatud kõrgendatud tähelepanu sellele, mil viisil ja määral (isiku)andmete töötlemise turvalisus tagatud on.
- Käesolev analüüs on lähemalt uurinud kolme tehnilise lahenduse õiguslikke aspekte ning teinud iga lahenduse all konkreetsed ettepanekud kehtiva regulatsiooni muutmiseks. Erinevate tehniliste lahenduste all välja pakutud regulatsiooni muutmise vajaduse ettepanekud kohati kattusid. Detailsema õigusanalüüsi saab läbi viia tehniliste lahenduste omaduste täpsustamisel. Eelanalüüs tegi muuhulgas järgmised ettepanekud:
  - o Vajadusel võib kasutada AvTS § 43 lg 3-s sisalduvat volitusnormi selliselt, et selle alusel välja antud Vabariigi Valitsuse määrus sätestaks krüpteerimiskohustuse asutusesiseseks tunnistatud teabe elektroonilisel edastamisel. Määruses võib sisalduda ka normatiivne alus täiendavate juhiste andmiseks.
  - o Alternatiivse lahendusena võib täiendavalt analüüsida ka AÜA määruse sisulise uuendamise otstarbekust. Põhimõtteliselt saaks määrust uuendada viisil, et määruse reguleerimisalasse lisanduks riigiasutustevaheline e-kirjavahetus ning määruses kehtestada nii e-kirjavahetussüsteemi kasutamise kohustuslikkus kui ka viited infoturbealastele nõuetele, sh krüpteerimisele.
  - o Kolmanda võimaliku lahendusena võib kaaluda ISKE määruse uuendamist viisil, et sinna lisada riigiasutustele kohustus kasutada valituks osutunud krüpteerimise lahendust ning samasisuline täiendav meede ISKE meetmete hulka lisada.
  - o Olenevalt sellest, kuidas lahendatakse e-kirjavahetussüsteemi haldamine ja koordineerimine, võib osutada vajalikuks ka vastavalt uuendada koordineeriva ja haldava asutuse põhimäärust ning muid seotud normatiivdokumente. Näiteks võib nii käesolevas eelanalüüsis pakutud lahenduste kasutamise kohustuslikkust riigiasutuste infoturbesüsteemi osana kui ka selle haldamisega seotu kehtestada Vabariigi Valitsuse määrusega "Infoturbe juhtimise süsteem".
  - o Teeme ettepaneku sertifitseerimisteenuse osutaja poolt pakutav sertifikaadi kontrollimise võimaluse (hetkel LDAP kataloogi kaudu) kasutusloogikale määratud tingimused uuesti läbi vaadata ning sertifikaadi kontrollimise teenuse pakkumise õiguslikke aluseid ITDS-s täpsustada. Eesmärgiks võiks olla sertifikaatide kehtivuse kontrollimise teenuse parem kättesaadavus. Selleks tuleks täpsustada sertifikaadi kontrollimise teenuse pakkumise õiguslikke aluseid ITDS-s viisil, mis võimaldaks sertifikaadi kontrollimise ka isiku nime alusel. Lisaks võiks sertifitseerimisteenuse osutaja täiendavalt avaldada sertifikaatide kehtivuse kontrollimisel isikuandmete töötlemise põhimõtted. Sellega seoses soovitame küsida ka õiguskantsleri arvamust.
  - o Kui sertifitseerimisteenuse osutaja poolt sertifikaatide kehtivuse kontrollimiseks vajalike isikuandmete töötlemise alused leiduvad seaduses, pole andmesubjektidelt eraldi nõusolekut küsida vaja. Kui siiski on tarvilik andmete töötlemiseks eraldi andmesubjekti nõusoleku küsimine ning isikuandmete töötlemise aluste täiendav selgitamine, võiks seda teha ID-kaardi väljastamisel (hetkel kasutatakse praeguse sertifitseerimisteenuse osutaja poolt koostatud dokumenti "Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasustingimused").
  - o Vastavalt sobivaima tehnilise lahenduse teostusele, soovitame kaasata AKI, kellelt võiks paluda soovituslikke juhiseid konkreetses lahenduses AvTS-i rakendamiseks.
- Iga üksiku ettepaneku juures tuleb kaaluda tasakaalu ülereguleerimise (nt seadusemuudatused, mis toovad endaga kaasa selguse asemel uusi kitsendusi) ning *laissez*

*faire* (nt regulatsiooni üldine puudumine, mis annab küll rohkem tegutsemisvabadust, kuid ei ole läbipaistev ega paku õiguskindlust) lähenemise vahel.

- Enamikel juhtudel (vt erandite kohta analüüsist) ei keela AvTS riigiasutustes töötavate ametnike ja töötajate nimede ja meiliaadressite taaskasutamist eelanalüüsis pakutavate tehniliste lahenduste tarbeks loodavates sertifikaatides ja nende avalikustamisel. Ka riigil endal võiks olla huvi oma asutustes töötavate ametnike ja töötajate käesolevas analüüsis välja pakutud tehniliste lahenduste kontekstis käsitletavate sertifikaatide avalikustamise osas, sest see võimaldaks kodanikul soovi korral riigiesindajatega turvaliselt suhelda.
- eIDAS määrus artikkel 2 lg 2 sätestab, et õigusakti ei kohaldata selliste usaldusteenuste osutamise suhtes, mida kasutatakse eranditult suletud süsteemides, mis tulenevad siseriiklikust õigusest või määratletud osalejate kogumi vahelistest kokkulepetest. Küll aga tuleneb määrusest kohustus avalikule sektorile piiriülevalt tunnustada teiste liikmesriikide omadustelt samaväärseid ning teavitatud elektroonse identiteedi skeeme.

## **Poliitika**

Lisaks eespool mainitud soovitudele ja tähelepanekutele tuleks kindlasti arvestada ka sellega, et suure tõenäosusega ei suuda kõik riigiasutused kõiki nimetatud meetmeid korrektselt implementeerida ja hallata. Seetõttu oleks soovitatav teenuseid konsolideerida.

Lisaks on iga lahenduse korral vajalik asutustevaheliste kokkulepete tegemine.

# Lisa 1 – Intervjuude kokkuvõte

Intervjuud viidi läbi veebruaris 2016. a. kaheksa riigiasutuse IT-turbe esindajatega. Intervjuud olid osaliselt struktureeritud alljärgnevalt loetletud teemade kaupa ning kestsid üldiselt ligikaudu 60 minutit. Järgnevalt on ära toodud ülevaatlilik kokkuvõte intervjuude käigus saadud infost.

## 1. E-kirjavahetuse hulk ja kiirus

- Keskmiselt (meilide hulk nädalas jagatud päevade arvuga) võetakse vastu suurusjärgus 30 000...40 000 kirja, lisaks umbes 10...20 korda rohkem spämmi.
- Ühe meili suuruseks on kuni 20...25 MB, mõnes kohas 10 MB plaanidega tõsta see 25 MB juurde.
- SMTP proovib saata kolmel korral kahe ööpäeva jooksul.
- Meili kohalejõudmist oodatakse 1-2 minuti jooksul. Paaritunnised viivitused kannatab ajuti ära. Elatakse üle ka natuke suuremad viivitused kord kvartalis.
- Ülekaalukalt on kasutusel Microsoft Exchange, lisaks veel GroupWise (plaaniga minna üle MS Exchange'le). Kasutatakse ka Linux-i-põhiseid meiliservereid.
- Väga tähtsal kohal on käideldavus. Mõnes kohas ei kasutata isegi greylisting'ut, et mitte tõkestada kirja kohalejõudmist.
- Ühes kohas lisatakse ka vastavalt kirja päritolule teemale lisainfot: [VÄLJAST] kui kiri on väljastpoolt asutust ning [OLE ETTEVAATLIK] kui meil saadetakse asutuse meiliaadressilt välisvõrgust.
- Üldiselt määravad sõnumi mahu MS Exchange'i vaikimisi sätted. See muutub Exchange 2016. aasta versiooniga 30 MB-ks.
- Meilivoog varieerub vastavalt välistele sündmustele.

## 2. Peamised suhtlussuunad

- Asutus - asutus
- Asutus - kodanik ja asutus - (e-)resident
- Asutuseväline partner (mitteresident)
- Resident - asutus
- Mitteresident (EL-st) - asutus
- Mitteresident (väljastpoolt EL-i) - asutus

Üldiselt olid kõik erinevad suhtlussuunad esindatud.

Suhtlus käib aktiivselt ka mitteresidentidega, seega ID-kaardi omamist ei saa üldjuhul eeldada. Samuti ei saa ID-kaardi kasutamist eeldada residentilt. Signeeritud kujul asjade saatmine võiks olla ka võimalik masin - inimene suunal.

## 3. Krüptograafia kasutamine

- Lõppkasutajalt lõppkasutajale sõnumi krüpteerimine
  - 1) Vajadusel kasutatakse CDOC-i ning ID-kaardiga krüpteerimist. Majast välja saatmisel krüpteeritakse manus ID-kaardiga ning meili sisus ei ole lubatud manust kirjeldada.
  - 2) Kohati oli kasutusel ka PGP-l põhinev meilide sisu krüpteerimine.
  - 3) ACID - Suhtlus EL suunal (saadetakse sõnumeid kuni tasemega EL Piiratud).
  - 4) Väliste osapooltega on kasutusel ka parooliga ZIP konteiner koos AES krüpteerimisega, kusjuures paroole edastatakse kas varem või hiljem ja eelistatult muud kanalit mööda.
- Seansikihi turvamine

- 1) Seansikihi turvamiseks kasutatakse asutuste vahel selleks eraldatud liine ja/või asutustevahelist VPN-ühendust.
  - 2) Meilikliendi ja serveri vahelisel suhtlusel kasutatakse meiliklienti sisseehitatud võimalusi ühenduse turvamiseks (lisaks VPN-ile).
  - 3) Mõned asutused kasutavad meiliserverite vahelisel suhtlusel TLS-i.
  - 4) Mõnedel seadmetel ahelas võib puududa võime TLS-i kasutada.
  - 5) Data Leakage Protection (DLP) süsteemide kasutamine on pigem harv.
4. Isikukoodide ja ID-kaartide kasutamine  
Kaugtöö puhul on ID-kaart enamasti kohustuslik VPN-ühenduse loomisel. On kohti, kus VPN-i ei kasutata. Isikukoodi keegi eraldi ei talleta (v.a. oma töötajate info). Sisevõrgust ID-kaardiga võimalik arvutisse sisse logida, välisvõrgust kohustuslik. Kuna ID-kaarti on tarvis erinevate registritega suhtlemiseks niikuinii tarvis, ei soovi tavakasutajad üldjuhul eraldi asutusesisest kiipkaarti.
  5. Arvutitöökohtade haldamine  
Kõik asutused kasutavad kesksel haldamisel, peamiselt on kesksel halduseks kasutatav Microsoft System Center
  6. Mobiilsete seadmete kasutamine ja haldamine  
Palju mõeldakse mobiilsete seadmete (telefonid ja tahvlid) keskhalduse peale, kuid kellelgi veel seda täielikult implementeeritud polnud. On katsetatud Microsoft Intune ja (VMware) AirWatch lahendusi Nutiseadmest saab meili lugeda MS Active Sync protokolliga abil. Ei toetata SMTP ega IMAP. Kasutusel alati SSL 443 port. Sertifikaadihaldus asutuse poole pealt. Mobiilne ligipääs tehakse lahti küsimise peale. MS Active Sync surub peale poliitika. OWA on väljast loetav, sest iPad ei toeta ei ID-kaarti ega mobiil-ID.
  7. Brauseripõhine meililugemine  
Brauseripõhine meililugemise võimalus on enamikel asutustel olemas, kuid mõned asutused tahaks selle kasutamise turvakaalutlustel asendada ainult meilikliendipõhise lähenemisega. Microsoft Outlook Web App (MS OWA) on mobiiliga kättesaadav. Mõned asutused mainisid eraldi ära, et ootavad RIA lubatud liidestust, mis võimaldaks MS OWA süsteemi sisse logimisel kasutada mobiil-ID või ID-kaarti. Seejärel oleks võimalik muuta kohustuslikuks mainitud lahenduse (liidestuse) kasutamine brauseripõhiseks meililugemiseks.  
On asutusi, kus lubatakse veebimeili lugeda välisvõrgust ilma VPN-ühenduseta.
  8. Kasutusel olevad suhtlustarkvarad  
Skype, Skype for Business, Lync, JIRA, vähemal määral ka muud tooted, nt Fleep. Kasutatakse ka MS SharePoint baasil siseveebi teadete edastamiseks. Veel ka Polycom-seadmed videokõnedeks ning VoIP telefonid. Tundlikuma info edastamiseks krüptotelefon Tetra või Facetime. Väga tundlik info läbi telefoni ei lähe.
  9. Asutuste poolt tõstatatud probleemid ja vajadused
    - Kasutatavus  
Lõppkasutajale peaks olema lahendus võimalikult nähtamatu/lihtne. Kõik leidsid, et PGP oleks tavakasutajale liiga keeruline. Äripoolele on keeruline maha müüa turvalahendust, kui kasutaja ise peab sekkuma. Krüptograafia kasutamine võiks olla võimalik ühest kohast. Praegu on üsna ebamugav, et fail tuleb ühe rakenduse abil krüpteerida, teise abil allkirjastada ja kolmanda rakenduse abil adressaadile saata.

- Terviklus  
Mitmed intervjuueeritavad töid eraldi välja vajaduse veenduda sõnumite tervikluses.
- Konfidentsiaalsus  
Kodanikule konfidentsiaalse info saatmine on keeruline, kuid vajalik (nt parkimistrahvid, meditsiiniline info, jne).  
Konfidentsiaalse info edastamine isikule, kellel ei ole ID-kaarti, on keeruline.
- Lõppseadmete varundus on valus teema – lõppseadmes hoitava võtme haldus võiks olla teistmoodi lahendatud kui tuima lõppseadmete varundamisega.
- Sertifikaatide ajamine iOS seadmetesse on problemaatiline.

#### 10. Failivahetus-süsteemid

Dokumendihaldussüsteem ei ole Internetist kättesaadav.

MS Sharepoint'i baasil pikaajalised kasutajad.

Mitmes asutuses on kasutusel DVK.

Mitmes asutuses on kasutusel DHS.

Välisveebi failiserver, kuhu saab linkida (kasutatakse harva, umbes 10 korda aastas).

#### 11. Regulatsioonid

Üldiselt on kasutusel asutusepõhine infoturbe poliitika, mida enamik teab ja austab.

Spetsiifilisemaid asju teavad umbes 50% töötajatest.

Infoturbe teema on käsitletud ka uue töötaja koolitusel.

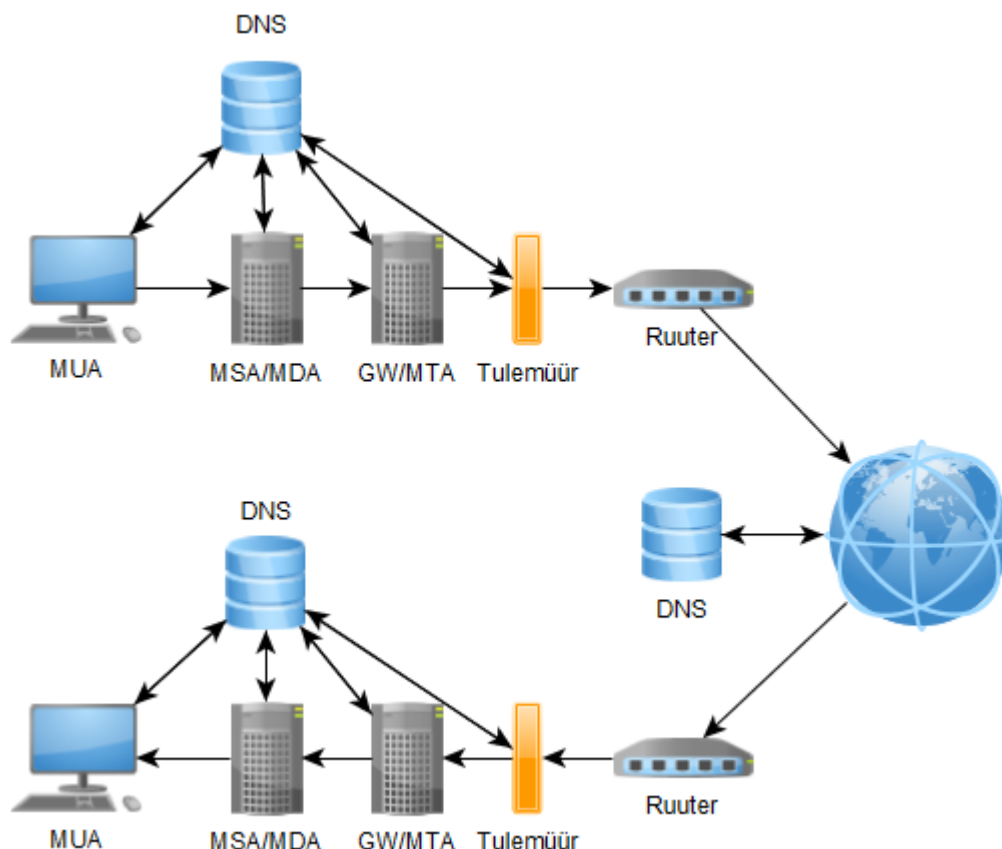
Lisaks on asjaajamiskord, mis reguleerib seda, kuidas käidelda erineva märgistusega infot.

Avalik info võib olla ka välismaal, aga suurem kui S0 tase peab olema Eesti territooriumil.

Ei soosi Google Docs'i kasutamist ning mõned juhivad ka tähelepanu sellele, kui keegi teine seda teeb.

## 12. Referentsarhitektuur

Tavapärase arhitektuuri üldjoontes selline:



Pilt 3 - referentsarhitektuur

„Pilt 3 - referentsarhitektuur“ kujutab intervjuude käigus kogutud info põhjal loodud üldist arhitektuurimudelit, kus lühendid märgivad järgmist:

- MUA – *Mail user agent* ehk meiliklient
- MSA – *Mail submission agent*
- MDA – *Mail delivery agent* ehk *Message delivery agent*
- MTA – *Message transfer agent*

Tüüpiline MUA on MS Outlook 2010-2013.

Tüüpiline MSA/MDA on MS Exchange 2007-2013.

Levinumad GW/MTA süsteemid on IronPort (Cisco Security) ja Postfix.

## 13. Lisaks välja toodud teemad

- Ühes asutuses kasutatakse DVK süsteemi 80% ulatuses riiklike dokumentide vahetuseks .
- Võib juhtuda, et tavameilile saadetakse ka piiratud turbetasemega infot.
- DLP on võimalik viia lõppseadmetesse.

## Lisa 2 – Vastused hankes esitatud küsimustele

- 1) Milliseid turvalahendusi riigiasutustes ja riigiasutuste vahel e-kirjade käitlemisel (hõlmaks nii saatmist kui hoidmist) kasutatakse?
  - Serveritevaheline TLS, piiratud hulgal
  - DigiDoc Krüpto
  - PGP, piiratud kujul
  - ACID<sup>116</sup>, väga vähesel määral
  - Parooliga ZIP-konteiner
- 2) Kas ja kuidas postkaste endid krüpteeritakse nii, et vastava loata administraatorid vm asutusesisesed isikud neid lugeda ei saa?
  - Tavaliselt postkaste ei krüpteerita.
  - Meilide lugemine on piiratud selgelt õiguste struktuuriga ning ei ole ühelgi juhul elementaarne.
- 3) Milliseid erinevaid tehnilisi lahendusi (näiteks DigiDoc3 krüpto, PGP, TLS) on võimalik turvalise, sh krüpteeritud e kirjavahetuse käitlemiseks (saatmine, salvestamine jm) kasutada (sh rahvusvaheline parim praktika)?

Alustehnoloogiatena on võimalik kasutada järgnevat lahendusi:

- Otspunktide vahelise konfidentsiaalsuse tagamiseks sõnumi sees – Digidoc3Krüpto
- Parooliga ZIP-konteiner vms krüpteerimist toetav pakkevahend, ACID<sup>117</sup>
- Otspunktide vahelise konfidentsiaalsuse ja tervikluse tagamiseks – DigiDoc koos DigiDoc Krüpto
- OpenPGP, S/MIME – seda siis X.509 või PGP tüüpi sertifikaati kasutades
- Sererite vahelise konfidentsiaalsuse tagamisel, ühtne asukoht, VPN, IPSEC, TLS

Lisaks on peatükis „4. Rahvusvahelised parimad praktikad ja lahendused“ ära kirjeldatud rahvusvahelised parimad praktikad.

- 4) Millised on erinevate tehniliste lahenduste plussid ja miinused, sh:
  - Hinnang lahenduste turvalisuse tugevusele – kasutatava krüptograafia tugevus (vajadusel krüptograafia muutmise võimalus, kui seni kasutatu muutub ebaturvaliseks), protsessiloogika tugevus, võimalikud haavatavused jne; need on kirjeldatud vastavate lahendusideede kirjelduses ja/või võrdlustabelis
  - Ühildatavus olemasolevate süsteemidega (riigiasutuste tehniline valmidus) – lahenduse hilisem haldamine; see on kirjeldatud vastavate lahendusideede kirjelduses ja/või võrdlustabelis
  - Kasutusmugavus lõppkasutaja vaatenurgast (võrreldes tavalise e-postiteenuse kasutamisega),

---

<sup>116</sup> <http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/eu-restricted/offline-file-encryptor/acid-cryptofiler-v7/>

<sup>117</sup> *ibid.*

sh automatiseeritus; kirjeldatud vastavate lahendusideede kirjelduses ja/või võrdlustabelis.

- 5) Milline on riigiasutuste organisatoorne valmidus lahendust kasutusele võtta?  
Olenevalt lahendusest on valmidus erinev. Suuremad muudatused põhjustavad tõenäoliselt ka suuremat vastuseisu.
- 6) Õiguslikust regulatsioonist (seadused, määrused vm) tulenevad nõuded ja õigusliku regulatsiooni võimalik muutmisevajadus selleks, et tehnilist lahendust välja töötada, juurutada ja kasutada.  
Õiguslikust regulatsioonist tulenevad nõuded ning ettepanekud kehtiva regulatsiooni muutmiseks on välja toodud iga tehnilise lahenduse all.
- 7) Lahenduse projektiplaan, st. välja töötamise, kasutuselevõtmise ja juurutamise ajakava ning täpsem ressursivajadus (sh aeg, inimesed, teadmised, oskused, maksumus).  
Projektiplaan on HTML-failina lisatud.
- 8) Hilisema haldamise organisatoorne kirjeldus (sh kes tegeleb süsteemi haldamisega? Kas toimub tsentraliseeritult või iga asutus ise? Kuidas toimub haldamise koordineerimine?).  
Kirjeldatud vastavate lahendusideede kirjeldustes ja/või võrdlustabelis.
- 9) Lahenduse haldamise kulud ja muu ressursivajadus (sh inimesed, oskused, teadmised).  
Kirjeldatud vastavate lahendusideede kirjeldustes ja/või võrdlustabelis.

## Lisa 3 – TLS, SPF, DNSSEC analüüsi tabelid

Kõigepealt tabel DNSSEC rakendamisest erinevatel skoobis määratud domeenidel.

Domeenid	DNSSEC /DNSKEY	MX-kirjed			
112.ee		mg2.smit.ee.	mg1.smit.ee.		
agri.ee		ns.agri.ee.	mail.agri.ee.		
aso.ee		mail.ria.ee.	smtp.aso.ee.		
aki.ee		mail2.just.ee.	mail1.just.ee.		
ecaa.ee		mail.mkm.ee.	smtp.aso.ee.		
eesti.ee	OK	smtp.aso.ee.			
emta.ee	OK	post.emta.ee.	mailgw.emta.ee.		
envir.ee		envir.envir.ee.			
epa.ee		mail2.just.ee.	mail1.just.ee.		
harju.maavalitsus.ee		mail.maavalitsus.ee.			
hiiu.maavalitsus.ee		mail.maavalitsus.ee.			
hm.ee		mail1.hm.ee.	mx.hm.ee.	mail2.hm.ee.	mail.hm.ee.
ida-viru.maavalitsus.ee		mail.maavalitsus.ee.			
jarva.maavalitsus.ee		mail.maavalitsus.ee.			
jogeva.maavalitsus.ee		mail.maavalitsus.ee.			
just.ee		mail1.just.ee.	mail2.just.ee.		
kaitseministeerium.ee		kaitseministeerium.ee.			
kapo.ee		gw2.gov.ee.	gw1.gov.ee.		
keeleinsp.ee		mx1.mlplus.com.	mx2.mlplus.com.		
kemit.ee		envir.envir.ee.			
keskkonnaamet.ee		envir.envir.ee.			
keskkonnaagentuur.ee		envir.envir.ee.			
kki.ee		mx1.envir.ee.			
konkurentsiamet.ee		mail2.just.ee.	mail1.just.ee.		
kra.ee		mailhost.mil.ee.	mail.kra.ee.		

<b>Domeenid</b>	<b>DNSSEC /DNSKEY</b>	<b>MX-kirjed</b>			
kul.ee		224.247.159.217.sta.estpak.ee.	mail.kul.ee.		
laane.maavalitsus.ee		mail.maavalitsus.ee.			
l-virumv.ee		-			
maaamet.ee		marja.maaamet.ee.			
mil.ee		miisu.mil.ee.	mailhost.mil.ee.		
mkm.ee		mail.mkm.ee.	smtp.aso.ee.		
mnt.ee		mail.mkm.ee.			
muinas.ee		mail2.just.ee.	mail1.just.ee.		
mv.werro.ee		mail.maavalitsus.ee.			
parnu.maavalitsus.ee		mail.maavalitsus.ee.			
pma.agri.ee		ns.agri.ee.	mail.agri.ee.		
politsei.ee		mg2.smit.ee.	mg1.smit.ee.		
polva.maavalitsus.ee		mail.maavalitsus.ee.			
pria.ee		ns.pria.ee.	smtp.aso.ee.		
prokuratuur.ee		mail2.just.ee.	mail1.just.ee.		
ra.ee		mx1.ra.ee.	mx2.ra.ee.		
rahandusministeerium.ee	OK	mailgw.emta.ee.	post.emta.ee.		
rapla.maavalitsus.ee		mail.maavalitsus.ee.			
ravimiamet.ee		mail.ravimiamet.ee.			
rescue.ee		mg2.smit.ee.	mg1.smit.ee.		
ria.ee	OK	mail.ria.ee.	smtp.aso.ee.		
riigikantselei.ee	OK	callisto.rk.ee.	niobe.rk.ee.		
rik.ee		mail2.just.ee.	mail1.just.ee.		
rmit.ee	OK	mailgw.emta.ee.	post.emta.ee.		
saare.ee		-			
siseministeerium.ee		mg1.smit.ee.	mg2.smit.ee.		
sm.ee		valvur.sm.ee.			

<b>Domeenid</b>	<b>DNSSEC /DNSKEY</b>	<b>MX-kirjed</b>			
smit.ee		mg1.smit.ee.	mg2.smit.ee.		
sotsiaalkindlustusamet.ee		post.sotsiaalkindlustusamet.ee.			
stat.ee	OK	mailgw.emta.ee.	post.emta.ee.		
tarbijakaitseamet.ee		mail.mkm.ee.			
tartu.maavalitsus.ee		mail.maavalitsus.ee.			
teabemet.ee		lutikas.teabemet.ee.			
ti.ee		valvur.sm.ee.			
tja.ee		mail.mkm.ee.	smtp.aso.ee.		
valga.maavalitsus.ee		mail.maavalitsus.ee.			
vet.agri.ee		gw.agri.ee.	mail.agri.ee.		
viljandi.maavalitsus.ee		mail.maavalitsus.ee.			
vm.ee		saturn.eu.estemb.be.	jupiter.vm.ee.		
vta.ee		mail.mkm.ee.			

Järgmises tabelis on kujutatud TLS kasutamine ja tugi erinevates GW/MTA seadmetes. Tabel saadi järgnevalt:

- 1) MX kirje sisaldab meiliserveri nime. Sellele vastav IP on DNS päringuga saadud esimene vaste.
- 2) Seejärel teostati Nmap skaneerimine, mis uuris port 25 valmisolekut meilide vastuvõtuks.
- 3) Küsiti serverilt (Nmap abil), kas ta pakub mõnda sertifikaati krüpteeritud ühenduse algatamiseks.
- 4) Kolmanda osapoole kinnitus – kontrolliti spetsiaalse skriptiga, kas TLS-i rakendamine vastab rahvusvahelistele parimatele praktikatele.

MX kirjele vastav server	IP	port	staatus	teenus	Nmap hinnangul kasutusel olev tarkvara	SSL-cert	Kolmanda osapoole kinnitus
224.247.159.217.sta.estpak.ee	217.159.247.224	25	open	smtp	netqmail smtpd	ssl-cert	
callisto.rk.ee	213.184.48.172	25	open	smtp	Postfix smtpd	ssl-cert	OK
envir.envir.ee	213.184.40.34	25	open	smtp	netqmail smtpd		
fmail.kaitseliit.ee	195.80.119.131	25	open	smtp		ssl-cert	OK
gw1.gov.ee	195.80.107.9	25	open	smtp	IronPort smtpd	ssl-cert	
gw2.gov.ee	195.80.112.88	25	open	smtp	IronPort smtpd	ssl-cert	
gw.agri.ee	213.184.49.190	25	open	smtp	IronPort smtpd		
jupiter.vm.ee	213.184.49.23	25	open	smtp	Cisco PIX sanitized smtpd		
kaitseministeerium.ee	195.80.124.199	25	open	smtp	Postfix smtpd		
lutikas.teabeamet.ee	213.184.38.57	25	open	smtp	Symantec Enterprise Security manager smtpd	ssl-cert	OK
mail1.hm.ee	193.40.57.6	25	filtered	smtp			
mail1.just.ee	213.184.53.9	25	open	smtp			
mail2.hm.ee	193.40.57.6	25	filtered	smtp			
mail2.just.ee	195.80.112.143	25	open	smtp			
mail.agri.ee	213.184.49.202	25	open	smtp	IronPort smtpd		
mailgw.emta.ee	213.184.49.71	25	open	smtp	Postfix smtpd	ssl-	OK

MX kirjele vastav server	IP	port	staat	teenus	Nmap hinnangul kasutusel olev tarkvara	SSL-cert	Kolmanda osapoole kinnitus
						cert	
mail.gov.ee	195.80.106.244	25	open	smtp		ssl-cert	OK
mail.hm.ee	193.40.57.2	25	open	smtp	Microsoft Exchange smtpd	ssl-cert	OK
mailhost.mil.ee	195.222.6.11	25	open	smtp	Postfix smtpd	ssl-cert	
mail.kul.ee	195.80.111.18	25	open	smtp	netqmail smtpd	ssl-cert	
mail.kra.ee	213.184.51.117	25	open	smtp		ssl-cert	OK
mail.maavalitsus.ee	195.80.100.210	25	open	smtp		ssl-cert	
mail.mkm.ee	195.80.102.58	25	open	smtp		ssl-cert	
mail.raviamet.ee	193.40.10.163	25	open	smtp	Microsoft ESMTMP		
mail.ria.ee	195.80.102.34	25	open	smtp	Postfix smtpd	ssl-cert	OK
marja.maaamet.ee	213.184.51.69	25	open	smtp	IronPort smtpd		
mg1.smit.ee	195.80.105.106	25	open	smtp	IronPort smtpd	ssl-cert	
mg2.smit.ee	195.80.105.110	25	open	smtp	IronPort smtpd	ssl-cert	
miisu.mil.ee	188.0.48.32	25	filtered	smtp			
mx1.envir.ee	213.184.40.185	25	open	smtp		ssl-cert	
mx1.mlxplus.com	90.190.150.153	25	open	smtp	Microsoft Exchange smtpd	ssl-cert	OK
mx1.ra.ee	195.80.106.157	25	open	smtp	IronPort smtpd		
mx2.mlxplus.com	90.190.150.154	25	open	smtp	Microsoft Exchange smtpd	ssl-cert	OK
mx2.ra.ee	195.80.106.110	25	open	smtp	IronPort smtpd		
mx.hm.ee	193.40.57.2	25	open	smtp	Microsoft Exchange smtpd	ssl-cert	
niobe.rk.ee	213.184.51.139	25	open	smtp	Postfix smtpd	ssl-cert	OK

<b>MX kirjele vastav server</b>	<b>IP</b>	<b>port</b>	<b>staatus</b>	<b>teenus</b>	<b>Nmap hinnangul kasutusel olev tarkvara</b>	<b>SSL-cert</b>	<b>Kolmanda osapoole kinnitus</b>
gw.agri.ee	213.184.49.190	25	open	smtp	IronPort smtpd		
ns.pria.ee	213.184.42.243	25	filtered	smtp			
post.emta.ee	195.80.123.36	25	open	smtp	Postfix smtpd	ssl-cert	OK
post.sotsiaalkindlustusamet.ee	213.184.49.162	25	open	smtp	IronPort smtpd		
saturn.eu.estemb.be	94.107.251.195	25	open	smtp	Cisco PIX sanitized smtpd		
smtp.aso.ee	213.184.32.85	25	open	smtp	Postfix smtpd	ssl-cert	OK
valvur.sm.ee	213.184.49.162	25	open	smtp	IronPort smtpd		

## Lisa 4 – Lahenduste võrdlustabel

Lahendused on nummerdatud järgnevalt:

L.1 (IRM)	Keskne IRM lahendus
L.2 (S/MIME)	S/MIME kasutamine DNSSEC-i ja ID-kaardiga
L.34 (DDweb)	DigiDoc Krüpto pistikprogramm (plugin) ja veebilahendus.

Kasutatavuse võrdluseks võtsime käesoleva dokumendi peatükis „4. Rahvusvahelised parimad praktikad ja lahendused“ väljatoodud omaduste alamhulga.

(K.1) Käivituskulud – teenuse ülespanek ja alustamine peaks olema kasutajale lihtne.

(K.2) Lihtsad usaldusküsimused – tavakasutaja käest tohib küsida vähe ning kergesti langetatavate otsuste kohta.

(K.3) Nähtamatu PKI (avaliku võtme taristu) – tavakasutaja saab süsteemi usaldusotsuste tegemiseks kasutada ka ilma PKI kontseptsioonidest aru saamata.

(K.4) On kasutaja jaoks mugav vastavalt intervjuudes välja toodud nõuetele.

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
K.1 (käivitus)	Lihtne	Ametnikule lihtne, muidu keskmise keerukusega	Lihtne
K.2 (usaldus-küsimused)	Kasutaja peab aktiivselt valima	On võimalik arendada ja disainida lihtsaks	
K.3 (Nähtamatu PKI)	Jah	Mööndustega	Mööndustega
K.4	Mööndustega, sõltub kliendi häälestusest	On võimalik arendada ja disainida lihtsaks	On võimalik arendada ja disainida lihtsaks
Koolitus-vajadus	Jah	Jah	Jah
Andmed serveris krüpteerituna	Ei	Jah	Jah
Meta-andmete avaldamine	Jah	Jah	Jah

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Grupitöö (kalendri tugi)	Jah	Jah	Jah
Meililistide tugi krüpteerituna	Serveri piires jah	Ei	Ei
Litsentsiga seotud kulu	Serverite ja klientide litsentsid.  Riigi litsentseerimise mudel tuleb üle vaadata.  Hinnanguliselt 3 miljonit eurot aastas.  Kokkuhoid võib tulla hetkel kehtivate lepingute lõpetamisest.	Lisakulusid ei ole, kui vahe-lahendustena kasutada vabavaralisi lahendusi	Ei ole

## Hinnang lahenduse turvalisusele

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Kasutatud krüptograafia tugevus	-	Sõltub ID-kaardi krüptost ja meiliklientide krüptograafia toest	
Krüptograafiliste algoritmide muutmise võimalus	Sõltub operatsioonisüsteemist ja meiliserveri tarkvarast	Sõltub meilikliendist	On võimalik arendada, disainida lihtsalt vahetatavaks
Probleemid		Saatja võib kasutada nõrgemat krüptot  Puudub n-ö „soft fail“	

## Turvalise sõnumi saatmise suunad

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Ametnik-Ametnik	Jah	Jah	Jah
Ametnik-Alltöövõtja	Mööndustega	Jah	Jah
Ametnik-Resident	Ei	@eesti.ee jah;  @domain.ee sõltub kasutajast või selle domeeni administraatorist	Jah
Ametnik-EL Ametnik	Ei	Mööndustega	Mööndustega
Ametnik-krüptograafiat mitte kasutav kodanik	Ei	Mööndustega	Mööndustega

## Haldamine

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Kliendi tarkvara haldus	Asutuse IT	Asutuse IT	Asutuse IT
Sertifikaadi haldus	-	SK + Asutuse IT	SK
Serverite haldus	Keskne haldus; mõni IT ühendasutus	DNS-Asutuse IT Meiliserver Asutuse IT LDAP>DNS GW Keskne haldus	SK
Arendus vajadus	Puudub	Jah  ID-kaardi draiver.  Sertifikaatide salvestamine DNS puusse DNSSEC kujul automatiseerimine.  Nupp "tava"-kasutaja jaoks.  Krüpto parema visualiseerimise plugin.  LDAP > DNS keskserver	Jah  Plugin erinevates meili-klientides
Implementeerimise hinnanguline ajamaht	Sõltub.  Tehniline ma 4 kuud	Sõltub  ID-kaardi tarkvara driver – 4 kuud  Skriptid – 2 kuud  LDAP DNS Gateway – 2 kuud  Sertifikaatide salvestamine DNS puusse DNSSEC kujul  Krypto parema visualiseerimise plugin 4 kuud  Rollout – 1 kuu kuni 1 aasta	14 kuud
Hinnanguline juurutusmaksumus koos koolitusega	Ca 4,4 Miljonit eurot	Ca 580 tuhat eurot	Ca 560 tuhat eurot

## Operatsioonisüsteemid / populaarsete meiliklientide tugi

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Windows			
Outlook	Jah	Jah	Plugin
Thunderbird	Ei	Jah	Plugin
Outlook Web Application	Jah	Mööndustega	Mööndustega –alla laadida ja Digidoc Krüpto tarkvaras lahti võtta.
Linux			
Thunderbird	Ei	Jah	plugin
Outlook Web Application	Jah	Jah	Mööndustega –alla laadida ja Digidoc Krüpto tarkvaras lahti võtta
Mac OSX			
Outklook	Jah	Jah	plugin
OSX Mail	Ei	Jah	Ei
Outlook Web Application	Jah	Jah	Mööndustega –alla laadida ja DigiDoc Krüpto tarkvaras lahti võtta
IOS			Kui arendada IOS rakendus
Message & Mail	Jah	Mööndustega (võib vajada eraldi sertifikaati seadmele)	Ei
Outlook	Jah	Mööndustega (võib vajada eraldi sertifikaati seadmele)	Ei
Android			
Mail	Jah	Mööndustega (võib vajada eraldi sertifikaati seadmele) või NFC-ga DigilID-d	Ei
Gmail	Ei	Ei	Ei

	L.1 (IRM)	L.2 (S/MIME)	L.3 (DDweb)
Windows Phone	Jah		Juhul kui arendada rakendus
Outlook	Jah	Mööndustega (võib vajada eraldi sertifikaati seadmele) või NFC-ga DigilID-d	Ei