Digitaalset allkirja kasutavate tööealiste (15-64-aastased) Euroopa liidu elanike osakaalu määramine 2015.aastal

Uuringu aruanne

Detsember 2015

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

Euroopa Liit
Euroopa Regionaalarengu Fond

Eesti tuleviku heaks

Building a better working world

Sisukord

1. Kokkuvõte

Digitaalne allkirjastamine on Eestis muutumas üha valdavamaks ametlikku asjaajamist ja äritegevust toetavaks tehniliseks võimaluseks. Selle kasutajad saavad turvaliselt sõlmida kokkuleppeid teiste osapooltega ja kinnitada oma tahteavaldusi ilma tülikate paberimajandusega kaasnevate logistiliste probleemideta. Kui Eestis on digitaalne allkirjastamine muutumas juba üldlevinud lahenduseks, siis paljudes teistes riikides see nii ei ole või toimub see teistsuguste tehniliste ja organisatsiooniliste lahendustega.

Käesoleva teema käsitlemisel on oluline teha vahet erinevat tüüpi digitaalse allkirjastamise meetodite vahel. Tänapäeval on kasutusele võetud kvalifitseeritud e-allkirja mõiste, mis on oma tehnoloogilise ja organisatsioonilise ülesehituse poolest võrreldav notariaalse kinnitusega, kuna selle abil saab suure tõestusväärtusega kindlaks teha allkirja andnud isiku. Kõigi kvalifitseeritud e-allkirjast madalamate nõuetega e-allkirjade korral on see kindlus oluliselt madalam ja sellised allkirjad sarnanevad pigem paberil antud allkirjaga, mille andmise sündmust on allkirjastajal hiljem võimalik vaidlustada ja eitada.

Käesolevas aruandes on kasutatud digitaalse allkirjastamise mõistet laiemas tähenduses ja juhul kui on tahetud täpsustada, siis on kasutatud kas täiustatud e-allkirja või kvalifitseeritud e-allkirja mõistet. Eestis kasutusel olev digitaalallkiri vastab kõigile kvalifitseeritud e-allkirja nõuetele, teiste riikide puhul seda aga eeldada ei saa.

Käesoleva uuringu eesmärgiks oli hinnata digitaalset allkirja kasutavate tööealiste elanike osakaalu EL riikides. Uuringus keskenduti kvalifitseeritud e-allkirjale ja kvalifitseeritud sertifikaadiga täiustatud e-allkirja kasutusele, kuid vaadeldi ka muid kvalifitseeritud allkirja andmise tehnilisi nõudeid nagu kvalifitseeritud allkirja andmise vahendi nõuetele vastavus, ajatempli kasutamine ning kehtivuskinnitusega seotud küsimused.

Uuring hõlmas kokku 28 EL liikmesriiki ja kaasas täiendavalt Norra, Šveitsi ja Islandi. Lähtuvalt projekt lähteülesandes etteantud metoodikast toimus uuringu algandmete kogumine EL usaldusteenuse osutajate nimekirjades olevatelt teenusepakkujatelt. Kuna usaldusteenuste pakkujad ei oma otseselt andmeid antud e-allkirjade ega allkirjastajate kohta, siis koguti andmeid kehtivate väljastatud digitaalse allkirjastamise sertifikaatide ja nende kasutusalade kohta, mille põhjal anti võimalusel hinnanguid digitaalse allkirjastamise kasutajate arvu kohta.

Nagu eelpool mainitud, on paljudes riikides kvalifitseeritud e-allkirjast enam levinud mitte-kvalifitseeritud e-allkirja kasutamine. Sageli on sellised lahendused olnud kasutuses juba pikaajaliselt, nende kasutamine on muutunud harjumuspäraseks ja seetõttu tähendaks uutele lahendustele üleminek suurt muudatust ühiskonnas laiemalt.

Kuigi töö eesmärgiks oli saada hinnang digitaalsete allkirjastajate arvu ja osakaalu kohta, siis tegelikkuses ei osutunud piisava usaldusväärsusega kvantitatiivsete andmete saamine paljude riikide puhul võimalikuks ja konkreetne allkirjastajate osakaal õnnestus hinnanguna esitada 14 riigi osas.

Töö tulemusena võib öelda, et vaatlusgrupis oli 4 riiki, kus kvalifitseeritud sertifikaadiga digitaalset allkirjastamist on praktiseerinud vähemalt 10% tööealisest elanikkonnast. Ülejäänud riikides anti kvalifitseeritud e-allkirja vähem või ei õnnestunud riigi kohta informatsiooni koguda. Sellest ei saa järeldada, et neis riikides pole digitaalne allkirjastamine üldsegi levinud. Suure tõenäosusega on mitmes riigis levinud väiksematele turvanõuetele vastav digitaalne allkirjastamine, mis jäi käesolev uuringu ulatusest välja.

Üheks käesoleva uuringu tulemuseks võib pidada parema arusaama tekkimist digitaalse allkirjastamise mõõtmise ja rakendamisega seotud laiemate probleemide osas, millest olulisemad on digitaalse allkirjastamise alaste mõistete ja põhimõtete erinev tõlgendus nii riigiti kui erialaringkondades ning sellest tulenev erinev lähenemine mitmetele digitaalse allkirjastamise nõuetele. Sellisteks näideteks on ajatempli kasutamise nõude rangus, kehtivuskinnituse võtmise olulisus ja ajastus digitaalsel allkirjastamisel jt. Uuringu käigus tekkis veendumus, et digitaalse allkirjastamise leviku edendamiseks on vajalik selle erinevuste ja eeliste väljatoomine võrreldes tava-

allkirjaga. Paljude riikide praeguses õigusruumides samastatakse digitaalallkiri omakäelise allkirjaga, kuid tegelikult on kvalifitseeritud e-allkirja näol tegemist omakäelisest allkirjast oluliselt tugevama seosega allkirja andja ja allkirjastatavate andmete vahel.

Uuringu tulemusena tehti mitmeid soovitusi nii edaspidiste sarnaste uuringute läbiviimise kui digitaalse allkirjastamise edendamise osas EL riikides, millest olulisematena võib välja tuua järgmised:

- Kriitilise tähtsusega on e-allkirjastamisega seotud mõistete ja selle kasutamise arusaamade ühtlustamine – digitaalse allkirja kasutamise edendamiseks on oluline teadvustada laiemale üldsusele digitaalse allkirjastamise olemust ja selle eeliseid tavaallkirja ees. Tuleb rõhutada, et kvalifitseeritud allkiri on tavaallkirjaga samase õigusjõuga, annab sellele lisaks oluliselt tugevama kindluse isiku ja dokumendi seose vahel ning kehtib ka riigipiiride üleselt;
- Uuringu läbiviimine peaks edaspidi toimuma liikmesriigis kohapeal, sest tulenevalt riikide erinevast digitaalse allkirjastamise praktikatest ja tavadest on riigis kohapeal (näiteks regulaatoril või järelevalveorganil) parem arusaam riigis valitsevast olukorrast, samuti on riigisisene suhtlus oluliselt tulemuslikum;
- Tuleks luua lahendused usaldusteenuste osutajate poolse digitaalse allkirjastamisega seotud sarnaste statistiliste andmete esitamiseks kas riigi või EL tasemel, mis võimaldab saada parema ülevaate turust, aga anda ka individuaalset statistilist tagasisidet teenuseosutajatele nende andmete osas võrreldes turuga. See aitaks kaasa andmete riigiti võrreldavuse parendamisele;
- Allkirjastajate arvu hindamisel tuleks eristada kvalifitseeritud ja muid allkirju ning kaaluda ka muude digitaalse allkirjastamisega seotud statistiliste andmete kogumist, nagu näiteks välja antud kehtivate sertifikaatidega e-ID kaartide arv.

Laiema digitaalse allkirjastamise edendamise soovi korral tuleks luua terviklik tehniliste ja organisatoorsete lahenduste komplekt ehk „kvalifitseeritud e-allkirjastamist võimaldav keskkond“, mis vastab kõigile e-allkirjastamise tehnilistes spetsifikatsioonides defineeritud nõuetele. See peaks lisaks kvalifitseeritud sertifikaadile hõlmama ka e-allkirja andmise turvalist vahendit, selle kasutamiseks vajalikke riist- ja tarkvaralisi vahendeid, kvalifitseeritud usaldusteenuste kasutamist (sh ajatempli teenus, kehtivuskinnituse teenus) ning kokkuvõttes ka e-allkirjade käsitlemise vahendit, mis käitleb (st loob ja valideerib) standardses formaadis e-allkirju.

2. Sissejuhatus

2.1 Uuringu taust

Ernst & Young Baltic AS viis koostöös Tarvi Martensiga Majandus- ja Kommunikatsiooniministeeriumi tellimusel läbi uuringu „Digitaalselt allkirja kasutatavate tööealiste (15-64-aastased) Euroopa elanike osakaal 2015. aastal".

Infoühiskonna arengukava eesmärgiks on majanduse kasvu, riigi arengut ja elanike heaolu toetava IKT-taristu ning avaliku ja erasektori ühtse teenusruumi arendamine. Üheks tegevuste edukuse mõõdikuks on digitaalse allkirja kasutamine Euroopa Liidu tööealise elanikkonna poolt. Digitaalse allkirja kasutamine soodustab teenuste piiriülest osutamist, säästab ressursse ning lihtsustab ja kiirendab asjaajamist.

Uuringu eesmärk oli kaardistada digitaalse allkirjastamise hetkeolukord EL liikmesriikides, Norras, Šveitsis ja Islandil ning leida digitaalset allkirja kasutavate tööealiste EL elanike hinnanguline osakaal. Uuringu tulemusi on plaanis kasutada avaliku ja erasektori ühtse piiriülese teenusteruumi arendamisel ning digitaalse allkirja kasutamise edendamise tegevusplaani koostamisel.

Tulenevalt hanke tööde kirjeldusest lähtus uuringu metoodika EL määruses nr 910/2014[1] (edaspidi eIDAS määrus) esitatud täiustatud e-allkirja definitsioonist, mille kohaselt:

- digitaalne allkiri peab olema seotud ainuüksi allkirja andjaga;
- selle abil on võimalik tuvastada allkirja andjat;
- see antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja;
- see on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatavad.

Hanke tingimuste järgi tuli uuringus käsitleda digitaalse allkirjana selliseid e-allkirju, mis on antud kvalifitseeritud sertifikaadil kvalifitseeritud usaldusteenuse osutaja poolt ning on seaduse järgi võrdsed käsitsi antud allkirjaga.

2.2 Aruandes kasutatavad mõisted ja lühendid

Lühend/Termin	Seletus
ATO	Ajatempliteenuse osutaja
CRL	Sertifikaatide tühistusnimekiri Inglise keeles: Certification Revocation List
Digitaalallkiri (või digiallkiri)	Digitaalallkiri on tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mida allkirja andja kasutab, märkimaks oma seost dokumendiga. (Digitaalallkirja seadus)
eIDAS määrus	Euroopa Parlamendi ja Nõukogu määrus (EL) nr 910/2014 (vastu võetud 23. juuli 2014) e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul
Elektrooniline allkiri (või e-allkiri)	Käsitsi kirjutatud allkirja elektrooniline ekvivalent (Andmekaitse ja infoturbe leksikon; © Cybernetica AS, 2011 - 2015)
HSM	Riistvaraline turvamoodul

[1] **EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014,23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ**

	Inglise keeles: Hardware Security Module
KKTO	Kehtivuskinnituse teenuse osutaja
Kvalifitseeritud e-allkiri	Kvalifitseeritud e-allkiri on Täiustatud e-allkiri (AdES); - mis baseerub kvalifitseeritud sertifikaadil (QC), mis on väljastatud füüsilisele isikule; - mis on teostatud kasutades turvalise allkirja loomise seadet (SSCD). Inglise keeles: Qualified Electronic Signature, lühend „QES", vastavalt eIDAS määruse definitsioonile
Liiderkeskkond	Keskkond, mida kasutavad kõik / enamik digiallkirjastamist kasutavad kodanikud riigis
OCSP	Sertifikaatide kehtivuskinnituse teenus Inglise keeles: Online Certificate Status Protocol
QC	e-allkirja kvalifitseeritud sertifikaat – e-allkirja sertifikaat, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab eIDAS lisas I sätestatud nõuetele Inglise keeles: Qualified Certificate
SSCD	Kvalifitseeritud e-allkirja andmise vahend Inglise keeles (eIDAS termin): Secure signature creation device Vastab eIDASe määruse lisas II olevatele nõuetele.
STO	Sertifitseerimisteenuse osutaja Inglise keeles *CSP – Certification Service Provider*
EL usaldusnimekiri	Euroopa Liidu usaldusteenuste osutajate usaldusnimekiri (https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers) Inglise keeles: EU Trusted Lists of Certification Service Providers
Täiustatud e-allkiri	- digitaalne allkiri peab olema seotud ainuüksi allkirja andjaga; - selle abil on võimalik tuvastada allkirja andjat; - see antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja, - see on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatavad. Inglise keeles: Advanced Electronic Signature, lühend „AdES", vastavalt eIDAS määruse definitsioonile
Ajatempel (eIDAS määruse definitsioon: „e-ajatempel")	Elektroonilised andmed, mis seovad muud elektroonilised andmed kindla ajahetkega ja tõendavad, et viimatinimetatud andmed olid sel ajahetkel olemas. Ajatempleid väljastavad ATO-d.
Ajamärgend	Usaldusteenuse poolt salvestatav andmekirje, mis seob andmed kindla ajahetkega.

2.3 Uurimisülesanded

Uuringu eesmärgiks oli hinnata digitaalse allkirjastamise tänast taset EL 28 liikmesriikides ning Norras, Šveitsis ja Islandil ning välja töötada metoodika digitaalse allkirja kasutatavuse osas info regulaarseks kogumiseks ja jälgimiseks kõigis EL liikmesriikides.

Projektile püstitatud uurimisülesanded olid järgmised:

1. Tööealiste elanike digitaalse allkirja kasutamise osakaalu määramine EL 28 liikmesriigis ning Norras, Šveitsis ja Islandil
   - Milline on üldises võtmes realiseeritud digiallkirja tehniline lahendus?
   - Kui suur on digitaalset allkirja kasutav tööealise elanikkonna osakaal?
   - Kui palju on riigis kvalifitseeritud usaldusteenuste osutajaid?
   - Kui palju on väljaantud kvalifitseeritud sertifikaate?
   - Kas kvalifitseeritud sertifikaadid antakse välja turvalise allkirja andmise vahendile?
2. Töötada välja metoodika digitaalse allkirja kasutatavuse hindamiseks ja regulaarseks jälgimiseks EL-is
3. Tulenevalt uuringutulemustest anda poliitikasoovitused digitaalse allkirja kasutamise edendamiseks EL-s.

Etteruttavalt võib öelda, et tänases digitaalse allkirjastamise osas puuduliku andmekogumise olukorras on võimalik teha ainult ligikaudseid hinnanguid ja sedagi vaid teatud riikide osas.

2.4 Andmekogumise meetodid

Käesoleva uuringu andmekogumise allikateks olid peamiselt EL usaldusnimekirja kuuluvad kvalifitseeritud usaldusteenuste osutajad, samuti uuritavates riikides tegutsevad e-allkirjastamise valdkonna reguleerimisega seotud asutused. Valdkonna reguleerimisega seotud asutuste all on mõeldud kvalifitseeritud usaldusteenuse osutajate üle järelevalvet teostavate regulaatorite ja/või ministeeriumide esindajaid. eIDAS töögruppide liikmetega kontakteeruti suuremate riikide puhul, kui kvalifitseeritud usaldusteenuse osutajatelt ja valdkonda reguleerivatelt asutustelt ei õnnestunud vastuseid saada. Andmete allikate olulisus varieerus erinevates riikides olulisel määral – kui mõnes riigis olid andmeallikateks enam usaldusteenuse osutajad, siis teistes riikides olid nendeks pigem järelevalvet teostavad ametiasutused.

Tabel 1. Uuringu allikate ülevaade

	Kirjade saanute arv (tk)	Vastanute arv (tk)	Vastamise määr (%)
Kvalifitseeritud usaldusteenuse osutajad	143	31	22%
Regulaatorid	32**	21	65%
eIDAS töögrupi liikmed*	11	5	45%
Kokku	**186**	**57**	

* arvestatud 1 isik ühe riigi kohta, kuid tegelikkuses oli eIDAS töögrupis 3-4 inimest ühte riiki esindamas.

**Poolas ja Austrias olid kontaktiks 2 asutust. Islandi regulaatorile kirja ei saadetud.

3. Metoodika

3.1 E-allkirja mõiste erinevad tõlgendused

E-allkirja või digiallkirja mõiste on paljuski juurdunud erinevate gruppide teadvusesse läbi erinevate praktikate ja tõlgenduste skaala on väga lai. Ühtse arusaamise puudumine teeb raskeks ka dialoogi info hankimisel – e-allkirja olemusest ja kasutamisest saadakse väga erinevalt aru, mistõttu on ka andmed sageli madala kvaliteediga, raskesti kasutatavad ja ei ole omavahel võrreldavad.

Siinkohal on sobiv lühidalt kirjeldada e-allkirjade erinevaid liike, lähtudes turvalisuse tasemetest (alustades kõige madalamast).

a) e-allkiri – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida allakirjutaja kasutab allkirja andmiseks. Lihtsal e-allkirjal (*Basic Electronic Signature*) puuduvad täiendavad turvameetmed allkirjastaja ja allkirja autentsuse tagamiseks.

b) Täiustatud e-allkiri (AdES – *Advanced Electronic Signature*) – e-allkiri, mida saab valideerida füüsilisele isikule väljastatud sertifikaadi abil

c) Täiustatud e-allkiri kvalifitseeritud sertifikaadiga (AES/QC)

d) Kvalifitseeritud e-allkiri (*QES*) – eIDAS-e kohaselt on kvalifitseeritud e-allkiri täiustatud e-allkiri (defineeritud artiklis 26), mis antakse kvalifitseeritud e-allkirja andmise vahendi abil (nõuded toodud määruse lisas II) ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil (eIDAS määruse lisas I toodud nõuetele vastav sertifikaat, mis on väljastatud kvalifitseeritud usaldusteenuse osutaja poolt).

Selleks, et kvalifitseeritud e-allkiri oleks kehtiv, tuleb täiendavalt vaadata artiklit 32, mis toob sisse ka allkirja andmise aja olulisuse – just allkirja andmise ajal peab sertifikaat olema kehtiv, vastama nõuetele jne.

Käesolevas uuringus on vaatluse all ainult kvalifitseeritud e-allkirjad ja täiustatud e-allkirjad, mis põhinevad e-allkirja kvalifitseeritud sertifikaadil (e-allkirjade tasemed c ja d).

Põhilisteks vaatluse alt välja jäävateks e-allkirjade kategooriateks on:

- Igasugused e-kinnitused, mis ei põhine sertifikaadil („nõustun" - nupuvajutused jms digitaalne tõendusmaterjal).
- E-allkirjad, mis ei põhine kvalifitseeritud sertifikaadil: sertifikaat ei ole nõuetekohaselt väljastatud füüsilisele isikule. Siia hulka kuuluvad ka organisatsioonide poolt väljastatavad e-templid jms.
- Elektroonilise isikutuvastamise käigus moodustuvad andmekogumid ehk „autentimise tulemused", mille puhul kasutatakse kvalifitseeritud sertifikaadi nõuetele vastavaid, kuid mitte allkirjastamiseks mõeldud sertifikaate.
- E-allkirjad, mille puhul ei ole võimalik kindlaks teha määruse nõuete täidetust e-allkirja andmise ajal.

Viimane aspekt, kui juriidiliselt uudne Euroopa kontekstis, väärib pikemat käsitlust. Vastavalt eIDAS artikli 32 p.1. lõigetes (a) ja (b) toodud nõuetele kehtib täiustatud e-allkiri ainult siis, kui allkirja andmise ajal oli allkirja andmiseks kasutatud sertifikaat kehtiv, vastas kvalifitseeritud sertifikaadile esitatud nõuetele ja oli väljastatud kvalifitseeritud usaldusteenuse pakkuja poolt. Järelduvalt tuleb

allkirja loomisel fikseerida usaldataval moel selle tekitamise aeg kas otseselt (absoluutse ajana) või kaudselt (sündmusena teiste sündmuste jadas).

Allkirjastamise aja usaldatavuse tagamiseks tuleb sündmus fikseerida kolmanda osapoole juures. Sellisteks osapoolteks on ajatempli või ajamärgendi teenuse pakkujad, kes fikseerivad loodud allkirja andmed, lisades sellele ajalise mõõtme. eIDAS defineerib kvalifitseeritud e-ajatemplitele esitatavad nõuded artiklis 42.

Kui ajatempliteenuse pakkuja väljastab ajatempli koheselt, siis ajamärgendi teenuse osutajal on kohustus ajamärgendeid salvestada ja esitada vaid asjakohasel nõudmisel. Näiteks Eestis on loodud kombineeritud teenus, mis ühendab endas kehtivuskinnituse ja ajamärgendi funktsionaalsuse – (salvestatud) ajamärgend antakse kaasa iga teenuse poolt väljastatava positiivse kehtivuskinnitusega. Seda teenust kasutatakse Eestis eranditult kõikide digitaalallkirjade moodustamisel.

Kui e-allkiri sisaldab ajatemplit, kuid ei sisalda sertifikaadi kehtivusinformatsiooni, siis peab e-allkirja valideerijal olema võimalus seda informatsiooni saada täiendavatest allikatest lähtudes allkirjastamise ajahetkest.

Käesolev uuring ei loe kvalifitseeritud e-allkirjadeks neid e-allkirju, millel puudub ajatempel või -märgend.

Teine rohkelt vaidlusi tekitav teema, on e-allkirja andmise vahendi vastavus kvalifitseerituse nõuetele. Asjakohane määruse lisa 2 kasutab korduvalt mõisteid „piisavalt" ja „reaalselt", mis on hinnangulised, mitte defineerivad. Olukorda selgitavad Määruse preambula punktid 55 ja 56 , millest selgub, et asjakohaseid tehnilisi nõudeid ei pruugigi olemas olla ja et „kasu võiks olla vastastikusest hindamisest". See sedastus kirjeldab olukorda adekvaatselt, mistõttu ongi tekkinud olukord, kus must-valge vastavus kvalifitseeritud e-allkirja andmise vahendile on praktikas asendunud pigem „hinnangutega".

Harilikult kasutatakse kvalifitseeritud e-allkirja andmise vahendina omanikule füüsiliselt väljastatud kiipkaarti tema erinevates vormides (SIM-kaart, pangakaardi formaadis plastkaart, USB-pulk, jne). Sellisele vahendile on võimalik anda hinnang lähtuvalt asjaomastes standardites (EAL 4+ jm) kehtestatud nõuetest. Seda, aga erinevatel tasemetel: kas riistvara tasemel, kaardi operatsioonisüsteemi tasemel või kaardil oleva rakenduse tasemel. Kui vahend vastab (mingi taseme osas) fikseeritud nõuetele, siis saab sellele vahendile taotleda tootesertifikaati. Sellise tootesertifikaadi olemasolu annab aluse pidada vahendit ka kvalifitseerituks.

Kuna kvalifitseeritud e-allkirja andmise vahend peaks olema isiku ainuvalduses, siis ei tohiks sellele nõudele vastata lahendus, kus sertifikaat asub teenusepakkuja serveris. Selliseks näiteks on Austrias toimiv lahendus , kus kasutajad annavad infosüsteemi sisenemisel seadusekohase e-allkirja dokumendile „Mina, /isikuandmed/ avaldan soovi infosüsteemi /nimetus/ sisenemiseks /aeg/". Vastav e-allkirjastamine toimub paroolipõhiselt mobiiltelefoni abil, isikule omistatud allkirjastamiseks kasutatavaid andmeid (*privaatvõtit*) säilitatakse teenusepakkuja infosüsteemis, mitte isiku valduses. Kogu see skeem, vaadelduna e-allkirja andmise vahendina, on audiitori poolt hinnatuna kuulutatud kvalifitseerituks.

Käesolev uuring lähtub e-allkirja andmise vahendi kvalifitseerituks pidamisel selle „väljastaja" hinnangust.

Mõningatel juhtudel on privaatvõtme kandja väljastaja erinev sellele digitaalseks allkirjastamiseks sobiva privaatvõtme genereerijast ja sertifikaadi väljastajast. Näiteks võib tuua Saksamaa ID-kaardi, mille riik väljastab vaid digitaalse isikutuvastamise funktsiooniga ja koos „pesaga" sinna e-

allkirjastamise võimaluse lisamiseks. Viimast peab kaardi saaja tegema iseseisvalt valides endale sobiva teenusepakkuja vaba turumajanduse tingimustes. Kokkuvõtvalt võib öelda, et osapool, kes on formaalselt võtnud vastutuse e-allkirjastamise vahendi nõuetele vastavuse eest, ei pruugi tegelikkuses olla selle reaalne väljastaja.

3.2 Infoallikate ülevaade

Järgnevalt anname ülevaate töös kasutatud infoallikatest, organisatsioonidest, kellega töö käigus ühendust võeti ja nende poolt väljastatud informatsiooni koosseisust.

Ainukene süstemaatiline kasutatav allikas on hetkel Euroopa Liidu Usaldusteenuste osutajate Usaldusnimekiri[2]. EL liikmesriikidel on Teenuste Direktiivi rakendumisest tulenenud kohustus koostada ja avaldada omas riigis tegutsevate riikliku järelvalve all olevate sertifitseerimisteenuste osutajate (STO-de) nimekiri, kes väljastavad e-allkirjastamiseks ette nähtud kvalifitseeritud sertifikaate avalikuks kasutuseks. Nimekirja *võib* peale STO-de ja nende teenuste olla kantud ka sertifikaatide kehtivuskinnitusteenused ja ajatempliteenused.

Usaldusnimekirjast on võimalik teada saada STO kontaktinformatsioon ja väljastatavate sertifikaatide nimistu koos viidetega teenust kirjeldavale dokumentatsioonile. STO on kohustatud pidama arvet väljastatud sertifikaatide ja nende kehtivuse üle, kuid vastavat koondinfot ei ole ta kohustatud väljastama. Paljudel juhtudel STO jagab siiski meeleldi vastavat informatsiooni v.a. juhul, kui see ei ohusta tema ärihuve – STO-de vahel toimub mõnes riigis tihe konkurents. Kehtivate e-allkirjastamiseks mõeldud sertifikaatide arv aga ei anna käesoleva uuringu kontekstis siiski otseselt tegelike e-allkirjastajate arvu, kuna kõik kehtivate sertifikaatide omanikud ei pruugi neid kasutada.

Lisaks kehtivale kvalifitseeritud sertifikaadile ja allkirja andmise vahendile on e-allkirja moodustamiseks vajalik fikseerida ka selle moodustamise aeg. Seetõttu on teine oluline usaldusteenuse pakkuja ajatempliteenuse osutaja (ATO). Kõik asjakohased ATO-d ei pruugi olla Usaldusnimekirjas loetletud. ATO ei pruugi aga paraku omalt poolt teada, millisel otstarbel ta ajatempleid väljastab – ajatembeldada võib suvalist informatsiooni tagamaks selle tervikluse tõestust kindlal ajahetkel. Isegi kui ATO teab, milliseid tema poolt väljastatud ajatempleid kasutatakse just e-allkirjale lisamiseks, ei tea ta *kelle* e-allkirja ajatembeldatakse. Teiste sõnadega – ATO ei tea e-*allkirjastajatest* mitte midagi; parimal juhul oskab ta öelda e-allkirjadele lisamiseks väljastatud ajatemplite arvu.

Sertifikaatide kehtivust saab lisaks sertifikaadis endas sisalduvale algus- ja lõpptähtajale kontrollida kahel viisil: STO-de poolt väljastatava sertifikaatide tühistusnimekirja (CRL) või kehtivuskinnituse teenuse (OCSP) abil. Juhul, kui kehtivust kontrollitakse CRL abil, ei jää kontrollimise toimingust mingit jälge: seega ei ole vastav kasutusjuht allkirjade ja/või allkirjastajate arvu väljaselgitamise seisukohalt kasutatav. OCSP puhul aga küsib valideerija OCSP-teenuselt sidusrežiimis konkreetse sertifikaadi kehtivuse infot ning saab positiivsel juhul teenusepakkuja poolt e-templiga varustatud vastuse, milles sisaldub ka selle kinnituse väljastamise aeg.

Kehtivuskinnituse teenuse osutajad (KKTO-d) on üldjuhul needsamad STO-d, kes vastavaid sertifikaate väljastavad. Leidub ka erandeid, kus kehtivusteenuseid vahendatakse: näiteks Eestis pakutavast Proxy-OCSP teenusest[3] saab vastuseid ka Soomes, Lätis ja Leedus väljastatud sertifikaatide kehtivuse kohta.

[2] https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers
[3] https://www.sk.ee/teenused/kehtivuskinnituse-teenus/proxy-ocsp/

KKTO ei pruugi aga teada, kas tema poolt väljastatud kinnitusi kasutatakse e-allkirja moodustamisel või selle valideerimisel. Eestis kasutatav praktika, kus kehtivuskinnitus võetakse e-allkirjale koheselt selle moodustamise järel, on küll efektiivne[4], kuid sellist lähenemist mujal laialdaselt ei viljeleta. Seega teab KKTO, kes on e-allkirjastanud aga ei pruugi teada seda, mitu erinevat e-allkirja on keegi loonud. Põhiliseks probleemiks on aga asjaolu, et KKTO ei tee üldjuhul oma teenuse kasutamise kohta käesoleva uuringu jaoks huvi pakkuvat statistikat: loetakse küll päringute koguarvu, kuid ei peeta arvet päringute kohta individuaalsete sertifikaatide lõikes. Viimane annaks vastuse kui mitme erineva sertifikaadi kohta on kehtivust küsitud ehk siis (teatavate mööndustega[5]) mitme erineva isiku poolt on e-allkirju loodud või valideeritud.

E-allkirja saab iga kasutaja põhimõtteliselt luua iseseisvalt oma arvuti või nutiseadme töölauarakenduses (*a la* DigiDoc Client). Suur osa e-allkirjadest luuakse aga veebipõhistes allkirjastamisest võimaldavates infosüsteemides. Viimaste käes on olemas detailne informatsioon, kes ja milliseid e-allkirju on tema teenuses moodustanud. Kahjuks aga puudub igasugune süstemaatiline informatsioon selliste keskkondade ja nende haldajate kohta. Lisaks sellele, ei pruugi seal kogutav informatsioon allkirjastajate kohta olla avalik.

Riikliku järelvalveorgani põhiline ülesanne on järelvalve läbiviimine tema riigis töötava usaldusteenuse pakkuja üle. Järelvalve alla ei kuulu statistika kogumine järelvalvatavatelt, küll aga leidub riike, kus järelvalvaja on (vabatahtlikult) siiski mingil kujul sellist infot kogunud.

Viimaseks infoallika klassiks on eksperdid, kes on mingil põhjusel motiveeritud omama ülevaadet riigis toimuvast e-allkirjastamise alal. Eksperte võib leida kõigi ülalnimetatud organisatsioonide personali hulgast aga neid võib leiduda ka riiklikes organisatsioonides, kes teostavad laiapõhjalist IKT koordineerimist avalikus sektoris.

3.3 E-allkirjastajate arvu leidmiseks kasutatud metoodika

Eelmisest peatükis nähtub, et üldjuhul on praeguses situatsioonis täpse e-allkirjastajate arvu leidmine enamikes riikides väga keeruline. Järgnevalt toome välja mõned olulisemad põhjused:

1. Kehtivate e-allkirjastamiseks väljastatud sertifikaatide omanikud ei pruugi neid kasutada – mitmete riikide kohta õnnestus uuringu käigus teada saada kehtivate kvalifitseeritud sertifikaatide arv või selle hinnang, kuid tegeliku sertifikaatide kasutuse kohta allkirjastamiseks saime infot märgatavalt vähem.
2. ATO ei tea, kelle e-allkirju (ja kas üldse e-allkirju) ajatembeldatakse – infot väljastatud ajatemplite arvu kohta õnnestus saada vaid 1 riigi kohta, kusjuures ka selle riigi puhul ei saanud sellest infost tuletada kui paljud neist ajatemplitest olid e-allkirjade tarbeks.
3. KKTO (kui seda kasutatakse) ei pea arvet antud vastuste kohta sertifikaatide lõikes; Kehtivuskinnituste arvu osas saadi uuringu käigus infot kahe riigi kohta (Eesti ja Belgia). Belgia puhul kuulusid sinna hulka nii autentimise kui ka allkirjastamise päringud ja kuna nende eristamine ei ole hetkel kahjuks teostatav, siis ei saanud uuringus ka seda infot allkirjastajate arvu leidmisel otseselt ära kasutada. Samas peaks siiski KKTO-del olema soovi korral võimalik neid päringuid eristada ja vastavat statistikat koguda, mida Eesti KKTO AS Sertifitseerimiskeskus nende poolt väljastatud sertifikaatide kasutuse andmete esitamisega ka tõestas.

[4] **Ühte e-allkirja võib valideerida lugematu hulk kordi ning kui igal valideerimisel tehakse OCSP-päring, siis genereerib see ühe allkirja kohta palju päringuid. Seevastu, kui kehtivuskinnitus võetakse koheselt allkirja moodustamisel, genereerib see ainult ühe päringu allkirja kohta. Kinnitus liidetakse e-allkirja koosseisu ja on kasutatav vallasrežiimis kõikidele valideerijatele.**

[5] **Ühel isikul võib olla mitu erinevat sertifikaati**

4. E-allkirjastamist võimaldavate rakenduste kaudu allkirjastajate arvu leida on raske või võimatu:
    a. E-allkirjastamine töölauarakenduse abil arvutis või nutiseadmes ei ole jälgitav;
    b. E-allkirjastamine organisatsiooni siseses infosüsteemis ei ole jälgitav;
    c. E-allkirjastamist pakkuvate avalike veebipõhiste keskkondade usaldusväärset loetelu ei ole olemas. Kui ka oleks, siis sellegi poolest:
        i. Keskkondade haldurid ei pruugi oma kasutajate statistikat väljastada
        ii. Erinevad keskkondi kasutavad samad e-allkirjastajad, seega esineb ülekattuvusi
        iii. Üldjuhul puudub „liiderkeskkond", kus suure tõenäosusega oleksid esindatud kõik e-allkirjastamist kasutavad isikud riigis.
        Uuringu käigus tuvastati vaid üks juhtum (Island), kus selline lahendus oli käesoleva uuringu kontekstis kasutamiseks sobilik. Enamasti nn. „liiderkeskkonnad" ei kasuta kvalifitseeritud sertifikaate, mistõttu need jäävad käesoleva uuringu skoobist välja.

Kõige lähedasem meetod e-allkirjastajate arvu ligikaudseks leidmiseks tundub olevat kehtivate, e-allkirjastamiseks väljastatud kvalifitseeritud sertifikaatide arvu aluseksvõtt ning edasise hinnangu andmine sõltuvalt sihipärase nõudluse olemasolust ja eksperthinnangutest. Kehtivate sertifikaatide üle peavad STO-d arvet ning peaks olema nõus teatavatel tingimustel (konkurentsiriski puudumisel) nende koguarvu väljastama.

Sihipärane nõudlus on olemas siis, kui sertifikaadi omanik maksab ise e-allkirjastamiseks mõeldud sertifikaadi ja ainult selle eest. Sellistel juhtudel võib eeldada, et 100% sertifikaadi omanikest seda ka sihipäraselt kasutavad ehk siis e-allkirjastavad oma sertifikaadi alusel. Paljudel muudel juhtudel see nii ei ole – selliseks näiteks on riiklikud ID-kaardid, mida väljastatakse vaikimisi koos aktiivse e-allkirjastamise sertifikaadiga ja mille kasutusaktiivsus on märgatavalt väiksem.

Mitmete riikide puhul väljastati uuringu läbiviijatele infot sihipärase nõudluse alusel väljastatud kvalifitseeritud sertifikaatide osas. Samas vaadates selliste sertifikaatide osakaalu kogu tööealisesse elanikkonda ei ole see enamasti väga laialdase kasutusega.

Sihipärase nõudluse puudumisel saab kehtivate sertifikaatide e-allkirjastamiseks kasutamise määra leidmisel tugineda eksperthinnangutel, mida annavad eelmises jaotises nimetatud eksperdid. Peale sihipärase nõudluse ei tuvastanud töö läbiviijad ühtki teist korreleerivat parameetrit aktiivsete sertifikaatide ja e-allkirjastajate arvu vahel[6]. Kahjuks aga ei õnnestunud uuringu käigus ka selliselt kõikide riikide osas infot saada – peamine mure on suurte riikidega (Saksamaa, Prantsusmaa ja Hispaania), kus on palju STO-sid, kelledelt ammendavat katvust saada ei olnud võimalik ja ka regulaatorid ning eksperdid ei saanud või ei osanud asjakohaseid andmeid või hinnanguid e-allkirjastajate arvu osas anda. Eraldi juhtum suurte riikide seas on Ühendkuningriik, kus ei ole hetkel registreeritud ühtegi kvalifitseeritud sertifikaatide väljastajat. Sarnaseid väiksemaid riike on teisigi – näiteks Iirimaa, Taani, Malta jne.

Ühe faktorina saaks veel arvesse võtta riigi e-valitsemise (sealhulgas e-allkirjastamise kasutatavuse ja kultuuri) üldist küpsustaset, kuid selle mõõtmise metoodikaid ei ole uuringu läbiviijate teada

[6] **Näiteks puudub korrelatsioon ID-kaardi väljastamise praktika kaua-aegsuse ja selle elektroonilise kasutatavuse osas. Samas on see paljude riikide puhul ainsaks hetkel kättesaadavaks parameetriks mingigi asjakohase hinnangu väljatöötamisel.**

mõistlikul ja kasutataval kujul veel välja töötatud.

Allkirjastajate arvu eduka määramise näitena, kus õnnestus suure täpsusega määrata allkirjastajate arv, saab välja tuua kaks riiki:

- **Eesti**: kõikidele e-allkirjadele võetakse nende moodustamisel kehtivuskinnitus ning KKTO peab erinevate sertifikaatide kohta tehtud päringute üle arvet, mistõttu saadi täpne info uuritava vanusegrupi hulgas e-allkirja andnud isikute arvu kohta;
- **Island**: ühekordse riikliku kampaania raames tekkis nn „liiderkeskkond", kus viie kuu jooksul 12.2014 – 04.2015 andis e-allkirja ligi 80 tuhat Islandi residenti, mis on võrreldavas suurusjärgus kehtivate sertifikaatide arvuga.

4. Digitaalallkirja kasutamine

4.1 Digiallkirja tehnilised lahendused

Käesolevas jaotises on antud üldine ülevaade peamistest tehnilistest lahendustest, mida vaadeldud riikides kvalifitseeritud sertifitseerimisteenuse osutajad kasutavad. Eelkõige pööratakse tähelepanu kvalifitseeritud e-allkirjastamise vahendite kasutamisele ja erinevatele sertifitseerimise tugiteenustele, nagu kehtivuskinnituse ja ajatempliteenus.

4.1.1 Kvalifitseeritud e-allkirjastamise vahendid

eIDAS määrus defineerib kvalifitseeritud e-allkirja andmise vahendi kui seadistatud tark- või riistavara, mida kasutatakse e-allkirja andmiseks. Enamikes riikides on kasutusel e-allkirja andmise vahend, mis esineb erinevates kasutusvormides, näiteks kiipkaardi, SIM-kaardi, USB pulga või serveripõhise lahendusena. Seda, kas e-allkirja andmise vahend loetakse kvalifitseerituks või mitte sõltub sellest kuidas iga liikmesriik kvalifitseeritud e-allkirja andmise vahendi mõistet tõlgendab. Siin peatükis tuuakse lühidalt välja info uuringus hõlmatud riikides kasutatavate kvalifitseeritud e-allkirja andmise vahendite kohta.

Küsitavusi kvalifitseeritud e-allkirja andmise vahendile vastavuse osas võivad tekitada nn. serveripõhised allkirjastamise vahendid, kus allkirjastamise vahendina käsitletakse serveris asuvat digitaalse allkirjastamise privaatvõtit, mis aga ei ole turvalise allkirja andmise definitsiooni kohaselt omaniku ainuvalduses. Kui näiteks Austrias on serveripõhine lahendus audiitorite poolt tunnistatud kvalifitseeritud e-allkirja andmise vahendiks, siis on hulgaliselt riike nagu näiteks Belgia, Itaalia, Läti, Prantsusmaa, Šveits, kus sarnaselt Austriale hoiustatakse kasutaja privaatvõti turvamoodulis (HSM) serveris, kuid sellisele lahendusele ei ole antud turvalise e-allkirja andmise vahendi kvalifikatsiooni.

Enamik uuringus vastanud riikide esindajatest hindas, et riigis antakse kvalifitseeritud sertifikaadid valdavalt kvalifitseeritud e-allkirja andmise vahendile. Sõltuvalt Direktiivi 1999/93/EÜ adapteerimise tulemustest on paljudes EL riikides kvalifitseeritud sertifikaadi puhul kvalifitseeritud e-allkirja andmise vahendi kasutamine kohaliku seadusandluse järgi kohustuslik. Kui seda ei ole seadusega reguleeritud, siis võib kvalifitseeritud sertifikaate lisada ka mitte-kvalifitseeritud e-allkirja andmise vahendile.

Kvalifitseeritud e-allkirja andmise vahendina on laialdaselt kasutusel kiipkaart (vt tabel 2). Rohkelt väljastatakse kvalifitseeritud sertifikaate ka USB pulkadele. SIM-kaarte kasutati kvalifitseeritud e-allkirja andmise vahenditena põhiliselt mobiil-ID laadsete e-allkirjastamise lahenduste puhul. Viimasel juhul võib sertifikaat asuda kas SIM-kaardil või kvalifitseeritud usaldusteenuse pakkuja HSM serveris. Huvitava näitena paistis silma Itaalia, kus kvalifitseeritud sertifikaat paigaldatakse ka micro-SD kaardile.

Uuringus osalenud riikidest hindas ainukesena Norra riigis kasutatavad e-allkirjastamise vahendid kvalifitseeritud e-allkirja andmise vahendi nõuetele mittevastavateks. Lühidalt selgitades tähendab see, et Norras olevate kvalifitseeritud usaldusteenuste osutajate poolt välja antud kvalifitseeritud sertifikaatidega ei saa anda kvalifitseeritud digitaalset allkirja (QES), sest allkirja andmise vahendi väljastaja hinnangul ei ole privaatvõtmed ja sertifikaadid paigaldatud kvalifitseeritud e-allkirja moodustamise vahendile.

Mõnede riikide osas, nagu Malta, Taani ja UK ei ole teada milliseid kvalifitseeritud sertifikaate ja kvalifitseeritud e-allkirja andmise vahendeid kasutatakse, sest riigis ei ole registreeritud kvalifitseeritud usaldusteenuse osutajaid ning järelevalvet tegevad asutused ei oma selle kohta informatsiooni.

Uuringusse kuuluvates riikides kasutatavatest kvalifitseeritud e-allkirjastamise vahenditest annab ülevaate tabel 2.

Tabel 2. Kvalifitseeritud e-allkirja andmise vahendid

Riik	Kiipkaart	SIM-kaart	USB pulk	Serveri põhine	Micro-SD
Austria	√			√	
Belgia	√		√	*	
Bulgaaria	√		√		
Eesti	√	**		*	
Hispaania	√		√	*	
Holland	√		√		
Horvaatia	√		√		
Iirimaa	-	-	-	–	–
Island	√	√			
Itaalia	√	√	√	*	√
Kreeka	√		√		
Küpros	√		√		
Leedu	√	√	√		
Luksemburg	√		√		
Läti	√			*	
Malta	-	-	-	–	–
Norra	+		+		
Poola	√		√		
Portugal	√		√		
Prantsusmaa	√		√	*	
Rootsi	√				
Rumeenia	√		√		
Saksamaa	√				
Slovakkia	√		√		
Sloveenia	√		√		
Soome	√	√		*	
Šveits	√			*	
Taani	-	-	–	–	–
Tšehhi	√		√		
UK	-	-	–	–	–
Ungari	√		√	*	

*riikides on HSM server privaatvõtme hoiustamiseks kasutusel, kuid teadaolevalt ei ole need tunnustatud kui kvalifitseeritud e-allkirja andmise vahendid.
+ riigis antakse välja kvalifitseeritud sertifikaate kiipkaardile ja USB pulgale, kuid regulaatori hinnangul ei ole tegemist SSCD-ga.

- riigis ei anta välja kvalifitseeritud sertifikaate. Kvalifitseeritud e-allkirja andmise vahendeid ei kasutata.

**teadaolevalt asub privaatvõti teenusepakkuja serveris.

Riiklik elektrooniline ID-kaart

Üks oluline näitaja, mis iseloomustab riigi digitaalse allkirjastamise potentsiaali, on riikliku elektroonilise ID kaardi (e-ID kaart) olemasolu ja levik. Kuigi riikliku e-ID kaardi levik ei oma otsest

seost e-allkirjastamisega, siis loob ta siiski selleks eeldused eelkõige riigi elanike käitumisharjumuste kujundamisega ja usalduse kasvatamisega e-teenuste vastu.

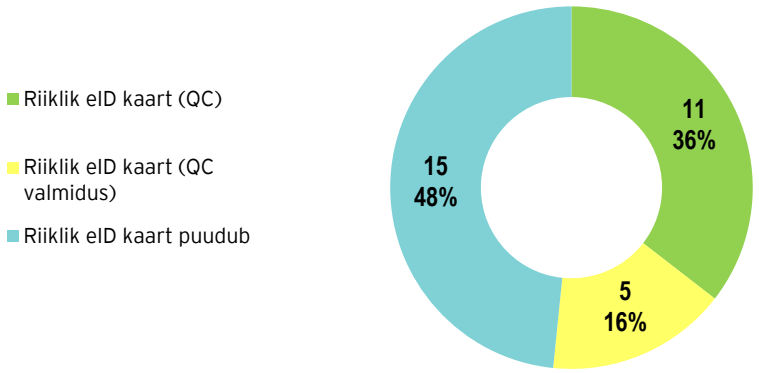
Uuringu käigus vaadeldud riikide seas võib eristada riike, kus on kasutusel riiklik e-ID kaart ja riike, kus sellist kaarti ei väljastata. 52% vaadeldavatest riikidest väljastatakse kvalifitseeritud sertifikaadiga riiklikult e-allkirjastamise vahendit. See näitaja ei kirjelda siiski e-ID kaardi levikut elanikkonna seas, vaid ainult riigis rakendatava e-ID kaardi omadusi.

Lisaks e-ID kaardi olemasolule eristati uuringus neid riike, kus e-ID kaardile kantakse ka kvalifitseeritud sertifikaat, mis on vajalik e-allkirja andmiseks ja neid riike, kus on e-ID kaardile paigaldatakse algselt mitte-kvalifitseeritud sertifikaat või esialgu sertifikaate e-ID kaardile ei panda, kuid see võimalus on olemas. Viimasel juhul on kaardiomanikul võimalik taotleda kvalifitseeritud sertifikaadi lisamine e-ID kaardile (mis on üldjuhul tasuline).

Uuringust selgub, et 11-s vaadeldud riigis (36%) antakse välja riiklikku elektroonilist ID-kaarti, millel on peal kvalifitseeritud sertifikaat e-allkirjastamiseks ja täiendavalt on 5-s riigis (16%) olemas selleks valmidus (vt. joonis 1).

e-ID kaardi kasutatavus sõltub ka riigi seadusandlusest, peamiselt asjaolust, kas selline kaart on kohustuslik või mitte. Näiteks Eestis ja Belgias on kohustuslik omada ID-kaarti, millele on juba väljastamise hetkel kantud kvalifitseeritud sertifikaadid. Samal ajal näiteks Rootsis on e-ID kaardi omamine soovituslik ning välja antud kvalifitseeritud sertifikaatide arv e-allkirjastamiseks tagasihoidlik.

48% riikides kas ei ole riiklikku e-ID kaarti kasutusel või põhinevad need mitte-kvalifitseeritud sertifikaadil, mistõttu need jäävad antud uuringu skoobist välja.



Joonis 1. E-ID kaardi olemasolu

Ülevaade riiklike e-ID kaartide olemasolu kohta uuringusse kuuluvates riikides on esitatud tabelis 3.

Tabel 3. E-ID kaartide kasutamine

Riik	e-ID kaardi olemasolu
Austria	Riiklik e-ID kaart puudub*
Belgia	Riiklik e-ID kaart (QC)
Bulgaaria	Riiklik e-ID kaart puudub
Eesti	Riiklik e-ID kaart (QC)
Hispaania	Riiklik e-ID kaart (QC)

Holland	Riiklik e-ID kaart puudub
Horvaatia	Riiklik e-ID kaart (QC)
Iirimaa	Riiklik e-ID kaart puudub
Island	Riiklik e-ID kaart (QC)
Itaalia	Riiklik e-ID kaart (QC võimekus)
Kreeka	Riiklik e-ID kaart puudub
Küpros	Riiklik e-ID kaart puudub
Leedu	Riiklik e-ID kaart (QC)
Luksemburg	Riiklik e-ID kaart (QC võimekus)
Läti	Riiklik e-ID kaart (QC)
Malta	Riiklik e-ID kaart puudub
Norra	Riiklik e-ID kaart puudub
Poola	Riiklik e-ID kaart puudub
Portugal	Riiklik e-ID kaart (QC)
Prantsusmaa	Riiklik e-ID kaart puudub
Rootsi	Riiklik e-ID kaart (QC)
Rumeenia	Riiklik e-ID kaart puudub
Saksamaa	Riiklik e-ID kaart (QC võimekus)
Slovakkia	Riiklik e-ID kaart (QC)
Sloveenia	Riiklik e-ID kaart (QC võimekus)
Soome	Riiklik e-ID kaart (QC)
Šveits	Riiklik e-ID kaart puudub
Taani	Riiklik e-ID kaart puudub
Tšehhi	Riiklik e-ID kaart (QC võimekus)
UK	Riiklik e-ID kaart puudub
Ungari	Riiklik e-ID kaart puudub

*Riiklik e-ID kaart puudub - e-ID kaardile ei lisata koheselt või ole võimalik hiljem lisada kvalifitseeritud sertifikaati. Mitte-kvalifitseeritud sertifikaate kandvad e-ID kaardid olid uuringu skoobist väljas.

4.1.2 Kehtivuskinnitusteenus (OCSP) ja ajatempel

Uuringu käigus uuriti EL Usaldusnimekirjas olevatelt STO-delt, kas nad pakuvad lisaks sertifikaatide tühistusnimekirjale (CRL) ka kehtivuskinnituse teenust, mis põhineb OCSP protokollil. Kui STO-delt ei õnnestunud selle kohta informatsiooni saada, tuginesid uuringu läbiviijad avalikes allikates olevale informatsioonile. Tabelis 3 on välja toodud riigid, kus enamik riigis tegutsevaid STO-sid pakuvad lisaks CRLile ka veel kehtivuskinnitusteenust. Selgub, et see teenus on kasutusel üle 50% vaadeldavates riikides suurema osa STO-de hulgas. Siiski ei tähenda see, et ülejäänud riikides pole kehtivuskinnitusteenust pakkuvaid STO-sid.
Lisaks kehtivuskinnitusteenusele uuriti, kas STO-d pakuvad ajatempliteenust. 54% vaadeldud riikides pakub suurem osa STO-sid ka ajatempli teenust, kusjuures näiteks Belgias ja Itaalias on STO-del kohaliku seaduse järgi kohustuslik lisada ajatempel e-allkirjastamise hetkel. Lätis ja Slovakkias on näiteks ajatempli lisamine kohustuslik juhul, kui allkirjastatud dokumendid saadetakse riigiasutustele.

Tabel 4. Kehtivuskinnitusteenuse rakendamine ja ajatempli teenus

Riik	OCSP rakendamine	Ajatempli teenus
Austria	√	√
Belgia	√	√
Bulgaaria	√	√
Eesti	√	√
Hispaania	√	√
Holland	√	
Horvaatia		
Iirimaa		
Island	√	
Itaalia		√
Kreeka	√	
Küpros	√	
Leedu	√	√
Luksemburg	√	√
Läti	√	√
Malta		
Norra	√	
Poola		√
Portugal	√	
Prantsusmaa		
Rootsi	√	√
Rumeenia		√
Saksamaa	√	√
Slovakkia		√
Sloveenia		
Soome	√*	
Šveits		√
Taani		
Tšehhi		√
UK		
Ungari	√	√

*kasutatakse Eesti riigis kvalifitseeritud usaldusteenuse osutaja SK poolt pakutavate teenust.

4.2 Kvalifitseeritud usaldusteenuste osutajate arv

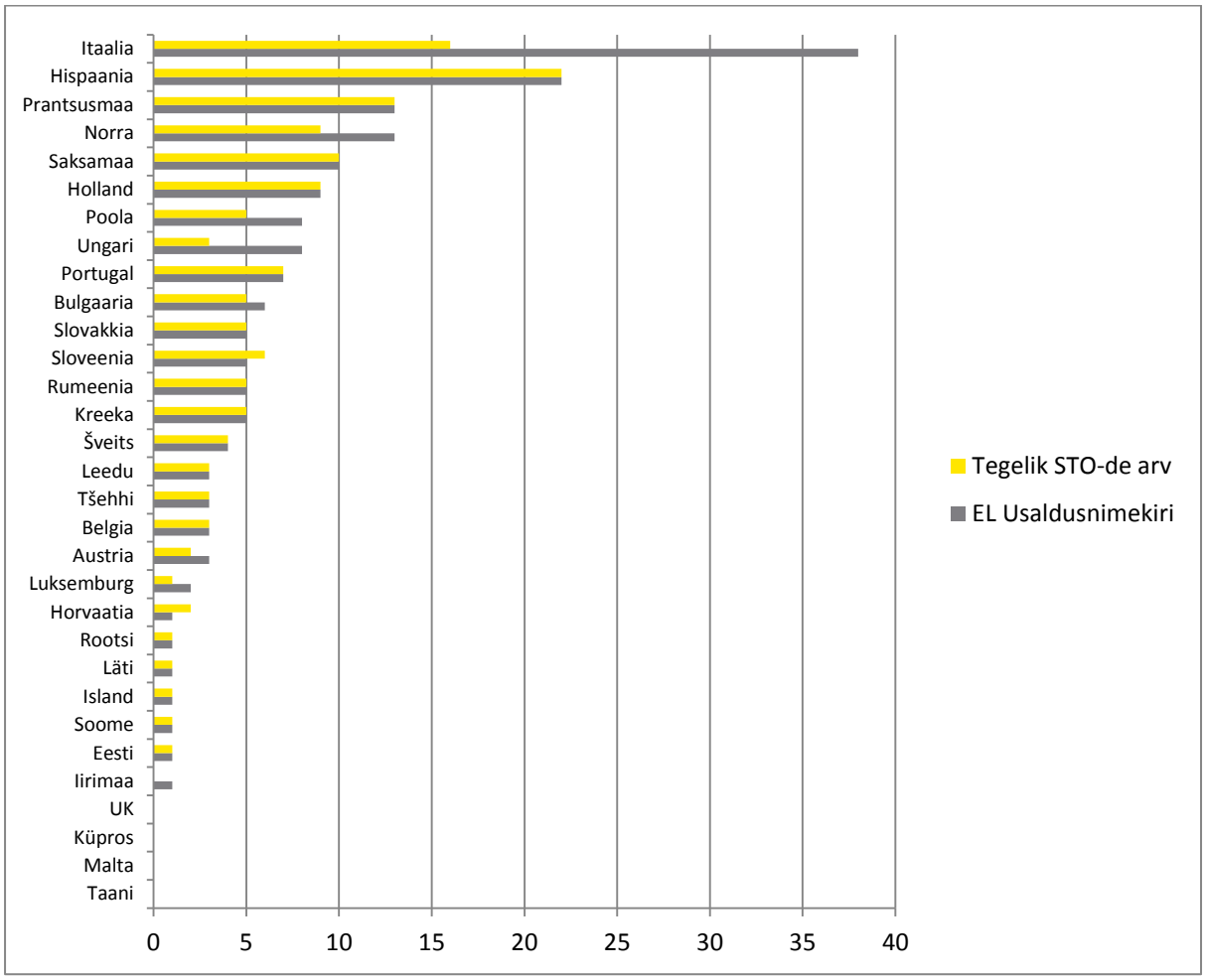
Iga Euroopa Liidu liikmesriik peab haldama kõigi riigis tegutsevate riikliku järelevalve all olevate sertifitseerimisteenuse osutajate (STO-de), kes väljastavad e-allkirjastamiseks kvalifitseeritud sertifikaate avalikuks kasutuseks, kohta nimekirja ning lisama need Euroopa Liidu Usaldusteenuste pakkujate Usaldusnimekirja. Nimekirja võib lisada ka sertifikaatide kehtivuskinnituse teenuseid, ajatempli teenuseid ning mitte-kvalifitseeritud sertifikaate pakkuvad STO-d, kuid see ei ole kohustuslik.

Järelevalvet tegeva asutuse roll riigiti on väga erinev. Näiteks kui Poolas, Leedus ja Itaalias kogub regulaator aktiivselt STO-delt informatsiooni välja antud ja kehtivate kvalifitseeritud sertifikaatide kohta, siis Saksamaal, Slovakkias ja Sloveenias selle kohta teadaolevalt infot ei koguta. Riikides, kus

on ainult üks STO, on regulaatori roll väike ning kehtivate kvalifitseeritud sertifikaatide arvu kohta nende poolt arvestust ei peeta.

Uuringu käigus selgus, et EL usaldusnimekirjas sisalduv informatsioon ei ole täies ulatuses ajakohane. Kui esialgsete EL Usaldusnimekirjade põhjal tuvastati 181 STO-d , siis uuringu käigus saadi kinnitus 143 STO tegutsemise kohta antud valdkonnas. Siiski ei saa olla kindel, et see on täpne number, sest kõikide riikide puhul ei õnnestunud järelevalvet tegevate asutuste käest küsimisega saada kinnitust kas EL usaldusnimekirjas olev STO-de arv vastab tegelikkusele. Käesolevas uuringus lähtuti STO-de arvu määramisel EL Usaldusnimekirjas olevast ja ka avalikes allikates kättesaadavast informatsioonist.

Kõige suurem erinevus Euroopa Usaldusnimekirja ja tegelike STO-de arvu osas oli Itaalial, kus EL usaldusnimekiri sisaldas 38 kvalifitseeritud usaldusteenuse osutajat, kuid teadaolevalt väljastavad kvalifitseeritud sertifikaate neist ainult 16. Väljatoodust vähem esines STO-sid veel näiteks Norras, Poolas, Ungaris, Austrias ja Bulgaarias (vt joonis 2). Siiski ei näita EL Usaldusnimekirja ebatäpsused seda kui tegus regulaator kohalikus riigis on.



Joonis 2 Kvalifitseeritud STO-de arv

Erinevuse põhilise põhjusena saab välja tuua asjaolu, et osad STO-d on lõpetanud kvalifitseeritud sertifikaatide väljaandmise, kuid EL usaldusnimekirja ei ole vastavalt uuendatud (kuigi järelevalvet tegevale asutusele on info teada). Näitena selgus uuringu käigus, et Luksemburgis ja Iirimaal lõpetab üks riigis tegutsev STO tegevuse. Ungari puhul on erinevuse põhjuseks suuresti lisaks tegevuse lõpetanud STO-dele veel asjaolu, et EL usaldusnimekirjas kajastub ka teenusepakkuja, kes väljastab mitte-kvalifitseeritud sertifikaate.

Esines ka riike, kus kvalifitseeritud sertifikaate avalikuks kasutamiseks väljastasid märgitust rohkem STO-sid. Sellisteks riikideks olid näiteks Sloveenia ja Horvaatia, kus mõlemal juhul on lisandunud uus kvalifitseeritud usaldusteenuse osutaja, kuid EL usaldusnimekirja ei ole uuendatud.

Neljas riigis (Malta, Küpros, Taani ja UK) kvalifitseeritud usaldusteenuse osutajaid ei eksisteerinud. Selle põhjal ei saa siiski väita, et riigis ei kasutata kvalifitseeritud sertifikaate digitaalseks allkirjastamiseks. Siiski ei ole teada Malta, Taani ja UK puhul, kas üldse ja kui palju nendes riikides kvalifitseeritud sertifikaate kasutatakse, sest järelevalvet tegevad asutused selle kohta infot ei omanud. Nii on näiteks Küprose puhul teada, et Kreekas väljastab kvalifitseeritud usaldusteenuse osutaja seal vähesel määral kvalifitseeritud sertifikaate.

4.3 Kehtivad kvalifitseeritud sertifikaadid e-allkirjastamiseks

E-allkirja kvalifitseeritud sertifikaat on eIDAS definitsiooni järgi e-allkirja sertifikaat, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab eIDAS määruse lisas I sätestatud nõuetele.

Kvalifitseeritud sertifikaat tõestab, et e-allkirjastamiseks antud privaatvõtit sisaldav e-allkirja andmise vahend on nimetatud konkreetse isiku ainukontrolli all. Kvalifitseeritud sertifikaate väljastatakse isikutele kas personaalseks või professionaalseks kasutuseks. Viimane tähendab seda, et kvalifitseeritud sertifikaat antakse organisatsiooni töötajale ametialaseks kasutamiseks. Näiteks, on levinud e-allkirjastamine notarite, juristide ja tervishoiutöötajate hulgas, kus tööalaselt tuleb anda palju e-allkirjasid. Sellisteks riikides on näiteks Prantsusmaa, Hispaania, Saksamaa, Poola ja Holland ning neid on veel.

Uuringu käigus uuriti kõikidelt kvalifitseeritud usaldusteenuse osutajatelt ning nende üle järelevalvet teostatavatelt asutustelt, kas on teada, kui palju on riigis kehtivaid kvalifitseeritud sertifikaate. Uuringu ülesandepüstituses oli küll küsitud väljaantud kvalifitseeritud sertifikaatide koguarvu, kuid projekti käigus leiti, et otstarbekas on vaatluse alla võtta eelkõige välja antud ja kehtivad sertifikaadid. Selle põhjuseks on asjaolu, et välja antud sertifikaatide arv on oluliselt suurem, kui kehtivate sertifikaatide arv ning viimane omab otsesemat seost kvalifitseeritud sertifikaatide kasutamisega e-allkirjastamiseks. Näitena võib tuua Poola, kus 2015. aasta veebruari seisuga oli kokku väljastatud kvalifitseeritud sertifikaate 1 093 065, samal ajal kui kehtivaid kvalifitseeritud sertifikaate oli ainult 318 182.

Kehtivate e-allkirja sertifikaatide arv näitab kui palju on riigis potentsiaalseid allkirjastajaid, st kui suur on inimeste hulk, kellel oleks soovi korral võimalik anda e-allkirja. Tabel 5 kirjeldab uuringu käigus kogutud kehtivate e-allkirjade kvalifitseeritud sertifikaatide arvu vaadeldavates riikides. Tabelis on välja toodud ka info selle kohta, kas kvalifitseeritud sertifikaate kasutatakse ainult e-allkirjastamiseks või tehakse sellega ka elektroonilist isikutuvastamist.

Enamikel juhtudel on tabelis 5 esitatud kvalifitseeritud e-allkirjastamise sertifikaatide arv subjektiivne ning põhineb uuringus osalenud riigi esindaja hinnangul. Seda, kas arv näitab ainult e-allkirjastamiseks mõeldud sertifikaate või sisaldub seal ka isikutuvastuseks või e-templite jaoks mõeldud kvalifitseeritud sertifikaatide arv, oli keeruline kindlaks teha. See sõltub suuresti riigi esindaja teadlikkusest, milleks kvalifitseeritud sertifikaate kasutatakse. Uuringus mainiti enamikel juhtudel, et kehtivad kvalifitseeritud sertifikaadid on kasutusel e-allkirjastamiseks. Ainukesena tõi Ungari välja fakti, et neil on väljastatud ligikaudu 20 000 kvalifitseeritud sertifikaati, kuid enamik neist on kasutusel e-templi andmiseks ning ainult mõni tuhat on kasutusel e-allkirjastamiseks. Tabelis toodud arvude puhul eeldame, et kvalifitseeritud usaldusteenuse osutajad või järelevalvet teostavate asutuste esindajad esitasid adekvaatselt kvalifitseeritud sertifikaatide arvu e-allkirjastamiseks.

Riikidesse, kus kvalifitseeritud sertifikaate kasutatakse lisaks e-allkirja andmisele veel elektrooniliseks isikutuvastuseks, tuleb suhtuda reserveeritult, sest see arv ei pruugi näidata e-allkirjastajate arvu. Võimalik, et kvalifitseeritud sertifikaadil põhinevat lahendust kasutatakse põhiliselt isikutuvastuseks.

Tabel 5 E-allkirja kvalifitseeritud sertifikaatide arv EL riikides

Riik	Kehtivate kvalifitseeritud sertifikaatide arv e- allkirja andmiseks	Kasutatakse ainult e-allkirja andmiseks	Kehtivate kvalifitseeritud sertifikaatide suhe riigi rahvaarvu (%)
Austria	710 000		8,4
Belgia	8 950 117	✓	79,3
Bulgaaria	153 897		2,1
Eesti	1 300 000	✓	98,8
Hispaania	-		-
Holland	442 000	✓	2,6
Horvaatia	221 400	✓	5,2
Iirimaa	30		-
Island	125 000	✓	38,5
Itaalia	8 104 615		13,3
Kreeka	-		-
Küpros	1 000		0,1
Leedu	900 000	✓	30,3
Luksemburg	400 000		80,6
Läti	130 000	✓	6,5
Malta	-		-
Norra	3 000 000		58,4
Poola	318 182		0,8
Portugal	-		-
Prantsusmaa	-		-
Rootsi	1 000		0,0
Rumeenia	200 000		1,0
Saksamaa	-	*	-
Slovakkia	-	✓	-
Sloveenia	-		-
Soome	900 000	✓	16,5
Šveits	75 000	✓	0,9
Taani	-		-
Tšehhi	-	✓	3,3
UK	-		-
Ungari	3 000	✓	0,0

*osa STOdest annavad välja eraldi sertifikaate.

Riikide rahvaarvu erinevuse tõttu toodi tabelis 5 välja kehtivate kvalifitseeritud sertifikaatide suhtarv riikide rahvaarvu. Kolmes riigis (Belgia, Luksemburg ja Eesti), kus suhe läheneb 100%-le, jagatakse kvalifitseeritud sertifikaate massiliselt, samal ajal kui paljudes teistes liikmesriikides peavad inimesed ise endale e-allkirja andmiseks vahendi koos sertifikaadiga soetama.

Riikides nagu näiteks Eesti, Belgia ja Luksemburg väljastatakse elanikele kvalifitseeritud sertifikaate koos riiklike ID-kaartidega. Seetõttu on kehtivate kvalifitseeritud sertifikaatide arv samas suurusjärgus tööealise elanikkonna arvuga. Enamikes riikides neid koos riikliku ID-kaardiga ei väljastata, kuid suund on sellele, et tekitatakse kvalifitseeritud sertifikaadi lisamise võimalus riiklikule ID-kaardile. Riiklikele ID-kaartidele on alustatud kvalifitseeritud sertifikaadi lisamist juba näiteks Horvaatias, Lätis ja Leedus. Riikides nagu Saksamaa, Sloveenia ja Itaalia on võimalik riiklikule ID-kaardile pärast kaardi kättesaamist lisada juurde kvalifitseeritud sertifikaat e-allkirjastamiseks.

Ehkki Maltal, Taanis ja UK-s ei ole kvalifitseeritud usaldusteenuse osutajaid, ei saa eeldada, et seal pole kvalifitseeritud sertifikaate kasutuses. Siiski ei õnnestunud uuringu käigus teada saada kas riigis üldse ja kui palju kvalifitseeritud sertifikaate väljastatakse. Eeldatavalt kasutatakse neis riikides vajadusel mõne teise Euroopa Liidu liikmesriigis kvalifitseeritud usaldusteenuse osutajate teenuseid.

Ka Küprosel ei ole registreeritud kvalifitseeritud usaldusteenuse osutajaid, kuid seal pakub teenust Kreekas kvalifitseeritud usaldusteenuse osutaja. Kuna teadaolevalt on Adacom ainus STO, kes seal teenust pakub, kasutati riigi kohta ülevaatliku hinnangu andmisel kasutuses olevate kvalifitseeritud sertifikaatide kohta.

4.4 Digiallkirja kasutamise osakaal

Uuringu eesmärgiks oli hinnata e-allkirjastamise taset EL 28 liikmesriigis ning Norras, Šveitsis ja Islandil. Lähtuvalt käesoleva uuringu ülesandepüstitusest käsitleti uuringus ainult kvalifitseeritud sertifikaadil põhinevaid täiustatud e-allkirjasid ning kvalifitseeritud e-allkirjasid.

Nagu käesolevas aruandes on eelpool täpsemalt selgitatud (vt. ptk **Error! Reference source not found.**), siis on tööealiste e-allkirjastajate arvu välja selgitamine keeruline, kuna sellekohaseid andmeid süstemaatiliselt ei koguta. Siiski on uuringus püütud e-allkirjastajate arvu võimalusel hinnata kaudsete meetoditega ja lähtudes andmetest, milleks enamikel juhtudel on kehtivate kvalifitseeritud e-allkirjastamise sertifikaatide arv. Uuringus kasutatud meetodid, nende tugevused ja nõrkused on pikemalt lahti seletatud peatükis 3.

Järgnevas tabelis on lühidalt välja toodud iga riigi kohta e-allkirjastajate arv ja selle suhe tööealisesse elanikkonda. Selgitusena on lisatud e-allkirjastajate arvu hindamise meetod ning andmeallikas, kust uuringu käigus riigi kohta põhiliselt informatsiooni saadi.

Algandmete allikateks olid peamiselt EL usaldusnimekirjas nimetatud kvalifitseeritud usaldusteenuse osutajate üle järelevalvet teostavad asutused (regulaatorid). Kvalifitseeritud usaldusteenuse osutajatelt saanud infot kasutati riigi e-allkirjastajate arvu leidmisel juhul, kui riigis oli ainult üks kvalifitseeritud usaldusteenuse osutaja, sest sellisel juhul oli võimalik saada riiki kattev info ühest kohast. eIDASe töögrupi liikmetega võeti ühendust juhul kui kvalifitseeritud usaldusteenuse osutajad ja regulaatorid ei vastanud.

Uuringu käigus selgus, et kvalifitseeritud e-allkirja andnud tööealiste elanike arvu on võimalik täpselt saada ainult Eestis ja Luksemburgis. Kui Eesti puhul on kehtivuskinnituse päringute põhjal täpselt teada, et 407 455 tööealist elanikku andis 2014.aastal vähemalt 1 digitaalse allkirja, siis Luksemburgis on saadud arv ligikaudne. Leidub ka teisi riike nagu näiteks Belgia ja Läti, kus tehakse kehtivuskinnituse päring allkirjastamise hetkel, kuid nende riikide puhul ei õnnestunud täpset e-allkirjastajate arvu teada saada. Üldiselt pakuti OCSP teenuseid ka teistes riikides, kuid allkirjastamise hetkel sertifikaadi kehtivuse kontroll sõltub suuresti e-allkirja keskkonna arendajatest ning sellest kuidas allkirjastamine on rakendatud.

Hinnangulise e-allkirjastajate arvu saime leida riikides, kus väljastatakse kvalifitseeritud sertifikaate kvalifitseeritud e-allkirja andmise vahendile ning seal on eeldatavalt elanikel sihipärane nõudlus e-allkirjastamiseks. Uuringus on võetud eelduseks, et kui riigis kvalifitseeritud sertifikaate elektroonilisele ID-kaardile vaikimisi ei väljastata ning inimene peab ise kvalifitseeritud sertifikaadil põhineva turvalise e-allkirja vahendi soetama, siis tõenäoliselt kõik vahendi soetanud isikutest ka kasutavad seda e-allkirjastamiseks. Riikide nagu Austria, Holland, Island ja Šveits puhul tugineti regulaatori või riigi eIDAS töögrupi liikme hinnangule. Siiski tuleb arvestada, et enamike riikide korral on e-allkirjastajate arv ja suhe tööealisesse elanikkonda hinnanguline ja ei pretendeeri statistiliselt usaldusväärsele tulemusele.

Ligi pooltes uuritud riikides ei olnud e-allkirjastajate arvu võimalik leida, kuna ainult sertifikaatide arvu põhjal ei olnud võimalik e-allkirjastamise kasutamise kohta hinnangut anda või ei olnud isegi informatsioon kehtivate sertifikaatide arvu kohta kättesaadav. Esimesse gruppi kuulusid enamasti sellised riigid, kus väljastatakse kvalifitseeritud sertifikaate riiklikule elektroonilisele ID-kaardile ning e-allkirjastajate osakaal oli teadmata. Selle tõttu ei ole näiteks e-allkirjastajate osakaalu hinnatud Belgia, Läti, Leedu ja Soome puhul.

Kehtivate sertifikaatide arvu väljaselgitamisel ei saadud piisavalt infot Hispaania, Prantsusmaa, Saksamaa, Portugali, Itaalia ja Kreeka puhul, kus uuringus osales ainult üks kvalifitseeritud usaldusteenuse osutaja, kellelt saadud kvalifitseeritud sertifikaatide arvu põhjal ei saanud e-allkirjastajate osakaalu hinnata peamiselt seetõttu, et riigis väljastasid kvalifitseeritud sertifikaate mitmed usaldusteenuse osutajaid, kellelt infot aga ei laekunud.

Uuritavast 31st riigist viies ei tegutsenud ühtegi kvalifitseeritud sertifitseerimisteenuse osutajat. Nendeks olid Iirimaa, Küpros, Malta, Taani ja UK. Neis riikides tegutsev regulaator ei omanud ülevaadet ka sellest, kui palju teiste Euroopa Liidu liikmeriikide STO-sid on riigis kvalifitseeritud sertifikaate e-allkirjastamiseks väljastanud. Iirimaal varasemalt tegutsenud STO lõpetas tegevuse, kuna riigis oli kvalifitseeritud sertifikaatide järele nõudlus väga väike – 2015. aasta oktoobris olid kehtivad ainult 30 kvalifitseeritud sertifikaati digitaalseks allkirjastamiseks. Taani on omamoodi näide selle kohta, kuidas riigis antakse palju e-allkirju, kuid need ei põhine kvalifitseeritud sertifikaadil.

Tabel 6. e-allkirjastamise näitajad ja kasutamise osakaalu hinnangud

SAADUD E-ALLKIRJASTAJATE ARV						
Riik	**Kehtivate kvalifitseeritud sertifikaatide arv e- allkirja andmiseks**	**E-allkirjastajate arv**	**e-allkirjastajate arvu hindamise meetod**	**Põhiline andmeallikas***	**E-allkirjastajate suhe tööealisse elanikkonda (%)**	**Täiendav info**
Eesti	1 300 000	407 455	Kehtivuskinnitu-se päringute arv	STO-d	46,6%	Allkirjastajate arv saadi e-allkirja sertifikaatide OCSP päringute statistika põhjal.
Luksemburg	400 000	87 000	Kehtivuskinnitu-se päringute arv	STO-d	23,6%	STO LuxTrust hinnangul ligikaudu 100 000 inimest andnud vähemalt 1 e-allkirja; Allkirjastajate arv korrigeeritud proportsionaalselt elanikkonna vanuselise struktuuriga;
HINNANGULINE E-ALLKIRJASTAJATE ARV:						
Island	125 000	80 000	Liiderkeskkond	STO-d	37,2%	80 000 QC kiipkaardil; 45 000 SIM kaardil; 12.2014-04.2015 riiklik kampaania e-allkirja andmiseks (80 000 e-allkirjastajat);
Austria	710 000	710 000	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	12,5%	550 000 QC serveripõhine lahendus; 160 000 QC kiipkaardil;
Holland	442 000	442 000	Sertifikaatide arv ja sihipärane nõudlus	eIDAS kontaktisik	4,0%	
Bulgaaria	153 897	153 897	Sertifikaatide arv ja sihipärane nõudlus	eIDAS kontaktisik	3,2%	47 657 QC eraisikutele; 101 934 QC juriidilise isiku esindajat; 4 306 QC ametialaseks kasutuseks; 3 251 QC erikasutus;
Horvaatia	221 400	80 000	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	2,8%	80 000 kehtivat QC ametialaseks kasutuseks; Juuni 2015 hakati välja andma QC riiklikule ID-kaardile;
Poola	318 182	318 182	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	1,2%	
Rumeenia	200 000	168 000	Sertifikaatide arv ja	Regulaator	1,2%	Allkirjastajate arv korrigeeritud proportsionaalselt elanikkonna vanuselise struktuuriga;

			sihipärane nõudlus			
Šveits	75 000	63 000	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	1,2%	E-allkirjastajate arvu korrigeeriti proportsioonis elanikkonna vanuselise struktuuriga.
Küpros	1 000	1 000	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	0,2%	QC-sid pakub Kreekas kvalifitseeritud STO;
Rootsi	<1 000	<1 000	Sertifikaatide arv ja sihipärane nõudlus	Regulaator	0,02%	QC kasutusel vähe, väga ulatuslikult kasutatakse mitte-QC põhinevaid e-allkirjastamise lahendusi;
Iirimaa	30	30	Sertifikaatide arv ja sihipärane nõudlus	STO-d	0%	Väike hulk kehtivaid QC-sid; Kohalik STO lõpetab QC-de väljastamise;
Ungari	3 000	3000	Sertide arv ja sihipärane nõudlus	Regulaator	0%	15 000 kehtivat QC-d väljastatud STO Microsec poolt; 2 162 kehtivat QC-d väljastatud STO NISZ poolt; Regulaatori sõnul ~20 000 QC-d kehtivat, kuid enamik neist on e-templid. Seega tabelis kajastub 3 000 QC e-allkirjastamiseks;
E-ALLKIRJASTAJATE ARVU EI SAA HINNATA:						
Belgia	8 950 117	-	-	Regulaator	-	~85 miljonit kehtivuskinnitus (OCSP) päringut kuus; 4 miljonit ajatempli päringut 2014.aastal;
Hispaania	-	-	-	-	-	20 000 kehtivat QC-d 1 STO ANCERTi poolt välja antud; Ülejäänud 21 STO-lt ei õnnestunud infot saada;
Itaalia	8 104 615	-	-	Regulaator	-	75% kehtivatest QC-dest kasutusel serveripõhise lahendusena; ~100 000 kehtivat QC välja antud 1 STO Lombardia Informatica S.p.A poolt; Ülejäänud 15 STO-lt ei õnnestunud infot saada; Regulaatorilt saadud QC arvu põhjal ei tea, kas kõik need on digitaalseks allkirjastamiseks või sisaldab number ka e-templite jaoks antud QC-sid;
Kreeka	-	-	-	STO-d	-	STO Adacom väljastab aastas ~3 000 QC-d; Ülejäänud 4-lt STO-lt ei õnnestunud infot saada;
Leedu	900 000	-	-	Regulaator	-	16 296 tööealist e-allkirjastajat, kus kasutatud Eesti STO SK QC mobiil-ID või SEB kaardil;

						769 129 e-ID kaarti (sh. ~14 000 avaliku teenistuja kaarti); 71 086 SIM-kaardid; 71 803 muud kaardid;
Läti	130 000	-	-	Regulaator	-	Juuli 2015.a väljastatud kokku 600 000 ID-kaarti, millest 130 000 kehtiva QC-ga;
Malta	-	-	-	-	-	Pole kvalifitseeritud STO-sid;
Norra	3 000 000	-	-	Regulaator	-	Bank-ID teenuse QC-d; Ei ole teada kui palju neist kasutatakse digitaalseks allkirjastamiseks;
Portugal	-	-	-	-	-	1 STO Digital Sign annab aastas välja ~15 000 QC; Ülejäänud 6 STO-lt ei õnnestunud infot saada;
Prantsusmaa	-	-	-	-	-	STO Caisse des Depots ~300 kehtivat QC;
Saksamaa	-	-	-	Regulaator	-	Regulaator ei kogu statistikat; Viimastel aastatel väljastatud ~100 000 QC aastas; 20 000 kehtivat QC väljastatud STO Bundesnotarkammeri poolt; 2 500 kehtivat QC väljastatud STO Datev eG poolt;
Slovakkia	-	-	-	Regulaator	-	~89 000 QC väljastati 2014.aastal;
Sloveenia	-	-	-	Regulaator	-	55 790 kehtivat QC väljastatud HAIcom-CA poolt; 199 843 kehtivat QC-d väljastatud siseministeeriumi poolt; 2013. aastal riigis tehtud uuringu järgi veidi rohkem kui10% täisealistest kodanikest omas QC.
Soome	900 000	-	-	STO-d	-	
Taani	-	-	-	Regulaator	-	Pole kvalifitseeritud STO-sid; Põhilised lahendused e-allkirjastamiseks kasutavad mitte-QC.
Tšehhi	-		-	Regulaator	-	~kuni 350 000 QCd väljastatakse aastas;
UK	-	-	-	Regulaator	-	Pole kvalifitseeritud STO-sid

„-„ andmed ei olnud usaldusväärsel viisil kättesaadavad või tuletatavad

5. Soovitused digitaalse allkirja kasutatavuse hindamiseks ja regulaarseks jälgimiseks

Käesoleva uuringu käigus tekkis läbiviijatel arusaam, et digitaalset allkirjastamist kasutavate isikute arvu ja selle osakaalu tööealise elanikkonna seas ei ole enamike riikide puhul otseste andmete põhjal võimalik määrata. Ainukesed riigid, kus selline informatsioon oli kättesaadav, olid Eesti, Island ja Luksemburg (andmete kogumise problemaatika on detailsemalt käsitletud peatükis 3.3).

Ülejäänud riikide puhul osutus piiratud osas kättesaadavaks ainult kehtivate kvalifitseeritud e-allkirjastamise sertifikaatide arv, kuid sageli jäi teadmata sertifikaatide tegeliku kasutuse iseloom ja ulatus digitaalseks allkirjastamiseks. Saadud andmete täpse tähenduse muutis raskesti tõlgendatavaks ka asjaolu, et arusaam digitaalse allkirjastamise mõistetest ei ole üheselt välja kujunenud. Näiteks esitati allkirjastamiseks mõeldud kvalifitseeritud sertifikaatide arvu asemel uuringu käigus infot väga erinevate sertifikaatide kohta – lisaks allkirjastamise sertifikaatidele esitati ka autentimiseks või e-tembeldamiseks mõeldud sertifikaatide arvud. Täpsustavatele küsimustele ei osatud sageli vastata.

Eeltoodust nähtub, et kuna riikide e-allkirjastamise praktika on sedavõrd erinev, siis on adekvaatse informatsiooni kogumine ja koondamine keeruline ja oleks kergemini teostatav kohaliku riigi regulaatori poolt, kellel on parem arusaam ja kontaktid kohaliku turu ja e-allkirjastamise praktikate kohta (täpsemalt on uuringu metoodilisi küsimus käsitletud peatükis 3.3).

Allpool on kirjeldatud põhimõtteid kuidas võiksid liikmesriigid e- allkirjastamise kasutust sõltuvalt teenuste ja infrastruktuuri hetkeolukorrast kas mõõta või hinnata.

5.1 Allkirjastajate arvu mõõtmine kvalifitseeritud allkirjade korral

Kvalifitseeritud e-allkirja moodustamisel on kohustuslik sellele lisada välise osapoole poolt antav ajatempel või –märgend. Seega oskab vastav teenuseosutaja kokku lugeda kõikide sellisel moel moodustatud allkirjade arvu (mitte allkirjastajate arvu). Kui allkirja moodustamisel lisatakse allkirjale ka sertifikaadi kehtivustõend OCSP vastuse näol, siis saab OCSP teenuse pakkuja arvet pidada ka individuaalsete allkirjastajate üle, sest sellised päringud teostatakse konkreetse isiku sertifikaadi kehtivuse kohta.

Seega on otsene allkirjastajate arvu mõõtmine võimalik vaid juhul, kui kvalifitseeritud e-allkirja moodustamist võimaldavad vahendid võtavad allkirjastaja sertifikaadi kehtivuskinnituse koheselt e-allkirja moodustamisel.

OCSP teenust pakuvad üldjuhul STO-d ise, lisaks on olemas ka OCSP vahendajaid. Vastavad teenusepakkujad peavad hakkama pidama arvet jagatud vastuste kohta sertifikaadiomanike lõikes.

5.2 Allkirjastajate arvu hindamine muude allkirjade korral

Mittekvalifitseeritud allkirjade puhul kui ajatemplit, ega –märgendit ei kasutata, puudub võimalus allkirjastajaid STO-delt kättesaadava info põhjal loendada. Sel juhul on siiski võimalik võtta aluseks sertifikaatide arv ja püüda selle alusel hinnata allkirjastajate arvu. Sellisel juhul on võimalik näiteks kasutada lisainformatsioonina väljastatud sertifikaatide kasutusala. Nagu käesoleva aruande metoodika peatükis on kirjeldatud, tuleks regulaatoril mitte-kvalifitseeritud e-allkirjade korral koguda informatsiooni nii kehtivate allkirjastamise sertifikaatide arvu kohta kui ka riigis levinud rakenduste ja keskkondade kohta.

Mittekvalifitseeritud allkirjade korral ei saa anda ranget valemit, kuidas allkirjastajate arvu leida, sest reaalne allkirjastamine on sertifikaatide arvust väiksem, kuid ei ole teada, kui palju väiksem. Sellisel juhul võib järgida järgmisi arutlusloogikaid:

- Nendel juhtudel, kui isikutele väljastatakse digitaalseks allkirjastamiseks mõeldud sertifikaadid ilma neile rahalist või administratiivset koormust tekitamata ja isikud ei ole sertifikaadi saamiseks ise jõupingutusi teinud, võib teha eelduse, et ainult suhteliselt väike osa sertifikaadi omanikest hakkab aktiivselt sertifikaadi abil allkirjastama. Sellist tüüpi olukorda iseloomustab näide, kus riiklikult on otsustatud hakata ulatuslikult välja andma elektroonilist ID kaarti koos e-allkirjastamise sertifikaadiga. Juhul kui sellisel kaardil on ka muu, näiteks isikut tõendava dokumendi otstarve, siis ei tarvitse e-allkirjastamise toimingud kujuneda kaardi oluliseks kasutusalaks. Sellistel juhtudel on sertifikaatide omanike seast allkirjastajate osakaalu hindamine võimalik näiteks küsitlusuuringu või ekspertarvamuse teel. Kui aga ID kaardiga digitaalse allkirja andmine on keskmisest oluliselt erinev mõningate kasutajagruppide puhul (firmaomanikud, juristid, meedikud jm), siis võib ühtlane küsitlusuuring anda eksitavaid andmeid ning selline võimalik sektoripõhine ebaühtlus tuleb võtta eelnevalt arvesse.
- Kui sertifikaadid väljastatakse isikutele nö vajaduspõhiselt ja otseselt digitaalseks allkirjastamiseks mõeldud sertifikaadi saamiseks tehakse ka kulutusi, siis võib eeldada, et selliste sertifikaatide kasutamine on aktiivsem, lähenedes sajale protsendile. Kuna ka sel juhul ei ole teada allkirjastajate täpne osakaal sertifikaatide omanikest, siis tuleks soovitavalt vaadelda sektoreid, kus allkirjastamise sertifikaate kasutatakse. Näiteks on mitmetes riikides levinud digitaalne allkirjastamine mõnes spetsiifilises sektoris, nagu tervishoid, avalik haldus, pangandus vms. Seega peaks regulaator tuvastama olulisemad digitaalse allkirjastamise valdkonnad ja kasutades valdkonnaekspertide arvamust allkirjastajate arvu hindamisel.

5.3 Usaldusteenuste osutajate poolne andmete esitamine

Selleks, et andmete koondamine toimuks süstemaatiliselt, on otstarbekas luua keskkond, kuhu usaldusteenuste osutajad (STO-d, ATO-d, KKTO-d) saaksid esitada statistilised andmed digitaalse allkirjastamise kohta. Nendelt kogutav informatsioon võiks hõlmata järgmist:

- Väljastatud sertifikaatide arv (näiteks kalendriaastas); väljastatud sertifikaatide arvu kaudu oleks võimalik jälgida aastate lõikes dünaamikat, mis annaks kaudset informatsiooni trendi osas;
- Kehtivate digitaalse allkirjastamise sertifikaatide arv (näiteks kalendriaasta lõpp); selle näitaja põhjal saaks hinnata kaudselt allkirjastajate arvu (eelpool kirjeldatud metoodika alusel);
- Antud digitaalsete allkirjade arv (juhul kui on võimalik arvutada ajatempli päringute alusel);
- Vähemalt ühe digitaalse allkirja andnud isikute arv (juhul kui on võimalik arvutada OCSP päringute alusel);

5.4 Organisatoorne korraldus

Riikide tegevust eelpool kirjeldatud viisil on otstarbekas teostada Euroopa Komisjoni (näiteks: DG DIGIT) poolsel koordineerimisel koostöös liikmesriikide järelevalveametitega.

5.5 Täiendavad alternatiivsed võimalused

- Digitaalse allkirjastamise eelduste hindamine

  Digitaalse allkirjastamise kasutatavuse hindamine käesoleva uuringuga sarnases kitsas ja ranges käsitluses (QES ja AES+QC) võimaldab saada kvaliteetsed uuringuandmed väga piiratud arvu riikide ja teenuseosutajate kohta. Põhjuseks on asjaolu, et enamik STO-sid ei tee statistikat või ei ole seotud allkirjastamise keskkondadega selleks, et teha statistikat digitaalseks allkirjastamiseks välja antavate sertifikaatide kasutamise kohta. Seetõttu tuleks kaaluda digitaalse allkirjastamise eelduste hindamist laiemalt ja mitte piirata uuringut ainult kvalifitseeritud e-allkirjade skeemidega. Näiteks võiks mõõta riigis väljastatud ja kehtivate e-ID kaartide arvu.

- Keskendumine avalikule sektorile

  Digitaalselt allkirjastajate arv on kõige täpsemini teada nende e-teenuste omanikel, kelle keskkonnas allkirjastamine toimub. Osa neist teenustest toimivad era-, osa aga avaliku sektori

poolel. Kuna erasektori osas on teenusosutajate osas ülevaade valdkonna mitte-reguleerituse tõttu puudulik ja ka aruandluskohustus puudub, siis perspektiivikamaks võimaluseks on alustada esialgu allkirjastajate kokku-lugemisega avalike teenuste raames, millistele on võimalik kehtestada aruandekohustus.

- Kokkuvõtvalt mõned soovitused andmete kogumise ja kasutatavuse edendamiseks:
  - Regulaarne andmete kogumine viia liikmesriigi tasandile – näiteks riigi järelevalve ameti või vastutava ministeeriumi juurde.
  - Anda STO-dele nendepoolsel andmete esitamisel neile tagasi agregeeritud informatsiooni nende turuosa kohta kogu sertifikaatide väljastajate turul, et nad saaksid mingit kasu sellest andmete esitamisest.
  - DG DIGIT (või on mingi sobivam organ) võiks koordineerida ja juhtida üle-Euroopaliselt andmete kogumist (vajadusel piloteerides väiksemas mahus andmetega valitud riikides);
  - Tõstatada eIDAS töögrupis terminoloogia ühtlustamise ja teadlikkuse tõstmise initsiatiiv.
  - Koguda andmeid ka mitte-kvalifitseeritud sertifikaatide ja allkirjade kasutamise aga ka teiste asjakohaste näitajate kohta, mis on eelduseks e-allkirjastamisele.
  - Hinnata iga-aastaselt digitaalse allkirjastamise skeemide potentsiaalsete kasutajate (väljastatud ja kehtivate sertifikaatide põhjal) arvu kaudu trendi, kuidas see näitaja muutub. Potentsiaalsete kasutajate arvu kasv näitab turu dünaamikat ja eriti juhul, kui sertifikaate ei väljastata automaatselt, siis ka huvi kasvu e-allkirjastamise teenuste kasutamise vastu.

6. Poliitikasoovitused digitaalse allkirja kasutamise edendamiseks

Digitaalse allkirjastamise üldine edendamine peaks toimuma mitmetasandiliselt. Ühest küljest peaksid liikmesriigid tegema jõupingutusi elanikkonnale digitaalse allkirjastamise tähenduse, võimaluste ja eeliste tutvustamisel, teisalt peaksid erialaringkonnad tegelema e-allkirjastamise tehniliste protsesside, kokkulepete ja regulatsioonidega.

Allpool on toodud välja uuringu käigus tekkinud ettepanekud selles osas.

6.1 Kvalifitseeritud e-allkiri on midagi enamat kui paberallkiri

Laialt on levinud teadmine, et (parimal juhul) on e-allkiri võrdne paberil antud allkirjaga.

Tõepoolest, igasugune e-allkiri, sh ka mitte-täiustatud ja mitte-kvalifitseeritud) aga ka näitleks nupu „nõustun" vajutamine, tuleb lugeda võrdväärseks paberallkirjaga, mis on antud tahteavaldusena, sidumaks allkirja andjat mingi informatsiooniga.

Kuigi on selge, et paberallkirja kaudu isiku ühene tuvastamine on põhimõtteliselt võimatu, kasutatakse võrdlevaid meetodeid allkirjastaja kindlaks tegemiseks lähtudes varem antud allkirjadest. Sellisel moel kasutatakse paberallkirja allkirja kui isiku biomeetrilist omadust – mille usaldusväärsus ei ole e-allkirjaga võrreldav.

Kvalifitseeritud e-allkiri aga võimaldab üheselt kindlaks teha allkirjastaja isiku, erinedes selle poolest kvalitatiivselt üksikust paberallkirjast. Seega on kvalifitseeritud e-allkiri midagi oluliselt enamat kui paberallkiri, sarnanedes rohkem „notariaalselt kinnitatud allkirjale". Säärane allkiri peab definitsiooni kohaselt olema aktsepteeritud igas situatsioonis võimaldades kolmandatel, tehinguvälistel osapooltel (näiteks kohtud), sellest ühemõtteliselt lähtuda.

E-allkirja selline käsitlus ei ole EL-s laialt teadvustatud. Ühelt poolt kindlasti saab väita, et sellise turvalisusega allkirja polegi igas situatsioonis (kus nõutakse paberallkirja) vaja. Samas on aga paratamatus, et must-valge digitaalmaailm ei tunne halle alasid ja e-allkiri kas on (kvalifitseeritud) või ei ole. Ja kui ei ole, siis saab allkirjastaja antud e-allkirjast alati taganeda sarnaselt nagu ka paberil antud allkirjast, vaatamata grafoloogide pingutustele.

Digitaalse allkirja kasutamise edendamiseks on oluline teadvustada laiemale üldsusele digitaalse allkirjastamise olemust ja selle eeliseid tavaallkirja ees. Tuleb rõhutada, et kvalifitseeritud allkiri on tavaallkirjaga samase õigusjõuga, annab sellele lisaks oluliselt tugevama kindluse isiku ja dokumendi seose vahel ning kehtib ka riigipiiride üleselt.

Sellise teavitustöö üheks võimaluseks on antud probleemi tõstatamine eIDAS töögrupis Eesti liikmete poolt ja erinevate tutvustavate meetmete (artiklid, koolitused, seminarid, juhendid, vms) kasutamine.

6.2 Kvalifitseeritud e-allkirja nõuete selgem defineerimine

eIDAS kui peamine digitaalse allkirjastamise alusdokument defineerib küll e-allkirjaga seotud põhimõisted, kuid mitmete oluliste põhimõtete definitsioon on antud kaudselt. Näiteks on ajamärgendi (ehk e-allkirja sidumine tema andmise ajaga) nõue esitatud kaudselt valideerimise kaudu, kus esmakordselt kirjeldatakse, et nõuetele vastav allkirjastamise sertifikaat peab kehtima allkirjastamise ajal.

Sündmuse toimumise aega ei ole aga usaldusväärselt võimalik fikseerida ilma kolmanda usaldatud osapoole (usaldusteenuse) abita. Kõige ilmsem teenus e-allkirja sidumiseks ajaga on ajatempliteenus. Samas Euroopa Komisjoni poolsetes selgitavates materjalides on ajatempliteenus enamasti leidnud käsitlemist täiesti eraldiseisva, e-allkirjast sõltumatu, teenusena.

Ajamärgendi andjaks saab lugeda ka OCSP teenust, mis tagastab päringu vastuses sertifikaadi kehtivuse kinnituse kõrval ka selle väljastamise usaldusväärse aja ning koos päringuga saadetud e-

allkirja unikaalselt identifitseeriva andmekogumi (signatuuri räsiväärtuse). Selline praktika on kasutusel Eestis, kus kaks kvalifitseeritud e-allkirja moodustamiseks vajalikku teenust (ajatempel ja OCSP) on ühendatud ühtsesse teenusesse.

Soovitus: kommunikeerida erinevatel tasanditel tõsiasja, et kvalifitseeritud e-allkirja moodustamise süsteem peab e-allkirja varustama ajatempliga või ajamärgendiga

6.3 Kehtivuskinnituse kohene lisamine kvalifitseeritud e-allkirjastamise moodustamisel

Kvalifitseeritud e-allkirja moodustamiseks osutatavad sertifitseerimisteenused võivad erineda muuhulgas selle poolest, kas sertifikaadi peatamine on eelseisund lõplikule tühistamisele (nagu enamuses EL riikides) või võib sertifikaadi peatatuse ka lõpetada (nagu Eestis), mille järel sertifikaat kehtib edasi nagu midagi poleks vahepeal juhtunud. Esmapilgul tühine nüanss on aga määrav kvalifitseeritud e-allkirja kehtivuse hindamise seisukohast.

Kui sertifikaadi peatamisele järgneb paratamatult selle tühistamine, kantakse tühistatud sertifikaat sertifikaatide tühistusnimekirja (CRL), mida STO levitab laialt oma teenuste, sh veebilehe kaudu. Kui valideerida e-allkirja, mis moodustati mingil (ajatembeldatud) ajahetkel minevikus, siis saab allkirjastaja sertifikaadi kehtivuse üle allkirjastamise ajahetkel otsustada puhtalt viimati STO poolt publitseeritud tühistusnimekirja järgi – kui allkirjastamise ajahetk langeb sertifikaadis märgitud kehtivusperioodi sisse ning kui vaadeldavat sertifikaati tühistusnimekirjas pole, siis saame selle lugeda kehtivaks. Juhul kui sertifikaat on hetkel kehtivas tühistusnimekirjas, siis tuleb täiendavalt kontrollida allkirjastamise hetkel kehtinud tühistusnimekirju. Kui nende järgi oli sertifikaat kehtiv, siis on ka allkiri kehtiv.

Tühistamisnimekirja kasutamisest toimub mingit jälge välisele teenuseosutajale maha ei jää. Tihti kasutatakse selliseks valideerimiseks ka OCSP teenust, sellisel juhul jääb OCSP teenuse pakkujale maha jälg igast (sama allkirja) valideerimisest.

Sertifikaadi peatamise lõpetamise teenuse olemasolul aga ülaltoodud loogikat kasutada ei saa. Juhul, kui kehtivuskinnituse teenusepakkuja ei paku mingit ebastandardset *ajaloolist* kehtivusteenust („kas sertifikaat X kehtis ajal Y"), on ainukene viis sertifikaadi kehtivuse tõestamiseks allkirjastamise hetkel kohene kehtivuskinnituse võtmine ning selle lisamine e-allkirjale.

Viimatinimetatud käitumismall võiks aga olla kasutusel igasugusel juhul – ühekordselt võetud kehtivuskinnitust saab korduval valideerimisel kasutada ilma täiendava välise teenuseta, tehes valideerimise lihtsaks ja ühemõtteliseks. Puudub vajadus hakata leiutama skeeme, mis masintöödeldaval kujul peegeldaksid sertifikaadi peatamise lõpetamise olemasolu (neid hetkel ei ole).

Soovitus: propageerida erinevatel tasanditel kvalifitseeritud e-allkirja koostamise viisi, kus e-allkirja moodustamise süsteem lisab e-allkirjale allkirjastaja sertifikaadi kehtivusinfo selle moodustamisel

6.4 Turvalise allkirjastamise vahendi väljastaja rolli selge eristamine

Turvalise allkirjastamise vahendi (edaspidi: *vahend*) all mõistame praktilistes rakendustes, mis põhinevad asümmeetrilisel krüptograafial, privaatvõtme loomist, säilitamist ja kasutamist võimaldavat süsteemi.

Euroopas hetkel kehtiv seadusandlus, aga ka eIDAS, eristab küll *vahendit* mõistena kuid paneb vastutuse selle nõuetele vastavuse kohta STO-le. Kuigi praktikas on see paljudel juhtudel aktsepteeritav (STO-d küsivad kiipkaardi tootjalt vastava sertifikaadi ja tegutsevad selle alusel), on see olemuslikult ebakorrektne. STO põhiülesanne on sertifikaadi väljaandmisel tagada, et mingi privaatvõti on just selle konkreetse omaniku valduses ning mille kohta STO väljastab omanikule vastava avaliku võtme tõendi ehk sertifikaadi. *Vahendi* enda kohta tema omadustele garantii andmine on aga mõnel juhul üsna keeruline (natuke sellekohaseid selgitusi tõime välja käesoleva punkti allpool olevas tekstis) ja on STO jaoks ülemäärane kohustus.

Markantseks näiteks on siin Austrias kasutatav mobiilset autentimist kasutav serveripõhine e-allkirjastamise süsteem, kus privaatvõtmeid säilitatakse serveris (tõenäoliselt turvamoodulis), mida ei halda või ei pruugi hallata sertifikaadi väljaandja. Sama situatsioon tekib pea igasuguses e-allkirjastamise süsteemis, kus *vahend* ja sellele vastav sertifikaat antakse välja rohkem kui ühe usaldust vajava osapoole poolt.

Soovitus: Seadusandluses tuua eraldi usaldusteenusena välja turvalise allkirjastamise vahendi väljastaja roll.

Vahendiga luuakse e-allkirjastamisel allkirja kõige olulisem osa – krüptograafiline signatuur, mis saadakse rakendades isikule kuuluvat privaatvõtit allkirjastatavale dokumendile (täpsemalt: selle krüptograafilisele sõnumilühendile). Siganatuuri moodustamiseks on vajalik „käivitada" privaatvõtme kasutamine, mille vahendajaks on tihtilugu mingi (mittesertifitseeritud) IT-komponent.

Nii näiteks mängib olulist rolli kiipkaardi kasutamise puhul selle juhtprogramm (draiver, tüürel). See võib olla kas eraldi paigaldatav tarkvara („PKCS#11 draiver") või siis täidab enamikku selle vajalikust funktsionaalsusest operatsioonisüsteem ise (näiteks Windows'i „minidraiveri" süsteem). Juhtprogrammi ülesandeks on muuhulgas küsida kasutajalt privaatvõtme kasutamiseks vajalikku PIN-koodi ja edastada see kaardile. Siit on lihtne järeldada, et pahatahtlik juhtprogramm ei pruugi kasutaja tahet arvestada ja võib toimetada privaatvõtmega oma (looja) äranägemise järgi.

Toodud suhteliselt tüüpiline kiipkaardi näide on vaid üks paljudest stsenaariumitest, kus e-allkirja moodustamisel osalevad lisaks privaatvõtme kandjale endale ka kolmandad, mittesertifitseeritud komponendid (näiteks PIN-koodi sisestust võimaldavad kiipkaardilugejad jms). Tegelikult määrab e-allkirja moodustamise turvalisuse ära lisaks privaatvõtme loomisele ja säilitamisele väga olulises osas ka privaatvõtme kasutamise turvatase.

Soovitus: Laiendada turvalise allkirja andmise vahendile esitatavaid nõudeid, käsitledes selle kasutamist kuni lõppkasutaja (ehk vahendi omaniku) tasemeni.

6.5 Kvalifitseeritud e-allkirja juurutamisest

Digitaalseks isikutuvastuseks (autentimiseks) vajalike komponentide hulk on suhteliselt väike ja lihtsalt käsitletav: näiteks vastava sertifikaadiga varustatud kiipkaart ja juhtprogramm arvutis; ülejäänu tagavad juba standardsed kiipkaardilugejad, brauserid ja veebiserverid. Parimal juhul kontrollitakse sertifikaadi kehtivust standardse tühistusnimekirja või OCSP teenuse abil. Seetõttu on näiteks ID-kaardi jagamine ja kasutamine autentimiseks laialt levinud.

Olukord on aga oluliselt komplitseeritum just e-allkirjastamisel kuna vajalikke komponente on oluliselt rohkem:

- turvaline allkirja andmise vahend (näiteks: kiipkaart, selle juhtprogramm pluss kiipkaardilugeja ja selle juhtprogramm);
- kvalifitseeritud sertifikaat;
- ajatempli- või ajamärgendi teenus;
- sertifikaadi kehtivuskinnituse teenus;
- e-allkirja andmise keskkond (-vahend), mis kasutab ülalnimetatud vahendeid ja teenuseid ning toodab standardse vorminguga e-allkirju;

Tänane ebamäärane e-allkirjastamise raamistik võimaldab ülalnimetatud komponente kasutada valikuliselt vastavalt e-allkirjastamise keskkonna looja soovile. Nii jäetakse näiteks võtmata nii ajatempel kui kehtivuskinnitus; e-allkiri moodustatakse vormingus, mida suudab käsitleda ainult keskkonna looja ise.

Kuna kvalifitseeritud e-allkirja tunneb ära tema koosseisu järgi, on määravaks tema vorming, mis peaks vastama kokkulepitud standarditele. Suur samm selles suunas on hiljuti defineeritud EN/ETSI

standardid *täiustatud* e-allkirjade ja nende kapseldusmeetodite baasprofiilide kohta (**AdES baseline profiles, AsiC baseline profile*, lisainfot leiab vastavatelt ETSI veebilehtedelt, näiteks *http://www.etsi.org/deliver/etsi_tr/119000_119099/119001/01.01.01_60/tr_119001v010101p.pdf*). Sellest tuleks edasi liikuda, defineerides üheselt kvalifitseeritud e-allkirja nõudeid kirjeldavad standardid.

Soovitus: tuua sisse mõiste „kvalifitseeritud e-allkirju käsitlev keskkond", millise nõuetele vastavust saab hinnata selle keskkonna võimekuse järgi käsitleda tehnilistes spetsifikatsioonides defineeritud kvalifitseeritud e-allkirja vorminguid.

Nii osutuks võimalikuks kvalifitseeritud e-allkirja võimaluste avamine laiale kasutajaskonnale, pakendades lisaks jagatavale ID-kaardile ja selle juhtprogrammile samasse komplekti ka ülalkirjeldatud e-allkirja vahendi (või viite sellele).