Lühendatud versioon

Digitaalallkirjade jätkusuutlikkuse analüüs

Uurimustöö

Redaktsioon: 1.0

19.04.2013

46 lk

Y-784-1

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti tuleviku heaks

Sisukord

1 Sissejuhatus

1.1 Töö eesmärk

Vastavalt Riigi Infosüsteemi Amet (RIA) ja Cybernetica AS 15. veebruaril 2013 sõlmitud lepingule teostas Cybernetica AS meeskond uurimustöö „Digitaalallkirjade jätkusuutlikkuse analüüs“. Töö eesmärgina plaaniti järgnevalt sõnastatud töid ja tulemeid.

Töö käigus Cybernetica

1) koostab Euroopa Liidus kasutusel olevate ning standarditavate allkirjavormingute loetelu;
2) hindab, millised vormingud lähiajal Euroopa Liidus laiemat kasutust leida võivad ning kirjeldab nende olulisi omadusi;
3) analüüsib nende vormingute Eestis kasutuselevõtu tehnilist keerukust;
4) analüüsib BDOC 2.0 allkirjavormingut, kirjeldab erinevusi aluseks võetud XAdES ja ASiC standarditest ning hindab pakutud vormingu optimaalsust;
5) analüüsib X-tee keskkonnas kasutamiseks sobivale digitaalallkirja vormingule esitatavaid lisanõudeid;
6) kirjeldab X-tee keskkonnas kasutamiseks sobivat allkirjavormingut;
7) teeb ettepaneku, kuidas aidata kasutajatel (asutustel ja kodanikel) digitaalallkirja korrektselt kasutada olukorras, kus lisandub erinevate omadustega allkirjavorminguid;
8) koostab plaani töökindla, paindliku, mitmeid erinevaid (k.a teiste riikide poolt defineeritud) digitaalallkirja vorminguid toetava digitaalallkirja tarkvara arendamiseks;
9) hindab X-tee turvaserverite riistvaraliste allkirjastamisvahenditega varustamise ja hooldamise maksumust;
10) kirjeldab X-tee turvaserveritele vajalike, digitaalallkirja seaduse nõuetele vastavate sertifitseerimis- ja ajatempliteenuste loomiseks, väljatöötamiseks ja haldamiseks vajalikke tegevusi ning hindab selleks vajaminevaid ressursse.

Kliendile antakse üle tehtud tööde aruanne, mis sisaldab

1) praegu Euroopa Liidus standarditavate ja kasutatavate oluliste allkirjavormingute loetelu koos nende omaduste kirjeldusega, k.a koos nende kasutuselevõtuks vajalike tehniliste tegevustega;
2) hinnangut BDOC 2.0 valiku optimaalsusele, BDOC 2.0 ja alusstandardite XAdES ja ASiC erinevuste kirjeldust;
3) X-tee keskkonnas kasutamiseks sobivale digitaalallkirja vormingule esitatavaid lisanõudeid;
4) ettepanekut X-tee keskkonnas kasutamiseks sobiliku digitaalallkirja vormingu osas;

5) plaani, kuidas korraldada kasutajate jaoks Eesti digitaalallkirja seaduse nõuetele vastavate ja turvaliste allkirjavormingute selge eristatavus mittevastavatest ja ebaturvalistest;
6) ettepanekut paljusid digitaalallkirja vorminguid jätkusuutlikult toetava digitaalallkirja tarkvara arenduse korraldamiseks;
7) hinnangut X-tee turvaserverite riistvaraliste allkirjastamisvahenditega varustamisele;

1.2 Taust

1.2.1 Projekti „Allkirjavormide turva ja jätkusuutlikkuse analüüs ja kasutusvõimaluste eeluuring“ lähteülesanne

Lähteülesande sisu on tellija poolt jagatud kaheks osaks: digiallkirjade jätkusuutlikkuse analüüs ja uuringud X-tee andmevahetuse tõestusväärtuse tugevdamiseks ja sõnumivahetuse standardiseerimiseks. Mõlemast osas kujunevad hiljem jätkuprojektid vajalikeks tarkvara arendusteks, vastavalt siis ID-kaardi baastarkvara ja X-tee tuumiktehnoloogia täiendusprojektid.

1.2.1.1 Digiallkirjade jätkusuutlikkuse analüüs

Seni on Eestis põhiliselt kasutatud üht digitaalallkirja vormingut – DDOC, millest on olemas mitmeid versioone. Vähem on pruugitud BDOC vormingut. Allkirjade loomiseks ja kontrollimiseks on eri aegadel kasutatud väga erinevaid programme. Enamus neist on loodud SK AS juhtimisel. Tarkvara on olnud kättesaadav lähtekoodi kujul. Paljud tarkvaraarendajad on loonud ka oma isiklike versioone sellest tarkvarast, millel on mingeid neile kasulike eriomadusi. Aastate jooksul on kasutusele võetud palju tarkvara, mida on päris kulukas uuendada. Tihti ei ole need programmid omavahel ühilduvad. SK AS on juhtinud uue vormingu – BDOC 2.0 väljatöötamist, mis on plaanis lähiajal ka kasutusse võtta.

Viimasel ajal on digitaalallkirjade praktilise rakendamise küsimused ka Euroopa Liidus teravalt päevakorda tõusnud. Tegevus toimub nii standardimise, seadusloome kui ka tehniliste lahenduste loomise osas.

Standardimise osas viiakse senist kogemust (ka Eesti oma) standarditesse. Tulemuseks peaks olema loodetavasti paremad digitaalallkirja vormingud, mille kasutamist tasuks ka meil kaaluda. Lisaks Eestis kasutatavale XAdES põhisele konteinervormingule on küllaltki populaarne ka allkirjade kapseldamine otse PDF dokumentide sisse. Erinevaid allkirjavorminguid ning viise olemasolevate standardite interpreteerimiseks on palju. Reaalse, jätkusuutliku ühilduvuse tagamine eri programmide vahel on tõsine väljakutse.

Töö käib ka Euroopa seadusandluse kallal, mis vastuvõtmise korral peaks Euroopa Liidus muutma kohustuslikuks teatud kindlate allkirjavormingute aktsepteerimise riigiasutuste poolt. Tõenäosus, et valitakse täpselt Eestis pruugitav allkirjavorming on väga väike. Vabalt võib olla, et kohustuslikuks muudetakse ka mitu vormingut. Eestis kasutatav allkirjavorming on ennast seni hästi tõestanud ja tehniliselt paljudest teistest parem. Seda oleks mõistlik edasi kasutada.

Kindlasti vajab käsitlemist ka allkirjade pikaajalise tõestusväärtuse temaatika. Eesti digitaalallkirjastamise algusaastatel kasutatud algoritmid ja võtmed on nõrgaks jäänud. Nende murdumine lähiaastatel on tõenäoline. Vaja on lahenduda vanade allkirjade tõestusväärtuse säilitamise küsimus. See võib tähendada veel ühe täiendava allkirjavormingu kasutuselevõtmist.

X-tee edasiarendamise plaanides on samuti täielikult digitaalallkirja seaduse nõuetele vastava digitaalallkirja juurutamine päringute allkirjastamiseks. X-tee esitab digitaalallkirja vormingule käideldavuse ning tootlikusega seotud nõuete täitmiseks täiendavaid nõudeid, mida ei ole aga mõistlik rakendada igapäevase digiallkirja juures. Seetõttu võib tekkida vajadus iseseisva allkirjavormingu järele, mida saaks aga siiski verifitseerida tavalise digitaalallkirja tarkvaraga.

Eelnevast tulenevalt on lähiajal ette näha vajadus luua kasutajatele võimalus mugavalt töötada väga erinevate digitaalallkirja vormingutega. Digitaalallkiri on Eesti riigi infosüsteemi üks nurgakive ning seetõttu peab RIA vajalikuks uurida

1) millised on potentsiaalselt toetamist vajavad vormingud;
2) mida nende vormingute toetamine tehniliselt kaasa toob (näiteks PDF digitaalallkirja vormingute toetamine eri operatsioonisüsteemide ning PDF tarkvarade juures);
3) kuidas aidata kasutajatel (nii kodanikel kui asutustel) digiallkirja korrektselt kasutada olukorras, kus erinevate omadustega allkirjavorminguid muudkui lisandub;
4) kas praegune plaan arendada XAdES ning ASiC standarditel baseeruvad BDOC 2.0 vormingut on parim võimalik;
5) kuidas korraldada töökindla, paindliku, mitmeid erinevaid (k.a. teiste riikide poolt defineeritud) digitaalallkirja vorminguid toetava digitaalallkirja tarkvara arendamine nii, et kasutajatel oleks kindlus loodavate ja aktsepteeritavate allkirjade õigusjõu osas.

Uuringu tulemus peab sisaldama:

1. Praegu Euroopa Liidus standarditavate ja kasutatavate oluliste allkirjavormingute loetelu koos nende omaduste kirjeldusega, k.a. koos nende kasutuselevõtuks vajalike tehniliste tegevustega.
2. Hinnangut BDOC 2.0 valiku optimaalsusele.
3. Plaani, kuidas korraldada kasutajate jaoks Eesti digitaalallkirja seaduse nõuetele vastavate ja turvaliste allkirjavormingute selge eristatavus mittevastavatest ja ebaturvalistest.
4. Ettepanekut paljusid digitaalallkirja vorminguid jätkusuutlikult toetava digitaalallkirja tarkvara arenduse korraldamiseks.

1.2.1.2 Uuringud X-tee andmevahetuse tõestusväärtuse tugevdamiseks ja sõnumivahetuse standardiseerimiseks

Tellitava uuringu eesmärk X-tee arendamise seisukohalt on selgitada välja, millised lahendused digiallkirjastamise tehnoloogias Eestis on järgnevaks mitmeaastaseks arendus-

perioodiks aluseks PKI rakendustel, et neid tehnoloogiaid kasutusele võtta signeeritud sõnumivahetuseks X-teel.

Esiteks on tõestusväärtuse tugevdamise teemalised nõuded X-teel tingitud mitme X-tee partneri seisukohast mitte aktsepteerida X-tee päringuvastuseid menetlusprotsessides ning nõuda X-tee kaudu saadud andmeid täiendavalt (digi)allkirjastatud kujul või siis lisada X-tee kaudu vahendatavatele andmetele täiendav digitempel. Sellega dubleeritakse X-tee funktsionaalsust.

Teiseks on sõnumivahetuse standardimise vajadus tingitud vajadusest viia X-tee turvaserverite vahel kasutatav protokoll samadele alustele digiallkirja lahendustes tänapäeval ja lähitulevikus kasutatavatele protokollidele (jälgides kõigis lahendustes Digiallkirja seaduse nõudeid), mis võimaldaks näiteks vahetult DigiDoc kliendiga käidelda X-tee sõnumeid.

Uuringu abil väljatöötatud lahendus peab vastama järgmistele nõuetele:

1. Turvaserveri poolt signeeritud sõnum peab olema Eesti ja EL seadusandlusele vastav (https://www.riigiteataja.ee/akt/694375), lihtsalt käsitsetav digitaalallkirjastatud dokument. Tuleb arvestada digitaalallkirja seaduse muutmise seaduse eelnõu projektiga (http://www.riso.ee/wiki/EID2011-04-08), kuna sellel on suur tõenäosus saada seaduseks.
2. Turvaserveri poolt signeeritud sõnum peab vastama vähemalt ühele Tööde kirjelduse A peatükis soovitatud digitaalsignatuuri standardile.
3. Kuna digitaalallkirja seaduses oleva turvalise allkirja andmise vahendi nõude täitmiseks peab turvaserveri allkirjastamisvõtmeid hoidma HSM-s või kiipkaardil, siis on vajalik turvaserverid vastavate seadmetega varustada. Anda hinnang, kui palju läheb maksma turvaserveritele vastava riistvara soetamine, paigaldamine, hooldamine ja uuendamine.
4. Turvaserverid moodustavad allkirju. X-tee keskus annab turvaserveritele selleks vajalikud sertifikaadid ning pakub ajatempliteenust. X-tee keskus on sertifitseerimis- ja ajatempliteenuse osutaja. Turvaserverite digiallkirjade õiguspärasuse kohta käivate vaidluste vältimiseks peab X-tee keskust saama registreerida sertifitseerimis- ja ajatempliteenuse osutajana. Alternatiiv oleks kasutada olemasoleva sertifitseerimisteenuse osutaja teenuseid. Anda eelhinnang sellise keskuse loomiseks, väljatöötamiseks ja haldamiseks vajaminevatest tegevustest ja ressurssidest.

1.3 Määratlused ja lühendid

AdES	Advanced Electronic Signature
ASiC	Associated Signature Containers
ASN.1	Abstract Syntax Notation One
ATO	Ajatempliteenuse osutaja
BDOC	digitaalallkirja vorming
CA	Certification Authority, sertifikaatide väljastamise süsteem
CAdES	CAdES CMS Advanced Electronic Signatures

CAdES-A	CAdES Archival Electronic Signature
CAdES-BES	CAdES Basic Electronic Signature
CAdES-C	CAdES Electronic Signature with Complete Validation Data References
CAdES-EPES	CAdES Explicit Policy-based Electronic Signatures
CAdES-T	CAdES Electronic Signature with Time
CAdES-X	CAdES EXtended Electronic Signature
CCID	Integrated Circuit(s) Cards Interface
CF	CompactFlash
CMS	Cryptographic Message Syntax
CPS	Certification Practice Statement, sertifitseerimispõhimõtted
CRL	Certificate Revocation List, tühistusloend
DAS	Digitaalallkirja seadus
Digidoc	allkirjavorming
DigiDocService	veebipõhine isikutuvastusteenus
EL	Euroopa Liit
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute
HSM	hardware security module, riistvaraline turvamoodul
H-tase	kõrgeim (high) turvaaste ISKE rakendusjuhendi järgi
IEC	International Electrotechnical Commission
ISKE	Infosüsteemide kolmeastmeline etalonturve
ISO	International Organisation for Standardisation
IT	infotehnoloogia
K3T3S3	turvaklass ISKE rakendusjuhendi järgi, kus K, T, S tähistavad käidelda-vuse, tervikluse ja salastatuse (konfidentsiaalsuse) osaklasse
Log	Logimissüsteem
MKM	Majandus- ja Kommunikatsiooniministeerium
OCSP	Online Certificate Status Protocol
ODF	Open Document Format
PAdES	PDF Advanced Electronic Signatures
PAdES Basic	Profile based on ISO 32000-1
PAdES Enhanced	PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles
PAdES for XML Content	Profiles for XAdES signatures of XML content in PDF

PAdES Long Term	PAdES-Long Term Validation Profile
PCI	Peripherial Component Interconnect
PDF	Portable Document Format
PKCS	public-key cryptography standards
PKI	Public Key Infrastructure, avaliku võtme infrastruktuur
RA	Registration Authority, Registreerimissüsteem
RFC	Request for Comments
RIA	Riigi Infosüsteemi Amet
Root CA	juursertifikaatide väljastamise süsteem
RPC	remote procedure call
RSA	public key algorithm
SDSB	Secure Distributed Service Bus, Turvaline hajutatud teenusevahendus-keskkond (X-tee uus versioon)
SK	AS Sertifitseerimiskeskus
SOAP	Simple Object Access Protocol
STO	sertifitseerimisteenuse osutaja
ZIP formaat	andmete pakkimise ja arhiveerimise formaat
TCP	Transmission Control Protocol
UCF	Universal Communication Format
XAdES	XML Advanced Electronic Signatures
XAdES-A	XAdES Archival electronic signatures
XAdES-BES	XAdES Basic electronic signature
XAdES-C	XAdES Electronic signature with complete validation data references
XAdES-EPES	XAdES Explicit policy electronic signatures
XAdES-T	XAdES Electronic signature with time
XAdES-X	XAdES Extended signatures with time forms
XAdES-X-L	XAdES Extended long electronic signatures with time
XML	Extensible Markup Language
XMLDSig	XML Signature
X-tee	riigi infosüsteemide andmevahetuskiht

2 Ülevaade allkirjavormingutest

Käesolev peatükk annab ülevaate olulisematest EL standarditavatest ja kasutusel olevatest allkirjavormingutest, kirjeldab nende olulisi omadusi, hindab nende elujõulisust EL-s ning nende Eestis kasutusele võtu tehnilist keerukust.

2.1 Euroopa Liidus standarditud allkirjavormingud

Digitaalallkirjade juriidiliseks lähtekohaks Euroopa Liidus on juba 1999. aastal vastu võetud direktiiv *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures* [1]. Direktiiv koos oma lisadega sätestab üldised nõuded allkirja andmise vahendile, sertifikaatidele jms. Muuhulgas määratakse ära täiustatud elektroonilise allkirja (*advanced electronic signature, AdES*) mõiste, millelt nõutakse, et

1) see oleks seotud ainuüksi allakirjutajaga;
2) selle abil oleks võimalik allakirjutajat tuvastada;
3) see loodaks vahendite abil, mis on ainuüksi allakirjutaja käsutuses, ja
4) see oleks liidetud nende andmetega, millele see viitab, nii et kõik hilisemad andmete muudatused oleks täheldatavad.

Küll aga ei määra see direktiiv ära konkreetseid vorminguid, milles allkirju esitada ning käsitleda.

Allkirjavormingute standardimisega tegeleb Euroopa Liidus peamiselt *European Telecommunications Standards Institute* (ETSI). ETSI poolt on standarditud järgmised olulisemad vormingud.

2.1.1 CAdES

Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), TS 101 733 [2]. Allkirjavormingu spetsifitseerimiseks kasutatakse krüptograafilist sõnumisüntaksit (*Cryptographic Message Syntax* (CMS)), mille omakorda spetsifitseerib IETF RFC 3852 [3]. Käesoleva kirjutamise ajal kehtib standardi TS 101 733 versioon 2.1.1; aprillis 2013 peaks hakkama kehtima ka versioon 2.1.2.

CAdES-e standard spetsifitseerib järgmised vormingud:

1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

2 http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.01.01_60/ts_101733v020101p.pdf

3 http://www.ietf.org/rfc/rfc3852.txt

- *CAdES Basic Electronic Signature (CAdES-BES)* – sisaldab allkirjastatud andmeid, kohustuslikke atribuute ja signatuuri;
- *CAdES Explicit Policy-based Electronic Signatures (CAdES-EPES)* – täiendab allkirjastatud andmeid viitega allkirjastamispoliitikale;
- *Electronic Signature with Time (CAdES-T)* – täiendab allkirjastatud andmeid ajatempliga;
- *Electronic Signature with Complete Validation Data References (CAdES-C)* -- täiendab allkirjastatud andmeid infoga, mis on vajalik allkirja kehtivuse kontrollimiseks (sertifikaadid, kehtivuskinnituse saamise meetodid (CRL, OCSP));
- *EXtended Electronic Signature (CAdES-X)* – võimaldab lisada CAdES-C vormingule mitmesugust signatuuri alla mitte jäävat infot, mis võib tulevikus osutuda kasulikuks allkirjastatud dokumendi kehtivuse kindlakstegemisel (mingil hetkel võetud kehtivuskinnitused või ajatemplid kogu allkirjastatud struktuurile või mõnele selle osale);
- *Archival Electronic Signature (CAdES-A)* – lisab CAdES-X vormingus konteinerile veel ühe üldise arhiiviajatempli.

Kuna CAdES on standardina väga üldine, on ETSI eraldi standardina TS 102 734 üllitanud profiilid erinevate rakendusstsenaariumite (e-arved, e-valitsuse rakendused jms) jaoks [4].

2.1.2 XAdES

Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), TS 101 903 [5]. Kui CAdES põhineb ASN.1 notatsiooni kasutaval krüptograafilisel sõnumisüntaksil, siis XAdES-vormingu eesmärk on saavutada sarnane funktsionaalsus kasutades XML-i. Aluseks on võetud IETF W3C standard *XML-Signature Core Syntax and Processing* (XMLDSIG)[6]. Standardist TS 101 903 kehtib alates detsembrist 2010 versioon 1.4.2.

XAdES-e standard spetsifitseerib järgmised vormingud:

- *Basic electronic signature (XAdES-BES)*;
- *Explicit policy electronic signatures (XAdES-EPES)*;
- *Electronic signature with time (XAdES-T)*;
- *Electronic signature with complete validation data references (XAdES-C)*;
- *Extended signatures with time forms (XAdES-X)*;
- *Extended long electronic signatures with time (XAdES-X-L)*;
- *Archival electronic signatures (XAdES-A)*.

4 http://www.etsi.org/deliver/etsi_ts/102700_102799/102734/01.01.01_60/ts_102734v010101p.pdf

5 http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf

6 http://www.w3.org/TR/xmldsig-core/

Oma funktsionaalsuselt on need vormingud samaväärsed CAdES-standardi vastavate vormingutega. Samamoodi nagu CAdES-standardi puhul, on ETSI lasknud välja eraldi standardi TS 103 171, mis kitsendab XAdESe korral kasutatavaid baasprofiile [7].

2.1.3 PAdES

Kõrvuti suvalises vormingus failide signeerimist toetavate CAdES- ja XAdES-standarditega on ETSI töötanud välja ka standardi PAdES, mis käsitleb kitsalt PDF-failide elektroonilist allkirjastamist. PAdES on teise taseme standard kui CAdES ja XAdES. PAdES kasutab CAdES ja XAdES allkirju PDF sisu allkirjastamiseks ja ei ole seega sõltumatu allkirjavorming. PAdES on oma olemuselt spetsiifiline konteinervorming.

ETSI standard TS 102 778 *Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES)* koosneb kuuest osast:

- *Part 1: PAdES Overview – a framework document for PAdES*[8]
- *Part 2: PAdES Basic – Profile based on ISO 32000-1*[9]
- *Part 3: PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles*[10]
- *Part 4: PAdES Long Term – PAdES-Long Term Validation Profile*[11]
- *Part 5: PAdES for XML Content – Profiles for XAdES signatures of XML content in PDF files*[12]
- *Part 6: Visual Representations of Electronic Signatures*[13]

Ka PAdESele on ETSI lasknud välja eraldi baasprofiilid standardis TS 103 172 [14].

7 http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

8 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

9 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf

10 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf

11 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf

12 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277805/01.01.02_60/ts_10277805v010102p.pdf

13 http://www.etsi.org/deliver/etsi_ts/102700_102799/10277806/01.01.01_60/ts_10277806v010101p.pdf

14 http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/01.01.01_60/ts_103172v010101p.pdf

PDF-dokumentidele on olnud võimalik elektroonilisi allkirju lisada juba rohkem kui 10 aastat[15]. PDF 1.7 vormingut spetsifitseeriv standard ISO 32000-1 (2008) *Document management - Portable document format - Part 1: PDF 1.7* [16] kasutas selleks algselt PKCS#7 vormingut [17], mis omakorda oli CMS-vormingu eelkäija.

Standardipere TS 102 778 eesmärk on spetsifitseerida erinevaid aspekte, mis esinevad digitaalallkirjade lisamisel PDF-dokumentidele. Võrreldes aluseks oleva ISO standardiga on parandatud ühilduvust CAdES- ja XAdES-vorminguga ning lisatud vahendid dokumentide tõestusväärtuse pikaajaliseks säilitamiseks [18].

PAdES käsitleb kitsalt vaid PDF-dokumente, ning ehkki teoreetiliselt saaks PDF konteinerisse kapseldada ka muid andmeid, ei ole selline vormingu mittesihipärane kasutamine ei efektiivne ega lihtne.

2.1.4 ASiC

CAdES- ja XAdES-standardid on ünsa paindlikud selles osas, kus paiknevad allkirjastatavad andmed. Andmed võivad sisalduda allkirja koosseisus või need võivad olla allkirjast eraldi ning allkirjas sisaldub neile vaid viide. CAdES ja XAdES allkirjavormingute rakendamisel kasutati allkirja ja allkirjastatud andmete sidumiseks väga erinevaid meetodeid. Näiteks Eestis seni kasutusel oleva ddoc-vormingu puhul [19] sisaldusid allkirjastatavad andmed XAdES allkirjas. Tulemuseks oli ebaefektiivne lahendus, mis suuremate failide korral töötlemiseks palju ressurssi nõuab.

Teine kasutatav lahendus on allkirja ning allkirjastatud failide pakendamine üheks failiks, kasutades ZIP failivormingut. See on palju efektiivsem meetod kui allkirjastatavate andmete lisamine vahetult XAdES struktuuri.

Praktilise koosvõime saavutamiseks lõi ETSI standardi TS 102 918 *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)* [20]. Sisuliselt on tegu OpenDocument-standardile vastava ZIP-konteineriga, millele ETSI standard TS 103 174 määrab ka baasprofiilid [21].

15 The AdES family of standards: CAdES, XAdES, and PAdES. http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf

16 http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf

17 http://tools.ietf.org/html/rfc2315

18 http://www.ascertia.com/blogs/ETSI_PAdES_-_explored_and_explained.aspx

19 http://www.id.ee/index.php?id=30289

20 http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.02.01_60/ts_102918v010201p.pdf

21 http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.01.01_60/ts_103174v020101p.pdf

2.2 Euroopa Liidus kasutusel olevad allkirjavormingud

Digitaalallkirjade kasutuselevõtt on Euroopas endiselt algusjärgus. Enamuses riikides ei ole laialt levinud digitaalallkirja kasutamise tava. Mõned riigid (sh Eesti) omavad pikaajalist digitaalallkirja kasutamise kogemust ja rakendavad hästi välja kujunenud allkirjavorminguid. Valdavalt on kasutusel ETSI poolt standardiseeritud vormingud, ennekõike XAdES-el põhinevad (näiteks Eesti [22], Läti [23], Leedu [24], Poola [2518] , Kreeka [26]), Oht, et peaks lähiajal peaks rakendama mõnd muud standardit tundub ETSI jõulist tegevust arvestades võrdlemisi väike.

2.3 Standardsete allkirjavormingute Eestis kasutusele-võtu perspektiivikuse ning tehnilise keerukuse hinnang

2.3.1 Allkirjavormingutele esitatavad üldised nõuded

Järgnevas analüüsis lähtume allkirjavormingutele esitatavatest nõuetest, mis on loetletud ETSI standardis SR 001 604 [27]. Selle lisa B.3 annab järgmise aspektide loetelu.

1. Signeeritavad andmevormingud – signatuuri andmevormingu valimisel tuleb arvestada, et potentsiaalselt võib olla signeerida erinevat tüüpi dokumente (PDF, pildifailid, struktuursed andmed, multimeedia jne).
2. Töövoog – signatuuri andmevorming peab vajadusel toetama mitme signatuuri lisamist nt järjestikku või paralleelselt.
3. Signeeritavate andmete ja signatuuri seos – signatuurivormingu valimisel tuleb arvestada, kuidas signatuur andmetele lisatakse (nt ühises konteineris või dokumendi enda sisse kapseldades).
4. Rühmsignatuurivõimekus – signatuurivorming peab vajadusel toetama paljude signatuuride andmist ühekorraga (nt riistvaralise turvamooduli abil).

22 http://id.ee/public/BDoc-2.0-est.pdf

23 https://www.eparaksts.lv/files/lvrtc_edoc_specification_v1_0.pdf

24 https://signa.mitsoft.lt/static/signa-web/webResources/docs/ADOC_specification_approved20090907_EN.pdf

25 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 listopada 2006 r. w sprawie sporządzania i doręczania pism w formie dokumentów elektronicznych, Dz. U. 2006 Nr 227 Poz. 1664.

26 http://www.eu-spocs.eu/index.php?option=com_processes&task=streamFile&id=18&fid=934

27 http://www.etsi.org/deliver/etsi_sr/001600_001699/001604/01.01.01_60/sr_001604v010101p.pdf

5. Aeg ja järjestus – signatuurivorming peab vajadusel toetama võimalust teha kindlaks, millises ajalises järjestuses on toimunud signatuuri kehtivuse seisukohast olulised sündmused (signeerimine, kehtivuskinnituse saamine, sertifikaati tühistamine jne).
6. Kogukond – signatuurivormingu valimisel tuleb arvestada selle kogukonna (nt riigi) traditsioone ning tehnilist võimekust, kus digitaalallkirju kasutama hakatakse.

2.3.2 Eesti kontekst

Erinevate standardsete vormingute kasutamise perspektiivikuse Eestis määrab suuresti kohalik kontekst. Seetõttu võtame selle konteksti olulisemad punktid siinkohal kokku.

Eestis allkirjastatakse väga erinevas vormingus faile (PDF, multimeedia, X-tee päringud ja vastused jne). Struktuursete andmete esitamiseks kasutatakse valdavalt XMLi.

Erinevatest võimalikest töövoogudest vajavad toetamist nii järjestikused (st üksteise alla jäävad) kui paralleelsed signatuurid.

Signatuuri seos dokumendiga peab olema võimalikult paindlik. See seos peab olema efektiivselt töödeldav ka suurte failitüüpide (nt multimeedia) korral.

Vajadus rühmsignatuuride järele kerkib Eesti kontekstis näiteks X-tee puhul, kus rohkearvulistest päringuvastustest motiveeritud nõuded võivad ületada tavalise kiipkaardi võimekuse.

Signatuuri kehtivust mõjutavate sündmuste ajalise järjestuse kindlakstegemiseks sätestab Digitaalallkirja seadus ajatempli nõude [28]. Seega peab kasutuselevõetav digitaalallkirjavorming toetama võimalust lisada allkirjale Eesti nõuetele vastav ajatempel.

2.3.3 Standardsete allkirjavormingute võrdlus

Järgnevas tabelis võrdleme kolme standardse signatuurivormingu vastavust esitatavatele nõuetele. Kuna PAdES on oma olemuselt CAdESest ja XAdESest erinev, kujutades enesest eraldiseisvat konteinervormingut, pole ta nendega otse võrreldav. Võrreldavuse tagamiseks lisame CAdESele ja XAdESele ka standardse konteinervormingu ASiC.

28 https://www.riigiteataja.ee/akt/694375

	CAdES+ASiC	**XAdES+ASiC**	**PAdES**
Andmevormingud	Sobivad kõik	Sobivad kõik	Ainult PDF
Töövoog	Võimaldab nii paralleelset kui järjestikku signeerimist	Võimaldab nii paralleelset kui järjestikku signeerimist	Võimaldab järjestikuseid, aga mitte paralleelseid signatuure
Seos signatuuriga	Signeeritava faili saab lisada ASiC konteinerisse	Signeeritava faili saab lisada ASiC konteinerisse	Signatuuri saab esitada ainult PDFi sisse kapseldades
Rühmsignatuurid	Vajab eraldi lahendust	Vajab eraldi lahendust	Ei toeta
Aeg ja järjestus	Toetab ajatempleid	Toetab ajatempleid	Toetab ajatempleid
Kogukond	ASN.1 on vananenud standard	XML on levinud standard	PDF on laialt kasutatav, kuid ei kata kõike

Tabelist näeme, et CAdES ja XAdES on oma funktsionaalsuselt paindlikumad kui PAdES, võimaldades signeerida suvalist tüüpi dokumente ning toetades erinevaid töövooge. Kuna on väga ebatõenäoline, et Eestis hakataks signeerima ainult PDF-vormingus dokumente, pole mõtet kaalude selle standardi toetamist primaarse digitaalallkirja vorminguna. Samuti tooks PAdESe kasutuselevõtt endaga kaasa vajaduse luua vastavad komponendid erinevate teenuste ja tarkvaratoodete jaoks. Seejuures tuleb arvestada, et paljud tooted, mida PDF-dokumentide loomiseks kasutatakse, on kommertsiaalsed ning nende riiklikul tasemel toetamine on nii õiguslikult küsitav kui tehniliselt keeruline. Kui EL toimuvate arengute tulemusel tekib vajadus piiriülese ühilduvuse tagamiseks PAdES vormingut toetada, siis peaks seda tegema võimalikult standardsel viisil. PAdES standardi keerukust arvestades ei ole mõtet seda ise realiseerima hakata, vaid kasutada mõnd, soovitatavalt vabavaralist, valmistoodet.

CAdES ja XAdES on muus osas nii oma funktsionaalsuselt kui ka paindlikkuselt sisuliselt samaväärsed, CAdESe kahjuks kõneleb aga tema tuginemine vanemale standardile ASN.1, mille toetamine vajalikul tasemel võib osutuda omaette väljakutseks. On ebaselge, kui suurt tehnilist jõupingutust nõuab olemasolevate ASN.1-teekide kohandamine Eesti vajadustele vastavaks ning see kujutab endast tarbetut riski. Kui pole mingit välistest nõuetest tulenevat vajadust toetada CAdES-standardit, siis soovitame seda käesolevaga mitte teha ning keskenduda edaspidistes arendustes XAdES-vormingule.

XAdES-e kasuks räägib ka lähiriikide suundumus ning kodumaine praktika. BDOC 2.0 arendusel on algusest peale tuginetud XAdES ja ASiC standarditele ning BDOC 2.0 vormingus allkirjad vastavad neile. Täpsemalt on seda vastavust analüüsitud peatükis 3.

Ühe suurema täitmata nõudmisena standardis SR 001 604 toodute seast võib välja tuua rühmsignatuuride toe. Seda teemat puudutame täpsemalt peatükis 4.

Standardsete allkirjavormingute Eestis kasutuselevõtu keerukusele anname hinnangu peatükis 6.

3 BDOC 2.0 standardikavandi analüüs

Peatüki eesmärk on analüüsida BDOC 2.0 digitaalallkirja vormingu standardikavandit ning anda hinnang plaanitava vormingu optimaalsusele lähtudes sealjuures aluseks võetud ETSI standarditest TS 101 903 (XAdES), TS 103 171 (XAdES põhiprofiil), TS 102 918 (ASiC) ja TS 103 174 (ASiC põhiprofiil).

Standardikavandi kohta võib teha järgmised väited:

- BDOC 2.0 on digitaalallkirja vorming, mis kitsendab XAdESe põhiprofiili ning spetsifitseerib ASiCul põhineva konteinervormingu allkirjastatud failide ja allkirjade kapseldamiseks.
- BDOC 2.0 on XAdES-allkirjale pikaajalise tõestusväärtuse andmiseks kasutatava OCSP *nonce*-laiendusel baseeruva kehtivuskinnituse protokolli spetsifikatsioon.
- BDOC 2.0 on allkirjastamispoliitika, mis sätestab eelpoolnimetatud kehtivuskinnituse protokolli kasutamise.

BDOC 2.0 spetsifitseerib nõuded eelkõige allkirjastatud dokumendi loojale. Kui lähtuda ühilduvusest XAdES-e põhiprofiiliga, siis peavad kooskõlalised valideerijad hakkama saama kõigi XAdESe elementidega.

Plaanitava vormingu optimaalsust saame hinnata vastates järgmistele küsimustele:

Tehniline optimaalsus: „Kas BDOC 2.0 vormingus digitaalallkiri on digitaalallkiri XAdES põhiprofiili ja ASiC põhiprofiili mõttes“. Vorming on optimaalne, kui vastus sellele küsimusele on „Jah“.

Sisuline optimaalsus: „Kas BDOC 2.0 poolt tehtavad kitsendused on mõistlikud?“ ja „Kas BDOC 2.0 poolt lisatav laiendus toob kaasa uusi ühilduvusprobleeme?“. Vorming on optimaalne, kui vastus esimesele küsimusele on „Jah“ ning vastus teisele küsimusele on „Ei“.

Vormiline optimaalsus: „Kas BDOC 2.0 standardikavand on selge ja üheselt mõistetav spetsifikatsioon?“ Vorming on optimaalne, kui vastus sellele küsimusele on „Jah“.

Täiendavalt analüüsime vormingu sobivust alternatiivsetes kontekstides nagu näiteks X-tee uusversioon SDSB või ajatempliteenuseosutaja Guardtime ajatemplid.

3.1 XAdES ja ASiC

3.1.1 XAdES ja XAdES põhiprofiil

W3C XMLDSIG defineerib reeglid XML formaadis digitaalallkirjade esitamiseks ja töötlemiseks. XAdES täiendab XMLDSIG spetsifikatsiooni defineerides uusi XML andmetüüpe, mille abil on võimalik luua pikaajalise tõestusväärtusega digitaalallkirju XML vormingus. XAdES spetsifitseerib neli digitaalallkirja vormingut ning nõudmised ühele või teisele vormingule vastamiseks.

XAdES'e poolt defineeritavateks vorminguteks on:

- XAdES-BES – digitaalallkiri moodustatakse vastavalt XMLDSIG spetsifikatsioonile, täiendavalt peab olema tagatud allkirjastamiseks kasutatud sertifikaadi allkirjastamine kas elemendi `xades:SigningCertificate` või elemendi `ds:KeyInfo` koosseisus.
- XAdES-EPES – vorming lähtub kas XMLDSIG vormingust või XAdES-BES vormingust, nõutud on `xades:SignaturePolicyIdentifier` elemendi kasutamine.
- XAdES-T – vorming kirjeldab digitaalallkirja koos allkirjastamise ajahetkega usaldusväärsest allikast. Vorming lähtub kas XAdES-BES vormingust või XAdES-EPES vormingust, kasutada on võimalik nii ajatembeldust kui ajamärgendust.
- XAdES-C – vorming lähtub XAdES-T vormingust ning kirjeldab digitaalallkirja, mis sisaldab viiteid kõigile allkirjastava sertifikaadi kontrollimiseks vajalikele sertifikaatidele ning tühistusinfole.

Täiendavalt kirjeldab XAdES vormingud XAdES-X, XAdES-X-L ning XAdES-A, mis kasutavad täiendavaid elemente pikaajalise tõestusväärtuse tagamiseks.

XAdES profiil kitsendab XAdES'e vormingute kasutusviise kirjeldades neli ühilduvustaset, mis võimaldavad tasemetele vastavatel rakendustel koos toimida. Profiili poolt defineeritavateks tasemeteks on:

- B – tase lähtub XAdES-BES ja XAdES-EPES vormingutest ning täpsustab XAdES'es defineeritud elementide kasutamist XMLDSIG allkirjas, täpsustab XMLDSIG elementide `ds:KeyInfo, ds:SignedInfo, ds:CanonicalizationMethod, ds:Reference ja ds:Transform` kasutamist ning XAdES'e elementide `xades:SigningCertificate, xades:SigningTime` ja `xades:DataObjectFormat` kasutamist. B-tasemel digitaalallkirja andmise aja kohta ei ole võimalik midagi väita.
- T – tase lähtub B-tasemest ning lisab allkirjale usaldatud osapoolelt saadud ajamärgi (määratlemata vormingus) või ajatempli (`xades:SignatureTimestamp`). mis võimaldab allkirja tekkimise hetke määratleda.
- LT – tase lähtub T-tasemest, välistab mitmete XAdES'e elementide kasutamise ning täpsustab elementide `xades:CertificateValues, xades:RevocationValues, xades:AttrAuthoritiesCertValues, xades:AttributeRevocationValue, and xadesv141:TimeStampValidationData` kasutamist. LT-tasemel digitaalallkirjaga kaasneb kogu allkirjastamisel kasutatud sertifikaadi kontrollimiseks vajalik info.
- LTA – tase lähtub LT-tasemest ning eeldab elementide `xades:ArchiveTimeStamp` või `xadesv141:ArchiveTimeStamp` kasutamist. LTA-tasemel digitaalallkiri on pikaajalise tõestusväärtusega.

3.1.2 ASiC ja ASiC põhiprofiil

XAdES spetsifitseerib digitaalallkirja vormingu ning andmete asukoha URI-mehhanismi kasutades. ASiC standard täiendab XAdES standardit spetsifitseerides konteinerformaadi digitaalallkirja(de) ja vajalike andmete seostatult talletamiseks ja töötlemiseks.

ASiC konteinerformaat baseerub ZIP formaadil. Lisaks XAdES digitaalallkirjadele toetatakse CAdES digitaalallkirju ning RFC3161 kohaseid ajatempleid. BDOC lähtub XAdES'e profiilist, seega peatume siin vaid XAdES'ega seonduval.

Suvaline ASiC konteiner sisaldab juurkataloogi ning META-INF alamkataloogi. META-INF kataloog sisaldab metainfot sisu kohta, muuhulgas digitaalallkirju. Standard spetsifitseerib kaks tüüpi ASiC konteinereid.

- ASiC-S ehk lihtne konteiner seostab ühe andmeobjekti ühe või enama allkirjaga, mis paiknevad ühes allkirjastruktuuris.
- ASiC-E ehk laiendatud konteiner võib sisaldada mitut andmeobjekti. Iga andmeobjekt võib olla allkirjastatud ühe või enama allkirja poolt, mis võivad paikneda erinevates allkirjastruktuurides.

Laiendatud konteiner on ühilduv OCF, UCF ja ODF andmevormingutega.

ASiC profiil täpsustab ASiC standardis kirjeldatud elementide kasutamist realiseerivate rakenduste vahelise ühilduvuse saavutamiseks. Profiil defineerib sarnaselt XAdES'ele tasemed B, T ja LT. LTA taset profiil ei defineeri.

3.2 Standardikavandi tehniline kooskõlalisus alusdokumentidega

BDOC 2.0 digitaalallkirjavorming lähtub XAdES ning ASiC standarditest ja nende põhiprofiilidest. BDOC 2.0 standardikavand ei defineeri ilmutatud kujul ja täpselt BDOC 2.0 vormingut, vaid kirjeldab vormingut üldjoontes, XAdES'ele ja ASiC'ule viidates. Lugedes standardikavandit ei ole alati võimalik üheselt mõista, millal esitatavad nõudmised lähtuvad täpselt alusdokumentidest ning millal tehakse täiendavaid kitsendusi. Selline esitamise viis sunnib algusest peale lugema kõrvuti ASiC'ut, XAdES't, nende profiile ning BDOC 2.0'i.

3.2.1 Ühilduvus standardiga ASiC

BDOC 2.0 standardikavand sätestab, et konteiner peab sisaldama faili mimetype, mis sisaldab stringi `application/vnd.etsi.asic-e+zip`. Siit järeldame, et BDOC 2.0 allkirjavorming peab olema kooskõlas ASiC-E andmevorminguga ning tulenevalt XAdES'e kasutamisest BDOC 2.0'is ka ASiC'u XAdES põhiprofiiliga. Kontrollime ASiC-E XAdES põhiprofiiliga ühildumise tingimuste täidetust. Lähtume nõudmiste numeratsioonist põhiprofiilis.

Nõudmine	**BDOC 2.0 vastavus**
Nõudmine 8.1, viitega ASiC klauslile 6.2.1. Andmete tüübi identifitseerimine.	Nõudmine on täielikult täidetud, kuna andmete tüübi identifitseerimiseks kasutatakse MIME tüüpi “application/vnd.etsi.asic-e+zip”.
Nõudmine 8.2, viitega ASiC klauslile 6.2.2. Allkirjastatud andmeobjekt konteineris.	Nõudmine on osaliselt täidetud. BDOC 2.0 jätab ilmutatud kujul nimetamata andmeobjektide miinimumhulga konteineris ning allkirjafailide laiendi („META-

	INF/*signatures*.xml“), muus osas lahknevusi ei ole.
Nõudmine 8.3.1, viitega ASiC klausli 6.2.2 punktile 2. Allkirjastatud andmeobjektide viitamine.	Nõudmine on osaliselt täidetud. BDOC 2.0 jätab ilmutatud kujul nimetamata allkirjafailide miinimumhulga konteineris, muus osas lahknevusi ei ole.
Nõudmine 8.3.2, viitega ASiC klausli 6.2.2 punktile 4b. META-INF kataloog ja manifest.xml	Nõudmine on osaliselt täidetud. BDOC 2.0 jätab ilmutatud kujul ütlemata, milline on kataloogi META-INF täpne sisu, muus osas lahknevusi ei ole.

Esitatud lahknevused ei ole põhimõttelised. BDOC 2.0 standardikavandis toodud näitefail on nendes punktides ASiC profiiliga kooskõlaline.

3.2.2 Ühilduvus standardiga XAdES

3.2.2.1 BDOC 2.0 põhiprofiil

BDOC 2.0 põhiprofiil põhineb standardikavandi väitel XAdES-BES vormingul (lk. 8) ja on määratletud XAdES klausliga 4.4.1. Täiendavalt defineerib standardikavand BDOC 2.0 jaoks elemendi SingaturePolicyIdentifier väärtuse ning nõuab selle kasutamist kohustusliku elemendina. Sellest tulenevalt lähtub BDOC 2.0 tegelikult XAdES-EPES vormingust ja on määratletud XAdES klausliga 4.4.2.

BDOC 2.0 standardikavand viitab tekstis XAdES profiili ühilduvustasemetele T ja LT. Kontrollime XAdES profiiliga ühildumise tingimuste täidetust lähtudes neist tasemetest. Lähtume nõudmiste numeratsioonist profiilis.

3.2.2.2 B-taseme ühilduvus

B-taseme ühilduvus on oluline, kuna iga järgmine ühilduvustase tugineb eelmisel.

Nõudmine	**BDOC 2.0 vastavus**
Nõudmine 6.1, viitega XAdES klauslile 6.3. Allkirja atribuutide kirjeldamine.	BDOC 2.0 standardikavand ei käsitle seda nõudmist täpselt, puudub selgus, kas kasutatakse atribuutide otsest (*direct incorporation*) või kaudset (*indirect incorporation*) kaasamist Esitatud näitefail vastab nõudmisele.
Nõudmine 6.2.1. Allkirjastamisel kasutatud sertifikaadi kaasamine.	Nõudmine on täielikult täidetud. Lisaks elemendile ds:KeyInfo kasutatakse elementi xades:SigningCertificate.
Nõudmine 6.2.2. ds:SignedInfo elemendi kanoniseerimine.	Nõudmine on täielikult täidetud. Spetsifitseeritakse kanoniseerimisalgoritmi "http://www.w3.org/2006/12/xml-c14n11" kasutamine.

Nõudmine 6.2.3. Elemendi ds:Reference profiil.	Nõudmine on täielikult täidetud.
Nõudmine 6.2.4. Elemendi ds:Reference teisendused.	Nõudmine on täielikult täidetud.
Nõudmine 6.3.1. Elemendi xades:SigningCertificate profiil.	BDOC 2.0 standardikavand ei käsitle seda nõudmist, esitatud näitefail vastab nõudmisele.
Nõudmine 6.3.2. Elemendi xades:SigningTime profiil.	Nõudmine on täielikult täidetud.
Nõudmine 6.3.3. Elemendi xades:DataObjectFormat profiil.	Nõudmine on täielikult täidetud.

3.2.2.3 T-taseme ja LT-taseme ühilduvus

XAdES profiiliga T-taseme ühilduvus eeldab B-taseme ühilduvust. Täiendavalt peab allkirjaga kaasnema usaldusteenuse pakkuja poolt loodud ajamärgend või ajatempel, mis võimaldab tõestada allkirja olemasolu teatud ajahetkel.

BDOC 2.0 profileerib xades:SignatureTimeStamp elementi ning teeb seda standardiga kooskõlaliselt.

BDOC 2.0 käsitleb ka LT-taseme ühilduvusega seotud elemente xades:CertificateValues ning xades:RevocationValues ning teeb seda korrektselt ja standardiga kooskõlas.

3.2.2.4 LTA-taseme ühilduvus

Nii XAdES, XAdES-profiil kui ka BDOC 2.0 standardikavand käsitlevad põgusalt pikaajalist tõestusväärtust. BDOC 2.0 võimaldab koostada LTA-tasemel ühilduvaid allkirju kasutades üleajatembeldamiseks XAdES klauslis 8.2.1 defineeritud meetodit. Alternatiivina kirjeldab BDOC 2.0 standardikavand teenusepakkuja poolset logimist, kus kõigist väljastatud vastustest säilitatakse jälg ning teenusepakkuja pakub avalikku liidest konkreetse kinnituse olemasolu kontrolliks. Pedantselt märgime, et puhtalt logimise teel pikaajalist tõestusväärtust tagades ei saa me rääkida LTA-taseme ühilduvusest vaid T- või LT-taseme ühilduvusest, kuna dokumendile ei lisata xades:ArchiveTimeStamp elementi.

3.3 Tehnilise idee põhjendatus

BDOC 2.0 standardikavandi poolt tehtavad kitsendused lähtuvad Eestis rakendatud parimatest praktikatest ning on mõistlikud, siiski on oluline viidata ohukohtadele seoses standardikavandi poolt tehtavate laiendustega.

3.3.1 OCSP põhine kehtivuskinnituste protokoll

Allkirjastamise ajahetke tõestamise põhilise meetodina spetsifitseerib BDOC 2.0 standardikavand OCSP protokolli *nonce*-laiendust (nonss) kasutava meetodi, mis seostab allkir-

jastatud andmed kehtivuskinnitusega ning kehtivuskinnituse andmise ajahetkega. Meetod on Eestis pikemat aega aktiivses kasutuses olnud, tema toimemehhanismi paikapidavusse usutakse ning meetodit ei ole kahtluse alla seatud. De facto standardi ametlik standardiseerimine/dokumenteerimine on vajalik samm. Standardikavandis on siiski mõningad küsitavused, mis eeldavad selgesõnalist vastust ning standardikavandi täpsustamist.

Esiteks – standardikavandist ei selgu, kas OCSP põhise kehtivuskinnituste protokolli kohta eksisteerib spetsifikatsioon, mis defineerib üheselt mõistetavalt kasutatavad andmevormingud ning algoritmid. Sellise spetsifikatsiooni puudumisel tuleb see spetsifikatsioon teha, sest vastasel juhul puudub informatsioon nii ühilduvate generaatorite, valideerijate kui sama protokolli rakendavate kehtivuskinnitusteenuste realiseerimiseks. Millisest andmestruktuurist räsi võetakse? Kuidas kodeeritakse räsiväärtus nonsis? Jätkub olukord, kus tegelik standard on olemas lähtekoodi kujul ning puudub võimalus lähtekoodi vastavust kontrollida.

Teiseks – standardikavand lahendab kehtivuskinnituse protokolli probleeme digitaalallkirja vormingu tasemel. Kriitika all on SigPolicyQualifier NonceAlgorithm element, mis on oluline informatsioon kehtivuskinnituste protokolli tasemel. Kuna antud protokoll on defineeritud OCSP protokolli laiendusena, siis oleks protokolli ülesehituse seisukohast mõistlik kaasata NonceAlgorithm juba OCSP protokolli tasemel kasutades nonssina näiteks järgmist ASN.1 andmestruktuuri:

```
TBSDocumentDigest  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     digest               BIT STRING
}
```

AlgorithmIdentifier on defineeritud RFCs 5280. NB! Tegemist on näitega, protokolli vajadused võivad nõuda täiendavaid välju, nt. versioneerimist, kuid kontseptuaalselt kokku kuuluv informatsioon on sellisel moel kapseldatud ühte kohta, mitte jagatud protokolli ja vormingu vahel. Protokolli ja vormingu eristamine võimaldab sama protokolli kasutada ka alternatiivsete standardiseeritud vormingute juures, praegune esitusviis sunnib kõigis kasutuskohtades laiendust NonceAlgorithm uuesti defineerima.

Kolmandaks – standardikavand võimaldab oma sõnastuses nii ajatemplite kui ajamärgendite kasutamist, kuid vormingust ei selgu, millisel moel teeb verifitseerija kindlaks, kas antud dokumendi näol on tegemist ajamärgendatud dokumendiga, ning millise URLi poole tuleb *time-marking authority* leidmiseks pöörduda. Kuidas käsitleda OCSP protokolli olukorras, kus dokumendile võetakse ajatempel? Kas sellisel juhul võimaldab standardikavand kasutada standardset OCSP'd? Kuidas teeb verifitseerija vahet olukordadel, kus on kasutatud kehtivuskinnituste protokolli standardse OCSP asemel?

Neljandaks – rangelt võttes ei ole OCSP põhine kehtivuskinnitus ei ajatempel ega ajamärk. Tegemist on mingi kolmanda viisiga dokumendi allkirjastamise ajahetke kinnitamiseks. XAdES spetsifikatsiooni ajamärgi definitsioon ütleb järgmist: “usaldatud teenuse poolt antud ajamärgil on samasugune efekt kui ajatemplil, kuid sellisel juhul ei lisata seda elektroonilisele allkirjale ning teenuseseosutaja kohustus on esitada nõudmisel tõend ajamärgi kohta.” OCSP kehtivuskinnitusteenuse vastus ilmselgelt lisatakse elektroonilisele all-

kirjale ning sellisel moel ei ole vajalik teenuseseosutaja kohustus esitada nõudmisel tõend ajamärgi kohta.

Neljas küsimus toob meid olulise sisulise küsimuseasetuse juurde. Kuidas interpreteerivad antud meetodiga ajamärgendatud digitaalallkirja verifitseerijad, mis ei ole teadlikud standardikavandis defineeritud märgendamismeetodist? Kas standardikavandit realiseeriv teenuseosutaja on kohustatud pakkuma neile liidest, mis võimaldab ajamärgendit nõuda? Kuidas lahendatakse võimalikud konfliktid OCSP vastuses sisalduva aja ning teenuseosutaja poolt edastatava aja vahel? Kas võime eeldada, et piisav ühilduvus saadakse tänu standardikavandis kohustuslikuks tehtud elemendile SignaturePolicyIdentifier, mida standardi XAdES klausli 4.4.2 järgi esinemise korral allkirja valideerimisel arvestada tuleb? Sellisel juhul peaks laiendust mittetundev verifitseerija lõpetama töö veateatega viidates tundmatule allkirjastamispoliitikale, mis oleks korrektne käitumine, ning välistaks erinevad arusaamised allkirjastamise ajahetkest. Kahjuks defineerib XAdES elemendi SignaturePolicyIdentifier töötlemist ühilduvate verifitseerijate poolt väga üldsõnaliselt.

OCSP põhise kehtivuskinnituste protokolli standardiseerimise idee on hoolimata tehtud kriitikast hea. Verifitseerijad kes tunnevad standardikavandis defineeritavat allkirjastamispoliitikat saavad aega verifitseerida, kuid XAdES põhiprofiiliga ühilduvad verifitseerijad, kes konkreetset poliitikat ei tunne, ei saa verifitseerida. Nende jaoks on dokumendi omadused kehvemad. Samas ei saa nad ka ajamärki kontrollida, sest kuna nad signeerimispoliitikat ei tunne, ei tea nad, kes on *time-marking auhority*. Kui võime eeldada, et kuna nad dokumenti täielikult verifitseerida ei suuda, siis nad seda ka ei kasuta, siis võime lugeda, et standardikavandi järgi loodud vorminguga dokumentide kasutamine on võimalik keskkonnas, kus suhtlevad osapooled poliitikat tunnevad – st Eestis. Suhtlemiseks rahvusvaheliselt, kus tuleb arvestada XAdES põhiprofiiliga ühilduvate verifitseerijatega, tuleb rakendada standardseid ajatempleid.

3.3.2 Pikaajaline tõestusväärtus

Standardikavand kirjeldab kahte meetodit pikaajalise tõestusväärtuse tagamiseks – teenuseosutaja poolset väljastatud kinnituste logimist ning talletaja poolset dokumendi üleajatembeldamist. Standardikavandit lugedes võib jääda ekslik mulje, et tegemist on samaväärsete meetoditega. Tegelikkuses on logimispõhine pikaajalise tõestusväärtuse tagamine kaitsetu räsifunktsioonide murdumise vastu ning kui standardikavand juba kirjeldab kahe meetodi erinevaid eelduseid ning sobivust erinevatesse kontekstidesse, siis tuleb ka sellele asjaolule tähelepanu juhtida. On tõsi, et üleajatembeldamine eeldab kliendipoolset aktiivsust ning olemasoleva ajatempli õigeaegset kindlustamist, kuid samas tagab see meetod allkirja kontrolliks vajaliku info kättesaadavuse ning dokumendi räsi uuenemise olukorras kus varem kasutatud räsifunktsioon on oluliselt nõrgenenud. Tõestusväärtuse tagamine logide põhjal lihtsustab talletamist, kuid eeldab logide kättesaadavust ning teenusepakkuja võimekust tagada logide terviklus ja usaldusväärsus.

Logide põhjal saab tõestusväärtust tagada ainult kasutatud räsifunktsiooni eluea vältel. Näiteks osatakse täna MD5 algoritmi kasutamise korral, lähtudes olemasolevatest andmetest ja räsist luua uued andmed, mis sama funktsiooniga räsimisel sama tulemuse annavad. Teisisõnu on rikutud MD5 räsifunktsiooni kollisioonikindluse omadus. Koostoimes allkirjastamisalgoritmi nõrgenemisega ajas võib tekkida olukord, kus selle räsifunktsiooni

alusel kehtivuskinnituse saanud allkirjastatud dokumendile võib kõrvale panna alternatiivse allkirjastatud dokumendi, mis räsides annab sama tulemuse. Kummale dokumendile anti kehtivuskinnitus? Kumb dokument kehtib? Sellist olukorda aitab vältida ainult dokumendi uuesti räsimine ja üleajatembeldamine kasutades mõnd uut ja turvalist räsifunktsiooni.

3.3.3 XAdESe kriitika ühilduvuse vaatenurgast

XAdES digitaalallkirja standard on samm ühildamaks erinevaid nägemusi digitaalallkirjast ning sellisena kasulik ja vajalik. Kahjuks on standardis mõned hallid alad, mis tekitavad potentsiaalseid ühilduvusprobleeme. Toome näitena välja ajamärgendamise ning allkirjastamispoliitikad, mis mõlemad on BDOC 2.0 standardikavandis intensiivset kasutamist leidnud.

Allkirjastamispoliitikate rakendamine on XAdES standardis alaspetsifitseeritud. Probleemi ei ole senikaua kuni allkirjastamispoliitika ei sekku XAdESe spetsiifikasse. Kui allkirjastamispoliitika viitab välistele asjaoludele (nt. sellises vormingus tohib allkirjastada ainult transaktsioone väärtusega kuni 1000 EUR), siis on verifitseerimine standardne ning lõpliku otsuse dokumendi sisu kohta teeb allkirjastamispoliitikast ja kontekstist lähtudes inimene või rakendus, kellele verifitseerija poolt antud verifitseerimistulemus on täiendavaks sisendiks. BDOC 2.0 standardikavand seevastu omistab allkirjastamispoliitika kaudu teatud standardsetele elementidele (OCSP vastus) senisest erineva tähenduse ning sisuliselt muudab allkirja verifitseerimise reegleid. Verifitseeriv tarkvara, mis ei ole sellest poliitikast teadlik, ei oska neid täiendavaid reegleid täita ning tekib olukord, kus allkirja kontrolliv inimene peab tegema täiendavat tööd veendumaks dokumendi tegelikus kehtivuses. Standardikavand ei eksi siin otseselt mitte ühegi reegli vastu, kuid vastamata küsimused on olemas.

Ajamärgendite kasutamine on XAdESes spetsifitseerimata – kui meil on dokument, millel puudub ajatempel, siis puudub meil võimalus veenduda, kas leidub teenuseosutaja, kes on nõus selle dokumendi kohta ajamärgendit väljastama. Ei ole teada ajamärgendi formaat, ega viisid erinevatest ajamärgendusmeetoditest teada andmiseks. Sellises olukorras on ajamärgendite kasutamine seotud ohtudega – näiteks kuidas toimida olukorras, kus dokumendile on võetud nii ajatempel kui eksisteerib ka ajamärgend mõnelt teenuseosutajalt?

3.4 Tehnilise idee vormistus – standardikavandi kvaliteet

BDOC 2.0 standardikavand kitsendab alusstandardite poolt pakutavaid võimalusi, kirjeldades alamhulga ehitusplokke, mille abil saame allkirjavormingu eraisiku ja firma vahel, kahe firma vahel, kodaniku ja riigiasutuse vahel suhtlemiseks. Eesmärgiks on ühilduvus.

Varasemate vormingute ajalugu näitab, et ühilduvuse saavutamine ei ole liiga kerge. Arendajapoolne vormingu vääritimõistmine võib viia tuhandete vormiliselt vigaste digitaalallkirjadeni. Teatud vormilised vead võivad rikkuda allkirja kehtivuse. Vääritimõistmisi ei saa välistada, kuid nende tekkimise tõenäosust saab vähendada ning siin saab omapoolse panuse anda ka standard. Kui tarkvara arendav programmeerija ei loe standardit, siis on standard ainult dokument riiulil ning jõustamine toimub läbi näidete ning standardile vas-

tavuse kontroll puudub. Selleks, et viia standard arendajani peab tema tekst olema arendajale kasulik – loetav ning üheselt mõistetav – „jah, niiviisi tuleb teha“, „ei, niiviisi ei tohi teha“, „mul on vabadus valida, kuidas teha“.

BDOC 2.0 standardikavand on lünklik – nt. kehtivuskinnituste protokoll ei ole spetsifitseeritud sellisel tasemel, et oleks võimalik realiseerida standardset verifitseerijat või generaatorit.

BDOC 2.0 standardikavand ei defineeri BDOC 2.0 vormingut ilmutatud kujul vaid kirjeldab seda XAdES'ele ja ASiC'ule viidates. Selline esitamise viis sunnib algusest peale lugema kõrvuti ASiC'ut, XAdES't, nende profiile ning BDOC 2.0'i. Eelpoolviidatud „nõuete osalised täitmised“ on seotud justnimelt asjaoluga, et vormingust aru saamiseks tuleb paratamatult lugeda emadokumente (Milline on kataloogi META-INF täpne sisu?). Selline lähenemine oleks aktsepteeritav, kui standardikavand oleks esitatud konkreetsete erinevustena aluseks olevatest profiilidest: „BDOC 2.0 vormingus digitaalallkiri on ASiC/XAdES EPES põhiprofiilile tuginev LT-taseme dokument, mis teeb järgmised kitsendused: ...“. Suur abi oleks juba struktuursetest illustratsioonidest nagu leiame nt. XAdES klausli 4.4.2 juurest. Praegu nõuab BDOC 2.0 ja XAdES erinevuste tuvastamine omajagu detektiivitööd.

Standardikavandiga ei kaasne vastavusteste, mis kirjeldaksid, kuidas toimub BDOC 2.0 vormingus allkirja verifitseeriva/genereeriva süsteemi standardile vastavuse kontroll. Standardikavand oma praegusel kujul sisaldab ühte näidet ühe allkirjaga dokumendist, kuid ka see näide on mõeldud inimesele lugemiseks, mitte tarkvarale kontrollimiseks.

Kui BDOC 2.0 standardiga kaasneks komplekt vastavusteste, mis käsitleksid nii positiivseid juhte kui veajuhte, siis oleks tarkvaraarendajatelt võimalik nõuda nende testide kasutamist oma süsteemide vastavuse kontrolliks ning kasutajatelt nõuda vaid testitud tarkvara kasutamist.

Kui süsteemide eluea jooksul ilmneksid vead, mida senised testid ei kata, siis oleks võimalik testkomplekte täiendada, aidates tagada seda, et tulevaste süsteemide arendajad samade rehade otsa ei astu.

3.5 Olemasolevate teenuste ja tarkvara kooskõla BDOC 2.0 vorminguga

Eestis on mitmeid osapooli, kes väljastavad digitaalallkirju ning tagavad erinevate mehhanismidega nende allkirjade tõestusväärtust. Vaatame alljärgnevalt, kuidas BDOC 2.0 vastab erinevate lahenduste vajadustele.

3.5.1 AS Sertifitseerimiskeskus

AS Sertifitseerimiskeskus on Eestis registreeritud sertifitseerimisteenuse ja ajatempliteenuse osutaja. Refereerime AS Sertifitseerimiskeskuse ajatembelduspõhimõtteid.

Sertifitseerimiskeskuse ajatempliteenus on vormistatud üldisema, nn. „kehtivuskinnituse“ teenusena. Kehtivuskinnituse teenuse abil on võimalik jagada infot nii sertifikaadi kehtivuse kohta kui ka kehtivuskinnituse väljastamise aja kohta. Osutatav teenus põhineb OCSP protokollil (RFC 2560) ning standardilaiendusel „nonss“ (nonce), mille algset tähendust täp-

sustatakse. Kui RFC 2560 kohaselt on tegemist on juhuslikult genereeritud baidijadaga, mis pannakse kaasa OCSP päringusse ning mis kaasatakse signeerituna OCSP vastusesse, siis Sertifitseerimiskeskuse OCSP teenus ei piira tehniliselt nonsi sisu ega pikkust ning seetõttu võib nonssi käsitleda kui digitaalselt allkirjastatud dokumenti või selle sõnumilühendit.

Nonsiga laiendatud OCSP päringut käsitletakse järgnevalt:

- klient saadab OCSP responderile allkirjastatud dokumendi (selle sõnumilühendi) ning vastava sertifikaadi, mille alusel ta selle dokumendi allkirjastas;
- OCSP responder väljastab digitaalselt allkirjastatud kinnituse semantikaga „hetkel, kui ma selle sertifikaadi alusel allkirjastatud dokumenti nägin, oli see sertifikaat kehtiv“

Signeeritud OCSP päringus sisaldub ka aeg, mistõttu saab OCSP kinnitust digitaalselt allkirjastatud dokumendile pidada vajalikuks ja piisavaks lisandiks selleks, et allkirjastatud ja OCSP kinnitusega varustatud dokumenti pidada kõigiti pädevaks Digitaalallkirja seaduse mõttes.

Vaatame AS Sertifitseerimiskeskuse ajatempliteenuse ja BDOC 2.0 standardikavandi kooskõlalisust.

BDOC 2.0 käsitleb ajamärgendamise mehhanismina modifitseeritud OCSP teenust. BDOC 2.0 kirjeldab AS Sertifitseerimiskeskuse OCSP teenuse laiendust ning toob BDOC 2.0 põhiprofiili kohustusliku elemendina sisse elemendi NonceAlgorithm, mis määrab modifitseeritud OCSP protokollis kasutatava nonsi arvutamiseks kasutatava krüptograafilise räsifunktsiooni. Sellisel moel on standardikavand AS Sertifitseerimiskeskuse teenusega kooskõlas.

3.5.2 GuardTime AS

GuardTime AS on Eestis registreeritud ajatempliteenuse osutaja.

GuardTime ajatempel on vormiliselt RFC 3161 kooskõlaline ajatempel. Sisuliselt baseerub GuardTime tehnoloogia Merkle'i puudel ning räsiahelate kontrollimisel. Ei ole ühtegi formaalset põhjust, miks GuardTime AS ajatemplid ei peaks BDOC 2.0 vormingusse sobima, probleemid on puhtalt praktilised nagu nt. verifitseerijapoolne oskus kontrollida ajatempliga kaasnevaid räsiahelaid ning konkreetselt Eestis motivatsioonipuudus tarbida GuardTime AS teenust olukorras, kus ainsa CA OCSP teenus juba väljastab ajatempliga samaväärse ajamärgendi.

3.5.3 Andmevahetuskiht X-tee

Riigi Infosüsteemi Ameti poolt hallatav X-tee on Eesti riigi põhilisi andmebaase ühendav andmevahetuskiht. Tegemist on tehnilise ja organisatsioonilise keskkonnaga, mis võimaldab asutustel/inimestel turvaliselt andmeid vahetada, samuti korraldada isikute juurdepääsu riigi andmekogudes säilitatavatele ja töödeldavatele andmetele. X-tees on mitmekülgne turvalahendus: autentimine, mitmetasemeline pääsuõiguste haldus, logide töötlemise süsteem, krüpteeritud ja ajatempliga varustatud andmeliiklus.

Käigusolev X-tee v5 infrastruktuur rakendab digitaalset allkirjastamist ning ajatembeldamist, kuid andmevormingud ei ole kooskõlalised olemasolevate digiallkirja vormingutega. Samuti ei saa rääkida X-tee v5 digitaalallkirjade ja BDOC 2.0 kooskõlalisusest.

Tehnoloogiaarenduskeskuses Eliko on Riigi Infosüsteemi Ameti, Eesti E-tervise Sihtasutuse ja Cybernetica AS koostöös väljatöötamisel kaasajastatud versioon X-tee andmevahetuskihist – SDSB. Uusversioon lähtub digitaalallkirjade ning ajatemplite käsitlemisel ASiC ja XAdES standarditest ning väldib teadlikult mitte-standardseid lahendusi. SDSB on tulevikus plaanitud asendama X-tee v5 taristut, sellest tulenevalt tõstatub küsimus, kas SDSB digitaalallkirjad ning ajatemplid peaksid olema kooskõlas digitaalallkirja vormingu standardiga BDOC 2.0.

Takistusi SDSB allkirjavormingu ja BDOC 2.0 allkirjavormingu mitte-kooskõlalisusele on kolm – SDSB pakksignatuurid, allkirja ajatembeldamine ning OCSP. Neist ajatembeldamise küsimus on põhimõtteline probleem. Kuigi mõlemad vormingud lähtuvad ASiC ja XAdES standarditest profileerivad nad neid erinevalt.

SDSB digitaalallkiri on tehniliselt vastav BDOC 2.0 põhiprofiilile. Sisuline erinevus on selles, et SDSB allkirjastab dokumendi räsi asemel pakksignatuuri andmiseks arvutatud Merkle'i puu tipu. Allkirja naiivne kontroll veendub selles, et Merkle'i puu tipp on korrektselt allkirjastatud. Veendumaks dokumendi korrektses allkirjastatuses tuleb lisaks Merkle'i puu tipu allkirjale verifitseerida ka dokumendi räsist puu tippu viivat räsiahelat. Selleks lisab SDSB ASiC konteinerisse lisaks Merkle'i puu tipule räsiahela ning konkreetse dokumendi. Vastavuse sisuliseks loomiseks tuleks täiendada standardikavandi poolt toetatavaid allkirjastamispoliitikaid.

BDOC 2.0 standardikavand oma praeguses esituses jätab spetsifitseerimata modifitseeritud OCSP protokolli abil saadud ja standardse OCSP protokolli abil saadud kehtivuskinnituste eristamise. SDSB näeb ette standardse OCSP, mis ei omista võimalikule nonsile eritähendust, kasutamise kehtivusteenusena.

BDOC 2.0 käsitleb ajatembeldamist standardi XAdES poolt määratud raamides. SDSB kasutab allkirjade pikaajalise tõestusväärtuse tagamiseks samuti ajatembeldust, kuid rakendab dokumendi ajatembeldamiseks ASiC-E Timestamp token konteinerivormingut. Sellest tulenevalt ei ole vormingud BDOC 2.0 ja SDSB omavahel ühilduvad.

3.6 Kokkuvõte

Anname hinnangu BDOC 2.0 standardikavandi optimaalsusele.

Tehniline optimaalsus: Võib öelda, et BDOC 2.0 vormingus digitaalallkiri on üldjuhul ASiC ja XAdES põhiprofiilide LT-taseme allkiri, mis lähtub XAdES EPES-profiilist ning on tehniliselt kooskõlaline alusdokumentidega.

Sisuline optimaalsus: Võib öelda, et BDOC 2.0 poolt tehtavad kitsendused on mõistlikud, kuid alusdokumente laiendav OCSP põhine kehtivuskinnituste protokoll ning selle kasutamine on spetsifitseeritult selliselt, et mõned küsimused jäävad lahtiseks:

- Puudub kehtivuskinnituste protokolli spetsifikatsioon.
- Laiendus NonceAlgorithm sellisel kujul on ebamõistlik.

- Vajalik on standardikavandi autori poolne hinnang esitatud küsimustele seoses ajamärgendite ja allkirjastamispoliitikatega.
- Vajalik on täpsustada pikaajalise tõestusväärtuse eeldusi standardikavandis.

Hinnang optimaalsusele sõltub vastustest.

Vormiline optimaalsus: Standardikavand ei ole vormiliselt optimaalne. Olukorra parandamiseks soovitame:

- Sõnastada täpselt, kui mitut erinevat liiki digitaalallkirjastatud dokumente võimaldab standard vormindada ning millistele XAdES ja ASiC tasemetele need vastavad. Esitada vormingud erinevuste kaudu alusdokumentidest. Näiteks võiks ASiC teemalise peatüki sisuliselt asendada lausega: kasutatakse ASiC põhiprofiilile vastavat ASiC-E XAdES-tüüpi konteinerit, faililaiendiks on 'bdoc'. Rohkem uut informatsiooni võrreldes emadokumendiga standardikavandis ei ole.
- Varustada andmetüübid ning algoritmid vastavustestide komplektiga.
- Parandamaks loetavust visualiseerida BDOC 2.0 dokumendi ja allkirja struktuure XAdES standardi jooniste näitel.

Olemasolevate teenuste ja tarkvara kooskõlalisus: Analüüsitud teenusepakkujatest vastas standardikavand AS Sertifitseerimiskesus vajadustele ning ei vastanud SDSB andmevahetuskihi vajadustele. GuardTime AS ajatempel mahub BDOC 2.0 vormingusse, kuid eelmises punktis viidatud küsitavus seoses OCSP protokollilaienduse kohustuslikkusega tuleks lõpliku positiivse hinnangu andmiseks lahendada.

De facto mehhanismi standardiseerimine on antud juhul kasulik ja vajalik. Kõrvutamine nt. SDSB digitaalallkirjadega viitab, et üsna varsti on olemas vajadus järgmise standardiseeritud digitaalallkirja vormingu järele. SDSB ning BDOC 2.0 vormingus digitaalallkirjade andmine toimub erinevates kontekstides, ning kui soovime standardi abil muidu üsna paindlikke ASiC ja XAdES vorminguid parema ühilduvuse huvides kitsendada, siis on BDOC 2.0 printsiibis igati asjakohane kavand.

4 Digiallkirja rakendamine X-tee süsteemis

4.1 X-tee keskkonnas kasutamiseks sobivale digitaalallkirja vormingule esitatavaid lisanõudeid

X-tee2 visioonis on nõutud turvalisele digitaalallkirja andmise vahendit. Sisuliselt on olemas kaks põhimõtteliselt erinevat lahendust sellise vahendi realiseerimiseks.

- Riistvaraline turvamoodul (*hardware security module*, *HSM*) – suure jõudlusega ja turvaline, aga väga kulukas (suurusjärgus paarkümmend tuhat eurot), mis teeb selle juurutamise paljudes väiksemates asutustes majanduslikult ebamõistlikuks.
- Kiipkaardipõhine turvamoodul (kiipkaart või integreeritud USB seade) – hinnalt mitu suurusjärku HSMist odavam, kuid oluliselt väiksema jõudlusega (ca 2-3 signatuuri sekundis).

Samas on X-tee päringute maht aasta-aastalt kasvanud, ulatudes kuni miljoni päringuni päevas ning ca 240 miljoni päringuni aastas [29]. Niisiis on tekkinud vajadus toetada võimalust anda ühe signatuurioperatsiooniga allkiri paljudele dokumentidele korraga, et ka väiksema jõudlusega turvamoodulid suudaksid teenindada suurt arvu päringuid.

Teine lahendamist vajav probleem kerkib üles seoses X-tee ajatempliteenusega. Kuna kõik päringud ja nende vastused ajatembeldatakse, peab ajatempliteenus tegema sama suure hulga tööd kui kogu ülejäänud X-tee kokku. Isegi juhul, kui kasutada ainult krüptograafiliselt odavaid operatsioone (näiteks räsimist), pole see X-tee päringute kiiresti kasvanud mahtu arvestades reaalne. Kuna ajatempliteenus nõuab ka võrgusuhtlust, tekitab iga päringut ja vastust eraldi ajatembeldav lahendus tarbetu käideldavusriski.

Kolmandaks kitsaskohaks on OCSP-kehtivuskinnituste võtmine. Sarnaselt ajatemplitega nõuavad need võrgusuhtlust ning ka OCSP server peaks tegema sama palju tööd, kui kõik turvaserverid kokku. Ka see ei tule tänaseid X-tee mahtusid arvestades kõne alla.

Neljas lahendamist vajav probleem on X-tee kõrgete käideldavusnõuete rahuldamine. Allkirju peab saama moodustada ka olukorras, kus kehtivus- ja ajatempliteenused ei ole kättesaadavad.

Alljärgnevalt kirjeldame X-tee vajadustest lähtuvalt projekteeritud kõrgetootliku ja kõrgkäideldava allkirjavormingu, mis põhineb XAdES ja ASiC standarditel.

Vorming kasutab eraldi OCSP kinnitust ning ajatemplit. BDOC 2.0 vormingu korral kasutusel olevat OCSP baasil realiseeritud kehtivuskinnituse teenust ei saa antud juhul

29 http://www.riso.ee/et/files/info%C3%BChiskonna%20aastaraamat_2011-2012%20EST%20FINAL_0.pdf

kasutada, sest sellise kasutusviisi korral peaks iga päringu allkirjastamisel tegema päringu OCSP teenuse poole.

Kuna loodav süsteem peab olema kasutatav rahvusvaheliselt ning töötama koos mistahes sertifitseerimis- ja ajatempliteenuse osutajate poolt pakutavate OCSP ja ajatempliteenustega, siis ei tee me lisaeeldusi nende teenuste realisatsioonide kohta, vaid kasutame neid lihtsaimal võimalikul viisil.

Allkirja loomisel lisab iga allkirjastaja sellele oma sertifitseerimisteenuse osutajalt saadud OCSP kinnituse. Allkirja kontrollija ei pea kunagi suhtlema „võõraste“ sertifitseerimisteenuse osutajatega. Kehtivuskinnituse võtab alati sertifitseerimisteenuse osutaja klient. Kehtivuskinnitusel on süsteemi poliitikaga määratud kehtivusaeg. Allkirjastatud dokumendi vastuvõtja võib kehtestada ka oma kehtivusaja. Eriti kriitiliste teenuste puhul saab nõuda eriti värsket kehtivuskinnitust. Samas võib näiteks kriisiolukorras, kus OCSP teenus ei ole kättesaadav, konfigureerida süsteemi aktsepteerima väga vana kehtivuskinnitusi, et tagada teenuste kättesaadavus. Sama OCSP vastuse võib allkirjastaja kaasa panna paljude sõnumitega, mida ta võib saata erinevatele vastuvõtjatele.

OCSP kehtivuskinnituse värskendamise protsess on sõltumatu päringute vahendamise protsessist turvaserveris. Serveris on alati olemas piisavalt värske (poliitika mõttes) OCSP vastus. Üksiku päringu vahendamisele ei lisandu OCSP teenusega suhtlemise viidet ja teenuse latents on madal.

Allkirjastatud dokumendi vastuvõtja peab selle ajatembeldama koos OCSP vastusega, et fikseerida asjaolu, et allkirjastaja sertifikaat kehtis peale signatuuri moodustamist. Vastasel korral on oht, et allkirjastaja eitab hiljem allkirja moodustamist enne kehtivuskinnituse hankimist ja väidab, et tegu on nn. *backdating* ründega, kus ründaja valdusesse sattunud privaatvõtmega moodustatud allkirja väidetakse olevat loodud ajal mil vastav sertifikaat veel kehtis. Kuna mittekehtivale sertifikaadile vastava võtmega moodustatud allkiri on kehtetu, peab allkirjastatud dokumenti vastu võttev ja selle alusel otsuseid tegev osapool koguma andmeid, mis võimaldaks tal hiljem tõestada, et sertifikaat oli allkirja loomise hetkel kehtiv.

Põhimõtteliselt ei ole allkirja täpset moodustamise aega välja selgitada, kuna allkirja andja saab seda teha sõltumatult mistahes välistest osapooltest. Seetõttu on süsteemis paika pandud poliitika, mis sätestab, kui suur ajaline vahe võib olla OCSP kehtivuskinnituse moodustamise ja selle koos signatuuriga ajatembeldamise vahel. Nagu ka kehtivuskinnituse puhul on ka siin võimalik seda ajavahemiku muuta sõltuvalt asjaoludest ja rakendusest.

Ajatempliteenuse kasutamise efektiivsemaks muutmiseks kasutab päringute vastuvõtja ajatemplite agregeerimist. Teatud perioodi vältel saabunud allkirjastatud sõnumid kogutakse kokku ning ajatembeldatakse üheskoos. Ajatembeldamise poliitikat saab seejuures vajadusel muuta.

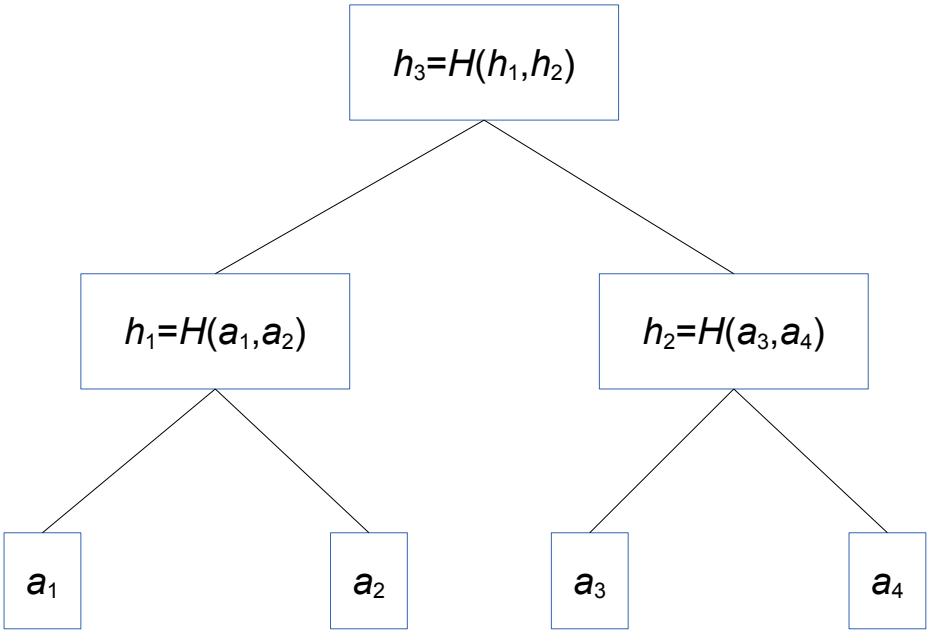
Viimane pudelikael, mida kirjeldatava allkirjavorminguga lahendatakse on signeerimise aeglus. Sarnaselt ajatembeldamisega kasutatakse agregeerimist ning ühe signeerimisoperatsiooniga allkirjastatakse mitu dokumenti. Selline lahendus võimaldab odavate ja aeglaste riistvaraliste allkirjastamisvahenditega saavutada süsteemi väga suurt läbilaskevõimet.

Niisiis tekib vajadus nii allkirjastamis- kui ajatemplipäringuid efektiivselt agregeerida. Selleks pakume välja uue andmestruktuuri – pakksignatuuri ja -ajatempli. See struktuur võimal-

dab hulga dokumente või ajatemplipäringuid esitada ühe sõnumilühendina, millele rakendatakse standardseid allkirjastamiseks või ajatembelduseks vajalikke operatsioone. Saadud digiallkirja või ajatempliga tuleb verifitseeritavuse tagamiseks kaasa panna sõnumilühendi taasmoodustamiseks vajalik lisainfo. Käesolev peatükk kirjeldabki selle sõnumilühendi moodustamist ning lisainfo struktuuri.

4.2 Pakksignatuuri- ja ajatempli moodustamine

Olgu meil tarvis agregeerida andmeüksused $a_1,...,a_n$ (nt dokumendid, ajatemplid). Neist ühise sõnumilühendi moodustamiseks kasutatakse krüptograafilist räsifunktsiooni H (nt SHA512, SHA3 vms). Selle räsifunktsiooni abil moodustatakse antud andmeüksustest nn *Merkle'i puu*. Illustreerime Merkle'i puu kontseptsiooni alljärgneval joonisel juhul n=4.



Kõigepealt rakendame räsifunktsiooni H andmeüksustele a_1 ja a_2, arvutades nende ühise sõnumilühendi $h_1=H(a_1,a_2)$, seejärel analoogiliselt $h_2=H(a_3,a_4)$ ning lõpuks kõigi andmeüksuste ühiseks sõnumilühendiks arvutame $h_3=H(h_1,h_2)=H(H(a_1,a_2),H(a_3,a_4))$. Väärtust h_3 kasutatakse standardse signeerimis- või ajatempliprotseduuri sisendina.

Vaatleme järgnevalt signeerimise näidet, kus moodustatakse digitaalallkiri s=Sig(h_3). Tõestamaks, et allkiri on seotud mõnega algsetest andmeüksustest, ei piisa enam allkirjast s, allkirjastatud sõnumilühendist h_3 ning kontrollvõtmest, vaja läheb ka tõestust, et sõnumilühend h_3 sõltub antud andmeüksusest. Selle tõestuse moodustavad osad Merkle'i puu moodustamisel kasutatud ja moodustatud vaheväärtused. Näiteks tõestamaks, et h_3 sõltub andmeüksusest a_2, tuleb juurde lisada väärtused a_1 ja h_2, misjärel on võimalik arvutada $H(H(a_1,a_2),h_2)=h_3$ ning kontrollida signatuuri s sõnumilühendil h_3.

Andmeüksuse a_2 pakksignatuuri moodustavadki digitaalallkiri s koos vajalike vaheväärtustega. Tulemuseks saadav andmestruktuur on siis sisuliselt $(s,(a_1,a_2,h_2))$. Struktuuri (a_1,a_2,h_2) nimetame edaspidi *räsiahelaks*.

4.3 Pakksignatuuri- ja ajatempli esitamine ASiC-konteineris

X-tee2 visioondokumendis[Error: Reference source not found] on toodud nõue, et X-tees kasutatavad digitaalallkirjad tuleb viia vastavusse Eesti ja EL digiallkirjastandarditega. Tänasel päeval tähendab see nõue sisuliselt, et X-tee digiallkirjad peavad vastama XAdES ja ASiC standarditele.

Selle vastavuse tagamiseks defineerime viisi, kuidas pakksignatuur ja -ajatempel ASiC-konteinerisse kapseldada. Pakksignatuur kapseldatakse järgmiste failidena:

- `merkletop.xml` – Merkle' puu tipp, mis viitab failile `merklechain.xml`,
- `merklechain.xml` – Merkle puu, mis viitab signeeritavale failile `data.foo`,
- `data.foo` – signeeritav fail,
- `META-INF/signatures.xml` – signatuur, mis signeerib `merkletop.xml` faili.

Pakkajatempel kapseldatakse sarnase struktuuriga, ainult viimaseks failiks on `META-INF/timestamp.tst`, mis sisaldab `merkletop.xml` ajatemplit.

Räsiahela kirjeldamiseks pakume välja uue andmevormingu (vt järgmist jaotist). Standardsed ASiC-konteinerina esitatud allkirja kontrollimise vahendid suudavad kontrollida faili `merkletop.xml` signatuuri. Lisaks on vaja uut tarkvaralist lahendust, mis verifitseeriks seose failide `merkeltop.xml` ja `data.foo` vahel. See tarkvara võib kujutada endast nii eraldiseisvat komponenti kui ka X-tee taristusse integreeritud moodulit.

4.4 Pakksignatuuri- ja ajatempliformaadi kirjeldus XSD-failina

Käesolevas jaotises kirjeldame võimalikku pakksignatuuri- ja ajatempliformaati XML skeemina XSD kujul.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://www.example.org/hashchain"
      xmlns:tns="http://www.example.org/hashchain"
      elementFormDefault="qualified"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <import schemaLocation="xmldsig-core-schema.xsd"
namespace="http://www.w3.org/2000/09/xmldsig#"></import>
```

Skeem defineerib uue nimeruumi `tns`, mida kasutatakse räsiahelate kirjeldamiseks. Kirjeldus tugineb standardsele XMLDSig skeemile, millele viitab nimeruum `ds`.

```
    <complexType name="HashChainType">
      <sequence>
            <element name="DefaultTransforms"
                  type="ds:TransformsType" minOccurs="0">
            </element>
            <element name="DefaultDigestMethod"
                  type="ds:DigestMethodType" minOccurs="0">
            </element>
            <element name="HashStep" type="tns:HashStepType"
                  minOccurs="0" maxOccurs="unbounded">
            </element>
      </sequence>
    </complexType>
```

Üks räsiahela element (tüübiga `HashChainType`) koosneb reast räsisammudest (tüübiga `HashStepType`). Enne räsimist rakendatakse räsisammu sisenditele potentsiaalselt mingeid vaiketeisendusi (nt XML-struktuuri normaalkujule viimine; teisendused on tüübiga `ds:TransformsType`) ning räsimiseks kasutatakse mingit vaikimisi määratud sõnumil-ühendialgoritmi (tüübiga `ds:DigestMethodType`).

```
    <complexType name="HashStepType">
      <sequence>
            <element name="HashValue" type="tns:AbstractValueType"
                  minOccurs="0" maxOccurs="unbounded">
            </element>
      </sequence>
      <attribute name="id" type="ID" use="optional"></attribute>
    </complexType>
```

Üks räsisamm (tüübiga `HashStepType`) võimaldab räsida kokku rea väärtusi (tüübiga `tns:AbstractValueType`).

```
    <complexType name="AbstractValueType">
      <sequence>
            <element name="Transforms" type="ds:TransformsType"
minOccurs="0"></element>
            <element name="DigestMethod" type="ds:DigestMethodType" mi-
nOccurs="0"></element>
      </sequence>
    </complexType>
```

Vajadusel võib konkreetse räsisammu juures kasutada teisi teisendusi ja/või sõnumil-ühendimeetodeid, kui kogu räisahela jaoks vaikimisi määratud.

```
    <complexType name="RefValueType">
      <complexContent>
            <extension base="tns:AbstractValueType">
                  <attribute name="URI" type="anyURI"></attribute>
            </extension>
      </complexContent>
    </complexType>
```

Üks võimalik väärtustüüp, mida räsisammu sisendina võib kasutada, on `RefValueType`. Väärtuseks olev URI võib viidata nii Merkle'i puu moodustamisel aluseks olevale andmeüksusele ASIC-konteineri sees või väljas (eelmise jaotise näites a_2) kui ka mõnele teisele Merkle'i puu harule.

```
    <complexType name="HashValueType">
      <complexContent>
            <extension base="tns:AbstractValueType">
                  <sequence>
                        <element name="DigestValue"
                              type="ds:DigestValueType">
                        </element>
                  </sequence>
            </extension>
      </complexContent>
    </complexType>
```

Teine võimalik väärtustüüp, mida räsisammu sisendina võib kasutada, on `HashValueType`. Vastava elemendi võimalikeks väärtusteks on räsiahela andmestruktuuri moodustavad räsiväärtused (eelmise jaotise näites h_2) või teised Merkle'i puu moodustamisel kasutatud andmeüksused (eelmise jaotise näites a_1).

```
    <element name="HashChain" type="tns:HashChainType"></element>

    <element name="HashChainResult" type="ds:ReferenceType"></element>
</schema>
```

Skeemi lõpus deklareeritakse äsjadefineeritud tüüpi elemendid. Element `HashChainResult` sisaldab Merkle'i puu juurväärtust (eelmise jaotise näites h_3) ning element `HashChain` räsiahelat (eelmise jaotise näites (a_1,a_2,h_2)).

5 Digiallkirja vormingutest teavitamine

5.1 Digitaalallkirja vormingustandardite teabe haldus

Tänu tehnoloogia kiirele arengule tekib digitaalallkirja vorminguid, standardeid, profiile jms pidevalt juurde, nii nagu ka olemasolevatel standarditel põhinevaid tark- ja riistvarala-hendusi. On teada ka juhtumeid, kus standardeid on valesti tõlgendatud ja nende põhjal loodud digitaalallkirja rakendused väljastavad tehniliselt vigaseid digitaalallkirju, mis ometi peaksid õiguspõhimõtete järgi kehtivad olema.

Kehtivas õiguslikus olukorras, kus digitaalallkiri on võrdsustatud tavaallkirjaga ja insti-tutsioonidel puudub õigus digiallkirja mitte arvestada, peab Eesti riigiasutustel, kodanikel ja erasektoril olema võimalus usaldusväärse teabe hankimiseks uutest digitaalallkirja for-maatidest ja nende realisatsioonidest, et ühelt poolt täita õigusaktidest tulenevaid nõudeid ja teiselt poolt mitte sattuda pettuste ohvriks vigase ja ebaturvalise allkirja aktsepteerimise tõttu.

Usaldusväärse informatsiooni kindlustamiseks tuleks luua register või täiendada olemasole-vat Sertifitseerimise registrit http://sr.riik.ee/, mille vastutav töötleja on Majandus- ja Kom-munikatsiooniministeerium, ning mille volitatud töötleja on Tehnilise Järelevalve Amet. Loo-dava (või olemasoleva) registri ülesanne (lisanduvad ülesanded) on koguda ja teha kätte-saadavaks informatsioon:

- Uutest ülemaailmse tähtsusega digitaalallkirja vormingutest (nt ÜRO initsiatiivid[30] vms);
- Euroopa Liidu sisemistest digitaalallkirja vormingutest;
- Eestis loodud ja kasutatavatest vormingutest;
- Digitaalallkirja tarkvarast, mis on läbinud testimise ja mille kasutamine on registripidaja poolt heaks kiidetud;
- Erandjuhtudest, kus vormingule mittevastava realisatsiooni abil on moodustatud vormilt vigaseid, ent siiski usaldusväärseid ja kehtivaid digitaalallkirju.

Iga vormingu kohta on registris avaldatud eksperthinnang: kas antud vorming on ebaturvali-ne, ebasoovitatav, turvaline või soovitatav. Riigi- ja kohaliku omavalitsuse asutused tohivad moodustada vaid soovitatavas vormingus digitaalallkirju ning ei tohi vastu võtta ebatur-valistes vormingutes digitaalallkirju.

Soovitatavad vormingud peavad olema varustatud ammendava testidekomplektiga, mis või-maldab kontrollida antud vormingut realiseeriva tarkvara korrektsust. Testid peavad katma nii positiivseid kui ka negatiivseid stsenaariume. Muud vormingud võivad omada testikomp-lekte.

30 http://www.uncitral.org/uncitral/publications/publications.html

Riigiasutused tohivad kasutada vaid digitaalallkirja tarkvara, mis on vigadeta läbinud testimise registrisse kantud testikomplektide vastu ning mis on registripidaja poolt heaks kiidetud. Sarnased regulatsioonid kehtivad enamikes arenenud riikides ja neid on mõistlik rakendada ka Eestis, et hoida ära piinlike ja segadust tekitavaid juhtumeid nagu allkirjastamine autentimisvõtmega, jms.

Registris oleva teave peab olema avalikult kättesaadav.

Juhul kui avastatakse mingi registreeritud vormingu tehniliselt vigane realisatsioon, siis tuleb esmalt infoturbe ja krüptograafia spetsialistide abiga veenduda, kas vigaselt realiseeritud digitaalallkiri muutub ebaturvaliseks ja teha üks järgnevatest otsustest:

- **Vigased digitaalallkirjad on turvalised ja usaldusväärsed.** Piisab kui teha vastav kanne registrisse, lisades sinna vigase vormingu kirjelduse ja märkuse, et selles vormingus digitaalallkirjad on turvalised. Samas peavad registris olevad andmed selgelt viitama, et kirjeldatud vorming on ebakorrektne. Vigase realisatsiooni loojale saadetakse soovitus viia realisatsioon standarditega kooskõlla.
- **Vigase digitaalallkirja vormingu kasutamine tulevikus on ebaturvaline, kuid juba antud allkirju võib korrektseks lugeda.** Digitaalallkirja kontrollimise teenus peab vahet tegema allkirjadel, mis on antud enne vigase vormingu avastamist ja avalikustamist, ja allkirjadel, mis moodustatakse pärast seda. Pärast avalikustamise kuupäeva loodud allkirjad kuulutatakse kehtetuteks. Tuleb teavitada kõiki riigiasutusi, kus mingil põhjusel võidakse kasutada vigast vormingut õigeks lugevaid digitaalallkirja kontrollimise rakendusi.
- **Kõik vigased digitaalallkirjad on ebaturvalised ja tuleb (tagantjärgi) kehtetuteks tunnistada.** Tuleb kokku kutsuda spetsialistidest ja valitsuse ametnikest moodustatud komisjon, mis hindab tekkinud kahju ulatust ja otsustab, kas ja kuidas korrigeerida vigase ja kehtetu digitaalallkirjaga menetlus- ja arhiividokumente. Üldkehtivaid detailseid juhiseid siin anda on väga raske. Lahendus sõltub konkreetsest juhtumist ja kahju ulatusest.

Registri töötleja peab osutama allkirjavormingu tuvastamise teenust, st saadetud digitaalallkirjastatud dokumentide kohta vastama, mis vormingus need on. Teenus on täisautomaatne. Kui vormingut tuvastada ei õnnestu, antakse viga. Kui vorming õnnestub tuvastada võib klient endale laadida vastava digitaalallkirja tarkvara ning selle abil allkirja kontrollida.

Riigiasutuste asjaajamiskorda (sh Asjaajamiskorra ühtsed alused[31]) tuleks muuta nii, et ametnikud, kes võtavad menetlusse digitaalallkirjaga dokumente, oleksid kohustatud pöörduma registri poole allkirja vormingu kindlakstegemiseks, juhul kui allkiri on ametnikule tundmatus vormingus. Sama nõudega võiks täiendada ka ISKE ID-kaart/PKI ohtude ja meetmete moodulit https://www.ria.ee/public/ISKE/id_ohud_meetmed.odt.

31 https://www.riigiteataja.ee/akt/119062012007

6 Digiallkirja tarkvara arenduse korraldamine

6.1 Taust

Digitaalallkirja tarkvara arenduse korraldus Eestis on aegade jooksul palju muutunud. Praegu vastutab digitaalallkirja tarkvara arendamise korraldamise eest Riigi Infosüsteemi Amet. RIA on seda teostanud digitaalallkirja tarkvara arendus- ja hooldusteenuse ostmiseks suunatud riigihangete korraldamise kaudu. Aegade jooksul on tarkvara on arendanud eri ettevõtted. Viimase, nüüd lõppema hakkava hanke võitja oli AS Sertifitseerimiskeskus (SK), mis on olnud pikka aega tihedalt seotud kogu ID-kaardi ja hiljem ka Mobiil-ID kasutamiseks vajaliku tarkvara loomisega. AS Sertifitseerimiskeskus on ennekõike sertifitseerimis- ja ajatempliteenuse osutaja, kes oma teenuse kasutatavaks tegemiseks on tellinud ja tegelenud ka digiallkirja tarkvara arendamisega.

Aja jooksul on nõuded digiallkirja tarkvarale muutunud ja tõenäoliselt muutuvad lähitulevikus veelgi. Sellega seoses peab ette nägema muudatusi nii tarkvaras kui ka selle arenduse korralduses.

6.2 Vajalikud muudatused

Digitaalallkirja tarkvara all peame silmas nii vahetult digitaalallkirjade andmiseks ja kontrollimiseks mõeldud programme, kui ka ID-kaardi kasutamiseks ja haldamiseks vajaliku tarkvara ning ID-kaardi ja Mobiil-ID kasutamiseks vajalikke teenuseid.

Digiallkirja tarkvara poolt lahendatav vajadus on olnud seni sõnastatud kui „pakkuda vahendeid ID-kaardi ja Mobiil-ID ning nendega seotud teenuste kasutamiseks“. See on arusaadav probleempüstitus vastava infrastruktuuri ja teenusepakkuja vaatevinklist, kes vajab vahendeid oma teenuse kättesaadavaks tegemiseks.

Paraku ei ole selline kitsas vaade valdkonnale enam piisav. Vaja on lahendada kasutajate (inimeste ja organisatsioonide) üldisemat probleemi: „kuidas rakendada digiallkirja“. See probleemipüstitus on aina enam järjest laiem kui lihtsalt ID-kaardi või Mobiil-ID abil DigiDoc konteineri loomine.

- EL arengud toovad endaga lähiaastatel tõenäoliselt kaasa vajaduse toetada igapäevaselt samaaegselt mitmeid digitaalallkirja vorminguid.
- Tekib vajadus toetada samaaegselt mitmeid usaldusteenuste pakkujaid, kes on kantud üleeuroopalisse usaldusteenuse osutajate nimekirja.
- Laiendamist vajab erinevate platvormide (k.a. nutiseadmete) tugi.
- Ühest lahendust vajab digitaalallkirja pikaajalise tõestusväärtuse säilitamise teema.

- Kuna nõuded digiallkirja kasutamisele EL-s ühtlustuvad, siis võiks arendatav tehnoloogia olla kasutatav ka väljapool Eestit – see tähendab täiendavaid kasutajagruppe ning -nõudeid, millest kõiki me veel ei tea.

Digitaalallkirja tarkvara on keeruline ja vastutusrikas tarkvaratoode, mille arhitektuuri ja realisatsiooni headusest sõltub paljude e-riigi lahenduste pikaajaline töökindlus ja toimimine. Seni on süsteemi arhitektuuri loomine toimunud suhteliselt juhuslikult. Tulemuseks on ebaühtlased ja -loogilised programmeerimisliidesed, vähene modulaarsus ning mitmed kriitilised tarkvaravead. Arendusprotsess on olnud suletud. Arhitektuursed otsused on teinud ennekõike konkreetne arendaja töö käigus oma parema äranägemise järgi. Olukorras, kus nõuded on muutumas, on senisest suurem vajadus modulaarse, heade ja stabiilsete programmeerimisliidestega, kergelt kasutatava, paljusid digiallkirja vorminguid ja ka teenusepakkujaid toeava digiallkirja tarkvara järele.

Erinevalt näiteks X-tee-st puudub hetkel tehnoloogiatarnija, kes oleks valmis ja võimeline panustama identifitseeritud nõudeid rahuldava digiallkirja tarkvara arendamisse, siis tasub kaaluda avatud protsessi rakendamist, mis võimaldaks arvestada kõigi osapoolte huvidega, kaasata oluliste arhitektuursete otsuste tegemisse parimaid tarkvara- ja turvainsenere ning pakkuda pikaajaliselt kvaliteetset lahendust.

6.3 Ettepanekud arenduse korraldamiseks

Järgnevas analüüsis alustame oluliste uuenduste kirjeldamisest ning hiljem näitame, kuidas neid kõige lihtsam oleks olemasolevas arendusmudelis realiseerida.

Kõige olulisem uuendus on nõuete avatud haldus – on defineeritud muudatuste halduse avatud protsess. Kõik muudatusettepanekud kirjeldatakse ühtses vormis, nii need mis tulevad RIA-st, need mis tulevad võimalikelt rahastajatelt, kes soovivad endale vajaliku funktsionaalsuse lisamist, kui ka need, mis tulevad vabatahtlikelt abilistelt. Need ettepanekud on avalikkusele aruteluks kättesaadavad. Arutelu käigus võib ettepanek muutuda, et sobituda süsteemi üldise loogikaga. Mõni ettepanek ei pruugigi sobituda ja lükatakse lõpuks tagasi. Ainus viis tarkvara muuta, on realiseerida avaliku arutelu läbinud ja heaks kiidetud muudatusettepanekud.

Kuna avalik arutelu ei pruugi olla piisavalt kvaliteetne ning lõpuks on vaja teha ka otsuseid ja muudatusi läbi projekteerida, siis peab olema olemas arhitektuurinõukogu. Sinna kuuluvad tarkvaraarenduse, krüptograafia ja infoturbe eksperdid. Arhitektuurinõukogu ülesanne on muudatusettepanekute läbiprojekteerimine, samuti tagasiside andmine juhul, kui mõni muudatus pole teostatav. Arhitektuurinõukogu töö kvaliteet ja kiirus on kriitilise tähtsusega. Nõukogu liikmete motiveerimiseks, konflikti vältimiseks nende põhitööandjatega ning neilt kvaliteetse tulemi nõudmiseks peaks selle töös osalemine olema tasustatud. Nõukogu peaks otsuseid langetama ühehäälselt – seda aitaks tagada toote kvaliteeti ja pikaajalist stabiilsust. Arhitektuurinõukogu poolt läbi töötatud muudatusettepanekud saavad ka realiseerimise mahuhinnangu, mis võimaldab plaanida ressursse muudatusettepanekute realiseerimiseks.

Kuna eesmärk on kindlasti rahvusvaheline kasutus, siis peaks töökeeleks olema inglise keel. See võimaldaks hiljem arhitektuurinõukoguse kaasata ka rahvusvahelisi eksperte.

Läbiprojekteeritud muudatuste realiseerimiseks peab rahastaja nende realiseerimise tellima. Ootuspäraselt on tellijaks algse muudatusettepaneku tegija, kuid rahastajaks võib olla kes tahes. Vastavad summad võivad tulla riigieelarvest, mõni ettevõte võib endale vajaliku muudatuse tellida vms. Avaliku arutluse läbinud ja arhitektuurinõukogu poolt läbi projekteeritud ning heaks kiidetud muudatusettepanekuid tagavad toote kvaliteedi sõltumata tellijast. Töö käigus võib selguda, et mõne muudatuse kvaliteetne realiseerimine on oluliselt kulukam, kui algul arvati. Sellisel juhul peab huvitatud osapool leidma kas täiendavaid vahendeid või jääb see muudatus hetkel realiseerimata. Poolikuid ja ebakvaliteetseid lahendusi ei realiseerita.

Muudatuse tegelikuks realiseerimiseks on mitmeid viise. See võidakse tellida ühekordse arendustööna. Või siis on organisatsioonil, mille juures arhitektuurinõukogu tegutseb, endal arendusmeeskond, mis suudab muudatusi realiseerida. Läbiprojekteeritud muudatus võidakse realiseerida ka vabatahtlike poolt ning annetada. Igal juhul on eesmärk toote pikaajaline kvaliteet. Realiseeritakse ainult läbiprojekteeritud muudatusi ning realisatsiooni kvaliteeti testitakse enne selle integreerimist põhjalikult.

Testimiseks on vajalikud nii infrastruktuur (näiteks tööjaamad kõigi toetatud platvormidega), kui ka kogu funktsionaalsust kattev testide komplekt, mida iga muudatuse realiseerimisel täiendatakse.

Ülaltoodud põhimõtete rakendamiseks on mitmeid viise. Alljärgnevalt kirjeldame, kuidas saaks seda ellu viia seni kasutusel olnud viisi laiendades. Eesti väiksust ja pädevate ekspertide nappust arvestades ei tundu otstarbekas mingi uue juriidilise keha loomine. Avatud arendusprotsessi kasutamise nõue tuleks lisada digiallkirja tarkvara arendamiseks korraldatavate hangete tingimuste hulka. Endiselt oleks süsteemis kaks põhitegijat: RIA ning hanke võitnud tarkvaraarendaja.

Osapoolte kohustuste plaanimisel peab arvestama sellega, et hange on tähtajaline ning järgmisel hankel peaks ka teised osalised suurema vaevata konkursil osaleda saama. Seetõttu võiks näiteks testimise, muudatuste halduse ning versioonihalduse infrastruktuur olla RIA omandis. Ka avatud protsessi defineerimine võiks olla RIA ülesanne. Samas protsessi elluviimine k.a. arhitektuurinõukogu töö korraldamine, heakskiidetud muudatuste realiseerimine hanke poolt etteantud piirides, testimise korraldamine jms võiks olla hanke täitja ülesandeks.

6.4 Muudatusettepanekud arhitektuurinõukogule

Alljärgnevalt on toodud esimesed muudatusettepanekud arhitektuurinõukogule arutamiseks.

1. Modulariseerida süsteem, luua stabiilsed ja kvaliteetsed liidesed moodulite vahele. Moodulid peavad olema ka iseseisvalt kasutatavad. Eraldi peaks olema kättesaadavad: signeerimismoodul – PKCS#1 allkirja loomiseks, allkirja loomise moodul, allkirja kontrolli moodul. Moodulid peaks suutma töödelda suvalise suurusega dokumente. Moodulid peaks suutma töödelda dokumente ilma ajutisi faile loomata.
2. Erinevate digitaalallkirja vormingute toe realiseerimine pluginate kaudu. Oluline on see just allkirja kontrollimise moodulis. Ka hetkel kasutusel oleva allkirjavormingud (k.a.

Digidoc, koos kõigi oma variatsioonide ja ajalooliste bugidega) tuleks eraldada eraldi pluginasse. Pluginatel peaks olema ühtne liides, mis sisemisel realiseeritakse olemasolevate või ka kolmanda osapoolte teekide kaudu. Halva kvaliteediga (mälulekked, krahhimine) teekide kasutamisel peaks plugin isoleerima teegi rakendusest (eraldi protsess plugina jaoks).

3. Standardse PKCS#1 allkirja loomine PKCS#11 liidese kaudu kõigile allkirjastamismeetoditele (k.a. Mobiil-ID). Oluline muude allkirjastamistarkvarade toetamiseks. Näiteks sekundaarse PAdES vormingu toetamiseks ei pruugi olla mõistlik hakata looma oma rakendust, vaid tasub kasutada olemasolevaid. See aga eeldab standardsete programmiliideste olemaolu (vs. mittestandardne DigiDocService teenus, mis loob kohe allkirjastatud konteineri).
4. Digiallkirja teegi varustamine RPC liidesega. Praegu on digiallkirja kasutamiseks kaks võimalust. Kas kasutada Java, C või C++ teeke (kusjuures C teegi tugi on plaanis lõpetada) või DigiDocService poolt pakutavaid teenuseid. DigiDocService probleem on sõltuvus kolmandast osapoolest, samuti vajadus saata potentsiaalselt konfidentsiaalset infot süsteemist välja. DigiDocService'i eelised on kasutamise suhteline lihtsus eri platvormidel (ehkki SOAP ei ole kõige kergekaalulisem RPC protokoll) ning digiallkirja funktsionaalsuse operatiivsem uuendamine ilma lõppkasutaja rakendust ümber ehitamata. Java ja C/C++ teekide probleem on kvaliteet, samuti piiratud valik platvorme ning uuendamise raskekaalulisus. Eelised on sõltumatus teenusepakkujast ning konfidentsiaalsete andmete parem kaitse. RPC liidesega teek, mille saaks evitada lokaalse teenusena, pakuks mõlema olemasoleva lahenduse eeliseid: autonoomse, standardse teenuse uuendamine on lihtsam kui rakendusse sisse kompileeritud teegi uuendamine, puudub sõltuvus välisest teenusepakkujast, konfidentsiaalseid andmeid ei pea süsteemist välja saatma, teek on kasutatav kõigil platvormidel. Tasub kaaluda mõne kergekaalulise RPC protokolli nagu JSON-RPC kasutamist. Nii saaks näiteks Javas kirjutatud digiallkirja teeki kasutada Pythonis, Rubys, Haskellis, Javascriptis jne.
5. Töötada välja vormingud ja protseduurid pikaajalise tõestusväärtuse säilitamiseks. Realiseerida vajalik tugi digiallkirja tarkvaras. Arvestama peab laiemat skoopi, kus vaja on tagada mitte ainult AS Sertifitseerimiskeskus poolt väljastatud sertifikaatide abil antud digiallkirjade kehtivus, vaid suvaliste usaldusnimekirja kantud teenuseosutajate poolt väljastatud sertifikaatidega antud allkirjade tõestusväärtus.

7 X-tee turvaserverite varustamine turvalise allkirja andmise vahenditega

X-tee uus versioon – SDSB – oskab vahendatavaid SOAP sõnumeid allkirjastada riistvaraliste krüptoseadmete poolt hallatavate võtmetega. Turvaliste krüptoseadmete kasutamine on vajalik üheselt mõistetava seadusliku digitaalallkirja moodustamiseks.

Turvaserver toetab põhimõtteliselt kõiki PKCS#11 liidest omavaid krüptoseadmeid, muuhulgas ka kiipkaarte ning riistvaralisi turvamooduleid (HSM). Nii kiipkaardid kui ka HSM-d pakuvad võrreldavaid turvatasemeid võtme kaitseks. Põhiline erinevus on seadmete tootlikkuses ja hinnas. HSM-d on kuni kolm suurusjärku suurema tootlikkuse ning hinnaga. Samuti on aeganõudvam nende paigaldamine ja häälestamine.

Kuna X-tee üks suur eelis on olnud tema kättesaadavus: X-teega liitumine on asutuse jaoks olnud sisuliselt PC-serveri (või virtuaalserveri) hinnaga, siis loomulikult tekitab täiendava spetsiifilise riistvara hankimise vajadus küsimuse, kas X-tee on endiselt kõigile kättesaadav?

See peatükk kirjeldab, kuidas võiks toimuda X-tee turvaserverite varustamine riistvaraliste krüptoseadmeteganing kuidas riistvaralise krüpto kasutamine mõjutab X-tee turvaserveri tootlikust.

- Kirjeldame SDSB turvaserveri võimekust kasutada aeglaseid signeerimisvahendeid sisuliselt piiramatu läbilaskevõimega signeerimisseadme konstrueerimiseks.
- Kirjeldame ühe turvaserveri signeerimisseadmetega varustamiseks vajalikud riistvarakomplektid ja tegevused.
- Kirjeldame, kuidas valida turvaserveri kasutuse iseloomu järgi optimaalne riistvaralise krüptoseadme lahendus.
- Hindame eri klassidesse kuuluvate turvaserverite arvu.

7.1 Riistvaralised allkirjastamisvahendid

Turvalised allkirjastamisvahendid jaguneva laias laastus kahte gruppi: kiipkaardid ja riistvaralised turvamoodulid. On veel olemas nn krüptopulgad, kuid enamasti on need samaväärsed CCID standardile vastava USB porti käiva kaardilugejaga, millesse on permanentselt asetatud krüptograafiline kiipkaart. Krüptopulga eelis kiipkaardilugeja ja kiipkaardi kombinatsiooni ees on ennekõike kompaktsus ning korrodeeruda võivate kontaktide puudumine. Muus osas võib neid vaadelda samaväärsetena.

Turvaliste ja võimekate krüptograafiliste kiipkaartide hinnad väikeseerias ostes algavad 6 eurost. Samas hinnakategoorias on kaardi kasutamiseks vajalik kaardilugeja. Selline 12-eurone seade suudab 2048-bitise RSA võtme abil moodustada 2–3 signatuuri sekundis. Selline seade suudab 2048-bitise RSA võtme abil moodustada 1000 signatuuri sekundis.

X-teel on turvaservereid, mis teenindavad mitmeid sadu päringuid sekundis ning mis vajavad seetõttu kõrgtootlikku riistvaralist turvamoodulit.

X-teel on praegu palju turvaservereid, mille poolt vahendatavate päringute arv on palju väiksem riistvaralise turvaserveri võimsusest. X-teel on turvaservereid, mille päringute arv on küll väike, kuid käideldavusnõuded nii suured, et vajalik on riistvara k.a. HSM dubleerimine.

Eeltoodust lähtuvalt on selge, et vaja on toetada mõlemaid seadmeid: nii kiipkaarte kui ka riistvaralisi turvamooduleid. Iga turvaserveri evitamisel on võimalik paindlikult valida, milliseid vahendeid kasutada ja niiviisi palju raha kokku hoida.

7.2 Pakksignatuurid SDSB turvaserveris

X-tee turvaserver toetab kiipkaartide (ja vajadusel ka riistvaraliste krüptomoodulite) kasutamist pakksignatuuri režiimis. Pakksignatuuri vormingut on lähemalt kirjeldatud peatükis 4. See peatükk kirjeldab, kuidas mõjutab pakksignatuuri kasutamine turvaserveri jõudlust.

Pakksignatuuri idee on lihtne:

- süsteemis on järjekord signeerimist vajavatest dokumentidest. Kui turvaserver peab signeerima väljamineva sõnumi, paneb ta selle järjekorda;
- süsteemis on kiipkaart või kiipkaardid, mis tegelevad järjekorda pandud sõnumite signeerimisega. Iga kord kui kiipkaart vabaneb, korjatakse kokku kõik seni järjekorda lisandunud sõnumid ning neist moodustatakse Merkle puu, mille tipp antakse kiipkaardile signeerida. Pärast signeerimist moodustatakse signeeritud Merkle puu tipust ja selleni viivast räsiahelast pakksignatuur, mis tagastatakse päringuvahendajale.

Kõik muud krüptooperatsioonid peale kiipkaardiga signeerimise on väga kiired. Kiipkaardiga signeerimine võtab aga ~0,5 sekundit. Pakksignatuuride mõju tootlikkusele on kolmesugune.

1. Ühe RSA operatsiooniga võib signeerida sisuliselt piiramatu arvu sõnumeid. Merkle puu moodustamine on väga kiire operatsioon, seda saab ka ette arvutada. Realistlik on signeerida tuhandeid sõnumeid sekundis. Serveri jõudlus on suurem kui tavasignatuuride korral.
2. Kiipkaardi kasutamine vabastab serveri protsessori ajamahukast RSA arvutamisest. Server saab tegeleda muude asjadega (näiteks SOAP sõnumite moodustamine).
3. Ühe konkreetse päringu töötlemise aeg suureneb. Halvimal juhul kui päring satub signeerimisjärjekorda täpselt sel hetkel, kui eelmine tsükkel algas, kulub päringu teenindamiseks kahe kiipkaardi RSA operatsiooni võrra aega. Parimal juhul on kiipkaart vaba ja sõnum signeeritakse kohe – siis kulub vaid ühe signeerimise jagu aega. Kuna allkirjastatakse nii päring kui vastus, kulub kokku kaks korda rohkem aega. Ehk siis praktikas liitub iga SDSB teenuse vahendamisele 1–2 sekundi pikkune viivitus.

Kindlasti on rakendusi, mille jaoks selline viivitus on lubamatu. Kodanikuportaal võiks olla üks selliseid. Näiteks kompleksteenuste korral liituvad üksikute järjest esitatud päringute viivitused. Sellisel juhul peab kasutama riistvaralisi turvamooduleid. Riistvaralisi turvamoo-

duleid võib olla soovitatav kasutada ka töökindluse tõstmiseks. Võib luua ka hübriidlahendusi, kus kallis turvamoodul on dubleeritud kiipkaartidega.

Pakksignatuuride kasutamisel ongi põhiline erinevus kiipkaardi ja riistvaralise turvamooduli vahel täiendavas latentsis. Tootlikus on mõlemal juhul samas suurusjärgus.

Riistvarakomplektid ja nende paigaldamine

See peatükk kirjeldab ühe serveri riistvaraliste allkirjastamisvahenditega varustamiseks mõeldud riistvarakomplektid ning hindab nende paigutamiseks kuluvat aega. Kokku on neli komplekti:

- Kaks kiipkaarti koos kahe välise lugejaga.
- Kaks kiipkaarti koos kahe sisemise lugejaga.
- PCI siinile mõeldud riistvaraline turvamoodul.
- Ethernet liidesega riistvaraline turvamoodul.

7.2.1 Kaks kiipkaarti koos kahe välise lugejaga

Lahendus on suhteliselt töökindel ja hooldusvaba, asendamine lihtne ja odav.

Probleemiks võib olla vabade USB portide nappus. Siis peaks lisaks plaanima USB hubi. Virtuaalserverite korral peab leidma viisi USB virtualiseerimiseks. USB hubist ei ole abi – sisuliselt on ühes hostmasinas olevate turvaserverite arv piiratud vabade USB portide arvuga. On ka USB-over-TCP lahendusi, aga nende hinda ja omadusi ei vaadeldud.

Seda lahendust võib soovitada väikesemale organisatsioonile, kes haldab oma turvaserverit ise.

7.2.2 Kaks kiipkaarti koos kahe sisemise lugejaga

Paigaldamine on aeganõudvam, kuna server tuleb lahti võtta. 1U serverite korral on probleemiks vaba koha leidmine serveris. Muud probleemid on samad mis eelmisel juhul.

Kaardilugejad on koos USB hubidega võimalik monteerida ka seadmekappi paigaldamiseks mõeldud kesta. Tulemus on viisakas, ehkki kallipoolne.

7.2.3 PCI siinile mõeldud riistvaraline turvamoodul

Lahendus kõrgete käideldavus- ja tootlikusnõuetega eraldiseisvale turvaserverile, mis vahendab teenuseid, mille korral on oluline väike viivitus. Paigaldamine võtab aega umbes tunni. Lahendus on suhteliselt töökindel ja hooldusvaba. Kui tegu on kõrgete käideldavusnõuetega, siis on mõistlik dubleerida juba kogu turvaserverit. Ühte serverisse mitut turvamoodulit lisada ei ole eriti mõistlik. Rikke korral võib olla probleemiks asendusseadme leidmine piisavalt lühikese ajaga. Mõistlik võib olla mitme organisatsiooni ühisost koos väikese isikliku laovaru tekitamisega. See lahendus ei toimi koos virtualiseerimistarkvaraga.

7.2.4 Ethernet liidesega riistvaraline turvamoodul

Kõige võimsam, universaalsem ja kallim lahendus. See on iseseisev seade, mis võib teenindada mitmeid kliente. Mõnedel tootjatel on võimalus turvamoodulite klastri moodustamiseks. Klientarvuti võib olla virtualiseeritud. Mõistlik lahendus majutusteenuse pakkujatele. Riistvaralist turvamoodulit võib jagada ka muude rakendustega.

7.3 Turvaserverite klassifitseerimine

Eesmärk on jagada turvaserverid klassidesse selle järgi, mis tüüpi allkirjastamisvahenditega peaks nad varustama.

Pakume välja viis klassi servereid.

1. Üksikuid päringuid vahendav turvaserver. Päringute vaheline aeg on enamasti suurem signeerimise ajast, seetõttu on lisanduv viide väiksem. Vahetult X-tee teenuseid kasutavate inimeste arv on väike. Mõistlik on kasutada kiipkaarte.
2. Põhiliselt infosüsteemide vahelisi päringuid vahendav turvaserver. Päringute arv võib olla suur, kuid lisanduv viide ei oma tähtsust. Mõistlik on kasutada kiipkaarte.
3. Mõnd portaali teenindav turvaserver. Väiksema viite saavutamiseks ja kasutajakogemuse parandamiseks on vajalik kasutada riistvaralist turvamoodulit.
4. Paljukasutatava andmekogu turvaserver. Töökindluse suurendamiseks ja teenuseid interaktiivselt kasutavate klientide kasutajakogemuse parandamiseks on mõistlik kasutada riistvaralist turvamoodulit.
5. Majutusteenuse pakkuja juures olev (virtualiseeritud) turvaserver. Halduse lihtsustamiseks ning kulude jagamiseks on mõistlik kasutada võrku ühendatud riistvaralist turvamoodulit.

7.3.1 Maksumuse arvutus

Maksumuse arvutamiseks tuleb hinnata eri klassidesse kuuluvate turvaserverite arvu X-tee tootekeskkonnas. 1. grupi servereid võiks saada eristada X-tee kasutusstatistika analüüsi alusel. Teiste gruppide serverite arvu on kasutusstatistika analüüsi teel raske hinnata. Vaja on eelteadmisi ja/või suhtlust serverite omanikega. Kuna tegelike serverite arv on eeldatavasti paarisaja piires ja täpsustamist vajavaid servereid veelgi vähem, siis peaks serverite loendamine vajadusel ka tehtav olema.

8 Kokkuvõte

Kokkuvõtlikult olid uuringu olulisemad järeldused ja soovitused järgmised:

1. Sertifitseerimise register peab hakkama haldama soovituslike allkirjavormingute nimekirja, mille järgimine on riigiasutustele kohustuslik. Soovituslikud allkirjavormingud peavad olema varustatud põhjaliku testikomplektiga. Vormingut realiseerivad tarkvaralahendused peavad läbima testimise vigadeta. Riigiasutused tohivad kasutada vaid testimise läbinud tarkvaralahendusi.
2. Eesti vajadusi rahuldava digitaalallkirja tarkvara arendamine peab keskenduma kasutajate vajaduste rahuldamisele, olema avatum, kaasama eksperte süsteemi arhitektuuri arendamisse, tagama eri allkirjavormingute kasutamise võimaluse.
3. Jätkata XAdES standardil baseeruva digitaalallkirja vormingu kasutamist põhilise allkirjavorminguna.
4. Hinnang BDOC 2.0 standardikavandi sisulisele optimaalsusele sõltub kavandi autorite vastustest tõstatatud küsimustele. Vormiliselt ei ole standardikavand optimaalne.

Lisaks:

1. Kirjeldati X-tee uusversiooni SDSB jaoks kasutamiseks sobilik kõrgkäideldav ja kõrgtootlik digitaalallkirja vorming.