Digitaalallkirja juurutamine riigiasutustes

Strateegiline plaan

November 2001

Arne Ansper
Ahto Buldas
Sven Heiberg
Monika Oit
Kaidi Oone
Olev Sepp
Jan Villemson

Aruande koostajad tänavad projekti juhtrühma ja töörühma järjekindla konstruktiivse kriitika ning asjalike ettepanekute eest, mis aitasid kaasa töö valmimisele. Eraldi tahaks ära märkida Aare Lapõnini, Andrus Kalli, Ülle Lauri ja Tuulikki Laessoni abi.

Sisukord

1. Sissejuhatus

1.1 Digitaaldokumendid

Digitaalallkirja rakendamise projekti üldine eesmärk on luua riigiasutustele võimalus digitaaldokumentide kasutamiseks oma tööprotsessides, nende vastuvõtmiseks ning väljaandmiseks. Selleks, et seniseid paberkandjal dokumente saaks asendada digitaaldokumentidega, tuleb tagada dokumentide *tõestusväärtuse* säilimine, st. peab olema võimalik kindlaks teha:

- dokumendi loomisaega
- dokumendi loojat
- et dokumenti ei ole peale loomist muudetud.

Paberkandjal dokumendi tõestusväärtus on reeglina tagatud, kui selles sisalduv teave omab piisavat tõestusväärtust ning dokument vastab kindlatele vorminõuetele, näiteks on varustatud omakäelise allkirjaga. Omakäeline allkiri on dokumendiga seotud kandja kaudu ja isikuga seotud läbi tema füsioloogiliste omaduste. Kuna digitaalselt esitatud teave ei ole seotud konkreetse andmekandjaga, nõuab tõestusväärtusega digitaaldokumendi tekitamine hoopis teistsuguseid võtteid kui paberdokumendi puhul. Mehhanismi, mis võimaldab tõestatavalt seostada digitaaldokumenti tema loojaga, nimetatakse digitaalallkirjaks, ent selle omadused võrreldes tavaallkirjaga on tegelikult oluliselt erinevad, mistõttu digitaalallkirja kasutuselevõtmine ei tähenda lihtsalt senistes dokumentitöötluse protseduurides tavaallkirja asendamist digitaalsega, vaid kogu dokumendihalduse tööprotseduuride loogika läbivaatamist uute vajaduste ja võimaluste valguses.

Eestikeelses kirjanduses on digitaaldokumendi mõiste nimetusena kasutatud ka sõnu *digitaalne dokument*, *elektrondokument* ning *elektrooniline dokument*, mida võib tegelikult võtta sünonüümidena. Kuna esimene süstemaatiline eestikeelne raamat selles vallas - Valdo Prausti koostatud "Digitaalallkiri. Tee paberivabasse maailma" [22] kasutab sõna *digitaaldokument*, siis on selle juurde jäädud ka käesolevas aruandes.

Üldisemas mõistes digitaaldokumendi sisuks võib olla niihästi mingi sisuga tekst, mingid andmed, pildid, video- või helilõigud või mistahes muu teave, mida on võimalik esitada digitaalkujul.

Asjaajamises kasutatavate digitaaldokumentide puhul tagatakse dokumendi sisu, vormi ja struktuuri arusaadavus dokumendi sisustruktuurile kehtestatavate reeglitega (kohustuslikud ja lisarekvisiidid). Järgnevas tekstis käsitletakse digitaaldokumendina vaid asjaajamises kasutatavat ning määratletud struktuuriga dokumenti, mille definitsioonina kasutatakse Arhiiviseaduses [7] toodud dokumendi määratlust - dokument on mistahes teabekandjale jäädvustatud teave, mis on loodud või saadud asutuse või isiku tegevuse käigus ning mille sisu, vorm ja struktuur on küllaldane faktide või tegevuse tõestamiseks.

1.2 Digitaalallkirja ülesanded

Digitaalallkiri on tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mida allkirja andja kasutab, märkimaks oma seost digitaaldokumendiga.

Digitaalallkirjal on tuvastusfunktsioon – allkiri võimaldab dokumendi saajal teha kindlaks digitaaldokumendi autori. Muuhulgas võimaldab allkiri kindlaks teha ka dokumendi terviklust, st. seda, et digitaaldokumenti ei ole peale allkirjastamist muudetud.

Digitaalallkirjal on tõestusfunktsioon – allkiri võimaldab tõestada dokumendi autorit kolmandale osapoolele. Tõestada saab ka seda, et digitaaldokumenti on peale digitaalallkirja andmist muudetud.

Digitaaldokumentide halduses on ka olukordi, kus autorluse ja tervikluse tõestamisest jääb väheseks ning on vaja tõestada ka digitaalallkirja andmise aega, st. näidata, et digitaalallkiri anti mingis kindlas ajavahemikus ja mitte varem ega hiljem. Digitaalallkirja seadusele vastav digitaalallkiri võimaldab täita ka seda ülesannet.

Ka riigiasutuste digitaaldokumentide puhul on digitaalallkirjal needsamad tavapärased ülesanded, mis aga erinevates kasutusstsenaariumites võivad olla erineva kaaluga.

1.3 Strateegilise plaani eesmärk

Eesti riigiasutustes digitaalallkirja rakendamise strateegilise plaani koostamise eesmärgiks on tuvastada võimalikud digitaalallkirja kasutusviisid ning sätestada ühtsed visioonid ja tegevuskava digitaalallkirja kasutuselevõtuks kogu avalikus sektoris. Strateegilise plaani väljatöötamine on esimeseks etapiks Justiitsministeeriumi, Rahandusministeeriumi, Siseministeeriumi, Teede- ja Sideministeeriumi, Majandusministeeriumi ning Riigikantselei vastavas ühisprojektis, mis käivitati 2001. aasta maikuus. Selle initsiatiivi ajendiks oli vajadus ellu viia Eesti Vabariigi Riigikogu poolt 8.märtsil 2000.a. vastu võetud Digitaalallkirja seadus ja 15.novembril 2000.a. vastu võetud Avaliku Teabe seadus ning Vabariigi Valitsuse 26.veebruari 2001.a. määrus nr 80 "Asjaajamiskorra ühtsed alused".

Edasise strateegia väljatöötamiseks on analüüsitud digitaalallkirja kasutusstsenaariume ning digitaalallkirja rakendamisega seonduvaid probleeme nii digitaalallkirja elutsükli lõikes (digitaalallkirja andmise, kontrollimise ja säilitamisega ning digitaalallkirja andmise vahenditega seotud probleemistikku), digitaalallkirja rakendamisel erinevates (infovahetus)suhetes kui ka digitaalallkirja rakendamisel erineva tekkeviisiga dokumentide puhul. On koostatud kokkuvõtlik ülevaade riigiasutustes digitaalallkirjaga seonduvatest probleemidest ning ohtudest ja antud ülevaade ka juba käivitatud ning digitaalallkirja rakendamist toetavatest initsiatiividest. Arvesse võttes riigiasutuste poolt sätestatud prioriteete on koostatud strateegiline plaan, mis sisaldab riigiasutustes digitaalallkirja juurutamise võimalikke lahendusvariante ning vajalikke samme nende elluviimisel.

Strateegilise plaani koostamisel on silmas peetud, et digitaalallkirja juurutamine riigiasutustes peab toetama riigiasutuste põhitegevusi ning olema ette nähtud

- avalike teenuste osutamise protsessi mugavamaks ning kvaliteetsemaks muutmiseks kasutajatele/kodanikele;
- riigiasutuste teenuste osutamise protsessi omahinna alandamiseks ning protsessi efektiivsemaks muutmiseks.

1.4 Kasutatud mõisted ja lühendid

Tagamaks ühest arusaama aruande tekstis kasutatavatest mõistetest ja akronüümidest on järgnevalt toodud digitaalallkirja rakendamisega seotud mõistete lühiseletused tähestikulises järjekorras. Juhul, kui mõiste on määratletud seadustes, on kasutatud seaduses toodud definitsiooni. Kui mingi probleemi selgitamisel on osutunud vajalikuks mõnevõrra teistsugune käsitlus, siis on seda ka vastava mõiste juures seletatud.

Aegumistähtaeg — hetk, mil aegub ja kustutatakse automaatselt *digitaalallkirja andmise vahendi* ja konkreetse *isiku* vaheline seos. Aegumistähtaeg määratakse kindlaks *isik-vahend seose* registreerimisel. Vajadus aegumistähtaja järele tuleneb vahendi seotusest moraalselt vananeda võiva

	tehnoloogiaga. Välistamaks situatsiooni, kus isikud kasutavad massiliselt moraalselt vananenud tehnoloogial baseeruvaid vahendeid, loetakse isik-vahend seos mingi fikseeritud ja mõistliku aja möödudes automaatselt kustunuks
Ajatempel	tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mis tõendab digitaaldokumendi või digitaalallkirja olemasolu kindlal ajahetkel. Ajatempli abil saab tõestada, et mingiks ajahetkeks oli digitaaldokument juba loodud. Ajatempel peab olema seotud digitaaldokumendiga sellisel viisil, mis välistab võimaluse tuvastamatult muuta digitaaldokumenti pärast ajatempli võtmist, st. mistahes muudatus digitaaldokumendis muudab eelnevalt võetud ajatempli kehtetuks. Ajatempli kinnitab ajatempliteenuse osutaja oma digitaalallkirjaga.
Ajatempliteenus	ajatemplite väljaandmine ja väljaantud ajatemplite kontrollimiseks tingimuste loomine. Kui eri ajatempliteenuse osutajate poolt väljaantud ajatemplite ajalist järgnevust ei ole võimalik kindlaks teha, loetakse need antuks üheaegselt. Ajatempliteenuse osutaja peab tagama, et oleks välistatud korrektse ajatempli väljaandmine selle taotlemise hetkest varasemale või hilisemale ajale või väljaantud ajatemplite järgnevuse muutmine. (vt. *ajatempel*)
Asutuse digitaalallkiri	Digitaalallkirja seadus sellist mõistet praegu ei käsitle, kasutatakse tähenduses "asutuse infosüsteemi poolt automaatselt (näiteks päringuvastusele) antud digitaalallkiri, mille eest vastutab asutuse juht (või mõni muu selleks volitatud isik)". Digitaalallkirja seaduse kontekstis võib seda vaadelda ka kui vastava isiku poolt antud digitaalallkirja. Asutuse digitaalallkirja võib kasutada, kui digitaaldokumendi saajale ei ole oluline mitte digitaaldokumendiga seotud füüsiline isik, vaid dokumendi pärinemine antud asutusest ning dokumendi ametlik staatus.
Autentimine	Arvutisüsteemi või arvutivõrgu (sealhulgas Interneti) kasutaja väidetud identsuse tuvastamine. Tuvastamiseks arvutisüsteemide omavahelise suhtluse korral võib kasutada spetsiifilisi krüptograafilisi protokolle, inimkasutaja autentimiseks võib arvutisüsteem nõuda näiteks parooli, aga võib rakendada ka kombineeritud meetmeid: ID-kaardiga autentimisel inimene sisestab kõigepealt ID-kaardi aktiveerimiseks vajaliku parooli, mispeale ID-kaart ja isiku identsust kontrolliv arvuti rakendavad spetsiifilisi krüptograafilisi protokolle.
DAS	Digitaalallkirja seadus, Eesti Vabariigis digitaalallkirja infrastruktuuri reguleeriv seadus
Digitaalallkiri	tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mida digitaalallkirja andja kasutab, märkimaks oma seost (mingi digitaalse) dokumendiga
Digitaalallkirja andmise vahend	tehniline seade (mis võib koosneda nii tarkvaralisest kui riistvaralisest osast), mille abil allkirja andja moodustab digitaalallkirja. Nimetatud tehnilisele seadmele on kaks vaadet. Esiteks koosneb seade materiaalsest osast ja immateriaalsest osast. Teiseks koosneb seade avalikust osast ja salajasest osast. Avalik osa võib olla kasutatav kõi-

	gile, kes seda kasutada saavad ja soovivad, salajane osa peab olema kasutatav vaid allkirja andjale. Vajadus salajase osa järele tuleneb otseselt tõestusfunktsioonist ja tuvastusfunktsioonist – kui vahendil puuduks salajane osa, siis võiksid kõik luua kõigi nimel digitaal-allkirju. Näitena võib allkirja andmise vahend olla isiklikku võtit sisaldav kiipkaart koos arvuti või seadmega, mis kiipkaarti kasutab. Allkirja andmise vahend võib olla ka näiteks personaalarvuti, millele on installeeritud vajalik tarkvara. Digitaalallkirja seadus nimetab digitaalallkirja andmise vahendiks ainult isiklikku võtit ehk vahendi immateriaalset salajast osa. Vahendi avalikku osa (avalikku võtit) nimetab seadus allkirja kontrollimise vahendiks Käesolevas aruandes on aga läbivalt digitaalallkirja andmise vahendiks nimetatud kogu vastavat tehnilist süsteemi, et probleemide käsitlustes oleks lihtsam anda üldisemaid vaateid. (Samas *digitaalallkirja vahendi registreerimisel* fikseeritakse tegelikult just seos isiku ja seaduse mõttes digitaalallkirja andmise vahendi vahel, aga see on ka ainus koht, kus sellel tasemel detailsus oluline on)
Digitaalallkirja andmise vahendi registreerimine	tegevus, mille käigus fikseeritakse isiku ja allkirja andmise vahendi immateriaalse salajase osa ehk isikliku võtme vaheline õiguslik seos, st registreerimise tulemusena muutub digitaalallkirja andmise vahend kehtivaks. Reeglina fikseeritakse registreerimisel ka tähtaeg, mille jooksul vahend on kehtiv (vt. *aegumistähtaeg*). Vahendi registreerimise hilisemaks tõestamiseks kasutatakse tavaliselt isiku omakäelise allkirjaga avaldust, milles on nii isikut kui ka vahendi salajast osa (isiklikku võtit) üheselt identifitseeriv teave
Digitaalallkirja kontrollimine	protseduur, mille käigus digitaalallkirja kontrolliv isik tuvastab, kas dokumendi digitaalallkiri on kehtiv st. varustatud korrektse kehtivus-tõendiga (vt. *digitaalallkirja kontrollimise vahend, kehtivustõend*)
Digitaalallkirja kontrollimise vahend	tehniline seade (mis võib koosneda nii tarkvaralisest kui riistvara-lisest osast), mis digitaalallkirja ja kehtivustõendi põhjal teeb kind-laks, kas digitaalallkiri on kehtiv. Digitaalallkirja seaduse mõttes on digitaalallkirja kontrollimise vahendiks vaid avalik võti, aruandes on aga jälle edasiste käsitluste üldisema taseme tagamiseks vaadeldud digitaalallkirja kontrollimise vahendina tehnilist seadet, mis võimaldab läbi viia digitaalallkirja kontrollimise protseduuri..
Digitaaldokument	digitaalsele teabekandjale jäädvustatud teave, mis on loodud või saadud isiku või asutuse tegevuse käigus ja mille sisu, vorm ja struktuur on küllaldane faktide või tegevuse tõestamiseks. Üldjuhul võivad kuuluda digitaaldokumendi juurde metaandmetena ka tema interpreteerimise reeglid (dokumendiformaadi kirjeldus).
Digitaaldokumendi arhiveerimine	tegevus, mis garanteerib digitaaldokumendi kättesaadavuse ettenäh-tud aja jooksul. Arhiiviseaduse [7] kohaselt on arhiveerimine arhi-vaalide korrastamine, kirjeldamine ja nende üleandmine arhiivi. Digi-taalsete arhivaalide korral ei pruugi arhiveerimisega seonduvad tege-vused lõppeda üleandmisega arhiivi, vaid tuleb tagada ka digitaalsete dokumentide tõestusväärtuse pikaajaline säilimine juhul, kui tõestus-

	väärtus on tagatud krüptograafiliste vahenditega.
Eraisik	residendist füüsiline isik, kes võib olla Eesti Vabariigi kodanik, elamisloaga mittekodanik või lihtsalt mittekodanik (vahetegemine on oluline, sest elamisloa omanikel on riigiga palju tihedam side).
Huvitatud pool	isik, kes on otseselt huvitatud digitaalallkirjaga dokumendi tõestusväärtusest ja selle säilitamisest. Näiteks võlakirja puhul on selleks võlausaldaja. Kui riigiasutus soovib põhimõttelist võimalust oma töötajat digitaalallkirja põhjal kohtusse kaevata, siis on huvitatud pooleks vastav riigiasutus
Isik	füüsiline või juriidiline isik
Isik-Vahend seos	digitaalallkirja andmise vahendi registreerimise teel tekkiv juriidiline seos isiku ja digitaalallkirja andmise vahendi vahel. Tegelikkuses luuakse seos allkirja kontrollimise vahendi ja isiku vahel. Kuna allkirja kontrollimise ja allkirja andmise vahendi vaheline seos ei ole praktiliselt võltsitav, siis eksisteerib läbi selle seose kaudne seos ka isiku ja allkirja andmise vahendi vahel. (vt. *isik, allkirja andmise vahend, allkirja kontrollimise vahend*)
Kehtivustõend	digitaaldokument, mida (kohtu)praktika loeb piisavaks tõendiks, et selle esitamisel digitaalallkirja kehtivuse üle toimuva vaidluse[1] käigus läheks vastupidise tõestamise kohustus üle digitaalallkirja väidetavale andjale. DAS-i järgi piisab tõendamisest, et (1) digitaalallkiri oli antud isiku nimele registreeritud vahendiga ja (2) see vahend ei olnud digitaalallkirja andmise hetkel ei peatunud ega kehtetu. Kehtivustõendi ülesanne ei ole tõestada, et digitaalallkirja väidetav andja ka tegelikult digitaalallkirja andis, vaid näidata, et digitaalallkiri rahuldab fikseeritud nõuete komplekti [näiteks (1) ja (2)].
PKI	PKI (ingl.k *Public Key Infrastructure)* teenuse osutamiseks vajalike infrastruktuursete vahendite komplekt (avaliku võtme infrastruktuur)
PKI teenus	teenus mis võimaldab (1) isikutel registreerida ja tühistada oma digitaalallkirja andmise vahendeid; (2) huvitatud pooltel saada usaldusväärset (ja tõendina kasutatavat) teavet digitaalallkirja andmise vahendite kehtivusest (vt. *kehtivustõend*)
Registriväljavõte	digitaaldokument, mis moodustatakse automaatselt väljavõttena digitaalsest andmebaasist (registrist)
Sertifikaat	digitaaldokument, milles allkirja andmise vahend seotakse üheselt füüsilise isikuga. Sertifikaat on üks võimalikke isik-vahend seose esitusi. (vt. *isik-vahend seos*)
Sertifitseerimisteenus	digitaalallkirja andmiseks vajalike sertifikaatide väljaandmine, sertifikaatide alusel antud digitaalallkirjade kontrollimise võimaldamine ning sertifikaatide kehtivuse peatamise, kehtivuse peatatuse lõpetamise ja kehtetuks tunnistamise menetlemine. (vt. *sertifikaat*)
SRR	sertifitseerimisteenuse osutajate riiklik register - riiklik register, mis peab arvet sertifitseerimisteenuse osutajate ja ajatempliteenuse osuta-

[1] Vaidlus toimub huvitatud poole ja digitaalallkirja väidetava andja vahel.

	jate üle, tagab erinevate ajatempliteenuse osutajate ajatemplite võrreldavuse ning täidab ka muid talle seadusega pandud funktsioone
STO	sertifitseerimisteenuse osutaja (vt. *sertifitseerimisteenus*)
Terviklusfunktsioon	digitaalallkirja üks põhifunktsioone, mis seisneb võimes tagada, et peale digitaalset allkirjastamist ei saa digitaaldokumenti muuta ilma digitaalallkirja muutmata. Terviklusfunktsiooni täitmine tagatakse krüptograafilise koodiga, mis arvutatakse lähtuvalt dokumendi sisust ja digitaalallkirja andja valduses olevast salajasest võtmest.
Toiminguteks pädev isik	Isik, kellel on ametikohustustest tulenevalt õigus asutuse nimel teatud toiminguteks. Näiteks välja anda teatud sisuga dokumente.
Tõestusfunktsioon	allkirja üks põhifunktsioone, mis seisneb allkirja võimes tõestada allkirja andja soovi allkirja anda (lad. *animus signandi*). Arvutisüsteemi nõrkusi ära kasutades võib põhimõtteliselt olla võimalik digitaalallkirja perfektne võltsimine jälgi jätmata, mistõttu digitaalallkirja tegelikku andjat ei ole praktikas võimalik tõestada. Seetõttu realiseeritakse digitaalallkirja tõestusfunktsioon kaudsete meetoditega: lepitakse kokku ühtsed (tehnilised ja organisatsioonilised) kriteeriumid, mille kehtides loetakse isiku digitaalallkiri "kehtivaks". Kui nimetatud kriteeriumidele vastav digitaalallkiri esitatakse kohtuvaidluse käigus tõendina isiku (kui allkirja väidetava andja) vastu, siis läheb vastupidise tõestuskohustus (vt. *tõestuskohustus*) üle nimetatud isikule
Tõestuskohustus	(lad. *onus probandi*) - kohustus esitada (näit. kohtuvaidluse käigus) tõendeid oma väite kehtivuse toetuseks. Kohtuvaidluses osapoolte vahel esitab üks osapool, kellel on antud hetkel tõestuskohustus, mingid tõendid, mille piisavuse korral, vastavalt kohtumenetluse reeglitele ja traditsioonidele, toimub vastupidise tõestuskohustuse üleminek teisele osapoolele
Tõestusväärtus	dokumendi väärtus, mis tuleneb otseselt tema tõestusfunktsioonist. Näiteks võlakirja (või esitajaobligatsiooni) tegelik väärtus võlausaldaja (vastavalt obligatsiooni esitaja) jaoks seisneb selles, et tõestusfunktsiooni kaudu saab dokumendi tõestusväärtust teisendada rahaliseks väärtuseks
Tühistus	tegevus, mille käigus katkeb õiguslik seos isiku ja digitaalallkirja andmise vahendi vahel. Pärast tühistust antud digitaalallkirju ei seostata enam isikuga (tühistatud vahendiga antud digitaalallkirjad ei too enam kaasa õiguslikke tagajärgi). Tühistus on vajalik isiku ja digitaalallkirja andmise vahendi õigusliku seose lõpetamiseks enne vahendi kehtivuse tähtaja lõppemist näiteks juhul, kui isik mingil põhjusel kaotab usu vahendi turvalisusesse ja usaldatavusse või kui vahend on muutunud isiku jaoks kasutuskõlbmatuks (näiteks kiipkaart on hävinenud)
Valideerimisteenus	teenus, mis (1) registreerib sertifikaatide tühistusavaldusi, mis tulevad digitaalallkirja andjalt; (2) vastab huvitatud osapoolelt tulevale (paarina digitaalallkiri/sertifikaat esitatud) kehtivuspäringule, saates vastu kinnituse, et valideerimisteenuse osutaja on päringu kätte saanud ja et päringus viidatud sertifikaat ei olnud enneaegselt tühistatud päringu kättesaamise hetkel (vt. *sertifikaat*). DAS järgi on validee-

	rimisteenuse osutamise kohustus sertifitseerimisteenuse osutajatel.
Äriühing	äriregistris või mõne teise riigi analoogilises asutuses registreeritud juriidiline isik

1.5 Viited seonduvatele dokumentidele

1. Avaliku teenistuse seadus (RT I 1999, 7, 112)
2. Digitaalallkirja seadus (RT I 2000, 26, 150)
3. Asjaajamiskorra ühtsed alused (Vabariigi Valitsuse 26.02.2001.a. määrus nr. 80, RT I 2001, 20, 112)
4. Avaldustele vastamise seadus (RT I 1994, 51, 857)
5. Avaliku teabe seadus (RT I 2000, 92, 597)
6. Andmekogude seadus (RT I 1997, 28, 423)
7. Arhiiviseadus (RT I 1998, 36, 552)
8. Arhiivieeskiri. Vabariigi Valitsuse 29.12.1998.a. määrus nr.308. (RT I 1998, 118, 1904)
9. Riigi Teataja seadus (RT I 1999, 10, 155)
10. Riigihanke kood 0460 "Avalike teenistujate andmebaas" dokumendid: Lisa 1. Avalike teenistujate andmebaasi andmemudel, AS Assert, 08.05.1999, Lisa 2. Infosüsteemi kantavad andmed (andmekoosluse täiendav nimekiri).
11. Isikut tõendavate dokumentide seadus (RT I 1999, 25, 365)
12. Tehnilise normi ja standardi seadus (RT I 1999, 29, 398)
13. ESTEID sertifitseerimispoliitika. Nõuded Eesti Vabariigi siseriiklikule isikutunnistusele digitaalallkirja ja isikutuvastust võimaldavate sertifikaatide väljastamiseks ja teenindamiseks. (Projekt. Versioon 1.1.)
14. Kohtutäituri seadus (RT I 2001, 16, 69)
15. Pankrotiseadus (RT I 1997, 18, 302)
16. Notariaadiseadus (RT I 2000, 194, 684)
17. Advokatuuriseadus (RT I 2001, 36, 201)
18. Riigi- ja kohaliku omavalitsuse asutuste riikliku registri pidamise põhimäärus, kinnitatud Vabariigi Valitsuse 07.12.1999.a. määrusega nr.371 (RT I 1999, 92, 82)
19. Äriseadustik (RT I 1998, 91, 1500)
20. Haldusmenetluse seadus (RT I 2001, 58, 354)
21. Riigivastutuse seadus (RT I 2001, 47, 260)

1.6 Muud viited

22. Valdo Praust. Digitaalallkiri. Tee paberivabasse maailma. Ilo, Tallinn 2001.
23. EV ST 3-92 Haldusdokumentide vormistamise põhinõuded
24. Margus Freudenthal. Isiklikud turvakeskkonnad. Magistritöö, Tallinna Tehnikaülikool, 2001. (vt. http://www.cyber.ee/research/publications.html)

25. Arne Ansper "e-Riigist andmeturbe seisukohalt". Magistritöö, Tallinna Tehnikaülikool, 2001. (vt. http://www.cyber.ee/research/publications.html)
26. E-kodaniku projekt http://www.riik.ee/ekodanik
27. X-tee projekt http://www.riik.ee/ristmik
28. E-maksuameti projekti info http://www.ma.ee/ema/
29. Riigikassa e-teenused http://www.fin.ee/files/abi_kb_aasta.htm
30. E-õigus http://www.just.ee/oldjust/e_oigus/eoigus.html
31. E-maakond http://emaakond.rae.ee/
32. Dokumendihalduse programm http://www.riik.ee/dh/ylevaade/
33. ID kaardi spetsifikatsioonid http://www.id.ee/esteid/
34. Riiklike institutsioonide infosüsteemi juhend http://www.riik.ee/ab/help/help.html
35. Riigi ja kohalike omavalituse asutuste register http://www.fin.ee/pages.php/0107130503
36. Arne Ansper, Ahto Buldas, Meelis Roos, Jan Willemson, "Efficient long-term validation of digital signatures".September 19, 2000. http://www.cyber.ee/research/publications.html
37. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

    http://www.qlinks.net/comdocs/elsig/

2. Digitaalallkirja rakendamine riigiasutustes

Digitaalallkirja seadus kehtib Eesti Vabariigis juba ligi aasta, ent digitaalallkirja tegelik rakendamine ei ole veel märkimisväärselt käivitunud, kuna nõuab küllalt põhjalikku eeltööd. Ministeeriumidevaheline ühisprojekt toetamaks digitaalallkirja rakendamist avalikus sektoris on käivitatud kaheetapilisena:

1.etapp - digitaalallkirja rakendamise strateegilise plaani koostamine;

2.etapp - strateegilise plaani juurutamine piiratud arvus ministeeriumides.

Projekti 1. etapi tulemusena töötatakse välja **digitaalallkirja rakendamise strateegia** riigiasutustes, selle rakendamise taktikaline plaan ja detailne ajakava ning ressursivajaduste hinnang. Töö käigus on plaanis koordineerida valdkonnaga seotud tegevusi ühisprojekti osapoolte teistes projektides, sealhulgas X-tee, DHP, ID-kaart ja sertifitseerimisteenuste osutamine.

Projekti 2. etapi eesmärgiks on **digitaalallkirja rakendamise plaani realiseerimine**, mille käigus loodetakse teostada vähemalt alljärgnev:

- määratleda riigiasutuste sertifitseerimisteenuse ja ajatempliteenuse kasutamise protseduurid, sealhulgas vajadusel teenuseosutaja valimine, teenuste tarnimine ja kvaliteedi kontroll;
- defineerida digitaalallkirja tehniline profiil ning määratleda selle kasutamise erinevad stsenaariumid lähtuvalt majanduslikust ja juriidilisest otstarbekusest;
- koordineerida erinevates valdkondades toimuvaid digitaalallkirja juurutamise projekte, s.h. tagada vajalike tehniliste kokkulepete väljatöötamine (nt sertifikaadi formaat, rollide kasutamine, turvanõuded jne);
- korraldada digitaalallkirja valdkonna komponentide nõudmiste süstematiseerimine ning dokumenteerimine (vajadusel standardimine ning õigusaktide täiendamine ja ettevalmistamine). See peab tagama ühildavuse ning läbipaistvuse vähemalt alljärgnevates dokumentide vahetuse kanalites:
  - riigiasutuse sisemine dokumendivahetus;
  - riigiasutustevaheline dokumendivahetus;
  - kodaniku ja riigi vaheline dokumendivahetus;
  - eraõigusliku juriidilise isiku ja riigi vaheline dokumendivahetus;

Järgnev analüüs annab ülevaate digitaalallkirja juurutamisel käsitlemist vajavatest probleemidest, et nende põhjal püstitada adekvaatseid strateegilisi eesmärke.

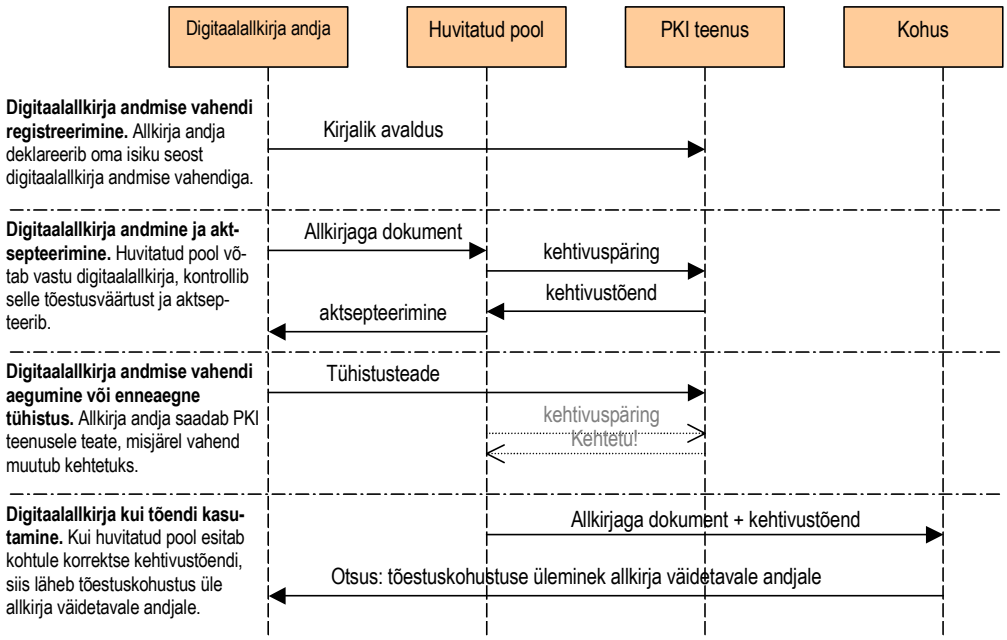
2.1 Digitaalallkirja elutsükkel

Digitaalallkiri on tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum märkimaks allkirjastaja seost digitaaldokumendiga. Digitaalallkirja andmiseks on allkirjastada soovival isikul vaja digitaalallkirja andmist võimaldavat vahendit. Digitaalallkirja andmise vahend on tehniline seade, mille abil digitaalallkirja andja moodustab digitaalallkirja.

Lisaks digitaalallkirja andmise vahendile on digitaalallkirja kasutamiseks vaja spetsiifilisi teenuseid, mis võimaldavad kasutajatel registreerida/tühistada digitaalallkirja andmise vahendit, kontrollida teiste poolt antud digitaalallkirjade kehtivust, hoida alal digitaalallkirja tõestusväärtust jne.

Digitaalallkirja üldises kasutusstsenaariumis võib eristada järgmisi etappe (Joonis 1):

- *Digitaalallkirja andmise vahendi registreerimine*, mille käigus tuvastatakse isik ning fikseeritakse isiku ja digitaalallkirja andmise vahendi seos. Näiteks võib seda teha isikut tõendava dokumendi ning kirjaliku avalduse esitamisega PKI teenuse osutajale. Avalduses peab olema nii isikut kui ka digitaalallkirja andmise vahendit üheselt identifitseeriv teave, sest vastasel korral ei oleks isiku ja digitaalallkirja andmise vahendi seos tõestatav.
- *Digitaalalllkirja andmine ja aktsepteerimine*, mille käigus (1) digitaalallkirja andja moodustab digitaalallkirja andmise vahendi abil dokumendile digitaalallkirja, (2) huvitatud pool kontrollib PKI teenuse osutajalt digitaalallkirja andmise vahendi kehtivust ja positiivse vastuse – kehtivustõendi – saamise korral aktsepteerib allkirja. Kehtivustõend ise peab olema kasutatav ka tulevikus, st tema tõestusväärtus ei tohi muutuda. Vastasel korral ei saaks huvitatud osapool allkirja aktsepteerida, sest puudub garantii allkirjastatud dokumendi tegeliku väärtuse kohta.
- *Digitaalallkirja andmise vahendi aegumine või enneaegne tühistus*. Digitaalallkirja andmise vahendeid ei registreerita üldiselt tähtajatult, st on fikseeritud mingi kindel tähtaeg, mil vahendi kehtivus lõpeb ning hiljem selle vahendiga antud digitaalallkirjad on kehtetud. On võimalik, et digitaalallkirja andmise vahendi kehtivus tuleb enne-tähtaegselt lõpetada. Lõpetamise aluseks võib näiteks olla vahendi volitamatu kopeerimise kahtlus ja isiku vastavasisuline avaldus (tühistusteade), mis saadetakse PKI teenuse osutajale. Aegumine ja tühistuse võimalikkus on kaitsemehhanism eelkõige isiku enda huvides, mis osaliselt piirab digitaalallkirja andmise vahendi volitamatust kasutusest tulenevat ebaõiglast vastutust.



Joonis 1. Digitaalallkirja kasutamise üldine skeem.

- *Digitaalallkirja kui tõendi kasutamine*. Huvitatud pool esitab näiteks kohtule digitaalallkirjaga dokumendi ja allkirja kehtivust kinnitava kehtivustõendi. Kohtunik kontrollib kehtivustõendi vastavust sellele tõendile kehtestatud nõuetele ning vastavuse korral läheb digitaalallkirja tegeliku kehtetuse tõestamise kohustus üle digitaalallkirja väide-

tavale andjale. Kuna huvitatud pool kontrollis tõendi korrektsust juba enne digitaalallkirja aktsepteerimist, siis on (ja peabki olema!) nõuetele vastavus huvitatud poolele juba ette teada, sest vastasel korral puuduks huvitatud poolel igasugune alus allkirja aktsepteerimiseks ja selle tõestusväärtusele lootma jäämiseks.

DAS järgi toimub tõestuskohustuse tingimusteta üleminek huvitatud osapoolelt isikule (allkirja väidetavale andjale), kui esitatakse:

(1) dokument, mis seob üheselt isiku ja allkirja andmise vahendi või viitab üheselt nende seotusele, näiteks isiku avaldus digitaalallkirja andmise vahendi saamiseks;

(2) tõendid, et digitaalallkirja andmise hetkel ei olnud vahend aegunud ega enneaegselt tühistatud.

Ainult tingimuse (1) nõudmine oleks ebaõiglane allkirja väidetava andja suhtes. Kui aga nõuda rohkem kui (1)+(2), näiteks ümberlükkamatut tõestust, et allkirja väidetav andja põhjustas tahtlikult sündmuste ahela, mille lõpptulemusena moodustus digitaalallkiri, siis oleksid nõudmised ilmselt ülekohtused huvitatud osapoole suhtes.

Piisavaks tõendiks ei saa pidada teenuseosutaja poolt välja antud digitaalset avaliku võtme sertifikaati, milles isikuandmed seotakse digitaalallkirja andmise vahendit üheselt identifitseeriva teabega (nn. avaliku võtmega), sest puudub objektiivne kinnitus, et sertifikaadis esitatud andmed vastavad tõele.

2.2 Digitaalallkirja kasutamisega seotud vahendid ja teenused

Käesolevas punktis antakse ülevaade digitaalallkirja andmise vahendite ja vajalike teenustega seotud üldistest probleemidest ja ohtudest.

2.2.1 Digitaalallkirja andmise vahendid

Digitaalallkirja andmise vahendile kui tehnilisele seadmele on kaks vaadet. Esiteks koosneb seade materiaalsest osast ja immateriaalsest osast. Teiseks koosneb seade avalikust osast ja salajasest osast.

Immateriaalne vahend eksisteerib inimestest sõltumatuna. Kasulikuks (käideldavaks) saab vahend läbi materialiseerumise (näiteks RSA võti paigutatakse kiipkaardile). Kui immateriaalset vahendit on ideaalis kerge saladuses hoida – võtame vahendi ja õpime selle endale pähe ja kellelegi ei ütle (välistame mõtete lugemise), siis materiaalse vahendiga on rohkem probleeme – seda tuleb kusagil säilitada ja ei ole teada hinnalt sobilikku tehnoloogiat, mis võimaldaks

- tagada materiaalse vahendi kättesaadavust ainult selleks volitatud isikutele;
- vältida informatsiooni kopeerimist ehk digitaalallkirja anamdise vahendi immateriaalse osa paljundamist tema materiaalse kandja vahendusel.

Tänapäeval ei tunta veel tehnoloogiat, mis lubaks luua kergesti päheõpitavat digitaalallkirja andmise vahendit, mistõttu tuleb kasutada teisi viise vahendi säilitamiseks, mis aga tekitab ohu, et vahend väljub volitatud valdaja kontrolli alt. Seda võimalust tuleb arvesse võtta ja eelnevalt kirjeldada protseduurid juhuks, kui kellegi vahend varastatakse või kopeeritakse.

Digitaalallkirja andmise vahend koosneb kahest osast – avalik ja salajane osa. Osad on seotud viisil, kus mõlemad määravad teineteist üksüheselt. Samas peab avalikust osast salajase osa tuletamine olema praktiliselt lahendamatu ülesanne (digitaalallkirjal on tõestus- ja tuvastusfunktsioon!). Samuti peab materiaalse vahendi avaliku osa abil (asutuse arvuti) immateriaalse vahendi salajase osa (RSA privaatvõti) teadasaamine olema praktiliselt lahendamatu ülesanne.

Näiteid digitaalallkirja andmise vahenditest:

- Lauaarvuti
- Arvuti ja kiipkaart
- Klaviatuuriga kiipkaart
- Pihuarvuti

Näide vaadetest digitaalallkirja andmise vahendile:

Allkirja andmise vahendi osa:	**Materiaalne**	**Immateriaalne (andmed)**
Salajane	Kiipkaart	RSA privaatvõti
Avalik	Kiipkaardilugeja	RSA avalik võti

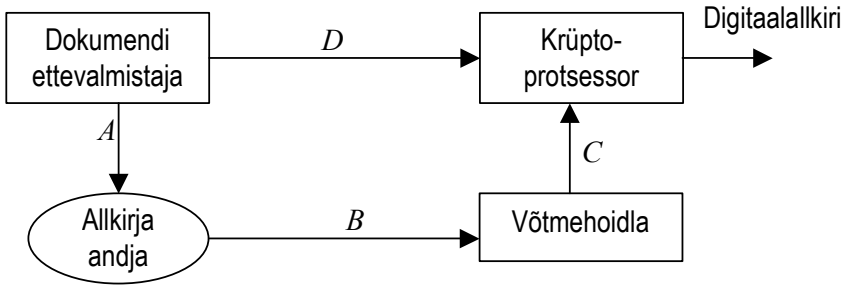
2.2.1.1 Digitaalallkirja andmise vahendi funktsionaalne struktuur.

Kõik peamised digitaalallkirja andmise vahendid koosnevad järgmistest funktsionaalsetest komponentidest:

Andmete ettevalmistaja — Seade, mis võimaldab (1) allkirja andjal tutvuda dokumenti sisuga, (2) teisendada allkirjastatav dokument digitaalallkirja andmiseks sobivasse formaati (näiteks krüptograafilise lühendi moodustamine)

Krüptoprotsessor — Seade, mille ülesanne on krüptograafiliste teisenduste teostamine

Võtmehoidla — Seade, mille ülesanne on turvaliselt hoida signeerimiseks kasutatavat salajast võtit.



Joonis 2. Digitaalallkirja andmise vahendi üldine loogiline struktuur.

Digitaalallkirja moodustamine ise koosneb järgmistest etappidest (vt Joonis 2):

A. Digitaalallkirja andja tutvub allkirjastatava dokumendiga, kui see on sobiv, siis:
B. Digitaalallkirja andja annab võtmehoidlale käsu väljastada võti.
C. Võtmehoidla edastab krüptoprotsessorile võtme.
D. Ettevalmistatud dokument edastatakse krüptoprotsessorile ja toimub digitaalallkirja moodustamine.

2.2.1.2 Ohuanalüüs.

Digitaalallkirja andmise etappidel toimuvas infoedastuses esinevad ohud (vt Joonis 2):

A. Dokumendi modifitseerimise oht. Kui digitaalallkirja andjale näidatakse muudetud teksti, siis on võimalik, et digitaalallkiri antakse sõnumile, mida allkirja andja tegelikult ei soovinud allkirjastada.

B. Infolekke oht. Võtmehoidlale edastatav käsk sisaldab tavaliselt salajast parooli, mis on mõeldud võtme kaitseks volitamata isikute eest. Parooli teadasaamisest piisab, et edaspidi anda käske digitaalallkirjade moodustamiseks, eeldusel, et krüptoprotsessor ja võtmehoidla on vähemasti "musta kastina" olemas. Kui aga kasutada on eraldi võtmehoidla, siis on võimalus ka võtme lekkeks.

C. Infolekke oht. Võtme leke võimaldaks volitamata isikul piiramatult digitaalallkirju võltsida.

D. Dokumendi modifitseerimise oht. Kui digitaalallkirja andjale näidatakse üht sõnumit (etapp A) ja allkirjastamiseks antakse modifitseeritud sõnum, siis on võimalik, et digitaalallkiri antakse sõnumile, mida allkirja andja tegelikult ei soovinud allkirjastada.

Komponentide valdusega seotud ohud:

- *Andmete ettevalmistaja* – osapool, kelle valduses see komponent on, saab modifitseerida infot etappidel A ja D, st tal on võimalus allkirjastada õige sõnumi asemel mingi muu sõnum.
- *Krüptoprotsessor* – osapool, kelle valduses see on, saab juurdepääsu võtmele ja seega võimaluse piiramatult digitaalallkirju moodustada.
- *Võtmehoidla* – osapool, kelle valduses see on, saab juurdepääsu etapil B edastatavale paroolile ja samuti etapil C edastatavale võtmele ning seega võimaluse piiramatult digitaalallkirju moodustada.

2.2.1.3 Struktuur valdamise järgi.

Eeldame, et digitaalallkirja andmise vahendi komponendid võivad olla mitme erineva osapoole valduses. On otstarbekas jagada osapooled järgmistesse klassidesse:

- *Digitaalallkirja andja* ise.
- *Usaldatud osapooled* – osapooled, kelle kohta võib kindlalt väita, et nad ei saa kunagi olema huvitatud osapoole rollis antud digitaalallkirja mõttes, st nende huvid pole digitaalallkirja kehtivuse mõttes kunagi vastandlikud allkirja andjaga.
- *Muud osapooled* – osapooled, kes võivad olla huvitatud osapoole rollis, st need osapooled, kelle kohta ei saa kindlalt väita, et nad on usaldatud osapoole rollis.

Digitaalallkirja andmise vahend ei ole peaaegu kunagi digitaalallkirja andja täieliku kontrolli all – kasutatakse aparatuuri ja programme, mis on loodud kolmandate isikute poolt ja mille siseehitust allkirja andja ei tea (ega saaks teadmise korral ka enamasti sellest aru). Seetõttu on alati olemas põhimõtteline oht, et kolmandatel osapooltel on võimalik allkirja andmise vahendit kasutada ka ilma vahendi omaniku teadmata.

See oht ei ole kuigi suur, kui nimetatud kolmandad isikud on digitaalallkirja kehtivuse üle toimuvas vaidluses neutraalsed. Kui aga üks nimetatud kolmandatest isikutest langeb kokku hu-

vitatud osapoolega[2], siis avaneb allkirja väidetaval andjal juba tõsine võimalus väita, et allkirja andmise vahendit on kuritarvitatud – motiiv väärkasutuseks oleks siis täiel määral olemas.

Näiteks kui digitaalallkirja andmine toimub personaalarvutis, siis nimetatud kolmandate isikute all võivad kõne alla tulla järgmised:

(1) Protsessoreid ja muid arvuti komponente tootvad ettevõtted.

(2) Arvuti baastarkvara (operatsioonisüsteem, tekstiredaktorid jms) tootvad ettevõtted.

(3) Arvuti tema omanikule müünud firma.

(4) Arvuti omanik ja seda arvutit hooldavad isikud, kes ei tarvitse kokku langeda digitaalallkirja väidetava andjaga.

(5) Teised arvutile ligipääsu omavad isikud.

Digitaalallkirja väidetaval andjal on põhimõtteliselt võimalik digitaalallkirja andmise eitamiseks viidata ükskõik millisele nimetatud võimalustest, kuid võimalused (1) – (3) ei tule tõsiselt arvesse olukordades, kus neis nimetatud isikutel puudub otsene nähtav seos allkirja andjaga ja ka allkirja võltsimise motiiv st. (1) – (3) võib pidada usaldatud osapoolteks. Riist- ja tarkvarafirmade süüdistamist konkreetse digitaalallkirja võltsimises on lihtne pareerida, uurides firmade toodete teisi eksemplare. Kui neis kahtlasi jälgi ei leita, puudub igasugune alus kinnituseks, et just antud isikule müüdud arvutisse oli suurtootjate poolt sisse ehitatud vajalik "tagauks".

Hoopis teine lugu on aga võimalustega (4) ja (5), mis tulevad arvesse näiteks siis, kui vaidlusaluse digitaalallkirja moodustas asutuse töötaja oma tööarvutis ja kui huvitatud osapool on asutus. Näiteks kui Maksuamet püüab süüdistada oma töötajat, kasutades tõendina töötaja poolt (väidetavalt) antud digitaalallkirja. Sel juhul on töötajal täielik alus väita, et allkirja andmise vahend ei olnud tema kontrolli all ja et kontrolli alt väljumine ei olnud põhjustatud tema kuritahtlikust hooletusest. Seaduse järgi saab allkirja väidetav andja enda kaitseks kasutada üksnes DAS 3 lõiget 4,

> (4) Digitaalallkirja andmine ilma vastava sertifikaadi omaniku nõusolekuta loetakse tõendatuks, kui sertifikaadi omanik tõendab asjaolud, mille esinemisel võib eeldada, et allkiri anti tema nõusolekuta.

mis ei ole oma väljaütlemiselt piisavalt selge ja töötaja poolt esitatud ja tõestatud faktid [(1) Vahend ei olnud tema kontrolli all, (2) kontrolli alt väljumine ei olnud põhjustatud allkirja väidetava andja kuritahtlikust hooletusest, vaid hoopis tema töö iseloomust] ei tarvitse olla piisavad, et nimetatud paragrahv rakenduks. Siiski oleksid esitatud tõendid (arvestades ka tööandja võimalikku motiivi) piisavad selleks, et tekitada allkirja kehtivuse küsimuses täielikku määramatust.

Seega peaks segaduste ära hoidmiseks vältima olukordi, kus digitaalallkirja andmise vahendi üle omab osalist või täielikku kontrolli kolmas isik, kes teatud olukordades võib olla nimetatud vahendiga antud allkirjade kehtivuse üle toimuvates vaidlustes huvitatud pooleks.

Sellest aspektist ei muuda midagi ka süsteem, kus asutuse töötaja kasutab digitaalallkirja andmiseks kiipkaarti, st kui allkirja andmise vahend koosneb kiipkaardist ja tööarvutist. Kui tööarvuti on kolmanda isiku (tööandja) kontrolli all, siis on seda samavõrd ka arvutisse sisestatud kiipkaart, ehkki viimast saab tööandja kuritarvitada ainult siis, kui see on sisestatud arvutisse. Vajaliku ründetarkvara loomine ei ole seotud märkimisväärsete kuludega ja on jõu-

[2] Näiteks kui allkirja andmise vahend on allkirja väidetava andja tööarvuti ja huvitatud osapool on tööandja.

kohane pea igale arvuti alal ülikooli lõpetanud inimesele. Saab luua ka ründetarkvara, mis peale arvutisse sisestatud kiipkaardi kuritahtlikku kasutamist (allkirjastab töötaja nimel dokumendi, mida töötaja ise ei soovinud allkirjastada) kustutab nii ennast kui kõik oma tegevuse jäljed (olles eelnevalt saatnud võltsallkirja vajalikule adressaadile).

Kodune personaalarvuti allkirja andmise vahendina on palju loomulikum konstruktsioon, kui tööandja arvuti vastavas rollis. Koduarvutit on kodanikul vabadus hankida ükskõik milliselt arvutifirmalt ja lasta seda hooldada neil, keda ta ise usaldab. Tööandja arvutiga selline võimalus enamasti puudub. Kiipkaardi kasutamine ei anna midagi olulist juurde ka koduarvutis digitaalallkirja moodustamisele.

2.2.2 Digitaalallkirja kontrollimise vahendid

Digitaalallkirja kontrollimine on protseduur, kus lähteandmete (Dokument, Digitaalallkiri, Kehtivustõend) põhjal otsustatakse (seda teeb Huvitatud pool), kas digitaalallkiri on aktsepteeritav.

Ideaalis peaks aktsepteeritavus tähendama seda, et digitaalallkirja ja kehtivustõendi ettenäitamisel läheks tõestuskohustus üle digitaalallkirja väidetavale andjale. Praktiliselt pole aga selline üleminek vahetult võimalik, sest digitaaldokument ei saa kunagi tõestada allkirja väidetava andja osalemist allkirja andmise protsessis. Seetõttu toimub tõestuskohustuse üleminek sammhaaval "kõrgemast instantsist" (SRR) vahepealsele (STO) ja seal edasi "madalaimale" – digitaalallkirja väidetavale andjale.

Digitaalselt allkirjastatud dokumendiga varustatud isik:

(1) ei tarvitse olla allkirjastaja ise,

(2) ei tarvitse olla huvitatud allkirjastatud dokumentidega seotud turvanõuete täitmisest,

(3) võib soovida võltsida allkirja või modifitseerida dokumenti,

(4) ei tarvitse ise omada digitaalallkirja andmise vahendit.

See isik võib pidada vajalikuks digitaalselt allkirjastatud dokumendi sisuga tutvumist ja allkirja kontrollimist.

Digitaalselt allkirjastatud dokumendi sisuga tutvumise eelduseks on, et digitaalselt allkirjastatud dokumendist on võimalik eraldada esialgne dokument sellisel kujul, nagu ta oli allkirjastamise hetkel. Teiseks eelduseks on, et erinevate formaatide olemasolu korral on sisuga tutvuda soovivale isikule loodud võimalus vaadelda erinevates formaatides olevaid digitaalselt allkirjastatud dokumente. Käsitlemist vajavaks probleemiks on see, kuidas tagada ühtne interpreteerimine mõlemal poolel – nii allkirjastaja kui ka sisuga tutvuja poolel.

Kontrollimise järel võib isik allkirja aktsepteerida või mitte aktsepteerida. Mitteaktsepteerimise põhjuseks võib olla näiteks see, et antud sisu ja allkirja vahelise seose kehtivust ei olnud võimalik kontrollida, või ei olnud võimalik kontrollida, et antud vahendit oli allkirja andmiseks kasutatud siis, kui eksisteeris seos vahendi ja väidetavalt allkirjastanud isiku vahel. Mitteaktsepteerimise põhjuseks võib olla ka turvanõuetele mittevastamine või siis kontrollija soov antud allkirja mitte aktsepteerida.

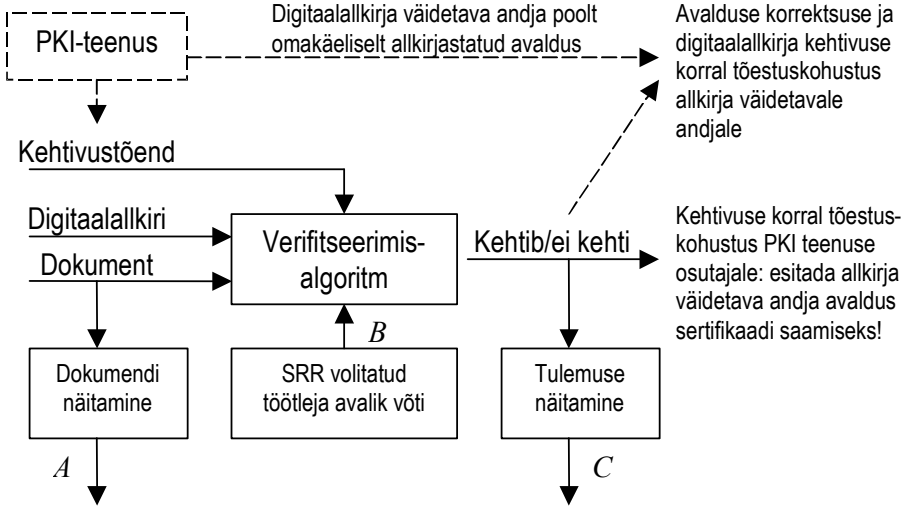
Asjaolust, et digitaalallkirja kontrollija või allkirjastaja ise võib tahta digitaalallkirja mitte aktsepteerida ka siis, kui kõik nõuded on täidetud, tuleneb, et allkirja tõestusfunktsiooni täitmiseks tuleb tagada see, et ei digitaalallkirja ega temaga seotud turvaatribuute ei oleks kellelgi võimalik muuta ilma digitaalallkirjaga dokumenti ennast kehtetuks tegemata. Kui atribuute muuta nii, et digitaalallkirjaga dokument muutub kehtetuks, ei saa huvitatud osapool digitaal-

allkirja oma huvides kasutada. Seega peab huvitatud osapool hoolitsema digitaalallkirja ja tema tõestusväärtuse säilimise eest.

2.2.2.1 Digitaalallkirja kontrollimise vahendi funktsionaalne struktuur

Kõik digitaalallkirja kontrollimise vahendid saab mahutada järgmisesse loogilisse struktuuri, kus on kasutatud mõisteid järgmises tähenduses:

Dokumendi näitamine	kasutajale näidatakse dokumendi sisu
Sertifitseerimise Riikliku Registri avalik võti	SRR avalik võti, mis on salvestatud mingisse võtmehoidlasse, kas tarkvaralisse või riistvaralisse. Oluline, et seda võtit ei saaks volitamatult muuta
Verifitseerimisalgoritm	arvutiprogrammina või riistvaraliselt realiseeritud algoritm, mis digitaalallkirja ja kehtivustõendi põhjal otsustab, kas digitaalallkiri on kehtiv
Tulemuse näitamine	Tehniline meetod, kuidas kasutajale näidatakse digitaalallkirja kontrollimise tulemust (kehtib/ei kehti)



Joonis 3. Digitaalallkirja kontrollimine (punktiiriga lisatud võimaliku vaidluse käik).

A. Huvitatud osapool tutvub dokumendi sisuga. See ei pruugi tingimata olla dokumendi kuvamine inimkasutajale, vaid võib olla automaatne kontroll mingi seadme poolt.

B. Verifitseerimisalgoritm hangib Sertifitseerimise Riikliku Registri avaliku võtme autentse koopia ja arvutab kolmiku (Dokument, Digitaalallkiri, Kehtivustõend) põhjal välja verifitseerimistulemuse (kehtib/ei kehti).

C. Tulemus esitatakse huvitatud osapoole jaoks loetaval kujul. See ei tähenda tingimata loetavust inimese jaoks.

DAS raames saab PKI-teenusele tõestuskohustust tekitada üksnes digitaalallkirja abil. Seega peab PKI-teenuse poolt välja antud avaliku võtme sertifikaadil olema tõestusväärtusega digitaalallkiri, st

(1) peab saama dokumentaalselt tõestada, et teenuse osutaja digitaalallkirja andmise vahend on ametlikult registreeritud;

(2) peab olema esitatud tõestus, et teenuse osutaja vahend ei olnud tühistatud hetkel, mil sertifikaat välja anti.

Tõestust ei pea iga digitaalallkirja jaoks eraldi hankima, see võib alati sertifikaadiga kaasas käia.

Punktis (2) mainitud tõestuse andmiseks kasutatav valideerimisteenus ei saa olla PKI teenuse osutaja enda poolt osutatav PKIX-tüüpi ajatempliteenus, sest siis oleks PKI-teenusel võimalik üsna lihtsal viisil loobuda igasugusest vastutusest välja antud sertifikaatide eest – ta tühistab nii sertifikaatide väljaandmiseks kasutatud võtme kui ka ajatempliteenuse osutamiseks kasutatava võtme, misjärel puudub igasugune võimalus teenuse osutaja õiguslikuks seostamiseks tema välja antud sertifikaatidega.

2.2.2.2 Struktuur valdamise järgi

Osapooled võib ka siin jagada kolmeks:

- *Huvitatud pool* - osapool, kes on huvitatud digitaalallkirja õigsusest ja kokkuvõttes digitaalallkirjaga dokumendi tõestusväärtusest
- *Usaldatud osapool* – osapool, kellel digitaalallkirja õigsuse küsimuses ei ole vastandlikke huvisid huvitatud osapoolega, st paralleelseid huvisid allkirja andjaga.
- *Muud osapooled* – osapooled, kellel võib olla digitaalallkirja õigsuse küsimuses vastandlikke huvisid huvitatud osapoolega.

2.2.2.3 Ohuanalüüs.

Kui sammul A ei näidata dokumendi sisu õigesti, siis võib juhtuda, et allkirja verifitseerimise positiivne tulemus kehtib hoopis mingi teise sisuga dokumendi kohta. Seega, kui mingi osapool saab aktiivselt sekkuda allkirja kontrollimisse sammul A, siis tegelikult on tal võimalik panna huvitatud osapoolt aktsepteerima mistahes dokumenti, st tekitada mulje, nagu dokumendil oleks kehtiv digitaalallkiri, mis aga tegelikult on antud hoopis teistsuguse sisuga dokumendile.

Kui osapool saab muuta SRR-i volitatud töötleja avalikku võtit, siis saab ta põhimõtteliselt ise välja anda uusi sertifikaate ja tekitada "aktsepteeritavaid" allkirju mistahes dokumentidele, mis aga tegelikult ei oma mingit õiguslikku katet ja seetõttu puudub neil igasugune riskide maandamise funktsioon.

Kui osapool saab aktiivselt sekkuda allkirja verifitseerimise tulemuse näitamise protseduuri, siis on tal võimalik panna huvitatud osapoolt aktsepteerima allkirju mistahes dokumentidel. Seega:

Digitaalallkirja turvaliseks verifitseerimiseks peavad sammud A, B ja C olema täielikult üksnes huvitatud osapoole enda või siis usaldatud osapoolte valduses.

2.2.3 Sertifitseerimisteenus

Digitaalallkirja andmise vahendi avaliku ja salajase osa seotus tagab, et avaliku osa abil on võimalik teha kindlaks, kas mingi isiku valduses on konkreetne salajane osa. Seeläbi on võimalik luua seos digitaalallkirja ja mingi vahendi salajast osa valdava isiku vahel.

Seos isiku ja digitaalallkirja andmise vahendi vahel ei ole ei vahendi ega isiku põhjal üksüheselt tuletatav. Siit tuleb vajadus vahendi registreerimise järele. Registreerimine toimub vasta-

va institutsiooni (Sertifitseerimisteenuse osutaja) juures, kus vahendi avalik osa seostatakse konkreetse isikuga. Seos on üldjuhul avalik informatsioon. Kuna vahendi avalik ja salajane osa on teineteisega tehnoloogia abil seotud, saavad kõik registreerimise järel tehtud operatsioonid fikseeritud kontekstis kindla tähenduse.

Digitaalallkirja andmise vahendi registreerimisel deklareerib isik ametlikult oma seost ühe konkreetse digitaalallkirja andmise vahendiga, st. peale vahendi registreerimist on võimalik lugeda kõiki antud vahendiga sooritatud allkirjastamisi konkreetse isiku poolt tehtuks.

Siin kerkivad koheselt esile kaks ohtu:

- Isikuga seostamine peab olema tehtav nii, et oleks garanteeritud seose terviklus. Kui isikul puudub seos mingi allkirja andmise vahendiga kõigi vahendite hulgast, siis peab olema välistatud seose loomise võimalikkus ilma antud isiku nõusolekuta ja teadmata.
- Isikuga seostatud digitaalallkirja andmise vahendi sattumise korral võõrastesse kätesse saab isiku teadmata tema nimel allkirju anda keegi teine. Tegelik probleem on see, et erinevalt tavaallkirjast ei ole digitaalallkirja andmise vahend üldjuhul isikuga otseselt seostatud – kui digitaalallkirja andmise vahend oleks isiku pärisosa, siis taanduks esimene samm isiku seostamiselt vahendiga isiku nõusoleku võtmiseks kasutada digitaalallkirja.

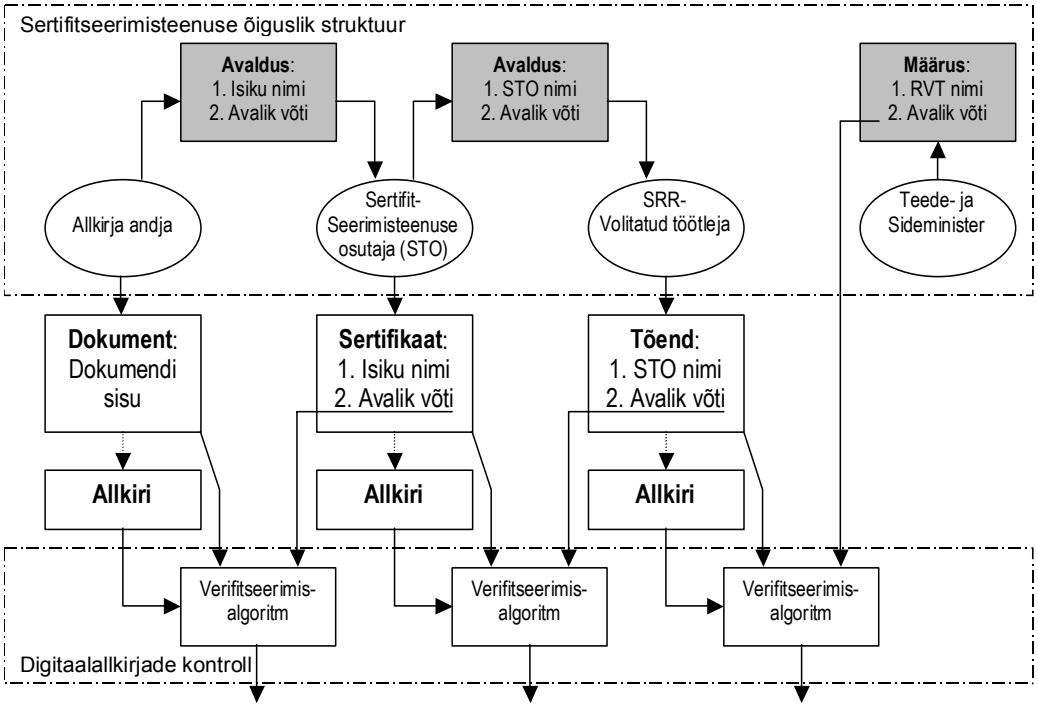
Sertifitseerimisteenuse osutaja annab välja sertifikaadi, st elektroonilise dokumendi, milles sisaldub kindlasti isiku nimi, tema avalik võti ja vahendi kehtivustähtaeg. Sertifikaadi kinnitab teenuse osutaja oma digitaalallkirjaga. Sertifikaati saab hiljem kasutada, kui peamist pidepunkti Isik-Võti seose elektrooniliseks verifitseerimiseks.

Samas tuleb tähele panna, et sertifikaadi esitamine üksi ei tõesta veel, et Isik-Võti seos tõepoolest kehtib. Sertifikaadi ettenäitamine ja sellel oleva digitaalallkirja edukas kontroll tõestvad üksnes seda, et sertifikaat on teenuse osutaja nimel allkirjastatud ja tõestuskohustus läheb üle teenuse osutajale, kes on kohustatud esitama tõendid, et sertifikaadi välja andmiseks oli alust. Selliseks tõendiks piisab, kui teenuse osutaja esitatab isiku poolt omakäeliselt allkirjastatud avalduse, milles sisaldub kindlasti isikut identifitseeriv teave ja vahendit üheselt identifitseeriv teave (avalik võti) ning STO on eelnevalt tuvastanud isiku tema isikut tõendava dokumendi alusel. Alles siis läheb tõestuskohustus üle digitaalallkirja väidetavale andjale.

Nimetatud avaldus on ainus dokument, mis tegelikult seob isikut ja digitaalallkirja andmise vahendit. Kui näiteks teenuse osutaja selle dokumendi kaotab ja ei ole võimeline seda vaidluse ajal esitama, siis seaduse järgi langeb vastutus digitaalallkirjaga seotud toimingu tagajärgede eest teenuse osutajale endale.

Kui registreerimisavalduses või mõnes muus registreerimisprotsessil allkirjastatavas dokumendis puudub üheselt arusaadav viide konkreetsele avalikule võtmele, siis kaob ära igasugune õiguslik alus seostada vastava vahendiga antud digitaalallkirju isikuga. Ei piisa lihtsalt isiku "volitusest teenuse osutajale avaliku ja isikliku võtme moodustamiseks", nagu see on kirjas Digitaalallkirja seaduse [2] paragrahvi 8 lõikes 1: teenuse osutajale esitatakse:

> 3) sertifikaadi taotleja avalik võti või volitus sertifitseerimisteenuse osutajale isikliku ja avaliku võtme moodustamiseks.



Joonis 4. Sertifitseerimisteenuse õiguslik ja tehniline struktuur (hallid kastid tähistavad paberdokumente).

2.2.4 Ajatempliteenus

Kuna tänapäeval teadaolevad digitaalallkirja andmise vahendid on enamikus lahus isikust ja tugevas sõltuvuses mingist konkreetsest tehnoloogiast, mis võib aja jooksul osutuda turvalisuse mõttes ebapiisavaks, siis on aktuaalne allkirja andmise vahendi aegumise (ja tühistamise) probleem. Digitaalallkirja andmise vahendi aegumise üheks võimalikuks tagajärjeks on seose tühistumine isiku ja vahendi vahel.

Samas ei tohi aegumisega (tühistusega) kaasneda enne seda antud digitaalallkirjade tagantjärele tühistumist. Seega tuleb ka peale tühistust eristada allkirju, mis on antud siis, kui seos vahendi ja isiku vahel kehtis nendest allkirjadest, mis anti siis, kui seos enam ei kehtinud.

Ajatempliteenus loob võimaluse usaldatavalt fikseerida digitaalselt allkirjastatud dokumentide tekkeaega, st tõestada, et dokument ja digitaalallkiri olid olemas enne teatud ajahetke.

Ajatempliteenused on otstarbekas jagada kahte klassi:

(1) *Usaldust mittenõudvad teenused* – teenused, mille osutamisel kasutatud turvameetmed välistavad olukorra, kus teenuse osutaja annab välja ajatempli "tagasiulatuvalt" (*back-dating attack*), mistõttu kehtetud digitaalallkirjad muutuvad formaalses mõttes kehtivateks.

(2) *Usaldust nõudvad teenused* – teenused, mis põhinevad teenuse osutaja usaldatavusel, st teenuse osutajal puudub võimalus enda antud ajatemplite õigsust objektiivselt tõestada (näiteks PKIX tüüpi ajatempliteenused).

Tingimusteta usaldatav ajatempliteenuse osutaja (kelle ajatempleid ei saa ega ole vajadust kohtulikult vaidlustada) näib olevat üksnes abstraktsioon juriidilises mõttes – ei ole selge, kas

ükski instants (peale kohtuvõimu enda) saab demokraatlikus riigis sellist staatust omada[3], sest tema võimuses on objektiivsetest asjaoludest lähtuvalt kehtivaks muuta mistahes kehtetu digitaalallkiri. Seega:

Mitteriiklike ajatempliteenuse osutajatena saavad kõne alla tulla ainult usaldust mittenõudva (st linkimisel põhineva) teenuse pakkujad.

Nimetatud arutelu ei kehti sertifitseerimisteenuse osutamise kohta, sest sertifikaadi välja andmise alust saab teenuse osutaja objektiivselt tõestada, näidates ette sertifikaadi taotluseks esitatud (omakäeliselt allkirjastatud) avalduse.

2.2.5 Valideerimisteenus

Sertifikaadist ja tõendist ei piisa üldiselt veel, et täita kehtivustõendi põhinõudeid, st nende esitamisest ei piisa tõendamaks, et allkiri anti sertifikaadis (ja allkirja andja poolt esitatud avalduses) märgitud kehtivusaja jooksul. Selle fakti tõestamiseks piisab ajatempliteenusest (st digitaalallkirjale võetud ajatemplist).

Vaja on veel nn valideerimisteenuste infrastruktuuri, mis üldjuhul võib olla sõltumatu sertifitseerimisteenuse struktuurist. DAS näeb küll ette, et valideerimisteenust osutavad STO-d.

Valideerimisteenuse all mõeldakse teenust, mis

(1) registreerib sertifikaatide tühistusavaldusi, mis peamiselt tulevad allkirja andjalt;

(2) vastab huvitatud osapoolelt tulevale (paarina Digitaalallkiri/Sertifikaat esitatud) kehtivuspäringule, saates vastu kinnituse, et teenuse osutaja on päringu kätte saanud ja et päringus viidatud Sertifikaat ei olnud enneaegselt tühistatud või muul põhjusel kehtetu päringu kättesaamise hetkel.

Valideerimisteenuseid ei ole otstarbekas analoogiliselt ajatempliteenustega jagada usaldust nõudvateks ja mittenõudvateks teenusteks, sest *valideerimisteenused, mis usaldust üldse ei nõua*, on tänapäeva teadusele veel tundmatud – kõige raskem asjaolu on objektiivselt tõestada, et tühistusteadet ei ole kätte saadud. Seetõttu praktikas saab täna arvestada vaid usaldust nõudvate teenustega – st kehtib järgmine järeldus:

Positiivset kinnitust ei saa teenuse osutaja kunagi objektiivselt põhjendada, mistõttu positiivse kinnituse kohtus tõendina esitamisel (ehkki sellel on teenuse osutaja digitaalallkiri) ei saa tõestuskohustus siin üle minna teenuse osutajale.

Valideerimisteenuse osutajatele saab kehtestada ainult üldisi nõudeid. Näiteks üks kindel kriteerium, millele valideerimisteenused peavad vastama on tingimus, et

(VC) *Juba tühistatud sertifikaati ei tohi teenus enam hiljem kehtivaks kuulutada*.

See kriteerium annab ainukese mõõdetava võimaluse tõestada teenuse osutaja mittenõuetekohast käitumist, kui nõuda, et tühistusteatele peab teenuse osutaja vastama digitaalselt allkirjastatud kinnitusega, et sertifikaat on tühistatud.

Kui allkirja andja on saatnud tühistusteate ja saanud vastu teenuse osutaja poolt allkirjastatud tühistuskinnituse, siis ta saab ennast edukalt kaitsta vaidlustes, isegi kui teenuse osutaja hiljem ekslikult kinnitab sertifikaadi kehtivust – allkirja väidetav andja saab siis tõestada, et teenuse osutaja ei ole täitnud põhinõuet (VC).

[3] Siin oleks vaja tingimata ka juristide arvamust.

Valideerimisteenust kasutavad omal viisil nii allkirja (väidetav) andja kui ka huvitatud osapool. On olemas järgmised tähtsamad ohud:

- *Valideerimisteenuse osutaja kinnitab huvitatud osapoolele, et sertifikaat kehtis, ehkki tegelikult on see juba tühistatud*. Kui allkirja väidetaval andjal puudub võimalus see väide ümber lükata, näiteks kriteeriumi (VC) kasutades, siis on kannatajaks pooleks (ebaõiglaselt!) allkirja andja. Isegi kui oleks võimalik väidet ümber lükata, siis siin ei ole ohtu huvitatud osapoolele, sest vastutab ikka kas allkirja väidetav andja või siis teenuse osutaja.
- *Valideerimisteenuse osutaja ei saa tühistusavaldust kätte, või siis saab küll kätte, kuid ei reageeri sellele*. Ohtlik allkirja väidetavale andjale, sest tühistamise põhjuseks võis olla võtmeleke ja iga tühistamise juures on iga minut kallis. Ilma lisaeeldusi tegemata puudub allkirja väidetaval andjal igasugune kaitse selle ründe vastu.

Ainuvõimalik kaitsemeetod näib siin olevat uue teenuse olemasolu, mis lubaks allkirja andjal valideerimisteenuse osutaja mittereageerimise korral teavitada sellest "kõrgemalseisvat" instantsi (näiteks SRR-i), st saata sellele instantsile oma tühistussõnum ja märkus, et valideerimisteenuse osutaja sellele ei reageeri. Kõrgem instants võib siis ise proovida tühistussõnumit saata. Kui temal see õnnestub, saata tühistuskinnitus allkirja andjale tagasi, ja kui ei õnnestu, siis on võimalik diskvalifitseerida teenuse osutaja (st võtta talt tegevuslitsents ära). Selline lahendus aga:

1. Ei lahenda tühistuse probleemi. Keegi peab ikkagi kinnitama, et tühistus tegelikult toimus, ja see keegi saab antud juhul olla ainult "kõrgem instants". Nii aga tekivad kaks alternatiivset tühistusviisi, mis omakorda on ohtlik huvitatud osapoolele – valideerimisteenus võib tunnistada kehtivaks sertifikaadi, mis "tegelikult" on kehtetu, sest kõrgem instants on juba kätte saanud tühistusteate.
2. On ohtlik teenuse osutajale, sest ründaja võib blokeerida teenuse osutajale saabuva, või temast väljuva võrguliikluse ja sellega võtta teenuse osutajalt ebaõiglaselt ära litsentsi.

Esimese probleemi lahenduseks võib igale digitaalallkirjale võtta kinnituse ka "kõrgemalt instantsilt", kuid siis muutub teenuse osutaja ise kogu skeemis ülearuseks. Seega tundub olevat lihtsaim lahendus valideerimisteenus ise viia "kõrgemasse instantsi" (SRRi ?).

Valideerimisteenusel kui sertifikaate tühistaval teenusel ei pea olema mingit seost sertifikaate välja andva teenusega, st see teenus ei pea teadma, millised sertifikaadid kehtivad ega seda, millised kunagi kehtisid. Ainuke asi, mille üle teenus peab arvet pidama, on enneaegselt tühistatud sertifikaadid, mille kehtivus ei ole veel lõppenud (nendesse kantud kehtivuse tähtaja mõttes).

Praegune DAS ei reguleeri peaaegu üldse valideerimisteenuse osutamist huvitatud osapoole seisukohast. Tühistusteenuse kohustus on pandud Sertifitseerimisteenuse osutajatele ja samuti ka kohustus *tõendada huvitatud isiku nõudmisel oma esindaja digitaalallkirjaga enda poolt väljaantud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust* (DAS par. 22 lg 5), mis sisuliselt on valideerimisteenus. Samas ei sätestata mingeid muid tingimusi sellele teenusele. Tegelikult oleks ilmselt vajalik eraldi töögrupi poolt üle vaadata valideerimisteenuste osutamise kord ja vajaduse korral teha seaduses muudatusi.

2.2.6 Digitaaldokumentide arhiveerimine ja nende tõestusväärtuse säilitamine

Digitaalallkirja tehnoloogiline aegumine on situatsioon, kus isiku kasutada olev digitaalallkirja andmise vahend (kas siis materiaalne või immateriaalne) on moraalselt vananenud (räsimeetod on murtud, kiipkaart on kergesti kopeeritav), kuna selle aluseks olev tehnoloogia ei suuda enam garanteerida tõestus- ja tuvastusfunktsiooni täitmist. Siin kerkivad üles mitmed probleemid.

2.2.6.1 Digitaalallkirja andmise vahendiga seotud probleem

Kui allkirja andmise vahend baseerub mingil tehnoloogial ja allkiri peab tagama pikaajalise tõestusväärtuse, siis peab tegelikult see tehnoloogia tagama pikaajalise tõestusväärtuse. Tuleb vältida olukorda, et 20 aastat hiljem kontrollimise ajahetkel on digitaalallkiri kergesti võltsitav, sest digitaaldokumentide puhul ei ole võimalik tuvastada, kas nad loodi täna või eile.

2.2.6.2 Arhivaalide mahu probleem

Ideaaljuhul ei nõua allkirjastatud digitaaldokumendi säilitamine huvitatud osapoolelt midagi muud kui kandjat, mis on võimeline garanteerima informatsiooni pikaajalise säilumise. Teisest küljest ei ole meil ainuüksi digitaaldokumendi säilimisest kasu, kui sellega ei kaasne informatsiooni seoste baasi oleku kohta allkirjastamise ajahetkel. Kui peame säilitama ka kogu seoste info, tähendab see arhivaalide mahu olulist kasvu.

2.2.6.3 Formaatide muutuse probleem

See probleem on seotud nii tehnoloogia kui hinnaga. Tehnoloogia arenedes muutuvad ka allkirjastatavad dokumendid ja allkirjastamiseks kasutatavad vahendid. Vahendite ja dokumentide muutudes muutuvad ka nendega seotud protseduurid ja formaadid. On oht, et 20 aastat peale allkirja andmist ei ole võimalik konkreetset allkirja kontrollida, kuna puudub ligipääs vastavale tehnoloogiale või andmeformaatidele. St. võimalik, et tuleb arhiveerida nii dokumente kui nende töötlemiseks vajalikku tehnoloogiat.

2.3 Digitaalallkiri erinevates suhetes

Digitaalallkirja seaduse §43 näeb ette, et Riigi- ja kohaliku omavalitsuse asutused ning avalikõiguslikud juriidilised isikud korraldavad oma asjaajamise 2001.aasta 1.juuniks ümber nii, et asutuste asjaajamises on võimalik kasutada ka digitaalselt allkirjastatud dokumente. See hõlmab nii asutusesisest asjaajamist kui ka suhteid teiste institutsioonidega.

Kuna koostame digitaalallkirja juurutamise strateegiat Eesti riigi jaoks, siis on põhirõhk siin küsimusel, kes suhtleb Eesti riigiga st. riigi- ja kohalike omavalitsuste asutustega. Seega taanduvad selles peatükis analüüsitavad probleemid järgmistele küsimustele:

1. kes suhtlevad Eesti riigi- ja kohalike omavalitsuste asutustega?
2. milliste Eesti riigi- ja kohalike omavalitsuste asutustega on võimalik suhelda?
3. millistel eesmärkidel riigi- ja kohalike omavalitsuse asutustega suheldakse?
4. millistel eesmärkidel nendega üldse suhelda saab?

Riigi- ja kohalike omavalitsuste asutustega suhtlevad:

- Eraisikud – eraisikud võivad olla Eesti Vabariigi kodanikud, elamisloaga mittekodanikud ja lihtsalt mittekodanikud (vahetegemine on oluline, sest elamisloa omanikel on riigiga palju tihedam side).

- Äriühingud – äriühingud võivad olla registreeritud Eesti Vabariigi äriregistris või mõne teise riigi analoogilises asutuses.
- Riigiasutused – riigiasutused võivad olla Eesti Vabariigi või mõne teise riigi asutused või ka Euroopa Liidu institutsioonid.
- Füüsilisest isikust ettevõtjad
- Avalik-õiguslikke ülesandeid täitvad eraõiguslikud isikud (notarid, kohtutäiturid)

2.3.1 Riigiasutuse suhted eraisikutega

Eraisikutega seonduvad probleemid:

- Digitaalallkirja moodustamine. Eraisikul peab olema digitaalallkirja andmise vahend, mis võimaldab anda Eestis kehtivate õigusaktide mõttes kehtivat digitaalallkirja (DASi alusel). Nimetatud vahend peab vastama neis õigusaktides sätestatud tehnoloogilistele ja organisatoorsetele nõuetele.
- Volitamine. Tavatingimustes võib eraisik volitada kedagi enda nimel esinema. Kuidas toimub see digitaalallkirja kasutamise korral? Võib eristada kahte juhtumit – volitaja ise omab digitaalallkirja moodustamise vahendit või volitaja ei ole digitaalallkirja kasutaja. Kuidas kehtib volitus? Kas volitus kehtib mingi konkreetse tegevuse sooritamiseks või kehtib ta mingi kindla aja vältel? Milline asutus peab arvet kehtivate volituste üle?
- Isiku tuvastamine. Riigiasutusel peab olema võimalus saada teada, milline füüsiline isik digitaalallkirja eest vastutab. Siin võib eristada residente ja mitteresidente, kuna residentide puhul võib olla lihtsam luua ühtset lahendust (näiteks ID-kaart).
- Suhetest tulenevate õiguste ja kohustuste muutumise probleem. Kui kodanik lakkab olemast kodanik, siis ei tohi ta ka enam riigiasutusega suhelda saada kui kodanik. Teisipidi – kui mittekodanikust saab kodanik, siis peavad tema kodanikuõigused alates kodanikuks saamise hetkest tagatud olema. Ilmselt peab olema võimalik otsustada, kas isik on mingi allkirja andmise ajal olnud kodanik või mitte. Kas selleks on kasulik pruukida organisatsioonilisi või tehnilisi meetmeid?

2.3.2 Riigiasutuse suhted äriühingutega

Äriühingutega seonduvad probleemid:

- Probleemid on suuresti sarnased eraisikutega seonduvatega. Tunduvalt teravam on aga allkirjaõiguse tuvastamise probleem, sest äriühing koosneb inimestest. Äriühingu allkiri võib olla selle äriühingu mõttes allkirjaõigusliku isiku allkiri, ent esiteks ei ole äriühing igavene, teiseks ei ole isiku seos äriühinguga igavene. Isegi kui isiku seos äriühinguga säilib, võib muutuda tema staatus allkirjaõiguslikkuse mõttes. Seega riigiasutuste ja äriühingute vahelises suhtluses on aja probleem äärmiselt oluline.
- Digitaalallkirja andmise vahendi võiks tegelikult välja anda ka äriühingule. Sellisel juhul oleks kõik väljuvad dokumendid allkirjastatud ühe digitaalallkirjaga ja väljast ei pruugi olla võimalik kindlaks teha, kes isiklikult allkirjastamise protseduuri läbi viis. Samas allkirjaõigusega kaasneb ka vastutus. Seega, kuigi väljapoole ei pruugi olla oluline, kes digitaaldokumendi allkirjastas, peab allkirjastaja isik hiljem ikkagi tuvastatav olema. Seega süsteemi siseselt tuleb allkirjastamiste ajalugu ikkagi teatava terviklusastmega säilitada. Teatava terviklusastme all mõeldakse siin seda, et teatud aja möödudes teatud allkirjad või nendega seotud (kuri)teod aeguvad. Seega ei pruugi

olla oluline (ettevõtte ja riigi seisukohalt) säilitada ajalugu sajandite vältel. Seadused seavad omad tingimused andmetele, mida kohtus tõendina kasutada saab. Ajaloo säilitamise süsteem peab neile tingimustele vastama.

Eesti Vabariigi äriregistris registreeritud äriühingutega suhtlemise jaoks on võimalik luua ühtne infrastruktuur, mille alusel saavad äriühingud suhelda riigiasutustega ja omavahel. Isikute ja ettevõtete vahelisi seoseid võiks vahendada Äriregister ise (hetkel on seal info ainult juhtide kohta).

2.3.3 Riigiasutuse suhted välisriikidega

Digitaalallkirja seaduse §40 näeb ette ka välismaiste sertifitseerimisteenuse osutajate poolt väljaantud sertifikaatide tunnustamist võrdväärsena DAS alusel väljaantud sertifikaatidega, kui on täidetud vähemalt üks järgmistest tingimustest:

1) välismaine STO vastab SRR vastutava töötleja otsuse kohaselt DAS ja selle alusel kehtestatud õigusaktide nõuetele;

2) välismaise STO sertifikaate garanteerib mõni DAS alusel tegutsev STO, kes on sertifikaatides sisalduvate andmete tõesuse eest endale vastutuse võtnud;

3) välismaise STO poolt väljaantud sertifikaadid on tunnustatud Eesti Vabariigi välislepinguga.

Ilmselt sõltub digitaalallkirja kasutamine suhtluses välisriikide kodanike ja äriühingute ning riigiasutustega ikkagi riikidevahelisest kokkuleppest. Digitaalallkirja juurutamisel peaks samas ette nägema protseduurid juhuks, kui keegi välisriigist ikkagi tahab Eesti riigiasutustega digitaaldokumentide vahendusel suhelda (kas laseb oma sertifikaadi mõnel Eesti STO-l üle sertifitseerida vms.).

2.3.4 Riigiasutuse suhted teiste riigiasutustega

Riigiasutuste omavahelisel suhtlemisel on sisuliselt samad probleemid, kui suhetes äriühingute ja eraisikutega.

Üks suur ja ühine probleem on selles, et digitaalallkiri baseerub tehnoloogial. Tehnoloogiaga saab lahendada probleeme – näiteks tagada andmete terviklust või määrata andmete loomise ajahetke suhtelises ajas. Samas tuleb tehnoloogiat vaadelda muutuvas ajas: vahendid, mis täna tagasid andmete tervikluse, võivad homme aegunud olla.

Kui riigiasutus vahetab digitaalselt allkirjastatud dokumente ükskõik millise teise osapoolega, siis peavad mõlemad silmas pidama järgmist:

- Andmete formaat peab olema kokku lepitud ja mõlema poolt aktsepteeritav. S.t. formaat peab vastama mõlema osapoole nõuetele. Seda eriti juhul, kui üks osapooltest on kohustatud suhtluses digitaalallkirja kasutama.
- Osapoolte vahel peab valitsema üksmeel lahendatavate probleemide osas. Kui riigiasutus nõuab talle saadetavalt digitaalselt allkirjastatud dokumendilt pikaajalist tõestusväärtust, siis peab ka teisele osapoolele vastav vajadus selge olema.
- Osapoolte vahel peab valitsema üksmeel probleeme lahendavate tehnoloogiate vallas. Kui ühine seisukoht puudub ja üks osapool ei usu, et mingi konkreetse tehnoloogiaga saab tagada 5 aastast tõestusväärtust tõenäosusega 99%, siis peab leiduma alternatiivne lahendus. Kohustusliku suhtluse korral võib alternatiiviks olla tavaallkiri, mittekohustusliku suhtluse korral võib üks osapooltest lihtsalt mingist hüvest ilma jääda.

2.3.5 Riigiasutuse suhted füüsilisest isikust ettevõtjatega

Riigiasutuse suhtlus füüsilisest isikust ettevõtjaga ei oma digitaalallkirja rakendamise aspektist üldiselt erinevusi suhtlusest kodanikuga. Erinevusi on vaid suhetes Maksuametiga, ent sel korral taandub suhtlus suheteks äriühinguga selle vahega, et Äriühingute volitusinfo allikaks saab olla ainult Äriregister, füüsilisest isikust ettevõtjate kohta peab registrit ka Maksuamet ise, Äriregistris on kohustatud registreerima end ainult osa füüsilisest isikust ettevõtjatest.

2.3.6 Riigiasutuse suhted avalik - õiguslikke ülesandeid täitvate eraõiguslike isikutega

Avalik-õiguslikku ametit pidavaks üksikisikuteks Eesti Vabariigi seaduste järgi on vastavalt Kohtutäituri seadusele [14] kohtutäiturid ning Notariaadiseadusele [16] notarid. Digitaalallkirja seaduse rakendumise mõttes erineb see suhtlustüüp riigiasutuste omavahelistest suhtlusest vaid kohtutäiturite ja notarite volitusinfo kättesaadavuse osas, st. kuna kohtutäiturid ja notarid ei ole ei riigiametnikud ega ettevõtjad, siis ei kuulu nad registreerimisele ei Äriregistreis ega ka riigiametnike registris. Edaspidi ettenähtud atesteerimisprotsessi käivitamisega ilmselt niikuinii mingid registrid (ilmselt siis vastavalt Justiitsministeeriumi ja Notarite Koja juures) tekivad, kuid hetkel andmekogude seadusele vastavat st. vastutavat töötlejat omavat andmekogu volitusinfo kohta ei ole (näiteks sarnase tegevuslaadiga advokaatide osas näeb Advokatuuriseadus [17] ette advokatuuri registri pidamist advokatuuri juhatuse poolt, kusjuures nõutakse ka registri avalikkusele kättesaadavaks tegemist elektroonilises andmekogus).

2.4 Digitaalallkiri erineva tekkeviisiga dokumentide puhul

Ametnike tööülesanded on erineva iseloomuga ning erineva detailsusega spetsifitseeritud. Ametnik võib näiteks teha rahaliselt kaalukaid otsuseid, ent nende otsuste tegemise protsess on väga täpselt determineeritud. Sellist tegevust on võimalik automatiseerida ning toetada ametnikku tema töös mitmesuguste tehnoloogiliste süsteemidega. Samas kõrgemad ametnikud peavad aga tegelema otsustustega väga laias valdkonnas, mis ei ole formaliseeritavad ning mille toeks on võimalik luua vaid väga üldisi tehnoloogilisi süsteeme (nagu näiteks tekstitöötlus). Need erinevused kajastuvad ka selles, millises mahus ja millisel viisil on digitaalallkirja võimalik ja otstarbekas neis tööprotsessides rakendada.

Tööprotsesside käigus tekkivate digitaaldokumentide elutsükkel on erinev ja neid võidakse signeerida erinevates stsenaariumides. Järgnevalt vaatleme neist stsenaariumidest mõnesid tüüpilisemaid ning käsitleme digitaalallkirja andmisel tekkida võivaid probleeme.

2.4.1 Registriväljavõtted

Registriväljavõtted on dokumendid, mis moodustatakse automaatselt väljavõtte tegija valduses oleva andmebaasi alusel. Väljavõte võib näiteks kujutada enesest vastust mõne isiku poolt tehtud päringule. Järgnevalt vaatame probleeme, mille lahendamise juures oleks võimalik kasutada ka digitaalallkirja.

2.4.1.1. Autentsuse tagamine

Väljavõtet nõudnud isik peab suutma veenduda, et väljavõtte tegija on antud registri tegelik usaldatav valdaja. Üldjuhul on selleks valdajaks seaduse poolt määratud riigiasutus; nii on mõtet usaldada Autoregistrit, aga mitte piraatandmebaasi. Info, mis võimaldab väljavõtte tegija autentsust kontrollida, peab samuti tulema usaldatavatest allikatest, selle tagamine on aga omaette probleem. Nii võib autentsuses veendumisel põhimõtteliselt tekkida vajadus väga

pika ja raskesti jälgitava usaldamiste ahela järgi, mida kasutajad mugavusest kontrollida ei viitsi, tekitades niimoodi soodumuse mitmesugusteks väärkasutusteks.

2.4.1.2. Tervikluse tagamine

Väljavõtet nõudnud isik peab suutma veenduda, et

- keegi peale väljavõtte tegija ei ole väljavõtet hiljem (ega varem) modifitseerinud;
- väljavõtte tegija on väljavõtte teinud korrektselt.

Kord juba antud väljavõtte tervikluse tagamiseks võib kasutada näiteks digitaalallkirja, kuid registri valdaja tegevuse kontrollimine on raskem ja seni veel lõpuni lahendamata probleem. Arvatavasti ei pääse lahendus mööda registri regulaarsest auditeerimisest.

2.4.1.3. Konfidentsiaalsuse tagamine

Teatud (nt delikaatseid andmeid puudutavaid) väljavõtteid peab saama teha vaid teatud isik ning see isik võib soovida, et väljavõtte sisu (ja väljavõtte tegemise fakt) jääks kõrvalistele isikutele saladuseks. Kui sisu saab edukalt kaitsta krüptograafiliste vahenditega, siis päringu tegemise fakti on nt võrguliikluse analüüsi eest üsna raske peita.

2.4.1.4. Kehtivusaeg

Teatud registriväljavõtteid võib isik soovida säilitada suhtluseks teiste asutustega või tõendina kasutamiseks. Seetõttu peaksid vähemalt mõned väljavõtted kehtima kauem kui vaid kättesaamise hetke. Teisest küljest võib väljavõtte aluseks olnud registri seis ajas muutuda ja väljavõte nii vääraks muutuda. Seetõttu on registri iseloomu ja väljavõtete kasutusvaldkonda arvestades olla otstarbekas kehtestada väljavõtetele teatud kehtivusaeg.

2.4.1.5. Salgamise vääramine

Pärast väljavõtte andmist ei pruugi registri valdaja olla huvitatud väljavõtte sisu ega väljavõtte andmise fakti eest vastutamisest. Kui aga päringu esitaja tahab väljavõtet näiteks kohtus tõendina kasutada, tuleb niisuguse salgamisvõimaluse vastu võidelda.

Tehnika *versus* inimene - kuna registripäringult oodatakse vastust reeglina reaalajas, esitab vastavad signeeritud väljavõtted üldjuhul arvuti. Väljavõtete signatuuri eest peab aga sellegipoolest vastutama inimene. Kuidas seda vastutust täpselt määratleda (näiteks juhul, kui signatuur anti ekslikult tänu tarkvaralisele veale), pole õigusaktides veel täpselt paika pandud.

2.4.2 Läbipaistmatu menetlusega dokumendid

Läbipaistmatu menetlusega on dokumendid, mis moodustatakse inimeste otsese sekkumisega, kuid dokumendi saajale ei ole selle dokumendi menetlusprotsess (sekkuvate inimeste otsused) olulised. Näiteks on selline dokument pass, kus tähtis on see, et pass on ikka riigi poolt välja antud, kuid mitte see, kes konkreetselt passiblanketti trükkis.

Kuigi tegu on läbipaistmatu menetlusega dokumentidega, võib ikkagi tekkida vajadus tuvastada, kes dokumenti menetles, või vähemalt kes menetlemise eest vastutab (näiteks tõuseb see vajadus päevakorda juhul, kui dokument sisaldab olulisi vigu). Samuti peab dokumendi saaja suutma veenduda menetleja volitustes.

Põhiliseks erinevuseks registriväljavõtete ja läbipaistmatu menetlusega dokumentide vahel on nende väljastamise tehniline külg. Kui registriväljavõtted annab arvuti ja väljavõtte eest vastutab kindel isik, siis läbipaistmatu menetlusega dokumente käsitleb vähemalt mingis osas

inimene. Seejuures ei pruugi käsitleja ja menetlusprotsessi eest vastutaja isikud kokku langeda, mis võib tekitada probleeme süüdlase kindlakstegemisel.

Kõik registriväljavõtete juures vaadeldud probleemid tekivad ka antud juhul. Samas kui registriväljavõte on reeglina ühekordse operatsiooni tulemus, siis praegu vaatluse all oleva klassi dokument võib tekkida paljude osapoolte koostöös ning omada nõnda ka mitut allkirja. See asjaolu põhjustab uue probleemi.

Allkirja semantika - tehniliselt on võimalik allkirjastada dokumendi sisu nii mitme sõltumatu signatuuriga kui ka signeerida dokument üle koos eelmis(t)e allkirja(de)ga. Mõlemad lahendused võivad teatud situatsioonis kasulikuks osutuda, kuid igal juhul tuleb täpselt määratleda, mille eest millise allkirja andja vastutab.

2.4.3 Läbipaistva menetlusega dokumendid

Läbipaistva menetlusega on dokumendid, mille koostamise aluseks olnud menetlusprotsess peab olema nähtav ka dokumendi saajale. Siia klassi kuulub enamus riigiasutuste vahel liikuvaid dokumente nagu kirjad, seaduseelnõud jm. Reeglina nõutakse, et nende dokumentide menetlemisest peab jääma ka mingi jälg, mida saab hiljem nt kohtus tõendusmaterjalina kasutada.

Piir läbipaistva ja läbipaistmatu menetlusega dokumentide vahel ei ole alati selge. Nii näiteks on ka läbipaistmatu menetlusega dokumendi saamislugu võimalik kohtus avada või kui kaks asutust koostavad mingit dokumenti koos, siis nende sisemine protsess võib olla nähtav vaid asutuste sees, samas mõlema asutuse osalus protsessis paistab välja. Seetõttu on läbipaistva ja läbipaistmatu menetlusega dokumentide korral tekkivad turvaprobleemid praktiliselt samad.

2.5 Toiminguteks volitatud isiku kindlakstegemine

Digitaalallkirja kehtivusel on kaks aspekti:

(1) allkiri on antud mingi kindla isiku poolt;

(2) isikul oli õigus antud dokumendile alla kirjutada.

Näiteks kui dokument (mingi tõend vms.) anti välja riigiasutuse ametniku poolt, siis ei piisa kindlakstegemisest, et dokumendil on kindla füüsilise isiku digitaalallkiri. Vaja on ka kinnitust, et antud isikul oli (näiteks ametikohustustest tulenev) õigus asutuse nimel dokumendile alla kirjutada. Sellise õiguse allikaid on mitmeid. Kõige tüüpilisem on kahtlemata isiku tööleping antud asutusega või ametisse nimetamise käskkiri ja ametijuhend, mis kehtestab tema õigused, kohustused ja vastutuse. Samas võib aga olla ka muud liiki suhteid, mis nimetatud õiguse annavad – näiteks antud asutuse juhi poolt antud erivolitus. Õigus mingit dokumenti allkirjastada ei tarvitse alati tähendada *allkirjaõiguslikkust* selle tavalises tähenduses.

Dokumendi saajale (kui huvitatud poolele) ei ole tavaliselt kuigi oluline teada, millised konkreetsed õiguslikud suhted annavad isikule õiguse kirjutada alla riigiasutuse poolt välja antavale ametlikule dokumendile. Kõige olulisem on huvitatud poolele see, et riigiasutus hiljem ei distantseeruks dokumendist, st ei väidaks, et dokumendil ei ole mingit seost riigiasutuse poolt välja antava ametliku informatsiooniga ja seetõttu ka riigiasutus dokumendi sisu eest ei vastuta.

Info riigiasutuste nimel tegutseda võivatest isikutest peab seetõttu olema huvitatud poolele operatiivselt ja usaldusväärselt kättesaadav ja sellel infol peab olema ka tõestusväärtus. Näiteks, kui Internetist saadava info põhjal oli isikul õigus allkirja anda, kuid hiljem tuvastatakse, et tegelikult siiski ei olnud, siis kannataks huvitatud osapool ebaõiglaselt. Seetõttu

peab ka kinnitus esindusõiguse olemasolu kohta ise olema ametlik informatsioon, mille esitamisel allkirja õigsuse üle toimuva kohtuvaidluse käigus langeks tõestuskohustus õige volitusinfo esitamise eest kellelegi teisele (mingile riigiasutusele või riigiametnikule) peale huvitatud poole enda. Vastasel korral ei saaks ilma suure riskita aktsepteerida mitte ühtegi riigiasutusest tulevat digitaalallkirjaga dokumenti.

Samad probleemid tekivad siis, kui füüsiline isik esindab juriidilist isikut. Ka siin on lisaks töölepingule ilmselt olemas muid võimalusi, kuidas esindusõigus (ja sellest tulenev vastutus) tekib.

Kõigi nende suhete üksikasjalik käsitlemine digitaalallkirja kontrollimisel on ilmselt mõeldamatu. Samahästi on asjade praegust seisu arvestades ebareaalne loota, et kõik allkirja andmise õigusega seotud suhted oma originaalkujul digitaalmaailmas kajastamist leiaksid. Seetõttu on siin tarvis leida teatud kompromisslahendusi, mis tehnika hetkeseisu arvestades võimaldaksid siiski digitaalallkirju turvaliselt aktsepteerida.

Ühelt poolt on olemas hästidefineeritud protsesse, milles osalevate ametnike ülesanded ja õigused on täpselt paika pandud. Selliste protsesside toeks on ehitatud spetsiaalsed infosüsteemid, mis töötlevad (pool)automaatselt teatud kindlatüübilisi dokumente. Kuna nii ametnike rollid kui ka kasutatavad dokumenditüübid on defineeritud võib ametniku õiguse mingeid dokumente allkirjastada esitada paarina (*D*,*I*), kus *D* on dokumenditüübile üheselt viitav identifikaator ja *I* on isikut üheselt identifitseeriv teave. Paar (*D*,*I*) tähendab, et isikul *I* on õigus alla kirjutada dokumendile tüübiga *D*. Näiteks *D* võib tähendada elamisluba. Paar peab loomulikult olema digitaalselt allkirjastatud asutuse (või firma) juhi poolt – muidu ei oleks tal tõestusväärtust. Kui huvitatud poolel on asutusest (või firmast) saadud digitaalallkirjaga dokument ja lisaks sellele firma kinnitus, et dokumendile alla kirjutanud isikul oli ka õigus antud tüüpi dokumendile alla kirjutada, siis sellest järeldub, et dokument on tõepoolest "ametlik". Paaride (*D*,*I*) kohta võib arvet pidada asutuse juhi vastutusalas olev register, milles on alati olemas ajakohane teave õiguste kohta.

Teiselt poolt on olemas palju selliseid protsesse, mis ei ole täpselt defineeritavad, mis toimuvad harva või on hoopis unikaalsed ning mida pole seetõttu mõtetki formaliseerida ja spetsialiseeritud infosüsteemide loomisega toetada. Samas aitaks digitaalselt allkirjastatud dokumentide kasutamine neid protsesse kiiremaks muuta. Nendes protsessides osalevate ametnike volituste piisavalt täpseks kirjeldamiseks peab ilmselt kasutama inimkeelt. Vastava volituste alusel allkirjastatud dokumentide kontrolli ei saa teostada automaatselt, sest vaid inimene suudab kontrollida, kas vastav dokument mahub antud ametniku volituste piiridesse.

3. Ohud digitaalallkirja rakendamisel

Käesolevas peatükis võtame lühidalt kokku peamised üldised probleemid, mis võivad ohustada digitaalallkirja kasutuselevõttu tavaallkirja asendavas funktsioonis.

3.1 Allkirja andmise vahendiga seonduvad ohud

3.1.1 Personaalse turvakeskkonna puudumine

Võimalikuks ohuks on see, et ei suudeta luua täielikult kontrollitavat personaalset turvakeskkonda. Kuna digitaalallkirja korral esindab allkirja andmise vahend sisuliselt inimese tahet, on tema turvaline hoidmine esmatähtis. Ideaaljuhul peaks vahendi omanik selle kõiki koopiaid kogu aeg kaasas kandma ning iga allkirja andmise korral olema veendunud, et mõni tehniline lüli vahendit ei kuritarvita (näiteks ei muuda allkirjastatavat dokumenti). Samuti tuleb garanteerida, et ligipääs vahendile on olemas vaid selle legaalsel omanikul. Senini ei ole riiklikul tasandil piisavalt tähelepanu pööratud piisavalt turvalise digitaalallkirja andmise keskkonna probleemidele. Ainult kiipkaardi kasutamine seda probleemi ei lahenda, veelgi enam – ei vii ka märkimisväärselt lahenduse suunas edasi.

3.1.2 Automaatne tuvastamine

Võimalikuks ohuks on, et ei suudeta leida mugavat, töökindlat ja turvalist füüsilise isiku automaatse tuvastamise tehnoloogiat. Hetkel tuvastatakse (allkirja andmise vahendi poolt) isikuid enamasti teadmuspõhiselt, st mingi parooli või PINi alusel. Inimlik laiskus sunnib meid aga oma paroole üles kirjutama või neid maksimaalselt lihtsustama, põhjustades mõlemal juhul tõsiseid turvaprobleeme. Alternatiiv oleks kasutada mingeid biomeetrilisi vahendeid (nt sõrmejälje või silmapõhja tuvastus), kuid vastav tehnika pole veel 100% usaldatav.

3.1.3 Ebaõiglane vastutus

Ebapiisavatest turvameetmetest võib tuleneda ebaõiglane vastutuse oht**.** Absoluutselt turvalise allkirja andmise vahendi puudumise tõttu jääb alati alles oht, et allkirja andmise vahendit kasutatakse ilma isiku nõusolekuta (st võltsitakse allkirju). Kui ei rakendata piisavaid turvameetmeid ega piirata digitaalallkirja kasutamisest tulenevat vastutuse määra, siis on tõsine oht, et inimesed võivad kanda ebaõiglast vastutust nende vahendiga kellegi teise poolt antud digitaalallkirjadest tulenevate õiguslike tagajärgede eest.

3.1.4 Ebapiisav tõestusväärtus

Ebapiisavatest turvameetmetest võib tuleneda ka oht, et digitaalallkirjaga dokumendil on ebapiisav tõestusväärtus. Kuna digitaalallkirja andmisel ei teki otsest ilmutatud seost inimese tahtega, jääb digitaalallkirja andmise vahendi valdajale tegelikult alati alles võimalus väita, et "ma tõesti ei tea, kuidas minu allkiri selle dokumendi alla sattus". Juriidiliselt võib isiku muidugi oma digitaalallkirja eest vastutavaks teha (tõestuskohustuse üleminek teatud selgelt määratletud tingimuste korral), kuid mingi eksituse võimalus jääb paratamatult alles. Ei ole selge, kuidas mõjub sellisele eksimisvõimalusele apelleerimine digitaalallkirja õigsuse üle toimuva kohtuvaidluse tulemust. See võib aga ohustada huvitatud pooli, kes peavad lootma jääma just digitaalallkirja tõestusväärtusele. Samuti võib ohustada tõestusväärtust STO poolt rakendatav ebapiisav sertifikaadi taotlemise protseduur, st kui näiteks ei tekitata tõestatavat seost isiku ja konkreetse avaliku võtme vahel.

3.2 Standardimisega seonduvad ohud

3.2.1 Digitaaldokumendi ühese interpretatsiooni puudumine.

Digitaaldokument on tehniliselt võttes vaid bitijada, mille ühene esitus (nt visuaalne või auditiivne) pole alati selge (näiteks HTML-dokument omab ettekavatsetult nii lähte-koodipõhist kui brauseripõhist vaadet). See asjaolu võib põhjustada hilisemaid salgamisi digitaalselt allkirjastatud dokumendi sisust arusaamise osas. Ka dokumendile metaandmete lisamine ei lahenda seda probleemi lõplikult, sest metaandmedki esitatakse digitaalkujul ja neid tuleb samuti kuidagi interpreteerida.

3.2.2 Avaliku ja standardse dokumendiformaadi puudumine.

Vastavalt seadustele lõppeb iga riigiasutustes ringleva dokumendi elutsükkel arhiveerimisega. Arhiiv on kohustatud tagama ligipääsu arhiveeritud dokumentidele veel aastakümneid, kuid infotehnoloogia tormilise arengu ja ristuvate ärihuvide tingimustes vananevad failivormingud tunduvalt kiiremini ja tänased dokumendid ei pruugi 20 aasta pärast kasutatava tarkvaraga loetavad olla. Ka dokumentide konverteerimine pole lahendus, sest see rikuks digitaalallkirja kontrollimisel vajalikku terviklust. Seetõttu oleks parim lahendus kasutada mõnd avalikku ja standardset formaati (nt XML).

3.3 Digitaalallkirja usaldatavust tagavate teenustega seonduvad ohud

3.3.1 Standardsete usaldust mittenõudvate ajatempliteenuste puudumine.

Digitaalallkirja tõestusväärtuse pikaajaliseks säilitamiseks ei piisa ainult standardsest (näiteks PKIX) avaliku võtme infrastruktuurist, lisaks on vaja veel vähemalt turvalist (usaldust mittenõudvat) ajatempliteenust. Viimase standardiseerimine hetkel alles käib (ISO) ja kuni see protsess ei ole stabiliseerunud, ei saa digitaalallkirju pikaajalise tõestusmaterjalina kasutada.

3.3.2 Standardse PKIX ajatempliteenuse kasutamisega seonduvad usaldusprobleemid.

Usaldust nõudvate ajatempliteenustega seotud juriidilised probleemid ja samuti atesteerimise ja auditeerimise reeglistik ei ole tänaseks piisavalt läbi töötatud. Seetõttu on oht, et PKIX tüüpi ajatempliteenuse osutaja kätte koguneb aja jooksul üha suurenev võim: võimalus tagantjärele (ja jälgedeta) võltsida digitaalallkirju ükskõik millise isikliku võtmega, mis on aja jooksul kogemata avalikustunud. Probleem ei ole lahendumatu, kuid nõuab detailset tehnilist ja organisatsioonilist-õiguslikku lahendust.

3.3.3 Autentse ja käideldava publitseerimise probleem.

Üks turvalise (usaldust mittenõudva) ajatempliteenuse eeltingimusi on võimalus publitseerida andmeid usaldatavasse ja kergesti ligipääsetavasse meediumi. Madala usaldustaseme pärast ei sobi lihtne avaldamine Internetis, kehva käideldavuse tõttu aga trükkimine ajalehes. Sobivat lahendust ei ole hetkel veel välja pakutud.

3.3.4 Avaliku võtme infrastruktuuri killustatus.

PKI loomise üks ideid oli moodustada selline ülemaailmne sertifitseerimisvõrk, et kõik kasutajad suudaksid läbi oma usaldusahelate üksteise signatuure kontrollida. Praktikas on ühe suure võrgu asemel tekkinud hulk väikeseid, mille ühendamine ei ole lihtne ülesanne. Tänu

sellele ei pruugi kõik vajalikud allkirjad alati kõigile kontrollitavad olla. See probleem puudutab eelkõige rahvusvahelist allkirjade aktsepteerimist.

3.4 Ohud digitaaldokumentide säilitamisel

3.4.1 Tarkvara vananemine

Tegelikult tuleb siin eristada kahte probleemi:

- failivormingute vananemine (vanad formaadid ei võimalda esitada uusi asju või uus tarkvara ei toeta vanu vorminguid);
- tarkvara enda moraalne aegumine (turule tulevad tunduvalt mugavamad, odavamad, ... paketid).

Kui uus tarkvara toetab vana vormingut (ega sunni kasutajat kuidagimoodi uut eelistama), siis probleemi tegelikult ei ole. Näiteks piisab, kui kontoripakettide uuendamisel peavad kõik asutused silmas ühilduvust kehtivate XML-standarditega.

Kui suhtluses kasutatakse aga kinnist vormingut ning seda valdav firma otsustab formaadi toetamise (nt ärilistel kaalutlustel) lõpetada, peab arhiiv dokumentide loetavuse säilitamiseks mingeid samme astuma. Välja on pakutud mitmeid alternatiivseid lahendusi.

Migreerimine - loodetavasti annab formaadi omanik vähemalt mingiks ajaks kasutusse vormingute uuendamise vahendid. Neid kasutades saab loodetavasti dokumentide loetavuse päästa. Samas ei saa sel moel säilitada digitaalallkirjade kehtivust, samuti ei pruugi konverteerimisvahendid olla väga automaatsed ja migreerimiseks vajalik töömaht võib kasvada ebareaalseks.

Emuleerimine - uued keskkonnad oskavad sageli emuleerida vanemaid (nt Windows 2000 emuleerib MSDOSi). Selle meetodiga saab küll säilitada digitaalallkirjad, kuid sajaprotsendilise usaldatavuse saamiseks tuleks peale konkreetse tarkvaraprodukti emuleerida ka operatsioonisüsteemi või koguni riistvaraplatvormi ja see ei pruugi enam reaalne olla.

Teisendamine mingile standardkujule - nii võib näiteks kõiki dokumente esitada TIFF-pildina, mis garanteerib küll dokumendi loetavuse, kuid mitte digitaalallkirja ja käideldavust.

Nagu näeme, head lahendust arhiveerimise vaadeldud osa probleemidele veel ei tunta ning see on üks olulisemaid põhjusi avatud standardite soovitamisel.

3.4.2 Füüsilise meedia ebapiisav säilimine.

Hetke üks populaarsemaid salvestusmeediaid on CD/DVD-plaadid, mille füüsiliseks elueaks loetakse hoiutingimustest sõltuvalt 2-75 aastat. Seda võiks isegi piisavalt olla, kuid arvatavasti ei ole 75 aasta pärast meie käsutuses enam ühtki töötavat CD-lugejat. Niisiis räägime ka andmekandjate korral eeskätt moraalsest vananemisest.

Üks ilmseid lahendusi säilitusmeedia vananemise probleemile on regulaarne ümberkopeerimine. Füüsiliste meediate regulaarne vahetamine arhiivis on kooskõlas arhiivinduse arengusuundadega paratamatu ning sellega on Rahvusarhiiv ka arvestanud – arhiivieeskirjas on kehtestatud nõuded ka füüsilisele meediale ning jätkuv sellesuunaline tegevus Rahvusarhiivis toimub.

3.4.3 Kasutatavate krüptograafiliste primitiivide murdumine.

Juhul kui mõni kasutatavatest krüptograafilistest vahenditest muutuks üleöö ebaturvaliseks (räsifunktsioon murduks, signatuurialgoritm ei osutuks võltsimiskindlaks vms) saaks volitamata osapooled hakata moodustama kehtivaid digitaalallkirju. Õnneks on selline üleöö

murdumine väga ebatõenäoline, sest tavaliselt jõutakse edukate rünneteni pika aja jooksul. Kummatigi tuleb vastaval tööl silm peal hoida ja nõrgenev primitiiv aegsasti välja vahetada, mis tähendab kõigi digitaalallkirjade ületöötlemist. See tähendab, et digitaaldokumentide arhiiv ei ole mitte staatiline vaid muutuv andmekogum, See seab olulisi lisanõudeid arhiveerijale.

3.5 Ohud konfidentsiaalsete digitaaldokumentide käsitlemisel

Seni oleme vaikimisi eeldanud, et allkirjastatavad digitaaldokumendid ei sisalda konfidentsiaalset informatsiooni. Konfidentsiaalset informatsiooni sisaldavate dokumentide korral tekivad täiendavad ohud, millega tuleb süsteemide projekteerimisel arvestada. Ehkki see probleem ei ole otseselt seotud digitaalallkirja juurutamisega, kerkib ta tihti esile selliste ülesannete lahendamise juures, kus ka digitaalallkirja vaja läheb, mistõttu sellest ka siin juttu tuleb.

Ennekõike kerkivad konfidentsiaalsusküsimused üles digitaaldokumentide transpordi ning arhiveerimise juures. Dokumendi muudel eluetappidel (näiteks dokumendi ettevalmistamisel arvutis) tagatakse konfidentsiaalsus paljuski samade vahenditega kui terviklus (füüsilise juurdepääsu piiramine arvutile, protsesside mäluruumi eraldatusega, jne). Eraldi vajab käsitlemist veel virtuaalmälu kasutamisest tekkiv konfidentsiaalsete andmete lekke oht.

Digitaaldokumentide transpordi ning arhiveerimise korral liiguvad andmed väljaspool neid kaitsvat arvutisüsteemi, mistõttu tuleb arvestada täiendavate ohtudega.

3.5.1 Konfidentsiaalsete dokumentide transport

Ründajal on võimalik avaliku andmesidevõrgu kaudu edastatavate andmete sisu teada saada mitmel viisil:

- kuulata pealt füüsilisi sidekanaleid,
- muuta andmete teele jäävate võrguseadmete konfiguratsiooni või tarkvara nii, et tekiks võimalus pealt kuulata neid läbivaid andmeid;
- marsruutimisinfot manipuleerides suunata andmed läbi ründaja kontrolli all olevate võrguseadmete.

Toodud loetelu pole kaugeltki ammendav. Praktikas on ainus mõeldav viis edastatavate andmete konfidentsiaalsuse tagamiseks on nende krüpteerimine. Uute vahendite kasutuselevõtuga kaasnevad ka uued ohud. Ründaja saab endiselt andmeid ühel või teisel viisil pealt kuulata, sekkuda võtmevahetusprotokolli käiku, jne. Välja on töötatud terve rida eri omadustega sideprotokolle, mille korrektne kasutamine tagab vähemalt lühiajalises perspektiivis piisava kaitse parimate teadaolevate rünnete vastu. Samas ei ole mitte kõik protokollid mõeldud pikaajalist väärtust omavate konfidentsiaalsete andmete edastamiseks. Ründaja võib salvestada krüpteeritud sideseansid ning dešifreerida need hiljem, siis kui tal on õnnestunud enda valdusesse saada vajalik krüpteerimisvõti. On olemas terve rida protokolle, mis tagavad täieliku tulevikuturbe (*PFS – Perfect Forward Security*). See tähendab, et isegi kui ründaja saab oma valdusesse ühe suhtluspoole pikaajalise võtme, ei saa ta dešifreerida vanu, salvestatud sideseansse. Kasutatud privaatvõtme avalikuks tulekul ei ole täieliku tulevikuturvet tagavate protokollide kasutamisel tagasiulatuvat mõju. Ka ei ole nende protokollide vastu olemas efektiivseid passiivseid ründeid.

3.5.2 Konfidentsiaalsete dokumentide arhiveerimine

Arhiveerimisel võib dokumentide konfidentsiaalsust tagada nii füüsilise juurdepääsu piiramisega arhiivikoopiatele kui ka arhiveeritud dokumentide krüpteerimisega. Arhiivi-

koopiate krüpteerimise korral tuleb lahendada kasutatud krüpteerimisvõtmete haldamise probleem: efektiivse kaitse korral ei ole ka andmete omanikul neid pärast krüpteerimisvõtme hävimist andmeid lugeda. Seetõttu tuleb arhiivikoopiate krüpteerimisvõtmetest säilitada mitut koopiat. Väga pikaealiste dokumentide käsitlemisel tekivad veel järgmised täiendavad probleemid:

1. Digitaaldokumentide allkirjastamiseks kasutatud krüptoalgoritmid võivad murduda, mistõttu dokumentide allkirju tuleb aeg-ajalt värskendada. See eeldab dokumentide ajutist dešifreerimist.
2. Digitaaldokumentide krüpteerimiseks kasutatud algoritmid võivad aja jooksul murduda, mistõttu dokumendid tuleb üle krüpteerida kasutades paremaid algoritme. Seejuures on oluline, et kõik vana algoritmiga krüpteeritud koopiad saaks hävitatud.
3. Andmekandjad, millele digitaaldokumendid on salvestatud, vananevad ning dokumendid tuleb kopeerida uutele andmekandjatele. Selle protseduuri juures tuleb tagada vanade andmekandjate hävitamine.

Üldiselt tekitab konfidentsiaalsete dokumentide pikaajaline arhiveerimine väga suuri probleeme ning mida pikema aja vältel dokumente säilitada soovitakse, seda vähem kasu krüpteerimisest on.

3.6 ID-kaardi rakendamisega seotud ohud

3.6.1 Autentimisprotseduuri üldine kirjeldus

Autentimisvahend – seade, mida kasutatakse isiku digitaalse tunnuse tuvastamiseks

Autenditav isik – isik, kes soovib saada mingit Interneti vahendusel pakutavat teenust ja kelle kohalolu kontrollitakse selle isiku autentimisvahendi abil.

Autenditav arvuti – arvuti, mille vahendusel isik teenust saada soovib (näiteks koduarvuti, tööarvuti, avaliku Internetipunkti terminal vms.)

Autentija arvuti – arvuti, mis on teenuse osutaja valduses ja mida kasutatakse (teenust saada soovivate) isikute autentimiseks. Isik osaleb autentimisprotsessis autenditava arvuti vahendusel.

Autentimisprotokoll – reeglistik autentija arvuti ja autenditava arvuti vaheliseks sõnumivahetuseks, mille eesmärk on tuvastada isik Interneti vahendusel.

3.6.2 ID-kaardi turvamehhanismide üldkirjeldus

ID kaart on isikut tõendavate dokumentide seaduse [11] järgi Eesti Vabariigi kodanikele ja Eestis püsivalt viibiva välismaalastele valjastatav siseriiklik isikut tõendav dokument - isikutunnistus. Vastavalt seadusele kantakse isikutunnistusele digitaalset tuvastamist võimaldav sertifikaat ning digitaalset allkirjastamist võimaldav sertifikaat, kusjuures sertifikaat on piiramata kasutusvaldkonnaga. Vastavalt spetsifikatsiooni kavandile [33] saab ID-kaardil olema kaks võtit – autentimisvõti ja digitaalallkirja võti, mis vastavalt plaanitavale sertifitseerimispoliitikale [13] genereeritakse sertifitseerimisteenuse osutaja poolt. Mõlemate võtmete kasutus on kaitstud eraldi paroolidega:

- autentimisparool koosneb 4-12 numbrimärgist {0,1,…,9}
- digitaalallkirja parool koosneb 5-12 numbrimärgist {0,1,…,9}

Mõlema parooliga on seotud eksimiste loendur, mis normaalolukorras on võrdne 3-ga. Iga vale parooli sisestus vähendab loendurit ühe võrra ja iga korrektne sisestus seab loenduri uuesti võrdseks 3-ga.

3.6.3 Tehnilised ohud autentimisel

3.6.3.1 Autenditava isiku imiteerimine ründaja poolt

Kiipkaardi puhul on see vähetõenäoline oht, kuna isikut imiteerida on raske (praktiliselt võimatu) omamata koopiat autentimisvahendist.

3.6.3.2 Autentimisvahendi kopeerimine

Ka see oht on vähe tõenäoline, kuna autentimisvahendi kopeerimine on raske vahendis (ID-kaardis) sisalduva unikaalse salajase võtme tõttu, mille kasutamine on autentimisprotokollis vajalik, kuid mille väljalugemine kaardist on raske.

3.6.3.3 Autentimisvahendi vargus

Selline oht on väga tõenäoline, samas ohu mõju vähendab autentimisvahendis rakendatav paroolkaitse, st vahend ei hakka tööle ilma vahendi omaniku poolt õigesti sisestatud paroolita.

3.6.3.4 Paroolide läbiproovimine

Selle ohuga tuleb arvestada juhul, kui arvuti on mõeldud ainult autentimiseks, aga mitte digitaalallkirja andmiseks, st arvestatakse võimalust, et arvuti, mille kaudu autentimisprotsess toimub, omab küll ligipääsu autentimisparoolile, kuid mitte digitaalallkirja paroolile. Siis omab mõtet uurida, kas arvuti ei saa juhusliku läbiproovimise teel leida digitaalallkirja andmiseks kasutatavat parooli. Võib kasutada asjaolu, et eksimiste loendur on arvutile kättesaadav ja kui proovida juhuslikult ühte allkirja parooli, siis ebaõnnestumise korral jääb kasutajale veel kaks katset ja suure tõenäosusega ei juhtu kaardiga midagi. Kui kasutaja on hiljem sisestanud üks kord juba õige parooli, siis on loendur jälle võrdne kolmega ja võimalik on proovida järgmist parooli jne.

3.6.3.5 Parooli vargus

See on võimalik, kui autenditav arvuti ei ole usaldusväärne.

3.6.3.6 Autentimisvahendi volitamata kasutus autentija arvuti poolt

Ka selle ohu realiseerumine on suhteliselt raske, sest standardne SSL kliendi autentimisprotseduur ei võimalda autentijal (serveril) kasutada autenditavasse arvutisse (klient) sisestatud autentimisvahendit (ID-kaarti).

3.6.3.7 Autentimisvahendi volitamata kasutus autenditava arvuti poolt

Selline oht on küllalt realistlik, kui autenditav arvuti ei ole usaldusväärne.

3.6.4 Inimfaktorist tulenevad ohud

3.6.4.1 Autentimisparool ja digitaalallkirja parool on seatud võrdseteks.

Mitmete erinevate paroolide meeleshoidmine on raske ja tülikas. Antud juhul on juba ID-kaardi juures kaks erinevat parooli. On üsna suur oht, et paljud isikud, teadvustamata sellest tulenevat ohtu, panevad autentimisparooli ja digitaalallkirja parooli võrdseks, et neid oleks

lihtsam meeles pidada. See asjaolu aga muudab võimalikuks kaarditerminalidel, mis on mõeldud üksnes autentimiseks, võltsida kasutajate digitaalallkirju.

3.6.4.2 Digitaalallkirja parooli üleskirjutamine

Eeldatavasti läheb digitaalallkirja parooli tunduvalt harvemini vaja kui autentimiseks kasutatavat parooli. Kui aga parooli tuleb harva kasutada, siis on üsna suur tõenäosus, et parool läheb lihtsalt meelest ära, mida veelgi võimendab asjaolu, et digitaalallkirja parool on pikem kui autentimisparool. Siit tuleneb oht, et inimesed hakkavad üles kirjutama oma digitaalallkirja paroole, mis aga muudab kaardi varguse ja kaardi väärkasutuse hoopis ohtlikumateks rünneteks. Näiteks kui ründajal on õnnestunud teada saada digitaalallkirja parool, siis tarvitseb ainult mingil moel sekunditeks enda valdusse saada ID-kaart (see on lihtne, kui ründaja ise valdab arvutit või kaarditerminali, kuhu kaart sisestatakse).

3.6.4.3 Isikuid ei ole piisavalt teavitatud ID-kaardiga seotud vastutusest

ID-kaardi saajad ei ole teadlikud ohtudest mis neid kaardi kasutamisel ähvardavad, vastutusest mida kaardi kasutamine endaga kaasa toob ning oma võimalustest ohtudega võidelda.

Digitaalallkirja kontekstis on kõige ohtlikumad ID-kaardi vastu suunatud ründed need, mille eesmärgiks on dokumendi allkirjastamine kasutaja teadmata. Sõltuvalt dokumendist, sellest millistes suhetes (eraõiguslikes või avalik-õiguslikes) seda dokumenti kasutatakse ja sellest kelle nimel see dokument on allkirjastatud (asutuste ja äriühingute juhid saavad allkirjastada oma tööandja nimel) on reeglid kasutaja teadmata loodud dokumendi kehtivuse kohta erinevad.

Avalik-õiguslikes suhetes saaks kasutaja põhimõtteliselt oma digitaalallkirja kasutuvaldkondi piirata, kuid vastavad mehhanismid pole praktikas realiseeritud. Seega kehtivad kõik sellised dokumendid. Samas, kuna huvitatud osapooleks on sellisel juhul enamasti mingi riigiasutus, kelle puhul võib loota, et ta ei lasku kodanike digitaalallkirjade võltsimiseni, siis ei pruugi tegelik risk sedasorti dokumentide kaardiomaniku teadmata allkirjastamiseks olla väga suur. Küll aga võidakse selliseid ründeid võidakse sooritada pigem kättemaksuks, kellegi mustamiseks või huligaansetel ajenditel, sest kodaniku nimel riigiasutustele mingeid dokumente saates võib kodanikule palju pahandust ja ebameeldivusi valmistada. Ainus viis avalik-õiguslikes suhtes antud dokumentide kehtivuse vaidlustamiseks, on ise tõestada, et lepingu alla kirjutamise hetkel ei olnud allkirja andmise vahend allkirja väidetava andja valduses, mis aga praktikas on üsna raske, kui mitte päris võimatu.

Eraõiguslikes suhetes kasutatakse digitaalallkirja vastavalt poolte kokkuleppele. Kui kokkulepet pole, siis digitaalallkirjastatud dokumendid ei kehti. Kokkulepet võib sõlmida mitmel viisil. Käsitleme kaht olulisemat viisi: suuline kokkulepe ja kirjalik kokkulepe.

Kirjaliku kokkuleppe puhul on hästi kaitstud huvitatud osapoole huvid: ta saab veenvalt näidata, et dokumendi aktsepteerimise aluseks oli eelnev kokkulepe. Allkirjastaja ainus võimalus allkirjast taganeda on näidata, et allkirja andmise vahend oli väljunud tema kontrolli alt. Nagu mainitud on see väga raske ülesanne. Seega peab signeerija olema väga hoolas mitmesuguste kirjalike kokkulepete sõlmimisega, kus võivad sisalduda klauslid digitaalallkirja kasutamise kohta, sest sellega võtab ta endale küllalt suure riski.

Suulise kokkuleppe puhul ei ole huvitatud osapoole huvid kuigi hästi kaitstud. Suulist kokkulepet võib vaidluse korral kohtus üritada tõestada vaid mingite kaudsete vahenditega: näiteks kui osapoolte vahelise digitaalallkirja abil toimunud suhtluse tagajärjel on allkirja andja käitunud nii nagu leping kehtiks (näiteks kulutanud ära digitaalse laenulepingu alusel saadud raha, vastu võtnud mingeid kaupu) siis võib kohtunik jõuda järeldusele, et eelnev

suuline kokkulepe eksisteeris. Küll aga pole selge milline see täpselt oli: ka kokkuleppe detailidest võib sõltuda mingi digitaalallkirja kehtivus.

Seega eelneva suulise kokkuleppe korral on digitaalallkirjal ligikaudu sama tõestusväärtus, mis suulisel kokkuleppel endal. Seega peaks soovitama huvitatud osapoolele kindlasti eelneva kirjaliku lepingu sõlmimist.

Suulise kokkuleppe võimalus pakub tehniliselt võimekale ja nahaalsele petturile võimaluse ettevaatamatult kaardiomanikult raha välja petta. Selleks teeb ta kaardiomanikule "kingituse", mille vastuvõtmine annab talle hiljem alust väita nagu eksisteeriks nende vahel mingi kokkulepe. Kui ründaja saab võimaluse allkirjastaja teadmata tema nimel digitaalallkirju anda (näiteks "kingitusega" samasorti esemete ostu-müügilepingutele), saab ta hiljem väita, et ehkki tema on "kauba" üle andnud, pole ta raha saanud. Eduka ründe sooritamiseks peab pettur kohtuni välja minema või oma "võla" kellelegi lihtsameelsele maha müüma.

Mitmesuguseid pettusvõimalusi võib tekkida ka juhul, kui isik annab allkirja teise isiku nimel (näiteks firma juht allkirjastab dokumendi firma nimel). Kui allkirjastajaid on mitu, võib tekkida olukord, kus üks ei tea (veel) teise sõlmitud kokkuleppest ning allkirjastab dokumendi, mis hiljem osutub kehtivaks. Või ei tea kokkuleppe sõlmija sellest, et teine allkirjaõiguslik isik oma ID-kaarti ja ei pööra kokkuleppe digitaalallkirja andmise punktidele tähelepanu.

Igal juhul tekitab firma või ametiasutuse juht ID-kaarti võttes ja sertifikaati mitte peatades suure riski ka enda juhitavale ettevõttele.

Kõigist neist ohtudest tuleb kaardi saajaid teavitada. Neid ohte tuleb arvestada ka vaidluste (näidis)lahendamiste juures.

Neid ohte saaks palju paremini hallata juhul, kui vastutuse võtmine teatud liiki dokumentide eest toimuks ilmutatud kujul, kolmanda osapoole kaasabil. See jätaks palju vähem ruumi hilisemateks (kohtu)vaidlusteks. Nagu eelnevalt öeldud, on DAS kohaselt avalik-õiguslikes suhetes võimalik sertifikaadi kasutusvaldkonda piirata. Mõistlik oleks, kui see võimalus laieneks ka eraõiguslikele suhetele ning lisaks realiseeritaks vajalikud tehnilised vahendid sedasorti piirangute praktiliseks kehtestamiseks.

3.6.4.4 Ebausaldatavad terminalid

Paljud inimesed võivad olla vähe instrueeritud ja mitte teada, et terminalid ei pruugi olla täiesti turvalised. Vähemasti juhul, kui terminal palub kasutajal sisestada digitaalallkirja parooli, aga tegelikult ei kavatsetagi üldse anda digitaalallkirja, vaid kasutada ID-kaardi autentimiseks, siis terminali sellistele palvetele vastata ei tohi, kuna sellega võib kaasneda isikule piiramatu kahju.

3.6.5 ID-kaardi kui autentimisvahendi kasutamise keskkonnad

Autentimisvahendi (ID-kaardi) kasutamine mitteusaldusväärses arvutis on äärmiselt ebasoovitav, sest autenditaval arvutil on alati võimalik täielikult imiteerida isikut autentimisprotokollis ja saada seetõttu isiku nimel mis tahes Internetis pakutavat teenust, eeldusel et teenuse osutaja ei rakenda eraldi paroolkaitset.

Kui aga seda siiski soovitakse teha, tuleb kasutatavad teenused grupeerida, jagades need: (1) turvatundlikeks ja (2) vähem turvatundlikeks teenusteks. Turvalistel teenustel jääb siis ikkagi alles eraldi paroolipõhine autentimine. Isegi siis ei saa turvatundlike teenuste puhul isiku autentimiseks kasutada ebausaldatavat autenditavat arvutit, sest see teeks võimalikuks paroolide varguse ja eraldi paroolkaitse kaotaks mõtte.

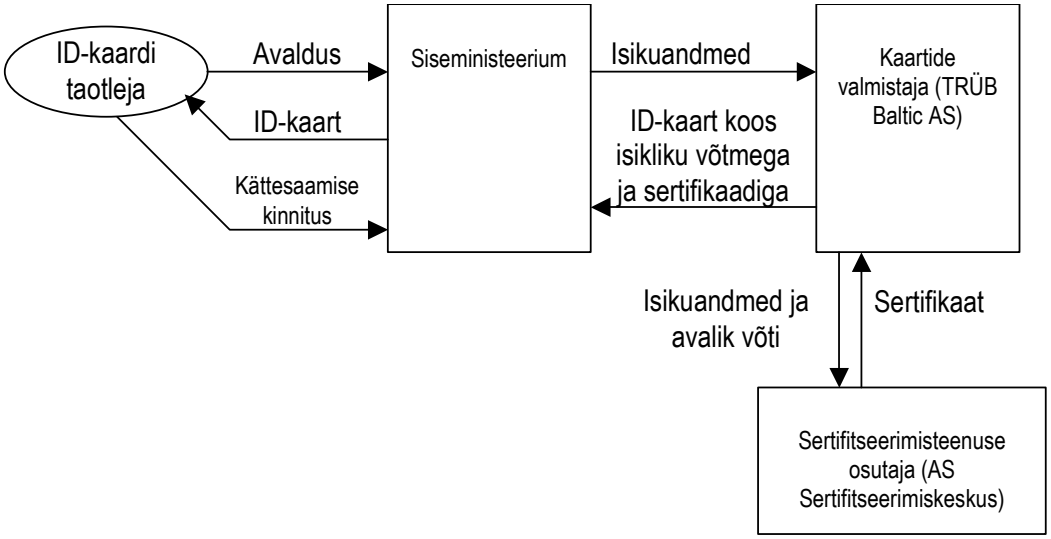
Näide. Juhul kui ID-kaarte saaks kasutada ka ebausaldatavatest arvutitest autentimiseks, siis näiteks pangateenuste jaoks on ikkagi vaja eraldi paroolkaitset: ID-kaardiga seotud autentimisparoolist ei piisa, sest see võib olla sattunud ebausaldatava arvuti kaudu petturite kätte, kel siis avaneb soodne võimalus Interneti kaudu pangakonto tühjendada.

3.6.6 Isikute instrueerimine

Isikuid tuleb tingimata põhjalikult teavitada, kui oluline on autentimisfunktsiooni ja digitaalallkirja funktsiooni lahushoidmine, st et ei pandaks autentimisfunktsioonile ja digitaalallkirja funktsioonile sama parooli.

3.6.7 ID kaardi väljastamisprotseduurist tulenevad ohud

ID-kaardi väljastamise protseduur on kirjeldatav järgmise skeemi abil:



Joonis 5. ID-kaardi väljaandmise protseduuri skeem.

1. Kodanik esitab Siseministeeriumile avalduse ID-kaardi saamiseks. Avalduses sisaldub:
   - viide taotletava sertifikaadi sertifitseerimispoliitikale;
   - märge selle kohta, et klient volitab kaartide valmistajat (TRÜB Baltic AS) genereerima kliendile võtmepaari;
   - märge selle kohta, et klient volitab sertifitseerimisteenuse osutajat (AS Sertifitseerimiskeskus) genereerima kliendi võtmepaarile vastava sertifikaadi;
   - viide teavituskanalile, mille kaudu edastatakse kliendile sertifitseerimisteenuse osutamisel tekkinud informatsiooni (näiteks informatsiooni sertifikaadi peatamise kohta);
2. Siseministeerium edastab isikuandmed kaartide valmistajale, kes kannab isikuandmed kaardile, genereerib vajalikud võtmed ja edastab isikuandmed ja avalikud võtmed sertifitseerimisteenuse osutajale.
3. Sertifitseerimisteenuse osutaja annab välja sertifikaadid (ühe autentimiseks ja teise digitaalallkirja andmiseks) ja saadab need kaartide valmistajale tagasi.

4. Kaartide valmistaja salvestab sertifikaadid kaardile ja edastab kaardi Siseministeeriumile.
5. Siseministeerium annab kaardi otse või vahendaja kaudu edasi ID-kaardi taotlejale, kes kirjutab omakäeliselt alla ID-kaardi väljastamise akt-blanketile (kinnitus, et ID-kaart on kätte saadud).

Tundub, et EstEID (Versioon 1.1) sertifitseerimispoliitika kavandi [13] koostamisel on arvestatud peamiselt autentimisfunktsiooniga ja pakutavad teenused võimaldavad kaardil seda funktsiooni ka edukalt täita. Tõestusfunktsioonile ei ole aga pööratud piisavat tähelepanu. Ennekõike väljendub see alaspetsifitseeritud kaardi väljastusprotseduuris, mis loob kaardi omanikule võimaluse taganeda antud allkirjadest. Väite illustreerimiseks vaatleme järgmist olukorda:

- Isik *A* taotleb ID-kaarti vastavalt ülalkirjeldatud protseduuridele.
- *A* allkirjastab ID-kaardiga mõned dokumendid.
- *A* tühistab ID-kaardi ja hävitab selle, viidates kaardi kadumisele.
- *A* eitab dokumentidele alla kirjutamist, väites et ta ei ole oma kaardiga andnud ühtegi allkirja.
- Kohtuvaidluse käigus esitab huvitatud pool kohtule digitaalallkirjaga dokumendi, sertifitseerimisteenuse osutaja poolt allkirjastatud sertifikaadi ja kinnituse et sertifikaat kehtib (st kehtivustõendi).
- *A* eitab endiselt allkirja andmist, väites et ta on küll ID-kaardi saanud, kuid ei ole seda kaarti kunagi allkirja andmiseks kasutanud.

Väga oluline on teada, milline on antud juhul kohtuvaidluse edasine käik. On mitu võimalust:

- Tõestuskohustus läheb üle sertifitseerimisteenuse osutajale, kes peab tõestama, et sertifikaadi väljaandmiseks *konkreetsele avalikule võtmele* oli alus, näiteks Siseministeeriumi poolt saadetud andmed. Kui need andmed saadeti Siseministeeriumist sertifitseerimisteenuse osutajale elektrooniliselt, siis peavad ka need olema allkirjastatud Siseministeeriumi ametniku poolt ja allkirja õigsus tõestatud. Siin tekib aga probleem, kui allkirja õigsuse tõestamiseks püüab sertifitseerimisteenuse osutaja kasutada iseenda poolt välja antud kehtivustõendit (sertifitseerimisteenuse osutajale ei ole enam erapooletu tunnistaja rollis!). Seega antud juhul suure tõenäosusega kannab vastutust allkirja õiguslike tagajärgede eest sertifitseerimisteenuse osutaja, st on kohustatud hüvitama huvitatud osapoolele tekitatud otsese ja kaudse kahju.
- Tõestuskohustus läheb üle Siseministeeriumile, kes peab tõestama, et isikule anti just sellele avalikule võtmele vastav ID-kaart. Seda aga ei ole praegusi protseduurireegleid arvestades võimalik tõestada, sest kaart ise on hävinenud. Riik on siis tõenäoliselt kohustatud hüvitama huvitatud poolele tekitatud otsese ja kaudse kahju (Riigivastutuse seadus)
- Kohtusse kutsutakse tunnistajaks kaardi valmistaja, kelle poolt antud tunnistus loetakse otsustavaks ja seda ei vaidlustata. Sellega aga antakse kaardi valmistajale väga suured volitused – mõjutada kõiki digitaalallkirjaga dokumente tõenditena käsitletavate kohtuprotsesside (tsiviil-, haldus- ja kriminaalõiguslike) lahendeid. Tundub kaheldav, kas selline otsust üldse võimalik on.
- Tõestuskohustus läheb tingimusteta üle allkirja väidetavale andjale. See annaks aga kaardi väljaandjatele (kõigile protsessis osalenud isikutele) piiramatu võimaluse ükskõik millise

Eesti Vabariigi elaniku nimel allkirju anda, ilma et elanikel oleks võimalus end kohtus kaitsta.

Probleemi juured peituvad ennekõike keerulistes vastutussuhetes, neid saaks (vähemalt formaalselt) vähendada, kuid kodaniku poolt kaardi vastuvõtmisel omakäeliselt allkirjastatav paberdokument sisaldaks ka kodaniku avaliku võtit.

4. Digitaalallkirja rakendamist toetavad initsiatiivid

4.1 Riiklikud registrid

Riiklikud registrid on volitusinfo võimalikud allikad, kuigi paraku registrite praeguses seisus on neis registreeritav teave volituste kohta ebapiisav, samuti ei rahulda ka praegused nõuded andmete aktualiseerimisele. Samas on võimalik olemasolevate registrite andmekoosluse täiendamisel ning andmete aktualiseerimisnõuete tõhustamisel neid kasutada ka tugisüsteemidena digitaalallkirja rakendamisel.

4.1.1 Äriregister

Äriregistrit peetakse Äriseadustiku [19] alusel kohtute registriosakondade poolt, Keskäriregistrit haldab Justiitsministeeriumi Registrikeskus. Keskäriregister sisaldab infot juriidiliste isikute ja füüsilisest isikust ettevõtjate kohta (juriidilise isiku registrikood, nimi ja kontaktandmed, põhikirja registreerimisega seotud andmed, omakapitali suurus, juhtkonna andmed jms). Hetkel Äriregistrisse kantud andmetest on digitaalallkirja rakendamise projekti jaoks kõige huvipakkuvamad andmed juhtkonna kohta, mis sisaldavad informatsiooni äriühingute juhatuse ning nõukogu koosseisu kohta.

Äriregistri kasutamist digitaalallkirja rakendamise projektis piirab hetkel Äriseadustikust tulenev nõue, et registripidajale esitatud dokumentide läbivaatamine ning kandeotsuse tegemine toimub kirjalikus menetluses (§22 lg (5)), samuti aktualiseerimisprotsessi aeglus, mis samuti on sätestatud Äriseadustikus - registripidaja teeb kande registrisse hiljemalt viiendal tööpäeval pärast kandeotsuse allakirjutamist (§33 lg (4)). Ka hetkel kehtivad nõuded äriühingute andmete muudatuste esitamiseks Äriregistrile on suurusjärgus 2 kuni 6 kuud, mis digitaalse asjaajamise rakendumisel kindlasti läbivaatamisele peaksid kuuluma. Äriregistri tehnoloogiline lahendus võimaldaks olemasolevat süsteemi kindlasti ka digitaalallkirja tugisüsteemina kasutada.

Tegelikult tuleb võimaliku volitusinfo allikana vaadelda ka Äriregistriga samas tehnoloogilises keskkonnas peetavaid mittetulundusühingute, sihtasutuste ja laevaregistreid. Kuna ka nende registrite andmete esitamis- ja aktualiseerimisnõuded on analoogilised Äriregistriga, siis kasutamiseks digitaalallkirja juurutamise tugisüsteemina vajavad nad samuti muutmist.

4.1.2 Riigi- ja kohaliku omavalitsuse asutuste riiklik register

Riigi- ja kohaliku omavalitsuse asutuste riiklikku registri [35] vastutav ja volitatud töötleja on Rahandusministeerium. Registrisse kantakse andmed järgmiste riigi- ja kohaliku omavalitsuse asutuste kohta:

1. valitsusasutused
2. valitsusasutuste hallatavad riigiasutused
3. valla või linna ametiasutused
4. valla või linna ametiasutuste hallatavad asutused

Registris võib registreerida ka valitsusasutuste piirkondlikke struktuuriüksusi, kui see on sätestatud vastava valitsusasutuse põhimääruses. Eelnevalt (kuni 2001.aastani) on see info olnud ka Keskäriregistris (Ettevõtteregistri andmed, nüüdseks mitteaktualiseeritav).

Vastavalt riigi- ja kohaliku omavalitsuse asutuste riikliku registri pidamise põhimäärusele [18] kantakse registrisse andmed ka asutuste kinnitatud ja komplekteeritud koosseisu kohta (§6 p.8), kuid need on vaid arvnäitajad ja ei sisalda informatsiooni konkreetsete töötajate kohta, isegi mitte asutuse juhi kohta. Registriandmete koosseisu täiendamisel vastava asutuse

nimel toiminguid tegema volitatud isikute andmetega ning nende andmete piisavalt kiire aktualiseerimise tagamisel oleks riigi- ja kohaliku omavalitsuse asutuste riiklik register kasutatav ka digitaalallkirja rakendamise tugisüsteemina. Samas dubleeritaks sellise lahenduse puhul mingil määral plaanitavat riigiametnike registrit (vt.4.1.3). Selge ei ole ka riigi- ja kohalike omavalitsuse asutuste registri ja täpselt reguleerimata initsiatiivi http://www.riik.ee/ab/ suhe (viimast esitletakse veebis kui Riiklike institutsioonide info-süsteemi [34], aga informatsiooni selle süsteemi ülesehituse, volituste ja aktualiseerimis-mehhanismide kohta ei õnnestunud leida)

4.1.3 Riigiametnike register

Riigiametnike register ehk korrektsema nimetusega Avalike teenistujate andmebaasi hankimiseks korraldati hankekonkurss 2001.a. kevadel, vastavalt pakkumiskutse dokumentidele [10] hangiti andmebaas, milles olevate andmete avaldamine internetis peab olema lihtne ja mugav kasutada, võimaldama teostada interneti kaudu ka lihtsamaid statistikapäringuid ning peab olema integreeritav olemasoleva www.riik.ee/ab/ veebipõhise "Isikute ja asutuste" andmebaasiga. Avalike teenistujate andmebaas peab toetama mitmesugust aruandlust ning tagama üleriigiliste ametnike personaliandmete kiire kättesaadavuse ja seoste nägemise ametiasutuste, nende koosseisude ja ametnike andmete vahel. Avalike teenistujate andmebaas kogub andmeid riigiasutuste personaliarvestuse süsteemidest automaatse andmeedastuse teel.

Vajaliku aktualiseerimiskiiruse ning info käideldavuse tagamisel oleks riigiametnike register sobilik volitusinfot sisaldav tugisüsteem digitaalallkirja rakendamisel.

4.2 Teenuseosutajad

4.2.1 Sertifitseerimise Riiklik Register (SRR)

SRR on vastavalt digitaalallkirja seadusele loodud riiklik register, mille vastutavaks töötlejaks on Teede- ja Sideministeerium ning volitatud töötlejaks Sideamet. SRR ülesandeks on registreerida sertifitseerimis- ja ajatempliteenuse osutajaid (vastavalt STO ja ATO) ning väljastada vastuseid registripäringutele.

SRR-s registreeritud teenuseosutajate poolt väljaantud sertifikaadid ja ajatemplid on digitaal-allkirja seaduse järgselt sobivad kasutamiseks avalikus sektoris, sõltuvalt sertifikaatidesse märgitud kasutusvaldkonna piirangutest.

4.2.2 AS Sertifitseerimiskeskus

AS Sertifitseerimiskeskus on Eesti Telekomi, Hansapanga ja Ühispanga initsiatiivil loodud sertifitseerimisteenuse osutaja. Sertifitseerimiskeskus on hetkel ainsa STO-na registreeritud SRR-s.

Siseministeeriumi poolt korraldatud hankekonkursi tulemusena hakkab AS Sertifitseeri-miskeksus oma sertifitseerimisteenuseid pakkuma EV isikutunnistuse projektis (ID-kaart). Lisaks osutab AS SK ID-kaardi projektis isikutunnistuste levitusteenust ning tagab kaardi valdajatele täisteeninduse läbi Ühispanga ja Hansapanga struktuuride.

Digitaalallkirja juurutamise projektis on võimalik AS SK kasutada sertifitseerimisteenuse osutajana. Võimalik on AS SK teenuseid kasutada ka sertifikaatide väljastamiseks kiipkaardil.

4.3 Riiklikud programmid ja projektid

4.3.1 Valitsusasutuste dokumendihalduse programm (DHP)

DHP on Riigikantselei algatatud valitsusasutuste koostööprogramm üleminekuks digitaalsele dokumendihaldusele valitsusasutuste vahelises asjaajamises. DHP kestuseks on ette nähtud aastad 2000-2002 ja selle aja jooksul tahetakse jõuda tulemusteni kolmes valdkonnas (vt ka http://www.riik.ee/dhp):

1. riigi asjaajamise ettevalmistamine üleminekuks digitaaldokumentide põhisele töökorraldusele (sh digitaalallkirjade kasutamisele);
2. vajalike rakenduslike õigusaktide väljatöötamine;
3. digitaalseks asjaajamiseks vajalike infotehnoloogiliste standardite ning metoodika väljatöötamine.

Riigi asjaajamises ringlevate dokumentide elutsükkel lõppeb arhiveerimisega. Samas on arhiveerimisele esitatavad nõudmised karmimad kui tavaringluse korral, kuivõrd dokumendid peavad olema ligipääsetavad veel aastakümneid. Seepärast on DHP üks olulisi tegevussuundi arhiivindusstrateegiate ja -standardite väljatöötamine. Suurimaks käsitlemist vajavaks riskiks selles vallas osutub ühest küljest salvestusmeedia moraalne ja füüsiline ning teisest küljest kasutatavate dokumendiformaatide moraalne vananemine. Nende probleemide lahendamiseks teeb DHP tihedat koostööd Riigiarhiivi ja selle infosüsteemiosakonnaga.

Kui salvestusmeedia vananemise vastu saab võidelda varukoopiate tegemise ning optimaalsete säilitustingimustega, siis dokumendiformaatide vananemine kujutab enesest tunduvalt raskemat probleemi. Juhtiva kontoritarkvara tootja Microsofti turustrateegia on oma failivormingute pidev muutmine ning seetõttu tuleb pikaajalise säilitatavuse tagamiseks eraldi vaeva näha. DHP raames kaaluti läbi erinevaid lahendusvariante ning otsustati soovitada riigiasutuste vahelises asjaajamises XMLi kasutamist. XMLi kasutuselevõtu kasuks räägivad järgmised argumendid:

- XML on struktureeritud vorming, mis toetab dokumentidele metaandmete lihtsat lisamist;
- XML on avalik ja standardne;
- XML-dokumendid sobivad veebis esitamiseks;
- on välja töötatud mitmed metoodikad XML-dokumentidele digitaalallkirjade lisamiseks.

XML-põhisele asjaajamisele üleminekuks tuleb lahendada mitmeid probleeme. XML-keeles tuleb kirjeldada kõigi riigi asjaajamises kasutatavate dokumentide struktuur. DHP raames on näidisena valminud asutustevahelise kirja struktuur, kuid sellesisulist tööd tuleb jätkata.

Nagu ülal mainitud, ei toeta hetkel valdav MS Office kontoripakett vaikimisi sobival kujul XMLi. Seepärast tuleb välja töötada XMLi MS Office'iga integreerimise strateegia ja/või üleminekustrateegia alternatiivsele tarkvarale.

Pole selge, milline erinevatest XML-dokumendile digitaalallkirja lisamise meetod on sobivaim. Ka selle otsuse langetamine seisab veel ees.

Loomulikult ei saa uuele asjaajamise korrale üle minna üleöö, peale täienduste tarkvaras tuleb täiendada ka kasutajate teadmisi. Selleks on DHP ühe tegevussuunana 2001. aastal ette nähtud mitmekülgse koolituse korraldamine riigiasutustes, mille läbimine annab osalejatele teadmised digitaalse dokumendihaldusega seotud õigusaktidest, digitaalsete dokumentide loomisest, ringlusest ja säilitamisest ning digitaalallkirja kasutamisest. Koolitusprojekti käigus luuakse ka vastavad õppematerjalid, mis saavad kõigile soovijaile avalikuks.

Viimase suurema osa DHP tegevusest moodustab mitmesuguste digitaalse asjaajamise pilootprojektide käivitamine. Nii näiteks loodi 2000. aasta lõpul Riigikantselei, Majandusministeeriumi ja Justiitsministeeriumi osalusel seaduseelnõude kooskõlastamise pilootrakendus eÕigus. Seda menetluskeskkonda toetavad ka digitaalne Riigi Teataja, õigusaktide register ja Vabariigi Valitsuse infosüsteem. 2001. aasta algul testis DHP digitaalset asjaajamist praktikas Rahandusministeeriumi ning Teede- ja sideministeeriumi vahel Postipoisi tarkvara vahendusel. Digitaalarhiivi loomist katsetati 2001. aastal koostöös Maksuametiga tuludeklaratsioonide elektrooniliseks arhiveerimiseks. Käesoleval hetkel käivad projektid on E-maakond (Eesti maakondade dokumendisüsteemide ühtlustamiseks) ning DHP loodab tuge saada ka digitaalallkirja rakendamise projektist.

4.3.2 Riigi andmekogude teeninduskihi loomise projekt (X-tee)

X-tee projekti algseks eesmärgiks oli "välja arendada tarkvaraliste, riistvaraliste ja organisatsiooniliste meetmete kogum riigi halduses olevate andmekogude ühtlustatud kasutamiseks". Kuna X-tee arhitektuur on piisavalt üldine, saab valmivat infrastruktuuri kasutada tegelikult suvaliste sõnumite (mitte ainult andmebaasipäringute ja –vastuste) liigutamiseks asutuste vahel. X-tee süsteemi võimaluste täielikumaks mõistmiseks olgu siinkohal esitatud väga kokkuvõtlik ülevaade süsteemi arhitektuurist.

Vastavalt X-tee projekti turvaanalüüsi tulemustele on X-tee süsteemi näol realiseeritud kahetasemeline autentimise, pääsuõiguste kontrolli ja tõendusmaterjali tekitamise süsteem. Need kaks taset on asutustevahelise suhtluse tase ning asutusesisese suhtluse tase. X-tee tegeleb ennekõike asutustevahelise suhtluse vahendamise ja turvamisega. Asutusesisese suhtluse organiseerimine on jäetud asutuse enda hooleks (teatud minimaalsed vahendid selleks projekti raames siiski luuakse).

4.3.2.1 Asutustevaheline suhtlus

Asutustevahelise suhtluse korraldamisega tegelevad X-tee keskserverid ning X-tee turvaserverid. Keskservereid haldab X-tee keskus, turvaservereid aga X-teega liitunud organisatsioonid (igaüks omi). X-teega liitumine eeldab lepingu sõlmimist X-tee organisatsiooniga, milles liituja kohustub täitma X-tee reegleid ja protseduure ning võtab endale vastutuse enda valduses olevate turvaserverite poolt saadetud sõnumite eest. Just see organisatsiooniline pool ja sõlmitavad lepingud annavad loodud infotehnoloogilistele vahenditele mõtte ja võimaldavad neid kasutada reaalses asutustevahelises suhtluses.

X-tee turvaserverid tegelevad muuhulgas edastatavate sõnumite salastatuse, autentsuse ning konfidentsiaalsuse tagamisega, kuid digitaalallkirja juurutamise projekti kontekstis on vast kõige olulisem see, et X-tee süsteem suudab anda vahendatud sõnumitele tõestusväärtuse. Tõestusväärtus tekib järgmiste organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete koostöös:

1. X-tee liitumislepingus võtab liituv organisatsioon endale vastutuse tema valduses olevate turvaserverite poolt väljastatud sõnumite eest.
2. X-tee turvaserverid signeerivad kõik väljuvad sõnumid võtmega mis on liitumisprotsessi käigus registreeritud antud asutuse nimele.
3. X-tee turvaserverid logivad kõik vastuvõetud sõnumid krüptograafiliselt kaitstud logisse.
4. X-tee turvaserverid saadavad X-tee keskserverile perioodiliselt logide vaheväärtusi. See välistab turvaserveri logide hilisema muutmise turvaserveri haldajate poolt.

Vaidluse korral on sõnumi vastuvõtjal koostöös X-tee keskusega alati võimalik teatud kindlusega näidata, milline asutus, millal ja millise sõnumi talle saatis. Tähelepanuväärne on, et X-

tee süsteemi poolt sõnumite kaitseks kasutatavate meetmete kompleks vastab ühtlasi ka digitaalallkirja seaduse paragrahvis 2 toodud digitaalallkirja definitsioonile.

Kokkuvõtteks võib öelda, et X-tee on kindlasti kasutatav oma peaeesmärgi täitmiseks: allkirjastatud registriväljavõtete liigutamiseks asutuste vahel. X-tee võib digitaalallkirja juurutamise projektis olla kasutatav ka muuks otstarbeks, näiteks mingite alamülesannete lahendamiseks:

- allkirjastatud sõnumite turvalise transpordi korraldamiseks asutuste vahel;
- vahendatud sõnumite arhiveerimiseks vms.

Erinevate kasutusviiside võimalikkus sõltub vaid kokkulepetest ning turvaserverite vahendusel suhtlevate infosüsteemide suutlikkusest.

4.3.2.2 Asutusesisene suhtlus

Võib tekkida küsimus, kelle nimel siis turvaserver ikkagi allkirju annab. Kui lähtuda eeldustest, et juriidilisel isikul endal allkirja pole ning et juriidilise isiku tegevuse eest vastutab tema juht, siis võib öelda, et turvaserver annab allkirju juriidilise isiku juhi nimel.

Juhul kui asutuse juht ise turvaserverid ei halda (suurema asutuse puhul on see ilmselt nii) ja selleks on palgatud eraldi süsteemiülem, siis tuleb vastutus süsteemi korrektse administreerimise eest ametijuhendiga panna süsteemiülema õlule. Juhul kui turvaserveri kaudu saavad sõnumeid saata ka teised isikud peale asutuse juhi, siis tuleb vastutus süsteemi korrektse ja õiguspärase kasutamise eest ametijuhenditega panna neile töötajatele.

Sellisel juhul vastutab saadetud sõnumi eest asutuse juht, juhul kui ta ei ole võimeline näitama, et:

1. sõnumi saatmise põhjustas süsteemiülem oma reeglitevastase käitumisega või;
2. sõnumi saatmise põhjustas mõni töötajatest oma reeglitevastase käitumisega.

Kuna süsteemiülema-kindla infosüsteemi tegemine ja ekspluateerimine on väga kallis, X-teega liituvaid asutusi väga palju ning paljud vajalikud rakendused ei vahenda nii tähtsaid sõnumeid, et see kulu oleks õigustatud, siis ei ole majanduslikel kaalutlustel turvaserverites ette nähtud mingeid erimeetmeid süsteemiülema tegevuse hilisemaks tõestamiseks. Pahatahtliku süsteemiülema tegevust saab tõestada vaid kaudsel viisil, seega tuleks süsteemiülemaks valida võimalikult usaldusväärseid isikuid.

Mis puutub ametnike tegevuse tõestamisse, siis kuna ametnikud saavad turvaserveriga suhelda (saata sõnumeid) vaid asutuse infosüsteemi vahendusel, võib nende tegevuse tõestamiseks kasutada kuitahes kindlaid meetodeid. Näiteks võib ametnik infosüsteemile esitatava päringu allkirjastada oma isikliku digitaalallkirjaga. Infosüsteem edastab päringu sisu pärast ametniku volituste kontrolli läbi turvaserveri teisele asutusele. Seega saab töötajate reeglitevastast käitumist tõestada kasutades nende poolt digitaalselt allkirjastatud dokumente.

Tuleb tähele panna, et see on ainult üks võimalus seda probleemi lahendada. X-tee süsteem ei soodusta ega pärsi seda kuidagi, jättes selle täielikult asutuse infosüsteemi loojate otsustada. Projekti raames valmiv MISP süsteem ei toeta vähemalt esimeses versioonis digitaalallkirja andmist, kuid vajadusel on selline funktsionaalsus süsteemile lisatav.

4.4 Pilootprojektid

4.4.1 Digitaalallkirja kasutamise testimine eÕiguse pilootprojektis

2000.aasta sügisel alustati Majandusministeeriumi, Justiitsministeeriumi ja Riigikantselei osavõtul õigusaktide eelnõude elektroonilise kooskõlastamise pilootprojekti eÕigus läbiviimist. Kuna seaduseelnõude korral on dokumentide autentsus ja terviklikkus esmatähtsad, moodustab digitaalallkirja kasutamine eÕiguse olulise osa. Digitaalselt tuleb allkirjastada kõik n.ö. ametlikud dokumendid - esitluskiri, eelnõu, kooskõlastuskiri jmt.

Projekti I etapis töötati välja menetlemise funktsionaalsed nõuded ning katsetati signeerivate dokumentide vorminguna PDF-formaati ja signeerimiseks TrueSign Sognerit. Digitaalselt allkirjastab dokumendid vastavalt allkirjaõigust omav ametnik. Allkirjaõigus tuleneb samadest aktidest, mis hetkel allkirjaõigust reguleerivad - Vabariigi Valitsuse reglement, asutuse põhimäärus, asjaajamiskord, struktuuriüksuste põhimäärused, ametnike ametijuhendid, samuti muud aktid, mis reguleerivad erinevate õigusaktide andmist.

eÕiguse pilootprojekt käsitleb ka erinevaid digitaalallkirja rakendamise stsenaariume, pakkudes näiteks välja lahendused juhtudeks, kui sama dokumendi signeerib üks või mitu osapoolt.

Projekti II etapi rakendamise tähtaeg on aprill 2002., milleks tuleb rakendada süsteem, kus õigusaktide eelnõude elektrooniline menetlemine võetakse kasutusele kõigi ministeeriumide poolt. II etapis peab eÕigus hõlmama endas ka digitaalallkirja tõestusväärtuse pikaalajise säilitamise meetodeid (ajatembeldust, valideerimsiteenust)

5. Riigiasutuste prioriteedid

Väga üldisel tasemel taanduvad riigiasutuste digitaalallkirja rakendamisega seonduvad protsessid järgmistele tegevustele:

1. Digitaaldokumentide vastuvõtmine (st. on vajadus olla võimelised vastu võtma ja töötlema digitaalselt esitatud dokumente)
2. Digitaalne arhiveerimine (digitaalselt esitatud dokumentide arhiveerimine)
3. Automaatsete õigusjõuga andmebaaside ja registrite päringuvastuste genereerimine
4. Elektrooniline asjaajamine, st tööprotsesside maksimaalne toetamine digitaalse tehnoloogiaga nende kiirendamise ja jälgitavuse parendamise huvides (sealhulgas digitaalallkirja loomise ja allkirjastamise vahendid)
5. ID-kaardi põhine kasutajate autentimine (kasutamaks ära võimalust, et kõigil Eesti Vabariigi residentidel saab olema vahend, mis tagab isiku digitaalset autentimist).

Olenevalt oma tööprotsesside iseloomust peavad erinevad asutused prioriteetsemaks erinevaid tegevusi, ent ülaltoodud viite protsessi läheb lõppkokkuvõttes vaja kõigil asutustel.

Järgnevalt esitatakse võimalik loend ministeeriumide lõikes prioriteetseks peetavatest toimingutest, kus digitaalallkiri võiks olla rakendatav. Kui ministeeriumil on juba ka käimasolevaid pilootprojekte digitaalallkirja rakendamiseks, siis on toodud ka viited projektidele.

5.1 Rahandusministeerium

Rahandus ministeeriumi haldusalas on kaks suuremahulise infotöötlusega riigimaksude kogumisega tegelevat ametit - Maksuamet ning Tolliamet - ning mõnes mõttes sama tegevusega seonduv Riigikassa.

Hetkel on Maksuamet oma prioriteete ette näinud järgmises järjekorras:

1. ID-kaardi põhine autentimine Maksuameti infosüsteemis (e-Maksuametis)

2. Digitaalarhiivi rakendamine

3. e-Maksuameti kasutamise lepingute digitaalne sõlmimine (nii juriidiliste isikute poolt volitatud isikute kui ka füüsiliste isikutega)

4. Digitaalselt esitatavad avaldused käibemaksukohustuslaste ja/või füüsilisest isikutest ettevõtjate registrisse kandmiseks

5. Muude dokumentide digitaalne esitamine (sealhulgas maksudeklaratsioonid)

Näiteid käimasolevatest pilootprojektidest:

5.1.1 E-riigikassa

- Riigiametnik esitab digitaalallkirjaga maksekorralduse Riigikassale;
- Riigikassa teostab esitatud maksekorralduse põhjal ülekande pangasüsteemis Interneti kaudu.

Riigikassa peab säilitama digitaalallkirjaga maksekorralduse, sest viimane tõestab, et ülekande tegemiseks oli alus. Kehtiva digitaalallkirja korral läheb tõestuskohustus üle maksekorralduse allkirjastanud ametnikule. Antud stsenaariumis jagunevad rollid järgmiselt:

Allkirja andja: Mingi riigiasutuse ametnik, kes allkirjastab maksekorralduse.

Huvitatud osapool: Riigikassa.

Märkus: Riigikassa kontrollib maksekorralduse põhjendatust ainult maksekorraldustel, mille väärtus on suurem kui sada tuhat krooni.

5.1.2 Maksudeklaratsioonid

- Füüsiline isik või juriidiline isik esitavad Maksuametile vastavalt tulu- või käibe-maksudeklaratsiooni, mis on isiku või tema esindaja poolt digitaalselt allkirjastatud.
- Maksuametnik (inspektor) kontrollib deklaratsioonis esitatud andmeid ja andmete korrektsuse korral koostab otsuse ning edastab osakonnajuhatajale
- Osakonnajuhataja kontrollib otsuse õigsust, allkirjastab otsuse ning saadab Maksuameti laekumise talituse töötajale digitaalselt allkirjastatud maksekorralduse deklaratsioonis märgitud tagastatava summa ulatuses.

Maksuametnik ei saa kunagi täielikult kontrollida esitatud deklaratsiooni õigsust. Pettus võib välja tulla hiljem – siis kui raha on juba üle kantud. Sellepärast on siin esitatud deklaratsiooni tõestusväärtus oluline.

Selles protsessis võib oluline olla ka digitaalallkirja kasutamine Maksuameti siseses dokumendivahetuses: ka osakonnajuhataja ei saa täielikult kontrollida inspektori otsuse aluseks olnud dokumente ning seetõttu täielikult veenduda inspektori otsuse õigsuses.

Allkirja andja: Füüsiline isik (kodanik) või juriidilise isiku esindaja

Huvitatud osapool: Maksuamet

Allkirja andja: inspektor

Huvitatud osapool: osakonnajuhataja

Allkirja andja: osakonnajuhataja

Huvitatud osapool: laekumise talituse töötaja

5.1.3 Tollideklaratsioonid

- Füüsiline või juriidilise isiku esindaja esitab Tolliametile digitaalselt allkirjastatud tollideklaratsiooni, milles sisaldub üleviidava kauba kirjeldus ja kogus.
- Tolliametnik arvutab tollimaksu suuruse ja saadab deklaratsiooni esitajale vastu maksekorralduse tollimaksu tasumiseks. Tolliamet säilitab deklaratsiooni.
- Füüsiline või juriidiline isik tasub tollimaksu.
- Kui kaup saabub piirile, siis (mingi teine) tolliametnik kontrollib selle kirjeldust, kogust ja vajaliku tollimaksu tasumist. Kui kõik klapib deklaratsioonis esitatuga, siis laseb kauba läbi.

Allkirja andja: Füüsiline või juriidiline isik.

Huvitatud osapool: Tolliamet

5.2 Justiitsministeerium

Justiitsministeeriumi haldusalasse kuuluvad riigiasutused võib jaotada kolmeks grupiks. Esimesse gruppi kuuluksid **kohtud, prokuratuur, vanglad, kriminaalhooldus**. Selle grupi riigiasutuste esmaseks prioriteediks on nii kohtu- kui tsiviilmenetlusprotsessi maksimaalne digitaliseerimine nii aja kui ka muude ressursside kokkuhoiu eesmärgil. Menetlusprotsesside iga samm peab olema tõendatav, kogu dokumendivahetus arhiveeritakse.

Üldistest prioriteetidest on seega olulised:

1. Digitaalsete dokumentide vastuvõtt ja edasine töötlus
2. Tööprotsesside maksimaalne digitaliseerimine
3. Digitaalne arhiveerimine

Teine grupp moodustub avalik-õiguslikke ülesandeid täitvatest eraõiguslikest isikutest (**Advokatuur, Notariaat, kohtutäiturid, pankrotihaldurid**). Nende esmaseks prioriteediks on ilmselt olla võimelised vastu võtma digitaalseid dokumente, aga edaspidi ka ülejäänud ülaltoodutest.

Kolmanda grupi moodustavad **Registrikeskus, Registriosakonnad ning Kinnistusametid,** kes tegelevad riigi põhiregistrite (äriregister, kinnistusraamat) ning muude registrite (sihtasutuste register, mittetulundusühingute register, kommertspandi register, laevaregister) pidamisega.

Neil lisandub ülaltoodud kolmele veel ka

4. automaatsete õigusjõuga päringuvastuste genereerimine.

Näiteid protseduuridest:

5.2.1 Kohtuasja menetlus

Kohtuasja andmete sisestamine arvutisüsteemi.

Süüdistusakti koostamine:

- Prokurör tutvud kohtuasjaga seotud materjalidega ja
- Allkirjastab süüdistusakti.

Kohtuniku määrus:

- Kohtunik tutvub arvutisüsteemi abil kohtuasjaga seotud materjalidega; ja vajadusel
- Kohtunik allkirjastab kohtuniku määruse

Eksperdi arvamus:

- Ekspert tutvub kohtuasjaga seotud materjalidega
- Allkirjastab eksperdi arvamuse

5.2.2 Kohtuotsuse täitmine

Vangla teavitamine kohtuotsusest:

- Kohtunik saadab vanglale digitaalselt allkirjastatud kohtuotsuse
- Vangla viib kohtuotsuse täide (kedagi hoitakse vangis või vabastatakse ennetähtaegselt vms.) ja hoiab alles dokumendi.

5.3 Riigikantselei

Riigikantselei on digitaalallkirja juurutamise projektiga tihedalt seotud Valitsusasutuste dokumendihalduse programmi (DHP) vastutavaks täitjaks. DHP on Riigikantselei algatatud valitsusasutuste koostööprogramm üleminekuks digitaalsele dokumendihaldusele valitsus-asutuste vahelises asjaajamises. Seetõttu on DHP digitaalallkirjaga seonduv problemaatika ka Riigikantselei esmaseks prioriteediks.

Teise olulise prioriteedi määrab Riigikantselei roll Vabariigi Valitsuse teenindamisel. Teine prioriteet on õigusaktide tervikliku infosüsteemi loomine, mille komponentideks on

- Eelnõude elektrooniline kooskõlastamine (projekt eÕigus)
- Valitsuse istungite teenindamine valitsuse istungite infosüsteemi arendamisega (projekt VIIS)
- Õigusaktide avalikustamine elektroonilise Riigi Teataja kaudu (projekt eRT)

Üldised lahendamist vajavad küsimused on:

1. Ühtsete digitaaldokumentide loomine (sh kooskõlastused, viseerimine, süstemati-seerimine, allkirjastamine),
2. Digitaalsete dokumentide süsteemi haaramine, registreerimine, töötlus
3. Digitaaldokumendi arhiveerimine ja digitaalallkirja sertifikaatide hoidmine ja arhiveerimine
4. Õigusjõuga dokumentide loomine
5. Tööprotsesside automatiseerimine

Riigikantselei haldusalas olev Riigiarhiiv on juba küllalt tõsist tööd teinud digitaalse arhiveerimise korraldamisel tekkivate probleemide selgitamisel ja kindlasti saavad ja peavad digitaalallkirja juurutamise projekti raames plaanitavad lahendused tekkima koostöös DHP ja Riigiarhiiviga.

Näiteid protsessidest:

5.3.1 eÕigus

Õigusaktide elektrooniline menetlemine (ministeeriumidevaheline ühisprojekt)

Ministeerium saadab teisele ministeeriumile digitaalselt allkirjastatud õigusakti eelnõu koos arvamusega

Teine ministeerium kontrollib digitaalallkirja, teeb parandused, allkirjastab need digitaalselt ja saadab kolmandale ministeeriumile.

Allkirja andja: ministeeriumi ametnik (Kantsleri või Ministri viseering?)

Huvitatud osapool: teine ministeerium

5.3.2 VIIS

Valitsuse istungite ettevalmistamine ja läbiviimine

- Ministeeriumid esitavad Riigikantseleile Vabariigi Valitsuse istungile panemiseks õigusaktide eelnõud koos vajaliku lisadokumentatsiooniga, sealhulgas kooskõlastuskirjadega, mille esitajateks võivad olla ministeeriumid, maavalitsused, kohalikud omavalitsused, ühendused, kojad ja muud organisatsioonid.
- Riigikantselei vaatab esitatud dokumendid läbi ja paneb istungi päevakorda. Ministrid annavad infosüsteemi kaudu päevakorda esitatud eelnõudele oma arvamuse.
- Valitsuse istungil vaadatakse eelnõud läbi ja tehakse nende kohta otsus, mis dokumenteeritakse.

Allkirja andjad: ministrid, kantslerid, eelnõu menetlejad Riigikantseleis

Huvitatud osapool: Riigikantselei

5.3.3 Elektrooniline Riigi Teataja (ERT)

- Andmeesitaja saadab ERT volitatud töötlejale avaldamisele kuuluva õigusakti, mis on digitaalselt allkirjastatud andmeesitaja poolt. Andmeesitajaks võib olla Riigikogu Kantselei, Vabariigi Presidendi Kantselei, Riigikantselei, ministeeriumid, Vabariigi Valimiskomisjon, Eesti Pank, Riigikohus, kohalikud omavalitsusüksused ja halduskohtud.
- Andmeandja kontrollib ERT-le esitatud tekste ja kui tekst on avaldamiseks küps, siis saadab ERT-le andmeandja poolt digitaalselt allkirjastatud avaldamisotsuse. Andmeandjaks võib olla Riigikantselei, ministeeriumid ja Eesti Pank.
- ERT kontrollib digitaalallkirju, säilitab need ja avaldab õigusaktid elektrooniliselt.

Allkirja andjad: Andmeesitajad ja andmeandjad

Huvitatud osapool: ERT volitatud töötleja

5.4 Teede- ja Sideministeerium

Teede- ja sideministeeriumi haldusalasse kuuluvad riigiametitest Sideamet, Maanteeamet, Lennuamet, Veeteede Amet ja Raudteeamet ning Autoregistrikeskus.

Autoregistrikeskuse õigusjõudu omavatest päringuvastustest on juba ammu huvitatud operatiivülesannetega riigiametid, eeskätt Politsei ja Piirivalve. Tegelikult peavad riiklikke registreid ka kõik teised Teede- ja Sideministeeriumi ametid, aga nende infovahetus ei ole sedavõrd intensiivne, et seal digitaalallkirja rakendamisega olulist tööprotsesside ökonoomiat saaks eeldada. Pigem on selle ministeeriumi prioriteediks seadustest tuleneva kohustusena:

1. Digitaalselt esitatud dokumentide vastuvõtuvõimaluse tagamine.

Autoregistri huvidest tulenevalt siis ilmselt veel ka:

2. Õigusjõuga päringuvastused
3. Digitaalne arhiveerimine

5.5 Siseministeerium

Siseministeerium on Eesti Vabariigi kõige olulisema põhiregistri - rahvastikuregistri - vastutav töötleja. Rahvastikuregistri puhul on prioriteetideks

1. Digitaalsete dokumentide vastuvõtmine
2. Õigusjõuga päringuvastused
3. Digitaalne arhiveerimine

Teiseks Siseministeeriumi suureks registripidajaks (kuni Rahvastikuregistri seadusjärgses mahus käivitumiseni) on Kodakondsus- ja Migratsiooniamet, kelle prioriteedid võiksid olla samad, mis Rahvastikuregistri puhul.

Siseministeeriumi haldusala teiste riigiametite - Politseiameti, Kaitsepolitseiameti, Piirivalveameti, Päästeameti ning Andmekaitse Inspektsiooni esimeseks prioriteediks on ilmselt digitaaldokumentide vastuvõtmise tagamine.

5.6 Majandusministeerium

Majandusministeeriumi prioriteetseim (suurima kasutajaskonnaga) infosüsteem saab lähiajal olema ehitisregistri infosüsteem, mis hakkab asendama varem eksisteerinud ehitusregistrit ning hooneregistrit. Vajalikuks peetakse ka kodanike digitaalset suhtlust omavalitsustega. Olulisemate vajadustena nähakse seega ette:

1. Digitaalsete dokumentide vastuvõtt ja edasine töötlus
2. Tööprotsesside digitaliseerimine
3. ID-kaardi põhine kodanike autentimine
4. Õigusjõuga päringuvastused

Näide protsessist:

5.6.1 Ehituslubade ja kasutuslubade esitamine Kohalikele Omavalitsustele ja nende hilisem menetlemine

- Füüsiline või juriidiline isik esitab kohalikule omavalitsusele (KOV) digitaalselt allkirjastatud taotluse ehitus- või kasutusloa saamiseks
- KOV esitab taotleja ja objekti andmed registrile
- Registri ametnik teeb otsuse ja allkirjastab selle
- KOV omavalitsus annab otsuse alusel vastava loa välja

Allkirja andja:	Füüsiline või juriidiline isik
Huvitatud osapool:	Kohalik omavalitsus

Allkirja andja: Registri ametnik

Huvitatud osapool: Kohalik omavalitsus

5.7 Lahendamist vajavad ülesanded

Digitaaldokumentide vastuvõtmine ja edasine digitaalne töötlus nõuab lahendusi järgmistele probleemidele:

1. Dokumendivormingud
2. Sertifitseerimine
3. Volitusinfo esitamine
4. Dokumentide transport

Digitaalne arhiveerimine nõuab lahenduste saamiseks kogu arhiveerimisprotsessi edasist täiendavat käsitlust, mis sisaldaks ka digitaalallkirjade ning arhiivist tehtavate päringute tõestusväärtuse säilimise tagamist jms. Lisanduvad lahendamist vajavad probleemid seega

5. Digitaalallkirjade pikaajalise tõestusväärtuse tagamine
6. (Arhiveerimisprotsess)

Automaatsed õigusjõuga registripäringud nõuavad eelkõige lahendusi juriidilisel tasandil - st. soovitavalt asutuse või registri digitaalallkirja mõiste sissetoomist haldustoimingutesse. Tehnoloogiliselt täiendavaid lahendamist vajavaid probleeme ei teki. Ka **tööprotsesside digitaliseerimine** ei too sisse täiendavaid kooskõlastatud lahendust vajavaid probleeme.

ID-kaardi põhine kasutajate autentimine kasutab ära juba ID-kaardi projektis loodavat Eesti Vabariigi residentidele tekkivad elektroonilist identiteeti tuvastada võimaldavat lahendust ning täiendavaid lahendamist vajavaid probleeme ei tekita. Samas kuna ID-kaardi projekt ei ole hetkel oma lahendustega veel lõplikus ja stabiliseerunud seisus, siis tuleb hoolega jälgida ning vajadusel toetada sertifitseerimispoliitika väljatöötajaid ka digitaalallkirja rakendamiseks sobiliku sertifitseerimisskeemi evitamisel.

6. Võimalikud lahendused

Käesolev peatükk vaatleb analüüsi käigus identifitseeritud ning digitaalallkirja rakendamise mõttes prioriteetseks peetavate probleemide võimalikke lahendusvariante.

6.1 Dokumendivormingute kooskõlastamine

Erinevate digitaaldokumendivormingute *de jure* standardimisega on rahvusvahelised organisatsioonid (ISO, W3C) tegelenud juba aastaid. Nende tegevuse tulemusena on valminud mitmed üldtunnustatud vormingud (ASCII, SGML, HTML). Standardimisega paralleelselt toimivad aga ka äriprotsessid ja nende käigus on erafirmade väljatöötluses loodud mitmeid alternatiivseid formaate, millest mõned on saanud *de facto* standarditeks.

Üheks tugevamaks firmaks selles vallas tuleb kindlasti pidada Microsofti, kes on suurepärase turustrateegia abil suutnud ka Eestis enamuse riigiameteid ja firmade kontoreid oma tarkvaraga täita. Põhiprobleemiks selle tarkvara juures osutub tema suletud iseloom: Office'i failiformaatide (DOC, XLS, PPT jne) kirjeldused ei ole avalikud. Teisalt on erinevad firmad ja organisatsioonid töötanud välja ka avaliku definitsiooniga vorminguid (XML, PostScript, PDF). Nii võimegi erinevad formaadistandardid jagada kahte suurde klassi: *avatud* ja *kinnised*.

Mõlemal klassil on potentsiaalsete standarditena omad eelised ja puudused, mida järgnevas lühidalt käsitlemegi.

6.1.1 Kinnised ja avatud standardid

Kinniste standardite eelisteks on nende kuuluvus (reeglina ühele) firmale, kes võib oma vorminguid käsitlevat tarkvara müüa ja garanteerida nii vastava tarkvara kommertstoe.

Kinniste standardite puudusteks on aga asjaolud, et

- sidudes kogu riigi asjaajamise mõne kinnise vormingu külge seame me end selle vormingu omanikust väga tugevasse (majanduslikku) sõltuvusse;
- kinnise standardi alusel koostatud arhiveeritud dokumendi loetavust pole võimalik garanteerida, sest ühest küljest lähevad firmad aegajalt pankrotti ja teisest küljest ei pruugi konkreetse kinnise formaadi igavene toetamine firma ärihuvidega kokku langeda;
- kui hakata kinnises vormingus dokumenti signeerima, puudub signeerijal tegelikult igasugune kontroll allkirjastatava sisu üle.

Avatud standardite eelised:

- lihtkodanikele ning asutustele on nende käitlemine reeglina tasuta;
- tänu formaadikirjelduse avalikkusele on tunduvalt kergem tagada arhiivi säilimist isegi kui dokumendi loomisel kasutatud originaaltarkvara on hävinud;
- signatuuri andjal on põhimõtteliselt võimalik kontrollida, et allkirjastatav dokument ei sisalda midagi üleliigset.

Samas tuleb avalike vormingute toetamisse kasutajatel rohkem investeerida.

Avatud ja suletud vormingute eeliseid ja puudusi arvestades tundub avalikus sektoris olevat mõistlikum lahendus võtta kasutusele avatud formaadil põhinev dokumendihalduse kord.

6.1.2 Üleminek XML-põhisele dokumendihaldusele

Juba üle aasta samade probleemidega tegelenud DHP programmi raames on kaalutud erinevaid võimalikke avatud dokumendiformaate ja otsustatud soovitada riigiasutustes kasutada W3C väljatöötlust XML. XMLi kasuks kõnelevad mitmed asjaolud:

- XML on struktureeritud vorming, mis toetab dokumentidele metaandmete lihtsat lisamist;
- XML on avalik ja standardne;
- XML-dokumendid sobivad veebis esitamiseks;
- on välja töötatud mitmed metoodikad XML-dokumentidele digitaalallkirjade lisamiseks.

Samas tuleb arvestada ka Eesti riigiasutustes kujunenud hetkeolukorraga, kus praktiliselt kõigis on kasutusel Microsoft Office tarkvara. Erinevatel põhjustel (eeskätt harjumusest ning soovimatusest töötavat süsteemi lõhkuda) ei soovita seda arvatavasti niipea välja vahetada. Nõnda seisab DHP programm valiku ees: kas aktsepteerida Microsofti *de facto* standardit ka *de jure* või töötada välja üleminekustrateegia üleminekuks XML-formaadile.

Kuna Microsofti formaadid on kinnised ja ülaltoodu põhjal seega avalikus sektoris kasutamiseks tegelikult ebasobivad, tuleks perspektiivis valida just üleminekustrateegia.

XML-standardile üleminekul tuleb läbida neli suurt etappi:

Raamistiku loomine uute dokumendiformaatide väljatöötamiseks, publitseerimiseks ja arhiveerimiseks. DHP programmil pole mõtet hakata ise tegelema kõigi ringlevate dokumentide tüüpide defineerimisega. Pigem tuleks luua kord, mille alusel asutused saaksid ise vajalikke vorminguid välja töötada ning neid teistele kasutamiseks levitada. DHP roll selles protsessis peaks olema vastava tegevuse koordineerimine ja asutuste nõustamine XML-dokumentide tüüpide määratlemisel.

Riigi dokumendihalduses kasutatavate dokumentide struktuuri kindlaksmääramine ja esitamine XML-keeles. XML kasutab struktuuri määramiseks dokumentide tüübidefinitsioone (DTD, *Document Type Definition*). Nende abil tuleb kirja panna kõigi kasutatavate dokumendiklasside (kiri, seaduseelnõu, ...) formaadid. Asutustevahelise kirja näidis-DTD on DHP raames juba valminud, lähiajal tuleb koostöös konkreetseid dokumenditüüpe vajavate asutustega lisada ka ülejäänud.

XML-formaadi integreerimine Microsoft Office keskkonda. Seda etappi saab lahendada mitmeti, näiteks luues Office'it programmeerimiskeskkonnana kasutades selle sees uue tekstitoimeti. Ükski seni väljapakutud lahendustest ei ole väga elegantne, kuid ajutiselt lahenduselt ei tule seda eeldadagi. On olemas variant, et Microsoft Office mõni tulevane versioon hakkab ka otse XMLi toetama, kuid esiteks ei saa sellele variandile loota ja teiseks ei ole selge, kas sel juhul saaks dokumente luua suvaliste DTDde alusel.

XML-formaati toetava tarkvara kasutuselevõtt. Käesoleva plaani kirjutamise ajaks on ilmunud esimesed XML-i toetavad WYSIWYM-redaktorid (nt XXE). Lähemas tulevikus võib ennustada paljude sarnaste (ka vabavaraliste) tarkvaratoodete ilmumist, seega ei ole Eesti riigil mõtet hakata ise tekstitöötluse alasesse tarkvaraarendusse investeerima. Põhiprobleemiks kujuneb ilmselt kasutajaharjumuste muutmine, sest XMLi kasutamine eeldab dokumentide struktuurset esitamist, mida praegused bürootarkvarapaketid ei toeta

6.2 Sertifitseerimine

6.2.1 Eraisikute sertifitseerimine

Eraisikutele digitaalallkirja andmiseks sobivate sertifikaatide jagamisega tegeleb ID-kaardi projekt. Hetkel on ette nähtud väljastada kõigil Eesti Vabariigi residentidele piiramatu vastutusega sertifikaadid. Kuna ID-kaart on kõigile kohustuslik, tuleks enne ID-kaardi juurutamise alustamist veelkord läbi vaadata sertifikaatide piiramatu vastutuse kontsepti vastuvõetavus (sellealaseid uuringuid ning arvamusküsitlusi ei ole seni tehtud ning isikutele ei ole isegi selgitatud ID-kaardi kasutamisest tulenevat vastutust). Kui ID-kaardi sertifitseerimispoliitikat ei muudeta, siis tuleb täiendavalt ette näha vastutust piiravate volitussertifikaatide väljaandmise võimalus.

6.2.2 Riigiasutuste töötajate sertifitseerimine

Kuna kõigil residentidel eeldatakse ID-kaardi olemasolu, siis maksimaalselt nähakse ette eraisikute sertifikaatide kasutamist tööülesannete täitmisel.

Vajadus riigiasutuste töötajatele spetsiaalsete sertifikaatide väljastamiseks tekib juhul, kui volitusinfo edastamiseks otsustatakse kasutada rollisertifikaate. Rollisertifikaatide kasutamist on eelmises peatükis kaunis täpselt kirjeldatud, seetõttu kordame siin üle vaid põhipunktid:

- tegu on tavaliste avaliku võtme sertifikaatidega, mis kannavad endas lisaks omaniku (füüsilise isiku) nimele ka asutuse nime ning töötaja õigused asutuses;
- sertifikaadi väljaandmine saab toimuda vaid töötaja ning asutuse juhi kahepoolsel nõusolekul. Sertifitseerimisteenuse osutaja peab arhiveerima mõlemad avaldused;
- sertifikaadi võib tühistada emb-kumb: kas töötaja või asutuse juht;
- sertifikaadi võib välja anda kasutaja ID-kaardil olevale privaatvõtmele. Sellisel juhul vastab kasutaja ID-kaardil olevale privaatvõtmele kaks sertifikaati: üks, mis on kantud kaardile ID-kaardi väljaandja poolt ning mida ta kasutab kodaniku rollis ning teine, mida hoitakse vaid asutuse infosüsteemis ning mida ta kasutab ametniku rollis.

Nagu eelmises peatükis nägime sobiks riigiasutuste töötajate sertifitseerijaks Riigi- ja kohalike omavalitsuse asutuste register, kes väidetavalt peab juba praegu arvet asutuste juhtide üle, kuigi põhimäärusest seda ei järeldu. Teine võimalik kandidaat oleks Riigiametnike register. Võiks kaaluda ka nende kahe liitmist. Vähemalt digitaalallkirja rakendamise aspektist oleks see otstarbekas. Sellist lahendust on üritatud realiseerida ka Riiklike institutsioonide infosüsteemi projekti raames [32]

Rollisertifikaatide jaoks tuleks defineerida profiil (mis võiks omakorda baseeruda ID-kaardi sertifikaadi profiilil). Profiil peaks defineerima kaks volituste defineerimise viisi, mis:

- võimaldaks kirjeldada nii masintöödeldavaid kui ka inimloetavaid volitusi;
- arvestaks maksimaalselt olemasoleva PKI tarkvara piiratud võimalustega.

6.2.3 Äriühingute töötajate sertifitseerimine

Äriühingute töötajate sertifitseerimine on digitaalallkirja juurutamise projektiga seotud seetõttu, et äriühingute töötajad peavad suhtlema riigiasutustega. Kindlasti eksisteerib neile sertifikaatidele terve rida kasutusviise ka äriühingutevahelises ja -siseses suhtluses, kuid seda praeguses aruandes ei käsitleta.

Riigiasutusi huvitab äriühingutega suhtlemise juures ennekõike see, et nende kõigiga oleks võimalik suhelda ühtemoodi. Teiselt poolt oleks väga kasulik, kui tehnilisest vaatepunktist

poleks vaja vahet teha ka äriühingute ning riigiasutuste vahelisel suhtlusel: s.t. et mõlemal juhul oleks võimalik kasutada samu meetodeid ja vahendeid.

Seega oleks mõistlik, kui:

1. kõik äriühingud kasutaks oma töötajate volituste esitamiseks sama meetodit;
2. see langeks kokku riigiasutuste töötajate volituste esitamise meetodiga.

Hetkel tegelevad riigiasutuste ja äriühingute üle arvepidamisega erinevad registrid. Kui neile mõlemale lisandub ülesanne pakkuda digitaalallkirja kasutamiseks vajalike teenuseid, kus-juures täpselt samade standardite ja profiilide alusel, siis tekitab see küllalt suure ja asjatu lisakulu. Digitaalallkirja rakendamise aspektist oleks mõistlik nii riigiasutuste kui äriühingute registrid liita üheks registriks (nagu kunagi Ettevõtteregister oli).

6.3 Volitusinfo esitamine

Järgnevalt vaatleme võimalusi volitusinfo esitamiseks. Volituste süsteem on kahetasemeline:

1. Äriregister ning Riigi- ja kohalike omavalitsuse asutuste register peavad arvet asutuste juhtide üle. Info füüsilise isiku õiguse kohta mingi juriidilise isiku nimel esineda tuleb neist kahest registrist. See info peab olema kättesaadav ka digitaalkujul alltoodud nõudmisi rahuldaval viisil.
2. Asutuse juht võib anda oma alluvatele õiguse allkirjastada asutuse nimel mingeid dokumente. See info peab olema kättesaadav digitaalkujul alltoodud nõudmisi rahuldaval viisil.

Nõudmised, mida me esitame mingi dokumendi allkirjastaja volitusinfole on järgmised:

1. volitusinfo peab olema esitatud tõestusväärtust väärtust omaval viisil. See võimaldab usaldatud osapoolel hilisema võimaliku kohtuvaidluse korral näidata, millisel isikul tekivad antud digitaalallkirjaga seoses õigused või kohustused;
2. volitusinfo tõestusväärtus peab säilima vähemalt sama kaua, kui kehtib antud digitaaldokument;
3. volitusinfo peab olema üheselt arusaadav nii huvitatud osapoolele kui ka kohtunikule. Selleks peavad volitusinfo interpreteerimisreeglid olema avalikud ja soovitavalt ajas vähe muutuvad;
4. volitusinfo peab kajastama antud dokumendi allkirjastamise ajal kehtinud volitusi (volitused on ajas muutuvad: volitusi võib tühistada, nad võivad mingi aja pärast ka uuesti tekkida, volitusi võib peatada, peatamist võib lõpetada, jne.).

Need nõudmised kehtivad mõlema taseme volitusinfo puhul.

6.3.1 Asutuste juhtide volitused

Vaatame kõigepealt võimalusi, kuidas täita neid nõudmisi Äriregistri ning Riigi- ja kohaliku omavalitsuse asutuste registri poolt väljastatava info korral. Lahendamist vajavaid küsimusi on kolm:

1. kuidas esitada volitusinfot (volitusinfo vorming)?
2. kuidas tagada volitusinfo ajakohasus?
3. kuidas tagada volitusinfo tõestusväärtus?

6.3.1.1 Volitusinfo vorming

Äriregistri ning Riigi- ja kohalike omavalitsuste asutuste registri poolt väljastatav volitusinfo loob seose antud asutuse (äriühingu, riigiasutuse) ja konkreetse füüsilise isiku vahel. Põhiküsimus vastava seose loomisel on seotud osapoolte nimetamisega. Kuna mõlemad registrid on volitatud haldama vastavat liiki asutuste nimeruumi ja tagama, et kõigil asutustel oleks unikaalsed nimed ning registrikoodid, siis ei teki asutuse nimetamisel probleemi. Füüsilise isiku üheseks identifitseerimiseks, juhul kui ta on kas Eesti Vabariigi kodanik või omab Eestis alalist elamisluba, on piisav kasutada isikukoodi, mida võib mugavuse ja kindluse huvides täiendada isiku ees- ja perekonnanimega.

Oluline on tähele panna, et seda volitusinfot soovitakse kasutada koos füüsilise isiku poolt antud digitaalallkirjadega. Enamasti on digitaalallkirja andval isikul olemas ka mingi sertifitseerimisteenuse osutaja poolt välja antud sertifikaat, mis seob isiku avaliku võtme tema nimega. Reeglid isiku nime esitamiseks sertifikaadis on paika pandud sertifitseerimisteenuse osutaja sertifitseerimispõhimõtetega. Selleks, et hõlbustada volitusinfot töötlevate rakenduste tööd, võiks volitusinfosse kantava füüsilise isiku nimi olla samasugune (sama struktuuriga, sisaldada samu andmeid, samas kodeeringus) kui isiku digitaalallkirja sertifikaadis olev nimi.

Lahendamata jääb veel probleem, kuidas identifitseerida üheselt isikut, kellel ei ole Eesti Vabariigi isikukoodi, kuid ta peaks olema kantud Äriregistrisse kui mingi firma juhatuse liige. Kuna volitusinfot on vaja mingi füüsilise isiku digitaalallkirja sidumiseks mingi juriidilise isikuga, siis muutub see probleem aktuaalseks juhul, kui antud füüsiline isik suudab anda Eestis kehtivat digitaalallkirja. Selleks peab tal üldjuhul olema mingi sertifikaat, mis on välja antud mingi sertifitseerimisteenuse osutaja poolt.

Juhul, kui tegu on Eesti Vabariigis Sertifitseerimise Riiklikus Registris registreeritud teenuseosutajaga, siis on see teenuseosutaja antud kodaniku nimetamise mingil aktsepteeritaval viisil juba lahendanud ja piisab, kui kasutada tema nime sellisel kujul, nagu see on sertifikaadis.

Juhul, kui tegu on mõnes välisriigis asuva sertifitseerimisteenuse osutaja poolt välja antud sertifikaadiga, siis see on juba probleem, mis vajab üldist lahendust ja väljub antud küsimuse käsitlusalast.

6.3.1.2 Volitusinfo värskuse tagamine

Volitusinfo ajakohasusel on kaks aspekti: ühelt poolt, kui kiiresti jõuavad muudatused registrisse ning teiselt poolt: kui kiiresti jõuavad muudatused registrist huvitatud osapoolteni. Registritesse muudatuste tegemise kord on reguleeritud seadusega ning vastavate protsesside kiirendamine ei ole otseselt antud projekti eesmärgiks, kuigi ka seda tuleks teha. Kindlasti aga vajab käsitlemist info jõudmine registrist huvitatud osapooleni.

Garanteeritult värske volitusinfo saamiseks peab huvitatud osapool esitama päringu vastavat volitusinfot sisaldavale registrile ning ootama ära selle vastuse. Selle lahenduse puuduseks on asjaolu, et juhul, kui vastav register pole mingil põhjusel kättesaadav, ei saa huvitatud osapool üldse mingit infot. Päringute arvu kasvades võib tekkida ka probleeme vastava serveri tootlikkuse ning sideliinide läbilaskevõimega.

Päringuvastusest peab selguma ka vastuse loomise aeg. See on oluline, sest nagu mainitud võivad õigused tekkida ja taas kaduda.

6.3.1.3 Volitusinfo tõestusväärtuse tagamine

Et anda volitusinfo andmebaasi päringuvastustele tõestusväärtust, peavad päringuvastused olema varustatud digitaalallkirjaga. See võimaldab huvitatud osapoolel hiljem tõestada antud füüsilise isiku õigust anda antud juriidilise isiku nimel allkirju, seda isegi juhul, kui vastavat

volitusinfot sisaldanud registri terviklus saab rikutud. Selline lähenemine, mille korral digitaaldokumendi mitmesugused tõestusväärtust tekitavad atribuudid arhiveeritakse koos dokumendiga ning vabanetakse niiviisi kolmandate osapoolte usaldamise vajadusest, aitab pikas perspektiivis vähendada digitaaldokumentide kasutamisega tekkivaid väliseid ja raskelt juhitavaid riske.

6.3.2 Asutuse töötajate volitused

Nagu sissejuhatavas käsitluses selgus võib asutuse juhi poolt töötajatele antavad täiendavad õigused jagada kahte kategooriasse:

1. dokumentide masintöötluseks mõeldud volitused;
2. inimeste poolt tõlgendamiseks mõeldud volitused.

Esimest tüüpi volitustes loetakse üles dokumenditüübid, mida antud ametnikul on õigus allkirjastada. Teist tüüpi volitustes kirjeldatakse ametniku õigusi inimkeeles.

Esimest tüüpi volituste kasutamine eeldab, et asutus on defineerinud kasutatavad dokumendivormingud ja nende tähendused ning omistanud neile identifikaatorid. Sedasorti dokumente töötlev tarkvara saab siis automaatselt kontrollida, kas mingi dokumendi allkirjastanud ametnikul oli selleks tegelikult õigus.

Teist tüüpi volituste kasutamine eeldab, et volitusi kontrollib inimene, kes loeb läbi dokumendi ning allkirjastaja volitused ja leiab, kas antud dokument mahub antud volituste raamidesse.

Asutuse töötajate volituste kättesaadavaks tegemiseks on kaks võimalust:

1. Vastav info on kättesaadav keskregistritest. Ehk siis Äriregistri ning Riigi- ja kohalike omavalitsuse asutuste registri infosüsteem oskaks vastata ka ametnike volituste kohta käivatele päringutele.
2. Asutus ise haldab vastavat andmebaasi.

Mõlemal variandil on oma head ja vead:

- Esimene variant on pisematele asutustele palju lihtsam kasutada: pole vaja serverit paigaldada ja turvata.
- Esimese variandi korral ei ole volituste kohta infot jagava süsteem nende isikute kontrolli all, kelle volituste kohta infot jagatakse. See võib aidata ära hoida teatud pettusekatseid.
- Teise variandi korral on andmebaasi värskena hoidmine lihtsam. Esimese variandi korral tuleks defineerida protokoll, mille abil asutuse juht saaks piisavalt lihtsalt andmeid keskregistris muuta.

6.3.3 Lahendused volitusinfo esitamiseks

6.3.3.1 Suhtlus läbi asutuse serveri

Asutuses on server, läbi mille toimub dokumentide saatmine asutusest välja. Server autendib ametnikke (vajadusel digitaalallkirja abil), lisab välja saadetud dokumentidele ametniku nime, ja kui ametnikul on volitus dokumendile alla kirjutada, allkirjastab digitaalselt dokumendi koos nimega ja ametikoha määratlusega. Näiteks:

(*) Dokument *X*, allkirjastatud Maksuameti inspektori Jaan Kase poolt.

Serveri poolt antud allkirjade eest võib vastutada kindel töötaja või asutuse juht. Rõhutame, et dokumendile (*) antud serveripoolne digitaalallkiri tähendab lihtsalt seda, et asutuse juht (või mõni muu vastutav töötaja) võtab endale vastutuse järgmiste väidete eest:

(1) On kontrollitud, et dokument pärines Jaan Kaselt;

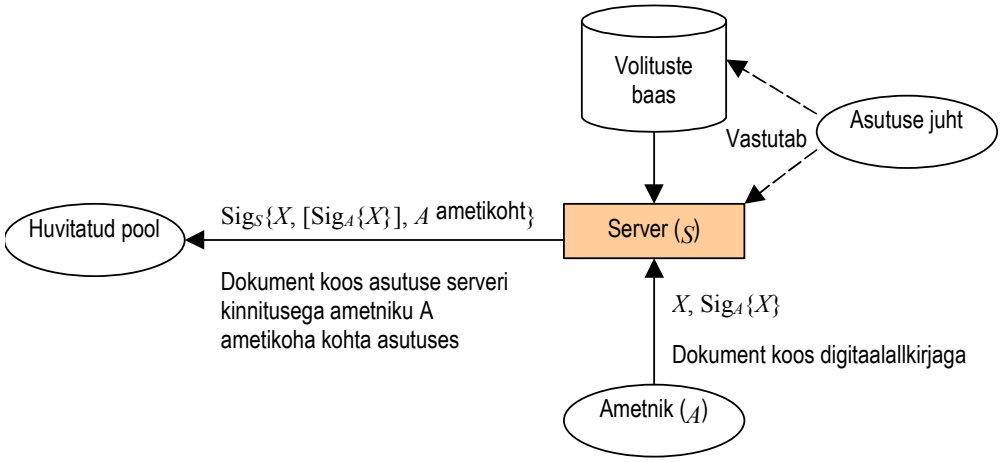
(2) Jaan Kask on Maksuameti inspektor ja tal on õigus dokumenti *X* allkirjastada.

Seega, allkiri dokumendil (*) ei tähenda sedasama, mis dokumendile *X* antud digitaalallkiri. Kui server kasutas Jaan Kase autentimiseks tema digitaalallkirja Sig{*X*} dokumendil *X*, siis on serveri poolt allkirjastatud sõnumite eest vastutajal alati võimalik tõestada, kellelt tegelikult pärines dokument *X*.

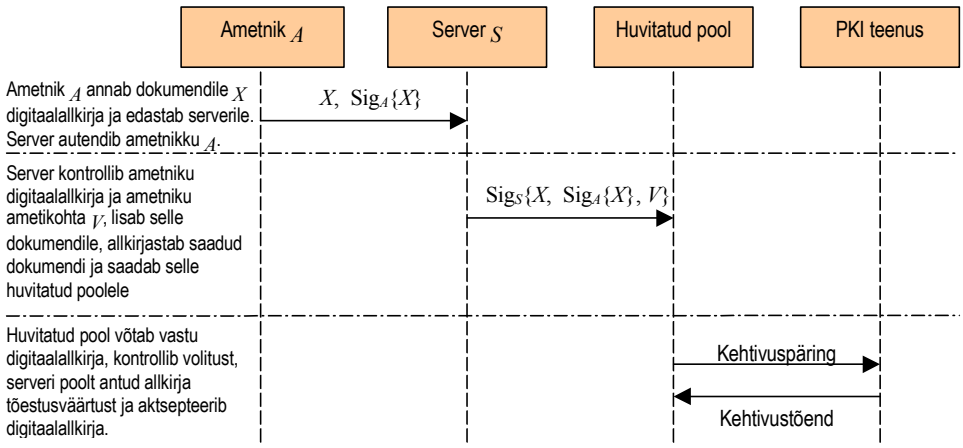
Kui mingil põhjusel on vaja dokumendi saanud isikul endal Jaan Kase digitaalallkirja kontrollida, siis võib serveri poolt allkirjastatav sõnum olla järgmine:

(**) Dokument (*X*, Sig{*X*}) allkirjastatud Maksuameti inspektori Jaan Kase poolt.

Sellest sõnumist on välja loetav ja vajadusel kontrollitav nii allkirja andnud isik kui ka isiku õigus allkirja anda. Asutusest väljuv dokument muutub seega "ametlikuks", kui ta läbib asutuse serveri. Lahenduse eelis on tema lihtsus.



Joonis 6. Lahendus asutuse serveri poolt antava digitaalallkirja abil.



Joonis 7. Tegevuste järgnevus suhtluse korral läbi asutuse serveri.

Huvitatud osapoolel on otseselt vaja tõestada ainult serveri *S* poolt antud digitaalallkirja kehtivust, sest ametniku *A* poolt antud allkirja tõestuskohustus langeb siis asutuse juhile.

Kirjeldatud skeemis on oluline, et server kontrolliks sõnumi värskust. Vastasel korral võib juhtuda, et keegi teine saadab serverile vana sõnumi, mis oli allkirjastatud ametniku *A* poolt sel ajal kui tal *veel ei olnud* volitust *V*. Üks viis värskuse kontrolliks on ametniku autentimine ametniku ja serveri vahelise suhtluse käigus. Ametnik võib ka lisada signatuuri alla signeerimise aja. Sellisel juhul peaks server kontrollima, et sõnum oleks moodustatud peale ametniku volituste kehtima hakkamist.

Sarnast süsteemi kasutatakse X-tee juures, kus ametnike volituste kontroll on asutuse infosüsteemi ülesandeks. Asutustevahelises suhtluses aga kontrollitakse ainult asutuse kui terviku volitusi.

6.3.3.2 Volituste register

Asutuses olev register seab küllalt suuri nõudmisi asutuse infosüsteemile. Soovides vabaneda asutuses olevast serverist, jõuame *volituste registri* kontseptsioonini. Volituste register on avalik andmebaas (realiseeritud serverina *S*), mille kaudu huvitatud osapoolel on võimalik operatiivselt saada usaldatavat ja tõestusväärtusega informatsiooni isikute õiguste kohta sooritada mingeid toiminguid. Registrit võib näiteks vaadelda Äriregistri (või Riigi- ja kohalike omavalitsuste asutuste registri) osana.

Andmebaas on kättesaadav serverile *S* päringut tehes. Päringu vastus (volituskinnitus) on lause:

(***) Päringu kättesaamise hetkel on Jaan Kask Maksuameti inspektor,

mis on digitaalselt allkirjastatud serveri *S* poolt. Selleks, et päringuvastusest oleks kasu Jaan Kase poolt antud digitaalallkirja[4] $s = \mathrm{Sig}_A\{X\}$ tõestusväärtuse kontekstis, tuleb päringuvastus vääramatult siduda digitaalallkirja *s* andmise hetkega. Vastasel korral ei oleks päringuvastusest hiljem kasu –

(a) see võidi küsida varem ja digitaalallkiri *s* ise olla moodustatud hiljem, siis kui volitus *enam ei kehtinud*.

(b) see võidi küsida hiljem ja digitaalallkiri *s* ise võis olla moodustatud varem, siis kui volitus *veel ei kehtinud*. (vt. peatatuse probleemi käsitlus)

Tehniliselt näeb registri lahendus välja järgmiselt:

- **Andmehõive**. Asutuse juht saadab registrile (digitaalselt) allkirjastatud avalduse, st dokumendi, milles on märgitud töötaja isikuandmed *A* ja ametikoht *V*. Register säilitab avalduse ja kannab avalduses olnud andmed Volituste baasi, mida kasutab server *S*, mille abil pääsevad kasutajad ligi baasis olevale informatsioonile.
- **Digitaalallkirja andmine asutuse nimel**. Ametnik *A* allkirjastab dokumendi *X*, lisades metaandmetena kuupäeva *t*, oma nime *A* ja ametikoha *V*. Allkiri $s=\mathrm{Sig}_A\{X,t,A,V\}$ saadetakse huvitatud poolele.

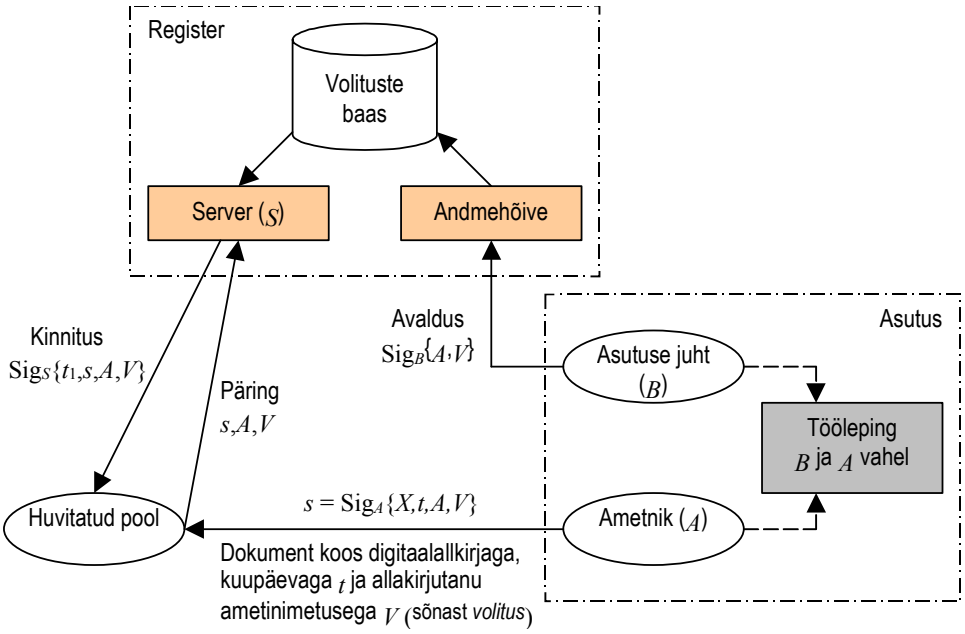
[4] Siin tähistab Sig_A Jaan Kase poolt antud digitaalallkirja.

- **Volituse kontroll**. Huvitatud pool saadab serverile S päringu, milles sisaldub digitaalallkiri s, nimi A ja ametikoht V. Server saadab vastu kinnituse, milles sisaldub: aeg t_1, millest alates ametikoht on pidevalt kehtinud ja kolmik (s,A,V). Kinnitus on digitaalselt allkirjastatud serveri S poolt. Kinnitus $\text{Sig}_S\{t_1,s,A,V\}$ tähendab sisuliselt serveri S poolt välja öeldud lauset:

  "Alates hetkest t_1 kuni allkirja s sisaldanud päringu kättesaamise hetkeni on isik A pidevalt olnud ametikohal V"

  Huvitatud osapool kontrollib, kas $t_1<t$.

- **Sertifikaatide kehtivuse kontroll**. Huvitatud osapool hangib PKI-teenuse osutajalt kehtivustõendid digitaalallkirjadele $\text{Sig}_A\{X,t,A,V\}$ ja $\text{Sig}_S\{t_1,s,A,V\}$.



Joonis 8. Lahendus volituste registriga.

Antud protokollis taandatakse volituse kontroll seega kahe digitaalallkirja kehtivuse kontrollile, st on vaja hankida kaks kehtivustõendit. Järgnevas osas vaatleme võimalust, kuidas ülesannet taandada üheainsa digitaalallkirja tavalisele kontrollile.

6.3.3.3 Volitused koos avalike võtmetega

Tehniliselt näeb see lahendus välja järgmiselt:

- **Andmehõive**. Asutuse juht saadab registrile (digitaalselt) allkirjastatud avalduse, st dokumendi, milles on märgitud töötaja isikuandmed A, tema avalik võti PK_A ja ametikoht V. Register säilitab avalduse ja kannab avalduses olnud andmed Volituste baasi, mida kasutab server S, mille abil pääsevad kasutajad ligi baasis olevale informatsioonile. Vajadusel kontrollib andmeid (näiteks STO-delt).

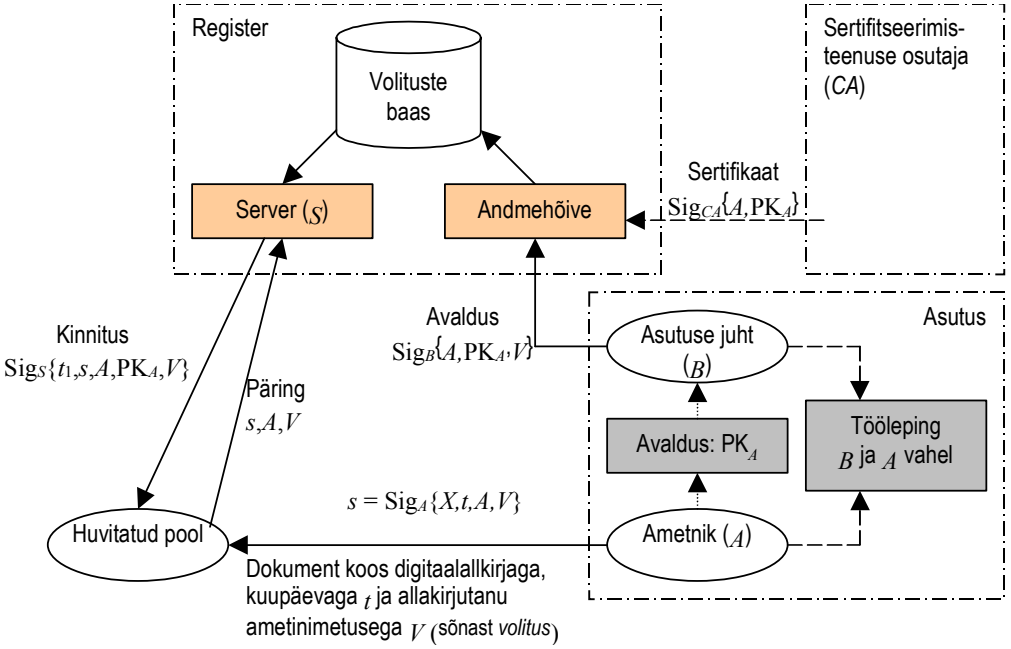
- **Digitaalallkirja andmine asutuse nimel**. Ametnik A allkirjastab dokumendi X, lisades metaandmetena kuupäeva t, oma nime A ja ametikoha V. Allkiri $s=\text{Sig}_A\{X,t,A,V\}$ saadetakse huvitatud poolele.

- **Volituse kontroll**. Huvitatud pool saadab serverile S päringu, milles sisaldub digitaalallkiri s, nimi A ja ametikoht V. Server saadab vastu kinnituse, milles sisaldub: aeg t_1, millest alates ametikoht on pidevalt kehtinud ja nelik (s,A,PK_A,V). Kinnitus on digitaalselt allkirjastatud serveri S poolt. Kinnitus $\mathrm{Sig}_S\{t_1,s,A,\mathrm{PK}_A,V\}$ tähendab sisuliselt serveri S poolt välja öeldud lauset:

  > "Alates hetkest t_1 kuni allkirja s sisaldanud päringu kättesaamise hetkeni on isik A kes kasutab avalikku võtit PK_A pidevalt olnud ametikohal V"

  Huvitatud osapool kontrollib, kas $t_1<t$.

- **Sertifikaatide kehtivuse kontroll**. Huvitatud osapool hangib PKI-teenuse osutajalt kehtivustõendi digitaalallkirjale $\mathrm{Sig}_S\{t_1,s,A,\mathrm{PK}_A,V\}$.



Joonis 9. Volitused koos avalike võtmetega.

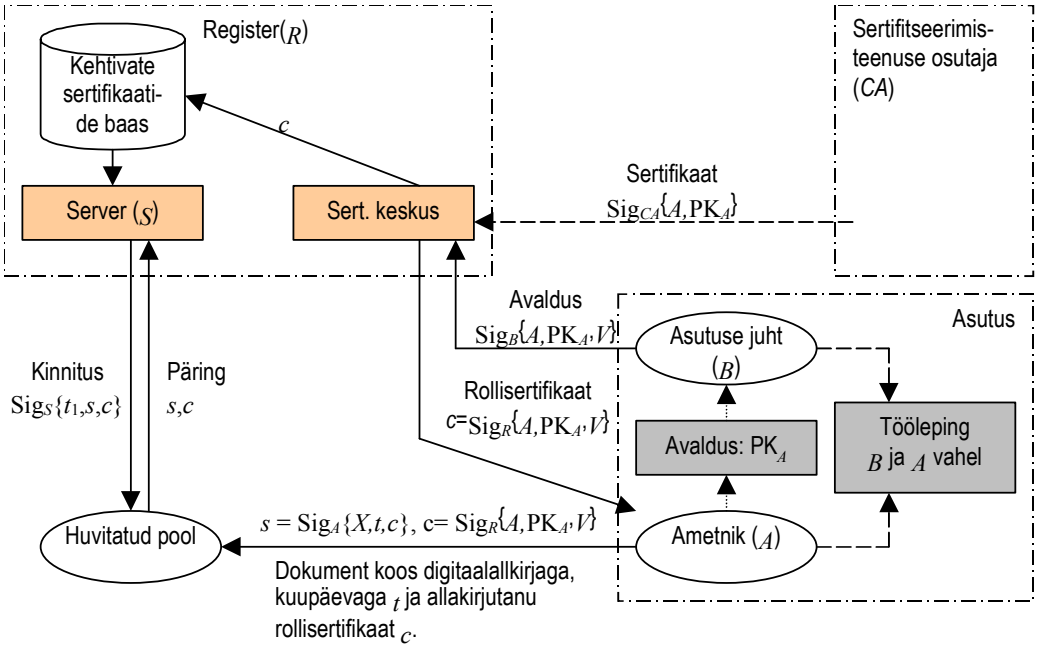
Lahenduse peamine eelis on see, et allkirja õigsuse kontrollimiseks ja tõestusväärtuse säilitamiseks on vaja ainult ühte kehtivustõendit.

6.3.3.4 Rollisertifikaadid

Eelmises osas kirjeldatud tehnilises mõttes väga efektiivsel skeemil on see väike puudus, et ta ei ole päris üks-üheselt realiseeritav tavaliste PKI vahenditega. Näiteks volituse kehtivus-kinnitus ei ole tavaline sertifikaadi kehtivuskinnitus (*a la* OCSP), vaid spetsiifiline dokument. Skeemi realiseerimisel võib olla kasulik tähele panna, et register esitab tegelikult kolmiksuhet (isik, võti, volitus). Registrit (R) võib tehnilises mõttes vaadeldagi sertifitseerimisteenuse osutajana, kes asutuse juhi avalduse (mis võib olla allkirjastatud näiteks ID-kaardi abil) põhjal annab välja sertifikaadi:

$$c = \mathrm{Sig}_R\{A,\mathrm{PK}_A,V\},$$

mida nimetame *rollisertifikaadiks* ja mille esitamiseks saab kasutada tavalist X.509v3 sertifikaati. Suhtluse skeem on muus osas kattuv eelmise punkti lahendusega.



Joonis 10. Volituste lahendus rollisertifikaatidega.

Tuleb tähele panna asjaolu, et ehkki rollisertifikaatidega lahenduses taandub allkirja kontrollimise probleem jällegi kahe digitaalallkirja kontrollile, milleks on

- Rollisertifikaat c= $\mathrm{Sig}_R\{A,\mathrm{PK}_A,V\}$; ja
- Rollisertifikaadi kehtivuskinnitus $\mathrm{Sig}_S\{t_1,s,c\}$,

on nende haldust võimalik realiseerida (suures osas) juba valmis PKI tarkvara abil.

Ära on võimalik kasutada ka ID-kaarte. Rollisertifikaat võib olla antud ametniku ID-kaardil olevale salajasele võtmele. Sellisel juhul vastab ühele privaatvõtmele mitu sertifikaati: kõik erinevate õiguste või erinevate rollide jaoks. Dokumendi üheselt mõistetavuse huvides peab allkirjastatud dokumendis sisalduma ka sertifikaat, mille alusel soovitakse seda dokumenti allkirjastada. Vastavalt allkirjastatavale dokumendile tuleb valida õigete volitustega sertifikaat. Automaatset töötlemist võimaldavate volituste korral, kus sertifikaadis on üles loetletud kõik dokumenditüübid, mida antud sertifikaadiga võib allkirjastada, saab asutuse infosüsteem dokumenti allkirjastamiseks ette valmistades valida automaatselt õige sertifikaadi vastavalt allkirjastatava dokumendi tüübile.

6.3.3.5 Suhete peatamise probleem ja selle üldine lahendus

Nii volituste kui ka tavaliste sertifikaatide vms suhte kehtivuse piirkond ei tarvitse olla pidev, st moodustada mingit sidusat ajalõiku – suhe võib mingil hetkel lakata kehtimast (näiteks sertifikaadi peatamine) ja mõne aja möödudes taas kehtima hakata (näiteks sertifikaadi peatatuse lõpetamine).

Server, mis väljastab kinnitusi suhte kehtivuse kohta, ei saa lihtsalt väljastada lauseid tüüpi: "Ajahetkel t suhe R kehtis", sest see lause ei ütle midagi suhte kehtivuse kohta mingitel muudel ajahetkedel. Näiteks kui meil on kinnitatud laused:

- "Ajahetkel t_1 suhe R kehtis"
- "Ajahetkel t_2 suhe R kehtis"
- "Digitaalallkiri s moodustati ajahetkel t", kus $t_1 < t < t_2$,

siis sellest veel *ei järeldu*, et digitaalallkirja s andmise hetkel suhe R kehtis. Selleks, et muuta teenus kasutuskõlbulikuks, peaksid väljastatavad laused olema kujul:

- "Ajavahemikus t_1 … t_2 kehtis suhe R pidevalt"

Kui nüüd veel õnnestuks saada tõestus lausele "Digitaalallkiri s moodustati ajahetkel t" ja kui $t_1 < t < t_2$, siis tõepoolest võime järeldada, et digitaalallkirja s andmise hetkel seos R kehtis.

Märkus. Tegelikkuses aga ei ole võimalik tõestada digitaalallkirja andmise täpset hetke, vaid ainult vahemikku, millal allkiri anti. Selleks on kaks võtet, mida tuleb rakendada:

(a) allkirja andja A lisab allkirjastatavale dokumendile allkirja andmise aja t ja saadab digitaalallkirja $s = \mathrm{Sig}_A\{X,t\}$ ajatempliteenuse osutajale TSA.

(b) ajatempliteenuse osutaja annab välja ajatempli[5] $T = \mathrm{Sig}_{\mathrm{TSA}}\{s,t'\}$ ajahetkele $t'>t$; see tempel tõestab, et allkiri oli tõepoolest olemas juba enne ajahetke t'.

Ajatempli T olemasolu korral võib eeldada, et A allkirjastas dokumendi ajavahemikus $[t \ldots t']$. Selleks et tõestada, et suhe R kehtis allkirja s moodustamise hetkel, on vaja:

(a) Suhte kehtivuskinnitust: "Ajavahemikus t_1 … t_2 kehtis suhe R pidevalt"

(b) Ajatemplit: "Ajahetkel t' saadeti mulle s"

(c) Kontrollida, et $s = \mathrm{Sig}_A\{X,t\}$ ja et $t_1 < t < t' < t_2$.

Skeemi saab lihtsustada, kui lülitada päringusse ja kehtivuskinnitusse allkiri s:

- A moodustab allkirja $s = \mathrm{Sig}_A\{X,t\}$, kus t on hetkeaeg A kella järgi.
- Huvitatud pool saatis allkirja s päringuna serverile S ja saab vastuse kujul:

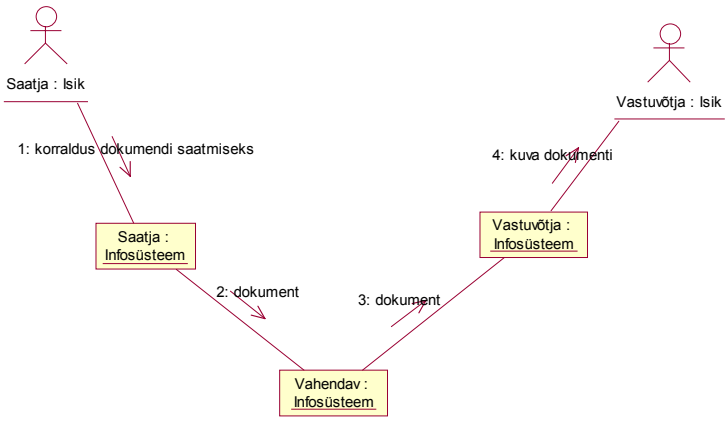
"Alates ajahetkest t_1 kuni päringu s kättesaamise hetkeni kehtis seos R pidevalt"

Selleks, et tõestada seose R kehtivust allkirja s andmise hetkel, on vaja nüüd ainult veenduda, et $t_1<t$, st eraldi ajatemplit ei lähe nüüd enam vaja.

6.4 Digitaaldokumentide transport

Käesolev peatükk vaatleb võimalusi digitaaldokumentide edastamiseks isikute vahel. On käsitletud dokumentide edastamist üle avaliku võrgu. Mingil erijuhul võib osutuda otstarbekaks digitaaldokumentide edastamine andmekandjate füüsilise transpordi teel, kuid neid väga spetsiifilisi juhte me siinkohal ei vaatle. Ka ei ole käsitletud asutusesisest andmevahetust, kuna see on väga tihedalt seotud infosüsteemi ülesehituse ja valitud vahenditega.

[5] Ajatempel tähendab TSA poolset lauset: "Ajahetkel t' saadeti mulle andmed s".



Joonis 11. Digitaaldokumendi teekond.

Joonisel 6 on esitatud olulised sammud digitaaldokumendi teel ühelt isikult teisele. Iga Infosüsteem koosneb vähemalt ühest arvutist. Sõnumite suunad antud joonisel kujutavad vaid lõpptulemuse jaoks oluliste andmete liikumist ega määra lokaalse suhtluse suunda, mis võib eri lahenduste korral olla erinev.

Igal infosüsteemil on oma funktsioon:

- Saatja infosüsteem valmistab dokumendi saatmiseks ette (muuhulgas allkirjastab dokumendi). Teatud juhtudel võib saatja infosüsteem krüpteerida dokumendi, et tagada tema salastatust teekonnal läbi vahendava infosüsteemi.
- Vastuvõtja infosüsteem võtab dokumendi vahendavalt infosüsteemilt vastu, vajadusele dešifreerib selle, kontrollib allkirja ning kuvab kasutajale.
- Vahendav infosüsteem organiseerib dokumendi jõudmise saatjalt vastuvõtjale.

Lahendused, mida saame kasutada ühe või teise sammu realiseerimiseks sõltuvad oluliselt vastavas sammus tegevuses oleva isiku võimalustest ja soovidest.

Vaatame millised võimalused dokumentide saatmiseks erinevatele isikutele eksisteerivad. Vaatleme, milliste omadustega need lahendused on. Uurime, kas ja kuidas oleks võimalik rahuldada kaht olemasolevates protsessides tihti esinevat nõuet:

1. tagada dokumendi salastatus;
2. tagada dokumendi kättesaamise fakti salgamise vääramine.

6.4.1 Dokumendi saatmine eraisikule

Üldjuhul tuleb eraisikule digitaaldokumendi saatmiseks sooritada järgmised tegevused:

1. tuvastada, kas antud isik on üldse võimeline digitaaldokumente vastu võtma;
2. tuvastada, millist sideviisi peab temaga suhtlemiseks kasutama;
3. tuvastada sideviisi spetsiifilised parameetrid (näiteks kasutaja meiliaadress);
4. saata dokument teele.

Universaalset, igal juhul sobivat ja garanteeritult toimivat lahendust neile probleemidele ei ole kahjuks olemas.

Võimalikud on osalised lahendused, mis sobivad mõnede kodanike või mõnede protsesside puhul:

- avalik kataloogiteenus, kus kodanikud saavad registreerida oma kehtiva sidepidamisviisi ja aadressi;
- "ametlik" meiliaadress (midagi stiilis eesnimi.perenimi.isikukood@eesti.ee) või kasutajakonto portaalis;
- kodanik on ise protsessi eelmistel sammudel andnud oma kehtiva meiliaadressi.

Mingid omaalgatuse korras tekkinud kataloogid on olemas, kuid nende sisu kvaliteet on üsna madal: registreerunud on suvalised isikud, suvalisel ajal ja enamasti pole andmeid kunagi uuendatud. Keegi pole ka kontrollinud, et isikud on registreerunud oma õige nime all. Seega võib öelda, et kasutatavat kataloogiteenust hetkel ei eksisteeri. Sellise teenuse loomine on sammuti kaheldava väärtusega ettevõtmine: kuidas sundida kodanikke end registreerima? Kuidas tagada, et nad andmeid uuendavad?

Ametlik meiliaadress või konto ametlikus portaalis nõuaks mingi infrastruktuuri (võimsad meili- ja veebiserverid) loomist. Võrreldes kataloogiteenusega lisanduvad veel probleemid nagu kasutajakontode haldus jms. Ja põhiprobleemiks jääb ikkagi see, et me ei saa kindlad olla, et vastav isik oma meili sellest ametlikust serverist iial loeb või sellesse portaali logib. Seda tõenäosust saab küll suurendada, pakkudes selle portaali või meiliserveri kaudu mingeid muid kasulikke teenuseid, kuid see kõik muudab süsteemi veelgi kallimaks ja garanteeritud tulemustest oleme ikka sama kaugel.

Eraisik on ise andnud oma kehtivad digitaalsed kontaktandmed. Nende protsesside puhul mida algatab eraisik võib kohe esimesel sammul küsida talt tema meiliaadressi ning kasutada seda hilisema suhtluse jaoks antud protsessi vältel. See on töötav ja praktiline lahendus, mis ei nõua mingi täiendava infrastruktuuri loomist. Piiranguks on see, et juhul kui suhtluse algatajaks protsessis on ametiasutus, siis see skeem ei tööta.

Juhul kui tegu on positiivse sisuga dokumendiga, siis võib ametiasutus küll üritada saata dokumenti isiku viimasele teadaolevale aadressile, kuid igal juhul tuleb valmis olla selleks, et see ei jõua kohale.

Juhul kui tegu oli negatiivse sisuga dokumendiga (kohtukutse, kutse kordusõppustele), siis pole tõenäoliselt mõtet seda välja saatma hakatagi, sest isegi kui dokument kohale jõuab, ei ole selle saajal mingit huvi seda tunnistada. Sellega jõuame kättesaamise salgamise vääramise võimalikkuse juurde suhtluses eraisikutega.

Mõnedes meilisüsteemides on seda nõuet täita püütud, kuid praktikas ei ole olemas töökindlat ja veel vähem mingit tõestusväärtust tekitavat viisi dokumendi kättesaamise fakti salgamise vääramiseks. Isegi kui me rakendame serverite tasemel mitmesuguseid turvameetmeid ja võtame kasutaja käest iga dokumendi kohta digitaalallkirja, et ta on selle kätte saanud, jääb kasutajale alati üle võimalus väita, et tema arvuti "jooksis kinni" või "ei suutnud seda dokumenti kuvada", vms. Seega ei tohiks ühtki digitaaldokumente kasutavat süsteemi üles ehitada eeldusel, et sõnumi saatjal on võimalik tõestada selle kättesaamist.

Sõnumi toimetamisel eraisikuni on kaks arvestatavat lahendust:

1. e-meili vahendusel;
2. veebiportaali vahendusel.

Tuleb tunnistada, et S/MIME standardi olemasolu ning küllalt hea toetatuse tõttu, on e-meili vahendusel toimuval suhtlemisel suured eelised veebiportaali kaudu toimuva dokumendivahe-

tuse ees. Ka on elektronposti kasutamine mugavam dokumendi saatjale: kõigile meiliaadressidele saab dokumente saata ühtmoodi. Mingi dokumendi saatmine läbi portaali on aga väga portaalispetsiifiline tegevus, mida on ebamugav automatiseerida (pealegi võib portaali tarkvara uus versioon ka dokumendi laadimist teisiti korraldada).

6.4.2 Dokumendi saatmine äriühingule

Tundub, et äriühingule digitaaldokumendi saatmine on lihtsam kui eraisikule dokumendi saatmine. Erinevalt eraisikutest, kelle puhul isegi sissekirjutus on mittekohustuslik, peavad äriühingud Äriregistris registreerima oma andmed, k.a. kontaktandmed. Ka ametlike, asutusele suunatud digitaaldokumentide saatmise viis ning konkreetsed aadressid võiksid seal kirjas olla. Juhul, kui asutus on need andmed avaldanud, peaks tal olema ka kohustus vastavat infosüsteemi töökorras hoida.

Sõnumite toimetamisel äriühinguni on kolm arvestatavat viisi:

1. e-meili vahendusel;
2. asutuse kodulehe vahendusel;
3. X-tee vahendusel.

Evitamise ja kasutamise lihtsuse ning standardsuse koha pealt on parim e-meil. Asutuse koduleheküljel olev dokumendi laadimise vorm oma kõiki neid samu puudusi, mis portaal eraisiku puhul. X-tee ei ole universaalne lahendus mistahes dokumentide jaoks, kuid teatud tüüpi dokumentide jaoks (rohkearvulised hästi defineeritud tüübi ja (pool)automaatse töötlusega dokumendid) on ta arvestatav lahendus.

6.4.3 Dokumendi saatmine riigiasutusele

Probleemid, võimalused ja lahendused on sarnased kui äriühingute puhul. Keskseks registriks on aga antud juhul Riigi- ja kohalike omavalitsuste asutuste register.

Võrreldes äriühingutega on riigiasutustele lihtsam teha mitmesuguseid ettekirjutusi selles osas, kuidas nad oma välissuhtlust peavad korraldama. Seetõttu saab riigiasutuste vaheline ühtne dokumentide vahetamise kord tekkida palju varem.

6.4.4 Konfidentsiaalsete dokumentide transport

Ohtude analüüsist järeldus, et konfidentsiaalseid dokumente tuleb transportida krüpteeritult. Krüpteerimiseks vajaliku seansivõtme genereerimine toimub sõltuvalt kasutatavast protokollist ning valitud algoritmidest erinevalt, kuid igal juhul on selleks vaja teada mingit saajakohast informatsiooni. Seejuures on oluline, et see informatsioon oleks autentne: kui ründajal õnnestub seda infot võltsida on tagajärjeks dokumentide avalikustumine.

Vaatleme kõigepealt erinevaid protokolle koos nende poolt pakutavate võimaluste ja seatavate piirangutega.

6.4.4.1 Protokollid

6.4.4.1.1 SSL ja TLS

SSL protokoll on rakendustaseme protokoll, mis on mõeldud TCP ühenduste turvamiseks. Protokoll eeldab, et serveril on X.509 sertifikaat ning kliendil on võimalus kontrollida selle autentsust. Protokoll lubab sertifikaadi olemasolu ka kliendil: sellisel juhul tagatakse kahepoolne autentimine. Protokollis võib salastatuse tagamine toimuda kahel eri viisil:

1. klient genereerib juhusliku võtme ja saadab selle serveri avaliku võtmega krüpteeritult serverile.
2. kliendi ja serveri vaheline krüpteerimisvõti lepitakse kokku Diffie-Hellmani võtmevahetusalgoritmi abil.

Esimene meetod ei taga täieliku tulevikuturvet ning on aldis passiivsetele rünnetele. Teine meetod tagab täieliku tulevikuturbe ning on murtav vaid aktiivse ründega. Seetõttu tuleks kindlasti alati eelistada teist võtmevahetusmeetodit (ehkki ta on pisut rohkem ressursse nõudev).

SSL ja TLS protokollid on kasutusel väga paljudes rakendustes. Käesoleva dokumendi kontekstis väärivad neist rakendustest ennekõike äramärkimist:

1. turvaline veeb (HTTPS protokoll on sisuliselt HTTP protokoll üle SSL toru);
2. turvaline meilivahetus (TLS protokolli tugi SMTP protokollile);
3. turvaline meililugemine (TLS protokolli tugi IMAP ja POP3 protokollile);
4. X-tee (X-tee süsteemis kasutatakse turvaserverite vahel liikuvate andmete turvamiseks SSL protokolli).

Tihti arvatakse, et SSL protokolli kasutamine näiteks veebirakendustes asendab digitaalallkirja ning et näiteks SSL protokolli kõigi sõnumite salvestust saaks kasutada tõendamaks mingi infovahetuse toimumist. Tegelikult ei ole see nii. SSL ühenduse algatamisel lepivad osapooled kokku jagatud saladuse ning kogu järgneva infovahetuse kaitse, kaasaarvatud tervikluse ning autentsuse tagamine, toimub selle baasil. Kuna see väärtus on teada mõlemale osapoolele siis on neil võimalus hiljem konstrueerida suvalisi korrektseid paketijadasid. Sama omadus on ka teistel levinud transporditurbe protokollidel nagu SSH ja IPsec

6.4.4.1.2 IPsec

IPsec on võrgutaseme protokoll ning mõeldud IP pakettide turvamiseks. Täpsemalt on tegu terve protokollide ja standardite perega, millest erinevad tootjad on realiseerinud erinevaid osi, lisades oma toodetele veel firmapäraseid laiendusi. Seetõttu on IPsec'i evitamine pikalt vindunud, olles alles viimastel aastatel jalad alla saanud, seda ennekõike VPN'de loomise ning turvalise kaugtöö korraldamise juures.

IPsec'i võtmevahetusprotokoll IKE on küllalt heade omadustega ning tagab täieliku tulevikuturbe. Osapoolte autentimiseks võib kasutada mitmeid eri tüüpi vahendeid (paroolid, sertifikaadid, jne). Mingit erilist usaldusmudelit ette ei kirjutata ega fikseerita: süsteemi ülesseadja võib luua ühtviisi hõlpsalt nii väga avatud kui ka täiesti suletud süsteemi.

6.4.4.1.3 S/MIME

S/MIME on turvalise meili standard. Võimalik on kirju signeerida ning krüpteerida. Usaldusmudel üritab tagada saatja aadressi autentimist. S.t. meiliprogrammid kontrollivad, et kirja saatja aadress (*From*: rida kirja päises) klapiks kirja keha allkirjastamiseks kasutatud sertifikaadis sisalduva aadressiga. Kuna tegu ei ole interaktiivse protokolliga, siis ei ole võimalik tagada täielikku tulevikuturvet.

6.4.4.2 Rakendused

6.4.4.2.1 Turvaline veeb

Veebi turvamisel on oluliseks disainikriteeriumiks olnud sujuva surfamise tunde tagamine. Kasutaja tegelikult ei märka, kui ta siseneb turvalisse veebialasse või lahkub sealt, samuti võib praktikas probleeme tekitada erinevate serverite eristamine.

Probleemi põhjused on ennekõike veebi olemuses: tegu on ju hüperlingitud dokumentidega, mis üritavad serveritevahelisi piire kaotada. Turvaliste veebirakenduste puhul oleks aga just vaja tekitada pisikesi suletud piirkondi, mis aga brauserite võimaluste rohkuse tõttu (JavaScript, ümbersuunamised, freimid) väga raske on.

Teine probleem on selles, et brauserid ei esita serveri (turva)infot kasutajale käideldaval viisil, mis muudab vahendusrünnete sooritamise kasutajate vastu kaunis lihtsaks. Võttes arvesse veel sellised klassikalised veebirakenduste loomise probleemid, nagu seansihalduse (kus on väga lihtne suuri vigu teha) ning kasutajate hoolimatuse turvaküsimuste suhtes, võime tõdeda, et veebi kasutamine suletud ja turvaliste süsteemide loomiseks on keeruline ülesanne.

6.4.4.2.2 Turvaline meilivahetus

Enamuse SMTP protokolli kasutavate meilivahetusprogrammide (sendmail, postfix, jne) uusversioonid toetavad sõnumite edastamist TLS protokolliga kaitstult. Kui meil on hulk servereid, mis peaks üksteisele konfidentsiaalseid sõnumeid saatma, siis võime genereerida neile kõigile võtmed, sertifitseerida need (või lihtsamal juhul laadida suhtluspartnerite endasigneeritud sertifikaadid otse serveri konfiguratsiooni) ja käivitada turvalise meilivahetussüsteemi.

Erinevalt klassikalisest VPN süsteemist on selles meilivahetussüsteemis osalevate asutuste sisevõrgud üksteisest endiselt täiesti lahutatud. Ka on sellise süsteemi ülesseadmine lihtne ega nõua suuri investeeringuid. Kuna elektronpost on üks enamlevinud viise sõnumite vahendamiseks, siis aitaks asutustevahelise meililiikluse autentsuse, tervikluse ja konfidentsiaalsuse tagamine oluliselt kaasa dokumentide vahetuse paremale korraldamisele.

6.4.4.2.3 Turvaline meililugemine

Enamus kaasaaegseid postiprogramme toetab kasutaja postkasti poole pöördumist TLS protokolliga turvatult. Sellisel viisil välistatakse kasutaja arvuti ning meiliserveri vahelise võrguliikluse pealtkuulamine, samuti autentimiseks kasutatavate paroolide leke.

Kui eelmine vahend (turvaline meilivahetus) oli mõeldud just dokumentide kaitseks nende teel ühest asutusest teiseni, siis turvaline meililugemine kaitseb neid asutuse sisevõrgus. Loomulikult on meililugemisprotokollide turvamine eriti oluline juhul, kui asutuse meiliserverile on juurdepääs ka välisvõrgust.

6.4.4.2.4 S/MIME

On konfidentsiaalsuse tagamisel mõnes mõttes alternatiiv ning mõnes mõttes täiendus kahele eelmisele rakendusele. S/MIME võimaldab dokumendi saatmist krüpteeritult ühelt kasutajalt teisele, nii et isegi nende serverite administraatorid, mida dokument läbib ei saa seda lugeda. Turvaline meilivahetus koos turvalise meililugemisega kaitsevad dokumenti aga ainult teel üle avaliku võrgu ning ei kaitse teda serverites.

Turvalise meilivahendussüsteemi saab käivitada praktiliselt ilma kasutajate koostööta ning ta töötab alati: kasutajal pole võimalust teda "välja lülitada". S/MIME süsteemi evitamine on palju suurem töö, kusjuures põhiraskus on just kasutajate koolitamisel.

Neid kaht süsteemi võib ka kombineerida, saates S/MIME sõnumeid läbi turvaliste sidekanalite.

S/MIME sõnumitega on seotud veel üks oht: dešifreerimisvõtme hävimine. Kuna iga kiri on krüpteeritud eraldi ning dešifreerimisvõti on vaid ühe isiku (kirja saaja) valduses, siis selle võtme hävimise korral ei ole vastavat dokumenti enam võimalik lugeda. Selle ohu vastu on välja mõeldud mitmesuguseid abinõusid, kuid nende rakendamisel lähevad suures osas kaotsi S/MIME eelised turvalise meilivahendussüsteemi ees.

S/MIME on sobilik juhul, kui kasutajate hulk on väike, kasutajad ise arukad, ning dokumentide konfidentsiaalsusnõuded kõrged.

6.4.4.2.5 VPN

VPN süsteem võimaldab liita organisatsiooni sisevõrgu eraldiseisvad osad üheks tervikuks. VPN süsteeme saab kasutada ka asutustevahelise suhtluse turvamiseks, kuid see ei ole enamasti otstarbekas. VPN süsteem seob osavõrgud väga tihedalt, pakkumata samas võimalusi mingi suhtlusakti toimumise tõestamiseks. See toob kaasa vastutuse hajumise osapoolte vahel, mis on ebasoovitav. Käesoleva dokumendi kontekstis on VPN süsteemid olulised, kuna nende kaudu võidakse vahetada ka näiteks konfidentsiaalseid dokumente asutuse siseselt.

6.4.4.2.6 Turvaline kaugpöördus

Turvaline kaugpöördus on lahendus, mis võimaldab üksikul töökoha arvutil, mis asub väljapool asutuse sisevõrku, pöörduda sisevõrgus olevate serverite poole ning saada juurde neis sisalduvatele andmetele. Turvalise kaugpöörduse korral kehtib sama reegel, mis VPNi korralgi: tegu on asutuse siseasjaga. Kui ühe asutuse töötaja peab saama ligi teise asutuse inforessurssidele, siis pöördub ta kõigepealt oma sisevõrku ning seejärel sealt üldisi kanaleid pidi edasi.

6.4.4.2.7 X-tee

X-tee süsteemis kasutatakse andmete kaitseks SSL protokolli. Diffie-Hellmani võtmevahetusalgoritmi kasutamisega tagatakse täielik tulevikuturve. Osapoolte sertifikaadid on välja antud X-tee keskuse poolt. Enne sertifikaatide kasutamist kontrollitakse nende kehtivust keskserveri andmebaasist turvalise nimeteenuse abil.

Ehkki X-tee oli algselt mõeldud andmebaasipäringute vahendamise süsteemiks, saab teda edukalt kasutada suvaliste sõnumite edastamiseks osapoolte vahel, tagamaks nende turvalist transporti.

6.5 Digitaalallkirjade pikaajalise tõestusväärtuse tagamine

Digitaalallkiri peab säilitama oma kehtivuse ka pärast seda, kui sertifikaat, mille alusel ta anti, tühistatakse. Erinevalt omakäelisest allkirjast ei ole digitaalallkirja andmise vahend omanikuga igavesti seotud (omanik vastutab vaid piiratud aja vältel antud allkirjade eest).

Et digitaalallkirju saaks praktikas kasutada, peab digitaalallkirja verifitseerimine kauges tulevikus andma sama tulemuse, kui digitaalallkirja verifitseerimine antud ajahetkel, mil allkirjastatud dokumendi alusel hakatakse mingit otsust tegema. Kasutatavate digitaalallkirja süsteemide oluline omadus on võime anda digitaaldokumendile pikaajaline tõestusväärtus.

Ehk siis: kui dokumendi verifitseerimine õnnestus üks kord, peab ta õnnestuma ka edaspidi ning andma alati sama tulemuse. Et seda nõuet täita tuleb:

1. fikseerida allkirja andmise aeg;
2. alati kontrollida allkirja kehtivust tuginedes allkirja andmise ajal kehtinud seostele.

Sertifikaatide kasutamisel muuks otstarbeks (näiteks autentimisel veebirakendustes) on oluline vaid sertifikaadi kehtivus antud ajahetkel. Kogu infrastruktuur (kataloogiteenus jms.) on üles ehitatud pakkuma vaid hetkel kehtivaid andmeid (sertifikaate, tühistusnimekirju).

Digitaalallkirja puhul on meil aga oluline säilitada asjade seis allkirja andmise ajal. Allkirja andmise aja fikseerimiseks kasutatakse ajatembeldust. Kuid ainult ajatembeldusest ei piisa. Huvitatud osapool peab olema valmis näitama, kes vastutas allkirjastamise hetkel (see selgub ajatemplist) antud digitaalallkirja andmise vahendi abil moodustatud allkirjade eest.

Seos isiku ja allkirja kontrollimise vahendi vahel on kirjas sertifikaadis. Sertifikaati võib säilitada koos dokumendiga. Kuid see ei lahenda veel kogu probleemi. Meil on vaja veel näidata, et:

1. antud sertifikaat kehtis allkirja andmise hetkel (ei olnud tühistatud);
2. antud sertifikaadi signeerimiseks kasutatud võti kuulus allkirjastamise hetkel sertifikaadis nimetatud sertifitseerimisteenuse osutajale ja ei olnud tühistatud;
3. sertifitseerimiskeskuse sertifitseerija võti kehtis;
4. jne, kuni tipmise sertifitseerimiskeskuse avaliku võtmeni välja;
5. näidata milline oli sel hetkel tipmise sertifitseerimiskeskuse avalik võti.

Tühistusnimekirjade kasutamise korral loetakse sertifikaat mingi ajahetke suhtes kehtivaks siis, kui:

- antud ajahetk jääb sertifikaadis kirjas oleva kehtivusaja piiridesse;
- antud ajahetkel kehtiv tühistusnimekiri ei sisalda antud sertifikaati.

Seega peaks nõuete 1.-4. täitmiseks koos dokumendiga ajatembeldama ka kõigi sertifitseerimiskeskuse osutajate sertifikaadid ja tühistusnimekirjad. Lisaks peab kuidagi arvet pidama ka tipmise sertifitseerimiskeskuse avalike võtmete kehtivuse üle.

Olukorra muudab veelgi komplitseeritumaks asjaolu, et tühistusnimekirju avaldatakse perioodiliselt. Kuni uus tühistusnimekiri pole välja tulnud ei saa me kindlad olla, et meid huvitav sertifikaat endiselt kehtib. Kui tühistusnimekirju avaldatakse väga harva, siis muudab see aeglasemaks kogu digitaalallkirju kasutava süsteemi (kõik peavad ootama järgmise tühistusnimekirja taga). Kui tühistusnimekirju avaldatakse väga tihti, siis tekitab see suure koormuse suhtluses kataloogiteenusega.

Seda probleemi ja võimalike lahendusi sellele on põhjalikult analüüsitud töös [34]. Lisaks tühistusnimekirjade kasutamisele on seal vaadeldud ka sertifikaatide kehtivusinfot jagamist on-line teenuse kaudu (näiteks OCSP protokolli abil) ning signatuuride kehtivuse kinnitamist valideerimisteenuse (nimetatakse ka digitaalnotari teenuseks) abil.

Valideerimisteenuse kasutamisel on märkimisväärsed eelised teiste skeemidega võrreldes:

- võimaldab sertifikaatide kiiret tühistamist;
- sidekanalite kasutamine on efektiivne;
- võimaldab otseselt kinnitada allkirja kehtivust;
- kehtivuskinnitused on kompaktsed;
- võimaldab pakkuda ühtlasi ka ajatempliteenust (praktilises rakenduses sulavad valideerimisteenus ja ajatempliteenus tegelikult üheks teenuseks kokku).

6.5.1 Usaldust nõudvad ajatempliteenused

Usaldust nõudvat teenust saaks pakkuda vaid piisavalt usaldusväärne riigiasutus. "Piisavalt usaldusväärne" on seejuures suhteline mõiste ja vaadelda tuleb seda mingi konkreetse dokumentide klassi suhtes, võttes arvesse dokumendi tagantjärele võltsimisel tekkivaid probleeme. Selline teenus ei ole universaalselt kasutatav. Ühe dokumendiklassi kohta tehtud positiivne otsus konkreetse teenuseandja poolt pakutava teenuse kohta ei ole automaatselt ülekantav teisele dokumendiklassile.

6.5.2 Usaldust mittenõudvad ajatempliteenused

Sellist teenust võiks põhimõtteliselt pakkuda suvaline isik. Kuna võltsimisvõimalused on minimaalsed, siis on võimalik teha universaalne otsus konkreetse teenuseosutaja poolt pakutava teenuse kõlblikkuse kohta. Probleemideks on vähene standardiseeritus ning hea publitseerimiskanali puudus.

6.6 Arhiveerimine

Digitaaldokumentide pikaajalise säilitamise juures tuleb arvestada nelja põhiprobleemiga:

- arhiveerimise korra muutumine seoses üleminekuga digitaaldokumentidele;
- dokumentide loomisel kasutatud tarkvara moraalne vananemine;
- säilitusmeedia füüsiline ja moraalne vananemine ning
- töö lõpetanud STO-de ja ATO-de arhiivide säilitamine.

Kui dokumentidega koos tuleb säilitada ka digitaalallkirja, ajatemplite jms tõestusväärtus, siis lisandub veel üks mure:

- kasutatud krüptograafiliste primitiivide murdumine, mistõttu saab võimalikuks tõestusväärtusega info tagantjärele võltsimine.

Nende probleemide lahendamiseks peavad metoodikad ilmselt valmima ning standarditud saama enne digitaalse dokumendihalduse ja digitaalallkirja laialdast kasutuselevõttu. Tarkvara ja säilitusmeedia vananemist on käsitletud eespool, järgnevalt vaatleme lühidalt arhiveerimise ja krüptograafiliste primitiivide murdumisega seotud probleemide lahendamisvõimalusi.

6.6.1 Arhiveerimise korra muutumine

Arhiveerimise korda reglementeerivad Eesti Vabariigis Arhiiviseadus [7] ja Arhiivieeskiri [8], neist esimene sätestab üldised põhimõtted ja teine täpsustab tehnilised üksikasjad.

Vastavalt arhiveerimist käsitlevatele õigusaktidele (Arhiiviseadus ja Arhiivieeskiri) on iga asutus arhiivimoodustaja, kelle ülesanne on organiseerida dokumendid sarjadesse ning need siis arhiivile sobivuse hindamiseks vastavale arhiivitöötajale edastada. See peab ilmselt nii jääma ka digitaalse asjaajamise korral, ainult et sarja ei saa enam käsitleda kaustade reana riiulil, vaid kataloogina kõvakettal, konteinerformaadina vms. Täpset tehnilist lahendust hetkel ei ole, seepärast **tuleb välja töötada standardformaadid dokumendisarjade esitamiseks.**

Kindlasti on arhiivimoodustajatele tarvis pakkuda kasutamiseks ka mingit valitud formaati toetavat näidistarkvara.

Pärast sarja aktsepteerimist arhiivi poolt peab arhiiv tagama selle säilimise. Ilmselt tähendab see laekunud andmete salvestamist mingile kandjale ning kandjate organiseerimist teataval süsteemsel ja ligipääsetaval moel. Muuhulgas tähendab see kõigi arhivaalide kirjeldamist, mille üldise korra määrab Arhiivieeskiri. Nii salvestamist, kirjeldamist kui säilitamist võib

läbi viia mitmeti ja mingi ühtse standardi kehtestamise vajadus pole hetkel selge. Pigem on küsimus "heade tavade" väljakujunemises ning selleks läheb veel paar aastat aega. Seni piisab kui arhiivid oma digitaaldokumentide säilitamise praktika piisava põhjalikkusega dokumenteerivad ning tagavad säilikutele ligipääsetavuse seaduses ettenähtud korras.

Küll aga võib DHP raames töötada välja soovitused "heade tavade" kujundamiseks ning võimaldada ligipääsu vajalikele rahvusvahelistele standarditele ja tarkvarale.

6.6.2 Töö lõpetanud teenuseosutajate arhiivide säilitamine

Vastavalt Digitaalallkirja seadusele peavad töö lõpetanud STO-d ja ATO-d andma oma arhiivid üle Sertifitseerimise riiklikule registrile. Seadus jätab lahtiseks, mida SRR saadud andmetega edasi peab tegema.

Arvestades, et need andmed võivad nt tulevastes kohtuvaidlustes tõenditena kasutust leida, tuleks kindlasti tagada nende süstematiseeritus, terviklikkus ja ligipääsetavus. Need ülesanded kuuluvad aga loomulikul moel avalikule arhiivile. Niisiis on otstarbekas **täiendada seadusi nägemaks ette töö lõpetanud teenuseosutajate andmete jõudmine avalikku arhiivi.**

6.6.3 Krüptograafiliste primitiivide murdumine

Praktiliselt ükski digitaalallkirja andmisel kasutatav algoritm ei ole 100% turvaline. Võib juhtuda, et mõne algoritmi vastu leitakse niisugune rünne, mis võimaldab näiteks arhiiviteenuse osutajal tagantjärgi ajatemplite järjestust muuta.

Arhiiv on senini olnud usaldatav osapool, kelle tõendid ei ole üldjuhul vaidlustatavad. Paberdokumentide spetsiifikast lähtuvalt on vanade dokumentide võltsimine suhteliselt hästi tuvastatav ja praktikas ei kujuta arhiivi usaldamise vajadus endast probleemi. Digitaaldokumentide võltsimine jälgi jätmata pärast nende moodustamiseks kasutatud krüptograafiliste primitiivide murdumist on võimalik ja lihtne. Kui arhiiv ei värskenda perioodiliselt arhiveeritud dokumentide ajatempleid, siis kaob igasugune võimalus vaidlustada arhiivi väiteid.

See paneb arhiivile väga suure vastutuse. Otstarbekas oleks seda vähendada **digitaalarhiivide sobilike protseduuride ning tehniliste lahenduste kasutamisega.**

7. Digitaalallkirja rakendamiseks vajalikud tugisüsteemid

Digitaalallkirja rakendamine on ka maailma maastaabis täiesti uudne valdkond. Nagu eelpooltoodud analüüsist järeldada võib, tekivad digitaalallkirja rakendamisel nii tehnoloogilised, õiguslikud kui ka organisatsioonilised probleemid. Erinevaid probleeme on uuritud erineva põhjalikkusega, mõne lahenduse osas on juba käimas standardimisprotsess, ent suurema osa probleemide jaoks olemasolevaid valmislahendusi ei eksisteerigi.

Seetõttu ei tekkinud ka Eesti Vabariigi tingimustes digitaalallkirja rakendamiseks strateegilise plaani koostamise käigus ühtset, universaalset ning kõiki probleeme lahendavat arhitektuuri, vaid on pakutud erinevaid tugisüsteeme erinevate probleemide lahendamiseks. Maksimaalselt on püütud ära kasutada juba olemasolevaid struktuure ning suurte riiklike programmide ja projektide käigus tekkivaid lahendusi.

Kuna digitaalallkirja rakendamisega seonduvad protsessid on jätkuvalt muutuvad ning arenevad, võib arvata, et praegused lahendused ei ole lõplikud ning lähema paari-kolme aasta jooksul leitakse võib-olla paljudele probleemidele hoopis uudsed ning paremad lahendused. Järgnevalt pakutud skeemid annavad prioriteetsete digitaalallkirja kasutusvaldkondade probleemidele küllalt optimaalse lahenduse.

7.1 ID-kaardi põhine isikute autentimine veebis

Meie hinnangul on see koheselt teostatav kasutades standardseid vahendeid. ID-kaardi sertifitseerimisteenuse osutaja poolt pakutavad teenused on selleks piisavad.

7.2 Digitaalselt allkirjastatud registripäringud

2001 aasta lõpul valmib andmekogudele ühtlustatud juurdepääsu võimaldav süsteem X-tee. Süsteem on projekteeritud eeldusel, et teda saab kasutada kooskõlas kehtiva seadusega, mille kohaselt andmete õiguspärase kasutamise eest vastutab andmekogu töötleja, ning et kõik süsteemi poolt vahendatud päringud ja päringvastused omaks tõestusväärtust. Tõestusväärtus on tagatud ühelt poolt digitaalallkirja definitsiooni rahuldavate infotehnoloogiliste vahendite kasutamisega ning teiselt poolt X-tee keskuse ja liitunud asutuste vahelise lepingute süsteemiga.

On olemas praktiline vajadus kasutada neid päringuvastuseid haldustoimingutes. Juristid on pidanud võimalikuks kasutada automaatselt väljastatud ja tõestusväärtust omavaid päringuvastuseid haldustoimingute aluseks.

Õigusjõuga registripäringute tegemiseks soovitame kasutada X-tee süsteemi. Tehniline valmisolek selleks tekib aasta lõpul, organisatsioonilise tööga (infrastruktuuri käivitamine ja lepingute sõlmimine) saadakse valmis loodetavasti järgmise aasta algul.

X-tee süsteemi juriidilisi alustalasid saaks veelgi tugevdada, kui registreerida X-tee keskus Sertifitseerimise Riiklikus Registris nii sertifitseerimisteenuse osutajana kui ka ajatempliteenuse osutajana. Sisuline valmisolek selleks on olemas, SRR-s registreerumiseks vajalikud dokumendid on suures osas koostatavad olemasoleva X-tee dokumentatsiooni põhjal.

7.3 Asutuste ja ettevõtete vaheline dokumendivahetus

Esitatav lahendus eeldab järgmiste üldiste sammude teostamist:

- Luuakse kõikide dokumenditüüpide ühtne klassifikaator.
- Äriregistrile lisatakse ka riigi- ja kohaliku omavalitsuse asutuste registri funktsioon.

- Äriregistrile lisatakse andmed äriühingute töötajate ning riigiametnike volituste kohta.
- Äriregistri juurde luuakse volituste kontrollimise teenus – volituste register.
- Täiendatakse Äriregistri infosüsteemi, nii et volituste kontrollimise teenuse osutamine saaks võimalikuks.

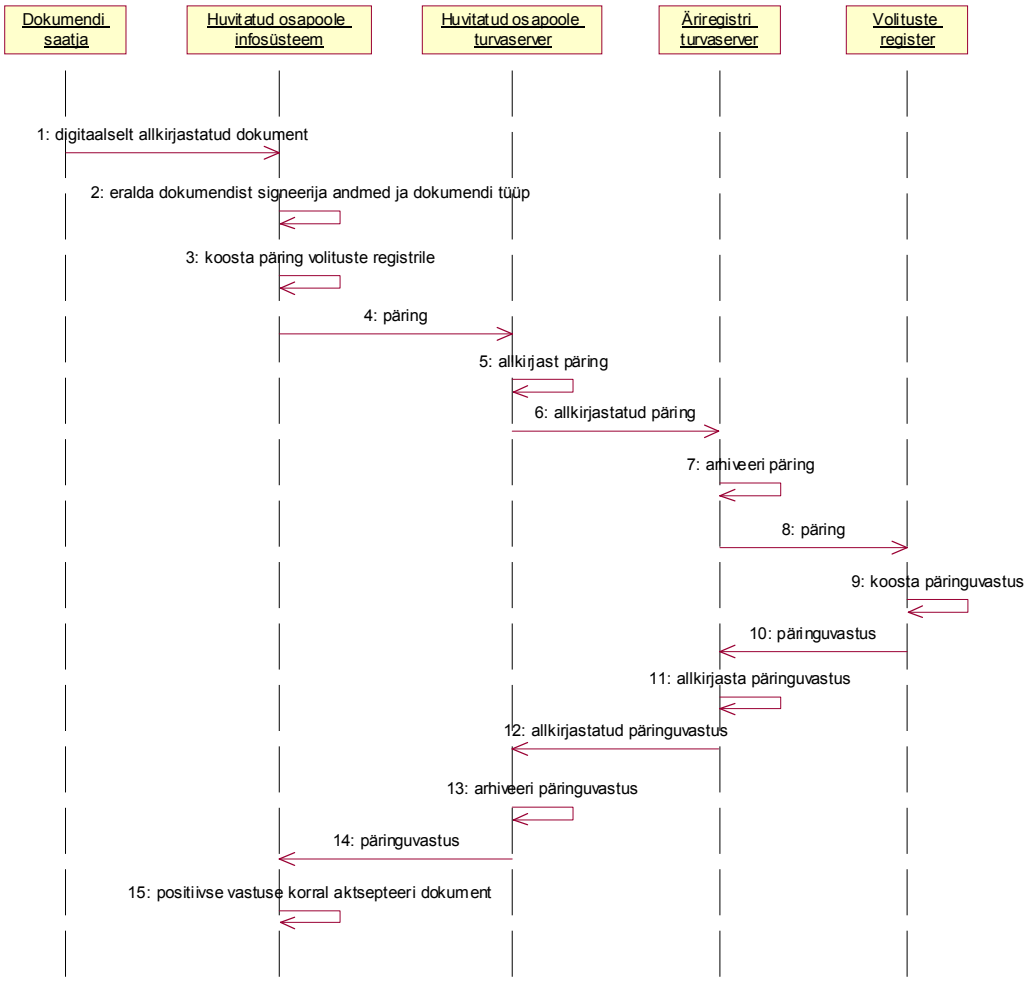
Tehniline lahenduse luuakse kahes etapis.

1. Esimese etapi tulemusel saavad suured (infotehnoloogiliselt tugevad) asutused ja äriühingud, kes on valmis ja suutelised X-teega liituma, vastu võtta ka väikeste, X-teega mitteliitunud asutuste poolt digitaalselt esitatud dokumente. Esimeses etapis realiseeritakse juurdepääs volituste registrile läbi X-tee.
2. Teise etapi tulemusel tagatakse alternatiivse, X-teega mitteseotud juurdepääsutehnoloogiaga volituste registrile digitaalsete dokumentide vastuvõtu võimalus kõigile ülejäänud asutustele ja äriühingutele ning ka eraisikutele.

7.3.1 Esimene etapp

Juurdepääs volitusinfole tagatakse X-tee infrastruktuuri kaudu, realiseerides lahendusvariandid Volituste register (6.3.3.2.) ja Volitused koos avalike võtmetega (6.3.3.3.).

Eeltingimus lahenduse kasutamiseks on see, et huvitatud osapool ja Volituste register liituvad X-teega.



Joonis 12. Volitusinfo kontroll X-tee kaudu.

Käesolev lahendus kasutab ära automaatsete õigusjõuga registripäringute esitamiseks loodud X-tee süsteemi, andes selle kaudu juurdepääsu volitusinfo registrile. X-tee funktsiooniks on päringutele ja päringuvastustele tõestusväärtuse andmine ning selle säilitamine.

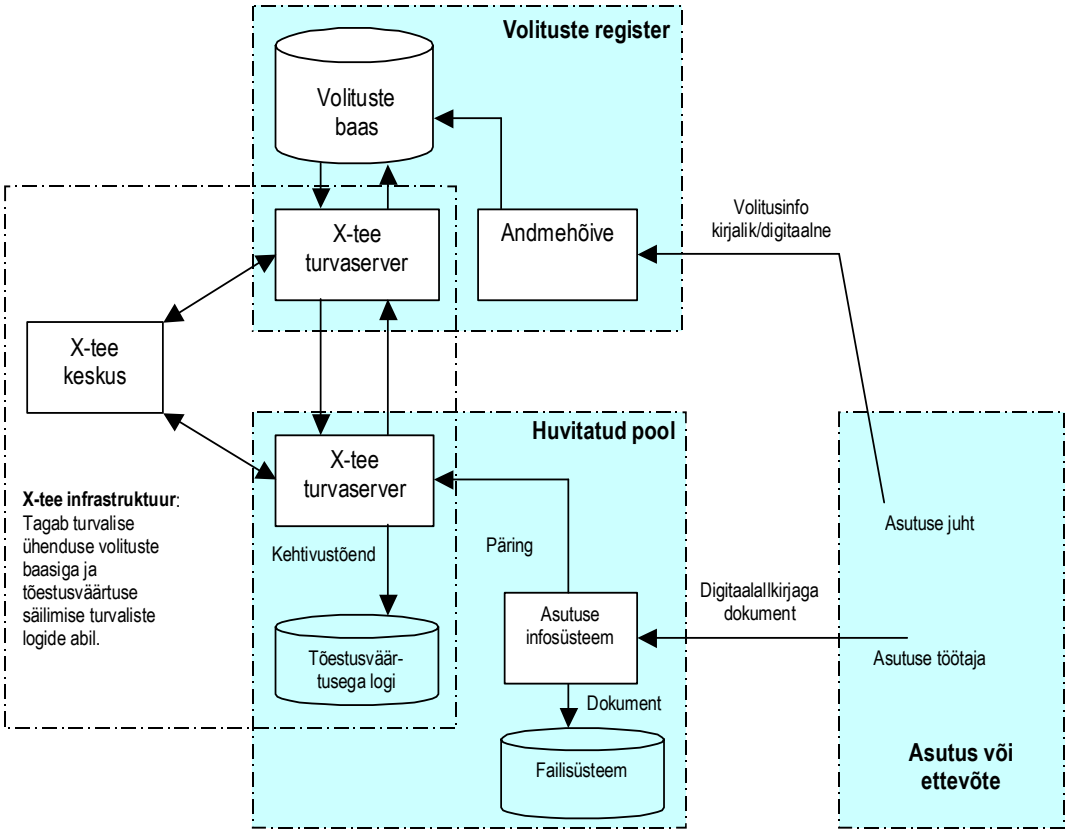
Selle süsteemi evitamiseks tuleb realiseerida:

- volituste register, koos X-tee liidese ja andmehõive protseduuride ning reeglitega;
- kontrollitava dokumendi alusel X-tee päringu koostamise moodul, mida oleks võimalik hõlpsalt integreerida huvitatud osapoole olemasoleva infosüsteemiga.

Sellise süsteemi saab realiseerida kiiresti – reaalne oleks süsteemi piloteerida märtsis 2002. Seega saavad X-teega liitunud asutused ja ettevõtted hakata vastu võtma digitaalallkirjaga dokumente teiste asutuste ja ettevõtete töötajatelt alates aprillist 2002.

Selle lahenduse puudus on see, et huvitatud osapool peab olema liitunud X-teega, see kitsendab huvitatud poolte klassi. See on ka põhjus, miks on vaja teist etappi.

NB! Igal juhul peavad konkreetsed huvitatud osapooled defineerima ja arendama endale sobiliku dokumentide hoidmise süsteemi, nii et side digitaalallkirja ja tõestusväärtusega säiliks.



Joonis 13. Volituste kontroll X-tee infrastruktuuri kaudu

7.3.2 Teine etapp

Teise etapi eesmärgiks on tagada juurdepääs volitusregistrile kõigile isikutele, ka neile, kes ei suuda X-teega liituda. Selleks lisatakse olemasolevale volituste registrile alternatiivne liides, mis baseerub rollisertifikaatidel (6.3.3.4.).

Vajalik tehnoloogia on põhimõtteliselt olemas, kuid seda on kindlasti vaja kohandada konkreetse kasutusjuhu jaoks. Samuti on vaja SRR's registreerida rollisertifikaatide väljaandja.

Rollisertifikaatide ning kehtivuskinnituste kasutamine võimaldab luua kompaktseid ja terviklike, iseseisvalt tõestusväärtust omavaid digitaaldokumente, mida võivad huvitatud osapooltena vastu võtta ja säilitada isegi eraisikud, samuti ka kõik need asutused ja ettevõtted, kes pole X-teega liitunud.

7.4 Digitaalne dokumendivahetus üksikisikutega

ID-kaardi digitaalallkirja sertifikaadi abil moodustatud dokumentide vastuvõtmiseks on olemasolevale infrastruktuurile vaja lisada kas ajatempliteenus või veel parem: ajatempliteenusega kombineeritud valideerimisteenus.

"ESTEID sertifitseerimispoliitika" alapunkti 4.2.4 "Sertifikaadi kontroll ja tõestamine" kohaselt hakkab ID-kaardi sertifitseerimisteenuse osutaja valideerimisteenust ka pakkuma. Vastavalt sertifitseerimispoliitikale ei ole tehnilised lahendused ja ilmselt ka ajakava veel kindlaks määratud. Lihtsaim lahendus probleemile olekski see, kui see teenus käivituks. Kui seda mingil põhjusel ei juhtu, siis on sõltumatult sertifitseerimisteenuse osutajast võimalik käivitada eraldiseisev valideerimisteenus, mis saab sertifikaatide kehtivusinfot sertifitseerimisteenuse osutaja kataloogiteenusest.

Lahenduse eelmistes punktides nägime ette asutuste ning äriühingute töötajate volitusi arvestava digitaalallkirjade kinnitamise süsteemi loomist. Selle süsteemi tehniline lahendus sobiks põhimõtteliselt ka eraisikute digitaalallkirjade valideerimisteenuse loomiseks. Isegi kui tegu saab olema kahe erineva teenusega oleks otstarbekas luua standard vastava teenuse pakkumiseks: see võimaldaks lihtsustada digitaaldokumente kasutavaid infosüsteeme.

Ka eraisiku digitaalallkirjade valideerimisteenuse loomine võiks toimuda kahes etapis, milledest esimesel pakutakse allkirjade kinnitamise võimalust läbi X-tee ning teisel lisandub alternatiivne liides eraisikute ning väikefirmade tarbeks. Nagu eelnevalt viidatud, plaanib valideerimisteenust pakkuda ka ID-kaardi sertifitseerimisteenuse osutaja, seetõttu on juhul, kui pakutav teenus hakkab vastama loodavale standardile, mõistlik seda teenust ka kasutada ning mitte kulutada raha riikliku teenuse loomisele.

7.4.1 Kasutusvaldkonna piirangute esitamine ilmutatud kujul

Projekti töörühmas tekkis arutelude käigus otsus mitte luua tehnilisi vahendeid sertifikaadi kasutusvaldkonna piirangute ilmutatud esitamiseks. Käesolev peatükk dokumenteerib väljapakutud lahenduse, mida aga hetkel realiseerima ei asuta. Lahendus on dokumenteeritud puhuks, kui osutub, et kirjeldatud ohud tõepoolest realiseeruvad ning tekib praktiline vajadus riskide maandamiseks sertifikaatide kasutusvaldkondade piiramise süsteem abil. Otsuse langetamiseks oleks vaja, et tekiks digitaalallkirja reaalne kasutus.

7.4.1.1 Kasutusvaldkondade kirjeldamise süsteem

Käesolev peatükk kirjeldab üht, hetkel praktilisena tunduvat kasutusvaldkondade kirjeldamise süsteemi.

Enamus digitaalallkirja rakendusi, mis hakkavad vastu võtma eraisiku poolt allkirjastatud dokumente, töötlevad neid dokumente automaatselt. Sellest tulenevalt peavad ka kasutusvaldkondade kirjeldused olema masintöödeldaval kujul.

Nii nagu asutuste ja äriühingute töötajate volituste kirjeldamise juures, võiks ka siin masintöödeldavate kasutusala piirangute esitamiseks kasutada lubatud dokumenditüüpide loendit. Kuna küllalt palju olulisi dokumente on seotud rahaliste suhetega, siis võiks dokumenditüübi siseselt olla võimalik ka rahalise piirangu lisamine.

Asutuste ja äriühingute töötajate volituste kirjeldamise süsteemi juures nähti ette ka teist liiki volitused, mis on mõeldud kasutamiseks ainult koos inimese poolt interpreteeritavate dokumentidega. Sel juhul on volituse sisuks vaba tekst. Kas sedasorti kasutusala piirangute kirjeldamise viis on vajalik ja otstarbekas ka selle süsteemi juures pole päris selge.

Esimeses lähenduses võiks seega kasutusvaldkondi esitada dokumenditüüpide nimekirjana, kus iga dokumenditüübi juures võib olla esitatud ka maksimaalne lubatud tehinguväärtus.

Näiteks:

Kodanik X Y ID-kaardi digitaalallkirja kasutusvaldkondade kirjeldus:

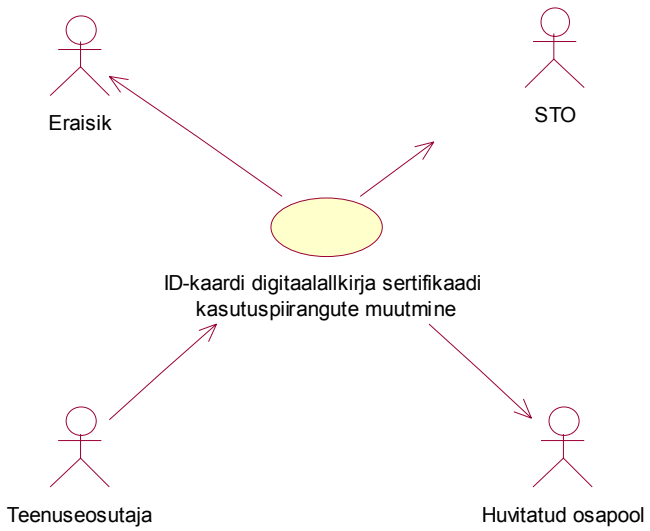
Dokumenditüüp	Maksimaalne tehinguväärtus (EEK)
Tuludeklaratsioon	-
Ostu-müügi leping	100
Pangaülekanne	1000
Pangakonto avamise leping	

7.4.1.2 Tehniline lahendus

Luua STO juurde kasutusvaldkondade register, mis:

- registreerib uusi dokumenditüüpe;
- võtab vastu kodanike omakäelisi avaldusi oma digitaalallkirja sertifikaadi kasutusvaldkonna muutmiseks;
- teeb selle info kättesaadavaks huvitatud osapooltele.

Kirjeldame selle registri seoseid muu maailmaga.



Joonis 14. Ülevaade tegijatest.

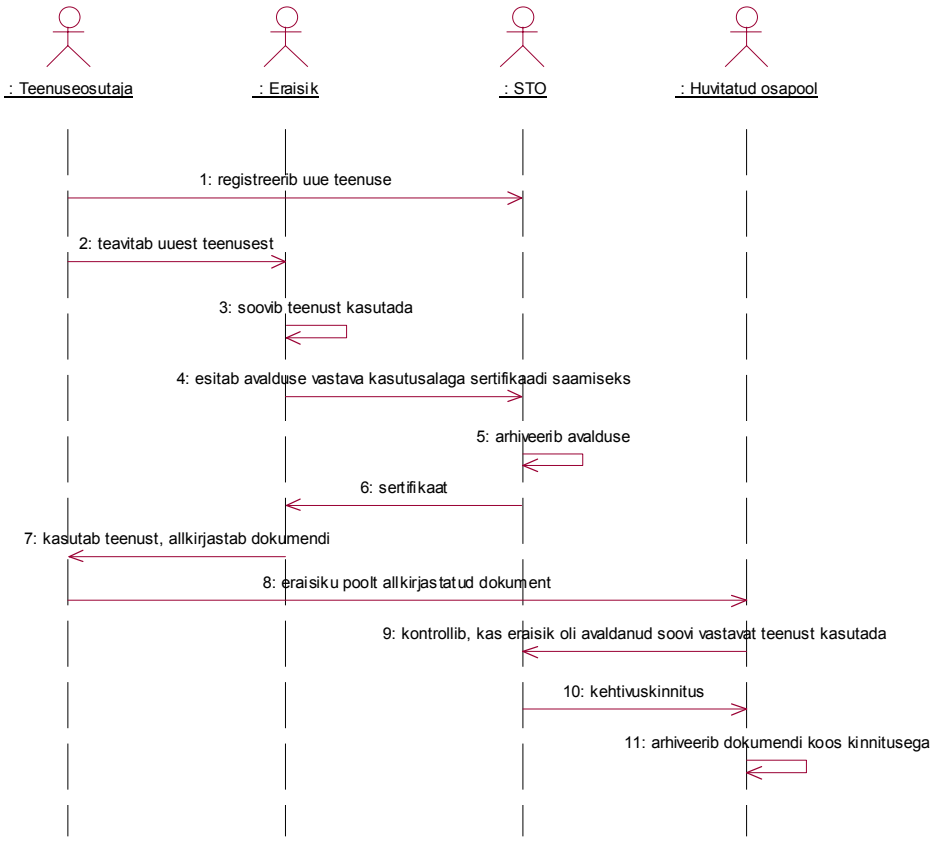
Teenuseosutaja on isik, kes pakub mingit teenust, mille kasutamine eeldab digitaalallkirjade andmist teenuse kasutaja poolt. Teenuseosutaja defineerib teenuse osutamiseks vajalikud dokumenditüübid (juhul, kui mõni olemasolevatest dokumenditüüpidest sobib, siis pole uute tüüpide defineerimine vajalik).

Eraisik on ID-kaardi omanik, kes soovib teenust kasutada.

STO on sertifitseerimisteenuse osutaja, kes jagab kasutusvaldkondade registri kaudu infot kodanike poolt soovitud kasutusvaldkondade kohta.

Huvitatud osapool on isik, kes kontrollib eraisiku poolt antud digitaalallkirja kehtivust.

Märkus: skeemil on kujutatud rolle, teenuseosutaja ja huvitatud osapool võivad tegelikult olla üks ja sama isik.



Joonis 15. Uue teenuse registreerimine.

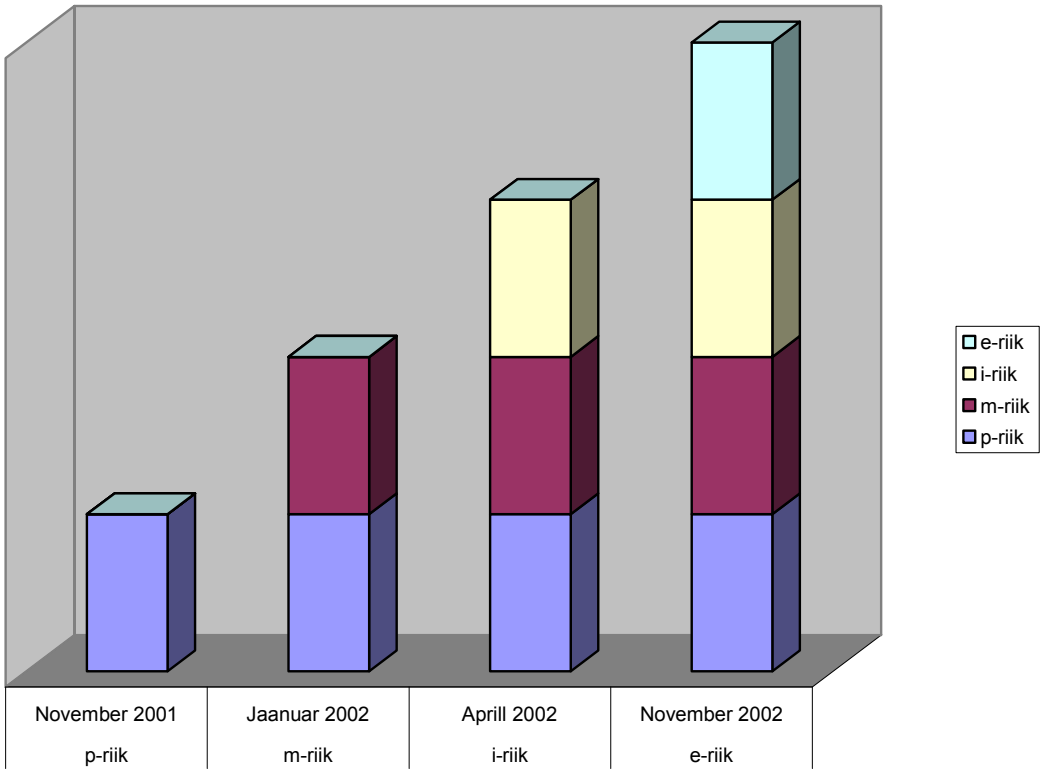
Ainus samm, mis eeldab kodaniku füüsilist kohaleilmumist ning omakäelist allkirja on neljas samm. Samas võib sama avaldusega laiendada sertifikaadi kasutusvaldkonda mitme dokumenditüübi võrra. Samuti võib vastava avalduse täita koos ID-kaardi saamise avaldusega, mis jällegi vähendab klienditeenindusepisoodide arvu.

Tehnilise poole pealt on süsteem täpselt sarnane asutuste ja firmade töötajate volituste kättesaadavaks tegemise süsteemiga. Erinev on ainult registri seisu muutmise kord. Seega saaks teenuse osutamiseks kasutada ka sama tarkvara (kohendamine on ilmselt vajalik).

7.5 Arengu järjepidevus

Käesolev peatükk näitab pakutud lahenduste arenguloogikat ja kord juba realiseeritud süsteemide korduvkasutust järgneva taseme süsteemide poolt.

Järgnev joonis kujutab asjaajamise digitaliseerituse kasvu aja möödudes. Oleme tähistanud praegust olukorda väljendiga "p-riik", mis viitab paberlikule asjaajamisele. Viimase etapi lõpus valitsevat olukorda tähistame väljendiga "e-riik", mis viitab elektroonilise asjaajamisele. (Vahepeal on veel kaks taset, mida on tähistatud, kasutades tähestikus "p" ja "e" vahele jäävaid tähti, väljenditega "m-riik" ja "i-riik": kui neile mingit tähendust omistada, siis ehk "moderniseeritud asjaajamisega riik" ja "innovaatilise asjaajamisega riik")



Joonis 16. Arengufaasid.

Kirjeldame, millised süsteemid mingil etapil realiseeritakse, kuidas realiseeritavad süsteemid kasutavad juba olemasolevaid ning millised on prioriteedid igal arenguetapil.

7.5.1 p-riik

Ettevalmistused X-tee käivitamiseks. Põhirõhk on kahel tegevusel:

- X-tee õigusliku baasi kindlustamine, registreerimine STO ja ATO'na;
- X-tee serverite ning asutuste ja andmekogude infosüsteemide poolt tekitatavate, tõestusväärtust omavate logide arhiveerimise küsimuste lahendamine.

Etapi lõpul on võimalik X-tee kaudu esitada päringuid registritesse ning saada õigusjõudu omavaid päringuvastuseid, mida saab kasutada haldusmenetluse protsessis.

7.5.2 m-riik

Ettevalmistused asutuste ja firmade töötajate volitusi haldava registri käivitamiseks. Põhirõhk on kolmel tegevusel:

- volituste registri loomine ja käivitamine, kasutades X-tee poolt pakutavat tõestusväärtust tekitavat transpordikihti;
- kodanikusertifikaatide kehtivusinfo kättesaadavaks tegemine X-tee kaudu;
- dokumendivormingute väljatöötamine ja standardimine.

Etapi lõpul on X-teega liitunud asutustel võtta vastu suvaliste asutuste ja firmade töötajate ning eraisikute poolt digitaalselt allkirjastatud dokumente. Selle eesmärgi saavutamiseks kasutati ära eelmisel sammul loodud infrastruktuur (X-tee).

7.5.3 i-riik

Ettevalmistused rollisertifikaatide väljastamiseks. Põhirõhk on kolmel tegevusel:

- rollisertifikaatide väljastamise ning kehtivuskinnituste väljastamise teenuse loomine, eelmisel etapil loodud volituste registri baasil;
- valideerimisteenuse ja ajatempliteenuse loomine ID-kaardi digitaalallkirja sertifikaatide jaoks;
- seoses huvitatud osapoolte ringi laienemisega üle vaadata arhiveerimise temaatika.

Etapi lõpul saavad kõik isikud toimida huvitatud osapooltena ning aktsepteerida digitaalselt allkirjastatud dokumente. Selle eesmärgi saavutamiseks kasutati ära eelmisel sammul loodud infrastruktuur (volituste register).

7.5.4 e-riik

Põhimõtteliselt oleme jõudnud olukorda, kus elektrooniline asjaajamine on võimalik kõikides riigiga seonduvates suhetes.

8. Tegevuskava

Käesolevas peatükis on välja pakutud konkreetsed sammud, mis digitaalse dokumendihalduse ja digitaalallkirja rakendamiseks lähitulevikus astuda tuleb.

8.1 Täiendavad uuringud

8.1.1 Seonduvate õigusaktide analüüs

Strateegilise plaani koostamise etapil pöörati põhitähelepanu seadustele ning muudele õigusaktidele, mis esitavad mingeid nõudmisi seoses digitaalallkirja rakendamisega. Täiendavalt on aga vajalik uurida:

- milliste õigusaktidega reguleeritakse valdkondi, mida mõjutavad digitaalallkirja juurutamiseks pakutavad lahendusskeemid
- kas need regulatsioonid üldse segavad digitaalallkirja juurutusprotsessi
- kas neisse on vaja teha mingeid muudatusi, hõlbustamaks digitaalallkirja rakendamist ning millised need muudatused võiksid olla

8.1.2 Vaidluste menetlemise protsess digitaalallkirja puhul

Analüütiliselt oleks vaja läbi mõelda (kohtu)vaidluste protsess digitaalsete tõendite puhul, kaasaarvatud ID-kaardi abil antud digitaalallkirjad. Sellest õiguslikust analüüsist võiks tuletada rea pilootkaasusi, mille lahendamisel tuleb kaasata nii IT-spetsiliste kui ka juriste.

8.1.3 Juriidilise isiku vastutuse määratlemine digitaalallkirja puhul.

Protsesside analüüsil on tuvastatud vajadus asutuse digitaalallkirja järele. Analüüsimist vajab selle mõiste tähendus vastutuse aspektist (mille alusel saab panna juriidilist isikut varalisel või mingil muul viisil digitaalallkirja eest vastutama). Vajadusel ja võimalusel tuleks muuta Digitaalallkirja seadust.

8.1.4 Digitaaldokumentide unifitseeritud klassifikaatori kontseptsioon

Digitaalse dokumendivahetuse eelduseks on asutuste ja ettevõtete poolt väljaantavate digitaalsete dokumentide klassifitseerimine. Teatud eeltööd selles osas on juba tehtud DHP raames, aga see ei puuduta äriühingute poolt vahetatavaid dokumente.

8.2 Vajalikud muudatused õigusaktides.

Digitaalallkirja kasutamisega seotud küsimusi ja korda käsitleb Eesti Vabariigis mitu seadust: Digitaalallkirja seadus, Avaliku teabe seadus, Haldusmenetluse seadus, Andmekogude seadus ning hulk madalamaid õigusakte, sealhulgas Vabariigi Valitsuse määrus "Asjaajamiskorra ühtsed alused" [3]. Vajadus pakutud lahenduse korral õigusaktide muutmiseks nõuab täiendavat analüüsi, sest ilmselt on soovitud tulemusi võimalik saavutada mitmel viisil. Järgnevalt on antud vaid põgusad vihjed

8.2.1 Muudatused seadustes

Kui eeldada, et eelistatakse optimaalset lahendust volitusinfo esitamisel, siis nõuaks **Äriseadustiku** muudatust Riigi- ja kohalike omavalitsuste andmete ning volitusinfo integreerimine Äriregistrisse. Kui otsustatakse Riigi- ja kohalike omavalitsuste andmeid siiski eraldi registrina säilitada, siis äriühingute volitusinfo lisamine nõuab Äriseadustiku muudatust ikkagi. Sama käib ka **Mittetulundusühingute seaduse** ja **Sihtasutuste seaduse** kohta, mis peaksid nõudma ka volitusinfo esitamist vastavas registris.

Digitaalallkirja seaduse muutmine esialgu vajalik ei ole, kuigi kusagil tuleks sätestada automaatselt (registripäringutele) antava digitaalallkirja kasutamine. Arvatavalt võib see kaasa tuua vajaduse muuta **Andmekogude seadust.**

Ilmselt oleks kasulik täpsustada digitaalallkirja nõudeid **Haldusmenetluse seaduses**. Võimalik, et sama puudutab ka teisi menetlusprotsesse reguleerivaid seadusi.

8.2.2 Muudatused madalamates õigusaktides

Olenevalt valitud lähenemisest kuuluvad muutmisele registrite (Äriregistri, Riigi- ja kohalike omavalitsuste registri, Mittetulundusühingute registri, Sihtasutuste registri) pidamist reguleerivad õigusaktid.

Arvatavasti kuuluvad muutmisele ka menetlusprotsessidega seonduvad regulatsioonid. Selliseid õigusakte on väga mitmel tasemel (ministeeriumide, allasutuste, haldusala asutuste).

Digitaalallkirja rakendumisel on arvatavalt vaja muuta ka asutustesiseseid töökorralduslikke regulatsioone.

8.3 Vajalikud pilootprojektid

Erinevaid tehnoloogilisi pilootprojekte on juba tehtud ja tegemisel ning tehnoloogiate osas täiendava piloteerimise vajadust esialgu ette näha ei olegi.

8.3.1 Volituste registri info kontroll X-tee kaudu

Kindlasti vajaks aga piloteerimist volitusinfo kontroll X-tee kaudu siis, kui volituste registreerimise süsteem on juba käivitunud.

8.3.2 ID-kaardi põhine autentimine

ID kaardi pilootkasutus kasutajate autentimiseks mingis käimasolevas projektis (e-Maksuamet, e-riigikassa vms)

8.3.3 Digitaaldokumentidel põhinev vaidlusprotsess

Kasulik oleks läbi mängida ning dokumenteerida üks piloot-vaidlusprotsess, et saada lähtematerjali digitaalallkirja kasutamise protseduurireeglite koostamiseks.

8.4 Standardimine

Digitaalse suhtluse ühtlustamiseks on standardeid igal juhul vaja, selle tegevuse jätkusuutlikkuse tagamiseks **tuleb asutada Eesti digitaalse asjaajamise standardimisega tegelev organisatsioon või volitada selleks tööks mõnd olemasolevat.** Asjaajamise üleviimisel digitaalsetele alustele tuleb standardida järgmised valdkonnad:

- digitaalseks dokumendivahetuseks kasutatavad andmeformaadid, protokollid ja/või tarkvara;
- volitusinfo esitamise viis, rollisertifikaatide profiil;
- digitaalarhiivindus.

8.4.1 Andmeformaadid, profiilid, protokollid

Digitaalallkirja seadus fikseerib digitaalallkirja kasutuselevõtuga seotud tehnilised lahendused:

- sertifikaadi ja nõuded sellele;

- nõuded sertifitseerimisteenuse osutajale;
- nõuded ajatempliteenuse osutajale;
- sertifitseerimise riikliku registri;
- teenuseosutajate kindlustamise ja järelevalve nende üle.

Seaduses on küll kirjas, millised elemendid peavad sertifikaadis sisalduma ja milliseid nõudeid peab rahuldama ajatempel, kuid konkreetset tehnilist lahendust seadus (loomulikult) ei anna. Samas on selge, et asutustevahelise suhtluse tagamiseks tuleb tagada kasutatavate vahendite ühilduvus. Sertifikaadivormingute osas on maailmas valitsevat hetkeolukorda arvestades selge, et kasutusele on mõtet võtta IETFi poolt standardiseeritud X.509v3 sertifikaadid. Samas on X.509 suur ja palju mittekohustuslikke osi sisaldav standard ning sellest on kasutamiseks mõtet fikseerida vaid mingi alamhulk. Osa vajalikust tööst on juba ära tehtud Eesti tulevase ID-kaardi profiili ette valmistades. X.509 sertifikaadistandardit ja ID-kaardi profiili arvestades **tuleb X.509 raamistikus standardida üks konkreetne asutustevaheliseks kasutamiseks mõeldud sertifikaadiprofiil.**

Ajatembelduse osas aga nii head standardid puuduvad. Nagu näitab ka käesolevas dokumendis toodud analüüs, saab hetkel teadaolevatest lahendustest kasutamiseks soovitada vaid linkimispõhist ajatempliteenust. Selleks **tuleb Eestis juurutada linkimispõhise ajatempliteenuse standard**. Kui ISO pikaldane standardimisprotsess liiga aeglaseks osutub, tuleb see võib-olla ka ise välja töötada. See standard peab tegelikult katma ajatembelduse erinevaid tahke: ajatempli enda formaat, vajalik infrastruktuur ning selles infrastruktuuris liikuva info vorming.

Eraldi tähelepanu väärib küsimus, kas ja kuidas tagada dokumentide ja digitaalallkirjade koos kättesaadavus. Välja on pakutud erinevaid tehnilisi lahendusi, põhilistena võib mainida signatuuri lisamist XML-kapslisse või CMS-kapslisse (*Cryptographic Message Syntax*). Mõlemad variandid on avalikud ja standardsed, nii laias maailmas kui Eestis on enam kasutatud ja toetatud CMS-põhist lahendust. Tagamaks signeeritud dokumentidest arusaamist kõigi asutustes kasutatavate rakenduste poolt on otstarbekas **standardida CMS-kapsli kasutamine signatuuri lisamiseks dokumendile.**

8.4.2 Dokumendivormingud

Riigiasutuste vahelises suhtlemises on mõtet kasutusele võtta avatud dokumendivormingud. Kõige perspektiivsem raamstandard selles osas on hetkel XML, millele tuginedes saab kasutatavate dokumentide tüüpe määrata spetsiaalsete definitsioonide (DTD, *Document Type Definition*) abil. Dokumendi tüüp ei määra veel ära tema visuaalset esitust arvutiekraanil või paberil, selle fikseerimiseks läheb lisaks vaja laadilehte (CSS, *Cascading Style Sheet*).

Et tagada asutuste vahel liikuva info ühene arusaadavus kõikjal nii arvutite kui inimeste jaoks, **tuleb standardida kasutatavad DTD-d ja CSS-id ning kehtestada DTD-des kirjeldatud dokumendielementide tähendused.**

Seda standardimisprotsessi tuleb läbi viia samm-sammuliselt. Esimesel etapil tuleb identifitseerida kõige sagedasemad dokumentide tüübid (kiri, seaduseelnõu vms), töötada välja ning standardida vastavad DTD-d ja CSS-id. Kui mõni asutus edaspidi avastab, et tema andmevahetuseks vajalikku dokumenditüüpi pole veel defineeritud, võtab ta ühendust näiteks DHP-ga ning koostöös luuakse uued DTD-d ja CSS-id, mis DHP standardimiseks esitab. Kuna niisugust tööd tuleb teha korduvalt on otstarbekas **kehtestada uute dokumenditüüpide standardimise kord.**

8.4.3 Tarkvara standardimine

Juhul kui asutustevaheline suhtlus hakkab toimuma avatud standardite (nt XMLi) põhjal, ei ole tarkvara standardimise järele otsest vajadust. Iga asutus võib muretseda enda vajadustele ja võimalustele sobiva keskkonna, peaasi et see keskkond toetab kõiki vajalikke formaate.

Samas on asutuste töö kergendamiseks mõistlik koostada nimekiri etalontarkvarast (vabavara puhul koos viidetega allalaadimiskohtadele), mis standarditud vormingutega testitult hakkama saab.

Kui aga dokumendihalduses otsustatakse kinnise standardi kasuks, ei ole tarkvara standardimisele ilmselt alternatiive. Tegelikult saabki kinniseid vorminguid standardida ainult tarkvara kaudu; sel juhul tuleks hoolitseda, et kõik asutused kasutavad sama tarkvara ja soovitavalt ka sama versiooni. Tarkvara versioonide ühtlustamine nõuab igal juhul üsna suuri rahalisi ressursse ja ka organisatsiooniliselt ei saa see kerge olema.

8.5 Sertifitseerimis- ja ajatempliteenused

Minnes üle digitaalsele dokumendihaldusele, on tarvis fikseerida kolme liiki teenuseosutajate teenuste kasutamise kord:

- isikusertifikaatide väljaandja,
- rollisertifikaatide väljaandja,
- ajatempliteenuse osutaja.

Kasutamiseks sobivad isikusertifikaadid antakse välja ID-kaardi projekti raames ja vähemasti esialgu pole otstarbekas selle ülesande lahendamist dubleerida.

Rollisertifikaatide väljaandmise infrastruktuuri aga veel ei ole. Volituste info kättesaadavaks tegemist käsitlevas peatükis nägime, et peale isikusertifikaate välja andva sertifitseerimisteenuse osutaja on tarvis veel ühte riikliku registriga koos töötavat sertifitseerimiskeskust, mida hetkel ei ole. Niisiis **tuleb korraldada rollisertifikaate väljastava sertifitseerimisteenuse loomine.** Kas selle teenuse osutamine saab toimuma registri poolt osutatava teenusena st. hangitakse vastav süsteem või ostetakse selline teenus mingilt teenuseosutajalt, see selgub ilmselt vastava mõlemaid variante lubava riigihanke tulemusena, sest olemasoleva napi lähteinformatsiooni põhjal, ei saa hetkel otsustada, kumb variant majanduslikult kasulikumaks osutub.

Vastavalt Asjaajamiskorra ühtsete aluste määrusele on riigiasutusel õigus valida ajatempliteenuse osutajaks suvaline Sertifitseerimise Riiklikus Registris registreeritud ATO. Hetkel ühtegi ATO-d registreeritud ei ole. Arvestades eespoolmainitud vajadust kehtestada Eestis standardina linkimispõhine ajatembeldus, tuleb ette võtta järgmised sammud:

- **täiustada SRRi tehnilisi võimalusi**
- **kui digitaalallkirja rakendamisajal ei ole tekkinud ühtegi sobivat ATO-d, tuleb tagada ajatempliteenuse olemasolu.**

8.6 Infotehnoloogiliste keskkondade kohandamine

8.6.1 Vastavusse viimine X-tee nõuetega

Automaatsete registripäringute esitamiseks tuleb asutuste infosüsteeme täiendada X-tee XML-RPC päringute esitamise võimalusega. Kuna XML-RPC näol tegu on standardse ning küllalt hästi toetatud protokolliga, siis ei tohiks see süsteemiarendajatele erilisi raskusi luua. Kõik vajalikud spetsifikatsioonid on loodud ja saadaval RISO'st.

Ka tuleb asutusel viia oma turvameetmed vastavusse X-tee nõuetega. Vastavad nõuded ning protseduurid on piisava põhjalikkusega kirjas X-tee dokumentatsioonis. Dokumentatsioon on kättesaadav RISO'st.

8.6.2 Liitumine X-teega

Selleks, et reaalselt X-tee kaudu päringuid esitama hakata peab asutus liituma X-teega. Kui eelmises punktis kirjeldatud sammud on sooritatud on X-teega liitumise protseduur lihtne.

8.6.3 ID-kaardi kasutusvõimaluse tagamine

Ametnike digitaalallkirja andmise vahendina saab kasutada ID-kaardil olevat isikliku võtit. Selleks on vaja varustada ametnike töökohad kiipkaardilugejate ning vajalike draiveritega. Seejuures on oluline, et kasutatavad kiipkaardilugejad ning nende draiverid töötaks koos ID-kaardi ning selle draiveritega. Ainus viis selles veenduda on seda testida. Kuna erinevate omadustega kiipkaardilugejaid, mis sobivad erinevate vajaduste rahuldamiseks, on saadaval küllalt palju, siis oleks mõistlik, et KMA kui ID-kaardi projekti tellija korraldaks ka ID-kaardi testimise erinevate kaardilugejatega erinevatel platvormidel ning publitseeriks nimekirja sobivatest. Alles seejärel on võimalik asuda kaardilugejaid soetama.

8.7 Koolitus

8.7.1 Digitaaldokumentidega seonduv üldine koolitus

Digitaalne dokumendihaldus toob asjaajamises sisse olulisi muudatusi võrreldes seniste reeglitega. Kuna nüansse, mis tehniliselt eristavad paberdokumente digitaalsetest, on palju, on otstarbekas valmistada ette ning viia läbi põhjalik koolitusprogramm. Programm peaks hõlmama vähemalt järgmisi valdkondi:

- digitaaldokumentide omadused ja erinevus tavalistest dokumentidest;
- digitaaldokumentide ja –allkirja kasutamisega seotud ohud;
- digitaalallkirja kasutamisega seotud tehnoloogilised eeldused: sertifikaadid, ajatemplid, tühistamine;

Riigiasutuste lõikes on vajadus sellise koolituse järgi ilmselt erinev, ent selline koolitus-programmi olemasolu on ilmselt vajalik.

8.7.2 Kasutajakoolitus

Kasutajakoolitus hõlmab eeskätt konkreetsete dokumendihaldussüsteemide kasutamist tutvustavat, aga ka X-tee kasutamisega seonduvat koolitust:

- struktureeritud dokumentide moodustamine (XMLi baasil);
- etalontarkvara kasutajakoolitus.
- Infovahetusvõimalused X-tee kaudu

8.7.3 Tarkvaraarendajate koolitus

Tarkvaraarendajate koolituse põhisisuks on kursus süsteemiarendajatele, kuidas oma infosüsteemi X-teega liidestada.

8.8 Tegevuste ajakava

Tabelis on hinnatud vajalike tegevuste võimalikke algus- ja lõpuaegu ning maksumust. Potentsiaalseid tegijaid võib olla mitmeid ja konkreetseid tegijaid on välja pakutud vaid nende tegevuste puhul, mille korral on arvata, et see oleks otstarbekas kiireima tulemuse saamiseks. Kõik hinnangud on esialgsed ja võivad täiendavate uuringute käigus täpsustuda.

Jrk. nr	**Tegevus**	**Algus**	**Lõpp**	**Potentsiaalne tegija**	**Eeldused / sisendid**	**Tulemused /väljundid**	**Ligikaudne hinnang maksumusele**
	Otsused						
A	ID-kaardi digitaalallkirja sertifikaadi kasutusvaldkondade kohta	30.11. 2001.	14.12. 2001.	Töörühm + Juhtrühm	ID-kaardi piiramatu vastutusega digitaalallkirja sertifikaadist tulenevad ohud.	Esialgne töörühma otsus (29.11. koosolekul) oli maandada riskid inimeste teavitamise teel ja võimaluse andmise teel sertifikaadi koheseks peatamiseks ID kaardi kättesaamise hetkest alates. Kui otsustatakse, et probleem vajab täiendavat käsitlust, siis tuleb välja töötada ettepanekud DAS ja/või isikut tõendavate dokumentide seaduse ning ID-kaardi sertifitseerimispoliitika muutmise kohta	
B	Avatud dokumendivormingute kasutamise kohta	30.11. 2001.	14.12. 2001.	Töörühm + Juhtrühm	Avatud ja suletud vormingute eelised ja puudused - st. kas ollakse valmis XML-le üleminekuks?	Õigusakti eelnõu, mis sätestab XML kasutuse	

C	Riigi- ja kohalike omavalitsuste asutuste registri viimine Äriregistri juurde	30.11. 2001.	14.12. 2001.	Töörühm + Juhtrühm	Hõlbustaks oluliselt volitusinfo kättesaadavaks tegemist. Võimalikud ka muud lahendused.	Nii juhul, kui otsustatakse viia Äriregistri juurde või kui täiendatakse olemasolevaid registreid - ettepanekud muudatusteks vastavate andmekogude pidamist reguleerivatesse õigusaktidesse	
D	X-tee registreerimine STO ja ATOna	30.11. 2001.	14.12. 2001.	Töörühm + Juhtrühm		Annab X-tee päringuvastustele digitaalallkirjastatud dokumendi staatuse igas mõttes.	
	Täiendavad uuringud						
1.	Seonduvate õigusaktide analüüs	15.12. 2001.	Jaanuar 2002.		Kui 14.12. arvatakse, et pakutud lahendused on üldiselt vastuvõetavad	Ülevaade muudatusi vajavatest õigusaktidest + uute eelnõud	100 000
2.	Vaidluste menetlemise protsess digitaalallkirja puhul	15.12. 2001.	Jaanuar 2002.			Ülevaade käsitlemata probleemidest ning vajalikest täiendavatest regulatsioonidest	
3.	Juriidilise isiku/andmekogu digitaalallkirja mõiste	15.12. 2001.	Jaanuar 2002		Juriidilise isiku digitaalallkiri kui alias väljendile "juriidilise isiku juhi digitaalallkiri, mida annab automaatne infosüsteem"	Ettepanek, kuidas saaks asutuse või andmekogu digitaalallkirjale anda õiguslikku tähendust	
4.	Digitaaldokumentide klassifitseerimise alused	15.12. 2001.	Jaanuar 2002.	Cybernetica, Riigiarhiiv, DHP	Analoogiliselt paberdokumentidega tuleb tekitada süsteem digitaaldokumentide klassifitseerimi-	Digitaaldokumentide unifitseeritud klassifikaator	

					seks sisu ja vormi järgi.		
	Muudatused õigusaktides						
5.	Muudatused seadustes	Jaanuar 2002	Märts 2002		Lõpetatud uuringud 1 ja 2	Muudatusettepanekud	
6.	Muudatused madalamates õigusaktides	Jaanuar 2002	Märts 2002		Lõpetatud uuringud 1 ja 2	Muudatusettepanekud	
	Pilootprojektid						
7.	Volitusinfo kontroll X-tee kaudu	Jaanuar 2002	Märts 2002	Privador, Cybernetica, volituste register	On realiseeritud volitusinfo register (tegevus 18. ja 19.)	Töötav võimalus saada infot asutuste ja ettevõtete töötajate volituste kohta.	3M (koos tegevustega 18 ja 19)
8.	Digitaaldokumentidel põhinev pilootvaidlus	Aprill 2002	Aprill 2002	Justiitsministeerium + andmeturbe spetsialistid	On fikseeritud dokumenditüübid (tegevus 11.), on teada muudatusettepanekud 5. ja 6.	Dokumenteeritud näitlik digitaaldokumendipõhine menetlusprotsess	
	ID-kaardiga veebis autentimise piloot	Jaanuar 2002	Veebr. 2002		test-ID-kaart ja selle draiverid. STO poolt test-teenus.	Kogemus ID-kaardi kasutamisest autentimisel, töötav veebirakendus	
	Standardimine						
9.	Volitusinfo ja rollisertifikaatide vormingu standardimine	Jaanuar 2002.	Jaanuar 2002.	Privador			50 000
10.	Dokumenditüüpide standardimise kord	Veebr. 2002	Märts 2002		On vastu võetud otsus B osas, on lõpetatud välja töötatud klassifikaator		

					töötatud klassifikaator		
11.	Kasutatavad dokumenditüübid ja laadilehed (DTD, CSS)	Märts 2002	Märts 2002		On vastu võetud otsus B osas, on välja töötatud dokumentide klassifikaator		
11a.	Valideerimis- ja usaldust mittevajava ajatempliteenuse standardi väljatöötamine	Jaanuar 2002	Veebr. 2002	Cybernetica			200 000
12.	Arhiveerimisstandardi väljatöötamine	Dets 2001		Riigiarhiiv, DHP			
	Sertifitseerimis- ja ajatempli teenused						
13.	X-tee teenuste registreerimine SRR-s	Jaanuar 2002	Veebr. 2002	(X-tee Keskus)	X-tee on plaanijärgselt rakendunud	X-tee digitaalallkirjad on täielikult DAS-le vastavad	
14.	Rollisertifikaate väljastava teenuse lisamine volituste registrile	Aprill 2002	Nov 2002	Privador, Cybernetica, volituste register		Kõigil isikutel võimalik esineda huvitatud osapoole rollis.	4M
	Olemasoleva IT keskkonna kohandamine						
15.	Riigiasutuste IT-keskkonna X-tee nõuetele vastavaks tegemine	Dets. 2001.		Riigiasutused			sõltub asutusest. min 20k (riistvara)+ jooksvad kulud. max piirangut pole

16.	Liitumine X-teega	Jaanuar 2002		X-tee Keskus			kui 15 tehtud siis jooksvad kulud
17.	Riigiasutuste IT-keskkonna ID-kaardi kasutamisele vastavaks tegemine	Veebr. 2002.		Riigiasutused	KMA on koostanud testitud kaardilugejate ja platvormide nimekirja.	On kavandatud-hangitud juurutatud ID-kaardi kasutuskeskkond (kaardilugejad + vajalik soft)	sõltub millised kaardilugejad sobivad.
	Olemasolevate tugistruktuuride kohandamine						
18.	Äriregistri andmekoosluse täiendamine ja tarkvara täiendus	Jaan. 2002.		Äriregister, Reaalsüsteemid	On juba vähemalt kavandatud õigusaktid, mis seda lubavad.	Lisafunktsionaalsusega Äriregister, vastavalt modifitseeritud tarkvaralahendus	
19.	Riigiasutuste ja riigiametnike info kättesaadavaks tegemine	Jaan. 2002.		Oleneb otsusest C	On vastu võetud otsus C osas.	Lahendusskeem. Tarkvara projekt + realiseerimine. Ettepanekud muudatusteks õigusaktidesse.	
20.	Arhiveerimise korraldamine	Jaan 2002	Märts 2002	Riigiarhiiv			
	Koolitus						
21.	Seminar IT juhtidele üldistest lahendustest	12.12. 2001.	12.12. 2001.	Cybernetica Privador		Tagasiside pakutud lahenduste osas	
22.	Riigiametnike digitaalse asjaajamise koolitus	Märts 2002.					
23.	XML põhise dokumendihalduse koolitus	Märts. 2002.					

9. Lisa 1: Lühiülevaade riigiasutuste käimasolevatest projektidest

Lühiülevaade digitaalallkirjaga seotud projektidest on koostatud vastavalt Justiits-, Rahandus- ja Siseministeeriumis, Teede- ja Sideministeeriumis, Riigikantseleis ning Majandusministeeriumis 10.10.2001-19.10.2001 läbiviidud ankeetküsitlustele ja intervjuudele.

9.1 Justiitsministeerium ja valitsemisala

9.1.1 Äriregister (linna ja maakohtu registrid)

Projekt algatati 1995. aastal. Arendus on toimunud pidevalt ning praegu on süsteem aktiivselt kasutusel. Projekti eesmärgiks on tagada äriühinguid puudutava informatsiooni kättesaadavus ja kompaktsus. Vastav seadusandlus on selles projektis digitaalallkirja kasutamiseks veel puudulik.

9.1.2 eBüroo / JUHIS

Projektid algatati juunis 2000 ning on suunatud Justiitsministeeriumi ja selle haldusala asjaajamise digitaliseerimiseks.

eBüroo, kui JUHIS'e pilootprojekt, on ette nähtud ministeeriumi enda lahenduseks, JUHIS (JUstiitsHalduse InfoSüsteem) on selle laiendamine ja kohandamine haldusalasse (vanglad, kohtud, prokuratuurid). Projekt on seotud kohtute infosüsteemi ja hiljem ka süsteemiga Persona. Hetkel toimub projekti tehniline dokumenteerimine.

Loogilisteks komponentideks on dokumendi-, grupitöö- ja töövoohaldus. Projekti baasiks on MS Exchange, MS Sharepoint portal Server, MS Office jms. Oluline oleks digitaalallkirja mugav kasutamine nii allkirjastajale, kaasteenistujale kui ka publitseeritult avalikkusele. Süsteemi täielik kasutuselevõtt eeldab digitaalallkirja olemasolu, kuna kõik ametlikult väljuv kirjavahetus peab olema allkirjastatud. Testimise mõttes on vajadus digitaalallkirja järgi kohene. Dokumendihalduse käivitamise hiliseim tähtaeg on 31. märts 2002 (vastavalt AvTS-le).

9.1.3 Persona

Projekt algatati 1999.aastal ning on pidevas arenduses jätkuprojektidena. **Persona** on personaliarvestuse süsteem. Tellijaks/omanikuks on riik, koostööpartneriks/teostajaks AS Cell Network (endine AS Assert). Lähitulevikus peaks analüüsima, kuidas digitaalallkiri võib mõjutada/kasulikuks osutuda (a la väljastatud avaliku võtme lisamine, digitaalselt allkirjastatud dokumentide lisamine, sertifikaadi kasutusvaldkonna/piirangute kirjeldamisvõimalus vastavalt ametikohale jms.).

Süsteem on praegu iseseisev, kuid tulevikus on mõttekas see seostada eBüroo ja lokaalse finantstarkvaraga.

9.1.4 Täitis

Projekt algatati 1997. aastal ning on praegu rakendusjärgus, toimub ettepanekute kogumine täiendavaks arenduseks.

Täitis on oma iseloomult töökorralduslik infosüsteem. Kasutajateks on vabakutselised kohtutäiturid tsiviiltäitemenetluse (võlgade sissenõudmise) protsessis. Eesmärgiks on

hõlbustada kohtutäiturite tööd tohutute andmehulkade haldamisel, samuti on eesmärgiks ministeeriumi järelvalvetegevuse hõlbustamine kohtutäiturite töö üle.

Seotus teiste süsteemidega hetkel puudub, vajalik oleks (pikemas perspektiivis) seostatus Polis'e, ARK, kohtute IS, Rahvastikuregistri, haigekassa, kohtulahendite IS, Vanglas kinni peetavate isikute IS-ga.

Tarkvara on pidevas kasutuses (ettepanekute kogumine parandusteks). Probleemid on seotud andmetervikluse saavutamisega, andmed ei ole 100% usaldusväärsed, lisaks rakenduslikud probleemid ja IS mittevastavus ootustele.

9.1.5 KrimIS

Projekt algatati oktoobris 2001 ning on hetkel planeerimisjärgus.

KrimIS on oma iseloomult töökorralduslik infosüsteem kriminaalhooldajate töö planeerimiseks, kriminaalhoolduse käigus tekkivate dokumentide haldamiseks ning menetlemiseks.

Seotus teiste süsteemidega esialgu puudub, vajalik oleks (pikemas perspektiivis) seotus järgmiste süsteemidega:

Polise, ARK, kohtute IS, Rahvastikuregistri, haigekassa kohtulahendite IS, Vanglas kinni peetavate isikute Isga, samuti seos Kohtute IS-ga (tulevikus üks selle osasid), eBüroo, Juhis.

9.1.6 Kriminaalmenetlusregister

Projekt algatati veebruaris 2001, hetkel toimub tarkvara väljatöötamine. Plaanis on käivitada see alates 2002.a jaanuarist.

Projekti eesmärkideks on:

1. ühendada Eesti Vabariigis alustatud ja lõpetatud kriminaalmenetluste olulised andmed ühtsesse andmebaasi; tagada pidev ülevaade kriminaalmenetlustest;
2. võimaldada menetlejatel saada kuritegude efektiivseks menetlemiseks operatiivset teavet teiste menetletavate kuritegude kohta;
3. tõhustada prokurörijärelevalvet kohtueelse menetluse üle;
4. kergendada statistiliste ülevaadete tegemist kuritegevuse ja kriminaalmenetluste kohta.

Pikemas perspektiivis on eesmärgiks välja arendada kriminaalmenetluse infosüsteem– täisdigitaalne kriminaaltoimik. Otsene seos on projektidega POLIS ja KIS.

9.1.7 Kohtute infosüsteem KIS

Projekt algatati 2001.a sügisel ning planeeritud lõpptähtajaks on seatud 2002. aasta detsember. Hetkel tegeletakse lähteülesande püstitamisega.

Pikemas perspektiivis on projekti eesmärgiks täisdigitaalne kohtumenetlus, kohtute tööprotsesside optimeerimine, kohtute töökoormuse vähendamine tagamaks menetlustähtaegade vähenemist, halduskulude optimeerimine, avalikkuse parem teavitamine. Oluline seos digitaalallkirjaga väljendub võimes vastu võtta kodanike elektroonilisi hagisid/kaebusi jne.

Projekt seostub projektidega eBüroo, Juhis, kriminaalmenetlusregister, kriminaalhoolduse infosüsteem.

9.2 Rahandusministeerium ja valitsemisala

9.2.1 Riigikassa e-teenused

Projekti alustati 2001. aasta jaanuaris ning hetkel on selle arendus lõppjärgus. Projekti tulemusena valminud tarkvarakeskkonnas teostavad riigiasutused läbi veebiliidese makseid ja broneeringuid riigikassasse. Kasutajate autentimine toimub läbi Pankade e-teenuste. Projektiga on seotud piirkondlike riigikassade andmebaasi ja eelarve andmebaasi projektid. Hetkel on testimisel broneeringute moodul ning tavamaksete moodul, valmimas massmaksete moodul.

Projekti informatsioon veebis - http://www.fin.ee/files/abi_kb_aasta.htm

9.2.2 Rahaveeb

Projekti arendustööd on lõpetatud, valminud tarkvarakeskkonnas esitavad kõik riigiasutused raamatupidamise aastaaruandeid läbi veebiliidese. Antud projektiga on seotud riigi raamatupidamise projekt.

Projekti informatsioon veebis - http://www.fin.ee/pages.php/01071304,337

9.2.3 IT Masterplan

Projekti tarkvara juurutamine on lõppjärgus, sisuliselt on tegemist Tarkvara SAP moodulitega: riigi eelarve , riigikassa funktsioonid ning analüüs.

See projekt on olulise tähtsusega kõigi teiste Rahandusministeeriumi IT-projektide jaoks.

9.2.4 Tollideklarant (E-toll)

Projekti tulemuseks on võimalus edastada tollideklaratsioone läbi veebiliidese. Seotud projektiga Asycuda.

9.2.5 E-maksuamet

Projekti alustati jaanuaris 2000 ning hetkel jätkuvad arendustööd.

Projektis valminud keskkonnas saavad kasutajad esitada maksudeklaratsioone, neid autenditakse kas eraldi väljastatud paroolide või Internetipankade vahendusel.

Projekti informatsioon veebis – http://www.ma.ee/ema/

9.3 Riigikantselei ja haldusala

9.3.1 e-Õigus

Projekti alustati septembris 2000, selle I etapp lõppes 26.01.2001 ja II etapp kestab 01.10.2001 – 01.04.2002. Pilootprojekti eesmärgiks on rakendada eelnõude digitaalne kooskõlastamine ja menetlemine; ning välja töötada sellega kaasnev digitaalse asjaajamise õigusliku regulatsiooni eelnõud.

Laiemad eesmärgid:

- Analüüsida süsteemide valmisolekut õigusaktide eelnõude digitaalse kooskõlastamise-le üleminekuks (tehnoloogiline, organisatsiooniline, õiguslik jne); Välja töötada asu-tustevahelise õigusaktide kooskõlastamise infotehnoloogiline arhitektuur (eeldatavad tingimused andmebaasile, funktsionaalsused jne.); Analüüsida projekti tasuvust;

- Luua pilootrakendus kolmele asutusele (näidis).
- Luua kontseptsioon õigusakti infosüsteemile, mis sisaldab õigusakti terviklikku elutsüklit (eelnõu loomine kuni õigusaktide registrisse kandmine ja avalikustamine).
- Koostada õigusaktid ja asjaajamise korra alused, mis on vajalike süsteemi kasutuselevõtuks.
- Välja töötada strateegia kõigi asutuse üleviimiseks ühtsele kooskõlastamisele.
- Võtta kasutusele 12 ministeeriumis

Projekti informatsioon veebis: http://www.just.ee/oldjust/e_oigus/eoigus.html

9.3.2 Digitaalsete tuludeklaratsioonide arhiveerimine

Projekti alustati märtsis 2001 ning planeeritud lõpptähtajaks on märts 2002. Eesmärgiks on digitaalsete tuludeklaratsioonide andmekogu – maksumaksjate registri– elutsükli terviklahenduse pakkumine, mis sisaldab andmekogu ja temaga vahetult kaasneva dokumentatsiooni digitaalset arhiveerimist asutuses.

Projekti teostamisel läbitakse 3 etappi:
1) administratiivanalüüs ning dokumendi elutsükli analüüs;
2) digitaalse arhiivi sisseseadmiseks vajalike põhimõtete ja protseduuride kindlaksmääramine;
3) rakendamine.

Projekti tulemused:
1. asutuse digitaalse arhiveerimise põhimõtete ja protseduuride kehtestamine;
2. praktilise arhiveerimiskogemuse saamine;
3. asutuse digitaalse töökorralduse parandamine nii ametniku, kantselei- /arhiivitöötaja, IT töötaja kui ka asutuse juhtkonna jaoks.

Sügiseks 2001 on saavutatud:

Digitaalallkirja kasutamisest arhiivis on olemas teoreetiline arusaam, kuidas kasutada ja analüüs, millal kasutada.

Probleemid:

1. Vajadus digitaalallkirja arhiivis kasutada on üks lahendustee, kuidas digitaaldokumente arhiivis usaldusväärse ja terviklikuna hoida. Seni on maailmas digitaalallkirja kasutamisel arhiivis praktiseeritud juhul, kui sertifikaate annab riik. Probleem tekib üleandmisel vastuvõtmisel.
2. see on osa üldisest digitaalarhiivindusest; vajab organisatsiooni valmisolekut
3. digitaalallkirjade pikaajaline säilitamine vajab enne arendust uuringuid.
4. paremat reguleerimist kui seni vajavad riigi ja erasektori suhted valdkonnas

9.3.3 e-Riigi Teataja

Projekti alustati märtsis 2001 ning selle lõpptähtajaks on planeeritud september 2002.

Projektiga on seotud projektid VIIS ja e-Õigus ning hetkel on ettevalmistamisel projekti tarkvarahankekonkurss.

9.3.4 e-Maakond

Projekti alustati septembris 2001 ning selle lõpptähtajaks on planeeritud 01.02.2002.

Projekti eesmärgid:

- …et elanik teaks, mis sünnib maavalitsuses
- ...et elanik tunneks oma elu juhtivaid ametnikke
- ...et inimesel oleks võimalik ametnikult aru pärida
- ...et igaühel meist oleks nö siseinfo maakonnaelu kohta: me võiksime näha pooleliolevaid dokumente ja arutlustes kaasa rääkida. Nii ei sünni meie elu puudutavad otsused meile üllatusena.

Projekti informatsioon veebis: http://emaakond.rae.ee/

9.3.5 Dokumendihalduse Programm (DHP)

Projekti alustati 01.02.2000 ning planeeritud lõpukuupäev on 31.12.2002

Projekti eesmärgiks on riigiasutustevahelise digitaalse asjaajamise juurutamine ning lühikirjeldus on toodud aadressil: http://www.riik.ee/dh/ylevaade/vvk_kava1.htm

Seotud projektideks on e-Õigus, VIIS, tuludeklaratsioonide arhiveerimine, jpm.

Sügiseks 2001 on saavutatud järgmised tulemused:

moodustamisel on digitaalse arhiivi töögrupp, sõlmitud Maksuametiga digitaalsete tuludeklaratsioonide arhiveerimise koostöölepe, augusti lõpul toimusid esimesed testkoolitused, valminud on standardiseerimisvaldkonnas dokumendi elementide ja registrites kasutatavate kirjelduselementide soovitusloetelu.

Lisainfo: http://www.riik.ee/dh/varske_info/tegevused_uus.htm

9.4 Siseministeerium ja valitsemisala

9.4.1 Elektrooniline isikutunnistus (ID-kaart)

ID-kaardi projekti (http://id.ee) tulemusena väljastatakse kõigile Eesti residentidele kiipkaartidel põhinevad ID-dokumendid. ID-dokumentide trükkimiseks on hankeleping sõlmitud TRÜB AG-ga (http://www.trueb.ch). Hankekonkursi sertifitseerimisteenuse osutamiseks ja ID-kaartide väljastamiseks võitis AS Sertifitseerimiskeskus (http://www.sk.ee).

Esimene ID-kaart on planeeritud väljastada jaanuaris 2002. ID-kaart hakkab kandma vahendeid (sertifikaate) isiku tuvastamiseks ja digitaalallkirja andmiseks ning on ametlikuks siseriiklikuks isikutunnistuseks.

9.5 Teede ja Sideministeerium ja valitsemisala

9.5.1 Andmekogude ristkasutus (X-tee)

X-tee (http://www.riik.ee/ristmik) on RISO poolt tellitud projekt riiklike andmekogude ristkasutuseks, kus ühe päringuesitaja autentimisvahendina nähakse ka tulevast ID-kaarti. Põhilised X-tee teenuste kasutajad on riigiasutused ja -ametnikud.

Projekti peatöövõtja on AS Cell Network (endine AS Assert), koostööd tehakse Cybernetica AS-i ja teistega firmadega.

Projekti esimene olulisem tähtaeg on 15.12.2001, mil valmib pilootsüsteem.

Selleks ajaks valmivad kodaniku ja ametniku portaalilahendused.

Kasutajate autentimine käib läbi internetipankade. Kodanik saab teha kokku 4 päringut, peamiselt vaadata Rahvastikuregistrist andmeid, muuta mõningaid andmeelemente, saata teateid ning jälgida enda osalust juriidilistes isikutes.

Ametnikule valmib liides

1) kas oma töökohalt (asutuse infosüsteem) või

2) MISP liidesest (turvaline infosüsteemi liides X-teele)

Esialgu realiseeritakse 13 päringut, RR (rahvastikuregister); ÄR (äriregister) ja elektroonilise kinnistusregistri.

Autoriseerimist ehk rollide kontrolli projektis ei toimu, kogu vastutus lasub asutuse infosüsteemis asuval volituste andmebaasil või MISPi puhul lokaalsel volituste skeemil.

9.5.2 e-Kodanik

Projekti alustati oktoobris 2000 ning planeeritud lõpptähtajaks on detsember 2002. Projekti käigus luuakse e-kodaniku keskkond, mis võimaldab kodanikul saada mugavalt teavet riigi poolt pakutavatest teenustest ning oma õigustest ja kohustustest, kasutada vahetuid – ja menetlusteenuseid, olla “aktiivne” kodanik.

Projekti käigus formuleeritakse reeglid kodanikke teenindatavatele infosüsteemidele ning luuakse nende koostööd tagavad üldsüsteemsed vahendid.

Loodava portaali sisu:

- Situatsioonikiht (kodaniku käsiraamat)
- Teenustekiht (tüüpteenused)
- Vahetud teenused (juurdepääs)
- Menetlusteenused (juurdepääs)
- E-demokraatia süsteemid (juurdepääs)
- Kodaniku dokumendihalduse süsteem, e-postkast
- Minu portaal

Projektiga on seotud X-tee ja ID-kaardi projektid.

2000. aastal teostati struktuuri ja sisu kaardistamine, 2001. aastal töötati välja sisu põhimõtted ning hetkel (novembris 2001) on käivitumas hankekonkurss e-kodaniku portaali loomiseks.

Lisainfo: http://www.riik.ee/ekodanik

9.6 Majandusministeerium

9.6.1 Ehitisregister

Projekti alustati juba 1993.aastal ning enamik planeeritud funktsionaalsusest on kavas saavutada 1.03.2002

Ehitisregister sisaldab andmeid ehitatavate ja valmis ehitiste kohta (asukoha andmed ja tehnilised näitajad). Sisestatakse ehitus- või kasutusloa alusel. Ehitus- või kasutusluba antakse taotluse alusel. Taotluseid peab saama esitada digitaalselt.

Projekti lõplik eesmärk on täpsustamisel. Valmimisel on Ehitusseaduse alamastme dokumendid, mis täpsustavad andmete esitamise korra ja koosseisu. Samas kirjeldatakse ehitus- ja kasutusloataotluse esitamise kord.

Lahendamist vajavad ülesanded:

I. Senine eesmärk taotluste vormi nõuete osas on ette näha ka digitaalset formaati.

Kehtestatud nõuded peavad kirjeldama:

a) dokumendi formaadi (tekstidokumendid ning graafilise info esitamine dokumentidele)

b) digitaalallkirja lisamise nõude

II. Lahendamist vajab andmeesitajate autentimine.