

TALLINNA TEHNIKAÜLIKOOL
SÜSTEEMITEHNIKA TEADUSKOND
Automaatika instituut

e-Riigist andmeturbe seisukohalt

Arne Ansper

Väitekiri on esitatud Tallinna Tehnikaülikooli
tehnikateaduste magistri akadeemilise kraadi taotlemiseks

Tallinn 2001

Autorideklaratsioon

Deklareerin, et käesolev väitekirj, mis on minu töö tulemus, on esitatud TTÜ tehnikateaduste magistri akadeemilise kraadi taotlemiseks ja selle alusel ei ole varem teaduskraadi taotletud.

Annotatsioon

Eesti riigi infosüsteemid on seni olnud üksteisest küllaltki eraldatud, mistõttu on nendevaheline andmevahetus olnud aeglane ja väheefektiivne. Riigiasutuste vahelise töökindla ja kiire andmesidevõrgu valmimine on tänaseks kõrvaldanud põhitakistuse infosüsteemide tihendama liitmise teel ning loonud võimaluse kogu riigi asjaajamise kiiremaks ja efektiivsemaks muutmiseks. Selle võimaluse ära kasutamine eeldab andmekogude avamist elektroonilise suhtluse jaoks. Uuendatud, Interneti võimalusi ära kasutavat asjaajamise korda on populaarse tava kohaselt nimetatud e-Riigiks.

Käesoleva töö käigus analüüsitakse andmekogude avamisel tekkivaid turvaprobleeme, lähtudes seejuures olemasolevate seaduste poolt defineeritud süsteemist. Eraldi vaadeldakse ametiasutuste vahelise suhtluse ning kodaniku ja riigi vahelise suhtluse juures tekkivaid probleeme. Analüüsi käigus leitakse, et, tingituna oluliselt erinevatest riskidest ning kasutada olevatest turvameetmetest, ei ole tüüpilise äriettevõtte jaoks väljatöötatud komplekslahendusi demokraatliku riigikorraga riigis võimalik rakendada muutmata kujul. Analüüsi tulemuste põhjal luuakse e-Riigi ühe alusstruktuuri arhitektuuri kajastav mudel, mis võimaldab sobiva juriidilise raamistiku olemasolul saavutada analüüsi algul defineeritud turvaeesmärgid.

Töö tulemuseks oleva turvalise arhitektuuri kandavaks ideeks on tsentraliseerida vaid hädavajalikke teenuseid. Oma iseloomust lähtuvalt peavad tsentraliseeritud olema koordineerimis- ja järelvalvetegevus. Majanduslikest- ning turvakaalutlustest lähtudes on otstarbekas tsentraliseerida ka turvemonitoringu teenus. Detsentraliseeritud arhitektuur suurendab ühelt poolt süsteemi käideldavust, kuna mistahes kahe riigiasutuse vaheline suhtlus sõltub vaid nende asutuste infosüsteemide ning nendevahelise sidekanali toimimisest ning teiselt poolt andmete terviklust ja konfidentsiaalsust, kuna andmed ei läbi kolmandaid infosüsteeme.

Töös nähakse ette kodanikuportaali loomine, mis võimaldab kodanikul riigiga elektrooniliselt suhelda. Keskseks turvaprobleemiks kodanikuportaali loomise juures on kodanike autentimine. Probleemi lahendusena näeb autor Eesti ID-kaardi kasutamist.

Ülesande keerukust ja mitmetahulisust arvestades on käesoleva töö tulemused kasutatavad lähtekohtadena edasise uurimis- ning arendustöö juures.

Sisukord

Sissejuhatus	6
1. Muudatuste lähtekohad	9
1.1 Riik ja firma	9
1.2 e-Kuningriik või e-Vabariik	10
1.3 Riigiarendusprotsessi põhimõtted	11
1.4 Idealistlik ja realistlik lähenemine ümberkorraldustele.....	11
2. Andmekogude avamisel tekkivate probleemide analüüs	13
2.1 Tõendid.....	14
2.2 Elektroonilisi tõendeid kasutav süsteem	15
2.3 Elektrooniliste tõendite vahetamine ametiasutuste vahel.....	18
2.4 Lihtpäringute esitamine andmekogudele.....	19
2.5 Kokkuvõtte esialgsest analüüsist.....	20
3. Asutus – asutus infovahetus	21
3.1 Eeldused.....	21
3.2 Autentimine ja autoriseerimine	22
3.3 Salastatuse tagamine	24
3.4 Terviklus, jälitatavus ning tõestusvääratus.....	25
3.5 Käideldavus	27
3.5.1 Stiihilised ohud.....	27
3.5.2 Elektrikatkestused.....	28
3.5.3 Vandalism	28
3.5.4 Inimvead	28
3.5.5 Ründed.....	28
3.5.6 Kanali ebapiisav läbilaskevõime	28
3.5.7 Sidekatkestused	28

3.5.8	Teenusetõkestusründed.....	29
3.5.9	Käideldavus – kokkuvõte.....	29
3.6	Monitooring	29
3.7	Süsteemide atesteerimine	30
3.8	Analüüsi tulemuste rakendamine eritüübiliste infosüsteemide korral	30
3.8.1	Näide: Sertifitseerimise Riikliku Registri infosüsteemi turvameetmed ..	31
3.8.2	Näide: personaalne turvakeskkond.....	33
3.9	Lahenduste skaleeruvus.....	34
3.10	Järeldused asutus – asutus infovahetuse kohta	34
4.	Asutus – kodanik kasutus	36
4.1	Välise autentija kasutamine	37
4.1.1	Autentimine avaliku võtmega krüptosüsteemide abil	38
4.1.2	Autentimine jagatud saladuste abil.....	38
4.1.3	Volitusmehhanismide lisamine välist autentijat kasutavale skeemile....	39
4.2	Vastavus andmekogude seadusega	41
5.	Arhitektuur	42
5.1	Keskus	43
5.2	Ametiasutuse infosüsteem	44
5.3	Andmekogu.....	44
5.4	Andmekaitse Inspeksioon.....	44
5.5	Portaal.....	44
5.6	Volituste register	45
5.7	Väline autentija	45
5.8	ID-kaardi sertifitseerimisteenuse osutaja	45
	Kokkuvõte	46
	Edasised uurimissuunad.....	46
	Abstract	47
	Viited	48

SISSEJUHATUS

Viimasel aastakümne toimunud arvutite ja sidetehnika tormiline areng on tänaseks loonud täiesti uue ärikeskkonna. E-kommerts on võlusõna, mis tähistab kiiremaid ja odavamaid äriprotsesse, mille mootoriteks on Internet, veeb ning lähiolevikus ja -tulevikus ka avaliku võtme infrastruktuur (PKI). Internetikaubamajad, Internetipangad ja firmadevahelised B2B äri lahendused on uue tehnoloogia mõned eredad rakendusnäited.

Eesti riik ja riigivalitsemine ei ole seni oluliselt selle protsessiga kaasa läinud. Kuid mitmed asjaolud viitavad, et olukord on kiiresti muutumas.

Ühelt poolt ei paista olevat takistusi, miks ei võiks firmade jaoks välja töötatud tehnoloogiaid ja lahendusi rakendada ka riigi tasemel. Näeb ju riik välja nagu üks suur firma, mille eesmärgid, äriprotsessid ja organisatsiooni struktuur on defineeritud seaduste poolt.

Teiselt poolt kasvab riigi kodanike rahulolematus. Inimesi, kes ei käi kuude kaupa pangakontoris, kuid elavad sellest hoolimata vilgast finantselu, häirib riigi vanamoelisus. Iga pisiasja pärast peab ise riigiasutusse kohale minema. Maksab ainult paber. Ja paberi väljastamine võtab aega ja raha. Nad tahaks oma asju mugavalt ja kiirelt, arvuti tagant tõusmata, korda ajada [47].

Kolmandalt poolt näeb muudatuste vajadust ka valitsus [40]. Riigieelarve tasakaalus hoidmiseks peaks valitsemiskulusid kokku hoidma, kuid olemasolevate vahenditega jätkates ei paista selleks enam võimalusi olevat.

Kolmas ja eriti teine asjaolu ei ole omased kõikidele riikidele. Näiteks suhtub enamused USA tarbijaid seni veel kahtlevalt Interneti kaudu äritegemisse, pidades seda liiga ebaturvaliseks [10]. Eestis valitsev soosiv suhtumine Interneti kasutamisse tekitab veel neljandagi muudatusi soosiva asjaolu: piisavalt kiiresti ning radikaalselt riigivalitsemist reformides tekitame palju positiivset ja ligitõmbavat kõmu Eesti ümber (nagu näiteks [21]).

Need asjaolud on juba pikemat aega selged paljudele inimestele ja ideed e-Riigi tulekust on erineva radikaalsusastmega korduvalt väljendatud [33], [34], [16].

Kuigi eesmärk on küllalt selge ja kohalike visionääride poolt korduvalt kaunilt esitatud, ei ole siiani päris selge, millist teed pidi selleni jõuda: on neid, kes arvavad, et kõige tähtsam on Interneti viimine iga inimeseni [25], neid kes leiavad, et esmatähtis on digitaalallkirja kiire kasutuselevõtt [34], kui ka neid, kes loodavad XML-ilt tuge valitseva infotehnoloogilise anarhia korrastamiseks [49].

Maaailmas on mitmeid teadusasutusi (nagu näiteks IBM'i *The Institute for Electronic Government*; Albany Ülikooli *Center for Technology in Government*; Harvardi Ülikooli *John F. Kennedy School of Government*; Manchesteri Ülikooli *Institute for Development Policy and Management*) kes tegelevad e-Riigi (*E-governement*) probleematika uurimisega. Seejuures ei vaadelda e-Riiki mitte kitsalt infotehnoloogilise probleemina, vaid palju laiemalt. Teemale lähenetakse nii filosoofilisest (kas infotehnoloogia intensiivne kasutuselevõtt muudab riigi demokraatlikumaks või mitte), sotsioloogilisest (info lihtne kättesaadavus vaid elektrooniliste kanalite kaudu suurendab veelgi lõhet rikaste ja haritute ning vaeste ja harimatute vahel – nn *digital divide*), kui ka organisatsiooniteoreetilisest (e-Riigi loomine ongi tegelik haldusreform) vaatepunktist.

Arenenud riigid on juba ammu asunud aktiivselt e-Riigi loomise teele. Seatud on konkreetset eesmärgid, loodud vastavat tegevust koordineerivad ja suunavad asutused, mille käsutusse on antud piisavad ressursid. Selles vallas võiks eriti positiivse näitena esile tuua tüüpiliselt konservatiivseks ja vanamoeliseks peetud Suurbritanniat [51], samuti ka USA-d [52].

Eestis on e-Riigi loomist vaadeldud enamasti puhtpraktilisest aspektist ja küllalt kitsalt vaid infotehnoloogilise probleemina. Keskendutud on infrastruktuuri väljaehitamisele: sidekanalite väljaehitamisele ning arvutitöökohtade ja avaliku võtme infrastruktuuri (*PKI*) loomisele. Rahva harimisel on tublit tööd teinud Tiigrihüpe Sihtasutus.

Välismaised uurijad ([53], [54]) on toonud e-Riigi juures välja kolm osaliselt kattuvat valdkonda:

- 1) e-demokraatia;
- 2) e-kodanik;
- 3) e-administratsioon.

e-demokraatia all mõistetakse inimeste vahetut osalemist oluliste otsuste tegemise juures. Visionäärid näevad Internetis demokraatia päästjat ja võimalust inimesi tagasi riigi valitsemise juurde tuua. Selle valdkonna alla kuulub näiteks e-valimiste temaatika. Tegu on neist kolmest kõige keerulisema ja raskemini realiseeritav valdkonnaga.

e-kodaniku (või ka e-teenuste) all mõistetakse kodaniku ja riigi vahelise suhtluse elektrooniliseks muutmist. Praktikas tähendab see portaalide loomist, mille kaudu kodanik saab riigiga andmeid vahetada ning talle vajalike toiminguid teha. See on avalikkusele kõige enam nähtav osa e-Riigist.

e-administratsiooni all mõeldakse riigi sisemiste protsesside efektiivsemaks, odavamaks, kiiremaks ja kontrollitavamaks muutmist kasutades uusi infotehnoloogilisi vahendeid. See osa moodustab vundamendi kahele ülejäänule ning jääb enamasti avalikkuse eest varjule.

Eestis tegeldakse praegu aktiivselt e-administratsiooni [40] ning e-kodaniku [47] süsteemide loomisega. e-demokraatiast küll räägitakse (e-valimised), kuid tehniliselt on see projekt veel ebareaalne [50].

Suurim Eestis käimas olev e-Riigi projekt on Riigi Infosüsteemide Osakonna (RISO) poolt juhitud Riigi andmekogude moderniseerimise programm (X-tee), mille põhieesmärgiks on kehtivate seadustega kooskõlas oleva riigiasutuste ja andmekogude vahelist elektroonilist suhtlust võimaldava lahenduse väljatöötamine ning avalike

teenuste kodanikele kättesaadavaks tegemine Interneti vahendusel. Käesolev töö on alguse saanud just X-tee projekti turvaaspektide uurimisest.

Kuna e-administratsiooni olemasolu on tegelikult eelduseks muude ja silmapaistvamate e-riigi osade realiseerimiseks keskendubki käesolev töö just e-administratsiooniga seonduvate probleemide uurimisele. Eestis on riigi jaoks olulised andmed organiseeritud andmekogudesse, seetõttu uuritakse e-Riigi kontseptsiooni just andmekogude seisukohalt.

Töö esimene osa esitab põhimõtted, millest peaks lähtuma riigi valitsemiskorra muudatuste väljatöötamisel.

Töö põhiosa analüüsib põhjalikumalt üht olulist e-Riigi loomisel tekkivat probleemi: kuidas tagada riigi andmekogudes olevate andmete turvalisus asutuste ning kodanike ja riigi vahelise suhtluse digitaliseerimisel. Analüüsi tulemused on kokku võetud e-Riigi ühe alusstruktuuri arhitektuuri esitavasse mudelisse.

Autor tänab töö valmimisel osutatud abi eest Ahto Buldast ja Monika Oiti.

1. MUUDATUSTE LÄHTEKOHAD

1.1 Riik ja firma

Riik on mõnest küljest vaadatuna küllalt sarnane firmaga. Tal on mingi eesmärk, struktuur, äriprotsessid, eelarve, jne. Mõnest teisest küljest vaadates on aga riigi ning firma tegevuses suuri erinevusi.

Vaatame näiteks milliseid riske tekitab riigi ja firma tegevus kolmandatele osapooltele ning mida saavad need oma riskide maandamiseks ette võtta.

Firma puhul on kolmanda osapoole risk piiratud tema poolt mängu pandud rahaga. Näiteks panga puhul riskib panga klient vaid selle summa ulatuses, mille ta panka pani. Kas läheb pank pankroti või juurutab mingi uudse kuid ebaturvalise lahenduse, mille kaudu ründaja tema pangakonto tühjendab, ikkagi ei teki talle rohkem kahju, kui kontol raha on.

Riigi puhul ei ole kolmanda osapoole risk piiratud. Kui riik võtab oma funktsioonide täitmise hõlbustamiseks kasutusele ebaturvalise lahenduse, võib ründaja "heausksetele" ostjatele kantida nii kodaniku firmad kui ka kinnisvara (vt nt [44]), avaldada tema meditsiinilised andmed, kuulutada ta tagaotsitavaks, eriti ohtlikuks ja relvastatud kurjategijaks, manipuleerida valimistulemusi nii, et võimule tõuseb talle eriti ebasümpaatne äärmusvasak või –parempoolne partei, vms.

Erinev on ka see, mida saab tekkivate riskide maandamiseks ette võtta. Firma puhul võib olukorra halvenemise korral lihtsalt konkurendi teenuseid kasutama hakata. Riigi puhul konkurents puudub. Riigi vahetamine on tegevus, mis valdava enamuse inimeste jaoks on mitmesugustel põhjustel välistatud.

Konkurentsi olemasolu motiveerib firmasid käituma mõistlikult, sunnib neid pingutama seniste klientide säilitamise ja uute juurdevõitmise nimel. Riigi puhul see motivaator puudub.

Erinev on ka see, kuivõrd selgelt kajastuvad organisatsiooni eesmärgid ja nende saavutamiseks valitud strateegia iga struktuuriüksuse tegevuses ning kuivõrd hästi on eri osade tegevus koordineeritud. Firma on enamasti ühtne. Seatud eesmärgid ja nende saavutamise strateegia on kõigi juhtimisotsuste aluseks. Riik on hajutatud. Igal allüksusel on oma eesmärgid ja strateegiad, mis peaksid olema, kuid tihti ei ole kooskõlas teiste omadega.

Ja lõpuks, firma on oluliselt vabam oma tegevuses. Ühelt poolt saab ta oma töötajaid piiramatult motiveerida. Teiselt poolt saab ta vabamalt karistada neid, kes talle vastu

töötavad ja halba teevad. Näiteks võib ründaja kanda musta nimekirja ning teda mitte kunagi teenindada. Suurte ja mõjukate firmade selline käitumine on hästi teada ja pisikeses ühiskonnas on see küllalt distsiplineeriv. Riik seevastu on küllalt piiratud nii oma ametnike motiveerimis-võimaluste kui ka pahategijate karistusvõimaluste osas. Isegi kriminaalkaristused aeguvad.

Vaatame selle nimekirja veelkord üle.

	Riik	Firma
Riskid	Piiramatud	Piiratud
Valikuvõimalus	Puudub	Olemas
Juhtimine	Hajutatud	Ühtne
Mõjutusvahendid	Piiratud	Piiramatud

Kogu see ebaseeldiv jutt on paraku väga oluline, sest on ju andmeturbe lõppeesmärk riskide vähendamine. Selle eesmärgi saavutamiseks teostatakse süsteemi turvamise käigus riskianalüüs, mille tulemusi kõrvutatakse turvameetmete maksumusega ning leitakse optimaalne turvatase, mille korral kogukulud on minimaalsed. Kui arvutuslik risk ületab aktsepteeritava, leitakse, milliseid infovarasid kaitsta, milliste meetmetega. Kaalutakse ka turvakriitilistest, kuid väheolulistest infovaradest loobumist.

Kuna nii riskid, kui ka võimalikud meetmed on riigi ja firma puhul mõneti erinevad, siis ei saa ühe riskianalüüsi tulemusi mehhaaniliselt teisele üle kanda, võttes kasutusele valmisolevaid komplekslahendusi. Loomulikult ei tähenda see seda, et kõik tuleks uuesti ja uut moodi teha. Paljud üksiklahendused sobivad väga hästi kasutada ka riigi kontekstis, juhul kui on selge kuidas ja milleks neid kasutama hakatakse.

1.2 e-Kuningriik või e-Vabariik

Rääkides riigist üldiselt on vajalik ära mainida ka see, millise riigikorraga riigist jutt käib. Käesolevas dokumendis on eeldatud, et tegu on demokraatliku riigiga, kus kehtib muuhulgas ka võimude lahususe printsiip [14].

Paljud eelmises peatükis toodud eeldused ei kehti muu riigikorra puhul. Näiteks kuningriigi või diktatuuri puhul ei ole mõjutusvahendite puudumine või juhtimise hajutatatus probleemid. e-Kuningriigi rajamine oleks ilmselt lihtsam ja odavam kui demokraatliku e-Riigi loomine.

Demokraatliku riigikorra püsimiseks on vajalik vältida võimu liigset kontsentreerumist – paneme tähele, et tänapäeval on võim ennekõike teadmised (*knowledge is power*), tagada teatud funktsioonide lahusolek, luua teatud liiasust, välistamaks kriitiliste tõrkepunktide (*single spot of failure*) teket. Riigi püsimise tagamiseks on aegade jooksul välja kujunenud keerukas õigusaktide rägastik, mis kehtestab mängureeglid, on aluseks bürokraatiale ning toob süsteemi liiasuse.

See on väga oluline punkt. Uus tehnoloogia lubab süsteemi optimeerida, muuta seda kiiremaks ja efektiivsemaks. Aga optimeerimisega peab ettevaatlik olema. Üleoptyimeerimise korral läheb kaduma see hädavajalik liiasus, mis tagab süsteemi stabiilsuse. Kogu bürokraatia ei ole paha. Teatud kogus bürokraatiat on stabiilsuse tagamiseks hädavajalik.

Pöördudes tagasi sissejuhatuses käsitletud turvalahenduste vaimu juurde: on lahendusi, mis toimivad hästi kuningriigis, kuid mitte demokraatlikus riigis. Kuna firmad on oma olemuselt sarnased kuningriigile ei pruugi kõik lahendused, mis töötavad hästi või suurepäraselt firma keskkonnas, olla ülekantavad riigi keskkonda.

1.3 Riigiarendusprotsessi põhimõtted

Süsteemiarendus on juba küllalt vana teadus [22]. Aegade jooksul on proovitud ja uuritud paljusid meetodikaid, tehtud palju ränki vigu (vt nt [5]), mõeldud välja palju kavalaid vahendeid ja paradigmasid soovitud tulemuste efektiivsemaks saavutamiseks. Kõrvale on pandud ka palju lihtsaid tõeteri. Näiteks selline: "Mida varasemas etapis viga tehakse, seda suurem on tema hind" [32].

Ka riik on süsteem ja veel eriti keeruline süsteem, seega kehtivad samad põhimõtted ka riigi arendamise juures. Endiselt on kõige vastutusrikkam, ohtlikum ja käegakatsutavaid tulemusi mitteandev analüüsifaas, kus kogutakse kokku kõikvõimalikud sisendid: vajadused, nõuded, piirangud, põhimõtted, eesmärgid. Analüüsitakse neid, tuletatakse süsteemi kandidaatarhitektuurid, võrreldakse neid ja valitakse lõpuks üks, mida hakatakse edasi arendama, või siis loobutakse kogu projektist kui ebareaalsest.

Riigi arendamise juures on lähtematerjaliks ühelt poolt seadused, teiselt poolt ärakasutamist ootavad uue tehnoloogia pakutavad võimalused, kolmandalt poolt konkreetsete subjektide mured ja lootused. Need moodustavad sisendi analüüsiprotsessi. Analüüsi käigus peaks valmima tulevase e-Riigi mudel. On selge, et olemasolevate seaduste ja tehnoloogiliste lahenduste vahel on vastuolud, mistõttu tuleb mudeli loomisel teha kompromisse ja neid vastuolusid lahendada.

Muudatuste planeerimisel tuleks stabiilsuse säilitamiseks lähtuda võimalikult konservatiivsetest eeldustest. Arvestada tuleb ka seda, et uus tehnoloogia on oma olemuselt kiiresti muutuv, täpselt mõistetav vaid väikesele ringile spetsialistidele ning tõugatud võimsate ärihuvide poolt.

Analüüsigegevus on ühelt poolt tehniline, kuid vähemalt sama palju juriidiline ja poliitiline. Kuna selle lõpptulemus mõjutab meid kõiki, siis peab see protsess olema avalik ja arusaadav ka mittespetsialistidele. Samas peab protsess olema efektiivsuse tagamiseks ning lõpptulemuseni jõudmiseks kindlalt juhitud.

1.4 Idealistlik ja realistlik lähenemine ümberkorraldustele

Proovime defineerida, mida me üldse mõistame e-Riigi all. Milline peaks ja võiks olla muudatuste ulatus? Kuidas neid muudatusi läbi viia?

Idealistliku lähenemise korral kaardistatakse kogu riigi kõik äriprotsessid, luuakse riigi mudel, mudel optimeeritakse teatud määral ning seejärel realiseeritakse mudelile vastav infosüsteem, tehakse vajalikud õigusaktide muudatused ning korraldatakse ümber riigiasutuste töö. Sisuliselt oleks tegu totaalse haldusreformiga, mille tulemuseks oleks kellavärgina töötav riik. See plaan ei ole arvatavasti teostatav. Infotehnoloogilisest vaatepunktist ennekõike tema hirmsuurte mastaapide tõttu. Mingi ettekujutuse vastava mudeli suurusest annaks näiteks see kui kõik eksisteerivad andmekogud kokku võtta ja vaadata erinevate väljade arvu. Saadava mudeli hiiglasuured mõõtmed ei muuda projekti mitte ainult kalliks vaid ka inimesele mitteaaratavaks, ehk siis kaotsi läheb mudeli põhiväärtus: ülevaatlikus. Sellise, enamvähem "suure paugu" meetodil toimiva projekti puuduseks on ka oht uue süsteemi evitusfaasis riiki liigselt destabiliseerida.

Realistlik viis probleemile lähenemiseks oleks selline, kus kõigepealt kirjeldataks ära tüüpilised riigiasutused. Neid tüüpe ei tohiks olla väga palju, nad peaksid üksteisest erinema kindlasti oma suuruse aga ka käideldavate infovarade väärtuse poolest.

Seejärel koostatakse nende tüüpasutuste küllalt detailsed mudelid, mille tegelikkusele vastavust kontrollitakse mingi hulga reaalsete asutuste peal. Valik kasutusstenaariume, mis peavad mudeliga kaetud olema:

- igapäevane töö (kodanikega suhtlemine, otsuste tegemine, aruandlus);
- töö personaliga (töötajate tööle võtmine, ametikohuste muutmine, töölt vabastamine);
- tugitegevused (infosüsteemi hooldus, varundamine);
- eriolukorrad (infosüsteemi taastamine pärast katastroofi, turvaintsidentide käsitlemine, töö olukorras kus *online* süsteemid ei tööta).

Paralleelselt asutuste modelleerimisega toimub ka üleriigilise infrastruktuuri modelleerimine. Kõik need mudelid peavad olema omavahel kooskõlas ja arvestama üksteise poolt pakutavate teenuste ning esitatavate nõudmistega.

Nende mudelite baasil on võimalik välja töötada tüüpmeetmed ja –lahendused teatud korduvate probleemide käsitlemiseks, defineerida süsteemidevahelised liidesed ning määrata kindlaks kasutatavad standardid. Sellise lähenemise heaks näiteks on Saksamaa Infoturbeameti etalonturbe meetod [28].

Seejärel on võimalik alustada paralleelselt valitud mudelile vastava infrastruktuuri ning mõnede seda kasutatavate infosüsteemide loomisega. Väga tõenäoline on, et töö käigus parandatakse ka mudelit ja selle alusel loodud standardeid ning spetsifikatsioone. Kuid on väga tõenäoline, et seda tehakse hiljemgi. Ka sellealase koordineerimisega tuleb vastava projekti plaanimisel arvestada.

Ehkki tegu on väga suure projektiga, mis nõuab väga paljude eri alade spetsialistide ja firmade intensiivset koostööd, on selle läbiviimine autori hinnangul, pädeva arendusmetoodika, pädeva projektijuhtimise ning piisavate ressursside olemasolul siiski mõeldav.

Projekti tulemuseks on rida standardseid klotse või nende detailseid spetsifikatsioone, millest saab kokku laduda koostöövõimelisi infosüsteeme. Turvaaspektist on väga oluline see, et ka kasutatavad turvameetmed on põhjalikult läbi analüüsitud, nende koostoimed teada ning teatud standardse turvataseme saavutamiseks vajalik standardkomplekt olemas.

See lihtsustab oluliselt suure arvu infosüsteemide atesteerimise protseduuri ning annab reaalse võimaluse tõepoolest kõik tuhatkond eksisteerivat riigi infosüsteemi omavahel turvaliselt koos töötama panna.

Nagu eelpool põhjendatud peab infosüsteemide uuendamise projekt olema avalik ning kaasama paljude alade spetsialiste (juristid, infotehnoloogid, jne.). Arvestades ka projekti suurt mahtu, ei ole mõeldav, et käesolev töö käsitleks kõiki ülalmainitud teemasid.

Käesolev töö käsitleb vaid üht probleemi neist paljudest, mis tekivad e-Riigi rajamisel, analüüsides täiendavaid ohte, mis tekivad andmekogudele üldise elektroonilise juurdepääsu andmisel, samuti võimalikke lahendusi nende ohtude realiseerumisvõimaluse minimeerimiseks.

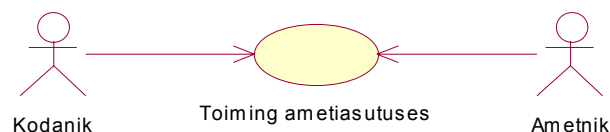
2. ANDMEKOGUDE AVAMISEL TEKKIVATE PROBLEEMIDE ANALÜÜS

Järgneva analüüsi eesmärgiks on jõuda põhimõtteni, millest lähtudes oleks põhimõtteliselt võimalik turvalise e-Riigi loomine. Turvalisuse [20, lk 13] all mõistame antud juhul olukorda, mille puhul meil on õnnestunud parandada andmekogude käideldavust, kahjustamata sealjuures andmete terviklust ja konfidentsiaalsust ning tagades seejuures andmete jälitatavuse.

- Andmete käideldavuse all mõistame nende takistusteta kättesaadavust volitatud kasutajatele.
- Andmete konfidentsiaalsuse all mõistame nende kättesaadavust vaid volitatud kasutajatele.
- Andmete tervikluse all mõistame nende muudetavust vaid volitatud kasutajate poolt.
- Andmete jälitatavuse all mõistame nende muutjate identifitseerimise võimalust.

Probleemi analüüsimiseks on otstarbekas kõigepealt luua analüüsitava süsteemi mudel. Me alustame elementaarse suhtlusakti modelleerimisest ja uurimisest ning liigume seejärel keerulisemate, paljude osapooltega süsteemide juurde.

Andmekogudele elektroonilise juurdepääsu andmise probleemi on võimalik lahendada mitmel, põhimõtteliselt erineval viisil. Erinevate süsteemide erinevusi aitab lihtsamalt mõista väike näide.



Joonis 1. Analüüsiv kasutusstenaarium ja selle osalised

Olgu, et kodanik soovib mingis riigiasutuses sooritada toimingut, mille eelduseks on teise riigiasutuse poolt väljastatud tõendi ettenäitamine (vt joonis 1). Praeguse kehtiva korra kohaselt läheb kodanik kõigepealt teise asutusse ning palub endale väljastada tõendi. Selle väljastamine võib toimuda kohe või võtta aega, võib olla tasuta või nõuda riigilõivu tasumist jne. Kui kodanik lõpuks tõendi kätte saab, võib ta selle viia teise asutusse ning esitada koos oma avaldusega toimingu läbiviimiseks. Vastav elektrooniline süsteem võib töötada mitmel erineval põhimõttel. Mõned näited.

1. Olemasoleva, paberdokumente kasutava süsteemi põhimõtete ülekandmine Interneti keskkonda. Selles süsteemis esitab kodanik elektroonilise päringu teisele riigiasutusele ning saab sellelt elektroonilise tõendi, mille ta võib siis elektrooniliselt esitada esimesele riigiasutusele koos elektroonilise päringuga mingi tegevuse sooritamiseks.
2. Riigiasutuste vahel on olemas otseside, nii et esimene asutus saab esitada päringu otse teise ameti andmebaasi ning saada sealt infot, mis enne liikus läbi toimingut sooritada soovinud kodanikule antud tõendi.
3. Välistatud pole ka muud variandid, nagu näiteks üksikute andmekogude likvideerimine ja neis olnud andmete liitmine ühte kesksesse andmekogusse, mille infosüsteemile on ametnikel juurdepääs turvalise kaugpöörduse vahendite abil.

Järgnevalt on vaadeldud lähemalt ainult esimest ja teist varianti. Ka kolmandas variandis toodud lahendus on tehniliselt täiesti reaalne, kuid kuna selle realiseerimine nõuaks väga suuri muudatusi nii seadusandluses kui ka asutuste töökorralduses, ega lahendaks eraõiguslike asutuste poolt andmekogude pidamise või andmekogudes olevate andmete kasutamise probleemi, siis antud töö piiratud mahu tõttu seda lähemalt ei vaadelda.

Süsteemi analüüsid on tehtud küllalt realistlik eeldus, et säilib ka mitte-elektroonilise suhtluse võimalus ametiasutustega. Samuti on käsitletud eraldi suhtlust, mis leiab aset:

- 1) ametiasutuste vahel ning;
- 2) ametiasutuse ja kodaniku vahel.

Seda põhjusel, et eeldused, mida saab teha kodaniku poolt kasutatava infosüsteemi kohta, on oluliselt erinevad neist, mida saab teha või mida on mõistlik teha ametniku poolt kasutatava infosüsteemi kohta. Nende erinevuste mitteametlik annaks tulemuseks paremal juhul ebaefektiivse ja halvemal juhul ebaturvalise süsteemi. Eeldatud on ka, et ametnikul on olemas oma tööülesannete täitmist võimaldav infosüsteem. Käesolevas töös mõistetakse infosüsteemi all riist- ja tarkvarast koosnevat tervikut, mis on võimeline võrdväärselt suhtlema teiste infosüsteemidega.

2.1 Tõendid

Järgnevalt tuleb palju juttu tõenditest. Mitmel korral on vastandatud tõendeid ja lihtpäringu tulemusi.

Erinevuseks tõendi ja lihtpäringu tulemuse (edaspidi lihtpäringu) vahel on defineeritud tõestusväärtuse olemaolu. Tõendi väljastajal ei ole pärast tõendi väljastamist mingit kontrolli tõendi kehtivuse üle. Tõendi saaja saab igal ajahetkel tõestada, kes tõendi välja andis ning milline oli tõendi sisu väljaandmise hetkel. Lihtpäringute vastustel selline omadus puudub, st. päringuvastuse loojal on igal ajahetkel võimalus eitada (salata) vastava vastuse andmist.

Lihtsaim võimalus elektrooniliste tõendite realiseerimiseks on digitaalallkirja mehhanismide [19, lk 217] kasutamine hästi defineeritud struktuuri ja tähendusega dokumentide allkirjastamiseks. Tõestusväärtuse olemasolu on oluline eri subjektide vahelise suhtluse juures tekkida võivate hilisemate vaidluste objektiivsemaks lahendamiseks.

2.2 Elektroonilisi tõendeid kasutav süsteem

Käesolev peatükk kirjeldab lähemalt, kuidas toimub toimingu sooritamise elektrooniliste tõendite kasutamise korral.

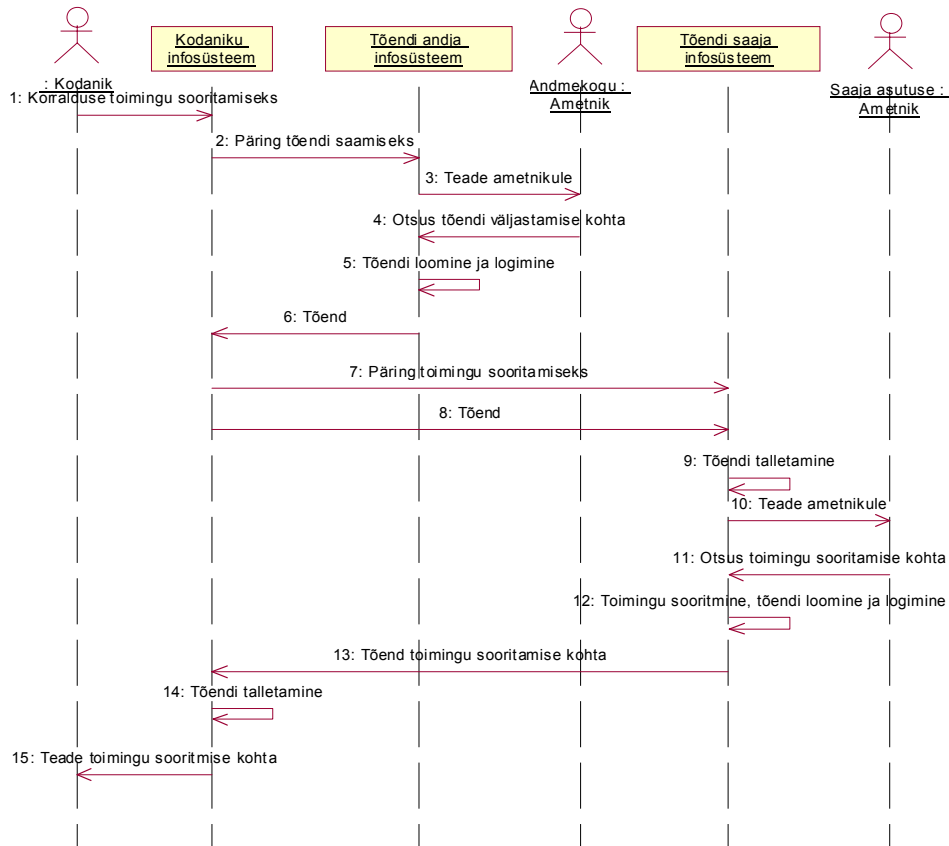
Kasutusstenaariumis (vt joonis 2) osaleb kolm tegelast:

- mingit tegevust sooritada sooviv kodanik;
- andmekogu haldava asutuse ametnik;
- toimingut sooritava ametiasutuse ametnik.

Kõigil neil on kasutada infosüsteem, mille abil nad üksteisega suhtlevad.

Teine ametnik ei saa enne toimingut sooritada, kui pole saanud andmekogust tõendit. Kui kodanik esitab oma infosüsteemile päringu tegevuse sooritamiseks, pöördub see kõigepealt andmekogu haldava asutuse poole ning esitab päringu tõendi saamiseks. Ametnikku informeeritakse tõendipäringust, ametnik teeb otsuse tõendi väljastamise kohta, süsteem loob tõendi, registreerib selle väljastamise fakti ning saadab tõendi kodanikule.

Kodaniku infosüsteem esitab nüüd päringu teisele ametiasutusele, saates koos päringuga kaasa ka esimest asutusest saadud tõendi. Teise asutuse ametniku infosüsteem annab teada saabunud päringust. Ametnik vaatab päringu läbi ning teeb otsuse. Positiivse otsuse korral sooritab infosüsteem soovitud toimingut, registreerib selle toimumise fakti, loob tõendi, mis kinnitab tegevuse toimumist ja tagastab selle kodaniku infosüsteemile, mis talletab selle tõendi hilisemate dispuutide tarvis ning annab kodanikule teada päringu edukast sooritamisest.



Joonis 2. Kasutusstenaariumi kirjeldus elektrooniliste tõendite kasutamise korral

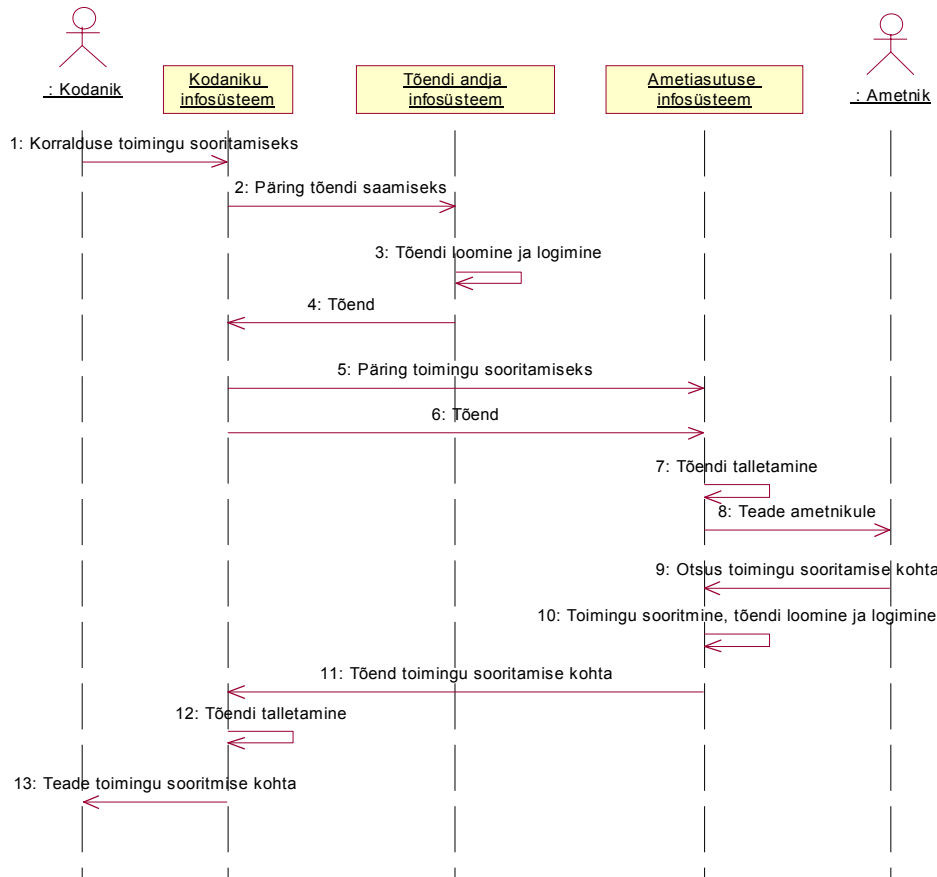
See skeem vastab üks-ühele olemasolevale, paberdokumente ja ametiasutustesse füüsilist kohaleilmumist kasutavale süsteemile, seetõttu ei tohiks selle kasutuselevõtu juures tekkida mingeid vastuolusid olemasolevate seadustega, välja arvatud juhul, kui päringute sooritamine on lubatud vaid paberkandjate kaudu.

Selle skeemi juures on kaks silmatorkavat asjaolu.

1. Mõlemad suhtlusaktid on tegelikult täpselt ühesugused. Kui vaadelda 8. sõnumiga edastatavat tõendit kui 7. sõnumiga edastatud päringu üht parameetrit, siis on sammud 2.-6. ja 7.-13. täpselt samad. Seega piisab, kui analüüsida vaid üht neist.
2. Andmekogu ametnik ei tee absoluutselt mitte mingit sisulist tööd. Praeguse süsteemi korral on ametniku ülesandeks kodaniku isiku kontrollimine (näiteks passi alusel) ning tõendi vormistamine, registreerimine ja väljastamine. Elektroonilise süsteemi korral on nii vormistamine, registreerimine kui ka väljastamine automatiseeritud. Ka kasutaja õiguste kontroll toimub täielikult arvutite abil. Seega ei jää andmekogu ametnikule enam mitte ühtki ülesannet ja ta võib sellest kasutusstenaariumist kõrvaldada. Juhul, kui näiteks päringu enda sisu vajab kontrollimist ning seda kontrolli ei ole mingil põhjusel võimalik automatiseerida, siis ei ole loomulikult võimalik ametnikuta hakkama saada.

Kas ka teise ametiasutuse ametniku saab samal viisil kõrvaldada? Mitte alati. Toimingute korral, kus sisuline otsustusvajadus puudub, võib kogu tegevuse tõepoolest automatiseerida. Toimingute korral, kus ametnik peab ka mingi (subjektiivse) otsuse

vastu võtma, teda kõrvaldada ei saa. Järgnevas analüüsis (vt joonis 3) vaadeldakse seetõttu täielikkuse huvides keerulisemat süsteemi, mis sisaldab ka ametnikku.



Joonis 3. Lihtsustatud kasutusstsenariumi kirjeldus elektrooniliste tõendite kasutamise korral

See mudel ei pruugi enam täiesti täpselt kehtivate õigusaktidega kooskõlas olla. Samas on mõttetu hoida töö ametnikku vaid sellepärast, et ta puhtalt oma olemasoluga täidaks seaduse nõudeid. Juhul kui tõendite automaatne väljastamine läheb vastuollu seadustega, tuleks seadusi vastavalt muuta.

Ülalkirjeldatud skeemide suur eelis kõigi järgnevate ees on see, et ühelegi ametnikule pole vaja anda suuremaid volitusi kui neil praegu on. Süsteemi saab üles ehitada nii, et ametnik ei saa omal initsiatiivil kellegi kohta päringut teha. Küll aga saab kodanik soovi korral endale vajaliku tõendi võtta ning selle siis ametnikule esitada.

Skeemi põhiline puudus on see, et ta ei aita kaasa mitteelektronilise suhtluse efektiivsemaks muutmisele. Kui kodanik tuleb ise ametniku juurde ja soovib sooritada toimingut, mis vajaks tõendit teisest asutusest, ei ole ametnikul õigust seda tõendit küsida. Sellise õiguse olemasolu korral oleks tegu järgmise skeemiga (vt joonis 4), kus tõendid liiguvad otse ametiasutuste vahel. Seega kaoks täpne kooskõla seadustega ning ametnike volitusi peaks suurendama.

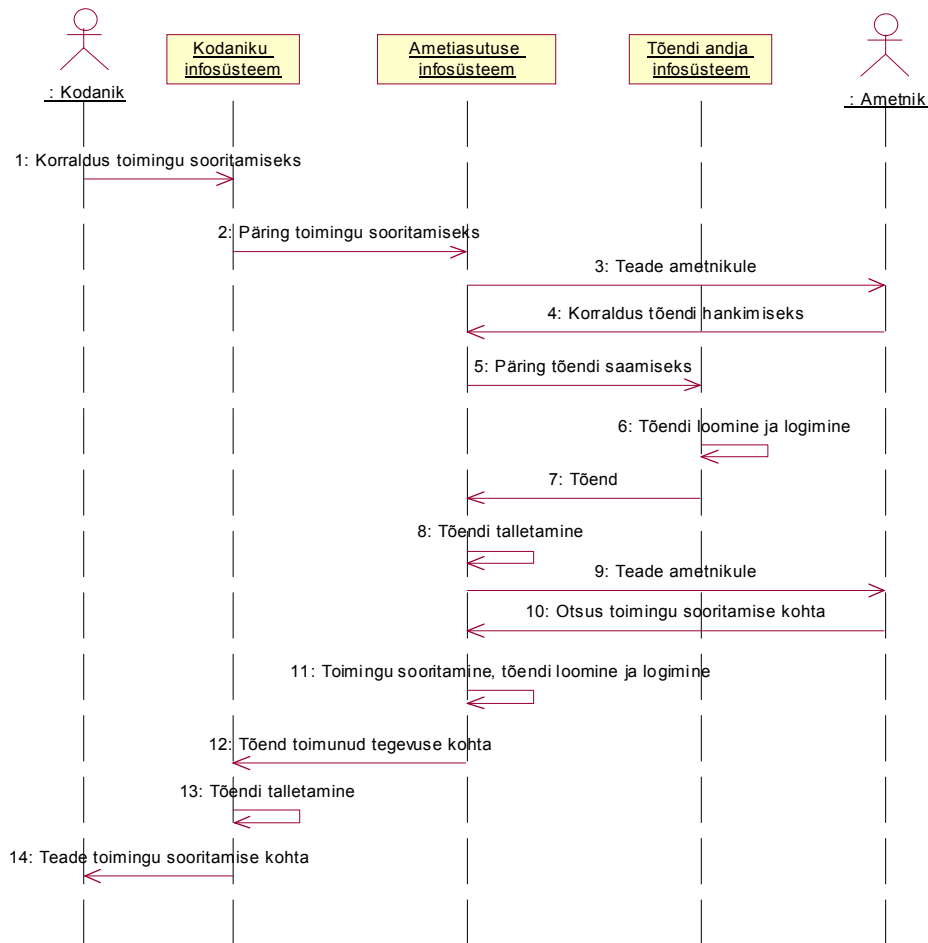
Samuti vajavad täiendavalt käsitlemist juhud, kus ametnikud saavad ilma kodanikuga koostöötaja tema kohta teiselt asutuselt andmeid. Sellise funktsionaalsuse saaks

realiseerida mõnega järgnevatest skeemidest, kuid sel juhul poleks enam mõtet viimatikirjeldatud süsteemi rakendada.

Muudest aspektidest, mida ei saa otseselt puudusteks ega eelisteks lugeda, tuleb märkida seda, et ülalkirjeldatud mudeli realiseerimiseks peavad mõlema asutuse infosüsteemid toetama digitaalallkirja andmist ja kontrollimist (et väljastada ja vastu võtta tõendeid). Kliendi infosüsteem võiks toetada digitaalallkirja andmist ja kontrollimist. See hõlbustaks oluliselt tõendeid väljastavate süsteemide loomist.

2.3 Elektrooniliste tõendite vahetamine ametiasutuste vahel

Variant, kus vajalikku tõendit ei küsi mitte kodanik ise, vaid tema poolt nõutud toimingut sooritav ametiasutus (vt joonis 4).



Joonis 4. Kasutusstenaariumi kirjeldus ametiasutuste vahelise otsese elektrooniliste tõendite vahetamise korral

Kodanik annab oma infosüsteemile korralduse toingu tegemiseks. Infosüsteem esitab päringu ametiasutuse infosüsteemile.

Ametiasutuse infosüsteem informeerib ametnikku saabunud päringust. Ametnik annab korralduse tõendi hankimiseks. Infosüsteem pöörduv andmekogu poole ning esitab

päringu. Andmekogu registreerib päringu, loob tõendi ning tagastab selle. Infosüsteem informeerib ametnikku tõendi saabumisest. Ametnik teeb otsuse, mille peale infosüsteem otsuse täide viib, selle registreerib, tõendi moodustab ja kodaniku infosüsteemile tagastab. Kodaniku infosüsteem salvestab tõendi ning informeerib kodanikku toimingu edukast sooritamisest.

Ametnikud saavad oma tööks vajamineva info, mille nad enne said kodanike poolt esitatud dokumentidest, nüüd kätte otse vastavast andmekogust. Kodanikul ei ole enam otsesest kontrolli selle protsessi üle. Ühelt poolt eeldab see, et *ametnikud peavad saama õiguse esitada suvalisi päringuid oma ametikohustuste piires*, mis aga ei pruugi mahtuda kehtiva õiguse raamidesse. Teiselt poolt aga *antakse ametnikule täiendav võimalus oma volituste kuritarvitamiseks ning ta võib esitada ametikohustuste täitmiseks mittevajalikke päringuid* ja kasutada nii viisi saadud infot ära oma huvides.

Pahatahtlike päringute esitamise võib muuta küll ebamugavaks, projekteerides ametniku infosüsteemi nii, et see võimaldab teha vaid asjakohaseid päringuid, kuid teatav risk siiski jääb. Selle vähendamiseks tuleks luua kuritarvituste tuvastamise mehhanismid, samuti tuleks ette näha võimalus ametnikku sellisel juhul karistada. Kuritarvituste tuvastamine eeldab, et ametniku poolt kasutatav infosüsteem salvestab konkreetse päringu esitamise fakti nii, et ametnikul puudub võimalus selle kustutamiseks või muutmiseks. Loomulikult peab sedasorti meetmete kasutamise fakt ametnikule algusest peale teada olema: see mõjub distsiplineerivalt.

Kasutatavatest meetmetest hoolimata ei ole siiski võimalik algolekut taastada, s.t. ebaseaduslikult välja antud infot "pudelsisse tagasi toppida".

Antud skeemi eelis on see, et oluliselt lihtsustub kodaniku infosüsteem, mis, arvestades nende infosüsteemide suurt arvu, on oluline võit.

Teiselt poolt on sama süsteemi abil võimalik korraldada ka ametiasutusse kohapeale ilmuvate kodanike kiiret teenindamist, sest ametnik saab vajaliku tõendi hankida Interneti kaudu.

Samas saab seda süsteemi kasutada ka andmete vahetamiseks ilma kodanikuga koostööta.

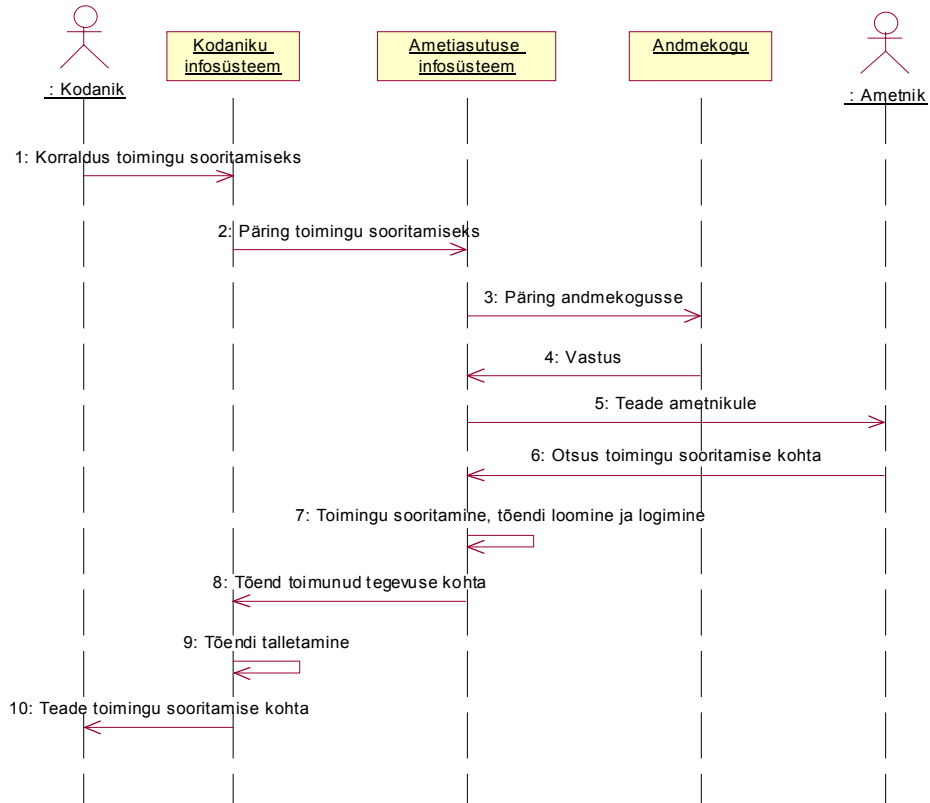
2.4 Lihtpäringute esitamine andmekogudele

Skeem (vt joonis 5) on üldjoontes samasugune kui eelmine, kuid selle vahega, et tehnilise lihtsuse huvides on loobutud tõendite vahetamisest ametiasutuste vahel ning piirduakse lihtpäringute esitamisega.

Võrreldes eelmise lahendusega puudub võimalus tõestada:

- kas mingi ametiasutus esitas teisele mingi päringu või mitte;
- kas ta sai vastuse või mitte;
- ega ka mitte seda, mis andmeid vastus sisaldas.

Juhul kui esitati mingi alusetu päring, mis võis põhjustada reaalselt kahju, on hilisemal uurimisel väga raske välja selgitada tegelikku süüdlast, sest sõltuvalt andmete andja ja saaja infosüsteemide turvalisusest on ametnikel kas iseseisvalt või sobingus oma süsteemiadministraatoriga võimalik kustutada ja/või võltsida töö käigus tekkida võivaid logisid ning sedaviisi oluliselt raskendada juhtumi uurimist.



Joonis 5. Kasutusstsenariumi kirjeldus otsepäringute tegemise korral

2.5 Kokkuvõtte esialgsest analüüsist

Arvestades, et kuna:

- ainult elektroonilisi tõendeid kasutava süsteemi loomisel ei ole võimalik lahendada kõiki kasutusjuhte ning;
- lihtpäringuid kasutava süsteemi korral ei ole kuritarvituste esinemisel võimalik tõenäoliselt objektiivsete asjaolude alusel süüdlast välja selgitada;

siis on otstarbekas kasutada tõendite otsevahetuse mudelil baseeruvat lahendust.

Järgnevates peatükkides on keskendunud tõendite otsevahetuse mudeli täpsemale analüüsile.

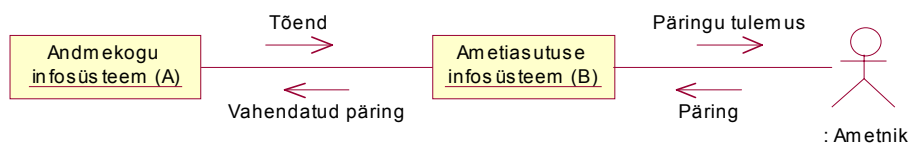
3. ASUTUS – ASUTUS INFOVAHETUS

Nagu sissejuhatavas osas mainitud, on ametiasutuste vahelist ning ametiasutuse ja kodaniku vahelist suhtlust käsitletud algul eraldi. Saadud tulemused on üldistatud ning ühte mudelisse liidetud analüüsi lõpuosas.

Analüüsi juures ei ole eeldatud, et "asutus" ja "andmekogu" peaksid olema tingimata riigiasutused. Tegu võib olla ka näiteks eraõigusliku ettevõttega. Analüüsi juures on oluline vaid see, et:

- tal oleks õiguslik alus soovitud andmeid saada ning;
- tema infosüsteem oleks atesteeritud.

Lihtsaimal juhul võtavad andmevahetusest osa kaks asutust (vt joonis 6). Ühe (andmeandja *A*) hallata on andmekogu ja teine (andmesaaja *B*) peab andmekogus hoitavate andmetega tööd tegema, s.t. andmekogu kuidagi kasutama. Analüüsi käigus vaadeldakse, millised on kasutusstsenariumid ning milliste ohtudega tuleb sealjuures arvestada. Unustada ei tohi ka väliseid tegureid, mis seda suhtlust mõjutavad – õigusaktid, head tavad, kasutajate teadlikkus jm., kuid neid antud hetkel ei vaadelda, s.t. eeldatakse, et teadlikkust tõstev ja häid tavasid selgitav alusdokument on olemas, ning et andmekogusse ligipääsu load antakse selle dokumendi alusel.



Joonis 6. Ametiasutuste vahelise andmekogude kasutuse lihtsaim juht

3.1 Eeldused

Esimene eeldus on see, et ametiasutus omab infosüsteemi (antud töö tähenduses), mis võimaldab ametnikul oma tööd teha. Infosüsteemi täpne realisatsioon pole oluline, küll aga on tehtud paar eeldust süsteemi funktsionaalsuse kohta.

Ametiasutuse infosüsteem eristab kasutajaid, mis praktikas tähendab seda, et infosüsteemi kasutamiseks peab ametnik sellesse sisse logima. Logimise tehnilised detailid pole siinjuures olulised. See võib olla seotud oma tööjaama logimisega (*Single-Sign On* lahendused [46]), paroolipõhise autentimisega, või elektrooniliste

lubade (*Authentication token*) abil, kasutades digitaalsignatuuri mehhanismi [19, lk 217], või olla realiseeritud hoopis füüsiliste pääsukontrollide abil.

Mistahes infosüsteemis, mille abil või vahendusel sooritatud tegevustel on tähendus väljaspool infosüsteemi, on kasutajate eristamise omadus vajalik selleks, et säiliks kasvõi teoreetiline võimalus potentsiaalsete vaidluste objektiivseks lahendamiseks ja võimalike kuritarvituste korral tegeliku süüdlase väljaselgitamiseks. Siinkohal tuleb märkida, et kasutajate eristamine on küll tarvilik, ent mitte veel piisav eeldus vaidluste objektiivseks lahendamiseks.

Teine eeldus on see, et kasutaja saab infosüsteemi sisse loginuna sooritada kõiki toiminguid, mis on vajalikud tema ametikohustuste täitmiseks. Praktikast tähendab see, et kasutajal on mingid õigused, mis tulenevad tema ametjuhendist ja teistest sarnastest dokumentidest. Nendes dokumentides kirjeldatud õigused on esitatud mingil masintöödeldaval kujul infosüsteemis. Õiguste seadmise eest vastutab ametiasutuse süsteemiülem (administraatori) rollis olija. Rollid määratakse asutuse juhataja või osakonnajuhataja (jällegi rollinimetused, mis olenevad vastutuse jaotusest asutuses) korraldusega. Õiguste süsteem võib olla realiseeritud mitmeti. Näiteks võivad õigused olla seotud mingi rolliga või kasutajate grupiga. Näiteks Windows NT's on rollid *Backup operators*, *Printer operators* jne. Ametiasutuses võivad näiteks olla rollid: klienditeenindaja, osakonnajuhataja jne. Iga kasutaja kas saab oma õigused kaudselt, oma rolli kaudu, või siis otse ja personaalselt.

3.2 Autentimine ja autoriseerimine

Kui ametiasutus vajab oma tööks andmeid välisest andmekogust, ei saa ta neid niisama küsima minna. Kokkuleppeid võõra andmekogu kasutamiseks ei saa sõlmida ka süsteemiülemate (administraatorite) ega süsteemiarendajate tasemel. Kuna vastutus andmekogu kasutamise eest lasub andmekogu haldava asutuse juhil ning andmeid kasutama hakkava asutuse nimel siduvaid kohustusi saab võtta vaid selle asutuse juht, tuleb kokkulepe sõlmida just nende poolt.

Asutustevaheline info- või andmevahetuse kokkuleppe sätestab, millistel tingimustel üks asutus teisele oma andmekogus hoitavatele andmetele juurdepääsu annab. Kokkulepe sätestab kindlasti mitmesugused tehnilised detailid, kuid kõige olulisem on see, et andmeid tarbiva asutuse juht võtab endale vastutuse talle antud andmetega hoolsa ümberkäimise ja nende sihipärase kasutamise eest. Kokkulepe ei pea kindlaks määrama, milline andmeid kasutava asutuse töötaja võib milliseid päringuid teha. See ei ole andmekogu haldava asutuse jaoks oluline: pärast kokkuleppe sõlmimist vastab andmekogu kõigile teisest asutusest tulnud lepingukohastele päringutele. Töötajate kaupa piirangute seadmine on andmeid kasutava asutuse ülesanne. Selle ülesande täitmist peab toetama andmeid kasutava asutuse infosüsteem. Kasutajate eristamine ning nende õiguste määramine on olulised funktsioonid selle eesmärgi täitmiseks.

Võib lihtsalt näidata, miks teise asutuse töötajate (isiku täpsusega) autentimine ja nende volituste kontroll andmeandja andmekogu juures ei oma mõtet.

Ametnik kasutab oma tööülesannete täitmiseks, mille hulka kuulub ka andmekogusse päringute esitamine, oma asutuse infosüsteemi. Kõik tegevused, kaasa arvatud võimalik autentimine andmekogu juures, käivad läbi tema asutuse infosüsteemi. Kõigi nende tegevuste turvalisus sõltub otseselt infosüsteemi turvalisusest. Kui keegi on volitatult süsteemi muutnud, paigaldanud võrguliikluse jälgimise vahendid, klaviatuurivajutuste

märkamatu registreerimisega tegeleva programmi, Trooja hobuse vms., saab ta märkamatu teadmisega kasutaja õigustes ilma kasutaja teadmata.

Teiselt poolt ei ole kasutaja jaoks enamasti selge, milliseid päringuid esitab tema kohalik infosüsteem tema esitatud päringule vastamiseks teistele andmekogudele. Ta peab oma infosüsteemi tahes-tahtmata usaldama.

Kuna andmekogu juures toimuva autentimise turvalisus (õigus) sõltub otseselt andmekogu kasutava asutuse infosüsteemi turvalisusest ja ei saa kuidagi kõrgema turvasemega kui on asutuse infosüsteem, siis ei anna see autentimine süsteemi turvalisusele midagi juurde. Kui asutuse infosüsteem on terviklik ja muutmata, siis registreerib ta adekvaatselt (muidu ei saaks ta akrediteeringut), milline kasutaja päringu sooritas. Kui aga asutuse infosüsteem on kompromiteeritud ja kasutab ebaseaduslike ja asjassepuutumate päringute esitamiseks mõne süütu kasutaja nime, siis jääb ka andmekogu logisse vale kasutajanimi, millest ei ole mingit abi tegeliku süüdlase väljaselgitamisel.

Võib koguni näidata, et autentimine otse andmekogu juures muudab süsteemi isegi ebaturvalisemaks. Nimelt muutub kasutajate ning nende õiguste haldus palju raskemaks. Kasutajate halduse juures vajavad käsitlemist vähemalt järgmised juhud:

- 1) uue töötaja tööletulek;
- 2) töötaja lahkumine töölt;
- 3) töötaja ametikohustuse muutumine.

Need on kõik asutusesisesed sündmused. Kui neid peab hakkama koordineerima asutuste vaheliselt, tekitab see mitmeid probleeme:

1. Töötaja lahkumisel või tema ametikohustuste muutumisel ei pruugita sellest kohe informeerida andmekogu omanikku, mis tekitab meile kohustusi mitteomava subjekti, kellel on samas võimalus andmekogule ligi saada. [29]
2. Kuna teise asutuse töötajate autentimine on alati seotud asutustevahelise suhtlusega, võib pikas perspektiivis kujuneda välja ebaturvaline kasutajate haldamise praktika (näiteks telefonitsi), mis pakub mitmeid võimalusi "*social engineering*" – tehnikate rakendamiseks. [1]

Kolmas argument ametniku kahekordse autentimise (eraldi kohaliku infosüsteemi ning andmekogu infosüsteemi juures) vastu on see, et suureneb mingi tegevuse sooritamiseks vajalike autentimisprotseduuride arv. Pärast kohaliku infosüsteemi sisselogimist peaks autenditav ametnik sisestama täiendavaid parooli vms. pääsutõendeid kui ta soovib sooritada päringut. Viimane vähendab süsteemi käideldavust ja soodustab paroolide lohakat hoidmist ja seetõttu ka paroolide lühikest eluiga.

Seetõttu on mõistlik rakendada kahetasemelist autentimissüsteemi, kus:

1. Ametnikud autendivad end lokaalselt oma asutuse infosüsteemile mistahes meetodil, mida on lihtne antud infosüsteemis realiseerida ning mis välistab piisava kindlusega võõra nime all süsteemi kasutamise ("piisav kindlus" määratletakse näiteks mingite üldiste õigusaktidega, millele vastavust nõutakse süsteemi tarnijailt ning millele vastavust kontrollitakse süsteemi auditeerimisel või atesteerimisel). Asutuse infosüsteem teostab ka volituste kontrolli ning lubab ametnikul esitada vaid neid päringuid, milleks tal on seaduslik õigus ning mis on vajalikud tema tööülesannete täitmiseks (need on üksteist täiendavad nõuded).

2. Infosüsteemid autendivad end üksteisele standardiseeritud viisil. Vastav autentimisviis tuleb välja töötada ja standardida koos muu infosüsteemide koostööd võimaldava süsteemiga. Ka sel tasemel toimub päringu esitaja volituste kontroll. Päringu esitajaks on aga antud juhul asutus, mitte ametnik ning kontrolli teostatakse lähtuvalt asutuste vahel sõlmitud infovahetuse kokkuleppest. See kokkulepe sätestab milliseid andmeid asutus andmekogust saada võib. Andmekogu infosüsteem kontrollib iga päringu korral selle vastavust lepingule.

Samas ei ole välistatud, et mitmesuguste õigusaktidega kooskõlas olemiseks ja tõestusmaterjali tekitamiseks edastab päringut tegev infosüsteem andmekogu infosüsteemile päringut tegeva ametniku nime või isikukoodi. Selline tegevus ei ole aga kindlasti käsitletav autentimisena. [20, lk 100]

Veel üks kahetasemelise autentimisega süsteemi eelis seisneb selles, et ametnik saab oma tööülesannete täitmiseks vajalikke päringuid teha vaid läbi oma asutuse infosüsteemi, mis on adekvaatselt turvatud ja kaitstud ning mis registreerib tema tegevusi. Juhul kui päringud toimuksid läbi ametniku koduarvuti või avaliku Internetipunkti, puuduks asutusel igasugune kontroll kasutatava infosüsteemi omaduste üle. Ennekõike peitub oht mitmesugustes viirustes ja trooja hobustes, mille olemasolu või puudumist ei ole ametnik reeglina võimeline hindama. [35] Nende arvutite füüsiline kaitstud on reeglina ebapiisav või hoopis olematu, mis muudab ohu veelgi suuremaks.

Kui võimalus kaugtöökõõ võõrastest arvutitest (või ka oma sülearvutist) on hädavajalik, siis tuleb see korraldada, järgides häid tavasid: asutuse sisevõrku võib luua vastava portaali ehk veebirakenduse, millele kasutaja autendib end, kasutades tavalisi vahendeid. Sisevõrgu ametkondlik portaal ise on kaitstud tulemüüri ja juurdepääs portaali üle Interneti on kaitstud turvalise kaugpõõrduse (*remote access*) vahenditega.

3.3 Salastatuse tagamine

Enamik andmekogusid sisaldab juurdepääsu piiranguga andmeid. Juhul kui andmekogusid kasutatakse lokaalselt, tagatakse juurdepääsu piirangud füüsiliste, organisatsiooniliste ja teatud määral ka infotehnoloogiliste vahenditega. Kaugkasutuse korral üldkasutatavate sidevõrkude kaudu muutuvad infotehnoloogilised vahendid aga prevalveerivaks. Näiteks ei saa kuidagi läbi andmete krüpteerimiseta.

Põhimõtteliselt on olemas rida standardeid, millele vastavad tooted sobivad antud probleemi lahendamiseks. Nende levikut ja kättesaadavust arvestades on soovitatav kasutada mõnd transpordiprotokolli (TCP) [48] tasemel toimivat protokolli nagu TLS [11] (tuntud SSL protokoll [17] edasiarendus) või SSH [42], mille puhul väga heterogeense ja hajutatud haldamisega (administreerimisega) võrgu loomine ja ülalpidamine on märksa lihtsam kui võrguprotokolli (IP) [26] tasemel toimivate protokollide (nagu näiteks IPsec [27]) korral. Transpordiprotokolli tasemel toimivate protokollide eeliseks on ka parema eraldatuse tagamine suhtluspartnerite vahel ning võimalike sisevõrgu aadressruumi konfliktide vältimine. Funktsionaalsuses ei ole SSH ja SSL protokollidel suurt vahet, samas on SSL protokollide kasutamise rakenduste haldamine kasutajate (asutuste) arvu kasvades lihtsam. Samuti on SSL protokoll integreeritud mitmete rakendusprotokollide (nagu HTTP [39], IMAP [37], SMTP [23], CORBA [9]) serveritega.

3.4 Terviklus, jälitatavus ning tõestusväärus

Enamiku andmekogude juures ei ole kõige olulisem mitte juurdepääsu piiramine, vaid hoopis andmekogu tervikluse tagamine. Lihtne näide on Äriregister, kus sisaldub info inimeste kohta, kellel on firmas allkirjaõigus. Kui keegi muudab volitamatault seda nimekirja ja lisab sinna mõne "tankisti", võib too firmale suurt ja korvamatut kahju teha, näiteks müües maha firmale kuuluva kinnisvara, mis seejärel veel paar korda edasi müüakse, kuni ostja on seaduse silmis piisavalt "heauskne" [44].

Probleemid alusetute kannete ja toimingutega esinevad ka mitteelektroniliste registrite korral. Kuid ohud, mis tavalise (paberil või lokaalses infosüsteemis hoitud) registri korral peaaegu kunagi ei realiseeru, muutuvad laiemale kasutajate ringile avatud registrite korral piisavalt oluliseks, et nõuda eraldi käsitlust.

Suletud süsteemi korral rakendatakse tervet rida organisatsioonilisi, füüsilisi ning infotehnoloogilisi turvameetmeid. Näiteks pääsevad registrile ligi ainult selleks volitatud töötajad, kelle tausta on kontrollitud ja kontrollitakse (*screening*). Nende tegevused registreeritakse turvatöötajate ja süsteemide poolt, register ise on üles ehitatud selliselt, et säiliks kogu tegevuste ajalugu: andmeid ei kustutata ega muudeta kunagi, mingi olemi oleku muutumist kajastatakse uue kirje lisamisega baasi, kusjuures kirje ise viitab muutuse aluseks olnud alusdokumendile ning loomulikult ka muutuse tegijale. Samuti toimuvad perioodiliselt auditid, kus kontrollitakse registri kooskõlalisust. Varundusprotseduurid on dokumenteeritud, katsetatud ning nende täitmist jälgitakse.

Avatud registri korral tuleb kõiki neid protseduure laiendada kõigile kasutajatele. Kuid see ei ole veel piisav. Kuna päring võib tulla ka väljastpoolt asutust, peaks selle tegija olema samal viisil tuvastatav kui sisemise päringu tegija. Antud juhul ei ole abi turvakaamera salvestustest, et tuvastada, milline töötaja millise arvuti taga muudatuse sooritamise ajal istus. Jah, naaberasutuses peavad loomulikult kõik turvameetmed paigas olema, kuid selleks, et andmeandja neile viidata saaks, peab tal olema objektiivne tõestusmaterjal, mille alusel saaks näiteks väita, et päring tuli väljastpoolt asutust.

Logidel võib olla kas:

- 1) tuvastusfunktsioon (asutusesiseseks otstarbeks) või;
- 2) tõestusfunktsioon.

Kuna tavalised logid (tekstifaili kujul) on lihtsalt muudetavad ilma jälgi jätmata, siis saab tavalistel logifailidel olla ainult tuvastusfunktsioon. Tõestusfunktsioon pole võimalik ilma krüptograafilise kaitseta, mis võib olla kas:

- 1) digitaalallkiri kannete allika tuvastuseks või;
- 2) ühesuunaline linkimine koos keskse auditiserveriga hilisema muutmise tuvastamiseks, mis ei tarvitse tõestada kande tegijat [30].

Antud juhul tuleb tagada nii kande tegija kui ka hilisema muutuse tuvastamine, mistõttu tuleb rakendada mõlemaid meetmeid.

Tõestusväärtust omav logifail võimaldab küllalt suure kindlusega väita, kas päring tuli asutuse seest või väljast ja kui väljast, siis millisest asutusest. Edasi peab juba see asutus oma tavaturvameetmete logisid kasutades välja selgitama, milline ametnik päringu tegelikult algatas.

Paneme tähele, et tegelikult on tõestusfunktsioon andmekogu valdajale enesekaitseks hädavajalik ka juhul, kui võrgu kaudu andmekogusse muudatuste tegemist ei võimaldatagi, võimalik on vaid andmepäringuid esitada ja neile vastuseid saada.

Vaatame jälle algset näidet. Oletame, et kinnistute registri ametnik soovib kontrollida, kas inimesel on õigus firma nimel tehingut teha või mitte. Selleks esitab ta päringu Äriregistrile isiku allkirjaõiguse kohta. Saades positiivse vastuse, sooritab ta soovitud toimingut.

Mis aga juhtub, kui kinnistute registri ametnik oli tegelikult sobingus petturitega? Oletame, et Äriregister andis päringule isiku allkirjaõiguse kohta negatiivse vastuse, kuid kinnistute registri ametnik sooritas siiski tehingu ning tehingu ilmsiktulekul väitis, et Äriregister andis talle positiivse vastuse. Kuna Äriregister ei suuda objektiivselt tõestada, millise vastuse ta kinnistute registri infosüsteemile saatis, võib ametnik alati väita, et ta sai positiivse vastuse, isegi kui vastus oli tegelikult negatiivne. Enamgi veel: ta võib süüdistada hoopis Äriregistri töötajaid sobingus petturitega. Objektiivse tõendusmaterjali puudumisel tuleb tegelda küllalt keeruka ja vaevanõudva uurimisega.

Kui objektiivse tõendusmaterjali tekitamise mehhanismid on paigas ja kõigile hästi teada, siis juba ainuüksi see fakt mõjub kui efektiivne profülaktiline turvameede. Teades, et tema tegevusest jääb järele tõestusväärtusega jälg, ei hakka enamik ametnikke üritamagi ebaseaduslikke päringuid.

Nagu tõdetud, tuleb kõik kahe asutuse vahel liikuvad sõnumid varustada digitaalallkirjaga. Oletame, et ametnikul on selleks vajalikud vahendid (võti, sertifikaat). Kui kasutaja allkirjastaks oma algse päringu (kohalikule infosüsteemile) tervikuna, ei oleks sellest suurt kasu, sest kohalik infosüsteem lõhub selle päringu alampäringuteks, milledest mõned esitatakse kohalikule infosüsteemile, mõned teise asutuse halduses olevale andmekogule, mõned mõnele kolmandale asutusele, jne. Kuna algne päring ei jõua andmekoguni, ei ole andmeandjal võimalik ka andmete saaja antud allkirja kontrollida. Teatud juhtudel (näiteks kriminaalasja uurimisel või siis KAPO tehtud päringu korral) on see lausa kohustuslik, et algne päring ja allkiri väljapoole ametiasutuse infosüsteemi ei jõuaks.

Alternatiiv, kus kasutaja signeeriks kõik alampäringud iseseisvalt, ei lahenda probleemi, sest kasutaja ei ole võimeline aru saama madala taseme protokollis sõnumite sisust, mida ta allkirjastab. Samuti halvendab selline lähenemine oluliselt süsteemi käideldavust. Seega ei aita ametnikupoolne päringu signeerimine kaasa tõestusmaterjali tekkimisele.

Lisaks toob päringu osadeks jagamine kaasa ründeohu päringut sooritava ametniku vastu: tema võrdlemisi süütu päring võidakse teisendada päringuteks andmekogudesse, mille poole pöördumise soovi ametnikul ei olnud ning mis võivad osutada tundlikeks või mille vastuseid kogub "tõlk" oma huvides. Mida (organisatsiooniliselt) kaugemal kasutajast asub "tõlk" – server, mis päringu alampäringuteks jaotab –, seda väiksem on töötaja võimalus teda mõjutada ning seda suurem on kirjeldatud rünnete tõenäosus. Sageli ei ole alampäringuteks jaotamine töötajale üldse läbipaistev, kuna toimub ainult "tõlgile" teadaolevate andmete alusel.

Kokkuvõtteks: logidel ilma päringute signeerimiseta ei ole praktiliselt kasutatavat tõestusväärtust. Lisaks tuleb tagada logide terviklus, toetudes nt. tsentraalsele ajatempli- või auditiserverile [6], [8], [7] ja kasutades turvalisi logimissüsteeme. Kindlustada tuleb ka logide salvestamise ja säilitamise viisil, mis ei võimalda asjaosalistel (töötaja, andmekogu pidaja, kummagi poole süsteemiadministraator, võimalik vahendaja) neid võltsida ega hävitada. Üheks võimaluseks on logide

publitseerimine, mis aga kahjustaks oluliselt konfidentsiaalsust. Teiseks võimaluseks on regulaarne serverite auditeerimine.

Et osapoolte logidesse jääks tõestusväärtusega jälg, kinnitamaks päringu toimumist ja vastuse saatmist, tuleb kõik saadetavad päringud siiski signeerida (kasutades mitte isiku-, vaid serverisertifikaate). Serveritevaheline signatuuripõhine autentimine aitab niisiis olulisel määral tõsta süsteemi turvalisust.

3.5 Käideldavus

Käesolevas alapunktis vaadeldakse kõigepealt ohte, mis süsteemi käideldavust mõjutavad. Süsteem koosneb kolmest komponendist:

- 1) andmekogu infosüsteem;
- 2) ametiasutuse infosüsteem;
- 3) nendevaheline sidekanal.

Infosüsteemile mõjuvad peamised ohud on:

- 1) inimvead;
- 2) mitmesugused stiihilised ohud (üleujutused, tulekahjud jms);
- 3) elektrikatkestused;
- 4) vandalism;
- 5) rüüanded (nii sisemised kui avalikust võrgust lähtuvad).

Sideliinide korral lisanduvad veel:

- 1) kanali ebapiisav läbilaskevõime;
- 2) sidekatkestus;
- 3) teenusetõkestusrüüanded.

Mingi ohu vastu võitlemiseks rakendatavad meetmed sõltuvad paljuski konkreetse andmekogu olulisusest riigi toimimiseks. Järgnevas vaadeldakse eraldi kõikidele ohtudele vastavaid turvameetmeid [20].

3.5.1 Stiihilised ohud

Olulised registrid peavad olema dubleeritud, mis on ka praktiliselt ainus kaitse süsteemi töö kiireks taastamiseks. Loomulikult peavad dubleeritud süsteemid asuma üksteisest geograafiliselt piisavalt kaugel. Samuti peavad nad olema pidevalt sünkroniseeritud, et vältida andmekogu tervikluse kadu, kui stiihiline oht realiseerub ebasobival ajal (kauge maa tagant sünkroniseerimisel on täiesti oma turvanõuded, mis veel eraldi käsitlust vajavad).

Vähemtähtsate registrite korral piisab järgmistest meetmetest:

1. Sage plaanipärane varundamine koos varukoopiate geograafilise eraldamisega.
2. Taasteplaani ja vajalike eellepingute (näiteks riistvara tarneteks) olemasolu.
3. Paberdokumente kasutava alternatiivse süsteemi olemasolu, mis võimaldab vastata olulisematele päringutele, kuni elektrooniline süsteem jälle töökorda saab.

sidekanalid selle võrgusõlmeni oleks üksteisest täielikult sõltumatud, soovitavalt ka eritüübilised.

3.5.8 Teenusetõkestusründed

Avalikust võrgust lähtuvate rünnete eriliik. Nende allikas on tavaliselt oluliselt raskemini tuvastatav, kui see üldse võimalik on. Parim soovitus sedasorti rünnete vastu võitlemiseks oleks see, et omavahel suhtlema pidavatest asutustest moodustatakse poolkinnine võrk, milles kulgeva liikluse jaoks eraldatakse KÕIGIS sidekanalites teatud kindel riba. See garanteerib süsteemi töö ka kõige ohtlikuma ründe ajal. Toimetulek teenusetõkestusrünnetega eeldab tihedat koostööd ISPdega [31].

3.5.9 Käideldavus – kokkuvõte

Käesolev peatükk käsitleb mõningaid olulisemaid käideldavusprobleeme, mis esinevad kahe süsteemi omavahelises suhtluses. Need probleemid on küllalt tõsised.

Mistahes vahendajate lisamine sellesse süsteemi suurendab oluliselt tõrgete tõenäosust. Näiteks, kui lisame süsteemi kolmanda osapoole, mille ainsaks ülesandeks on vahendada ühe süsteemi päringuid teisele, oleme saanud peaaegu kaks korda enam haavatava süsteemi (lisandub 1 sidekanal ning üks infosüsteem). Liitunud alamsüsteemide arvu kasvades kasvab ka oht, et kesksüsteemi muude süsteemidega ühendava kanali läbilaskevõime osutub ebapiisavaks.

3.6 Monitooring

Ükski süsteem ei püsi turvalisena ilma pideva jälgimise ja intsidentidele reageerimiseta. Ühelt poolt leitakse pidevalt uusi turvaauke, mida tuleb lappida. Teiselt poolt aga ei pruugi augu leidjad sellest üldse avalikult kuulutada, vaid võivad hoopis hakata "teadmuskapitali" realiseerimiseks rünnet praktikas rakendama. Lisaks on alati olemas kasutajad, kes oma volitustest ühel või teisel viisil üle astuvad. Juhul kui nad ei tegele mitte andmete aktiivse muutmisega, vaid hoopis sellest info kaevandamisega, võib nende tegevus küllalt kauaks märkamatuks jääda. Mida varem nende tegevusele jälile saadakse, seda väiksemad on kahjud.

Sedasorti rünnetest tekkiva kahju minimeerimiseks tuleb tagada kaitstavate süsteemide pidev monitooring [41]. Monitooring on küllalt kallis, eriteadmisi nõudev ning tömahukas tegevus. Ilmselt ei ole mõeldav, et iga andmekogu oma monitooringusüsteemi või –keskuse käivitaks. Tsentraalselt teostatav monitooring oleks ühelt poolt odavam, teiselt poolt aga pakuks sõltumatu vaate osapoolte vahelisele suhtlusele. Samas ei maksa välistada võimalust, et mõni eriti tähtsa andmekogu haldaja teostab monitooringut ka ise.

Millised on monitooringu funktsioonid? Kindlasti ei suuda monitooring teostada analüüsi üksikute päringute tasemel. Pigem on tema funktsioon trendide tuvastamine (näiteks päringute arvu ootamatu kasv võrreldes eelmise perioodiga vms.) ning ebaharilike kasutusmustrite leidmine. Samuti võiks monitooringut teostav meeskond tegeleda ka otseste rünnete (k.a. teenusetõkestusrünnete) avastamisega ning nende allikate kindlakstegemisega.

Näiteks panganduses on sedasorti monitooring küllalt suure eduga aktiivselt kasutuses. Kasutatavad meetodid ning tehnika võivad olla aluseks ka käesolevas töös vaadeldavas süsteemis, kuid täpsete kasutatavuse hinnangute andmine nõuaks täiendavaid uuringuid.

3.7 Süsteemide atesteerimine

Andmekogu omanik (*A*) vastutab oma andmekogu eest. Kui ta sõlmib teise asutusega (*B*) lepingu, milles annab tolele õiguse andmeid kasutada, on just *A* õigus ja kohustus seada *B*-le tingimusi ja piiranguid, tagamaks *A* infosüsteemi kaitset. Nendeks võivad olla päringutüüpide piirangud, nõuded *B* infosüsteemi turvasemele jpm. Samas ei tarvitse üksik *A* olla kompetentne vastavaid nõudeid seadma, eriti kui *B* on (hierarhiliselt) tunduvalt tugevamal positsioonil. Seega on riigi andmekogude käideldavuse tegeliku taseme parandamiseks vaja kasutajasüsteemidele esitatavad nõuded ja piirangud aidata määratleda riiklikul tasemel [3]. Viimasest kasvab välja vajadus riiklikul tasemel atesteerida kõiki kasutajasüsteeme, mis soovivad lülituda infovahetusse riigi andmekogudega. Viimane võib hõlmata nii infosüsteemi enda ülesehitust ja haldamist kui ka, tundlikumatel juhtudel, kasutajate oskuste ja tausta kontrolli.

Kasutajasüsteemide atesteerimise vajadus kasvab oluliselt, kui *A* lisaks lugemisõiguse andmisele avab oma andmekogu *B*-le ka kirjutamiseks.

Ka ainult lugemiseks avatud infosüsteemis võib olla vigu, mille ärakasutamisel saadakse lisaks kirjutamisõigus. Andmekogu *A* pidaja on seetõttu kohustatud olema pidevalt valmis andmete taastamiseks seisuga, milleni suudetakse tuvastada volitamata muutusi. Ka taaste vajadus kasvab sedamööda, mida rohkematele kasutajatele on süsteem kirjutamiseks avatud.

3.8 Analüüsi tulemuste rakendamine eritüübiliste infosüsteemide korral

Töö esimeses osas soovitati välja töötada tüüpasutuste mudelid ja klassifitseerida kõik asutused ühe- või teisetüübiliseks. Kuna konkreetseid, reaalsele vajadustele vastavaid tüüpe veel pole, siis oli eelnev analüüs suhteliselt neutraalne, kuid kirjeldas siiski pigem keskmistele ja suurtele asutustele kohaseid turvameetmeid ja situatsioone. Käesolev peatükk näitab, et esitatud kontseptsioonid on realiseeritavad ka väiksemate infosüsteemide korral.

Ka üks lauarvuti moodustab infosüsteemi. Käesoleva käsitluse mõttes piiritleb infosüsteemi ära haldusdomeen. Kõik sama asutuse halduses olevad arvutid moodustavad ühe infosüsteemi. Selline lähenemine on õigustatud, arvestades, et:

- me analüüsime süsteemi turvalisuse seisukohast;
- füüsilise juurdepääsu korral arvutile on võimalik kõiki selles sisalduvaid andmeid (k.a. programmid ise) lugeda ja muuta, sellest jälgi jätmata.

Eelnevast järelduvalt ei ole mõtet analüüsida süsteemi, mille mingi osa ei asu meie kontrolli all. Juhul kui infosüsteemi loomisel soovitakse mingi osa teenustest sisse osta [2], tuleb kindlasti pöörata tähelepanu teenusepakkujaga (*Application Service Provider, ASP*) sõlmitavate lepingute sisule. Lepingud peavad selgelt sätestama teenusepakkuja vastutuse ning kohustused. Kuna teenusepakkuja infosüsteem moodustab olulise osa analüüsitava infosüsteemist peab see läbima samasuguse auditeerimis- ja akrediteerimisprotseduuri nagu loodav süsteemgi ning olema vähemalt sama turvaline, kui peab olema loodav süsteem.

Iga asutuse infosüsteem vajab kaitset. Kaitset igasuguste rünnete eest. Ükski kaitsemeetod eraldivõetuna ei ole efektiivne, meetmeid on vaja kombineerida, jälgides,

et kõik võimalikud ründeviisid oleksid kaetud. See tähendab nii füüsiliste, organisatsiooniliste kui infotehnoloogiliste kaitsemeetmete kombineerimist.

Loomulikult ei saa midagi absoluutselt kindlalt kaitsta ja see pole ka vajalik. Vajaliku kaitse määra saab hinnata pärast riskianalüüsi ning sellele järgnevat tasuvusanalüüsi, kõrvutades infovarade hinda ning kaitsemeetmete hinda [20, lk 82].

Omadused, mida me infosüsteemilt nõuame, võivad olla realiseeritud mitmeti. Näiteks minimaalse asutuse korral, kus on vaid üks töötaja ja üks arvuti, koosneb infosüsteem sellestsamast arvutist. Kõigi päringute eest, mis on tehtud sellest infosüsteemist, vastutab seesama üks inimene. Sellise infosüsteemi kasutamiseks loa saamisel (atesteerimisel) tuleb näidata, kuidas välistatakse volitamatu juurdepääs sellele arvutile: ilmselt peab arvuti asuma ruumis, millele on juurdepääs vaid sellel inimesel, ilmselt peab olema see ruum varustatud valvesignalisatsiooniga (selle töökorrasolekut tuleb perioodiliselt kontrollida), turvaintsidentide korral (sissemurdmine) tuleb arvuti kogu tarkvara uuesti installeerida, kõik paroolid ja sertifikaadid vahetada, jne. Konfidentsiaalsed andmeid ei tohiks sellises üksikus arvutis olla.

Suures asutuses, kus on palju töötajaid, kes kasutavad keskses serveriarvutis olevaid ressursse, võib kaitse olla üles ehitatud oluliselt erinevalt. Kindlasti tuleb mitme töötajaga asutuse korral lahendada administraatorite töö üle järelvalve korraldamine. Vältida tuleks kõigis serverites kõiki õigusi omavate administraatoriametikohtade teket. Ka administraatorite tööd tuleks logida, nii et nad tekkivaid logisid ise muuta ei saaks. Töötajate isikliku vastutuse olemasolu võimaldamiseks peaks töökohtade administreerimine administraatorite poolt olema hästi reglementeeritud ja jälgitav. Vältida tuleks absoluutset kontrolli andvate administreerimis-vahendite kasutamist. Siin tekib taas kord klassikaline dilemma turvalisuse ja käideldavuse (hõlpsa administreeritavuse) vahel.

3.8.1 Näide: Sertifitseerimise Riikliku Registri infosüsteemi turvameetmed

Äärmuslikuks näiteks turvameetmete rakendamise kohta on Sertifitseerimise Riikliku Registri (SRR) infosüsteem, mille projekteerimises autor osales.

Sertifitseerimise Riiklik Register on loodud digitaalsignatuuri seaduse alusel [12] ning tema ülesandeks on pidada arvestust teenuse osutajate üle ning tagada ajatempliteenuse osutajate poolt väljaantavate ajatemplite ajalise järgnevuse võrreldavus registri vastutava töötleja kehtestatud täpsusega. Registri töö on korraldatud vastavalt registri asutamise ja pidamise põhimäärusele [43].

SRR üheks funktsiooniks on sertifitseerimis- ja ajatempliteenuse osutajatele sertifikaatide väljastamine, nende üle arvepidamine ning hetkel kehtivate STO ja ATO sertifikaatide kohta info jagamine. SRR infosüsteemi turvalisusest sõltub kõigi väljastatavate digitaalallkirjade usaldusväärsus. Seetõttu on SRR infosüsteemile esitatud äärmiselt kõrged konfidentsiaalsus-, terviklus- ning käideldavusnõuded.

Järgnevalt on esitatud ülevaade kasutatavatest turvameetmetest, mis koos tagavad esitatud nõuete täitmise.

3.8.1.1 Infotehnoloogilised turvameetmed

- **Süsteemi sisselogimine kiipkaardi abil.** Operaatori töökoha infosüsteemi on võimalik sisse logida ainult kiipkaardi abil. Logimise õnnestumiseks peab süsteemile esitama kehtiva kaardi ning lisaks teadma selle PIN-koodi.

- **Administraatori konto puudumine.** Süsteemis puudub administraatori (juurkasutaja) konto. Süsteemi kõik komponendid (tulemüür, serverid, operaatori töökoht) on disainitud nii, et nad ei vaja tavapärasest administreerimist (hooldus, logide rullimine). Juhul kui peaks tekkima vajadus tavapärase administreerimisfunktsioonide järele loetakse see lugeda kõrvalekaldumiseks spetsifikatsioonist ja kõrvaldatakse vastav puudus. Administraatori konto puudumisega välditakse hulk tavapärasest infosüsteemides tekkivaid usaldusprobleeme.
- **Lihtne varundusprotseduur.** Varukoopiate tegemine on väga lihtsaks tehtud, mistõttu ei tohiks operaatoris tekkida tõrget nende tegemise juures ja seetõttu on süsteemi krahhimise korral alati värske varukoopia käepärast võtta.
- **Kiire taasteprotseduur.** Süsteemi suvalise komponendi taastamine pärast krahhi on väga kiire. Tulemüüri korral kulub selleks ligikaudu 5 minutit, serveri korral 10 minutit ning operaatori töökoha korral 15-20 minutit.
- **Dubleeritud andmebaasid.** Andmebaasid on mitmekordselt dubleeritud. Nii on tagatud serverites pärast viimase varukoopia tegemist tekkinud andmete säilimine isegi siis kui üks ja mõnel juhul isegi kaks süsteemi komponenti krahhivad.
- **Tulemüür.** Süsteemi tundlikumad osad on paigutatud tulemüüri taha, mis kaitseb neid triviaalsemate võrgust lähtuvate rünnakute vastu.
- **Minimaalne vajalik funktsionaalsus.** Vigade ja turvaaukude esinemise tõenäosuse vähendamiseks on süsteemi loomisel sellele lisatud ainult minimaalne vajalik funktsionaalsus. Kogu süsteemis pole ühtki teenust ega serverit mis ei oleks hädavajalik süsteemi töötamiseks. Olemasolevad ja töötavad teenuseid pakkuvad serverid on valitud ja konfigureeritud nii, et potentsiaalselt ohtlikud funktsioonid oleks välja lülitatud. Nii näiteks ei võimalda registri publitseerimiseks kasutatav veebiserver käivitada CGI skripte. Isegi vastav funktsionaalsus puudub serverist täiesti.
- **Individaalsed varutoiteallikad.** Igal serveril, mis sisaldab olulisi andmeid on oma isiklik varutoiteallikas (*UPS*). Enne varutoiteallika aku tühjenemist seisatakse arvutid automaatselt.
- **Aktiivne monitooring.** Süsteemi kõik komponendid jälgivad oma naabrite ning iseendi tööd ja saadavad kriitiliste vigade korral tõrketeateid. Operaator saab määrata millistele meiliaadressidele või mobiiltelefonidele tõrketeateid saadetakse.
- **Logimine.** Süsteem logib kõiki operaatori tegevusi logisse, mis ei ole operaatori poolt muudetav. See tagab võimaluse auditeerida operaatorite tööd.
- **Varukoopiate signeerimine.** Süsteemi varukoopiad on signeeritud. Varukoopiate verifitseerimiseks vajalik võti salvestatakse süsteemi installeerimisel flopile, mis jääb installeerimise ja taastamise juures viibiva komisjoni valdusesse. Varukoopiate signeerimine väldib nende volitamatu muutmise kas operaatori või kellegi kolmanda poolt.

3.8.1.2 Füüsilised turvameetmed

- **ArvutišEIF.** Süsteemi kõik tundlikud komponendid paiknevad spetsiaalses arvutišEIFis, millele on juurdepääs ainult komisjoni juuresolekul. ŠEIFis paiknevad kõik arvutid, varutoiteallikad, sisevõrkude kontsentraatorid ja konsoolilüliti. ŠEIFist

väljas paiknevad monitor, klaviatuur, hiir, CD-kirjutaja varukoopiate tegemise tarvis, kiipkaardilugeja ja printer.

- **Piiratud juurdepääs.** Pääs ruumi, kus paikneb infosüsteem on piiratud vastavalt volitatud töötaja kehtestatud eeskirjadele. Samuti tuleb nende eeskirjadega reguleeritud tuleohutuse jms. küsimused.

3.8.1.3 *Organisatsioonilised turvameetmed*

Süsteemi haldusfunktsioonid jagunevad kolme isikute grupi vahel nii, et kõigi vastutus on täpselt piiritletud. Vastav regulatsioon on sätestatud registri tööeeskirjadega. Oluline on, et ühelgi üksikisikul eraldi võttes pole võimalust süsteemi jälgi jätmata muuta.

Kasutajategrupid ja nende funktsioonid on järgmised:

- **Komisjon.** Viibib juures igal šeiifi avamisel ning jälgib ja dokumenteerib haldustegevused mida operaator ja/või tehnilise toe isikud süsteemi kallal läbi viivad. Haldavad varukoopiate verifitseerimiseks vajaliku avaliku võtit sisaldavat flopiketast ning veenduvad operaatori töökoha iga installeerimise korral, et taastatud andmete signatuur verifitseeruks.
- **"Minister".** Loob operaatorite kontosid. Ministri töö juures on oluline, et ta oleks kindel operaatori isikus, kellele ta kontot loob ning et operaatori avaliku võtme sõnumilühend jõuaks muutmata kujul võtit kinnitavasse määrusesse.
- **Operaator.** Operaator tegeleb registri tegeliku pidamisega, võtab vastu ja arhiveerib dokumente, väljastab kinnitusi dokumentide vastuvõtmise, tehtud otsuste ning registriseisu kohta, jälgib süsteemi tööd ning teeb varukoopiadi. Operaatori tegemistest jääb infosüsteemi auditeeritav jälg. Operaatoril puudub füüsiline juurdepääs infosüsteemi arvutitele, samuti ei saa ta jälgi jätmata muuta varukoopiaid.

3.8.2 *Näide: personaalne turvakeskkond*

Teist äärmust esindavad personaalsed turvakeskkonnad (*Personal Security Environment*). Personaalne turvakeskkond on turvaseade, mis:

1. Sisaldab kogu turvaliseks sõnumivahetuseks vajaliku funktsionaalsust: kasutajaliidest, krüptoprotsessorit, võtmehoidlat ja sideliidest.
2. On füüsiliselt hästi turvaline: omab monoliitset, mitteavatavat korpust, mis on hästi varjestatud, krüptograafilisi võtmeid hoitakse ka füüsiliste rünnete eest kaitstult.
3. On piisavalt pisike ja kerge, et tema omanik saaks teda endaga pidevalt kaasas kanda.
4. Suudab oma omanikku autentida.

Personaalsed turvakeskkonnad võimaldavad luua lahendusi, kus isik ei pea oma ülesannete täitmisel usaldama mitte kedagi teist. Näiteks lauarvutitel baseeruva infosüsteemi korral peab arvutikasutaja usaldama vähemalt oma süsteemiadministraatorit, tihti ka töökaaslast, kellel on juurdepääs tema arvutile. Personaalsete turvakeskkondade korral on ainuke usaldamist vajav isik seadme valmistaja.

Personaalseid turvakeskkond kujutab endast tegelikult iseseisvat infosüsteemi ja on eriti sobilik kasutamiseks mobiilsust nõudvate süsteemide juures, kus klassikalisi füüsilisi ning organisatsioonilisi turvameetmeid ei saa rakendada.

Süsteemide turvalisusest rääkides kasutatakse tihti võrdlust ketiga. Kett on nii tugev kui tugev on tema nõrgim lüli. Personaalsete turvakeskkondade juures on viidud keti lülide arv miinimumini, mistõttu tugeva keti ehitamine on odavam kui muude lahenduste korral.

Väga hea ülevaate personaalsetest turvakeskkondadest leiab Margus Freudenthali magistritööst [18].

3.9 Lahenduste skaleeruvus

Seni käsitleti vaid kahe asutuse vahelist suhtlust. Millised lisategurid ilmnevad, kui liita rohkem kui kaks asutust? Ilmne on, et ükski turvaeeldustest ei kao. Ühtegi süsteemi ei saa muuta turvalisemaks sinna ainult teatud komponente lisades. Tekivad hoopis täiendavad probleemid:

1. Asutuste vahelisi lepinguid tekib palju rohkem, mis muudab veelgi olulisemaks atesteerimise ning standardsete lahenduste olemasolu.
2. Asutuste infosüsteemides kasutatavate sertifikaatide arv kasvab. Olukorda aitaks lahendada nende väljaandmise ning halduse tsentraliseerimine.
3. Dubleeritud süsteemide olemasolu koordineerimine muutub keerulisemaks, kuna neid tekib palju. Olukorda aitaks lahendada tsentraalse teenuste andmebaasi olemasolu.

Punktides 2 ja 3 pakutud lahenduste kasutuselevõtul tekkivad uued andmebaasid, millede kättesaadavusest sõltub kogu süsteemi toimimine. Need andmebaasid peavad kindlasti mitmekordselt dubleeritud olema, samuti omama dubleeritud sidekanaleid tähtsamatesse võrgusõlmedesse.

Punktis 3 kirjeldatud teenus on sisuliselt kataloogiteenus. Internetis on spetsialiseeritud kataloogiteenus realiseeritud kasutades DNS (*Domain Name System*) protokoll [36]. Kui oletada, et teenuste andmebaasist saab teenuse nime alusel teada vastava URL'i, siis tuleb enne tegeliku päringu esitamist tõlkida selles URLis peituv hostinimi DNS teenust kasutades IP aadressiks. Tegu on kahekordse kataloogiteenuse kasutamisega. Mõistlik oleks kui mõlemad kataloogid kasutaksid samu tehnilisi vahendeid ja protokolle. See vähendaks kaitsmist vajavate komponentide arvu ning muudaks süsteemi turvamise odavamaks.

DNS kasuks räägib ka see, et serverite dubleerimise ning päringuvastuste puhverdamise probleemid küllalt hästi ära lahendatud, samuti omab DNS turvalaiendusi [13], mis muudab levitatava info võltsimise võimatuks.

Tsentraalne monitooringuteenus hakkab end ära tasuma, kui jälgitakse paljude asutuste infosüsteeme. Väikese arvu asutuste korral on lihtsam, kui monitooringut teostavad asutused ise.

3.10 Järeldused asutus – asutus infovahetuse kohta

1. Digitaalallkirja kasutamine päringute toimimise tõestamiseks töötajate tasandil ei ole otstarbekas, kuna isiku autentimine asutusesiseselt ja tema tegevuse jälgede

kogumine toimub edukalt ka digitaalallkirja abita, kogutavad tõendid aga ei pea olema kasutatavad asutusevälistes juriidilistes toimingutes.

2. Vajadus keskse kasutajate (ametnike) autentimis- ja autoriseerimisteenuste järele puudub.
3. Otstarbekas on kasutada nõ digitaalallkirjastamist infosüsteemidevahelises andmevahetuses, kui signeerijaks on selles osalevad asutused (signatuuri annab asutuse server).
4. Logide kasutamine tõestusmaterjalina nõuab nii allkirjastamist kui regulaarset auditeerimist.
5. Asutuste vahel liikuvate andmete konfidentsiaalsuse tagamiseks on otstarbekas kasutada transpordiprotokolli taseme lahendusi nagu SSL või SSH.
6. Lisaks ühtsetele standarditele on otstarbekas luua mõned kesksed teenused, nagu näiteks ühenduvate infosüsteemide:
 - 1) sertifitseerimisteenus;
 - 2) nimeteenus;
 - 3) monitoorimisteenus ja;
 - 4) auditeerimisteenus.
7. Tuleb mõelda oluliste registrite käideldavuse tagamisele nende dubleerimise abil.
8. On vajadus ühendatavate infosüsteemide atesteerimise järele. See vajadus tuleneb sellest, et kui asutuste tasandil antakse B -le pääs A infosüsteemi juurde, sõltub A turvalisus B infosüsteemi turvalisusest. Kuna A ei tarvitse olla suuteline kehtestama ja uurima B infosüsteemi taset, on otstarbekas suurema hulga suhtlevate andmekogude korral luua ka keskne atesteerimisteenus.

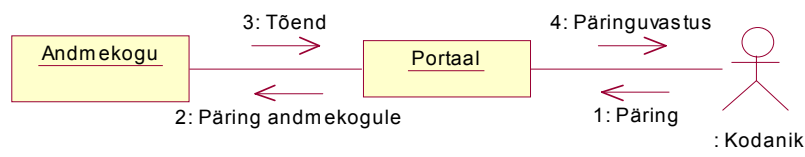
4. ASUTUS – KODANIK KASUTUS

Kodanik saab riigilt mitmesuguseid teenuseid, mille võib jagada kolme rühma:

1. Avalikud ja anonüümsed teenused, mille puhul kasutaja autentimine ei ole vajalik. Tegemist pole otseselt kodanikule, vaid kõigile võimalikele huvilistele suunatud teenustega.
2. Avalikud, kuid autentitud teenused. Näiteks võib planeeritav naabrimehe tuludeklaratsiooni vaatamine hakata kuuluma siia kategooriasse. Info on avalik, kuid selle vaatamisel edastatakse deklaratsiooni esitajale info selle kohta, kes tema deklaratsiooni on vaadanud.
3. Enesekohased päringud, mille puhul on nõutav eriti usaldusväärne autentimine isiku tasemel. Lisaks tuleb anda kodanikule infot ka selle kohta, kes (k.a. tema ise) ja millal on tema andmete vastu huvi tundnud. Viimane aitaks tuvastada ja vähendada võimalikke teesklusid. Samas ei saa isikule väljastatav päringute logi olla täielik, sest ei tohiks reeglina sisaldada (teatud grupi) ametnike päringute jälgi.

Autentimise seisukohast ei ole teisel ja kolmandal variandil tegelikult vahet. Seetõttu vaatleme kahte liiki teenuseid: autentimist vajavad ja autentimist mittevajavad.

Kuidas kasutaja riigiga suhtlema hakkab? Arvestades kasutajate suurt hulka ja nende poolt kasutatavate platvormide paljusust, samuti kodanikule pakutavate teenuste kiiret arengut projekti algfaasis, on mõistlik kasutada sellist lahendust, mis ei eelda kasutaja arvutisse täiendava tarkvara installeerimist. Mõistlik on eeldada, et luuakse portaal või portaalid, mille kaudu kodanik saab riigiga suhelda tavalist brauserit kasutades.



Joonis 7. Kodaniku suhtlus riigiga

Toodud skeem (vt joonis 7) näeb välja täpselt samasugune nagu ametiasutuste vahelise suhtlemise skeem: ametnik autendib end oma asutuse infosüsteemile ja see omakord andmekogudele. Antud juhul on ametniku asemel kodanik ning asutuse infosüsteemi asemel portaal.

Portaali haldab mingi riigiasutus, mille kohta kehtivad täpselt samad reeglid nagu teiste asutuste kohta (kui see nii poleks, tekitaks suur turvaauk ning kulutused ülejäänud süsteemi turvamiseks oleksid asjatud).

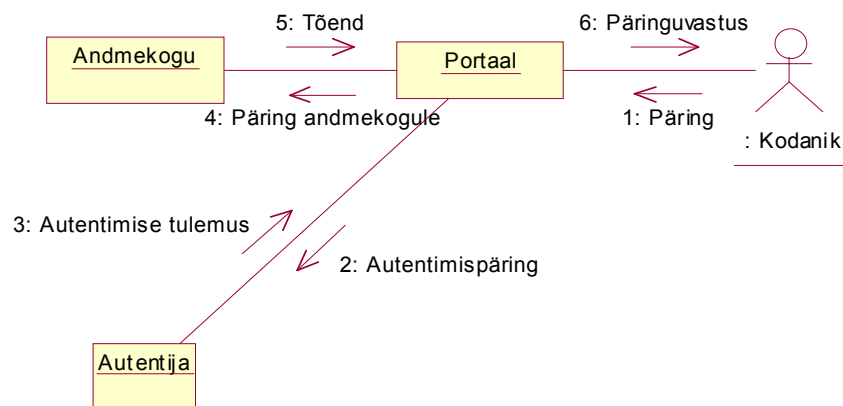
Keskendudes kodaniku ja portaali vaheliste suhete analüüsile, on vaja vastata järgmistele küsimustele:

1. Kuidas annab kodanik õiguse portaalile enda nimel päringuid teha? Ametnik annab selle õiguse asutuse infosüsteemile siis, kui ta sõlmib töölepingu ja kohustub täitma ametijuhendit ja töö sisekorraeeskirju.
2. Kuidas toimub kodaniku autentimine nende teenuste korral, mis seda vajavad?
3. Kuidas tagatakse kodaniku ning portaali vahelise suhtluse salastatus?

4.1 Välise autentija kasutamine

Üksikisikutest volitatud kasutajaid on suurusjärgus 1 miljon. Portaal peab suutma neid kõiki autentida. Miljoni kasutaja autentimisinfo haldamine on väga suur töö. Portaali loomine ja käigushoidmine oleks oluliselt odavam, kui kasutajate autentimise teenust saaks väljast sisse osta. Osutub, et mitmed suure kliendibaasiga ettevõtted nagu Hansapank [38] ja Ühispank [45] ongi asunud oma kliendibaasi ning enda tarbeks loodud autentimise infrastruktuuri baasil vastavat teenust müüma. Ka Eesti Telefoni toode "Teenustekaart Atlas" võimaldaks põhimõtteliselt sarnase teenuse pakkumist.

Välise autentija kasutamise korral (vt joonis 8) ei haldaks kasutajate autentimisinfot mitte portaal ise, vaid saaks kolmandalt osapoolelt (autentijalt) kinnituse päringut esitava kasutaja isiku kohta.



Joonis 8. Kodaniku autentimine välise autentija kasutamise korral

Seda skeemi võib ka modifitseerida. Näiteks võib kasutaja suhelda otse autentijaga ning edastada portaalile autentija poolt signeeritud autentimistokeni.

Milliseid uusi ohte välise autentija kaasamine endaga kaasa toob? Portaal usaldab täielikult autentija poolt antud kinnitusi kasutaja isiku kohta. See annab autentijale võimaluse esitada volitamata päringuid suvalise isiku andmete kohta. Võimalikud on kahte sorti ründed:

1. Esimene rünne eeldab, et kasutaja autentimine toimub paroolide või muu jagatud saladusel põhineva autentimisskeemi abil, mis definitsiooni kohaselt on autentijale

teada. Autentija võtab ühendust portaaliga ning väidab end olevat see kodanik, kelle andmeid ta soovib vaadata. Kuna kodaniku paroolid on talle teada, saab ta esitada õige parooli. Logidesse ei jää sellest ründest ainsatki kahtlast jälge.

2. Teine rünne töötab ka juhul, kui kasutaja autentimine toimub avaliku võtmega krüptosüsteemide abil, mistõttu autentijal ei ole võimalik otsest ja jälgi mittejätvat teesklusrünnet korraldada. Selle ründe puhul võtab autentija ühendust portaaliga ning väidab end olevat selle kodaniku, kelle andmeid ta soovib vaadata. Portaal esitab autentijale autentimispäringu. Ehkki autentimispäring ei ole tegelikult korrektne, annab autentija sellele siiski positiivse vastuse, mispeale portaal päringu edasi lubab. Kui portaal kõik autentimispäringud ja –vastused logib, on võimalik autentija kuritarvitust hiljem kindlaks teha.

Järelikult on välisel autentijal puhttehniliselt võimalik esitada omavoliliselt suvalisi päringuid suvaliste isikute kohta. Ehk teisisõnu: tal on (ebaseaduslik, kuid reaalne) võimalus esitada suvalisi päringuid riigi andmekogudesse. Potentsiaalsete autentijate ringi analüüsinult võib väita, et teatud sorti andmetest, mis seni vaid kodaniku enda teada on olnud, võiks autentijatel nende äritegevuse muudes valdkondades kindlasti kasu olla ja seetõttu ei tohi seda ohtu kindlasti ignoreerida.

4.1.1 Autentimine avaliku võtmega krüptosüsteemide abil

Avaliku võtmega krüptosüsteemide abil autentimise rakendamine eeldab kasutajalt igal juhul isikliku võtme ning sertifikaadi olemasolu. Mõne aasta jooksul peaks enamik inimesi saama endale ID-kaardi [24], mis kannab endas nii isiklikku võtit kui ka sertifikaati.

ID-kaardi kasutamine eeldab kliendi poolelt veel kiipkaardilugeja olemasolu, kuid see vajadus ei ole omane ainult antud projektile ning saab ilmselt lahenduse ID-kaardi kasutuselevõtu läbi muudes valdkondades.

Portaali poolel on vajalik sertifikaatide kehtivuse kontrolli võimalus. See on teenus, mida pakub sertifitseerimisteenuse osutaja, kes väljastab ID-kaardile kantud sertifikaate [12 pg 22, lg 6].

Mingeid muid eeldusi portaali poolele ei ole.

Kui eeldada, et kliendi autentimine toimub HTTPS [39] protokolliga turvava SSL ühenduse tasemel (kliendi autentimine SSL ühenduse loomisel on SSL protokolliga standardne omadus, mida kõik brauserid toetavad), siis piisab portaali poolele kliendi autentimiseks HTTPS serverist, mis saab esitada sertifitseerimisteenuse osutajale päringuid kasutajate sertifikaadi kehtivuse kohta.

Avaliku võtmega krüptosüsteemide abil autentimise korral puudub täielikult vajadus kasutada välist autentijat.

Selle autentimisviisi puuduseks on see, et tema üldkasutatavaks muutmine võtab mõne aasta aega. Sel ajal peab ilmselt rahulduma alternatiivsete autentimisviisidega või loobuma isikukohaste teenuste pakkumisest.

4.1.2 Autentimine jagatud saladuste abil

Ülaltoodud näidetest selgus, et sellel autentimisviisil on tõsiseid puudusi ja seda sõltumata sellest, kes autentimisinfo andmebaasi haldab. Igal juhul saab ta enda kätte

küllalt suure võimu. Teiselt poolt on jagatud saladuste haldamine töömahukas ning turvakriitiline protsess.

Kõne alla tulevad järgmised lahendusvariandid.

1. Luua riiklik infrastruktuur. Selle variandi puuduseks on ülisuured kulud ja ID-kaardi loodetavat tulekut arvestades väga lühike kasutusaeg. Ehk siis rahaliselt oleks tegu raiskamisega. Turvalisuse aspektist vaadates ja kõrvutades ühelt poolt ohtu, et olemasolevad autentijad hakkavad tegema volitamata päringuid ning teiselt poolt ohtu, et uue infrastruktuuri loomisel ja haldamisel tehakse fataalseid vigu, võib oletada, et teised ohud kaaluvad esimesed üles, ehk siis ka turvalisuse aspektist pole see lahendus otstarbekas.
2. Kasutada olemasolevate autentijate teenuseid. Majanduslikult oleks see kindlasti otstarbekas. Kui lisada sellele skeemile mõned volitusmehhanismid, millest allpool pikemalt juttu tuleb, võiks selle lahendusega nõustuda ka turvaaspektist.
3. Jagatud saladuste abil autentimisega süsteemi mitte luua ning oodata isikukohaste teenuste pakkumise alustamisega, kuni hakatakse ID-kaarte jagama. Turvaaspektist kindlasti parim lahendus. Ainult ID-kaardi abil autentimise võimalus oleks kindlasti ka tugev mootor ka ID-kaardi kiirele omaksvõtule.

Mõistlikud lahenduses on teine ja kolmas, kusjuures otsus nende kahe vahel valides on küllaltki poliitiline. Seejuures peaks arvestama, et kodanikke teenindav portaal ei saa tööd alustada enne, kui muu infrastruktuur paigas on; et kõigile turvanõuetele vastava infrastruktuuri loomine võtab vähemalt aasta ja et selleks ajaks on ID-kaartide väljastamine juba alanud, kaldub autor eelistama kolmandat varianti: **mitte käivitada kodaniku portaali enne ID-kaardi kasutuseletulekut.**

4.1.3 Volitusmehhanismide lisamine välist autentijat kasutavale skeemile

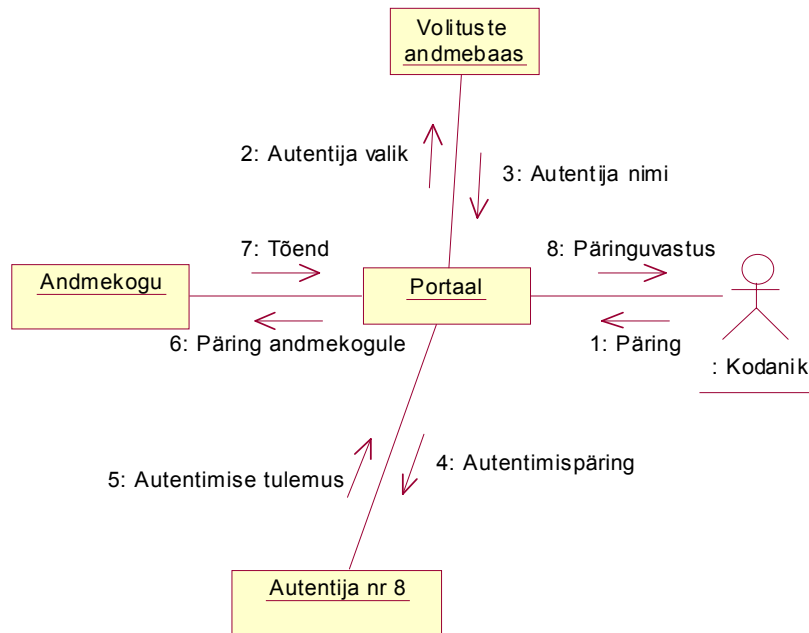
Kindlasti on olemas kodanikke, kellele on vastuvõetamatu risk, et välisel autentijal tekib võimalus tema andmeid vaadata.

Teiselt poolt ei ole ühegi võimaliku autentija kliendibaas nii suur, et ta suudaks autentida kõiki kodanikke. Välisel autentijal ei tohi olla võimalust anda positiivset autentimistulemust kasutaja kohta, kes ei ole tegelikult tema klient.

Neid kaht tõsiasja kombineerides võib jõuda järeldusele, et portaali juures peaks olema volituste andmebaas, kus on kirjas, milline autentija (kui üldse) võib autentida millist kodanikku. See andmebaas ei saa olla ühegi autentija juures (kuna ta on mõeldud just nende tegevusega seotud ohtude minimeerimiseks). Andmebaasis ei sisaldu üldse salajast infot, oluline on vaid selle baasi terviklus. Selle baasi seisu saab muuta ainult kodaniku avalduse alusel. Süsteemi käivitades ei tohiks seal olla ühtki kirjet. **Kõik inimesed peaksid kirjalikus vormis deklareerima, kas ja millist välist autentijat nad soovivad kasutada.**

Kergesti võib siin tekkida mulje, et viimane nõue on üsna pretsedenditu: näiteks on ju olemas võimalus tulumaksu deklareerimiseks läbi panga [15], miks ei võiks siis muudki teenused samamoodi vaikimisi lubatud olla? Vastuseks tuleb märkida, et tulumaksudeklaratsioon ja laias laastus kõik rahaga seonduv on pankade seisukohast pisut erandlikus seisus. Pangal on niikuinii olemas võrdlemisi täpne ülevaade oma klientide tuludest ja kuludest. Tuludeklaratsioon ei sisalda tema jaoks kuigi palju uut infot. Asi on oluliselt teine, kui me räägime infost kliendi tervise, kriminaalse mineviku vms. kohta. Ehkki ka see info võib olla pangale kasulik, ei anna kehtiv õigus nende

andmete kasutamiseks pankadele mingeid volitusi. **Tulumaksu-deklaratsioonide esitamise süsteemi ei saa seega niisama lihtsalt laiendada suvaliste päringute edastamiseks.**

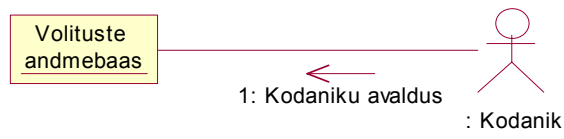


Joonis 9. Volituste andmebaasi kasutamine

Volituste baasi olemasolu korral toimub kodaniku päringu töötlemine järgnevalt (vt joonis 9):

1. Kodanik esitab päringu.
2. Portaal küsib volituste andmebaasist, millist autentijat kasutada.
3. Portaal edastab kodaniku autentimispäringu määratud autentijale.
4. Autentija tagastab autentimise tulemuse.
5. Portaal esitab päringu andmekogule.
6. Andmekogu tagastab tõendi, mis edastatakse kodanikule.

Süsteemi toimimine eeldab, et kodanik on esitanud volituste andmebaasile kirjaliku avalduse välise autentija valiku kohta (vt joonis 10). Samuti seda, et ta on valitud autentija klient.



Joonis 10. Kirje kandmine volituste baasi.

4.2 Vastavus andmekogude seadusega

Kodanikuportaali loomisel tuleb pöörata tähelepanu ka projekti juriidiliste aspektidele.

Vastavalt andmekogude seadusele [4] on andmekogu volitatud töötaja volitatud väljastama andmeid ainult siis, kui ta on kindlaks teinud päringu esitaja isiku ning veendunud, et andmeid, mida päringu esitaja taotleb, on tal õigus saada. Tal on tõestamiskohustus, et väljastas andmed volitatud andmesaajale, kelle identsuse ta kindlaks tegi ning et sellel isikul oli konkreetsetele andmetele juurdepääs.

Ka asutustevahelise suhtluse analüüs jõudis järeldusele, et see tõestamiskohustus tuleb vastavate lepingute abil lükata andmeid kasutavale asutusele. See omakorda peab valima kahe variandi vahel.

1. Autentima ametnikke infosüsteemi kasutamisel nii, et tekiks tõestusmaterjal, mis sisuliselt tähendab digitaalallkirja mehhanismi kasutamist kõigi päringute autentimiseks.
2. Sõlmima ametnikuga lepingu, mis vabastaks ta tõestuskohustusest, või täpsemalt, võtaks ametnikult õiguse vaidlustada asutuse väiteid päringu sooritamise kohta.

Täpselt sama situatsioon on ka kodaniku poolt portaalile esitatavate päringute korral. ID-kaardi kasutamisel päringute signeerimiseks tekib portaali jaoks piisav tõestusmaterjal. Jagatud saladustega autentimise korral tõestusmaterjali aga ei teki. Seega peab juriidilise korrektsuse huvides kodanik vabastama portaali tõestuskohustusest ehk loobuma õigusest päringuid vaidlustada.

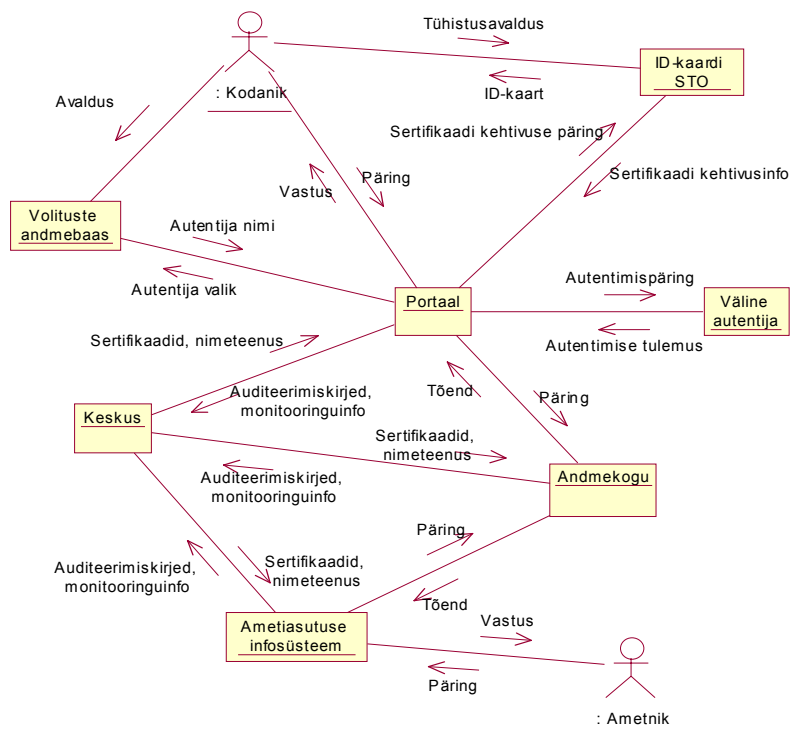
On mõeldav ja mõistlik, et seda tehakse sellesama avaldusega, mille kodanik esitab volituste andmebaasile (registrile).

Portaal peab ka tagama, et kodanikel oleks juurdepääs vaid neile andmetele, mida tal on õigus saada. Ehkki mõnel kodanikul võib näiteks oma ametikohast lähtuvalt olla õigus saada oluliselt rohkem andmeid kui teistel, ei ole otstarbekas kodanikuportaali pääsuõiguste haldust keeruliseks ja ebaturvaliseks ajada ning selliste päringute esitamise võimalust seal realiseerida. Kõige lihtsam ja mõistlikum on realiseerida portaalil vaid selliste päringute esitamise võimalus, mida võib esitada igäüks. Kui kasutada päringu ühe parameetrina päringu esitaja isikukoodi, mille me saame teada autentimisprotseduuri tulemusena, on lihtsalt ja unifikseeritult võimalik realiseerida ka sellised päringud, mis tagastavad andmeid, millele juurdepääs on vaid kodanikul endal.

Portaali jaoks esineb isik vaid eraisiku rollis. Ametniku rolli täitmiseks vajalikud päringud, koos vajaliku pääsuõiguste kontrolli mehhanismiga, realiseeritakse ametiasutuse infosüsteemis. Sellise lähenemise korral muutub kodanikuportaali andmekogude seaduse teise nõudega vastavusse viimine palju lihtsamaks: portaal realiseerib vaid universaalselt lubatud päringud.

5. ARHITEKTUUR

Käesolev peatükk võtab eelnevates peatükkides esitatud arutluste tulemused kokku ühisesse mudelisse, mis kirjeldab demokraatliku riigi põhimõtete vaimus loodud e-Riigi arhitektuuri, mis sobiva juriidilise raamistiku korral võimaldab saavutada soovitud turvaeesmärkide täitmist.



Joonis 11. Süsteemi võimalik arhitektuur

Mudeli (vt joonis 11) võib jagada kolmeks osaks:

- 1) ametiasutuste vahelist suhtlust võimaldav osa;
- 2) kodaniku suhtlust riigiga ID-kaardi abil võimaldav osa;
- 3) kodaniku suhtlust riigiga paroolide abil võimaldav osa.

Ametiasutuste vahelist suhtlust võimaldav osa loob vundamendi teiste osade jaoks ning ilma seda realiseerimata pole võimalik luua võimalusi kodaniku ning riigi vaheliseks suhtluseks. Ülejäänud kaht osa võib vaadelda kui alternatiive, kuid nad võib realiseerida ka paralleelselt. Nad loovad kodanikule võimaluse riigiga elektrooniliselt suhelda, kasutades selleks esimese osa poolt pakutavaid teenuseid, mistõttu nad ei ole realiseeritavad iseseisvalt.

Ametiasutuste vahelist suhtlust võimaldav osa koosneb kolme sorti komponentidest:

- 1) keskus;
- 2) andmekogu infosüsteem;
- 3) ametiasutuse infosüsteem.

Lisaks sellele on vajalik järelvalveasutuse olemasolu, mis ei osale otseselt süsteemi töös ning mida pole seetõttu joonisel kujutatud.

Kodaniku ning riigi vahelise suhtluse jaoks on kindlasti vaja kodanikuportaali, mis vahendab kodaniku päringuid riigi infosüsteemidesse. Lisaks sellele tuleb realiseerida vähemalt üks kahest autentimismeetodist:

- 1) autentimine ID-kaardi abil;
- 2) paroolipõhine autentimine välise autentija abil.

Esimese autentimismeetodi realiseerimine eeldab, et ID-kaardi projekt õnnestub ning kodanikele hakatakse jagama signeerimisvõimelisi kiipkaarte. Täiendav komponent ID-kaardi sertifitseerimisteenuse osutaja näol, mis hakkab jagama kinnitusi ID-kaartidele kantud sertifikaatide kehtivuse kohta, tekib lähtuvalt digitaalallkirja seaduse nõuetest antud projekti väliselt.

Teise autentimismeetodi realiseerimine eeldab spetsiaalse volituste andmebaasi loomist ning kodanike poolt sellele baasile avalduste esitamist millega nad annavad õiguse välisetele, juba eksisteerivatele autentimisteenuse pakkujatele õiguse end autentida.

Kirjeldame kõiki komponente ja nende funktsioone ka lähemalt.

5.1 Keskus

Seda alamsüsteemi on üks. Keskus täidab järgmisi funktsioone:

1. Süsteemiga liitunud infosüsteemide sertifitseerimine. Väljastatavate sertifikaatide arv on väike (võrdeline liitunud süsteemide arvuga), seepärast ei ole erilist mõtet vastavat teenust sisse ostma hakata, ega ka hakata viivitama projektiga, kuni vastav teenus tekib. Kuna väljastatud sertifikaatidest sõltub tekkivate andmete tõestusväärtus, tuleb sertifitseerimise protseduurid täpselt kirja panna ning neid järgida.
2. Nimeteenus. Vajalik alates süsteemi teatud suurusest. Kümnekonna alamsüsteemi puhul ei ole nimeteenus veel vajalik. Nimeteenus peab võimaldama dubleerimist ning tagama edastatava info tervikluse.
3. Monitooring. Keskus peaks pakkuma monitooringuteenust kõigile liitunud asutustele.
4. Auditeerimisserveri teenus. Vajalik logidele tõestusväärtuse andmiseks.

5.2 Ametiasutuse infosüsteem

Neid alamsüsteeme on niipalju kui on ametiasutusi, mis on süsteemiga liitunud. Ametiasutuse infosüsteem:

1. Atesteerib end Andmekaitse Inspektsioonis.
2. Sõlmib keskusega liitumislepingu, saab sertifikaadi, jne.
3. Sõlmib kasutuslepingud teda huvitavate andmekogudega.
4. Autendib oma töötajaid.
5. Esitab päringuid andmekogudesse.
6. Logib nii päringuid kui saadud tõendeid.
7. Edastab keskusele monitooringuinfot.
8. Läbib regulaarseid auditeid.

5.3 Andmekogud

Neid alamsüsteeme on niipalju kui on andmekogusid, mis on süsteemiga liitunud. Ametiasutuse infosüsteem:

1. Atesteerib end Andmekaitse Inspektsioonis.
2. Sõlmib keskusega liitumislepingu, saab sertifikaadi, kanded nimeserverisse, jne.
3. Sõlmib kasutuslepingud ametiasutustega, kes soovivad teda kasutada.
4. Vastab esitatud päringutele.
5. Logib nii saadud päringuid kui väljastatud tõendeid.
6. Edastab keskusele monitooringuinfot.
7. Läbib regulaarseid auditeid.

Olulised andmekogud peavad tagama dubleeritud serverite ning olulistesse võrgusõlmedesse (TIX-LAN) viivate dubleeritud sidekanalite olemasolu.

5.4 Andmekaitse Inspektsioon

(ei osale online töös, ei ole skeemil kujutatud)

Andmekaitse Inspektsiooni funktsiooniks on:

1. Atesteerimine. Süsteemiga liituvate infosüsteemidele liitumisloa andmine.

See funktsioon on tal ka praegu, kuid täielikkuse huvides märkisime selle siin ära.

5.5 Portaal

Kodanikuportaal. Mittekohustuslik element, vajalik kodanike ja riigi vahelise elektroonilise suhtluse võimaldamiseks. Portaal on sarnane ametiasutuse infosüsteemile ja peab läbi tegema kõik needsamad protseduurid. Lisaks on tal järgmised spetsiifilised ülesanded:

1. Sõlmib lepingud väliste autentijatega.
2. Kontrollib volituste andmebaasist autentijate volitusi.

3. Esitab ID-kaardi sertifitseerimisteenuse osutajale *online*-päringuid sertifikaatide kehtivuse kohta.
4. Autendib kodanikke välise autentija või ID-kaardi abil.

Portaal peab tagama dubleeritud serverite ning olulistesse võrgusõlmedesse (TIX-LAN) viivate dubleeritud sidekanalite olemasolu.

5.6 Volituste register

Volituste register on samuti mittekohustuslik element, mis on vajalik siis, kui käivitatakse kodanikuportaal. Pole päris selge, kes peaks seda baasi haldama. Igal juhul on vastava registri olemasolu hädavajalik väliste autentijate kasutamise korral. Kuna tema funktsioonid on tihedalt ja ainult seotud portaali omadega, siis oleks üks ja küllalt mõistlik variant, et volituste register ja portaal on sama asutuse hallata.

Volituste register:

1. Registreerib kodanike avaldusi välise autentija valikuks.
2. Vastab portaali päringutele konkreetset isikut autentida võivate autentijate kohta.

Volituste registrile kehtivad samad käideldavusnõuded mis portaalilegi.

5.7 Väline autentija

Mittekohustuslik element, vajalik siis, kui käivitatakse kodanikuportaal ning kui soovitakse autentida muudmoodi kui ID-kaardiga. Väline autentija:

1. Sõlmib lepingu portaaliga.
2. Sõlmib lepingud kodanikega.
3. Atesteerib end Andmekaitse Inspektsioonis.
4. Vastab portaali poolt esitatud autentimispäringutele.
5. Logib nii saadud päringuid kui väljastatud tööendeid.
6. Edastab keskusele monitooringuinfot.
7. Läbib regulaarseid auditeid.

5.8 ID-kaardi sertifitseerimisteenuse osutaja

Mittekohustuslik element, vajalik siis, kui käivitatakse kodanikuportaal ning soovitakse autentida ID-kaardiga. ID-kaardi STO:

1. Väljastab kodanikule ID-kaardil oleva sertifikaadi.
2. Võtab kodanikult vastu selle tühistusavaldusi.
3. Jagab kehtivuskinnitusi portaalile.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli esitada põhimõtted, millest peaks lähtuma riigi valitsemiskorra muudatuste väljatöötamisel, analüüsida riigi andmekogude digisuhtluse jaoks avamisel tekkivaid turvaproblemeid ja esitada turvaaspektist vastuvõetav e-Riigi ühe alusstruktuuri arhitektuuri mudel.

Esimese sammuna identifitseeriti e-Riigi rajamisel lahendamist vajav põhiprobleem: vastuolu demokraatliku riigi aluspõhimõtetega, mida esitavad olemasolevad seadused, ning pigem kuningriiki meenutava firmakeskkonna jaoks loodud tehnoloogiliste lahenduste vaimu vahel.

Vastuolu lahendamiseks soovitati lähtuda tänapäevase süsteemiarendusteaduse saavutustest ning käivitada arendusprotsess, mis oleks avalik, hästi juhitud ja varustatud, kaasaks laia spetsialistide ringi ning mille tulemuseks oleks vastuolusid mittedalav e-Riigi mudel, mis oleks ühtseks aluseks edasisele arendustööle ning seadusloomele.

Töö põhiosas analüüsiti lähtuvalt eelpoolkirjeldatud ideedest e-Riigi ühe põhikontseptsiooni: riigi andmekogude laialdase digikasutuse, realiseerimisel tekkivaid täiendavaid ohte. Analüüsi tulemused võeti kokku arhitektuuri üldmudelisse.

Lõpetuseks tahab autor veel kord kinnitada, et ta ei arva nagu eksisteeriks mingi üks tehnoloogia või lahendus mille kasutamine garanteeriks e-Riigi loomise projekti õnnestumise. Küll aga on ta veendunud, et eksisteerib terve rida tehnoloogiaid, mille mittekasutamine garanteerib projekti mitteõnnestumise.

Edasised uurimissuunad

Antud tööd võib vaadelda kui kontseptsiooni tõestavat. Kindlasti ei saa töös esitatud analüüsi võtta kui lõplikku, sest ka selle kitsa probleemi adekvaatse analüüs eeldab eri valdkondade spetsialistide tihedat koostööd.

e-Riigi praktiliseks rajamiseks tuleks käivitada hästijuhitud ja –varustatud arendusprojekt, mis toimuks avalikult, kaasaks eri alade parimaid spetsialiste (infotehnolooge, juriste, poliitikuid, majandustegelasi), mille tulemusena tekiks e-Riiki kirjeldav vastuoludevaba mudel.

Saadud mudel on aluseks nii tulevasele seadusloomele, kui ka süsteemiarendusprojektidele, mis hakkavad realiseerima e-Riigi erinevaid alamsüsteeme.

ABSTRACT

This far, the Estonian public administration databases have been kept isolated from each other. The data exchange between them has been slow and inefficient. Fast and reliable data communication networks between state agencies removed the major obstacle on the way of tighter integration of public administration information systems. They have created a possibility to make communication between state agencies faster, safer, and more efficient. To exploit the advantages of new technology, public administration databases should be made accessible not only to one single agency, but rather, to all authorized persons who need that information for doing their jobs more efficiently (and thereby, for improving public services in general). Such a renewed Internet-based public administration is called *e-State*.

In this work, we analyze the security problems that arise when the public administration databases are opened for a widespread electronic access. The analysis is grounded on the current legal situation as defined by Estonian laws. We present separate analysis for agency-to-agency and for citizen-to-public-administration data exchanges. During the analysis we draw an important conclusion that, due to substantially different scopes of risks and the countermeasures available, security solutions developed for business organizations cannot be directly adopted for using them in public administration environment. As a result of the analysis, a model for the e-State architecture is presented that, together with appropriate legal framework, allows us to achieve the main security objectives.

The main idea behind the new architecture is to minimize the number of centralized services. Due to their nature, the coordination and supervision must be centralized. The monitoring service should be centralized due to economical reasons. All other services are decentralized. On the one hand, a decentralized architecture improves the *availability* of the system, since the possibility of communication between two agencies relies only on the information systems of both agencies and on the communication channel between the agencies. On the other hand, it helps to ensure the *integrity* and *confidentiality*, because third parties have no access to data.

We propose to create a public Internet portal for citizens. This portal would allow a citizen to communicate with public administration and state registers. The major security problem in such a portal is user *authentication*. We see the upcoming Estonian electronic ID card as a solution to this problem.

VIITED

1. Abreu, E., Hurts So Good // The Standard veeb (WWW)
<http://www.thestandard.com/article/0,1902,20472,00.html?nl=nr> (01.05.2001)
2. An Introduction To Microsoft .NET // Microsoft Corporation'i veeb (WWW)
<http://www.microsoft.com/net/intro.asp> (01.05.2001)
3. Andmekaitse Inspektsioon // Andmekaitse Inspektsiooni veeb (WWW)
<http://www.dp.gov.ee/> (01.05.2001)
4. Andmekogude seadus // Riigi Teataja I osa (2001) nr 17 (WWW)
<http://seadus.ibs.ee/aktid/rk.s.19970312.108.20000101.html> (01.05.2001)
5. ARIANE 5 Flight 501 Failure // European Space Agency veeb (WWW)
<http://www.esa.int/htdocs/tidc/Press/Press96/ariane5rep.html> (01.05.2001)
6. Buldas, A., Laud, P., Lipmaa, H., Accountable Certificate Management using Undeniable Attestations // 7th ACM Conference on Computer and Communications Security. ACM Press, 2000, lk. 9-18
7. Buldas, A., Laud, P., Lipmaa, H., Villemson, J., Time-stamping with binary linking schemes // Advances on Cryptology -- CRYPTO '98, LNCS v. 1462. Springer-Verlag, 1998, lk 486-501
8. Buldas, A., Lipmaa, H., Schoenmakers, B., Optimally Efficient Accountable Time-Stamping // Public Key Cryptography '2000, LNCS v. 1751. Springer-Verlag, 2000, lk 293-305
9. Common Secure Interoperability V2 Specification // Object Management Group'i veeb (WWW) <http://www.omg.org/cgi-bin/doc?ptc/2001-03-02> (01.05.2001)
10. Consumer Privacy Attitudes and Behaviors // Privacy Leadership Initiative veeb (WWW) <http://www.understandingprivacy.org/content/library/research.cfm> (01.05.2001)
11. Dierks, T., Allen, C., The TLS Protocol Version 1.0, RFC 2246 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc2246.txt> (01.05.2001)
12. Digitaalalkirja seadus // Riigi Teataja I osa (2000) nr 26 (WWW)
<http://seadus.ibs.ee/aktid/rk.s.20000308.22.20001215.html> (01.05.2001)

13. Eastlake, D., Domain Name System Security Extensions, RFC2535 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc2535.txt> (01.05.2001)
14. Eesti Vabariigi põhiseadus // Riigi Teataja (1992) nr 26 (WWW) <http://seadus.ibs.ee/aktid/rh.s.19920628.1.19920703.html> (01.05.2001)
15. e-Maksuamet, Kuidas kasutada? // Maksuameti veeb (WWW) <http://www.ma.ee/ema/kasutamine.shtml> (01.05.2001)
16. e-riik // Eesti riigivõrgu keskuse veeb (WWW) <http://www.riik.ee/et/> (01.05.2001)
17. Freier, A. O., Karlton, P., Kocher, P. C., The SSL Protocol Version 3.0 // Netscape Communications'i veeb (WWW) <http://home.netscape.com/eng/ssl3/draft302.txt> (01.05.2001)
18. Freudenthal, M., Personaalsed turvakeskkonnad. Magistritöö, Tallinna Tehnikaülikool, 2001
19. Hanson, V., Buldas, A., Lipmaa, H., Infosüsteemide turve 2: turbetehnoloogia. Tallinn: Küberneetika AS, 1998. 371 lk.
20. Hanson, V., Infosüsteemide turve 1: turvarisk. Tallinn: Küberneetika AS, 1997. 125 lk.
21. Herbert, D., E-innovation, Estonian-style // Cable News Network LP, LLLP veeb (WWW) <http://europe.cnn.com/2001/WORLD/europe/03/30/estonia.technology/> (01.05.2001)
22. History of Software Engineering // Schloss Dagstuhl veeb (WWW) <http://www.dagstuhl.de/DATA/Reports/9635/report.9635.html> (01.05.2001)
23. Hoffman, P., SMTP Service Extension for Secure SMTP over TLS, RFC 2487 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc2487.txt> (01.05.2001)
24. ID.EE - Eesti ID-programm // ID-kaardi veeb (WWW) <http://www.id.ee/> (01.05.2001)
25. Internet muutub kättesaadavaks igale eestimaalasele // Hansapanga veeb (WWW) <http://www.hansa.ee/et/hp.9c09c905598456f1f279134ab2a13fb8.html> (01.05.2001)
26. Internet Protocol, RFC 791 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc791.txt> (01.05.2001)
27. IP Security Protocol // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/html.charters/ipsec-charter.html> (01.05.2001)
28. IT Baseline Protection Manual: Standard security safeguards // Saksamaa Infoturbeameti veeb (WWW) <http://www.bsi.de/gshb/english/menue.htm> (01.05.2001)
29. Kanellos, M., Former Intel employee admits to computer fraud // CNET Networks, Inc. veeb (WWW) <http://news.cnet.com/news/0-1003-200-2174535.html> (01.05.2001)
30. Kelsey, J., Schneier, Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs // Second International Workshop on the Recent Advances in Intrusion Detection (RAID '99) (WWW) <http://www.counterpane.com/auditlog2.html> (01.05.2001)

31. Kessler, G. C., Defenses Against Distributed Denial of Service Attacks // SANS Institute veeb (WWW) <http://www.sans.org/infosecFAQ/threats/DDoS.htm> (01.05.2001)
32. Kruchten, P., The Rational Unified Process : an introduction. Addison Wesley Longman, 1998. 255 lk.
33. Martens, T., Pildikesi tulevikust ehk ID-kaart tagataskus // Arvutimaailm (2000) nr 5 (WWW) <http://www.am.ee/arhiiv/00-5/martens.htm> (01.05.2001)
34. Marvet, P., Miks peab taotlema digiallkirja kiiret kasutusele võttu? // Äripäeva veeb (WWW) <http://www.aripaev.ee/temp/seminar/29032001/marvet.pdf> (01.05.2001)
35. Microsoft's software secret source codes stolen by computer hackers // Evansville Courier & Press veeb (WWW) http://www.courierpress.com/cgi-bin/view.cgi?200010/27+micro102700_latestnews.html+20001027 (01.05.2001)
36. Mockapetris, P. V., Domain names - implementation and specification, RFC 1035 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc1035.txt> (01.05.2001)
37. Newman, C., Using TLS with IMAP, POP3 and ACAP, RFC 2595 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc2595.txt> (01.05.2001)
38. Pangalingi tehniline kirjeldus // Hansapanga veeb (WWW) <http://www.hansa.ee/et/hp.4e822eef3603eed72ea96da3dff01894.html> (01.05.2001)
39. Rescorla, E., HTTP Over TLS, RFC 2818 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc2818.txt> (01.05.2001)
40. Riigi andmekogude moderniseerimise programm // Eesti riigivõrgu keskuse veeb (WWW) <http://www.riik.ee/ristmik/> (01.05.2001)
41. Schneier, B., Secrets and lies: digital security in a networked world. Wiley Computer Publishing, 2000. 412 lk.
42. Secure Shell // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/html.charters/secsh-charter.html> (01.05.2001)
43. Sertifitseerimise riikliku registri asutamine ja pidamise põhimäärus // Eesti riigivõrgu keskuse veeb (WWW) <http://www.riik.ee/riso/digiallkiri/sertreg.htm> (01.05.2001)
44. Süvari, A., Vedler, S. Krahviperekonnalt varastati maja // Eesti Ekspress (2000) 19. aprill. (E-ajakiri) <http://www.ekspress.ee/arhiiv/2000/16/aosa/kuum3.html> (01.05.2001)
45. Tehniline spetsifikatsioon // Eesti Ühispanga veeb (WWW) <http://www.eyp.ee/pages.php3/0102140201> (01.05.2001)
46. Tervo, T., Single Sign-On Solutions in a Mixed Computing Environment // Helsingi Tehnoloogiaülikooli veeb (WWW) <http://www.hut.fi/~totervo/netsec98/sso.html> (01.05.2001)
47. The e-Citizen, Estonia // Eesti riigivõrgu keskuse veeb (WWW) <http://www.riik.ee/ekodanik/ecitizen.rtf> (01.05.2001)
48. Transmission Control Protocol, RFC 793 // Internet Engineering Task Force'i veeb (WWW) <http://www.ietf.org/rfc/rfc793.txt> (01.05.2001)

49. Vallner, U., SGML formaadiperre lisandub XML - ja muudab maailma! // Eesti riigivõrgu keskuse veeb (WWW) <http://www.riik.ee/xml/xmlam.html> (01.05.2001)
50. Lipmaa, H., Mürk, O., E-valimiste realiseerimisvõimaluste analüüs (WWW) <http://www.just.ee/oldjust/JM/lipmaamyrk.pdf> (01.05.2001)
51. Office of the e-Envoy (WWW) <http://www.citu.gov.uk/> (01.05.2001)
52. CIO's Federal Architecture Working Group (WWW) <http://www.itpolicy.gsa.gov/mke/archplus/group.htm> (01.05.2001)
53. Heeks, R., Understanding e-Governance for Development (WWW) <http://idpm.man.ac.uk/idpm/igov11.pdf> (01.05.2001)
54. Caldow, J., The Quest for Electronic Government: A Defining Vision (WWW) http://www.ieg.ibm.com/thought_leadership/egovvision.pdf (01.05.2001)