e-Governance Academy

Global Information Society Initiative

ID-1 formaadis dokumentide funktsionaalsuse uuring

Tallinn 11.11.–15.12.2013

Sisukord

Kokkuvõte

Töö aluseks oli 7. novembril k.a e-Riigi Akadeemia Sihtasutuse (edaspidi eGA) ja Siseministeeriumiga sõlmitud leping, töö tegemise perioodiks oli 11.11.–15.12.2013. Töö eesmärgiks oli anda sisend ID1 formaadis dokumentide järgmise riigihanke ettevalmistamisse, töö põhiformaadiks oli vastava valdkonna ekspertidega tehtud intervjuud ja ajurünnakud.

Vaatamata ekspertide suurele koormusele aasta lõpus, õnnestus märkimisväärset hulka valdkondlikke eksperte töösse kaasata. Kogutud, süstematiseeritud ja analüüsitud informatsiooni põhjal koostatud ettepanekud on kindlasti abiks hanke ettevalmistamisel. Samas on oluline rõhutada, et iga teema ja ettepanek vajab enne lõplikku otsustamist süvaanalüüsi. Selle töö puhul on tegemist suhteliselt laia spektrisse kuuluvate eksperthinnangute kogumiga.

Kuigi pakkumiskutses on nimetatud lähima kümne aasta visiooni kohta seisukoha kujundamist, võib käesolevat dokumenti käsitleda kui hankesisendit, mille põhjal hakatakse isikutunnistusi välja andma 2017. aastal ning millest tulenevalt on viimased hankespetsifikatsioonile vastavad isikutunnistused käibel veel **2026.–2027**. aastal.

Muudatused, mida eksperdid soovitavad rakendada järgmise isikutunnistuse hanke raames, on järgmised: kontaktivaba kiip numbrite kiirgamiseks, näo- ja sõrmejäljebiomeetria ning permanentsete krüptovõtmete kasutusele võtmine, krüptotugevuse suurendamine, sertifitseerimispoliitika muutmine, hoolduse korraldamine ja muudatuste juhtimiseks sobiva tööjaotuse kehtestamine.

Kiibirakendus peaks elama oma elu sõltumata tema kandjast ehk kiibi valik ja -rakendus peaksid olema oma arendustsüklis.

Muudatuste soovitamisel on silmas peetud ka pikemaajalist kasu ehk võimaluste loomist tulevikulahenduste kasutusele võtmiseks kaardi eluea jooksul.

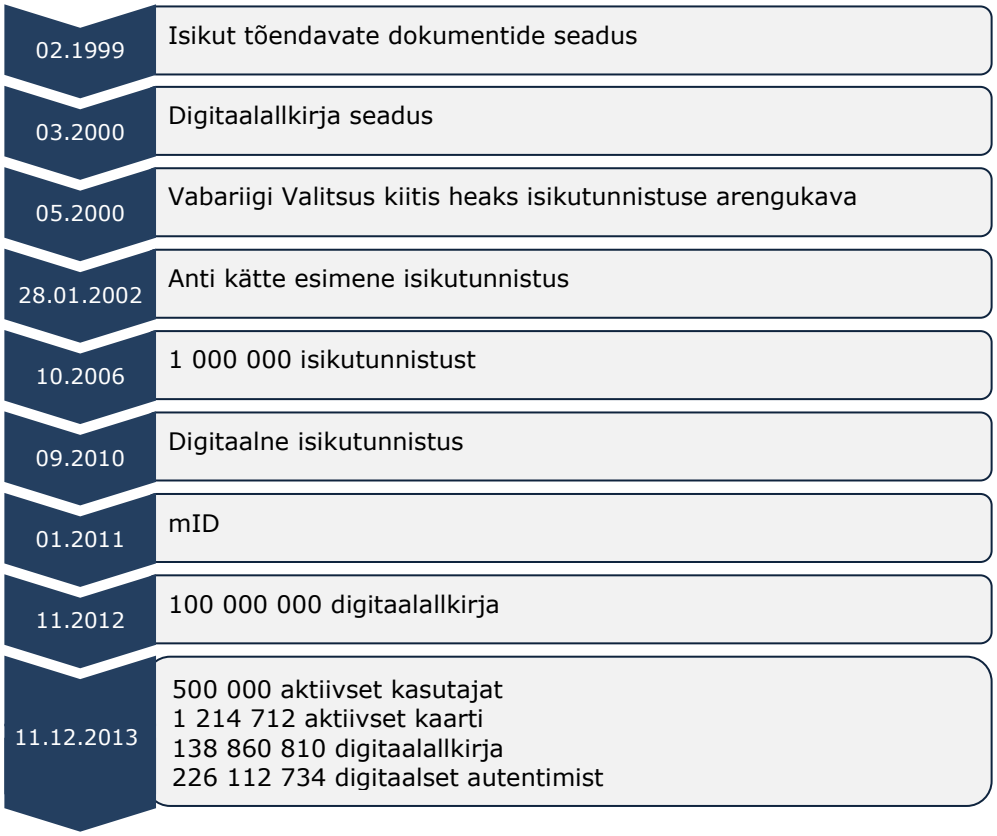
Eksperdid tõid välja ka terve rea kaasnevaid teemasid, mida on märksõnade tasemel kirjeldatud töö lisas, et mitte lasta väärtuslikul informatsioonil kaduma minna. Arvestades valdkonna kiiret arengut, võib mõni nendest ideedest isegi hanke välja kuulutamise ajaks kasutatav olla.

Eksperdid olid ühisel seisukohal, et isikutunnistuse arendamisse tuleb suhtuda teatava konservatiivsusega ja iga otsuse juures tuleb kaaluda selle mõju e-riigi jätkusuutlikkusele, turvalisusele ning kasutajate privaatsusele. Innovaatilisus peaks jääma teenuste arendamise poolele.

Sissejuhatus

Eesti e-riik, mille infrastruktuuri üks baaskomponente on digitaalse identiteedi kandjana isikutunnistus (samuti digitaalne isikutunnistus ja elamisloakaart), on rahvusvaheliselt tunnustatud edulugu.

Alates 28. jaanuarist 2002 on toodetud üle miljoni isikutunnistuse ning seda kasutades on antud peaaegu 140 miljonit digitaalallkirja ning oma isikut on tuvastatud üle 225 miljoni korra[1] (vt joonis 1).



Joonis 1. Olulised sündmused digitaalse dokumendi arenguloos.

Alates 2011. aastast antakse Eestis kehtiva elamisloa või elamisõiguse alusel püsivalt elavale või rahvusvahelise sõjalise koostöö seaduse alusel viibivale kolmanda riigi kodanikule välja elamisloakaarti.

Analüüsimisel on lähtutud pakkumiskutses kirjeldatud Eesti isikut tõendavate dokumentide ning identiteedihalduse poliitika kontseptsioonist, mille keskmes on järgmised põhimõtted:

- riigi monopol ja vastutus isiku tõsikindlal tuvastamisel,
- tsentraliseeritud identiteedihaldus,
- põhimõte „1 isik = 1 identiteet“,

[1] http://www.id.ee.

- digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavate sertifikaatide ühene seotus dokumendi kasutajaga,
- digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavate sertifikaatide avalik kontrollitavus isikukoodi kaudu.

Töö raames ei tegeletud *European Citizen Card* (ECC) temaatikaga ja jätkuvalt menetluses oleva uue usaldusteenuste regulatsiooni projektiga[2]. Eksperdid hindavad erinevalt selle projekti võimalikku mõju kehtima hakkamisel. Osa eksperte arvab, et mõju ei ole tegelikult märkimisväärne, sest liikmesriikidele jäetakse piisav otsustusvabadus. Osa eksperte on seisukohal, et regulatsiooni mõju saab olema suur, sest määrus kehtestab, milliseid identiteete peame usaldama ning millist digitaalallkirja formaati peab kasutama.

Pakutud lahendused aitavad ellu viia Vabariigi Valitsuse tegevusprogrammi peatüki „E-riigist I-riigiks" punkti 2 alapunktide a ja c[3] märgitud tegevusi ning saavutada infoühiskonna arengukavas aastaks 2020 sätestatud eesmärke.

Isikutunnistusel kui Eesti e-riigi infrastruktuuri olulisel baaskomponendil on ülim tähtsus Eesti kui eduka e-riigi rahvusvahelise kuvandi jätkusuutlikkuse tagamisel. Iga isikutunnistusega seotud areng mõjutab kogu Eesti ühiskonda – nii üksikisikuid, riigi- ja ärisektorit kui ka vabakonda ning Eesti rahvusvahelist mainet. Riskidest on rahvusvahelise renomee tõttu eriti olulised maineriskid.

Eksperdid on seisukohal, et Eesti võiks võtta enda peale rohkem e-riigi rahvusvahelise arenduskeskuse rolli, näiteks rahvusvahelist nime *EuroDoc* kandva baastarkvara arenduskeskuse rolli.

[2] *Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Brussels, 4.6.2012. COM(2012) 238 final. 2012/0146 (COD)* // asendaks *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.*

[3] Vabariigi Valitsuse tegevusprogramm 2011−2015. Punkt 2a: „Muudame e-teenused mugavateks ja inimsõbralikeks i-teenusteks, kujundades eesti.ee kodanikele käepäraseks ja ligitõmbavaks võrgu kaudu pakutavate avalike teenuste väravaks, võimaldamaks arukat ja otstarbekohast dialoogi riigi ja kodanike vahel.". Punkt 2c: „ID-kaart ja mobiil-ID peavad tagama turvalise ligipääsu igale Eestis pakutavale teenusele."

Uuringu metoodika

Arvestades ajaraamistikku nii pakkumuse ettevalmistamiseks kui ka rakendusuuringu läbiviimiseks, tehti eGA uuring järgnevalt kirjeldatud metoodika alusel.

Pärast lepingu sõlmimist koostati ja lepiti kohe kokku intervjueeritavate nimekiri ja allikate esmane nimekiri. Järgnevalt toimus töö allikatega sellises ulatuses, mis oli vajalik intervjuude ettevalmistamiseks ja läbiviimiseks.

Seejärel alustati intervjuude tegemist. Kokku tehti enne esimest ajurünnakut viis intervjuud.

Intervjuude ja täiendava allikate läbitöötamise tulemusena valmistati ette ajurünnak, millest kutsuti osa võtma Siseministeeriumi haldusala, Riigi Infosüsteemi Ameti (edaspidi: RIA), Trüb AG (edaspidi: Trüb), ASi Sertifitseerimiskeskus (edaspidi: SK) ja eGA eksperdid, kokku osales üheksa eksperti. Ajurünnak kestis kolm tundi ja selle tulemuseks oli esmane visioon ja sisend aruande vaheversiooni koostamiseks.

Ajurünnakule järgnes selle tulemuste analüüs ja täiendav allikate läbitöötamine ning seejärel valmistati ette teine ajurünnak, millest osavõtjad ja korraldus oli samalaadne kui esimese ajurünnaku puhul. Võrreldes esimese ajurünnakuga, olid esimest korda esindatud AS Datel ja AS SignWise, kokku osales kaheksa eksperti. Teise ajurünnaku tulemus oli sisendiks lõpparuande koostamisele.

Jätkusid intervjuud ja lisaks esimesele viiele intervjuule küsitleti veel 12 eksperti.

Seejärel vormistati lõpparuanne ning koguti ekspertidelt ettepanekuid.

Intervjuude, ajurünnakute või kommentaaride vormis andsid oma sisendi 25 eksperti: Arne Ansper (Cybernetica), Kalle Arula (RIA), Erki Arus (SMIT), Hannes Astok (eGA), Mark Erlich (RIA), Agu Kivimägi (SMIT), Helar Laasik (PPA), Andreas Lehmann (Trüb), Agu Leinfeld (Datel), Silvia Lips, Tarvi Martens (SK), Arvo Ott (eGA), Kalev Pihl (SK), Raul Rikk (eGA), Tiit Roosik (PPA), Mari Pedak (eGA), Jaan Priisalu (RIA), Kaido Raiend (SEB), Ott Sarv (SignWise), Ivar Tallo (eGA), Anto Veldre (RIA), Rene Vihalem (SM), Linnar Viik.

15. detsembril esitati aruanne Siseministeeriumile.

Digitaalsete dokumentidega seotud teenused

Isikutunnistus võimaldab tarbida järgmisi teenuseid: füüsiline tuvastamine (sh reisimisel Euroopa Liidu piires on tegemist reisidokumendiga), digitaalne tuvastamine, autentimine, digitaalallkirja andmine, krüpteerimine/dekrüpteerimine. Digitaalne isikutunnistus võimaldab tarbida ühe teenuse vähem – seda ei saa kasutada isiku füüsiliseks tuvastamiseks. Elamisloakaart võimaldab tarbida järgmisi teenuseid: füüsiline tuvastamine, digitaalne tuvastamine, autentimine, digitaalallkirja andmine, krüpteerimine/ dekrüpteerimine. Mobiil-ID abil saab ennast digitaalselt tuvastada, autentida ja anda digitaalallkirja.

Praegusel ajal on Eesti elanike identiteeti[4] kandvate digitaalsete dokumentidena kasutusel plastikkaardid (isikutunnistus, digitaalne isikutunnistus, elamisloakaart) ja mobiiltelefon (mobiil-ID).

Rääkides digitaalse dokumendi tulevikust, tuleb kõigepealt küsida, **milliseid teenuseid me tulevikus digitaalse dokumendiga seostame.**

1990.−2000. aastatel toimus Eestis diskussioon, milliste teenuste ja millise informatsiooni kandja peaks isikutunnistus olema. Isikutunnistus arendati välja põhimõttel, et kaardil endal on minimaalselt isikuinformatsiooni ja et tegemist on eelkõige e-riigi infrastruktuuri komponendi ehk infrastruktuurse teenusega – isikutunnistus võimaldab tarbida tuhandeid e-teenuseid. Sama põhimõte jäi kehtima ka hiljem välja arendatud digitaalse dokumendi kontseptsioonis.

Käesoleva töö tegemisel arutati teenuse vaadet ajanappuse tõttu üsna põgusalt. Muudatusettepanekud käsitlesid ainult krüpteerimisfunktsiooni (alates sellest loobumisest ja lõpetades permanentse krüpteerimisvõtme loomisega). Krüpteerimisfunktsioon on tegelikult kaasnev ja üsna vähe kasutatud funktsioon.

Seega võiks põhiteenuste pakett jääda traditsiooniliseks ja diskussiooniobjektiks võiks olla teenuste osutamise viis (alates digitaalse identiteedi kandjast ja lõpetades järelevalvega).

Identiteet ja autentimisteenus

Eesti digitaalne identiteet on kujundatud ümber Eesti isikukoodi[5]. Kasutusel olev lahendus võimaldab ühetaolist isikutuvastamist.

[4] Töö räägib füüsilistest isikutest. Lisatud tulevikuideede juures on põgusalt puudutatud ka juriidilisi isikuid.

[5] Töö kontekstis ei saa Eesti isikukoodi teemat lühidalt käsitlemata jätta, kuna see mõjutab otseselt nii teenuste kui ka kasutatavate tehniliste lahenduste valikult.

Eelkõige rahvusvaheliselt, vähemal määral riigisiseselt on tekitanud diskussiooni või lausa vastuseisu delikaatsete isikuandmete kasutamine isikukoodis. Me ei pea vajalikuks sekkuda sellesse diskussiooni, seda eriti riigi poolt osutatavate teenuste kontekstis.

Samas on märkimisväärse hulga teenuste puhul isikutel huvi ja õigus jääda anonüümseks, mida praegu pakutav autentimisviis ei võimalda – sertifikaatides sisaldub isikukood. Juba praegu on sellel põhjusel paralleelselt kasutusele võetud anonüümseid autentimisvahendeid, mis omakorda vähendab riigi poolt pakutavate lahenduste kasutatavust. Tulenevalt sellest on allpool välja pakutud suurema anonüümsusega autentimisvõimaluse lisamine (vt numbrite kiirgamise funktsionaalsus).

Ka isikutunnistuste maailmas on suund eri tugevusega autentimist võimaldavatele kaartidele (kaartide mitmekesisus). Lisaks riigi poolt välja antavatele digitaalsetele dokumentidele on tekkinud vajadus eelkõige korporatiivsete kaartide järele. Hea näide selles valdkonnas on SEBi töötõend[6], mille digitaalne funktsionaalsus erineb riiklikust ainult sellevõrra, et neid ei saa kasutada e-valimistel[7].

Eesti.ee keskkond (*single point*) peaks kajastama kõiki inimese digitaalseid dokumente (nii riigi- kui ka erasektori poolt välja antavaid). See välistaks/vähendaks identiteedivargusi. Vastasel juhul on olemas lihtne võimalus digitaalsete variidentiteetide loomiseks.

Eksperdid tõid välja tõsise vajaduse n.ö **testkodaniku[8]** loomiseks. Mistahes uute lahenduste loomine eeldab tänapäeval enne töökeskkonda lubamist tõsiseid testimisi, mida praegusel ajal saab teha ainult reaalsete isikute isikut tõendavaid dokumente kasutades (mis ei ole mõistlik) või toimub osa katsetusi alles töökeskkonnas (mis ei ole lubatav).

[6] Vt SEBi turvajuhi Kaido Raiendi ettekannet Sertifitseerimiskeskuse 2013. aastakonverentsil: https://www.sk.ee/upload/files/AK2013_Kaido%20Raiend_SEB%20t%C3%B6%C3%B6t%C3%B5endist.pdf

[7] Valimistel saab oma isikut tõendada digitaalset tuvastamist võimaldava sertifikaadiga, mis on välja antud isikut tõendavate dokumentide seaduse alusel.

[8] Testkodanikul peaksid olema võimalikult pikk nimi ja eesnimi, mis sisaldaksid kõiki keerukamaid tähti (näiteks õ, ä, ö, ü, x, y, z), samuti peaks tal olema isikukood, mille alusel saaks toota testkaarte.

Ettepanekud muudatusteks, mida tuleks järgmise hanke ettevalmistamise protsessis analüüsida

Aruande selles peatükis käsitletakse võimalikke muudatusi, mida eksperdid soovitavad rakendada järgmise isikutunnistuse hanke raames: kontaktivaba kiip numbrite kiirgamiseks, näo- ja sõrmejäljebiomeetria ning permanentsete krüptovõtmete kasutusele võtmine, krüptotugevuse suurendamine, sertifitseerimispoliitika muutmine, hoolduse korraldamine ja muudatuste juhtimiseks sobiva tööjaotuse kehtestamine.

Muudatuste soovitamisel on silmas peetud ka pikemaajalist kasu ehk võimaluste loomist tulevikulahenduste kasutusele võtmiseks kaardi eluea jooksul.

Kontaktivaba kiip

Isikutunnistusele on vaja uut liidest, mis annaks täiendavaid kasutusvõimalusi. See looks teenusepakkujatele uusi võimalusi mugavamate teenuste arendamiseks. Oluline on ka isikutunnistuse ja mobiiltelefoni suhtlemisvõimaluseks eelduse loomine.

Isikutunnistusel ja digitaalsel isikutunnistusel praegusel ajal kontaktivaba kiipi ei ole. Elamisloakaardil on kaks kiipi: üks kontakt- ja teine kontaktivaba kiip – seega oleks uue kiibi lisamisel kontaktivabasid kiipe kaks. Tehniliselt on see teostatav. Analüüsi käigus esitati ka küsimus, kas selline tehniliste lahenduste lisamine on ka õiguslikult lubatav, ning leiti, et Euroopa Liidu õigusaktid toetavad liikmesriikide poolt täiendavate funktsionaalsuste lisamist[9]. Sõltuvalt kontaktivabas kiibis kasutatavate rakenduste olemusest võib tekkida oht, et seni numbrite kiirgamisel anonüümsust kindlustav kaart võib anonüümsuse kaotada ehk selles osas kompromiteeruda.

[9] Elamisloakaardi vormi tehnilised nõuded tulenevad Euroopa Liidu Nõukogu määrusest (EÜ) 1030/2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks (EÜT L 157, 15.06.2002, lk 1–7) ja eelnimetatud määruse muudatusest (EÜ) 380/2008 (ELT L 115, 29.04.2008, lk 1–7). Euroopa Liidu Nõukogu määruse (EÜ) 380/2008 lisa 1 kohaselt võivad liikmesriigid andmeid salvestada raadiosageduskiibile või lisada elamisloale riigisiseseks kasutamiseks alternatiivliidese või eraldi kontaktkiibi, mis paikneb loa tagaküljel ning mis vastab ISO standarditele ja ei takista mingil moel raadiosageduskiibi kasutamist. Määruse artikli 1 punkti 4 kohaselt võivad liikmesriigid eelnimetatud kiibile salvestada andmeid e-teenuste, näiteks e-valitsuse ja e-äri jaoks ning samuti elamisloaga seonduvaid täiendavaid andmeid, kuid eelduseks on kogu siseriikliku teabe loogiline eraldamine biomeetrilistest andmetest. Määruse preambula punktis kuus on samuti nenditud, et lihtsustada tuleks sellistele uutele tehnoloogiatele nagu e-valitsusele ja e-teenustele juurdepääsuks kasutatava digitaalallkirja kasutamist, andes liikmesriikidele võimaluse kasutada elamislubades sel eesmärgil biomeetriliste tunnuste lisamiseks kasutatavat andmekandjat või täiendavat andmekandjat. Seega toetavad Euroopa Liidu õigusaktid liikmesriikide poolt täiendavate funktsionaalsuste lisamist.

Isikutunnistusele lisatava kontaktivaba kiibi kasutusvaldkondadest analüüsiti **numbri(te) kiirgamise** ja sertifikaatide kandmise funktsionaalsust ja enamik eksperte soovitas lähitulevikus piirduda neist esimese kasutusele võtmisega[10].

Kontaktivaba autentimislahendust võimaldava tehnoloogia NFC (*Near Field Communication*) kasutusnäited Eestis on EMT juhtimisel välja töötatud rakendus „Minu rahakott"[11] ja Tallinna ühiskaart.

Kiip on tehniline lahendus ja kiibi rakendus peaks elama oma elu sõltumata tema kandjast, seega kiibi valik ja rakendus peaksid olema oma arendustsüklis.

Numbrite kiirgamise funktsionaalsus

Kontaktivaba kiip numbrite kiirgamiseks ehk teisisõnu kliendikaardi funktsionaalsus on laialdaselt ja edukalt kasutusel.

Olulisem kui tehnilised küsimused on privaatsuse teema – kas teenuse kasutaja saab jääda anonüümseks või on ta jälitatav[12]. Jälitatavus ehk isiku seostamine välistatakse, kui iga transaktsiooni korral genereeritakse uus number (nii toimub see elamisloakaardi kasutamisel). Selline lahendus ei võimalda aga osutada püsiteenuseid ehk teisiti öeldes anda isikule mingeid püsivaid volitusi. Seda lahendust eksperdid ei toeta. Püsiva teenuse osutamist ja jälitamist mittevõimaldav lahendus on persistentsete numbrite kasutamine teenuse osutamisel, kusjuures seost inimese ja numbri vahel teab ainult numbri väljastaja (eeldab vastava andmekogu olemasolu). Selline funktsionaalsus võimaldaks inimesel tarbida teenuseid, mille puhul inimene soovib teenuse osutaja juures säilitada anonüümsust.

Teenusepakkuja tuvastab üldjuhul ühel või teisel moel isiku ja teeb püsikliendile reklaami saatmiseks kindlaks tema nime ja aadressi (erandiks on mitteisikustatud ühiskaart). Aga ta ei pea teadma isikukoodi. Risk ei ole niivõrd selles, et teenuseosutaja isiku tuvastab, vaid selles, et juhul, kui teenuseosutajatele on kättesaadav isiku unikaalne number, siis saavad nad andmeid (omavahel) ristata.

Numbrite kiirgamise funktsionaalsus võib olla kas püsiv, aktiveeritav või väljalülitatav. Eksperdid soovitavad inimestele valikuvabaduse loomist. Aktiveeritava funktsionaalsuse

[10] NFC sertifikaatide kandmise funktsionaalsuse kasutusele võtmist on käsitletud lisas „Ideed kaugemaks tulevikuks".

[11] Uudse makselahenduse kasutusele võtmiseks viisid Eesti juhtivad pangad ja tehnoloogiaettevõtted läbi rakendusuuringu, et otsida viise, kuidas võtta Eestis kasutusele NFC tehnoloogia. Sellele järgnes pilootprojekt, millega katsetati uudset makselahendust, kus pangakaardil olevad kiibi funktsioonid on tõstetud mobiiltelefoni SIM-kaardi kiibile. Projekti tulemusena võib pangaklient sooritada igapäevaseid kaardimakseid tavapärase plastikust pangakaardi asemel hoopis mobiiltelefoni vahendusel. Vt ka Marko Palmi artiklit „Mis on NFC ehk lähiväljaside?" (Mobiilne rahakott – „Minu rahakott"). Infotark 03.02.2013".

[12] Eestis praegu kasutusel olev sertifikaatide tüüp anonüümsust ei võimalda. Teenuse osutaja saab kergesti teenuse tarbija sertifikaatidel oleva informatsiooni põhjal tema isiku tuvastada.

korral seisneb inimese valikuvabadus otsuses funktsionaalsus kasutusele võtta või mitte. Väljalülitatava funktsionaalsuse korral saab inimene otsustada seda funktsionaalsust mitte kasutada (tehniliselt saab funktsionaalsuse hävitada/sulgeda, aga uuesti seda kasutusele võtta ei saa ehk siis vastav otsus oleks kaardi eluea mõttes lõplik).

Kaaluti ka mitme numbri kiirgamise võimalust, mida saaks kasutada erinevate teenusepakkujate juures (pangas, poes jne). Esimesel pilgul välistaks see kaardi inimesega seostamise ka siis, kui mõni teenusepakkuja isiku mingil moel siiski tuvastab – kasutusele võetakse uus number. Pikemas perspektiivis ei ole see siiski mõistlik lahendus, sest püsinumbrite korral, olgugi neid mitu, saadakse seosed ikkagi varem või hiljem teada.

Poolt: Mugavus. Transaktsioonikiirus.

Riskid: 1. Jälitamisvõimalus (keskmine risk, maandamismeetmed: a) valitakse vähem riskantne lahendus; b) luuakse funktsionaalsuse väljalülitamise võimalus). 2. Tehniline keerukus teise kiibi näol (madal risk). 3. Elamisloa anonüümsuse kompromiteerimine (kõrge risk, maandamismeede: a) valitakse vähem riskantne lahendus; b) luuakse funktsionaalsuse väljalülitamise võimalus).

Biomeetriliste tunnuste kasutusele võtmine

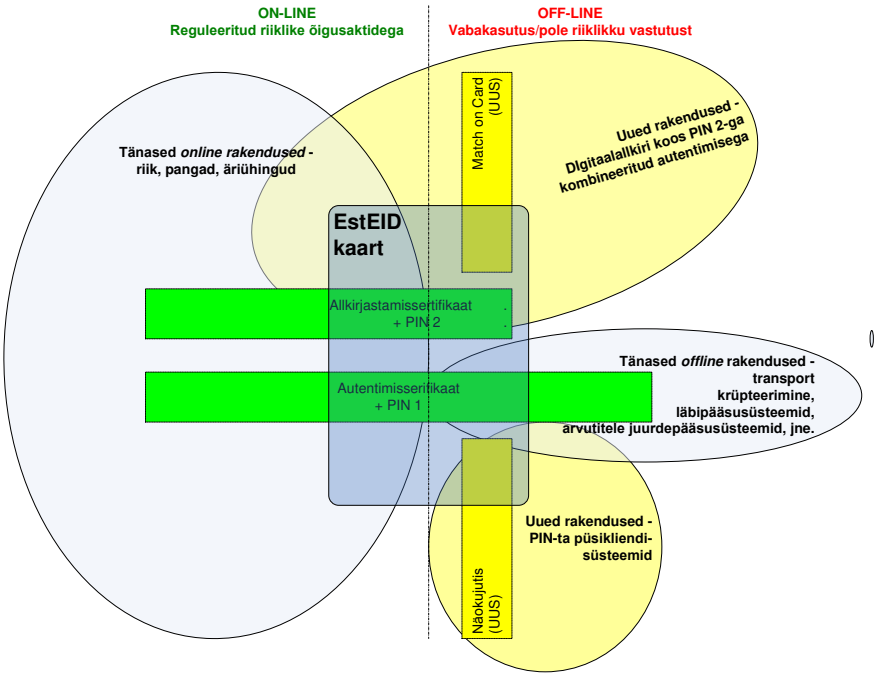
Biomeetriliste tunnuste laiemaks kasutamiseks isikutuvastuses tuleb luua täpsustatud regulatsioon identiteedihalduseks ja isikutuvastuse (riiklikuks) menetluseks, millele tuginedes saab toimuda tuvastamiseks vajalike andmete hõive.[13] Oluline on arvestada, et biomeetriliste tunnuste kasutamine iseenesest ei taga suuremat turvalisust, sest paljusid biomeetrilisi andmeid saab koguda ilma asjaomase isiku teadmata.

Eesmärgi piiramise põhimõtet tuleb järgida koos muude andmekaitse põhimõtetega ning eriti tuleb meeles pidada **proportsionaalsuse**, **vajaduse** ja andmete **minimeerimise** põhimõtet, kui määratakse mõne rakenduse erinevaid eesmärke. Kuna biomeetrilisi andmeid tohib kasutada ainult juhul, kui need on piisavad, asjakohased ja mitte ülemäärased, eeldab see töödeldud andmete vajaduse ja proportsionaalsuse ranget hindamist ja otsustamist, kas kavandatud eesmärgi saab saavutada vähem sekkuval viisil. Kavandatava biomeetrilise süsteemi proportsionaalsust analüüsides on kõige tähtsam kaalutlus see, kas süsteem on kindlaksmääratud vajaduse rahuldamiseks vajalik ehk kas see on oluline vajaduse rahuldamiseks või on see pigem kõige mugavam või kulutasuvam. Teine tegur, mida tuleks kaaluda, on see, kas süsteem on vajaduse rahuldamisel

[13] Isikutuvastuses identiteedihalduse ja isikutuvastuse riikliku menetluse rakendamine eeldab põhjalikumat juriidilist analüüsi ning tähendab ulatuslikumaid muudatusi õigusaktides või isegi täiesti uute normatiivaktide väljatöötamist. Praegu isikutuvastust kui eri menetluse liiki õigusaktide tasandil ei käsitleta. Kindlasti tuleb lahendada hõivatud isikuandmete (sh biomeetriliste andmete) kasutamise, säilitamise, ligipääsu jmt õiguslikud küsimused. Kas on tegemist eraldi andmebaasiga, kas toimub andmete ristkasutust teiste andmebaasidega jne.

tõenäoliselt tulemuslik, arvestades biomeetrilise tehnoloogia, mida kavatsetakse kasutada, erilisi omadusi. Kolmas kaalutav tahk on, kas kaasnev eraelu puutumatuse taseme langemine on proportsionaalne oodatava kasuga. Kui kasu on suhteliselt vähene, nagu mugavuse suurenemine või väike kulude kokkuhoid, ei ole eraelu puutumatuse taseme langemine asjakohane. Neljas aspekt biomeetrilise süsteemi sobivuse hindamisel on kaaluda, kas vähem eraellu sekkuvad vahendid võiksid saavutada soovitud tulemuse[14].

Isiku biomeetriliste andmete hõive toimuks kas kaardile ja/või andmekogusse ja neid saaks kasutada isikute tuvastamiseks järgmiselt: a) (riikliku) isikutuvastuse menetluse käigus; b) e-teenuste tarbimise jaoks sõltumata teenuseosutajast.



Joonis 2. Biomeetriliste tunnuste kasutusele võtmine isikutunnistusel võimaldab luua uusi rakendusi[15].

Enamlevinud ja odavamad isikutuvastuses kasutatavad biomeetrilised indikaatorid on sõrmejälgede kujutised ja näokujutis. Biomeetriliste tunnuste kasutusele võtmine isikutunnistusel loob võimaluse luua uusi rakendusi (vt joonis 2).

Sõrmejäljebiomeetria

Sõrmejälgede biomeetria valdkonnas on laialdast levikut leidnud ***Match-on-Card*** **(MoC)** kontseptsioon. MoC on sõrmejälgede kaartidel hoidmise ja võrdlemise kontseptsioon, mis

[14] Arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta. 00720/12/ET. WP 193. Artikli 29 alusel asutatud andmekaitse töörühm. Vastu võetud 27. aprillil 2013.

[15] Joonis: Trüb Baltic.

tõendab kaardiomaniku füüsilist kohalolekut ja tagab selle abil turvalise isikutuvastuse[16]. MoC on mitmete riikide rahvuslikel isikutunnistustel kasutusele võetud (Euroopas näiteks Portugalis). MoC kasutusele võtmise tagajärjel hoiab USA Riigidepartemang aastas ühe kasutaja kohta kokku 200 USD, kuna enam ei ole vaja käigus hoida salasõnade haldamise, sh uuendamise süsteemi, sest 30% kasutajatoe mahust oli salasõnadega seotud abi[17].

Poolt: 1. MoC võimaldab spetsiaalse lugeja[18] vahendusel tuvastada kaardiomaniku füüsilist kohalolekut ja tagab isiku tõsimeelset tuvastamist, mille kaudu a) väheneb identiteedivarguste ja -pettuste hulk; b) suureneb turvalisus; c) tekitatakse jälg ja auditeeritavus; d) suureneb kuluefektiivsus; e) säilitatakse kasutaja privaatsust; f) suureneb kasutajamugavus. 2. MoC ei vaja reaalajas ühendust ühegi andmebaasiga ehk on mõeldud kasutamiseks *offline*. Sõrmejäljekujutisi säilitatakse turvaliselt kiibis. 3. Sellise lahenduse kasutuselevõtmine on vajalik kõrgemat autentimistaset nõudvate teenuseosutajate (pangad, telekommunikatsiooniettevõtted jt) jaoks.

Riskid: 1. Vajadus spetsiaalsete lugejate järele, mis vähendavad kasutajamugavust ja ei ole odavad (keskmine risk, maandamismeetmed: kõrgemat autentimistaset nõudvad teenuseosutajad võimaldavad klientidele lugejaid tasuta või kasutatakse neid teenuseosutaja juures kohapeal). 2. Kohe ei ole palju kasutusvõimalusi (kõrge risk, maandamismeetmeks rakendamine ainult digitaalsel isikutunnistusel).

Näobiomeetria

Praegu ei ole Eesti isikutunnistuste kiibis biomeetrilist **näotuvastust** võimaldavat informatsiooni, samas on kontaktkiibis selleks piisavalt ruumi juba praegu. Tegemist on kõige odavama biomeetrilise indikaatoriga, mis on leidnud laialdast kasutamist. Seda tehnoloogiat on integreeritud *online*- ja mobiilsideteenustesse üksikisikute identifitseerimiseks, autentimiseks/kontrollimiseks või kategoriseerimiseks. Mitte väga ammu kuulus selline tehnoloogia ulmevaldkonda, kuid nüüd kasutavad seda nii avalikud kui ka eraorganisatsioonid.

Poolt: 1. Võimaldab kaamera vahendusel tuvastada kaardiomaniku füüsilist kohalolekut ja tagab isiku tõsimeelset tuvastamist, mille kaudu a) väheneb identiteedivarguste ja -pettuste

[16] Vt http://www.matchoncard.com/what-is-moc-

[17] http://www.matchoncard.com/references/case-studies/employee-id.

[18] Hetkel turul u 100 €.

hulk; b) suureneb turvalisus; c) tekitatakse jälg ja auditeeritavus; d) suureneb kuluefektiivsus; e) säilitatakse kasutaja privaatsus; f) suureneb kasutajamugavus. 2. Ei vaja reaalajas ühendust ühegi andmebaasiga ehk on mõeldud kasutamiseks *offline*. Näokujutisi säilitatakse turvaliselt kiibis. 3. Sellise lahenduse kasutuselevõtmine on vajalik kõrgemat autentimistaset nõudvate teenuseosutajate (pangad, telekommunikatsioonieettevõtted jt) jaoks.

Riskid: 1. Vajadus kaamera järele (madal risk: kaamerad on sotsiaalmeedias laialdast rakendust leidnud, samuti on uutel arvutitel kaamera juba sisse ehitatud). 2. Mainerisk, kui tuvastamine kaamera halva kvaliteedi tõttu ebaõnnestub. 3. Andmekaitselised riskid on kirjeldatud Euroopa Liidu asutamiselepingu artikli 29 alusel asutatud andmekaitse töörühma poolt ja siinkohal neid korrata ei ole otstarbekas[19].

Biomeetriliste tunnuste kasutusviisid

Isikutunnistuse uuendamisel tuleks tõsiselt kaaluda kas riikliku tuvastusteenuse loomist, mille korral toimub võrdlus riikliku andmebaasiga, või biomeetrilise autentimisvõimaluse loomist, mille puhul toimub võrdlus kiibil oleva malliga.

Praegu Eesti e-riigis kasutusel olevad tuvastamisvõimalused ei taga (eriti distantsilt) tõsikindlat teadmist, kes neid vahendeid ja nendega seotud teadmisi tegelikult kasutab.

Riiklik isikutuvastuse teenus

Nagu eespool öeldud, saab tuvastamisel andmeid võrrelda andmebaasiga ehk tegemist on biomeetrilise tuvastamisega: üksikisiku tuvastamine biomeetrilise süsteemiga on tavaliselt protsess, kus võrreldakse üksikisiku (tuvastamise ajal saadud) biomeetrilisi andmeid paljude biomeetriliste mallidega, mida säilitatakse andmebaasis (s.o üks mitmele tuvastusprotsess). Selline lahendus sobiks riiklikule tuvastusteenusele. Biomeetrilised andmed kogutakse ja säilitatakse riiklikus andmekogus ning neid kasutatakse tuvastusteenuse osutamisel. Näopildi tuvastamiseks riiklikus autentimisportaalis küsitakse PIN-i, genereeritakse näopilt (*videostream* serverisse) ja võrreldakse. Riik osutab teenust, mida e-teenuse osutajad riigilt saavad/ostavad.

Biomeetriliste tunnuste kontroll autentimisel

Samuti on olemas lahendused biomeetriliseks kontrollimiseks või autentimiseks: üksikisiku kontroll biomeetrilise süsteemiga kujutab endast tavaliselt üksikisiku biomeetriliste (kontrolli ajal saadud) andmete võrdlemist ühe biomeetrilise malliga, mida säilitatakse seadmes (s.o üks ühele tuvastusprotsess). Selline lahendus sobib kasutamiseks eelkõige teenuse osutamisel kohapeal. E-teenuste osutajatele tekib võimalus turvaliste lahenduste

[19] Arvamus 02/2012 näotuvastuse kohta *online*- ja mobiilsideteenuste puhul. 00727/12/ET. WP 192. Arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta. 00720/12/ET. WP 193.

otsimiseks. Sellisel juhul on biomeetrilised andmed identiteedikandjal (isikutunnistuse kiibil) ning igal teenuseosutajal on võimalus nõuda biomeetrilist autentimist.

Tegemist oleks autentimisvõimaluste mitmekesistamise ehk tugevama autentimisvõimaluse loomisega, kus lisaks PIN-ile saab võrrelda ka biomeetrilisi tunnuseid nagu sõrmejäljed (ei anna palju juurde, sest on madalama turvatasemega) ja näobiomeetria (oluliselt kergemini rakendatav).

Mitmeastmeline tuvastamine ei ole kõigis menetlustes/kontaktides vajalik. Ainult osa tehingute juures on mõistlik autentimisel kasutada kõrgemat turvataset.

Krüptotugevus[20]

Möödapääsmatu vajadus on suurendada krüptotugevust[21]. Digitaalsetes dokumentides kasutusel olev lahendus toetab ainult RSA operatsioone, mis isegi praegusel ajal ei ole rahuldav. Järgmise hankega tuleb luua elliptiliste kõverate kasutamise võimekus. Võimalikult kiiresti tuleb käibelt ära saada 1024 RSA-ga kiibid. 2048 RSA turvalisust hinnatakse ainult mõne aastaga. Uue hanke tulemusena hakatakse isikutunnistusi välja andma alles 2017. aastast kuni 2022. aastani, järelikult on sellel perioodil välja antud isikutunnistused ringluses kuni 2027. aastani. Sellises perspektiivis ei ole võimalik ennustada, millised (tehnilised) lahendused on turvalised.

Riskide maandamiseks tuleks kohe kasutusele võtta n.ö **varuvõimekusega kiip**[22] (kiip peab tulevikus olema valmis toetama tugevamat krüptograafiat). Üks võimalus ongi võtta kasutusele otseses mõttes võimekuse varuga kiip. Teine võimalus on luua kiipi krüptovõtmete varu, mida saab rakendada vastavalt vajadusele liikudes nõrgemalt tugevama suunas. Sellise lähenemise kasutusele võtmist planeeritakse mobiil-ID puhul.

Sellest tulenevalt muutuvad eriti tähtsaks protseduurilised küsimused. Krüpteerimise valdkonda käsitlevad õigusaktid siseriiklikul tasandil puuduvad[23]. Kuidas hinnatakse ja

[20] Töö tegemise ajal oli kättesaadav RIA tellimusel AS Cybernetica poolt 2011. aastal koostatud tehniline dokument "Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring". Uus kaasajastatud uuring oli valmis, kuid kahjuks antud töö tegemise juures seda kasutada ei saanud, sest uuring ei olnud töö lõpetamise ajaks avalikustatud.

[21] Näiteks on Microsoft, Google ja Firefox teatanud, et lõpetavad 01.01.2014 1-kiloste võtmete toetamise. Võib juhtuda, et selliste krüptovõtmetega kaarte ei saa Windows'is enam kasutada. RIA on arutanud kolme toetuse lõpetamise võimalust ja ainult üks neist jätaks kasutusvõimaluse alles.

[22] Soovitame nõuda hankes turvataset määravat sertifikaati omava operatsioonisüsteemiga kiipi (üldreeglina mitte vanem kui kolm aastat alates nõudehetkest).

[23] Riiklikul tasandil on turvastandardid praegusel ajal kehtestatud vaid infosüsteemide tasandil. Krüpteerimise valdkonda käsitlevad õigusaktid siseriiklikul tasandil puuduvad. Üksikud turvaküsimused on sätestatud konkreetsetes alamaktides (iga dokumendi tehnilises kirjelduses) või viidatud kasutatavale standardile. Elamisloakaardi kontaktivabale elektroonilisele andmekandjale digitaalsete andmete kandmisel lähtutakse Rahvusvahelise Tsiviillennunduse Organisatsiooni (ICAO) spetsifikatsioonist 9303-1.

vajadusel võetakse kasutusele (kehtestatakse) uued turvastandardid, mis võivad riigile kaasa tuua märkimisväärseid kulutusi ja ebamugavusi tarbijale? Tuleb välja arendada dünaamiline protseduur/protsess, mis võimaldab vajadusel kiiresti üle minna krüptoalgoritmide kasutamise järgmisele tasemele. Hanke kontekstis tähendab see, et kasutusele tuleb võtta tehniliselt võimekam kiip ehk n.ö varuga kiip. Kes juhib selliste otsuste vastuvõtmist, on seni arutelu all.

Krüpteerimine

Kasutusel oleva isikutunnistuse juures on eksperdid suure puudusena toonud välja krüpteerimisvõtmete muutumise isikutunnistuse vahetamise korral, mille tõttu ei saa uue kaardi korral avada eelmise kaardiga krüpteeritud informatsiooni.

Ekspertide üks soovitus on võtta kasutusele **permanentne krüpteerimisvõti**, et pikendada krüpteeritud dokumentide kasutamisaega. Esmane kasutus toimuks ikkagi kaardilt, aga uue kaardi võtmisel laetakse sinna samad krüpteerimisvõtmed. Väga erinevaid seisukohti esitati selliste võtmete genereerimise ja hoidmise kohta (võtmete genereerimine riigi, usalduspartneri või üksikisiku poolt; võtmete hoidmine tsentraalselt (mitme osapoole serveris) või üksikisiku enda poolt, samuti võtmete hoidmise teenuse pakkumine üksikisikutele, kes on oma võtmed ise genereerinud).

Permanentse krüpteerimisvõtme poolt: 1. Krüpteerimise kasutatavus muutuks oluliseks.

Riskid: 1. Suureneb inimeste hirm, et keegi saab võtme lahti muukida (keskmine risk, maandamismeetmed: a) luuakse spetsiaalne kasutuskeskkond; b) krüpteerimisvõtmete hajushoidmine; c) logimine ja logide säilitamine).

Esitati ka alternatiivne ettepanek: loobuda digitaalse dokumendi abil dokumentide krüpteerimist võimaldava teenuse pakkumisest (mobiil-ID ei võimalda seda teenust juba praegu)[24].

[24] Sama arvamuse esitas AS Cybernetica: "Praeguse ID-kaardi loomise ajal kuulus dekrüpteerimisfunktsioon nö „standardpaketti", mida kiipkaarditootjad oma toodete turundamiseks kasutasid. Ehkki ID-kaardi põhifunktsioon on isiku identifitseerimine, oli kasutatav tehnoloogiline lahendus (krüpto-kiipkaart) kasutatav ka andmete dekrüpteerimiseks. Seega lisati see võimalus ka ID-kaardi võimaluste hulka. Täna võime kahelda selle otsuse õigsuses. Krüptograafid on väga ammusest ajast soovitanud mitte kasutada sama võtit signeerimisel ja dekrüpteerimisel. 2012. aastal esitles rühm teadlasi konverentsil CRYPTO 2012 (http://eprint.iacr.org/2012/417.pdf) efektiivsemat rünnet andmete krüpteerimisel kasutatava PKCS#1 v1.5 täidistamismeetodi nõrkuste vastu, mis andis muuhulgas võimaluse võltsida signatuure. Rünne ei olnud küll praktiline, kuid ID-kaart sattus tugeva mainerünnaku alla. Asjatundjate soovitus on ID-kaardi uues versioonis mitte toetada PKCS#1 v1.5 täidisega krüptogrammide dekrüpteerimise funktsionaalsust, kuid kuna seeon jätkuvalt väga laialt levinud krüpteerimisviis, siis ahendab see kindlasti ID-kaardi kasulikkust andmete salastamisel. Kui vaadata eID laiemalt, siis Mobiil-ID ei võimalda põhimõtteliselt pakkuda samasugust turvalist andmete dekrüpteerimisteenust. Seega on eID kogukond jagatud kaheks – ühed, kes suudavad ja teised, kes ei suuda dekrüpteerida neile saadetud konfidentsiaalseid andmeid. Eesti eID oluline tugevus ja edutegur on olnud ühtsus ja

Poolt: 1. eID lahendused oleksid ühetaolised ja universaalsed (võimaldavad samu teenuseid). 2. Vähendab turvariske. 3. Vähendab inimeste hirmu, et eID võidakse kasutada nende omavahelise vestluse pealt kuulamiseks.

Vastu: eID mainekadu, sest kaob üks funktsioon.

Sertifitseerimine

Kontseptuaalselt tuleb läbi töötada ja otsustada, kas lubada inimeste kasutusse rohkem kui üks samalaadne digi-ID kandja (*token*).

Hetkel kehtib sertifitseerimispoliitika, mis lubab anda ühe samalaadse digi-ID. Tehnilised keskkonnad arvestavad vaikimisi, et inimesel on üks digi-ID. Tehniliselt ei ole probleem ka mitme digi-ID kasutamise lubamine, küll aga on tekkiv olukord keeruline baastarkvara ja kasutaja haldamise seisukohalt. Enam ei saa lihtsalt helistada ja sertifikaate kinni panna, peab tekkima protseduur, mis tagab, et õigete sertifikaatide kasutamine lõpetatakse. Samuti muutub inimestele keerulisemaks valik, millist sertifikaati allkirjastamisel kasutada jne. Praegu on Eestis võimalik ka ainult üks mobiil-ID (kehtib viimane).

Poolt: Turul on olemas (hetkel väike) nõudlus rohkem kui ühe digi-ID omamiseks.

Riskid: 1. Kasutus muutub keerukamaks, tuleb osata vahet teha erinevatel sertifikaatidel, et neid õigesti kasutada ja vajadusel neist õige sulgeda (keskmine risk, maandamismeetmed: a) rakenduste disaini kasutajasõbralikkuse suurendamine; b) e-teadlikkuse tõstmine).

Hooldus

Kriitilise tähtsusega on väljastatud kaartide hoolduse lülitamine hankesse. Nagu on näha tabelist 1, on käibes väga erinevate tunnustega isikutunnistusi ja selline mitmekesisus kestab pikki aastaid. Üle kuuesaja tuhande kasutuses oleva isikutunnistuse kiibirakenduste krüptotugevus on alla soovitatava (1024 RSA).

Sellesse paketti võiks kuuluda ka sertifikaatide uuendamise teema (kodus ja/või kontorites jne). Siia kuulub ka uute rakenduste peale panemise teema. Kas jätkata konservatiivset

---

universaalsus. Selline osaliselt kasutatav teenus ei tule sellele kuvandile kasuks ja tekitab tunde, et riik ei viitsi, ei oska, ei taha korralikku teenust pakkuda. Dekrüpteerimiseteenusega on seotud ka võimaliku andmekao probleem. Kõik andmed, mis on dekrüpteeritavad vaid sellekonkreetse ID-kaardiga, muutuvad kättesaamatuks, kui kaardiga midagi juhtub. ID-kaart ei sobi andmete pikaajaliseks salastamiseks. Salastamisteenus pole universaalne, vaid sobib ainult andmete transpordi turvamiseks. Lõpuks peab mainima ka NSA pealtkuulamisskandaali kiiluvees tekkinud teooriat, et riik võib kaartide võtmeid nende personaliseerimisel ka kopeerida ning omada niiviisi võimalust kodanike omavahelist suhtlust pealt kuulata. Nõutakse võimalust ise võtmeid genereerida jms. Oluline on tähele panna, et probleem ei ole seotud mitte ID-kaardi põhifunktsiooniga (isiku autentimine Internetis), vaid kõrvalfunktsiooniga (isikute vahelise andmevahetuse salastamine). Küll aga üldistatakse probleem kogu ID-kaardi turvalisusele („ID-kaart võib olla ebaturvaline"), tekitades sellega jällegi mainekahju."

poliitikat ja mitte lubada uute rakenduste lisamist? Eelistama peaks konservatiivset lähenemist, sest tegemist on tõsise ründevektoriga.

Tabel 1. EstEID versioonid kasutusel olevatel isikutunnistustel, digitaalsetel isikutunnistustel ja elamisloakaartidel.

Rakenduse versioon	**Krüptograafia**	**Kiibiplatvorm**	**Kommentaar**	**Kasutusel olevate kaartide arv 12.2013**
EstEID v 1.0	1024 RSA	Micardo 2.1		~300 000
	1024 RSA	Micardo 3.0		~300 000
EstEID v 2.0	1024 RSA	MultOS IE4 (DigiID)	DigiID - toetab ainult T=0	<30 000
EstEID v 3.4	2048 RSA	Java jTOP IFX SLE66	OAEP[1] tugi puudub	~700 000
EstEID v 3.5	2048 RSA	Java jTOP IFX SLE66	OAEP[1] tugi puudub	
	2048 RSA	Java jTOP IFX SLE78	Kiip toetab OAEP[1]	
EstEID v 4.0	2048 RSA, 256 ECC	...	Täielik OAEP[1] tugi toetab 256 ECC[2]	
EstEID v ?	256 ECC	...	Rakendusel on 256 ECC[2] sertifitseerimine MoC[3]	

[1] OAEP – Optimal asymmetric encryption padding[25]

[2] ECC – Elliptic Curve Cryptography[26]

[3] MoC – Match-on-Card[27]

Turvalisus

EstEID turvalisuse teema kerkis esile 2011. aastal. Kasutusel olnud operatsioonisüsteemidele kehtis sertifitseerimisnõue ja need olid sertifitseeritud. Rakenduste ja draiverite sertifitseerimisnõuet kehtestatud ei ole, samuti toimub ainult sertifitseerija (sh protsesside) auditeerimine. Trübi tellimusel on tehtud EstEID ver 3.5 turvaanalüüs[28].

Jätkata tuleb sertifitseeritud kiibi ja operatsioonisüsteemide kasutamist, rakendustele ja draiveritele tuleb esitada turvaanalüüsi tegemise ja (mitte ainult sertifitseerija) protsessidele auditeerimise nõue.

[25] Vt http://www.id.ee/public/kryptoalgoritmide_elutsykli_uuring_15-07-2011.pdf.

[26] Elliptiliste kõverate krüptograafia. Vt http://www.id.ee/public/kryptoalgoritmide_elutsykli_uuring_15-07-2011.pdf.

[27] Sõrmejälgede kaartidel hoidmise ja võrdlemise kontseptsioon, mis tõendab kaardiomaniku füüsilist kohalolekut ja selle abil tagab turvalise isikutuvastuse. Vt http://www.matchoncard.com/what-is-moc.

[28] EstEID on Trübi intellektuaalne omand.

Kõigepealt tuleks teha **turvaanalüüs tervikule** ja selle põhjal otsustada komponentide sertifitseerimis- või auditeerimisvajadus. Ühiskonna jaoks tuleb luua läbipaistvus.

Läbipaistvus ja turvalisus käivad käsikäes. Krüptograafiakogukonnas on juba enam kui sada aastat tagasi võetud omaks põhimõte, mille sõnastas 1883. aastal lingvist ja krüptograaf Auguste Kerckhoffs[29]. Nn Kerckhoffsi printsiip nõuab, et krüptosüsteemi enda kirjeldus ei tohi olla salajane, mis tähendab, et kogu saladus peab sisalduma võtmes. Seda põhimõtet on ajaloos erinevatel põhjustel korduvalt eiratud ning see eiramine on sageli viinud olukorrani, kus muidu nõrka krüptosüsteemi üritatakse kaitsta hämamisega (inglise keeles *security by obscurity*), kuid pärast süsteemi avalikuks tulekut on see kiiresti murtud.[30]

Poolt: (Mitte ainult tehnilise) usaldusväärsuse kasv.

Muudatuste juhtimine

Kuigi ülesandepüstitus ei olnud suunatud tööjaotuse või töökorralduse korrastamisele, tõstatati see teema kõigis intervjuudes ja ajurünnakutes. Kuna tegemist on valdkonnaga, mis on pidevas muutumises, peaks muudatuste juhtimine kui protsess olema kehtestatud, mis ei ole võimalik ilma vastava organisatsioonita.

Mistahes muudatuste läbiviimise otsuse tegemise juures tuleb alati arvestada nende (tehnilist ja rahalist) mõju teenuste osutajatele ja lõppkasutajatele. Seda mõju tuleb minimiseerida. Kes on pädev ja vastutav selliseid analüüse tegema ja otsuseid vastu võtma?

Enne hanget peab olema määratletud, kelle pädevuses on kaardirakenduste ja draiverite tellimine. Kes otsustab uute krüptoalgoritmide kasutusele võtmise? Kellegi juhtimisel tuleb korrastada versioonihaldus. Keegi peab hoidma visiooni. Need on ainult mõned esile kerkinud märksõnad intervjuudest ja ajurünnakutelt.

Hetkel on isikutunnistuse ja sellega seotud infrastruktuuri arendamisega seotud Siseministeerium, Politsei- ja Piirivalveamet (edaspidi: PPA), Majandus- ja Kommunikatsiooniministeerium, RIA, SK, Trüb, Cybernetica jt.

Esimene isikutunnistuste infrastruktuuriga seotud vastutuspakett on loogilise tööjaotuse kohaselt seotud isikutunnistuste väljaandmise ja hooldamisega (kaardid, nende isikustamine, sertifitseerimine, seotus x-tee andmevahetusega, kaardidraiverid jms). Partneriteks on PPA, Trüb ja Cybernetica, osaliselt SK (sertifikaatide väljaandmine, aktiveerimine ja kasutajatugi) ja RIA (draiverid ja baastarkvara paketti kuuluv ID-kaardi hooldusvahend).

Teine isikutunnistuste infrastruktuuriga seotud vastutuspakett võiks olla seotud isikutunnistuse kasutamisega (kasutajarakendused, teenuseosutajad, internet). Põhitegija

[29] Auguste Kerckhoffs. *La cryptographie militaire. Journal des sciences militaires, IX:161–191, 1883.*

[30] 2011 07 15 kryptoalgoritmide_elutsykli_uuring_15-07-2011.

RIA (CERT, baastarkvara paketti kuuluv DigiDoc), oluline partner SK (kehtivuskinnitusteenus ehk *Online Certificate Status Protocol* (OCSP), sertifikaatide haldus ja kasutajatugi).

Eksperdid rõhutasid vajadust olla rahvusvaheliste standardite ja normide väljatöötamisel aktiivsem[31]. Siseriiklikult peaks jätkuma e-kirjaoskuse arendamine.

[31] ISO/IEC-s arenduses on standardikavand 29003 „*Identity Proofing*". Eesti eksperdid peaksid kindlasti selle väljatöötamises osalema.

Elamisloakaartidel kasutatav lahendus

Pakkumiskutses esitati järgmine küsimus: „Teadaolevalt on tulenevalt Euroopa Liidu nõuetest ühtses vormis väljaantavate elamisloakaartide kohta (nõukogu 18. aprilli 2008. aasta määrus (EÜ) nr 380/2008, millega muudetakse määrust (EÜ) nr 1030/2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks) elamisloakaardile kantud nii kontaktivaba kui kontaktiga kiip, kus esimesele on kantud isiku sõrmejäljed. Kas säärane lahendus oleks vajalik ja põhjendatud ka isikutunnistuse puhul, pidades silmas biomeetrilistel andmetel põhineva identiteedihalduse perspektiivi…"

Eksperdid ei toetanud üksmeelselt ideed võtta elamisloakaardil kasutatav LDS biomeetriline lahendus kasutusele ka isikutunnistusel.

Piirikontrolli aspektist lähtuvana ei ole see mõistlik järgmistel põhjustel: biomeetrilise lahenduse kasutamine elamisloakaartidel on kohustuslik Euroopa Liidu regulatsioonidest tulenevalt ja see on välja töötatud piirikontrolli kinnise tsüklilise süsteemi jaoks; samas on isikutunnistus kasutusel reisidokumendina eelkõige Schengeni liitu kuuluvates riikides, kus piirikontrolli tavaolukorras ei toimu ja seega poleks LDS lahendusel ka selget ja regulaarset kasutust. Kaardiomanikud ei saa lahendusest mingit kasu ja selleks raha kulutamine ei ole põhjendatud.

Ristkasutuse aspektist lähtuvalt ei ole ühtegi mõistlikku ristkasutuse valdkonda, kus LDS lahendust kasutada saaks. LDS biomeetriline lahendus kasutab RFID kasutajaliidest. RFID liidesega kiibil on ligipääs andmetele hästi turvatud. Selle jaoks on üldreeglina[32] vaja spetsiaalset optilist lugejat, et arvutada MRZ andmetele ligipääsu koodi ja kiibil asuvat spetsiaalset näokujutist või kontaktkiibil asuva isikuandmete faili kaasaajastamist nii, et kontaktkiibilugejat saaks kasutada ligipääsukoodi arvutamiseks. RFID kiibil asuv näokujutis on madalama kvaliteediga võrreldes kaardile trükitud isikufotoga. Ainult nägu ise oleks sellega võrdne. Sõrmejälgede lugemine RFID kiibilt on lubatud ainult Euroopa Liidu piirikontrolli jmt institutsioonil. Ei ole loodud kaardiga seotud staatilist tuvastust, vaid tegemist on juhuvalikuga. Ei ole mõeldav isegi kõige lihtsama rakenduse kasutamine (nagu näiteks oli Tallinna pilet).

Kaaluda võiks RFID kiibil ladustatava näokujutise ekstraheerimist ja selle lisamist kontaktkiibil asuvasse isikuandmete faili. Isikuandmete fail vajab sellisel juhul muudatusi. Sellisel juhul tekiks võimalus ladustada kvaliteetseid isikufotosid, aga nagu iga uuendusega, kaasnevad sellega riskid.

[32] Osa nutitelefone saab selle funktsiooniga juba hakkama.

e-riik kui Šveitsi pank

Eesti infoühiskonna arengukavas kuni 2020. aastani on üheks eesmärgiks seatud muuta Eesti e-riik rahvusvaheliselt sama tuntuks ja usaldusväärseks kaubamärgiks kui on Šveitsi pank[33].

Šveitsi pankade usaldusväärsuse tagamise üks nurgakivisid on nende konservatiivsus, mille tõttu ei võeta julgeid riske, samas vähendatakse sellega tõenäosust, et midagi saab juhtuda. Tuleks tõsiselt kaaluda, kui konservatiivselt või innovatiivselt isikutunnistuse arendamisse suhtuda.

Isikutunnistuse edu põhjuseks olid lihtsus, ühetaolisus, riigi ja erasektori hea koostöö.

2001. aastal, kui arendati välja isikutunnistust ja uut reisidokumenti, võeti isikut tõendavate dokumentide arendamisel kasutusele konservatiivne strateegia. Isikutunnistuste arendamisel, mis oli tol ajal vägagi innovatiivne protsess, otsustati osta teenust erasektorilt. Reisidokumentide tootmist aga otsustati konservatiivselt jätkata riigi poolt. Sellise lähenemisega loodi olukord, kus ebaõnnestumise korral isikutunnistuse arendamisel oli olemas alternatiiv isikutuvastamiseks reisidokumentide ehk passide abil. Selline taktika on ennast õigustanud – hetkegi pole olnud ohtu, et Eesti kodanikel pole võimalik kasutada isikut tõendavat dokumenti.

Unustada ei tohiks, et isikutunnistus täidab ka nö konservatiivset visuaalse tuvastamise funktsiooni ja on ühtlasi Eesti kodanikele reisidokument.

Mistahes muudatuse juures peab olema viidud miinimumini risk, et isikutunnistusi ootamatult kasutada ei saa.

Eesti e-riigile (rahvusvahelise) tuntuse ja usaldusväärsuse tagamise üks nurgakivisid on isikutunnistus koos digitaalse identiteediga. Vähem teatakse ja tuntakse digitaalset isikutunnistust. Digitaalses maailmas ei ole vahet, kumba kaarti kasutatakse ja see loob võimaluse arendada erinevatel isikutunnistustel (või üldse erinevatel digitaalse identiteedi kandjatel) erinevaid funktsionaalsusi.

Sellest tulenevalt on välja pakutud kaks alternatiivi.

Alternatiiv 1

Isikutunnistuse arendamisse suhtutakse väga konservatiivselt ja sellel tehakse ainult möödapääsmatult vajalikke, eelkõige turvalisuse tagamisest tulenevaid muudatusi. Funktsionaalsusi muudetakse ainult siis, kui ollakse veendunud, et olulisi riske see kaasa ei too.

[33] Eesti infoühiskonna arengukava 2020.

Selle alternatiivi kasuks räägib asjaolu, et hetkel on käibel väga mitmesuguseid erinevaid operatsioonisüsteeme kandvaid erinevate baastarkvaraversioonide poolt toetatud ja madala turvatasemega kiipidega isikutunnistusi (vt tabel 1). Sellise mitmekesisuse haldamine on iseenesest väga suur risk.

Isikutunnistuse kaart on polükarbonaadist, keerulises disainiga ja turvaelementidega pigem ülereguleeritud, mistõttu selle tootmise on kallis ja aeglane protsess. Sellest tulenevalt võivad eksperimendid kaardi funktsionaalsusega tuua kaasas suuri kulutusi. Tulevikku vaadates võib mistahes turvaintsidendi likvideerimine samuti tuua kaasa ülisuuri kulutusi – eriti juhul, kui tuleb mingil põhjusel kaarte ümber vahetada.

Sellisel juhul võiks isikutunnistusel piirduda järgmiste muudatustega: 1) võimekuse varuga kontaktkiip; 2) permanentne krüpteerimisvõti; 3) näobiomeetria.

Hoopis teisiti on digitaalse isikutunnistusega, mis on valmistatud PVCst ja millel turvaelemente pole. Digitaalse isikutunnistuse kaartide tootmine on odav võrreldes isikutunnistuse kaardi tootmisega. Samuti tuleb arvesse võtta väiksematest tootmismahtudest tulenevat efekti – tootmine on kiirem ja odavam. Praegusel hetkel kasutab aktiivselt digitaalset isikutunnistust ainult u 6000 isikut ning tegemist on kindlasti teadlikuma ja nõudlikuma osaga kasutajatest. Isegi siis, kui digitaalse isikutunnistuse kasutajate hulk hüppeliselt (näiteks meelitatuna uutest funktsionaalsustest) kasvab, jääb nende arv oluliselt väiksemaks isikutunnistuste koguarvust.

Eelpooltoodust – odav, lihtne, väiksemaarvuline, sekundaarse tähtsusega – tulenevalt võiks innovaatilisi eksperimente teha digitaalse isikutunnistusega. Digitaalsel isikutunnistustel võiks arendada kõiki eespool kirjeldatud uuendusi.

Alternatiiv 2

Isikutunnistuse arendamisse suhtuda kui võimalusse rakendada innovaatilisi lahendusi ning tugevdada selle kaudu Eesti kui innovaatilise väikeriigi mainet.

Sellisel juhul tuleks isikutunnistuse ja digitaalse isikutunnistuse digitaalseid funktsioone ühtemoodi arendada.

Selle alternatiivi kasuks räägib ühetaolisus ehk inimestel on lihtsam aru saada, kui mõlemad (või kõik) isikutunnistused on digitaalses mõttes samade funktsioonidega.

LISA. Ideed kaugemaks tulevikuks

Kontaktivaba kiip kui sertifikaatide kandja. Sellisel juhul käituks NFC-võimekusega mobiiltelefon kui kaardilugeja. Kaardil peab olema NFC liides, mis võimaldaks sarnaselt kontaktliidesele kiibiga suhelda. Olgu siis tegemist lisavõtmepaari või integreeritud võtmepaariga. Tegemist on oluliselt keerukama arendusülesandega kui numbrite kiirgamise funktsionaalsuse kasutusele võtmine. Selline lahendus vajab NFC telefoni ja vastavat tarkvara telefonis. Praeguste võimaluste juures on andmevahetus ajamahukam. Teada on üksikud mobiiltelefoniga seotud edukalt töötavat lahendused[34]. Seega ei ole sellise lahenduse kasutusele võtmine lähiajal otstarbekas. Võtmepaaride lisamisel tuleks täiendada isikut tõendavate dokumentide seadust ja digitaalsele dokumendile kantavate andmete loetelu Vabariigi Valitsuse määrustes.[35] Sertifitseerimiskeskuse sõnul on kavas järgmisel suvel tuua turule mitme sertifikaadipaariga mobiil-ID[36].

[34] Vt http://randomoracle.wordpress.com/2013/02/24/windows-smartcard-logon-with-android-secure-element-and-nfc/

[35] Digitaalne dokument on isikut tõendavate dokumentide seaduse (ITDS) (§ 3 lg 3) kohaselt elektroonilises keskkonnas isiku tõendamiseks ja isikusamasuse kontrollimiseks ettenähtud dokument. ITDS § 20^2 lg 1 kohaselt kantakse digitaalsele isikutunnistusele digitaalset tuvastamist võimaldav informatsioon ning digitaalset allkirjastamist võimaldav informatsioon. Täpsem andmete loetelu kehtestatakse Vabariigi Valitsuse 26.06.2010. aasta määrusega nr 120 „Digitaalse isikutunnistuse vormi, tehnilise kirjelduse ja digitaalsele isikutunnistusele kantavate andmete loetelu kehtestamine", kus on detailselt määratletud, millised andmed tuvastamist ning allkirjastamist võimaldava sertifikaadi kohta digitaalsele isikutunnistusele kantakse. ITDS § 9 lõike 5 kohaselt võib dokumenti kanda digitaalset isiku tuvastamist võimaldavat informatsiooni, sealhulgas digitaalset tuvastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ja digitaalset allkirjastamist võimaldavat informatsiooni, sealhulgas digitaalset allkirjastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ning teisi digitaalseid andmeid. Eeltoodust tulenevalt võib seaduse alusel dokumenti kanda ka muid digitaalseid andmeid, kuid need peavad olema defineeritud vastavas Vabariigi Valitsuse määruses. Isikutunnistusele täiendavate sertifikaatide lisamisel on vajalik täpsustada ka isikut tõendavate dokumentide seaduse sõnastust.

[36] Mobiil-ID väljaandmisega seonduv on reguleeritud ITDS § 20^4, mille kohaselt mobiil-ID vormis digitaalne isikutunnistus on digitaalne isikutunnistus, mille digitaalset tuvastamist võimaldav sertifikaat ja digitaalset allkirjastamist võimaldav sertifikaat on seotud mobiiltelefoni SIM-kaardiga. Sama paragrahvi lõike 4 kohaselt, kui isikul on juba kehtiv mobiil-ID vormis digitaalne isikutunnistus, tunnistatakse see uue mobiil-ID vormis digitaalse isikutunnistuse väljaandmisel kehtetuks. Seega ei anna seadus hetkel võimalust ja alust mitme sertifikaadipaari üheaegseks kasutamiseks. Isikuga võib olla seotud mitu sertifikaadipaari, kuid ainult üks neist peab olema kehtiv. Mitme sertifikaadipaariga mobiil-ID kasutuselevõtmisel on vajalik täpsustada ITDS-is sätestatud mobiil-ID regulatsiooni (sealhulgas mobiil-ID definitsioon, kasutamise erisused, riigilõiv). Kuna hetkel on mobiil-ID vormis väljaantava digitaalse isikutunnistuse puhul regulatsioon ainult seaduse tasandil, siis sertifikaadipaaride lisandumisel ning sertifikaatides sisalduvate andmete erinemisel juba väljaantavatest vajab mobiil-ID vormis digitaalne isikutunnistus täpsemat reguleerimist juba ka Vabariigi Valitsuse määruse tasandil. Täiendamist vajab Vabariigi Valitsuse 26.06.2010. aasta määrus nr 120 „Digitaalse isikutunnistuse vormi, tehnilise kirjelduse ja digitaalsele isikutunnistusele kantavate andmete loetelu kehtestamine".

Pilvelahendused. Sertifikaatide pilvelahenduses hoidmist (kandja abiga aktiveeritakse autentimis- ja/või allkirjastamisteenus) või pilves asuvat digitaalse dokumendi hajuslahendust ei soovitanud turvaeksperdid tungivalt kasutusele võtta.

ID-kaardi riistvaraline uuendus: klaviatuur ja displei.

Keerulisemate protokollide toetamine. Räägime siiski aastast 2027.

Open Firmware kiibi tekitamine.

Seadmesse sisseehitatud turvamoodulid SIM-kaardita telefonidele ja kaardilugejata arvutitele jm seadmetele. Juba praegu on kasutusel suur hulk lõppkasutajaseadmeid, kuhu kaardilugejat külge panna ei saa: see on kas ebamugav või füüsiliselt võimatu. Oodata on SIM-kaardita mobiiltelefone. Lahenduseks on turvamooduli seadmesse sisseehitamine. Kui arvutite jaoks on juba olemas *Trusted Platform Module* (TPM), mis suudab genereerida ja väljastada sertifikaate, siis sisseehitatud turvamooduliga mobiiltelefone veel turul ei ole.

Juriidilistele isikutele mõeldud digitempel ja krüptosertifikaat on väheste kasutajate tõttu praegu kallid teenused, mis omakorda piirab nende kasutamist. Samas on tegemist turvaliseks infovahetuseks väga vajaliku teenusega, mille tähtsus ajas kasvab. Analoogselt isikutunnistuse kohustuslikkusele võiks juriidilistele isikutele mõeldud digitempli ja krüptosertifikaadi muuta samuti kohustuslikuks (näiteks oleks see mingist ajast alates kohustuslik uutele loodavatele juriidilistele isikutele, teistele antakse mõistlik üleminekuaeg). Pikemas perspektiivis võimaldaks see üleminekut kanalipõhiselt turvamiselt sõnumipõhisele turvamisele.

Kasutatud lühendid

LDS – *Logical Data Structure as described in ICAO9303*

MRZ – *Machine Readable Zone*

RFID – *Radio Frequency Identification (wireless non-contact)*

NFC – *Near Field Communication*

OAEP – *Optimal asymmetric encryption padding*

ECC – *Elliptic Curve Cryptography*

MoC – *CC certification Match-on-Card*

Allikad

1. Vabariigi Valitsuse tegevusprogramm 2011−2015. Vabariigi Valitsuse 05.05.2011 korraldus nr 209 lisa.
2. „Eesti infoühiskonna arengukava 2020" ja "Eesti infoühiskonna arengukava 2020 rakendusplaani 2014−2015" heakskiitmine.
3. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.*
4. *Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Brussels, 4.6.2012. COM(2012) 238 final. 2012/0146 (COD)*
5. *Council Regulation (EC) No 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals.* Official Journal L 115 , 29/04/2008 P. 0001 – 0007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:115:0001:01:EN:HTML
6. Nõukogu määrus (EÜ) nr 1030/2002, 13. juuni 2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks (EÜT L 157, 15.6.2002, lk 1). Muudetud: nõukogu määrus (EÜ) nr 380/2008, 18. aprill 2008.
7. Euroopa Nõukogu määrus (EÜ) nr 1030/2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:19:06:32002R1030:ET:PDF.
8. Euroopa Nõukogu määrus (EÜ) nr 380/2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:115:0001:0007:ET:PDF.
9. Isikut tõendavate dokumentide seadus.
10. Vabariigi Valitsuse 09.12.2010. aasta määrus nr 170.
11. Siseministri 12.08.2010. aasta määrus nr 36.
12. ICAO spetsifikatsioon 9303, http://www.icao.int/publications/Documents/9303_p3_v1_cons_en.pdf.
13. Arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta. 00720/12/ET. WP 193. Artikli 29 alusel asutatud andmekaitse töörühm. Vastu võetud 27. aprillil 2013.
14. Arvamus 02/2012 näotuvastuse kohta *online*- ja mobiilsideteenuste puhul. 00727/12/ET. WP 192. Artikli 29 alusel asutatud andmekaitse töörühm. Vastu võetud 22. märtsil 2012.
15. *World e-ID Congress 2013 Web Proceedings.*
16. Jan Willemson, Peeter Laud, Aivo Jürgenson, Märt Laur. Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring. 2011. http://www.id.ee/public/kryptoalgoritmide_elutsykli_uuring_15-07-2011.pdf.
17. Marko Palm „Mis on NFC ehk lähiväljaside?" (Mobiilne rahakott – „Minu rahakott"). Infotark 03.02.2013.