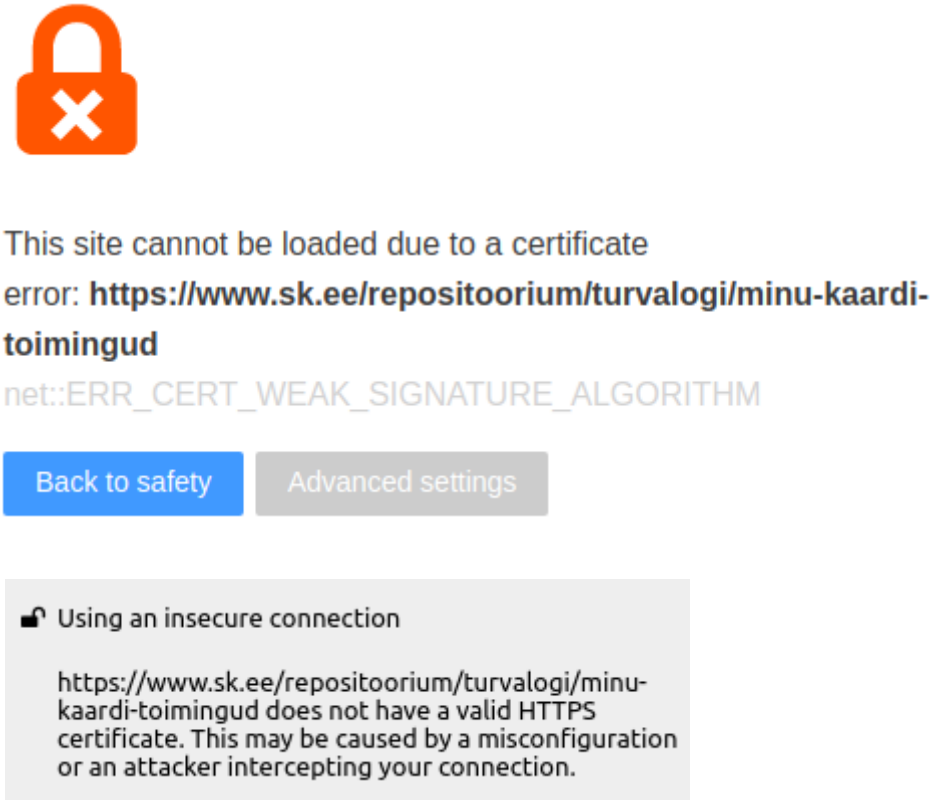
https://www.sk.ee/repositoorium/turvalogi/minu-kaardi-toimingud



CTRL+SHIFT+I (Chrome jne)

Obsolete connection settings

The connection to this site uses TLS 1.0 (an obsolete protocol), RSA (an obsolete key exchange), and AES_256_CBC with HMAC-SHA1 (an obsolete cipher).

https://www.sk.ee/minutoimingud/

https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf - kas ei oleks aeg kasutada maksimaalse kangusega krüptot? Ehk oleks aeg mõelda elliptilise krüpto peale koos maksimaalselt kõrge KDF'i (https://en.wikipedia.org/wiki/Key_derivation_function) väärtusega??
Kuidas on see kõik kvantarvutite valguses? Näiteks https://www.dwavesys.com/d-wave-two-system mille saab kätte ~15 mln $ eest (ilmselt hind kukub ajas kiirelt), mida on juba mitmeid müüdud....
Mis garanteerib mobiil-ID jt ID-lahenduste turvalisuse nüüd ja tulevikus (eriti kvantarvutite valguses)??

Lisaks:
http://www.sciencealert.com/breaking-a-brand-new-type-of-qubit-has-been-unveiled-and-it-finally-makes-quantum-computers-scalable

# # #

https://geenius.ee/eksklusiiv/mis-id-kaardiga-ilmselt-tegelikult-juhtus-ja-kui-ohtlik-see-eestile/
5.09.2017

Mis ID-kaardiga ilmselt tegelikult juhtus ja kui ohtlik see Eestile on?

Sellest hetkest, kui Riigi Infosüsteemi Amet teisipäeva hommikul teatas, et teadlased on avastanud Eesti ID-kaardis võimaliku turvaaugu, on IT-kogukond avalikult kättesaadava info põhjal proovinud aru saada, mis tegelikult juhtus. Pea kõik arutelud jõuavad välja ühte kohta: ilmselt on kõrvalistel isikutel võimalik kaardiga sisse logida ja allkirju anda ka ilma PIN-koode teadmata ja ilma kaarti omamata.

Geeniuse toimetus konsulteeris päeva jooksul paljude Eesti asjatundjatega, kes tunnevad nii kogu ID-kaardi süsteemi ülesehitust kui krüptograafiat laiemalt. Meil pole mingit siseinfot ning keegi pole meid ei avalikult ega salaja eraldi briifinud selle kohta, mis tegelikult juhtus, aga me toome siin ära stsenaariumi, mida eranditult kõik meiega rääkinud üksteisest sõltumatud spetsialistid kõige tõenäolisemaks pidasid. Teema on mitte-IT-spetsialistidele keeruline, aga me proovime seda teha ülimalt lihtsustatult, seega spetsialistid andku see lihtsustatus meile andeks.

Need reeturlikud avalikud võtmed

Väga kõnekas fakt kogu sündmustiku juures on see, et riik otsustas ohust teada saades sulgeda ID-kaardi avalike võtmete serveri, mida pidas SK ID Solutions AS, vana nimega

Sertifitseerimiskeskus. Et selle olulisust mõista, teeme ühe lihtsa põike sellesse, kuidas ID-kaardi krüptograafia üldse töötab.

Kaardiga on seotud kaks võtit: avalik ja salajane. See on maailmas väga levinud ja laialt kasutatav süsteem, millel ongi nimeks “Avaliku võtme krüptograafia” ja mis tähendab, et sõnumi saatja šifreerib sõnumi kasutades vastuvõtja avalikku võtit, vastuvõtja dešifreerib sõnumi enda salajase võtmega. Need kaks võtit on üksteisega seotud ning salajane võti, nagu nimigi ütleb, on salajane ja avalik on avalik. Salajane võti elab ID-kaardi kiibi peal väga kaitstud olekus ning avalik elab igal pool internetis, muuhulgas SK avalike võtmete andmebaasis.

Sealt sai kuni viimase ajani igaüks teha kasvõi oma internetibrauseri kaudu päringuid: sisestad otsitava inimese isikukoodi ja saad tema avaliku võtme vastu. Isikukoodid on ka Eestis avalikud, nii et näiteks kõigi firmade juhatuse liikmete isikukoodide andmebaas kokku panna ning selle abil kõigi nende inimeste avalikud võtmed oma arvutisse laadida oli mitte ainult triviaalne, vaid ka täiesti seaduslik ja normaalne tegevus. Avalik võti peabki avalik olema, see on kogu avaliku võtme krüptograafia süsteemi aluspõhimõte. Ilma avalike võtmeteta see lihtsalt ei töötaks.

Avaliku võtme krüptograafia toimib aga eeldusel, et avalikku võtit teades ei ole mitte mingil juhul võimalik sellest tuletada salajast võtit. Selleks peavad võtmed olema piisavalt pikad ja kasutatavad algoritmid piisavalt head, et see oleks inimkonnale praegu ja nähtavas tulevikus kättesaadavate arvutusvõimsuste juures sama hästi kui võimatu. Päris võimatu ta niikuinii ei ole, aga kui kogu maailma arvutusvõimsust korraga kasutusele võttes kuluks ühe parooli murdmiseks ikkagi kümneid või sadu aastaid, võime öelda, et see on sama hästi kui võimatu. Kui

tehnika areneb, saab kasutusele võtta uued ja paremad algoritmid ja seda ka tehakse.

Asjaolu, et Eestis pandi probleemi ilmnedes kohe avalike võtmete server kinni, annab Geeniusega konsulteerinud IT-spetsialistide sõnul loogilise aluse eeldada, et mingil põhjusel on võimatu osutunud võimalikuks: Eesti ID-kaartide avalikke võtmeid teades on neist võimalik tuletada salajased võtmed ehk meie elektroonilist identiteeti ja digiallkirju võltsida.

Kas keegi tegi vea?

Hea küsimus on see, miks selline asi üldse võimalik on, kui kogu süsteem on üles ehitatud eeldusel, et see ei ole võimalik. See on sama hull ja arusaamatu olukord, nagu oleks see, kui päike hakkaks ühel päeval Läänest tõusma ja Itta loojuma. Me kõik teame, et see pole võimalik, aga ometi ühel hetkel selgub, et on. Aga erinevalt päikese teistpidi käima hakkamisest on siin võimalikud loogilised seletused olemas.

Riigi esindajad näitasid teispäevasel pressikonverentsil üsna ühemõtteliselt kaartide tootja, rahvusvahelise suurfirma Gemalto peale. See pole ainult Eesti ID-kaartidega seotud probleem, vaid ligi miljardit kogu maailmas välja antud kaarti puudutav mure. Järelikult on Gemaltos kaartide tootmisel juhtunud midagi, mis teeb salajaste võtmete tuletamise avalikest võtmetest võimalikuks. Mis see on, võime ainult spekuleerida. Näiteks on võimalik, et kuigi kogu süsteem põhineb eeldusel, et salajased võtmed genereeritakse täiesti juhuslikest arvudest, siis võib-olla on selgunud, et need juhuslikud olema pidanud arvud tegelikult polnud nii väga juhuslikud.

Väga lihtsustatult, ütleme, et meil on vaja genereerida kümme juhuslikku arvu ja mingil põhjusel me teeme nii, et nende arvude algused on kogu aeg samad, näiteks 123456789 ja vahetame ainult kahte viimast numbrit. Nii et esimene

“juhuslik” arv on 12345678945, järgmine 12345678924 ja nii edasi. Siis pole koodi murdmiseks vaja ära arvata pikka juhuslikku arvu, vaid ainult seda viimast, mis vahetub ja see on tunduvalt lihtsam. See on üks võimalus, miks pikk murdmatu kood murtavaks osutus, aga neid on veel.

Eesti jaoks on kõige olulisem see, et probleem ei ole meie e-riigi arhitektuuris ega süsteemis laiemalt, vaid ühe tootja tarkvaras. Me ei pea oma e-riigi juures midagi põhimõtteliselt ümber tegema, vaid saama katkiste asemele lihtsalt korralikud ID-kaardid ja probleem on lahendatud.

Nad varastavad meie allkirjad

Nüüd saame minna küsimuse juurde, kui oluline see avastatud turvaauk on ehk miks valitsus nii laialt sellele reageeris ja mis saab edasi.

Kui see ülaltoodud IT-spetsialistide see arutluskäik on tõsi, siis on tegemist riigi jaoks üsna niru olukorraga. Kui avalikust võtmest saab tuletada privaatse, tähendab see, et kolmandad isikud saavad meie eest hakata ID-kaardiga pangaülekandeid tegema, digiallkirju andma ja, tõepoolest, ka e-valimistel osalema. Kui salajane võti murtakse, saab sellega teha kõike seda, mida inimesed ise oma ID-kaartidega teevad, kasvõi lepingutele alla kirjutada, laenu võtta, firmasid osta ja müüa ja nii edasi.

Kõige hullem on see, et sellisel juhul saaks kaarte rünnata ka ilma, et neid füüsiliselt vaja oleks. Kellelgi pole vaja meile tänaval nuiaga pähe lüüa ja meie rahakotte ära varastada selleks, et meie digitaalseid identiteete varastada. Meie kaardid ja PIN-koodid oleks meiega turvaliselt kogu aeg kaasas, aga rünnak toimuks puhtalt läbi interneti ja nii, et me ilmselt ei saagi sellest teada enne, kui ilmub välja suvaline inimene digiallkirjastatud lepinguga, mille kohaselt sa müüd talle 100 euro eest oma korteri või kingid ära oma firma. Kuna allkiri näib

100 protsenti ehtne, on pärast väga raske tõestada, et sa ei andnud seda ise, vaid see on võltsing.

Muidugi on salajase võtme murdmiseks sel juhul vaja avalikke võtmeid ja see on ka ilmselt põhjus, miks riik avalike võtmete serveri kinni keeras, aga see on paremal juhul poolpidune lahendus. Jah, nüüd pole enam ühte kohta, kust mugavalt kogu rahvastiku avalikud võtmed endale alla laadida, aga esiteks ei ole meil mingit garantiid, et üks või kasvõi miljon inimest või kolmetähelist organisatsiooni seda juba ammu teinud pole ning teiseks lendavad meie avalikud võtmed internetis avalikult ringi iga kord, kui me ID-kaardiga midagi teeme.

Avalikud võtmed on, nagu öeldud, avalikud ja kui välja valida inimesed, kelle digitaalset identiteeti tahetakse ära ajada, pole nende avalike võtmete hankimine eriline probleem. Serveri kinni keeramine teeb pigem keerulisemaks kõigi probleemist vaevatud 750 000 kaardi lahti murdmise, sest 750 000 avalikku võtit on tüütu ükshaaval koguda.

Riigi väike PR-trikk

Siin aga tuleb mängu riigi väike PR-trikk. Riigi teatel maksab kõigi Eesti kaartide lahtimuukimine umbes 60 miljardit eurot ja see on tõepoolest liiga suur raha, et ühele väiksele igavale riigile nagu Eesti seda kulutada. Ilmselt ei paneks sellist raha Eesti digitaalseks anastamiseks ei häkkerid ega venelased.

Aga esiteks, me ei tea, mis number on 60 miljardit ja kuidas see saadud on. Kas selle projekti hind oleks 60 miljardit näiteks sulle ja mulle, kui me läheks Euronicsisse ja ostaks hulga arvuteid, et seda koodi murdma hakata? Või on see hind sellisel puhul, kui ründajal on angaaritäis arvuteid juba olemas ning see on pelgalt kulu töötajatele ja IT-administraatoritele, kes seda ID-kaartide murdmise farmi üleval hoiavad? Kas selle hinna sees on ka koheva karvaga valge kass, keda

maailmavallutajast maniaki sõrmustatud käsi hellalt paitab? Me ei tea.

Küll aga teame me, et kui me jagame 60 miljardit eurot 750 000 kaardiga ja eeldame, et valdav osa sellest 60 miljardist on arvutusvõimsuse kulu, saame ühe kaardi murdmise hinnaks 80 000 eurot ning kuna selle numbri on välja käinud riik, kellel on igal juhul huvi näidata murdmise hinda pigem kõrgema kui madalamana, on mõistlik arvata, et see on ühe kaardi lahti murdmise maksimaalne hind. Ja see tähendab täielikku lahtimurdmist, nii PIN1 kui PIN2. Aga näiteks digiallkirjade andmiseks ei ole PIN1 üldse vaja, seega läks see projekt ühe kaardi kohta ründajale just poole odavamaks.

Me teame ka, et probleemi avastanud teadlased on vähemalt ühe kaardi juba lahti murdnud, et oma teooriat tõestada. Nii ütles meile täna üks asjaga kursis olev riigiteenistuja. Seega, kui riik üritab turvaauku näidata väga kalli teoreetilise ohuna, siis tegelikult tundub see olevat vägagi reaalne oht, kui murda lahti mitte 750 000 kaarti, vaid näiteks 1 või 10 või isegi 100.

Pealegi läheb arvutusvõimsus kogu aeg odavamaks, iga pooleteise aastaga umbes kaks korda.

PR-trikk seisnebki selles, et riik opereerib 750 000 kaardi lahti murdmise hinnaga, aga seda polegi ju kellelegi vaja. Eestile saab erakordselt palju probleeme kaasa tuua kasvõi näiteks ainult peaministri kaarti lahti murdes ja tema eest allkirju andes. Või murrame lahti Eesti TOP 20 firmade juhatuste liikmete kaardid, ainuüksi nendega saab palju kurja korda saata. Või, kui raha on rohkem, siis võtame ette mõne väiksema valla 100 elanikku ning hääletame volikogusse külakoer Pontu, lihtsalt nalja pärast. Eesti e-riigi maine on õrn ning kui paari sellise trikiga välja tulla, on eesrindlikust digiriigist ja tema kõrgestihinnatud jutlustest saanud üleöö naerualune ning hoiatav eeskuju.

Mis saab edasi?

Riigil ei ole siin häid lahendusi. Kui probleemi olemus on selline, nagu me kirjeldame, siis tähendab see, et meil on ringluses 750 000 nõrka ID-kaarti, millega tuleb midagi teha.

Esimene variant on see, et kaarte pole vaja füüsiliselt uuendada, küll aga kaartide peal olevat vigast tarkvara ja genereerida uued võtmed. Kui nii, siis võib juhtuda, et riik saab valmistada spetsiaalse tarkvara, millega inimesed saavad seda kodus ise teha. See tähendaks, et riik peab veenma kolmveerand miljonit inimest mingit programmi alla laadima ja oma kaarte uuendama. Võib täitsa kindel olla, et enamus neist ei viitsi seda teha ja nõrgad kaardid jäävad ringlusesse.

Teine variant on see, et kaarte saab uuendada näiteks Politsei- ja Piirivalveameti teeninduspunktides. Seega peaks paluma 750 000 inimesel oma kaartidega sealt läbi astuda. Jällegi, võib kindel olla, et väga paljud neist seda ei tee ja nõrgad kaardid on ikka ringluses.

Kolmas variant on see, et kaardid asendatakse uutega.

Kuna on vähetõenäoline, et vigaseid kaarte ringlusesse jättes inimesed viitsiks neid välja vahetada, siis paistab siit igal juhul terendavat tulevik, kus vähemalt vigaste kaartide sertifikaadid pannakse kinni, et neid kaarte elektrooniliselt kasutada ei saaks ja nende omanikud oleksid sunnitud oma kaartide elektroonsest kasutamisest kas üldse loobuma ja näiteks mobiil-ID peale minema või kaardid korda tegema.

http://tehnika.postimees.ee/4233255/id-kaardi-kiibis-avastati-teoreetiline-turvarisk

ID-kaardi kiibis avastati teoreetiline turvarisk

Eesti riik sai info teoreetilisest turvariskist ID-kaardi kiibis. E-valimiste toimumise otsustab vabariigi valimiskomisjon. Postimees teeb kell 14 algavast valitsuse pressikonverentsist otseülekande.

Vabariigi valimiskomisjoni esimees Meelis Eerik ütles, et teda on võimalikust ID-kaardi turvariskist teavitatud. «Mulle laekunud info kohaselt elu Eestis seisma ei jää – esmased lahendused riskide maandamiseks on tehtud, ühtegi reaalset intsidenti ei ole olnud. Oht on teoreetiline ja tõestamata. Spetsialistid tegelevad info kontrollimisega,» lausus ta.

Vabariigi valimiskomisjon teeb otsuse kohe, kui neil on piisavalt informatsiooni. Viimane tähtaeg e-valimiste toimumise kohta otsus langetada on oktoobri algus, kuid valimiskomisjon lubab, et kindlasti ei viivita oma otsusega nii kaua.

Teoreetiline turvarisk on reaalne

Peaminister Jüri Ratas ütles pressikonverentsil, et tegu on seni tõsiseima teabega turvariski kohta. «Teoreetiline turvarisk on reaalselt olemas,» sõnas ta. Peaminister soovitab inimestel võtta kasutusele mobiil-ID. Eesti riik läheb e-teenuste arendamisega Ratase sõnul igal juhul edasi.

RIA peadirektor Taimar Peterkop selgitas Postimehe ajakirjaniku küsimusele vastates, et turvarisk ei puuduta otseselt Eesti ID-kaarte, vaid kiipi, mida on maailmas välja antud üle miljardi. Tehnikud on tema sõnul öelnud, et haavatavus kiibis on olemas, kuid veel kunagi pole nähtud, et koodi lahtimuukimine oleks õnnestunud.

Samas ei ole RIA siiani jälile jõudnud turvaaugu põhjustajale, küll aga arvavad nad teadvat, mis võiks olla lahendus.

Kõiki meetmeid, mida turvariski maandamiseks kasutusele võetakse, riik avalikustada ei saa. «Et mitte teha pahade inimeste elu lihtsamaks,» tõdes Peterkop. RIA soovitab inimestel samamoodi võtta kasutusele mobiil-ID.

Digiallkirjad kehtivad edasi. Seda, mis täiendavate turvameetmete kasutusele võtmine riigile maksma läheb, RIA juht kommenteerida veel ei osanud.
Peterkopi sõnul koguvad nad erinevatelt teadlastelt pidevalt informatsiooni ID-kaardi turvalisuse kohta, kuid tema sõnul ei pea paika kuulujutt, et RIA sai info reaalselt eksisteerivast turvaaugust juba mullu sügisest.
Politsei- ja piirivalveameti peadirektor Elmar Vaher ütles, et mõjutatud ID-kaartide sertifikaate tühistama ei hakata. Küll aga töötab PPA koos RIAga selle nimel, et viia kaardid kõrgemale turvatasemele. Ka teeb PPA Vaheri sõnul koostööd pankadega.
Ettevõtlus- ja infotehnoloogiaminister Urve Palo tõdes, et mingit mõtet uut ID-kaarti soetama minna pole, kuna ka siis saab inimene sama kiibi. Küll aga võib paari kuu pärast hakata andma uue kiibiga kaarte, siis selle vahetuse ka riik korvab. Probleemi tõsidusest ollakse Palo sõnul ka aru saadud.

Risk puudutab 750 000 ID-kaarti

30. augustil informeeris rahvusvaheline teadlaste grupp riigi infosüsteemi ametit (RIA), et nad avastasid turvariski, mis mõjutab Eestis alates 2014. aasta oktoobrist välja antud ID-kaarte, mida on kokku 750 000.
Eesti ekspertide praeguse hinnangu järgi on turvarisk olemas. «Me jätkame teadlaste väidete kontrollimist,» ütles RIA peadirektor Taimar Peterkop ja lisas: «Oleme juba välja töötanud esmased lahendused riskide maandamiseks ning teeme kõik selleks, et ID-kaardi turvalisus oleks jätkuvalt tagatud.»

Lahtimuukimine maksab hinnanguliselt 60 miljardit eurot

Kõigi vigaste kaartide koodi lahtimuukimine maksab hinnanguliselt ligi 60 miljardit eurot.
Praeguse info järgi ei ole turvarisk realiseerunud ja kellegi digitaalset identiteeti ei ole selle abil kuritarvitatud. «Kõik ID-kaardiga tehtud toimingud kehtivad ja astume rea samme, et seda turvariski ei oleks võimalik Eesti ID-kaardi ründamiseks kasutada ka tulevikus. Sulgesime ID-kaardi avalike võtmete andmebaasi, kuna ilma avalikku võtit teadmata ei ole võimalik antud turvariski kaardi ründamiseks kasutada,» selgitas Peterkop.
Võimalik turvarisk puudutab alates 2014. aasta oktoobrist välja antud ID-kaarte (sealhulgas e-residentidele väljastatud kaarte) ehk kokku ligi 750 000 kaarti. Enne 2014. aasta 16. oktoobrit väljastatud ID-kaartidel oli kasutusel teine kiip ning neid see risk ei mõjuta. Samuti ei puuduta antud turvarisk mobiil-ID-d.
«Eesti digitaalne ühiskond kasutab maailmas uuenduslikke tehnoloogiaid. Uute tehnoloogiatega kaasnevad mugavused, kuid paraku alati ka riskid. Oluline on, kuidas võimalikke ohte avastatakse ja välditakse,» lausus RIA juht ja lisas, et juhtum on hea näide sellest, kuidas teadlased annavad avastustest meile teada ning Eesti riik saab asuda probleeme lahendama.
ID-kaartide väljaandmine jätkub, samuti töötavad edasi kõik riiklikud e-teenused.

Ansip: e-hääletamine peaks toimuma

Euroopa Komisjoni asepresident Andrus Ansip ütles «Aktuaalsele kaamerale», et praegu, mil Eesti e-riigi lahendused on seoses eesistumisega teravdatud rahvusvahelise tähelepanu all, võib probleemide kiire lahendamine näidata meie tugevust.

«Kohalikel valimistel peaks ID-kaardiga e-hääletamine toimuma,» leiab endine peaminister.

«Kui katus tilgub läbi, siis me parandame selle katuse ära ja elu läheb edasi. Me ei tule ju selle peale, et võiks maja maha lammutada või üldse koopasse elama minna. Neid probleeme on olnud ennegi ja küllap kahjuks tuleb ka tulevikus, kuid me oleme võimelised need probleemid lahendama,» ütles Ansip «Aktuaalsele kaamerale».

Rõivas: ei tohi sattuda paanikasse

Riigikogu aseesimees Taavi Rõivas (RE) tõdes, et kõiki turvariske tuleb võtta tõsiselt, kuid neist ei tohi sattuda paanikasse. Rõivas rääkis ETV saates «Ringvaade», et e-valimiste või ükskõik millise suure e-lahenduse pikemalt mõtlemata ärajätmine oleks kindlasti märk paanikast.

Ta lisas, et ka kõige turvalisem tehnoloogia või tarkvara vajab pidevat tähelepanu ja uuendamist. Tema sõnul on ID-kaartide kiibi peal olevat infot tõenäoliselt võimalik uuendada ilma, et kaarti füüsiliselt välja vahetada.

Hanso sõnul pole tõenäoline, et Venemaa üritab süsteemi häkkida

Endise kaitseministri Hannes Hanso (SDE) hinnangul pole tõenäoline, et Venemaa üritab Eesti e-valimiste süsteemi sisse häkkida, ütles ta «Ringvaates».

«Arvan, mida Taavi Rõivas juba ütles, et tegelikult keegi ei tea, ühtegi fakti pole selle kohta, et keegi oleks suutnud midagi ära häkkida. /.../ Ma ei usu, et paanikaks mingit põhjust on,» ütles ta.

Hanso ütles, et loodab, et e-valimised ära ei jää.

PPA koostas küsimus-vastus vormis ülevaate, mida see ID-kaardi turvarike inimestele tähendab. Loe pikemalt: ID-kaardi turvarike: mida see kasutajatele tähendab?

http://tarbija24.postimees.ee/4233465/id-kaardi-turvarike-mida-see-kasutajatele-tahendab

ID-kaardi turvarike: mida see kasutajatele tähendab?

Riigi Infosüsteemi amet (RIA) teatas täna, et ID-kaardil avastati turvarisk, mis puudutab pärast 2014. aasta oktoobrit väljastatud kaarte. PPA koostas küsimus-vastus vormis ülevaate, mida see inimestele tähendab.

Kas ID-kaardi kasutamine on turvaline?
Isikut tõendava dokumendina on kaart täiesti turvaline. Enne 2014. aasta 16. oktoobrit välja antud kaarte turvarisk ei puuduta.
Praeguse hinnangu põhjal on ID-kaardi kasutamine jätkuvalt turvaline ka internetis autentimiseks ja digiallkirjastamiseks. ID-kaardi kuritarvitamine on keeruline ja kallis; meile pole teada ühtki juhtu, kus seda tehtud oleks.
Kõik praegused sammud on eeskätt võimalikke riske ennetavad – tegemist on ettevaatusabinõuga, et ilmnenud turvanõrkust ei saaks ära kasutada.
RIA ja PPA monitoorivad pidevalt olukorda ja reageerivad kohe, kui risk kasvab.
Kuidas ma ID-kaarti kasutada saan?
Kõiki teenuseid saab edasi kasutada täpselt nii nagu varem. ID-kaart kehtib jätkuvalt nii isikut tõendava dokumendi kui ka reisidokumendina kuni kaardile märgitud kehtivusaja lõpuni.
Mobiil-ID omanike jaoks ei muutu samuti midagi.
Mis minu jaoks muutub?

Kuni sertifikaate ei ole peatatud ega tühistatud, ei muutu kaardiomaniku jaoks midagi. ID-kaarti saab kasutada nagu seni.
Kui sertifikaadid turvariski tõttu suletakse, antakse sellest kaardiomanikule teada e-posti teel ja teavitatakse avalikult.

Kas ma pean taotlema uue ID-kaardi?

ID-kaart kehtib jätkuvalt isikut tõendava dokumendina kuni kaardile märgitud kehtivusaja lõpuni ja on kehtiv reisimiseks Euroopa Liidus. Kehtiv elamisloakaart koos välismaalase passiga kehtivad reisimiseks.
Kui ID-kaardi kehtivusaeg lõpeb, tuleb taotleda uus kaart. Muul juhul uut ID-kaarti taotlema ei pea ja turvariski see ka ei maanda.

Kas ID-kaardile on alternatiive?

ID-kaardi asemel võib kasutada mobiil-ID-d. Paljudesse teistesse teenustesse, nt pangateenustesse sisse logimiseks saab kasutada ka Smart-ID-d, PIN-kalkulaatorit. Koodikaarte kasutada ei soovita, nende turvariskid on suuremad kui ID-kaardil.

Kuidas ma saan endale mobiil-ID?

Pöördu oma mobiilioperaatori poole, kes väljastab selleks sobiva SIM-kaardi. Seejärel tuleb mobiil-ID aktiveerida politsei.ee veebilehel. Mobiil-ID-d saab hakata kasutama kohe pärast aktiveerimist. Pärast seda võib ID-kaardi sertifikaadid sulgeda, et kuritarvituse riski vältida.

Mis see minu jaoks maksab?

Operaatori teenustasu on praegu 1 € kuus.

Kes mind nõustab?

ID-kaardi abiliini number on 1777.
Mobiil-ID osas saab nõu mobiilioperaatorilt, ka operaatori infotelefoni ja veebiteeninduse kaudu.

Kas mobiilioperaatorid on selleks koormuseks valmis?

Mobiilioperaatorid on vajadusest teadlikud ja arvestavad sellega, aga arvestada võiks tavapärasest pikemate järjekordadega.

TEHNILISED KÜSIMUSED

Mida see haavatavus tegelikult tähendab? Kas ID-kaart on häkitav? Mis andmeid on selleks vaja, et saaks kaarti häkkida ja häkitud kaarti kasutada?

Teoreetiliselt on võimalik kasutada ID-kaarti isikutuvastuseks ja digiallkirja andmiseks ilma kaarti omamata ja PIN koode teadmata. Ainult sertifikaadi avaliku võtme teadmisest kaardi lahtimurdmiseks siiski ei piisa – vaja on ka suurt arvutusvõimekust salajase võtme väljaarvutamiseks ja spetsiaalset tarkvara, millega allkirja anda. ID-kaardi tarkvara selleks ei sobi, sest eeldab ID-kaardi paiknemist kaardilugejas.
ID-kaardi kuritarvitamine on äärmiselt keeruline ja kallis, meile pole teada ühtki juhtu, kus seda tehtud oleks.

Paljud teenused (näiteks pangad) nõuavad teenusesse sisselogimiseks lisaks kasutajatunnust või salasõna või mõlemat korraga – ka neid tuleb teada.

Kas ja kuidas saan oma kaardi sertifikaadid tühistada? Kas seda peaks tegema?

Sertifikaate saab peatada ID-kaardi abitelefonil 1777. Lisainfot leiab id.ee lehelt.

Sertifikaadid võib peatada või tühistada iga kaardi omanik ise või teenusepakkuja. Praegu selleks otsest vajadust ei ole. Kui olukord muutub, siis teavitatakse sellest kaardiomanikke kohe.

Kui kaardiomanik tahab kuritarvituse võimaluse välistada, võib soetada mobiil-ID ja selle aktiveerimise järel ID-kaardi sertifikaadid peatada või tühistada.

Sertifikaadi peatamise korral saab sertifikaadi uuesti aktiveerida, tühistamise korral kaarti enam digitaalselt kasutada ei saa.

Kas saan tühistada ainult allkirjastamise võimaluse?

Autentimise ja allkirjastamise saab peatada või tühistada ainult korraga, sest turvarisk puudutab mõlemat.

Mis juhul võib riik tühistada minu sertifikaadid?

Sertifikaadid tühistatakse siis, kui nende häkkimise risk muutub reaalseks. Tühistamisest antakse kaardiomanikule kindlasti teada.

Kas ja kui kiiresti saab vigase ID-kaardi uue vastu vahetada?

Kõik praegu väljastatavad ID-kaardid on sama turvariskiga. Uus ID-kaardi lahendus on alles väljatöötamisel.

Isikut tõendava dokumendina on ID-kaart endiselt kehtiv.

Kas viga saab veebi kaudu parandada?

Praegu veel mitte, aga töötame selle kallal.

Mis juhtus 2014. aasta oktoobris, et selline viga tekkis? Kas Eesti oli sellest muutusest teadlik?

2014. aasta oktoobris võeti ID-kaartidel kasutusele uus kiip, mis oli kiirem, põhines uuemal tehnoloogial ja oli seega eelduslikult turvalisem. Kiibile antud Prantsusmaa ja Saksamaa turvasertifikaadid kinnitavad selle vastavust kõigile turvanõuetele. Sama kiip on kasutusel mitme teise riigi isikutunnistusel, ka maksekaartidel ja töötõenditel.

Turvarisk tekkis uue kiibi ja tarkvara koosmõjus.

Mis juhtus sertifikaatidega, et need enam turvalised pole?

See, et krüptograafilised algoritmid, millel sertifikaadid põhinevad, muutuvad arvutusvõimsuse kasvades tasapisi ebaturvaliseks, on tehnoloogia seisukohalt tavapärane areng. Just sel põhjusel vahetatakse ID-kaardi sertifikaate mõne aja tagant tugevamate vastu.

Praegusel juhul sattus ilmnenud turvarisk kokku arvutusvõimsuse kasvuga. Veel mõni aasta tagasi oleks sellise kaardi lahtimurdmine olnud oluliselt kulukam ja seega veelgi ebatõenäolisem kui praegu.

Kuidas te teada saite? Miks te alles nüüd sellest räägite?
Võimalikust turvariskist andis teada rahvusvaheline teadlaste rühm ametlike kanalite kaudu.
Iga sellise turvanõrkuse ilmsiks saamisel tõuseb hüppeliselt selle ärakasutamise oht. Sellepärast avalikustasime teabe siis, kui olime saadud infot omalt poolt kontrollinud ja ühtlasi võtnud kasutusele ettevaatusabinõud turvariskide vähendamiseks.
Mida saan kaardi kaitseks teha?
Kui ID-kaarti tehingute tegemiseks ei kasutata, võib ID-kaardi sertifikaadid peatada. Jääb võimalus kasutada alternatiive, mida turvanõrkus ei puuduta, näiteks mobiil-ID.
RIA ja PPA eksperdid jälgivad olukorda hoolikalt, vajadusel peatatakse sertifikaatide kasutamine. Sellest teavitatakse nii kasutajaid kui avalikkust.
KURITARVITAMINE
Kas ja kuidas saan kontrollida, kas keegi on minu kaarti/identiteeti kuritarvitanud?
ID-kaardi elektroonilise kuritarvitamise kahtluse korral pöördu politsei poole ja teavita RIA infoturbeintsidentide käsitlemise osakonda (cert@cert.ee).
Kas riik jätkuvalt garanteerib digiallkirja? Kui kaua?
ID-kaardiga antud digiallkiri kehtib, seda ka pärast sertifikaatide peatamist või tühistamist.
Kas pangad usaldavad EV ID-kaarti?
Pangad usaldavad ID-kaarti ja pangateenused on jätkuvalt ID-kaardi abil kasutatavad.
Kas ja millised tehtud toimingud saab kahtluse alla saada? Kas ma pean need uuesti tegema?
Kõik pärast 2014. aasta oktoobrit ID-kaardiga antud allkirjad ja tehingud kehtivad.
Kas riik on jätnud kiipide turvalisuse kontrollimata?
ID-kaardi ja kiibi nõuetelevastavust on kinnitanud pädevad Saksamaa ja Prantsusmaa sertifitseerimisasutused, sellel on kehtiv turvasertifikaat.
Turvanõrkuse ilmnemise järel oleme astunud samme, et viia riskid miinimumi: sulgesime ID-kaardi avalike võtmete andmebaasi, meie eksperdid analüüsivad riskikohti ja tegelevad lahenduse otsimisega, et taastada ID-kaartide turvalisus kõrgeimal tasemel.
Kuidas ja millal te sellest turvaaugust teada saite?
Teadlaste rühm informeeris avastatud turvariskist RIAt 30. augusti õhtul.
Kes need teadlased on?
Tunnustatud ülikoolidest pärit rahvusvaheline krüptograafiateadlaste rühm, kes teavitas RIAt ametlike kanalite kaudu.
Kas nad teadlased reaalselt mõne kaardi häkkisid?

Nad tõestasid, et see on matemaatiliselt võimalik, kui on olemas piisav arvutusvõimekus. Ühtki Eestist pärit võtit ei ole teadaolevalt lahti murtud.

Kas olete ise teadlaste väiteid kontrollinud? Kas suutsite häkkimist korrata?

Kontrollimine võtab aega, seda teeb RIA koostöös Eesti teadusasutustega. Praegused tulemused kinnitavad, et uuringut võib pidada usaldusväärseks ja turvarisk on tegelik. Ühtki võtit siiski lahti murtud ei ole.

Kus see teadustöö avaldatud on? Kas selle info alusel on võimalik igaühel kaarti murda?

Teadustöö avaldatakse eeloleval sügisel rahvusvahelisel teaduskonverentsil. Konkreetseid ründetööriistu ei ole akadeemilistes töödes tavaks avaldada.

Miks te ei ole veel kaarte kinni pannud? Kes sulgemise otsustab?

Tegemist on seni realiseerumata turvariskiga. Praeguses olukorras pole sulgemine põhjendatud ja tooks kaasa arvestatava ebamugavuse paljudele inimestele.

Mida te seni teinud olete?

RIA koos Eesti teadusasutuste ekspertidega on tegelenud väidete kontrollimise, riskide maandamise ja lahenduskäikude kaardistamisega. Seda on tehtud koostöös partnerite ja teenuseosutajatega, et vajadusel muudatusteks valmis olla.

VALIMISED

Kas e-valimised toimuvad? Kuidas nad toimuvad?

RIA on teavitanud turvariskist riigi valimisteenistust, kes tagab valimiste korraldamist. Otsuse e-hääletamise toimumise kohta teeb Vabariigi Valimiskomisjon.

Kas e-valimised on turvalised?

E-valimised pole rohkem ohus kui muud teenused. Häälte hulgaline võltsimine pole selle kõrge kulu tõttu mõeldav.

http://www.id.ee/index.php?id=38028

https://www.politsei.ee/et/nouanded/id-kaart-ja-pass/id-kaardi-ja-mobiil-id-kasutajale.dot

Kas ID-kaardi kasutamine on turvaline?

Isikut tõendava dokumendina on kaart täiesti turvaline. Enne 2014. aasta 16. oktoobrit välja antud kaarte turvarisk ei puuduta.

Praeguse hinnangu põhjal on ID-kaardi kasutamine jätkuvalt turvaline ka internetis autentimiseks ja digiallkirjastamiseks. ID-kaardi kuritarvitamine on keeruline ja kallis; meile pole teada ühtki juhtu, kus seda tehtud oleks.

Kõik praegused sammud on eeskätt võimalikke riske ennetavad – tegemist on ettevaatusabinõuga, et ilmnenud turvanõrkust ei saaks ära kasutada.

RIA ja PPA monitoorivad pidevalt olukorda ja reageerivad kohe, kui risk kasvab.

http://www.err.ee/616719/id-kaardi-kiibis-peitub-teoreetiline-turvarisk

ID-kaardi kiibis peitub teoreetiline turvarisk

Rahvusvaheline teadlaste grupp informeeris möödunud neljapäeval riigi infosüsteemi ametit (RIA), et nad avastasid turvariski, mis mõjutab Eestis pärast 2014. aasta oktoobrit välja antud ID-kaarte.

Eesti eksperdid nõustuvad seejuures, et teoreetiline risk on olemas, kuid see puudutab vaid osa käibelolevaid ID-kaarte. Siiski on nende arv väga suur - 750 000 kaarti, mis on välja antud pärast 2014. aasta 16. oktoobrit.
Peaminister Ratas ütles, et vahejuhtum ei too kaasa e-riigi kursimuutust. Otsuse nende kaartide kasutamise kohta eelseisvatel valimistel teeb vabariigi valimisteenistus.
Enne 2014. aasta oktoobrit väljastatud ID-kaartidel oli kasutusel teine kiip ning neid see risk ei mõjuta. Samuti ei puuduta antud turvarisk mobiil-ID-d. Valitsus soovitab seejuures kõigil mobiil-ID teha.
„Eesti ekspertide praeguse hinnangu kohaselt on turvarisk olemas ja me jätkame teadlaste väidete kontrollimist," ütles RIA peadirektor Taimar Peterkop. „Oleme juba välja töötanud esmased lahendused riskide maandamiseks ning teeme kõik selleks, et ID-kaardi turvalisus oleks jätkuvalt tagatud."
Reaalset identiteedivargust pole RIA kinnitusel toimunud. „Praeguse info kohaselt ei ole antud turvarisk realiseerunud ning mitte kellegi digitaalset identiteeti ei ole selle abil kuritarvitatud," ütles Peterkop.

Infosüsteemi amet sulges ID-kaardi avalike võtmete andmebaasi, kuna ilma avalikku võtit teadmata ei ole võimalik antud turvariski kaardi ründamiseks kasutada.“
PPA kinnitas, et ID-kaartide väljastamine ja kasutamine jätkub. "Risk on piisav selleks, et seda tõsiselt võtta, kuid mitte selleks, et kaarte sulgeda," lausus infotehnoloogia eest vastutav minister Urve Palo.
Eesti ametkonnad kinnitasid, et it-spetsialistidel on võimalus see turvarisk likvideerida, kuid see võtab aega.
Riski realiseerumiseks ei ole võimalikul ründajal vaja kasutada või kontaktis olla reaalse ID-kaardiga.

E-valimiste toimumine pole kindel

Vabariigi valimiskomisjoni esimees Priit Vinkel ütles ERR-ile, et valimiskomisjonil on oktoobri alguseni aega otsustada, kas võimaldada eelseisvatel kohalikel valimistel e-hääletamist või mitte.
"Vabariigi valitsus ja riigi infosüsteemi amet on tõepoolest vabariigi valimiskomisjoni esimeest ja valimisteenistust teavitanud ID-kaardi võimalikest riskidest. Seadusest tulenevalt, mis puudutab elektroonilise hääletamise kasutamist kohalikel valimistel, on valimiskomisjonil võimalik sisuliselt kuni oktoobri alguseni langetada otsus, kas ja milliste vahenditega elektroonilist hääletamist kasutama hakatakse," rääkis Vinkel.
Ta lisas, et valimiskomisjon kogub infot, suhtleb vastavate ametiasutustega ja langetab alles siis lõpliku otsuse.
Kui e-valimisi ei peaks toimuma, toob see valimisjaoskondadele kaasa suurema koormuse ja võib tuua kaasa täiendavate hääletuspunktide lisandumise.
"Kui peaks tõesti nii minema, et elektroonilist hääletamist otsustatakse mitte läbi viia, siis see võib tähendada täiendavaid mehitamisi valimisjaoskondades ja hääletamiskohtades. Peame olema valmis suuremaks hääletajate arvuks, aga see on kõik teostatav," kinnitas komisjoni esimees.

Riskiga kaarte maailmas veel

Riskiga kaarte on maailmas veel, sest rahvusvaheline teadlaste grupp uuris kõiki sarnaseid kaarte maailmas. Viga ilmneb kiibi ja tarkvara koostöös. Riski ei ole, kui rakenduse tarkvara kontrollib füüsilise kaardi olemasolu või kasutamist.
Taimar Peterkop tõdes, et Eesti on oma digiühiskonnaga maailmas ainulaadne ning kui mingid riskid said realiseeruda, siis on Eesti ühelt poolt kõige haavatavam, kuid teisalt ka maailmas kõige paremini valmis nende riskidega toime tulema.

http://www.err.ee/616731/ametid-loodavad-id-kaardi-turvariski-likvideerida-kahe-kuuga

Lähema kahe kuu jooksul on ID-kaardi kiibi turvarisk lahendatud, loodavad politsei ja piirivalveameti juht Elmar Vaher ja riigi infosüsteemide ameti juht Taimar Peterkop.

Vaher kinnitas, et turvariski lahendamisse on kaasatud parimad eksperdid. "Julgen öelda seda, et umbes kahe kuu jooksul suudame taaskord välja anda ja viia need 750 000 [turvariskiga] ID-kaarti veel tugevamale turvatasandile."

Riigi infosüsteemi ameti (RIA) peadirektor Taimar Peterkop ütles, et Eesti puhul on sõltuvus ühest tehnoloogiast nii suur, mistõttu on väljakutse ainulaadne ja teiste riikide pealt ei ole sisuliselt midagi õppida.

Peterkop kinnitas "Aktuaalsele kaamerale" antud intervjuus, et inimesed võivad ID-kaarti edasi kasutada samamoodi nagu siiani.

"Otsus, et ID-kaardid toimivad edasi nagu seni, põhineb meie teadlaste ja koostööpartnerite ohuhinnangul. See risk on teoreetiline. Et süsteemi praktikas rünnata, on vaja väga palju meetmeid ja raha," märkis Peterkop.

Küll aga soovitas Peterkop kõigil, kes digitaalseid teenuseid kasutavad, omada kaht tugevat autentimis- ja allkirjastamisvahendit ehk lisaks ID-kaardile ka mobiil-ID-d.

Ka Peterkop ütles, et probleem loodetakse lahendada paari kuu jooksul.

"Paar kuud on maksimumaeg, mis me tahame, et see teema oleks lahendatud. Töötame nii kiiresti kui võimalik. Valitsus andis meile selleks ka mandaadi, et ressursse lugemata palgake vajalikud inimesed Eestist, et see asi nii kiiresti kui võimalik ära lahendada. Oleme kaasanud Eesti tugevamad IT-ettevõtjad, et seda probleemi lahendada. Meil on Eestis maailmatasemel valdkonna eksperte," selgitas Peterkop.

"Teeme koostööd mitme juhtiva IT-ettevõtjaga, samuti teadlastega. Valitsus on andnud meile raha. Lahendus tuleb nii kiiresti kui võimalik," lubas RIA juht.

Kui palju probleemi lahendamine võiks maksma minna, Peterkop prognoosida ei osanud. Ta keeldus kinnitamast, et RIA on probleemi juurpõhjuseni jõudnud, kuid oli veendunud, et lahendus tuleb. Valitsusjuht Jüri Ratas lubas, et raha taha asi ei jää.

Tavainimene muretsema ei pea

Peterkop kinnitas, et tavainimesed ei pea muretsema, et keegi nende ID-kaardi andmeid varastab.

"Tavainimene kindlasti ei pea muretsema. See eeldab ikkagi väga suurt arvutusvõimsust, mille jaoks on vaja väga suurt rahalist ressurssi. See eeldab spetsiifilisi krüptograafiateadmisi, et selline ründepahavara valmis meisterdada. Tavainimeste ründamine ei tasu ära," rääkis RIA juht.

"Kui kõik need 750 000 kaarti lahti muukida, siis me räägime 60 miljardist dollarist nagu on teadlased välja pakkunud. Aga see tähendab ainult arvutusvõimsust, sinna tulevad lisainvesteeringud juurde. Need summad on kolossaalsed. Pigem mis võib ohustada, on

demonstratiivne rünnak meie maine pihta, mis ei pruugigi tegelikult olla küberrünnak, vaid puhas mainekujunduslik," lisas ta.

E-valimiste toimumise kohta ütles Peterkop, et RIA on valimiskomisjoni esimehele riskid välja toonud ja koos arutatakse, kuidas on võimalik e-valimised turvaliselt läbi viia.

"Valimised on riigi kõige olulisem poliitiline protsess ja seal turvalisusega mingeid kompromisse ei tehta," märkis ta ja lisas, et arvestades, kui lähedal valimised on, tuleb otsus e-valimiste kohta teha kiiresti.

Ratas: e-valimiste toimumise otsustab valimiskomisjon

Peaminister vastas pressikonverensil ka kõige põletavamale küsimusele ehk kas kohalikel valimiste saab e-hääletada.

"Seadus ütleb üheselt, et see on valimiskomisjoni otsus. Valimiskomisjon peab nõu valimisteenistusega. Olen veendunud, et nad kogunevad täiskoosseisus ja teevad selle otsuse," ütles Ratas.

Ratas rõhutas, et ID-kaardi turvarisk on teoreetiline, see tähendab, et keegi pole seetõttu kannatada saanud.

Eesti eksperdid on Ratase sõnul alates eelmise nädala neljapäevast riski hinnanud ja jõudnud järeldusele, et risk on tõepoolest olemas.

"See on tõsine häirekell. Tegu on kõige tõsisema teoreetilise riskiga senini," lausus peaminister. "Aga ühtegi reaalset identiteedivargust ei ole toimunud.

Kõik e-teenused jäävad vaatamata riskile toimima. "Eesti on ja jääb e-riigiks. Siiski soovitame inimestel tõsiselt kaaluda minna üle mobiil-ID peale."

Peaministri käest küsiti pressikonverentsil, kas seni ja edaspidi antud digiallkirjad kehtivad ja kas näiteks riigisaladusega kokku puutuvatel ametnikel on jätkuvalt õigus ID-kaarti kasutada. Peaminister vastas sellele jaatavalt.

Palo: ID-kaarti ei ole mõtet vahetama minna

Infotehnoloogia eest vastutav minister Urve Palo ütles, et turvarisk on piisavalt tõsine, kuid ta ei ole piisav selleks, et olemasolevad sertifikaadid sulgeda.

Kuna praegu pole veel teada, mil viisil turvarisk lahendatakse, pole Palo sõnul mõtet kellelgi minna uut ID-kaarti taotlema. Ametkonnad loodavad, et võib-olla saab turvariskist üle tarkvaralahenduse abil.

Teisipäeval sai avalikuks, et rahvusvaheline teadlaste grupp on leidnud turvariski, mis mõjutab Eestis pärast 2014. aasta oktoobrit välja antud ID-kaarte. Risk puudutab praeguse info kohaselt 750 000 kaarti, mis on välja antud pärast 2014. aasta 16. oktoobrit.

Enne 2014. aasta oktoobrit väljastatud ID-kaartidel oli kasutusel teine kiip ning neid see risk ei mõjuta. Samuti ei puuduta antud turvarisk mobiil-ID-d.

Reaalset identiteedivargust pole Riigi Infosüsteemi Ameti (RIA) kinnitusel toimunud. Otsuse nende kaartide kasutamise kohta eelseisvatel valimistel teeb vabariigi valimisteenistus.

http://tehnika.postimees.ee/4234361/repliik-ratas-andis-id-kaardi-jamaga-turmtuld-e-valimistele

Repliik: Ratas andis ID-kaardi jamaga turmtuld e-valimistele

Ma esitasin eile seoses lahvatanud ID-kaardi turvaskandaaliga paljudele inimestele rohkelt küsimusi. Kui jätta kõrvale tehniline spetsiifika, siis kuus küsimust ja vastused neile ei jätnud minu jaoks isiklikult kahtlust, et kogu PR-show teenis vaid ühte eesmärki: Jüri Ratase soovi kompromiteerida e-valimisi.

Allolevaid küsimusi ja vastused vaadates olen kindel, et vähemalt osad teist jõuavad minuga samale järeldusele: ID-kaardi kasutamine on (mingil arusaamatul põhjusel vaid ühe erandi - valimistega) jätkuvalt kõrgeimal tasemel turvaline.

Kaardi kasutamine ei ohusta isegi riigisaladust ega loo ohtu selle lekkimisele. Ka äärmiselt konservatiivsed pangad ei näe ID-kaardi kasutamises jätkuvalt mingisugust probleemi. Isegi vaatamata sellele, Riigi Infosüsteemi Ameti juht märkis, et probleemi juurpõhjus pole lõpuni selge.

Kuid jah, on üks suur erand. See suur erand kannab nime e-hääletamine. See on midagi kõrgemat riigisaladustest, pangakontodel olevatest eurodest ja Euroliidu tasemel antud digiallkirjadest rahvusvahelistele lepingutele, mille puhul kõik eile julgelt, kindlalt ja vankumatult kinnitasid, et mingit probleemi pole. Midagi nii kõrget, et ükski eile neist samadest sõna võtnud ametnikest ja poliitikutest ei julgenud öelda, et kas hääletamine ikka on turvaline.

Otsustada saavat vaid valimiskomisjon. Nagu üks mees lükati kõik selle komisjoni kaela. Seda tegid isegi need, kelle ülesanne riskidest komisjonile teada anda on. Seda olukorras, kus paberil hääletamine on jätkuvalt ebaturvalisem ja mõjutatavam kui e-hääletamine. Kas tõesti jõuti riigisaladuse ja Euroopa Komisjoni digiturvalisuse eest vastutavate ametnikega juba riigisaladuse ja digiallkirjade usaldusväärsuse osas eilseks analüüsid ja kooskõlastused tehtud? Ma tahaks optimistina väga loota.

Ma ei ole kaugeltki vandenõuteooriate austaja, kuid meie e-valimised ja eriti ID-kaart said eile kindlasti oma ajaloo suurima mainelöögi. Minu vandenõuteoreetilist maiku küsimus on: millisele parteile see kasulik on?

ID-kaardi väiksemaid nügimisi on olnud pidevalt ja tegelikult on suur probleem hoopis see, et ID-kaarti saab veebis enda tuvastamiseks järjest vähem kasutada – suurte tehnoloogiaettevõtete brauserid keelduvad järjest seda toetamast.

Ainus lahendus oma e-riigiga edasi minna paistabki olevat mobiilID ja SmartID - kasusaajaks on sel juhul selgelt pankadele ja Teliale kuuluv SK Solutions, senine eID valdkonna monopolist, kelle politsei viimase riigihankega riigipirukast eemale saatis. Tõenäoliselt on SK ettevõte, kellelt RIA

nüüd Ratase avatud rahakoti abil turvaprobleemi lahendamist tellib. Kuid kas eilsel viisil ID-kaardile vett peale tõmmata pole mitte liiga kõrge hind?

Õnneks juba sotsiaalmeedias käivitumas kampaaniad ID-kaardi toetuseks - lubadusega seda ikka julgelt ja püstipäi edasi kasutada.

Aga nüüd lubatud küsimused ja vastused, millest ülaltoodud järeldused tegin:

Küsimus üks: peaminister Jüri Ratas, kas riigisaladusele ligipääsu omavatel inimestel on jätkuvalt luba kasutada ID-kaarti?

Kõigil Eestis elavatel ja töötavatel inimestel on jätkuvalt õigus kasutada ID-kaarti, sealhulgas ka nendel ametnikel, kelle kohta te küsisite. Me oleme siin korduvalt öelnud, et enamusel või väga paljudel, kes igapäevaselt aktiivselt Eestis ID-kaarti kasutavad, on olemas ka mobiilID. Minu teada on see ca 134 000 inimest. Loomulikult on üleskutse suurendada seda arvu.

Küsimus kaks: peaminister Jüri Ratas, kas Eestis antud digiallkirjad kehtivad jätkuvalt kogu Euroopas?

Kehtivad nii Maarjamaal kui Euroopa Liidus. Jah, kehtivad.

Küsimus kolm: peaminister Ratas, kas sügisestel valimistel saab e-hääletada?

Vastus on väga lühike. Kohaliku omavalitsuse volikogude valimise seadus §12 lg 2 p4 ütleb üheselt: see on valimiskomisjoni otsus ja nii see on. Valimiskomisjon peab kindlasti nõu valimisteenistusega ja ma olen täiesti veendunud, et nad kogunevad täiskoosseisus ja teevad selle otsuse. Mis on kõige olulisem: et inimesed võimalikult kiiresti seda teaksid üle Eestimaa, ja kindlasti nad hindavad ka niisama seda turvalisuse aspekti ja teevad siin koostööd nii RIA kui PPA-ga. See ei ole mitte mingisugune valitsuse otsus, see ei ole riigikogu otsus.

Küsimus neli: valitsuse nõunik, kust tuli idee sedavõrd teoreetiline turvaprobleem sedavõrd mastaapse pressiüritusena välja mängida, varem on piirdutud lühikeste pressisõnumitega.

Idee tuli selgelt valitsuse juhilt, mitte ametkondadelt.

Küsimus viis, RIA juht Taimar Peterkop, kas olete tänaseks täpselt aru saanud, mis juhtus?

Sada protsenti ei saa öelda, et me oleme jõudnud juurpõhjuseni. Uurimine võtab aega. Küll oleme me veendunud, et me teame lahendust ja töötame selle nimel.

Küsimus kuus: LHV panga nõunik Priit Rum, kas avalike võtmete andmebaasi sulgemine mõjutab kuidagi teie netipanga tegevust? Kas pank on juhtumiga seoses pidanud midagi muutma või teatud samme astuma?

Avalike võtmete andmebaasi sulgemine meie teenuseid ei mõjuta.

https://geenius.ee/uudis/daniel-vaarik-kas-id-kaardi-turvaveast-raakimine-kellegi-vandenou/

Daniel Vaarik: kas ID-kaardi turvaveast rääkimine on kellegi vandenõu?

Kas ID-kaardi turvanõrkuse avaldamine on kellegi vandenõu või spin? Küsisime kommentaari Daniel Vaarikult, kes on kommunikatsioonieekspert ja partner firmas Akkadian. Vaarik teeb selle raames ka koostööd e-residentsuse meeskonnaga.

Eesti valitsus sai eelmisel nädalal rahvusvaheliselt teadlaste grupilt teate, et on avastatud teoreetiline turvarisk ID kaardi toimimises. Ilmselt seetõttu, et digitaalne ühiskond on Eestis paljudele südamelähedane teema, on erakirjavahetustes ja vestlustes ka minu käest küsitud, et kas võib olla võimalik, et ID-kaardi turvariskist teatamine on kellegi konspiratiivne soov kahjustada Eesti mainet.

Kuigi ma ei tea neid inimesi, kes meile probleemist teada andsid, ei ole niinimetatud karvase käe võimalus tõenäoline kolme põhjusel.

Esiteks, tegemist on olemasoleva veaga. Eesti valitsusele on ju teada antud olemasolevast nõrkusest meie süsteemi sees. Seda nõrkust ei loonud teadlaste grupi liikmed ise, vaid nad avastasid midagi, mis on nende analüüsi põhjal juba olemas. Eesti valitsuse suurim huvi on sellistest asjadest teada saada, mitte elada õndsas teadmatuses hetkeni, kuni asi tõeliselt probleemseks muutub. Pahatahtlikud uurijad ei annaks meile võimalust süsteem korda teha.

Teiseks, ajastus. Kuigi praegune ajastus ei ole ehk e-valimiste seisukohast ideaalne, oleks pahatahtlikult mõeldes Eestile mainele võimalik palju enam kahju teha siis, kui avaldada turvarisk vahetult pärast e-valimisi. Sellisel juhul ei oleks valitsusel enam mitte midagi võimalik ette võtta turvataseme tõstmiseks, keerulisem oleks avalikkust veenda valimiste õiguspärasuses ning spekulatsioonid selle üle, kas Tallinna linnapeaks sai õige inimene, võiks jääda avalikkust mürgitama pikaks ajaks. Pahatahtlik seltskond just nii teekski.

Kolmandaks, teadaandmise viis. Pahatahtlik uurijate grupp oleks läinud otse avalikkuse ette, kas läbi blogipostituste või meediakanalite, avaldanud võimalikult palju detaile ja instruktsioone teoreetilise turvariski praktiliseks ärakasutamiseks. See oleks omakorda viinud selleni, et Eesti valitsus oleks pidanud sõrkima sündmuste sabas ning rinda pistma võib olla ka väga suure hulga katsetega meie süsteeme mõjutada.

Teadlased aga toimisid teisiti. Nad andsid Eestile eelhoiatuse, et mõne kuu jooksul on ilmumas teaduslik artikkel ning tehti seda otse ühendust võttes. Kuna meie ühiskond on väga suurel määral digitaalne, siis ideaalset ajastust ju polegi. Ikka on olukordi, mis eeldavad digitaalse identiteedi kasutamist.

See kõik ei tähenda, et maailmas poleks pahasoovijaid, kes näeksid hea meelega, et meie digitaalne ühiskond ei toimimiks. See ei tähenda, et nad ka tänast olukorda edaspidi ei prooviks ära kasutada. Kuid minu arvates on oluline hinnata kõrgelt seda, et meile tullakse otse teada andma võimalikest

nõrkustest. See on parim asi, mis saab juhtuda ning mida rohkem kriitikuid meiega koostööd teeb, seda tugevamaks saavad meie digitaalse ühiskonna süsteemid.