

MOBIIL-ID TURVAUURING

RAPORTI KOKKUVÕTE (versioon 11.07.2008)

Tellija: Majandus- ja Kommunikatsiooniministeerium, RISO

Täitja: Jaak Tepandi, CISA (Tepinfo OÜ)

Mobiil-ID on traditsioonilise ID-kaardil põhineva isikutuvastuse ja allkirjastamise edasiarendus, mille puhul mobiiltelefoni SIM-kaarti (Mobiil-ID kaarti) võib e-keskkonnas käsitleda samasugune isikut tõendav dokumendina nagu ID-kaarti.

Mobiil-ID abil saab põhimõtteliselt end nagu ka ID-kaardiga autentida ning selle abil on võimalik dokumente digitaalallkirjastada, kasutades Mobiil-ID sertifikaate. Uuringus on Mobiil-ID-d käsitletud kui ID-kaardiga analoogilist isikutuvastuse ja digitaalallkirjastamise teenust (keskkonda, protsessi).

Uuringu eesmärgiks oli analüüsida Mobiil-ID turvalisust tema väljaandmisel ja kasutamisel, vaadeldes Mobiil-ID elutsükli kõiki etappe ning lähtudes seejuures Eesti ID-kaardi turvalisusest samades alamlõikudes. Eraldi uuriti Mobiil-ID võimalikku kasutuselevõttu ja sellest tulenevaid ohte e-hääletamisel.

Hindamisel lähtuti ID-kaardi turvalisusest - muuhulgas, kui Mobiil-ID turvalisus polnud väiksem kui ID-kaardi turvalisus, siis loeti seda piisavaks. Nendest põhimõtetest lähtudes analüüsiti Mobiil-ID kasutamise seotud kriitilisi ohte, riske ja võimalikke ründeid, uurides süstemaatiliselt läbi Mobiil-ID-ga seotud protsessid, osapooled, süsteemid ja kommunikatsioonid. Analüüsisides Mobiil-ID võimalikku kasutuselevõttu e-hääletamisel, lähtuti e-hääletamise üldkirjelduse ja turvaanalüüsi dokumentidest ning võeti arvesse eelnevas analüüsis saadud tulemused.

Mobiil-ID-le püstitatud nõuded

- **Konfidentsiaalsus** – kui seda on eeldatud, siis peab Mobiil-ID tagama andmete kättesaadavuse ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatuse kõigile ülejäänutele.
- **Terviklus** – kui seda on eeldatud, siis peab Mobiil-ID tagama andmete õigsuse, täielikkuse ning ajakohasuse, samuti päritolu autentsuse ja volitamatute muutuste puudumise.

Kuna Mobiil-ID on lisavõimalus ja ei välista ID-kaardi kasutamist, ei püstitata tema käideldavusele suuri nõudeid – ehk eeldatakse, et kui Mobiil-ID ei kindlusta eelnevalt kokkulepitud tööajal kasutamiskõlblike andmete õigeaegset ja hõlpsat kättesaadavust selleks volitatud tarbijaile, siis saab tema asemel kasutada näiteks ID-kaarti.

Mobiil-ID kasutamise seotud ohud ja riskid

Kuna Mobiil-ID-d saab kasutada mitmesugustes organisatsioonilistes, infrastruktuurilistes ja tehnilistes keskkondades, siis tulevad selle puhul kõne alla erinevad ohud, mida võib jagada järgmistesse kategooriatesse:

- Õnnetused, väärarnatu jõud
- Juriidilised probleemid, organisatsioonilised puudused
- Inimvead
- Tehnilised rikked
- Ründed

Analüüsitud ohud ja riskid on uuringus grupeeritud järgmiselt:

1. üldise iseloomuga ohud ja riskid, mis on seotud seadusandluse, krüptograafia, tarkvaraga;
2. tehnilised ohud ja riskid, mis on seotud Mobiil-ID kiibi, kiibi personaliseerimise ja transpordi, sertifitseerimisprotsessi, kasutaja arvuti, rakenduse serveri, DigiDocService, OCSP kehtivuskinnituse teenuse, mobiilioperaatori süsteemide ja teenuste, kasutaja telefoni, süsteemide vaheliste kommunikatsioonide, autentimis- ja allkirjastamisprotsessi, sertifikaadi peatamise, peatamise lõpetamise ja tühistamise ning muude objektide ja protsessidega;
3. e-hääletamisega seotud ohud ja riskid, mis on seotud e-hääletamise nõuete, protsessi ja süsteemidega.

Olulisuse seisukohast võib riskid jagada kolme rühma

1. Suur osa analüüsis vaadeldud Mobiil-ID riskidest on kas väga vähe tõenäosed või on nende tõenäosus ja mõju sama suurusjärku vastavate ID-kaardi riskide tõenäosuse ja mõjuga. Seega võib neid aktsepteerida.
2. Mitmete riskide leevendamiseks või probleemide lahendamiseks on uuringus pakutud soovitusi; peale nende rakendamist on jääkriskid kas väga vähe tõenäosed või on nende tõenäosus ja mõju sama suurusjärku vastavate ID-kaardi riskide tõenäosuse ja mõjuga. Seega võib vastavaid riske aktsepteerida peale uuringus toodud soovitusi rakendamist.
3. Lisaks eelpoolnimetatutele jäävad Mobiil-ID lisariskid, mida tuleb aktsepteerida, eriti e-hääletamise puhul.

Dokumendi EH-02-01: "E-hääletamise kontseptsiooni turve: analüüs ja meetmed" jaotises 5.6 on toodud e-hääletamise puhul aktsepteerimist vajavad riskid. Lisaks neile **on vaja aktsepteerida järgmisi lisariske**, mis on seotud võimaliku Mobiil-ID kasutamisega e-hääletamisel.

- Mobiil-ID kasutamisel lisanduvad sotsiaalsel laadi ründed, mida saab mobiiltelefonidega kergemini seostada kui ID-kaardiga.
- Vajadus usaldada mobiilioperaatorite infrastruktuuri ja protseduure ning hääletaja mobiiltelefoni.
- Kliendi ja serveri vaheline vahendusrünne (eeldab näiteks, et klient on eelnevalt juhutatud rakenduse veebisaidi asemel ründaja veebisaidile) on Mobiil-ID puhul kergemini teostatav kui ID-kaardi puhul.

- Kui ID kaardi kasutuselevõtt e-hääletamisel oli tagatud sellega, et enamikel võimalikest valijatest oli ID kaart - ja seega ka põhimõtteline võimalus valida - olemas, siis Mobiil-ID puhul on inimeste arv, kellel Mobiil-ID olemas on, esialgu tunduvalt väiksem. Seega lisandub e-hääletamise korral seoses Mobiil-ID kasutamisega hääletuse ühetaolisuse nõude mittetäitmise võimendumise lisarisk.

Enne kui kasutada e-hääletamisel Mobiil-ID-d, on soovitatav kõigi Eesti olulisemate mobiilioperaatorite kaasamine. See toob kaasa lisariski, mis on seotud suurema arvu e-hääletamise osapoolte usaldamise vajadusega.

Mobiil-ID kaardi (nagu iga kõrgete turvanõuetega objekti) reaalne turvalisuse tase sõltub väga suurel määral konkreetsete protseduuride, meetmete, süsteemide jne realisatsioonist konkreetsete isikute, organisatsioonide, infrastruktuuri, riistvara, tarkvara ja kommunikatsioonide keskkonnas antud ajamomendil.

Uuringu põhieesmärk oli Mobiil-ID turvalisuse analüüs tema väljaandmisel ja kasutamisel. Töö käigus tekkisid ka mitmed soovitused. Hindamise põhjal antud soovitused on jagatud nende prioriteetsuse järgi kahte klassi (kõrge ja keskmine prioriteet).

Kõrge prioriteediga soovitused toovad välja erinevad tööd mis võivad tõsta Mobiil-ID turvalisust. Valikuline lühikokkuvõte kõrge prioriteediga soovitustest:

- Mobiil-ID on seadusandlikul tasemel reguleeritud vaid kaudselt, digitaalalkirja seaduse raames. Kui Mobiil-ID-d käsitletakse sama taseme mõistena nagu ID-kaarti, ("Eesti Vabariigi e-identiteet"), siis tuleks kaaluda ka ID-kaardiga analoogiliste seadusesätete sisseviimist (nt dokumendi kuritarvitamise kohta).
- Lisaks avalikkuse harimisele arvutite ja ID-kaardi turbega seotud teemadel, tuleks avalikkust harida ka Mobiil-ID ohtudega seotud teemadel (muuhulgas rõhutades, et ei tohiks ära anda ei mobiiltelefoni ega Mobiil-ID PIN-koode).
- Pakkuda kasutajatele soovitusi oma mobiiltelefonide turvalisuse parendamiseks, analoogiliselt soovitustega arvutite turvamiseks. Eriti tuleks seda teha seoses Mobiil-ID-ga, muuhulgas ka Mobiil-ID-d tutvustavatel ning e-hääletamise veebisaitidel.
- Säilitada aktiveerimine. Küsida aktiveerimise käigus kasutaja telefoninumbrit. Teatada aktiveerimisel kasutajale, millise telefoninumbri on aktiveeritud sertifikaat seotud ning lasta kasutajal teha testautentimine ning testalkirjastamine. Eelpoolmainitud toimingud tuleks teha ka korduval aktiveerimisel.
- Luua kasutajale lihtne võimalus ülevaate saamiseks kõigist oma kehtivatest sertifikaatidest, kaasa arvatud Mobiil-ID sertifikaadid – seda eriti juhul, kui Mobiil-ID-d peaks kasutatama e-hääletamisel. Mobiil-ID sertifikaatide info peaks olema teatatud koos vastava telefoninumbri äratoomisega.
- Püstitada nõuded Mobiil-ID protsessi osapooltele (kiibi, operatsioonisüsteemi ja rakenduse tootjad; personaliseerija; ladustaja; mobiilioperaatorid; teenusepakkujad jne) ning kontrollida nende täitmist.
- Enne kui kaaluda Mobiil-ID kasutuselevõttu e-hääletamisel, peaksid olema kaasatud peamised Eesti mobiilioperaatorid.

- Enne kui kaaluda Mobiil-ID kasutuselevõttu e-hääletamisel, peaksid olema realiseeritud vähemalt käesolevas uuringus toodud kõrge prioriteediga soovitused.

Keskmise prioriteediga soovituste alla koondati peamiselt ettepanekud, mida Mobiil-ID osapooled võiksid jälgida pikemas perspektiivis, et nende süsteemid vastaksid IT turvalisuse trendidele maailmas. Keskmise prioriteediga soovitused puudutasid muuhulgas järgnevaid teemasid:

- Nii ID-kaardi kui ka Mobiil-ID puhul tuleks kaaluda ülemineku ettevalmistamist RSA algoritmile võtmepikkusega 2048 bitti ning SHA-2 variantide kasutamisele, eriti alates 2010.a.
- Kaaluda arengut Common Criteria (või minimaalselt, selle aluseks olevate põhimõtete) rakendamise suunas ID-kaardi, Mobiil-ID ja e-hääletamise tarkvara arendamisel.

Uuringu tulemus – esitatud soovituste täitmisel ja lisariskide aktsepteerimisel võib Mobiil-ID-d kasutada võrdväärselt ID-kaardiga

Suur osa analüüsis vaadeldud Mobiil-ID riskidest on kas väga vähe tõenäosed või on nende tõenäosus ja mõju sama suurusjärku vastavate ID-kaardi riskide tõenäosuse ja mõjuga. Seega võib neid aktsepteerida.

Enne Mobiil-ID kasutamist e-hääletamisel tuleks realiseerida vähemalt uuringus pakutud kõrge prioriteediga soovitused.

Lisaks dokumendi "E-hääletamise kontseptsiooni turve: analüüs ja meetmed" jaotises 5.6 toodud lisariskidele on vaja aktsepteerida ka ülal toodud lisariske, mis on seotud võimaliku Mobiil-ID kasutamisega e-hääletamisel.