



Õiguskantsler

Teie 24.09.2015 nr

Meie 03.11.2015 nr 6-1/151316/1504819

Isikutuvastus e-hääletamisel

Austatud avaldaja

Leian, et ID-kaart on sobiv valimistel e-häält andva isiku tuvastamiseks, sest ID-kaart kui digitaalne isikutunnistus on läbi mitme tehnilise ja õigusliku meetme seotud selle omanikuga. ID-kaarti kasutamine e-hääletaja tuvastamiseks ja e-hääle kinnitamiseks on kirjeldatud <http://www.vvk.ee/valijale/e-haaletamine/>.

Teie mure e-hääletuse turvalisuse pärast on arusaadav. Hääletamise korraldust tulebki pidevalt kriitiliselt hinnata ja vajadusel uuendada, et viia kuritarvituste ning eksituste võimalused miinimumini. Tuginedes sõltumatutele rahvusvahelistele eksperthinnangutele võib kinnitada, et Eestis on valimiste korraldus aus ja korrektne.

Valimiste üldisuse põhimõttest lähtudes peab ka hääletamise korraldus muutuma, mh arvestama inimeste suurenenud mobiilsust. Mitmes riigis, nt Saksamaal, on üha populaarsem kontrollimata keskkonnast lihtkirja teel hääletamine. Paljud riigid püüavad sisse viia interneti teel hääletamist, kuivõrd see on turvalisem alternatiiv kirja teel hääletamisele. Osa riike kasutab mitme kuu pikkust eelhääletuse perioodi, ent ka sellega kaasnevad oma riskid.

Kõikidele kohustuslik ID-kaart digitaalse isikutuvastuse ja digiallkirjastamise funktsiooniga on üks parimaid viise valija veatuks tuvastamiseks. ID-kaarti usaldusvärsus e-hääletamisel sõltub peamiselt kahest küsimusest: kuidas ID-kaart on seotud isikuga ja kui turvaline on ID-kaardi arvutivõrgu kasutamise tehniline lahendus. Järgnevalt on neid käsitletud lühidalt.

Eesti ID-kaart on isiklik isikutunnistus, mis antakse kasutamiseks ainult kaardil märgitud isikule. ID-kaart kehtib nii füüsilise isikutunnistusena (nt isiku tuvastamiseks pangakontoris) kui ka digitaalse isikutunnistusena (nt isiku tuvastamiseks internetipangas).

Arvutivõrgu kaudu ID-kaardiga hääletades peab üheselt olema tuvastatav ID-kaardi autentsus ja kaardiga seotud isiku samasus. Selle tagamiseks on nähtud ette:

- Füüsiline ID-kaart, mis on antud kasutamiseks ja isiku tuvastamiseks üksnes sellele isikule, kelle isikuandmed on kaardile kantud (*ID-kaardi kasutaja*).
- ID-kaardi sertifikaadid, mis laetakse ID-kaardile ja mida ID-kaardi kasutaja arvutivõrgu kaudu sertifitseerimiskeskusest perioodiliselt uuendab. Nii sertifikaatide uuendamiseks kui ka kõigi teiste ID-kaardiga tehtavate toimingute tarvis vajab ID-kaardi kasutaja PIN-koode.
- ID-kaardi sertifitseerimiskeskus, mis ID-kaardiga tehtava iga elektroonilise toimingu korral autendib ID-kaardi ja selle sertifikaadid.

- Kaks PIN-koodi, mis on unikaalselt seotud ID-kaardiga. PIN1 on ID-kaardi (ja selle kaudu isiku) tuvastamiseks, PIN2 on digiallkirja andmiseks. PIN-koodid on antud valdamiseks ja ID-kardiga kasutamiseks üksnes sellele isikule, kelle isikuandmed on kaardile kantud. E-häält andes inimene kõigepealt tõendab oma isikut, sisestades selleks ID-kaardi PIN1 koodi, ja seejärel hääletab ehk kinnitab digitaalalkirjaga oma valiku, sisestades selleks ID-kaardi PIN2 koodi.
- Kasutaja arvutisse installeeritav ID-kaardi haldus- jm tarkvara, kaardilugeja ajur, nendega ühilduv veebilehitseja jm tarvilik tarkvara.
- Valijarakendustarkvara, mida vastavalt vajadusele üha uuendatakse ja täiendatakse. Selle laeb alla ja käivitab ID-kaardi kasutaja.

E-hääletamist on võimalik ka testida. Proovihääletamisega saab hääletaja kontrollida, kas tema arvuti on õigesti seadistatud ning kas ID-kaardi sertifikaadid ja PIN-koodid kehtivad.

Infotehnoloogiliselt on tagatud, et e-hääletamisel isikut identifitseerivad andmed ja isiku antud hääle on hääle ülelugemiseni lahutamatud. E-hääletamise süsteemis on anonüümne isikutuvastus ja ühekordne hääletamine tagatud sarnaselt eelhääletamisel väljaspool elukohta kasutatava nn kahe ümbriku süsteemiga.¹ Identifitseeritud e-hääletaja antud hääle šifreeritakse ehk suletakse „sisemisse ümbrikusse“. Kui e-hääletaja kinnitab oma hääle digiallkirjaga, lisatakse šifreeritud häälele (ehk suletud „sisemisele ümbrikule“) „välimine ümbrik“ hääletaja isikuandmetega. Kuni hääle kokkulugemiseni valimispäeval säilitatakse iga šifreeritud hääle ja hääletaja isikuandmed koos. Selle otstarve on tagada, et ka korduvalt hääletades saab isik anda vaid ühe hääle. Korduva hääletamisega on valijale antud võimalus vabaneda võimalikest kõrvalistest mõjutajatest (nn „virtuaalne valimiskabiin“). Pärast korduvhääletamise kontrollimist ja eelnevate korduvhääle kustutamist eemaldatakse isikuandmed häälest. E-hääle ülelugemine ehk „sisemise ümbriku“ avamine on võimalik üksnes pärast e-häälele lisatud isikuandmete ehk „välimise ümbriku“ eemaldamist (meetmega tagatakse hääletamise salajasus). Isikuandmed eemaldatakse e-häälest valimiskomisjoni liikmetele jaotatud digivõtmete abil pärast valimisjaoskondade sulgemist ja enne hääle ülelugemist.

ID-kaardi ja digiallkirja kasutatavus ja turvalisus rajaneb ka inimeste üldisele usaldusele nende vahendite suhtes. See usaldus on enim leidnud kinnitust interneti-panganduses – kui inimesed oskavad ja usaldavad sel viisil kasutada ja kasutada oma (isiklikke) rahalisi vahendeid, küllap nad oskavad ja usaldavad seda teha ka oma poliitiliste tahteavaldustega. e-Riigi Akadeemia eestvõttel on koostöös erakondadega töötatud välja ausa e-hääletamise põhimõtted.²

Lisaks tehnilistele ja usaldusmeetmetele on rakendatud ka mitmeid karistusõiguslikke meetmeid. Kuritegudena on karistatavad järgmised rikkumised, mis otse või kaude võivad puudutada e-hääletaja isikusamasust ja tuvastatavust.

- 1) *Valimispettus*: valimisel või rahvahääletusel osalemine ilma hääleõiguseta või teise isiku nimel.³
- 2) *Tähtsa isikliku dokumendi kuritarvitamine*: teise isiku nimele väljaantud ID-kaardi kasutamine eesmärgiga kasutada teise isiku valimisõigust, samuti selleks enda nimele väljaantud ID-kaardi teisele isikule kasutamiseks andmine.⁴
- 3) *Valimisvabaduse rikkumine*: inimese takistamine valida või hääletada, samuti talle vara või soodustuse lubamine või andmine eesmärgiga mõjutada teda mitte valida või hääletama, või

¹ Vt E-hääletamise süsteemi lühikirjeldus: <http://www.vvk.ee/valijale/e-haaletamine/>.

² Vt <http://www.vvk.ee/valijale/e-haaletamine/e-haaletamise-hea-tava-3/>.

³ Karistusseadustiku (KarS) § 165. <https://www.riigiteataja.ee/akt/125092015007>.

⁴ KarS §-d 349 ja 350.

mõjutada teda valima või hääletama teatud valiku kasuks, samuti samal eesmärgil inimese mõjutamise eest, kasutades ametiseisundit, vägivalda, pettust või sõltuvust süüteo toimepanijast.⁵

- 4) *Hääletamissaladuse rikkumine*: valimisel või rahvahääletusel teise inimese tehtud valikuga ebaseaduslik tutvumine.⁶

Kõigi hääletamisviiside juures – eelhääletamisel, hääletamisel kodus, hääletamisel kinnipidamiskohas, hääletamisel välisriigis jne – on võimalikud väga erinevad hüpoteetilised rikkumised. Eelhääletamine ei ole erand. Selle riskid on lihtsalt teistsugused. Riskide hindamise üheks aluseks on tõenäosus, kui massiline võib hüpoteetiline rikkumine olla. Riskide esinemine – kui need ei ole oluliselt suuremad teiste hääletamisviiside riskidest – ei tohiks takistada valimisaktiivsust või valijate valikuvõimalusi suurendavate innovaatiliste vahendite kasutuselevõttu.⁷

Lugupidamisega

/allkirjastatud digitaalselt/

Ülle Madise

Mario Rosentau
Mario.Rosentau@oiguskantsler.ee

⁵ KarS § 162.

⁶ KarS § 166.

⁷ Seda põhimõtet kinnitas Riigikohus juba 2005. aastal: vt RK otsuse nr 3-4-1-13-05 p.-d 25 ja 26. Internetis: <http://www.nc.ee/?id=11&tekst=RK/3-4-1-13-05>.