Vabariigi valimiskomisjonile

Märt Põder
sündinud 11.09.1979
elukohaga Jakobi 13-2, Tartu 51006
kontaktitav gafgaf@infoaed.ee

VALIMISKAEBUS EUROOPA PARLAMENDI VALIMISTEL 2024

Minule teadaolevalt loeti 9.06.2024 häältelugemise käigus kokku kuni 153 269 kehtetu digiallkirjaga või korrektse digiallkirjata e-häält. Seejuures kontrolliti protseduuride käigus väidetavalt edastatud konteinerite vastavust digiallkirja vormingule (lisa 1), kuid tuvastati ainult 13 vormingule mitte vastavat häälekonteinerit (lisa 2).

See ei saa olla korrektne tulemus, sest teadaolevalt ei salvesta e-hääletuse süsteem häälekonteinereid korrektse digiallkirjaga, vaid hoiab digiallkirja kehtivuskinnitusi konteinerist eraldi (vt kontrollakendusega valimiste käigus allalaaditud näidishääled lisas 3 ja 4, mille kohta standardne Digidoc tööriist kinnitab faili avamisel, et tegu on kehtetute digiallkirjadega).

Seejuures määratleb VVK oma 20.09.2023 otsuses nr 92, et "elektrooniliselt allkirjastatud elektrooniline hääl on digitaalselt allkirjastatud fail" ja kuigi sealt on eemaldatud eelmises samasisulises 10.10.2022 otsuses nr 47 mainitud `ASiC-E LT` konteinerivormingu nõue, mida 2023. aasta Riigikogu valimiste häälekonteinerid samuti ei täitud, siis selle lühendi eemaldamine ei muuda digiallkirja nõuetele mitte vastavaid häälekonteinereid nõuetele vastavaks, vaid kutsub otsima täpsemat määratlust madalama taseme regulatsioonist nagu 14.05.2024 kuupeävaga "IVXV protokollide kirjeldus":

> "Käesolev spetsifikatsioon näeb ette Eesti Vabariigi Standardikavandis [BDOC2.1] defineeritud BDOC allkirjavormingu kasutamise. /—/ Käesolev septsifikatsioon näeb ette hääle kvalifitseerimiseks nii OCSP kehtivuskinnituse kui PKIX ajatempli võtmise. Sellisena on lõplik, kvalfitseeritud hääl, BDOC-TS vormingus." (lk 10)

Seejuures ei tee töötlemisrakendus kindlaks vastavust BDOC2.1 standardikavandile ja selles määratletud BDOC-TS vormingule, vaid hälbib sellest, sest kuulutab korrektseks, st mitte vigaseks

või kehtetuks digiallkirjad, mis on standardi järgi kehtetud või vigased.

Tegelikult on elektroonilise hääle määratlus VVK otsuses nr 92 vigane, sest elektooniline hääl on korraga:

- "digitaalselt allkirjastatud fail, mille nimi on teksti kujul e-hääletamise aeg (ajatempel)" (3.1)
- "krüpteeritud Riigikogu valimiste seaduse § 48^3 lõike 3 alusel hääletamiseks loodud elektrooniliste häälte salastamise võtmega andmefail", mille "nimi algab valimiste või rahvahääletuse identifikaatoriga ja lõpeb küsimuse identifikaatoriga" ja mille "laiend on .ballot" (3.2)

Seejuures on viga olnud teada juba läbi mitme valimistsükli, nt tõi selle esmalt välja Artur Boiko, kelle kirjeldatud puudusele vastas RIA esindaja 2021. aasta oktoobriss asutuse blogis "Kuidas allkirjastatakse e-hääli?" eksitavalt, et kirjasaatja kätte saattusid failid olukorras, kus hääletamisprotsess oli alles pooleli:

> "Ajakirjandusele kirja saatnud inimene võttis BDOC failid oma arvutis välja siis, kui hääletamisprotsess oli veel pooleli. Seda saab vastavate oskuste olemasolul teha iga arvutikasutaja. Sel hetkel oli e-hääl krüpteeritud ning signeeritud. Selleks, et tegemist oleks digitaalselt allkirjastatud dokumendiga, peaks sellele BDOC failile olema lisatud veel ajatempel ja isiku sertifikaadi kehtivuse kontrolli vastus. Need võetakse aga serveri poolel, kuhu kasutajal puudub ligipääs. Serveris lisatakse failile ajamärgend ning AS SK ID Solutions käest saadud sertifikaadi kehtivuse info."

See on osutunud valeks nagu ka on eksitavad olnud 2023. aasta Riigikogu valimistele järgnenud selgitused sellest, et digiallkirjad ei saagi olla kehtetud:

> "Digiallkiri ei saa olla kehtetu, allkiri kehtib alati, nagu ka inimese füüsiline allkiri. Kehtetu saab olla sertifikaat ja sellisel juhul kehtiva allkirjaga dokument, mille andmise ajal sertifikaadid ei kehtinud – allkirjastatud dokument ei kehti. Digiallkirjad ei ole kehtetud, sest digiallkirjad on antud ID kaardi või Mob-ID-ga ja sertifikaatide kehtivuskinnitus asub koos häälega valimiskastis."

Seejuures on olnud veelgi hilisemad selgitused sama eksitavad ja ka

vastuolulised väites kord, et e-hääletuse puhul eiratakse digiallkirja standardit selleks, et tagada valimiste *salajasust*, aga siis jällegi, et hääletuskasti *terviklust*.

Ilmselt pole ei VVK ega RVT võimuses defineerida ümber seda, mis on digiallkiri ja kuigi valimiste korraldaja veebisaidi "E-hääletamise faktikontroll: müüt ja tegelikkus" sektsiooni alles 2024. aasta veebruaris ilmunud uus alajaotis kehtetute digiallkirjade teemal kinnitab, et vajadusel parandab RVT digiallkirjade konteinerid selleks spetsiaalselt loodud rakendusega, siis a) seda teadaolevalt 2024. aasta e-häälte töötlemise käigus ei tehtud ja b) pole selge sellise parandamise õiguslik tähendus, sest RKVS §48^4 lg 1 järgi peab valijarakendus võimaldama "valijal valijarakenduse abil teha valiku, selle krüpteerida, digitaalselt allkirjastada ning saata elektrooniline hääl käesoleva lõike punktis 3 nimetatud koguja komponendile".

Midagi sellist ametlik valijarakendus teadaolevalt ei võimalda, vaid digitaalse allkirja asemel võimaldab see anda heal juhul krüptograafilise signatuuri, millel puudub vahetu õiguslik tähendus digiallkirja mõttes, ka annab kontrollrakendus valijale tagasi kehtetu digiallkirjaga häälekonteineri (näidised lisades 3 ja 4).

VVK kehtestatud hääletussedeli vormile mitte vastavad häälekonteinerid tuleks RKVS §60^1 lg 6 järgi kuulutada kehtetuks – kuigi e-hääle õigusliku alamääratletuse tõttu seaduse tasemel pole päris selge, mida see peaks tähendama, sest ei "kehtetu sedeli" ega "kehtetu hääle" terminit pole ühemõtteliselt defineeritud ega anna selle määratlusest aimu ka VVK otsused.

Sain puudusest teada häälte kokkulugemise protseduuride käigus ja taotlen e-hääte lugemist seaduse nõuetele vastavalt, mille järgi tuleb jätta valimistulemuse kindlakstegemisel kõvale VVK kehtestatud vormile mitte vastavad e-hääled ja/või häälekonteinerid – seega tuleks jätta valimisstulemusse arvestamata kuni 153 269 e-häält.

Lisad

1. `lisa_1_vormingule_vastavus.jpg`
2. `lisa_2_vigase_allkirjaga.jpg`
3. `lisa_3_Khlc_sbETRok9FZ4Z+OOPQ==.asice`
4. `lisa_4_w6KnjW4njpshIGR6gLwcLw==.asice`