Advokaadibüroole LEVIN OÜ

Märt Põder | Infoaed OÜ
+372 55643754 | tramm@infoaed.ee
17. märtsil 2023 Tartus

EKSPERTHINNANG

Kuidas riivab IVXV häälekontrolli süsteem hääle salajasust?

Eestis kehtiv IVXV e-hääletuse protokoll võimaldab valijal kontrollida oma isikliku hääle jõudmist valimisserverisse kuni 30 minuti jooksul pärast hääle andmist. Selle käigus tagastatakse valijale edastatud ruutkoodi (QR-kood) alusel digiallkirjastatud konteineris tema e-hääle krüptogramm ehk krüpteeritud sedel, mille saab avada ruutkoodis sisalduva krüptovõtmega.

Sellisel viisil antakse valijale digiallkirja tõendusjõuga tõend tema antud häälest, mida saab küll alla laadida vaid 30 minuti jooksul, kuid mille võib salvestada igaveseks, kui kasutada selleks sõltumatut kontrollrakendust. Tegelikult võib ruutkoodi alusel laadida valija hääle alla kestahes, kui ta suudab ruutkoodi lugeda nt arvutiekraanilt avalikus kohas, kodus või arvutisse paigaldatud ekraanilugeja abil.

Kui kasutada allalaaditud konteinereid kombineerituna AS Sertifitseerimiskeskuse poolt võimaldatud ID-toimingute logidega ning hankida valimisteenistuselt vastavalt nende endi soovitustele kinnitus selle kohta, et lugemisele läks valija e-hääl ja mitte pabersedelil hääl, siis on võimalik valijal kolmandatele osapooltele digiallkirja kindlusega tõendada, kelle poolt ta hääletas.

Rahvusvahelised regulatsioonid, mis pole küll õiguslikult siduvad, kuid mida käsitletakse Eestis kohaste abivahenditena põhimõtete nagu hääletamise salajasus jmt tõlgendamisel e-hääletuse kontekstis lubavad järeldada, et sellised võimalused oma hääle tõendamiseks on otseselt hääle salajasust riivavad ning sellise protokolliga e-hääletus vastuolus üldtunnustatud demokraatlike valimiste põhimõtetega.

Valija isikliku hääle kontrolli lühikirjeldus

Eesti e-hääletuse protokollis võimaldati valija isikliku hääle kontroll 2013. aasta KOV valimiste ajal lähtuvalt OSCE 2011. aasta raporti soovitustest, mis lähtusid ajalootudengi Paavo Pihelga poolt demonstreeritud kliendirünnetest valimisrakenduse vastu.

Valija isikliku hääle kontrolli eesmärk on anda valijale võimalus kontrollida, et tema poolt valimiste korraldajale edastatud hääl jõudis kohale muutmata kujul, st seda ei muutnud või selle edastamist ei takistanud kliendiarvutisse paigaldatud pahavara.

Hääle kontrollimiseks kasutatakse valimisrakendusest ja kliendiarvutist sõltumatut kanalit, mille tagab valija käsutuses olev nutitelefon oma eraldiseisva operatsioonisüsteemi ja potentsiaalselt ka eraldiseisva Interneti-ühendusega.

Valija isikliku hääle kontrollimine koosneb kolmest sammust:

- Hääle edastamise järel häältekogujale näidatakse valijarakenduses valijale unikaalset ruutkoodi
- Valija kasutab oma nutitelefoni paigaldatud häälekontrollirakendust ruutkoodi lugemiseks arvutiekraanilt
- Häälekontrollirakendus laadib ruutkoodi alusel kontrolliserverist valija antud hääle, kuvab nutiseadme ekraanil kinnituse allalaadimise õnnestumisest ja antud hääle sisu, st valitud kandidaadi nime ja numbri

Sel viisil algsest valijarakendusest eraldiseisvat arvutisüsteemi, st nutitelefoni, ja selle potentsiaalselt eraldiseisvat Interneti-ühendust kasutades saab valija kinnituse, et häältekogumisserver on tema hääle vastu võtnud ja salvestanud. Kui valijarakenduse käitumist mõjutab pahavara, siis peaks valija sellest eraldi sõltumatut suhtluskanalit kasutades teada saama, kui just pole korraga ja eeldatavasti koordineeritult manipuleeritud nii arvuti, kus jookseb valimisrakendus, kui ka nutitelefon. Sel juhul on võimalik valija häält siiski manipuleerida, kuid valija isikliku hääle kontroll sõltumatus kanalis annab siiski tõendatult küllaltki suure kindluse, et seda pole tehtud.

Häälekontrolli salajasuse riive põhiolemus

IVXV e-hääletuse protokollil põhinev häälekontrolli mehhanism riivab hääle salajasuse põhimõtet mitte oma tehniliste vigade või puudujääkide, vaid protokolli taotlusliku ülesehituse tõttu. Hääle salajasuse riive tuleneb sellest, et häälekontrolli käigus võimaldatakse valijal tema antud häälega unikaalselt seotud ruutkoodi alusel laadida alla hääle digitaalne konteiner, mille juurde kuulub:

- Konteineri loonud isiku, st valija digiallkiri, mis tõendab digiallkirja seadusliku jõuga fakti, et tegu on valija loodud konteineriga
- Konteineris olev krüptogramm ehk krüpteeritud sedel, millel on kirjas valija hääl

- Ruutkoodis sisalduv krüptovõti krüptogrammi ehk krüpteeritud sedeli dekrüptimiseks

Selle info alusel on võimalik valijal tõendada digiallkirja jõuga, et ta on andnud hääle just selle kandidaadi poolt, kelle nimi dekrüpteerub konteineris olevalt krüpteeritud sedelilt. Konteiner sisaldab ka muid digiallkirjastatud konteineriga kaasnevaid tunnuseid nagu ajatempel, mille alusel saab valija tõendada hääle andmise täpset aega.

Sellise tõendusjõuga informatsiooni andmine valija käsutusse ei vasta nt Euroopa Nõukogu soovituses CM/Rec (2017)5 e-hääletuse standardite kohta punkti 23 nõudele, et valija ei tohi saada antud hääle sisu tõendada kolmandatale osapooltele ja punkti 19 täiendavale nõudele, et valija hääle salajasus peab olema tagatud valimisprotseduuri kõigi etappide käigus. Nende punkte täie rangusega tõlgendades võib järeldada, et valija ei tohi saada tõendada oma antud häält ka juhul, kui ta selle ülehääletamisega hiljem tühistab nagu seda võimaldab Eesti e-hääletuse protokollistik selle loomisest peale.

Digiallkirjastatud hääle tõendamine kehtiva häälena

Kuigi ülehääletamise võimalust võib tõlgendada n-ö pehmendava asjaoluna hääle salajasuse ilmsele riivele, siiski saab valija soovi korral tõendada oma e-hääle sisu täiel määral, kui kasutab tõendamiseks täiendavaid andmeallikaid nagu nt AS Sertifitseerimiskeskuse poolt võimaldatud ID-toimingute logi, mille vahendusel on ligipääsetavad kõigi valija antud digiallkirjade ajatemplid.

Järgenva kirjelduse lihtsama mõistmise nimel märgime ära, et kui valija saab tõendada, et ülal kirjeldatud viisil alla laaditud konkreetne häälekonteiner on tema *kõige viimane häältekogumise serverisse laaditud konteiner*, siis on valija digiallkirja seadusliku jõuga tõendanud, et selles konteineris sisalduv ja ruutkoodis oleva krüptovõtme abil dekrüpreeritav hääl on tema kehtiv e-hääl.

Äärmusliku abinõuna saab valija tõendada, et tegu on viimase tema antud häälega, nt hävitades e-hääle andmise järel selleks kasutatud ID-kaardi füüsiliselt, nt purustades haamriga selle kiibi. Hääle tõendamise skeemi näitlikustamiseks sobib e-hääle andmine ja seejärel selleks kasutatud ID-kaardi hävitamine hästi ning pole kahtlust, et sel juhul on see tõepoolest viimane *selle ID-kaardi abil antud hääl*. Siiski on see äärmuslik võimalus, sellega kaasnevad kulud ja asjaajamise tüli, kuid see jätab lahti

ka täiendava võimaluse, et valijal on tagavaraks Digi-ID, mida saab tellida ID-kaardile lisaks, või kasutab ta Mobiil-ID teenust, millega annab ta siiski uue e-hääle.

Ent äärmusliku abinõu asemel on märksa lihtsam viis oma viimase hääle tõendamiseks ning selleks piisab, kui valija laadib endale ID-kaardi hävitamise asemel alla ID-toimingute logi, kust on näha tema digiallkirjade ajatemplid ajalises järgnevuses. Kui konkreetse allalaaditud konteineri ajatempel vastab viimasele allkirjastamise ajatemplile ID-toimingute logis kuni e-hääletuse perioodi lõpuni, siis tähendab see, et valija pole pärast e-hääle andmist kasutanud ID-kaarti digiallkirjastamiseks, st pole ka andnud uut e-häält pärast konkreetse e-hääle edastamist hääletekogumisserverile.

Kuigi võib olla mõnevõrra tülikas vältida digiallkirjastamist kuni e-hääletamise perioodi lõpuni, siiski pole see suur pingutus, kui valija tõepoolest soovib tõendada oma e-hääle sisu, sj pole selleks vaja hävitada ID-kaarti ega anda seda kellegi kätte hoiule vmt, et niimoodi veenda kedagi oma e-hääle lõplikus kehtivuses. Ebamugavuste vähendamiseks on tark anda selline tõendatav e-hääl nt e-hääletuse viimasel päeval või isegi tunnil, mis vähendab digiallkirjade vältimise aega miinimumini.

Kuna ID-toimingute logis on toodud ära kõigi valija e-hääletuseks sobivate digitaalsete isikutunnistuste (ID-kaart, Digi-ID, Mobiil-ID) digiallkirjastamiste ajatemplid, siis saab tõendada ka seda, et valija ei kasutanud neist pärast tõendatava konteineri allkirjastamist ühtegi. Kuna logis tuuakse ära ka muid toiminguid ning e-hääletamise toimingu tuvastamiseks logis on ka täiendavaid võimalusi, nt pöördumiste IP-aadressid, siis saab valija tehniliselt teadlikule huvilisele tõendada oma häält ka juhul, kui ta on pärast viimase konteineri allkirjastamist andnud veel digiallkirju – ent nende täiendavate võimaluste kirjeldamine ei kuulu selle eksperthinnangu raamidesse.

Oleme ülal näidanud ära, et:

1) Valija saab alla laadida oma e-hääle digiallkirjastatud kujul ning kuvada selle hääle sisu, st valitud kandidaadi nime ja numbri

2) Valija saab tõendada e-hääle andmise aega ning lisaks fakti, et e-hääletamise perioodil pole ta hiljem ühtegi digiallkirja andnud

3) Sellega tõendab ta digiallkirja seadusliku jõuga, et konkreetse e-hääle näol on tegu tema kehtiva e-häälega

Isegi kui ülehääletamise võimalust võis käsitleda pehmendava

asjaoluna hääle salajasuse riivele, siiski ei ole mõeldav, et see vastaks Euroopa Nõukogu soovituses CM/Rec (2017)5 e-hääletuse standardite kohta punkti 19 nõudele, et hääle salajasus on tagatud kõigi hääletuse etappide jooksul, kui käsitleda e-hääletust eraldiseisva etapina, mis lõppeb n-ö ametliku valimispäevaga, mil on valijal võimalik alates 2021. aasta KOV valimistest esmakordselt e-hääl omakorda ülehääletada.

Antud e-hääle tõendamine kokkuloetud häälena

Selleks, et lõplikult tõendada kehtivat e-häält *kokkuloetud häälena*, on vaja lisaks tõendada, et valija ei hääletanud valimispäeval e-häält üle pabersedeliga. Kuni 2021. aastani polnud selleks vaja pingutusi teha, kuid 2023. aasta Riigikogu valimistel tuleb selle tõendamiseks kirjutada valimisteenistusele digiallkirjastatud isikuandmete päring, mille tulemusena annab valimisteenistus vastuse, kas valimistel läks arvesse valija e-hääl või pabersedelil hääl.

Kui valimisteenistus kinnitab, et lugemisele läks valija e-hääl, siis on valijal võimalik ülejäänud enda valduses oleva informatsiooni abil võimalik tõendada, kelle poolt ta hääletas.

See ongi ilmselt kõige mugavam tõendada e-häält kokkuloetud häälena, kuid valijal võib olla soov teha seda valimiskomisjonist sõltumatult. Üks lihtne võimalus on mitte minna valimispäeval valimisjaoskonda, kuid see on tülikas ning ka samavõrra tülikas tõendada. Kõige lihtsam pabersedeil mitte üle hääletanud olemise tõendamiseks oleks ilmselt tõendada seda samal viisl nagu teeb seda valimisteenistus, st valijate nimekirjade põhjal, mida edastatakse valimiste infosüsteemi kaudu ja millele on ligipääs vähemalt osaliselt valimisjaoskondades. Kuna tegu on tavaliste isikuandmetega, siis on neile ilmselt laiemalt ligipääs kõigil, kellel on ligipääs valijate nimekirjadele, millega varustab valimiste läbiviijaid rahvastikuregister ja mille haldamisega kaasnes 2023. aasta Riigikogu valimiste e-hääletuse alguses omajagu segadust.

Sellist tõendamist lugemisele läinud häälena on ehk lihtsam kujutada ette häälteostu raames, mille tarvis võib pidada sellise nimekirja hankimist pärast valimisi üpris proportsionaalseks pingutuseks. Nii võib teha kokkuleppe hääle ostuks/müügiks valimiste ajal, aga hääle tõendamise ning tasu üleandmise lükata hilisemasse aega, kui valija esitab oma tõendid hääle kohta, st ID-toimingute logid ja allalaaditud konteineri, mida seejärel häälteostja kõrvutab nimekirjaga sellest, kas valija piirdus e-hääletamisega või hääletas selle üle pabersedeliga.

Tavapäraseks hääle tõendamiseks piisab aga siiski isikuandmete

päringust valimisteenistusele, mis on selleks kõige lihtsam viis. Selline tõendamine pole kindlasti kooskõlas Euroopa Nõukogu soovituses CM/Rec (2017)5 e-hääletuse standardite kohta punktis 23 seatud nõudega, et valija ei tohi saada kolmandatele osapooltele tõendada enda antud häält.

Eesti IVXV e-hääletuse protokoll on kujundatud sellisena, et valija mitte lihtsalt ei saa kolmandatele osapooltele anda kaudseid tõendeid oma häälest nagu pabersedelitega hääletades oleks foto hääletussedelist (võib sedeli rikkuda, selle tagastada ja küsida jaoskonnast uue sedeli, millega tegelikult hääl anda), vaid otsese ja digiallkirja jõuga tõendatud koopia oma tegelikust häälest valimistel.

Abivahendid häälte allalaadimiseks ja tõendamiseks

Kuna ruutkoodiga kontroll võimaldab häälekonteineri allalaadimist valimisrakendusest sõltumatus seadmes, siis ei toimu hääle allalaadimisel valija autentimist nagu see toimub valijarakenduses. See tähendab, et valija hääle võib ruutkoodi ja kontrollrakenduse abil alla laadida igaüks, kes suudab lugeda valija arvutiekraanilt välja valijarakenduse poolt kuvatud ruutkoodi. Kuna ruutkoodi alusel e-hääle allalaadimine on lubatud vaid 30 minutit pärast hääle andmist, seab see sellisele allalaadimisele piirangud, ka on allalaadimiste piirarv kolm iga antud hääle kohta.

Tülikas piirang nutiseadmesse laaditava ametliku häälekontrolli rakenduse juures on veel see, et see ei võimalda mugavalt häälekonteinerit koos digiallkirjaga salvestada, vaid laadib selle kõigest operatiivmällu ning toimetab sellega seal, näidates vajadusel nutiseadme ekraanil valitud kandidaadi numbrit ja nime. IVXV protokolli võimaluste täiemahuliseks kasutamiseks on hea kasutada sõltumatut häälekontrolli rakendust, mille Infoaed OÜ lõi käesolevate valimiste vaatlemise tarbeks. Erinevalt ametlikust häälekontrolli rakendusest võimaldab see:

- Avada hääle ruutkoodi ning salvestada selles oleva krüptovõtme, hääle identifikaatori ja seansikoodi
- Laadida hääle identifikaatori alusel alla ja salvestada tervikliku häälekonteineri koos registreerimistõendite jm protokolli poolt konkreetsetest seadistustest lähtuvalt võimaldatud lisainfoga
- Dekrüpteerida ruutkoodis sisaldava krüptovõtmega häälekonteineris sisalduva krüptogrammi ehk krüpteeritud

sedeli ning vaadata valija tahteavalduse avateksti, st valija valitud kandidaadi numbrit ja nime

- Säilitada allalaaditud häälekonteineri edaspidiseks kasutamiseks soovitud ajaperioodiks, st 30 lubatud häälekontrolli minuti asemel kasvõi lõputult

Sõltumatu häälekontrolli rakendus võimaldab lisaks nendele välistele saadustele ka lähivaadelda e-hääletuse toimimist protokolli tasemel, mõista valijal selle olemust ning veenduda selle töökorras. Ka annab see võimaluse häälekontrolliks neile, kes mingil põhjusel ametlikku kontrollirakendust kasutada ei saa, nt ei oma nutiseadet või ei taha sinna lisarakendusi paigaldada.

Sarnaste vahendite abil on võimalik häälte allalaadimist ka automatiseerida ning teha seda massiliselt, mille tulemusel on võimalik IVXV protokolli sisseehitatud saljasuse riivet skaleerida eri manipulatsioonideks nagu valijate häälte kogumine arvutiekraanidelt nende teadmata (nt avalikus ruumis, töökohal arvutisüsteemide operaatorite poolt või levitatava pahavara abil) või häälte ost/müük ruutkoodide alusel – näiteks võib luua anonüümse veebiteenuse, kus ruutkoodi, ID-toimingute logi ja valimisteenistuse kinnituse üleslaadimise korral lubatakse valijale mõnda hüve.

Alternatiivid salajasuse riivega häälekontrollile

OSCE 2011. aasta raportis tegelikult ei soovitatud rakendada häälekontrolli, mis lekitab valijate digiallkirjastatud hääli ja on vastuolus Euroopa Nõukogu soovitusega CM/Rec (2017)5 e-hääletuse standardite kohta, vaid sõnastus kõlas:

> "Sellise individuaalse tõestatavuse aluseks on tavaliselt hääletajale antud kood, mis võimaldab tal hiljem kontrollida, kas tema hääl salvestati õigesti ja loeti õigesti üle."

Kuigi e-hääletuse arendajad tõepooolest viisid sisse valija individuaalse hääle kontrolli, ei teinud nad seda "hääletajale antud koodi" kujul, mistõttu ei vasta see kontroll ei demokraatlikele valimistele seatavatele nõuetele ega ka OSCE vaatlejate nõuetele, mida tuletati meelde ka nende 2019. aasta raportis:

> "ODIHR EET läbivaadatud tehnilistest ja käitusraamistikest ilmneb, et digitaalsetele hääletussedelitele ligipääsev siseründaja võib murda iga hääletaja hääle salajasuse, kes avaldab onlainis oma ruutkoodi pildi, mh pärast koodi kehtivuse lõppu. See on vastuolus hääletamise salajasust puudutavate riiklike

seaduste ja rahvusvaheliste standarditega."

Ettepaneku loobuda hääle salajasuse riivest OSCE poolt 2011. aastal soovitatud kontrollkoodi kasuks tegi 2019. aastal ka oma 11. ettepanekus e-hääletamise vigade parandamise töörühm, sj toetasid ettepanekut selle liikmetest Heldur-Valdek Seeder ja Märt Põder, pidades seda kõrge prioriteetsusega sammuks, ja Tanel Tammet, kes pidas prioriteetsust keskmiseks, kuid pidades kõrgeks keerukust, mida pidasid jällegi keskmiseks kaks ülejäänud ettepaneku toetajat.

Valimiste korraldajate ja tiimiliikmete nagu Tarvi Martensi, Arne Koitmäe, Jan Willemsoni, Martti Allingu, Mariko Jõeorg-Jurtšenko, Epp Maateni poolt esitatud eriarvamused väitsid, et muudatus aitaks kaasa häältemüügile ja oleks vastuolus Euroopa Nõukogu soovitusega CM/Rec (2017)5 e-hääletuse standardite kohta. Ka Tanel Tammet osutas, et kaasneb risk hääletamise salajasusele, kuigi kontrollkoodi puhul see risk tegelikkuseks ilmselt väheneks ning seda soovitab ka rahvusvaheline praktika, mida on püüdnud meie valimiste läbiviijale tutvustada välisvaatlejad jt.

Ruutkoodi-süsteemi tehnilised võimalused

Häälekontrolli rakendus töötab valijarakendusest maksimaalselt sõltumatus süsteemis ja maksimaalselt sõltumatu Interneti-ühendusega, mistõttu selle raames valijat ühegi täiendava vahendiga, sj telefoninumbri alusel vmt ei identifitseerita. See tähendab, et ruutkoodi alusel saab hääli alla laadida kestahes.

Kui valija annab hääle, siis toimub mitu järjestikust sammu, aga peamine neist on valija tahteavalduse kandmine digitaalsele hääletussedelile ja selle krüptimine valimiskomisjoni avaliku võtmega. Krüptimine käib Egiptuse krüptograafi Taher A Elgamali järgi nime saanud ElGamali algoritmi abil, kus krüptimiseks on vaja sõnumi vastuvõtja avalikku võtit ja lisaks on tarvis valida juhuarv ehk efemeerne võti.

Efemeerset võtit kasutatakse sõnumi krüptimiseks, kuid selle võib pärast krüptimist hävitada, sest vastuvõtja saab sõnumi avada oma avalikule võtmele vastava privaatvõtmega. Efemeerne võti tagab krüptitud sõnumi indeterministlikkust, st sama algsõnumi krüptimisel saadakse enamasti erinev krüptitud tekst ja seetõttu pole head võimalust teada, missugused sama võtmega krüptitud sõnumitest on sama sisuga.

Siiski saab krüptija ise selle efemeerse võtmega dekrüptida omaenda sõnumi, kui ta selle hoolimata selle nime poolt sugereeritud tarvitusest ikkagi alles hoiab. Nii teebki valijarakendus kahte

asja – ta edastab valimiste läbiviija avaliku võtmega krüptitud sõnumi häältekogumise serverile ja saab sealt vastuseks vastuvõetud hääle identifikaatori. Valijale näidatava ruutkoodi sisse kodeeritakse 1) efemeerne võti, 2) hääle identifikaator, 3) kasutajasessiooni identifikaator.

Kontrollrakendus pöördub kontrolliserveri poole ja edastab sellele hääle identifikaatori, mille vastusena annab kontrolliserver vastu algse krüptitud hääletussedeli valija poolt digiallkirjastatud konteineris. Selle hääletussedeli saab dekrüptida valimiste läbiviija privaatvõtmega, aga ka valijarakenduse poolt kasutatud efemeerse võtmega, mis edastati ruutkoodis valijale. Seda ruutkoodis olevat võtit kasutab sedeli dekrüptimiseks vastavlt IVXV protokollile nii ametlik kontrollrakendus kui ka sõltumatu häälekontrolli rakendus, mida on ülal kirjeldatud.

Erinevalt ametlikust rakendusest laadib sõltumatu rakendus aga krüptogrammi alla ning salvestab selle edaspidiseks kasutamiseks. Mis tähendab, et valijale jääb arvutisse faili kujul tema krüpteeritud hääletussedel tema poolt digiallkirjastatud konteineris, mille juures saab ta a) digitaalse identiteedi vahenditega veenduda, et konteiner on tõepoolest tema digiallkirjastatud ja seal sees olev krüptitud hääletussedel kuulub talle, aga b) lisaks ka dekrüptida selle hääletussedeli ruutkoodist salvestatud efemeerse võtmega.

Erinevalt valimiste ametliku rakenduse poolt elluviidud osalisest protokollist saab valija niimoodi tõendada oma tahteavalduse sisu suure tõsikindlusega mitte ainult 30 minutit pärast hääle andmist visuaalse kinnitusega nutitelefoni rakenduses, vaid lõputu aja jooksul krüptograafia ja digitaalse identiteedi vahenditega andmete tasemel. Ruutkoodis sisalduvad tõsikindlad tõendid valija tahteavalduse kohta on avalikkuses ja valimiste läbiviija poolt suuresti teadvustamata, pole toimunud kampaaniaid vastava teadlikkuse tõstmiseks ja valimiste läbiviija pole ka reageerinud juhtumitele, kus ruutkood avalikustatakse tuntud isikute poolt nt televisioonis või sotsiaalmeedias, sj on teadvustamata fakt, et ruutkoodi alusel võib 30 minuti jooksul pärast hääletamist laadida alla häälekonteineri kestahes.

Valimiste läbiviija on seejuures pigem väitnud, et nende eri tegevuste, sh valijatele nende häälte kohta info mitte andmine või kontrollimehhanismide mitte võimaldamine on seotud hääle salajasuse tagamise ning mõjutusründe vältimisega. Nende väidete tõesus on kaheldav, arvestades seda, et kontrollimehhanismi soovitanud OCSE vaatlejad soovitasid selleks kasutada kontrollkoodi, sj kontrolkoodil põhinevad ka Norra ja Šveitsi sarnaste omadustega otsast lõpuni kontrollitavust tagada püüd-

vad e-hääletuse süsteemid ja OSCE vaatlejad on 2019. aastal eksplitsiitselt osutanud Eesti ruutkoodil põhineva häälekontrolli vastuolule hääle salajasuse põhimõttega.