CYBERNETICA

Elektrooniliste häälte töötlemise protsesside analüüs

Aruanne

Versioon 1.0

22.12.2022

ID D-16-174

Sisukord

1 Sissejuhatus

Siinse aruande eesmärk on analüüsida Eesti elektroonilise hääletamise süsteemi häälte töötlemise ja lugemise protsesse ning nende jõudlust ja otstarbekust. Eraldi pöörame tähelepanu sellele, milliseid töötlemise ja lugemise samme saaks läbipaistvuse tõstmiseks täiendavalt auditeerida ning milliste täiendavate riskidega seejuures arvestama peab.

1.1 Lühikokkuvõte soovitustest

Aruanne annab rea soovitusi, mille siinkohal lühidalt kokku võtame.

- Valimispäeva õhtul on siiani ajaliselt kõige kulukamaks protseduuriks osutunud anonüümitud häälte miksimine, mis on hinnanguliselt nõudnud ca 1,5 tundi. Seda aega saab märkimisväärselt lühendada, kui kasutada miksimiseks ja miksimistõendi kontrolliks võimsamat riistvara.
- Esimesed protseduurid häälte töötlemisel (valimiskasti tervikluse kontroll, korduv- ja topelthäälte eemaldamine ning sedelite anonüümimine) on deterministlikud, st annavad sama sisendi korral alati sama väljundi. Need protseduurid on valimispäeva õhtul volitatud audiitorite poolt ka täielikult auditeeritud. Teisalt käsitlevad need protseduurid miksimata hääli, niisiis pole nende avalik auditeerimine potentsiaalsete mõjutusrünnete tõttu nagunii võimalik. Kokkuvõttes ei anna valimiskasti tervikluse teistkordne kontroll, korduv- ja topelthäälte eemaldamine ning sedelite anonüümimine valimispäevale järgneval päeval tehniliselt midagi juurde. Seega võib teise päeva protseduure põhimõtteliselt alustada anonüümitud e-urni kontrollsumma kontrollimisest ning anonüümitud häälte miksimisest.
- Häälte dekrüpteerimisvõtme osakute koguarv ning võtme taastamiseks vajalike osakute arv tuleks sobivas dokumendis (näiteks Riigi Valimisteenistuse korraldusega) selgelt sätestada.
- Miksimistõend võimaldab tehniliselt kontrollimist sõltumatute osapoolte poolt, kuid seejuures tuleb arvestada, et miksimata hääli ei saa mõjutusrünnete vältimiseks avalikult välja panna. Sellegipoolest on miksimistõendi kontroll sõltumatu rakendusega võimalik valimiste korraldaja kontrolli all olevas keskkonnas.
- Ka lugemistõend võimaldab kontrollimist sõltumatute osapoolte poolt. Kuna loetakse miksitud hääli, võib selle kontrolli läbi viia põhimõtteliselt ükskõik kes. Arvesse tuleb aga võtta, et osad sedelid võivad sisaldada häälte asemel mittekorrektseid väärtusi, kusjuures need väärtused võivad kanda informatsiooni mõjutusründe läbiviimiseks. Seda probleemi saab ennetada näiteks nullteadmustõestuste lisamisega hääle andmise sammule, kuid niisugune lahendus eeldab protokollistiku põhjalikumat täiendamist ning suuremat tarkvaraarendust.
- Muuhulgas tuleb ette valmistada ja avalikustada lugemistõendi spetsifikatsioon, mis on piisavalt detailne sõltumatu auditirakenduse loomiseks.
- Peale miksimis- ja lugemistõendi saab täiendavalt auditeerida ka rakendust, mis teisendab andmevorminguid miksimisrakenduse ja ülejäänud süsteemi vahel.
- Eesti e-hääletamise süsteemi arendusse on otstarbekas kaasata laiemat rahvusvahelist kogukonda.

2 Hääletamisele esitatavad nõuded ja Eesti elektroonilise hääletamise süsteemi üldkirjeldus

2.1 Hääletamisega seotud üldised nõuded

Valimistele esitatakse mitmeid nõudeid. Nii näiteks sätestab Eesti Vabariigi Põhiseadus paragrahvis 60, et Riigikogu valimised peavad olema vabad, üldised, ühetaolised ja otsesed ning et hääletamine peab olema salajane.

Need nõuded pole sündinud tühja koha pealt, vaid pandud paika mitmete ajalooliste protsesside tulemusena. Samuti sõltuvad nad konkreetse riigi kultuurist ja traditsioonidest.

Nii näiteks pole valimiste otsesuse nõue (igaüks hääletab ise, ilma vahendajata) sugugi universaalne. Rahvusvahelise Demokraatia ja Valimiskorralduse Instituudi andmetel kasutab umbes 15% maailma riikidest vahendatud hääletamist[1].

Ka ühetaolisuse printsiip (üks hääl ühe valija kohta) pole alati olnud iseenesestmõistetav. Nii võis 19. sajandil ja veel 20. sajandi alguseski mitmetes riikides üks valija hääletada mitmes piirkonnas[2]. Arutelusid selle üle, kas ühetaoline valimissüsteem annab ühiskondlikult optimaalse tulemuse, on peetud juba üle 150 aasta tagasi [1] ja peetakse tänapäevalgi [2].

Kuidas iganes poleks aga otsustatud hääleõigust valijate vahel jagada, tuleb kontrollida, et sellest jaotusest peetakse kinni. Hääletamisega seotud riskide terminites tähendab see vajadust veenduda, et keegi pole valimiskasti pannud rohkem sedeleid kui tema hääleõigus lubab. Pabervalimiste puhul kasutatakse selle tagamiseks organisatoorseid meetmeid ning loodetakse jaoskonnakomisjoni liikmete aususele.

Valimiste üldisuse printsiip nõuab Riigikogu valimiste näitel, et kõigile täisealistele teovõimelistele kodanikele peab olema tagatud võimalus valimistest osa võtta. See tähendab muuhulgas, et kord valimiste korraldajani jõudnud hääl ei tohi niisama kaduda. Pabervalimiste puhul tuginetakse siinkohal jälle organisatsioonilistele ja füüsilistele eeldustele. Näiteks on vaja tagada, et valimisjaoskonnad oleksid füüsiliselt piisavalt turvatud, et valimiskaste ei saaks rünnata, varastada vms.

Ajalooliselt on üldisuse ja ühetaolisuse tagamiseks kasutatud teisigi meetodeid. Kuni 19. sajandi teise pooleni toimusid paljud valimised USA-s *viva voce*, st valimisõiguslikud kodanikud ütlesid oma eelistuse kõigi kuuldes selge häälega välja. Kohalolijatest võis igaüks kontrollida, et kõik valima tulnud on saanud oma hääle anda, ja soovi korral ka lõpptulemuse sõltumatult kokku arvutada. Nii oli lihtne veenduda, et kõigi hääleõigus on tagatud, kuid samas võimaldas *viva voce* hääletamine ka väga lihtsat häälte ostmist. Asi läks koguni nii kaugele, et parteide vahel valitsesid kokkulepped, kui suurt summat on viisakas valijatele “hääletamatuleku vaeva” eest pakkuda [3].

Häälte ostmine kujutab endast muidugi mõjutusrünnet, mis omakorda rikub valimiste vabaduse põhimõtet. Selle ründe neutraliseerimiseks hakati juba 17.-18. sajandil erinevates riikides katsetama salajast hääletamist, aga püsivalt võeti see kasutusele 19. sajandi keskpaigas Austraalias

[1] https://www.idea.int/data-tools/data/special-voting-arrangements/proxy-voting-in-country
[2] https://en.wikipedia.org/wiki/Plural_voting

koos teistegi toona innovaatiliste lahendustega (näiteks valimiste korraldaja poolt trükitud sedelid) [4]. Järgmiste kümnendite jooksul levis salajane hääletamine ka teistesse riikidesse. Huvitav on märkida, et hääle andmine *viva voce* pole sellegipoolest tänapäevalgi kadunud ja leiab kasutamist madala mõjutusriskiga ühiskondades, näiteks Šveitsi kantonites Appenzell Innerrhodenis ja Glaruses [5, 6].

Loomulikult kahandab salajane hääletamine võimalust üldisuse ja ühetaolisuse printsiipide järgimist kõigi soovijate poolt kontrollida. Üldistatult võib öelda, et kõik valimissüsteemid (olgu nad elektroonilised või paberil) peavad leidma tasakaalu erinevate nõuete vahel. Kõiki mõeldavaid nõudeid 100% täita ei saa (ning see väide on põhjendatav matemaatilise rangusega, vt nt [7] ja [8]).

Võimalike tasakaalupunktide iseloomu mõjutab tugevalt see, kas valimised toimuvad jaoskonnas või distantsilt. Ühest küljest on inimesed 21. sajandil väga liikuvad ning pole realistlik eeldada, et kõik nad saavad ühel ja samal päeval kodukohta naasta [9]. Teisest küljest muutis COVID-19 pandeemia paljude inimeste koondamise väikestesse ruumidesse mitmeks aastaks riskantseks, mis muuhulgas tekitas tõsiseid probleeme valimiste korraldajatele [10, 11].

Niisiis on kaughääletamise võimaluse pakkumine valimiste üldisuse põhimõtte tagamiseks hädavajalik. Täna on selleks laias laastus kaks võimalust – kas edastada hääl posti või Interneti teel. Postihääletamise ajalugu ulatub küll tagasi vähemalt USA kodusõjani[3], kuid sama kaua on teda vaevanud ka rida probleeme. Postiühendus võib olla ebakindel, raske on tagada valijate autentsust ning valimisprotseduuri mõjutuskindlust [12, 13].

Vähemalt ühenduse ebakindluse ja valijate autentimise probleeme saab lahendada hästi korraldatud elektroonilise kaughääletamisega. Osutub, et ka mõjutuskindluse osas on olukord postihääletamisest parem. Digitaalne andmetöötlus võimaldab mitmeid lahendusi. Näiteks saab valijale põhimõtteliselt anda mitu digitaalset identiteeti, millest nö õiget kasutab valija juhul, kui teda ei mõjutata, aga nö vale identiteeti siis, kui mõjutaja teda valimisprotseduuri ajal jälgib [14, 15]. Säärase skeemi kasutatavus on aga üsna madal [16].

Sellepärast on Eestis mindud teist teed ja mõjutuse all antud elektroonilist häält on lubatud asendada andes uue hääle, kusjuures seda saab teha nii elektrooniliselt kui ka jaoskonnas hääletades (alates 2021. aastast saab elektroonilist häält paberhäälega asendada ka valimispäeval). Seejuures saab ülehääletamise võimalust käsitleda mitte ainult vahendina, mis võimaldab pärast mõjutuse alla sattumist oma hääleõigust vabalt realiseerida, vaid ka ennetus- ja heidutusmeetmena. Kui potentsiaalne mõjutaja (näiteks häälte ostja) teab, et mõjutuse all antud häält saab muuta, pole tal õigupoolest mõtet valijat mõjutama hakatagi.

Kuna valimiste korraldajal puudub võimalus hinnata, millised hääled on antud mõjutuse all ja millised mitte, on ülehääletamise võimalus antud kõigile elektrooniliselt hääletanutele. Riigikohus väljendas 2005. aastal seisukohta, mille kohaselt "*Valija võimalus elektrooniliselt antud häält eelhääletamise ajal muuta annab olulise lisagarantii valimiste vabaduse ja hääletamise salajasuse printsiibi järgimisele elektroonilisel hääletamisel.*" Samuti märkis Riigikohus, et niisugune võimalus ei riku valijate võrdse kohtlemise printsiipi esinduskogude valimisel[4].

2.2 Eesti elektroonilise hääletamise süsteemi kirjeldus

See jaotis kirjeldab Eesti elektroonilise hääletamise süsteemi IVXV, mis on kasutusel alates 2017. aastast. Varasemalt kasutusel olnud hääletamissüsteem erines olulisel määral praegu kasutusel

[3] https://www.history.com/news/vote-by-mail-soldiers-war
[4] https://www.riigiteataja.ee/kohtulahendid/detailid.html?id=206127152

olevast. Ühe suurima uuendusena kaotas IVXV vajaduse usaldada serverite haldajaid elektrooniliste häälte tervikluse osas, kuna IVXV võimaldab audiitoritel kontrollida, kas IVXV serveripoolne osa toimis korrektselt.

2.2.1 Osapooled ja komponendid

Vastavalt elektroonilise hääletamise üldraamistiku kirjeldusele [17] eristatakse Eesti elektroonilise hääletamise süsteemis järgnevaid osapooli ja komponente.

Süsteemi peamistes rollides olevad osapooled

- **Korraldaja** rollis on valimiste korraldajad, kes määravad ülejäänud rollide täitjad. Korraldaja rollis on Vabariigi Valimiskomisjon ja Riigi Valimisteenistus. Korraldaja vastutada on häälte avamise võtme haldamine ja häälte kokkulugemine Võtmerakenduse abil.
- **Hääletaja** – hääleõiguslik isik, kes kasutab hääletamiseks Valijarakendust. Lisaks saab Hääletaja olla verifitseerija rollis, kui ta kontrollib Kontrollrakenduse abil, kas Valijarakenduse abil edastatud sedel registreeriti ning kas see jõudis korrektsel kujul Kogumisteenusesse.
- **Koguja** käitab Kogumisteenust. Seda rolli täidab Riigi Infosüsteemi Amet. Koguja allkirjastab pärast hääletamisperioodi lõppu elektroonilise valimiskasti kontrollsumma. Seejärel annab Koguja Töötlejale üle elektroonilise valimiskasti koos allkirjastatud kontrollsummaga kahes eksemplaris. Samuti annab Koguja Töötlejale üle logid.
- **Töötleja** töötleb kogutud e-hääli. Töötlemine hõlmab endas tervikluskontrolle, kehtetute sedelite eemaldamist ja krüpteeritud häälte anonüümimist. Peale Töötlemisrakenduse võib Töötleja käitada ka Miksimisrakendust. Töötleja rolli täidab Riigi Valimisteenistus.
- **Lugeja** dekrüpteerib anonüümitud hääled ja arvutab e-hääletamise tulemuse. Lugeja rolli täidab Korraldaja.

Süsteemi kõrvalrollides olevad osapooled

- **Audiitor** auditeerib valimisi. Audiitor tegutseb lepingu alusel ning tal on aruandluskohustus. Konfidentsiaalsuslepingule tuginedes on audiitoril lubatud auditeerida ka protsesse, mille raames töödeldakse anonüümimata ja miksimata sedeleid.
- **Vaatleja** rollis on isikud, kes vaatlevad valimisi. Vaatlejatega pole sõlmitud lepinguid ning mõjutusrünnete välistamiseks pole vaatlejatel lubatud auditeerida protsesse, mille raames töödeldakse anonüümimata ja miksimata sedeleid. Näiteks saab audiitor kontrollida miksimistõendit, kuid vaatleja mitte, sest miksimistõendi kontroll eeldab miksimata häälte töötlemist.
- **Klienditugi** vastab hääletajate poolt tehtud pöördumistele, registreerib hääletajate probleemid ning abistab neid Kogumisteenusest saadud info abil. 2021. aastal pakkus kliendituge Riigi Infosüsteemi Amet.
- **Valijate nimekirja koostaja ja täiendaja** koostab ja uuendab hääleõiguslike valijate nimekirju. Valimiste infosüsteem (VIS) kasutab selleks Rahvastikuregistri andmeid. Algne valijate nimekiri allkirjastatakse VIS-i peakasutaja poolt ning edastatakse elektroonilise hääletamise süsteemi. Valijate nimekirja muudatused allkirjastab VIS ja edastab need elektroonilise hääletamise süsteemi koos allkirja verifitseerimiseks vajamineva avaliku võtmega.

Süsteemivälised kriitilised teenused

- **Registreerimisteenus** – välise usaldatud osapoole poolt hallatav teenus, mis võtab vastu Kogumisteenuse poolt edastatud sedelite registreerimispäringuid ning väljastab Kogumisteenusele ajatembeldatud kinnitusi sedelite räside registreerimise kohta. Registreerimisteenust pakub SK ID Solutions AS. Pärast hääletamisperioodi lõppu edastab Registreerimisteenuse haldaja Töötlejale kõik registreerimispäringuid ja neile vastavad ajatembeldatud kinnitused koos allkirjastatud kontrollsummaga.
- **Tuvastusteenus** – teenus, mida kasutatakse Hääletaja identiteedi tuvastamiseks. Korraldaja määrab kasutatavad autentimisvahendid ja neile vastavad tuvastusteenused.
- **Allkirjastamisteenus** – teenus, mis aitab Hääletajal allkirja koostada ja võtta sellele kehtivuskinnituse. Korraldaja määrab kasutatavad allkirjastamise vahendid ja allkirjastamisteenused. Allkirjastamisteenust kasutavad Valijarakendus ja Kogumisteenus, mis küsib Valijarakenduse poolt edastatud signeeritud sedelile kehtivuskinnituse.

Süsteemis kasutatavad tarkvarakomponendid

- **Valijarakendus** – programm, mis tuvastab Hääletaja, võimaldab hääletada ning edastatud häält Kontrollrakenduse abil kontrollida. Korraldaja tagab, et Valijarakendus on hääletamisperioodi vältel Hääletajatele kättesaadav.
- **Kontrollrakendus** – nutiseadmerakendus, mis võimaldab Hääletajal vahetult pärast hääletamist tema poolt antud häält kontrollida, et tuvastada, kas see on registreeritud ning korrektsel kujul Kogumisteenuse poolt talletatud. Korraldaja tagab, et Kontrollrakendus on hääletamisperioodi jooksul Hääletajatele kättesaadav[5].
- **Kogumisteenus** tuvastab Hääletaja identiteedi, kontrollib kas Hääletaja on juba hääletanud, edastab Hääletajale valikute nimekirja, võtab vastu krüpteeritud kujul olevaid digiallkirjastatud sedeleid, kontrollib nende nõuetelevastavust, edastab sedelid registreerimiseks, saadab Valijarakendusele kinnituse sedeli vastuvõtmise ja registreerimise kohta ning säilitab valimisperioodi jooksul sedeleid ja sedelite registreerimisinfot. Kuna Kogumisteenuse ülesandeid saab täita paralleelselt, siis võib koormuse jagamiseks kasutada mitut Kogumisteenuse serverit. Kogumisteenust käitab Koguja.
- **Töötlemisrakendus** võtab pärast hääletamisperioodi lõppu vastu Kogumisteenuse poolt edastatud e-urni ja Registreerimisteenuse poolt edastatud registreerimispäringud. Lisaks edastatakse Töötlemisrakendusele paberhääletanute nimekiri ja valijate nimekirjad. Töötlemisrakendus kontrollib valijate hääleõiguslikkust, sedelite vormingu nõuetelevastavust, digiallkirju, allkirjastajate sertifikaatide kehtivust ja sedelite registreerimist. Lisaks tuvastab Töötlemisrakendus, milline valija sedelitest on viimane, ning eemaldab sedelid, mis sisaldavad eelnevalt antud hääli. Kuna paberhääl on ülimuslik, eemaldab Töötlemisrakendus paberhääle andnud Hääletajate elektroonilised sedelid. Töötlemisrakendust käitab Töötleja. Audiitor võib käitada Töötlemisrakendust Töötleja töötulemuste kontrollimiseks [17].
- **Miksimisrakendus** rekrüpteerib anonüümitud hääled ja järjestab need juhuslikult ümber, et välistada võimalus dekrüpteeritud häälte seostamiseks Hääletajate poolt tehtud valikutega. Miksimisrakendus väljastab tõestuse (miksimistõendi), mille abil saab kontrollida, kas miksimine toimus korrektselt. Miksimisrakendust käitab Töötleja, aga miksimistõendit võivad kontrollida ka Audiitorid.
- **Teisendamisrakendus** – kuna Miksimisrakenduse rolli täitev Verificatum kasutab teisi andmevorminguid kui IVXV süsteem üldiselt, on vaja töödeldavaid andmeid nende vormingute

[5] Kuna kontrollrakendust levitatakse rakendustepoodide kaudu, siis sõltutakse Google'i rakenduste poest Play Store ja Apple'i rakenduste poest App Store.

vahel teisendada. Selleks on IVXV raamistikus olemas eraldi komponent, mida nimetame Teisendamisrakenduseks.

- **Võtmerakendus** genereerib valimistespetsiifilise võtmepaari, dekrüpteerib pärast hääletamisperioodi lõppu sedelid, loeb hääled kokku ja väljastab tulemuse. Võtmerakendus väljastab ka dekrüpteerimistõestuse (lugemistõendi), mille abil saab kontrollida, kas kõik sedelid dekrüpteeriti korrektselt. Võtmerakendust käitab Korraldaja, aga lugemistõendit võivad kontrollida ka Audiitorid.
- **Auditirakendus** koosneb kolmest tööriistast, mis võimaldavad Audiitoril kontrollida miksimise korrektsust (tööriist *mixer*), dekrüpteerimise korrektsust (tööriist *decrypt*) ja teisenduste korrektsust e-valimiskastis olevate krüpteeritud sedelite andmevormingute ja Verificatumi andmevormingute vahel (tööriist *convert*)[6]. Auditirakendust käitab Audiitor.

2.2.2 Eesti elektroonilise hääletamise süsteemi ülevaade

See jaotis annab ülevaate Eesti elektroonilise hääletamise süsteemist IVXV. Hääletamissüsteemi komponente kirjeldatakse detailsemalt järgnevates alajaotistes ning hääletamissüsteemi dokumentatsioonis. Eesti elektroonilise hääletamise süsteemi üldskeem on esitatud joonisel 1.

Loetavuse huvides on Eesti elektroonilise hääletamise süsteemi kirjeldus esitatud nelja etapina: hääletamisperioodile eelnev aeg, hääletamisperiood, hääletamisperioodile järgnev töötlusfaas ja lugemisfaas. Selle raporti kirjutamise ajal (2022. aastal) kehtiva seadusandluse kohaselt toimub e-hääletamine eelhääletamise perioodil.

2.2.2.1 Valimiste korraldajad

Valimiste korraldajateks on Vabariigi Valimiskomisjon ja Riigi Valimisteenistus (RVT). Tehnilise poole pealt on kaasatud ka Riigi Infosüsteemi Amet (RIA), kes haldab valimiste infosüsteemi (VIS) ja tagab e-hääletamise tehnilise toimimise[7].

Vabariigi Valimiskomisjoni ülesanneteks on valimiste aluspõhimõtete järgimine, järelevalve valimiste korraldajate üle, kandidaatide registreerimine, üleriigiliste hääletamis- ja valimistulemuste kindlakstegemine, kaebuste läbivaatamine, elektroonilise hääletamise üldpõhimõtete tagamine ja hääletamistulemuste kehtetuks tunnistamine[8].

Riigi Valimisteenistuse ülesanneteks on valimiste seadusekohase korraldamise tagamine, elektroonilise hääletamise korraldamine, järelevalve valimiste korraldajate tegevuse üle, valimisseadustest tulenevate ülesannete täitmiseks vajalike tehniliste lahenduste arendus ja haldus[9].

2.2.2.2 Hääletamisperioodile eelnev aeg

Korraldaja peab tagama elektroonilise hääletamise süsteemi (EHS) toimimise. See hõlmab süsteemi arendust, hooldust, turvatestimist, hääletamissüsteemi käitlust ning järelvalvet.

Enne hääletamisperioodi tuleb ette valmistada nii hääletamistarkvara kui ka hääletamistarkvara

[6] https://github.com/vvk-ehk/ivxv/blob/49160800174473502e0bee4c8fa87b7ec75bd6f6/Documentation/et/seadistuste_koostejuhend/auditirakendus.rst

[7] https://www.ria.ee/riigi-infosusteem/kesksete-riiklike-infosusteemide-arendus/valimiste-infosusteem-ja-e-haaletamine

[8] https://www.valimised.ee/et/korraldajad/vabariigi-valimiskomisjon/vabariigi-valimiskomisjoni-koosseis-padevus-ja-ulesanded

[9] https://www.valimised.ee/et/korraldajad/riigi-valimisteenistus/riigi-valimisteenistus

seadistus. Riigikogu valimise seaduse kohaselt seab riigi valimisteenistus EHS-i kasutusvalmis hiljemalt kümnendaks päevaks enne valimispäeva[10]. Üldistatult hõlmab see hääletamissüsteemi serveripoolse tarkvara paigaldamist ja seadistamist, häälte salastamiseks ja avamiseks mõeldud ElGamali[11] võtmepaari genereerimist ning ettevalmistusi Valijarakenduse ja Kontrollrakenduse Hääletajatele kättesaadavaks tegemiseks. Serveripoolse tarkvara paigaldamise eest vastutab RIA ja seadistamise eest Riigi Valimisteenistus.

Häälte salastamiseks ja avamiseks kasutatavate võtmete genereerimise eest vastutab Riigi Valimisteenistus[12]. Võtmete genereerimiseks kasutatakse võrgust eraldatud arvutit, millelt on eemaldatud sisemised salvestusvahendid ning mis alglaaditakse väliselt kõvakettalt [18].

Võtmerakendus genereerib võtmepaari, väljastab avaliku võtme[13] ning jagab võtmepaaris sisalduva salajase võtme läviskeemi abil nii mitmeks võtmeosakuks kui on seadistuses määratud [19, 20]. Läviskeemi parameetrid määravad ära, mitu võtmeosakut genereeritakse ning mitut võtmeosakut on vaja salajase võtme taastamiseks[14]. Võtmeosakud genereeritakse operatiivmälus ning võtmerakendus salvestab need PKCS15-liidese vahendusel kiipkaartidele [19]. Vastavalt E-hääletamise käsiraamatule võib kiipkaartidele omistada PIN koodid [18].

Võtmeosakud jagatakse Vabariigi Valimiskomisjoni liikmete ja Riigi Valimisteenistuse vahel[15]. Riigi Valimisteenistuse juht määrab Riigi Valimisteenistuse esindajad, kellele antakse võtmeosakud. Iga isik saab ühe pitseeritud kiipkaardi, millele on talletatud unikaalne võtmeosak.

Võtmerakenduse poolt väljastatud avalik võti integreeritakse Valijarakendusse ja tehakse Kontrollrakendusele kättesaadavaks. Valijarakendus avalikustatakse valimiste korraldaja veebilehel koos juhistega Valijarakenduse tervikluse kontrollimiseks. Kui Kontrollrakendust on vaja uuendada, siis tuleb seda teha aegsasti, et uus versioon jõuaks enne valmisperioodi algust rakendustepoodidesse[16].

2.2.2.3 Hääletamisperiood

Hääletamisperioodi alguseks on Valijarakendus valimiste veebilehe kaudu avalikustatud. Kui Hääletaja soovib e-hääletada, peab ta esmalt valimiste veebilehelt Valijarakenduse alla laadima. Eeldatakse, et valija kontrollib pärast Valijarakenduse allalaadimist selle terviklust.

Valijarakenduse käivitamisel palutakse Hääletajal end tuvastada[17]. Seejärel kuvatakse Hääletajale Kogumisteenuse poolt edastatud valikute nimekiri. Pärast valiku tegemist palutakse Hääletajal otsus digiallkirjaga kinnitada. Selleks hetkeks on Valijarakendus Hääletaja poolt tehtud valiku valimiste avaliku võtmega krüpteerinud, kasutades ElGamali krüptosüsteemi[18]. Krüpteerimiseks vajaliku juhuarvu genereerib Valijarakendus. Hääletaja poolt antav digiallkiri erineb mõne-

[10] https://www.riigiteataja.ee/akt/RKVS#para48b3lg1

[11] Elektrooniliste häälte salastamiseks kasutatav krüptosüsteem ja võtmepikkus on määratud Riigi Valimisteenistuse korraldusega. Näiteks 2021. aasta vastav korraldus asub veebilehel: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/7cf162ec-798b-4cbe-98c4-e114db7f1f0f.

[12] https://www.riigiteataja.ee/akt/RKVS#para48b3lg3

[13] Avalik võti kirjutatakse välisele andmekandjale, milleks varasemalt on olnud DVD plaat.

[14] Osakute koguarv ja salajase võtme taastamiseks vajalike osakute arv pole üheski dokumendis selgesõnaliselt määratletud. Soovitame need kehtestada näiteks Riigi Valimisteenistuse korraldusega.

[15] https://www.riigiteataja.ee/akt/RKVS#para48b3lg3

[16] Nutiseadmete arhitektuurist tulenevalt levitatakse rakendusi rakendustepoodide kaudu. Seetõttu tekib sõltuvus kolmandast osapoolest, kelleks on rakendustepoe haldaja.

[17] Selle raporti kirjutamise ajal olid heakskiidetud autentimisvahenditeks Mobiil-ID ja ID-kaart. Lisaks saab kasutada mõningaid teisi riigi poolt väljastatud kiipkaarte nagu näiteks Digi-ID.

[18] ElGamali krüptosüsteem on randomiseeritud. Krüpteerimisel genereeritakse juhuarv, mis tagab, et sama väärtuse krüpteerimisel on tulemuseks erinevad krüptogrammid.

võrra tavapärasest digiallkirjast, kuna krüpteeritud sedelile lisatav digiallkiri ei sisalda kehtivuskinnitust. Valijarakendus edastab Kogumisteenusele digiallkirjastatud kujul oleva krüpteeritud sedeli koos allkirjastamise sertifikaadiga.

Kogumisteenus talletab vastuvõetud sedeli ja kontrollib, kas see sedel pärineb hääleõiguslikult isikult, kas krüpteeritud sedel on nõuetekohaselt vormindatud ja allkirjastatud, ning küsib hääle allkirjastamiseks kasutatud sertifikaadile kehtivuskinnituse. Kogumisteenus määrab iga vastuvõetud sedeli jaoks unikaalse identifikaatori ning loob vastuvõetud allkirjastatud ja krüpteeritud sedelist räsi. Seejärel loob Kogumisteenus sedeli registreerimise korralduse, mille koostamiseks allkirjastab Kogumisteenus sedeli räsi koos sedeli identifikaatoriga, ja edastab korralduse Registreerimisteenusele ajatembeldamiseks. Registreerimisteenus saadab Kogumisteenusele allkirjastatud ajatempli, mis sisaldab Kogumisteenuse poolt allkirjastatud korraldust. Nii Kogumisteenus kui Registreerimisteenus talletavad ajatemplipäringud (st Kogumisteenuse poolt loodud korraldused) ja väljastatud ajatemplid.

Vastuvõetud sedeli vastusena tagastab Kogumisteenus Valijarakendusele unikaalse sedeliidentifikaatori, Hääletaja allkirjasertifikaadi kehtivuskinnituse, Kogumisteenuse poolt väljastatud ajatemplipäringu ja sedeli registreerimist tähistava ajatempli. Valijarakendus kontrollib, et kehtivuskinnitus ja ajatempel vastavad nõuetele. Kui vigu ei tuvastata, siis kuvab Valijarakendus Hääletajale QR-koodi koos teatega, et Hääletajal on võimalik nutiseadmel toimiva Kontrollrakenduse abil tuvastada, kas hääl edastati korrektselt. Hääle kontrollimine Kontrollrakenduse abil on vabatahtlik, kuid ilma häält kontrollimata ei saa Hääletaja veenduda, et tema hääl on jõudnud muutmata kujul Kogumisteenuseni ja sai Registreerimisteenuse poolt registreeritud.

QR-koodi sisse on kodeeritud Kogumisteenuse poolt vastuvõetud sedeli unikaalne identifikaator ning hääle krüpteerimiseks kasutatud juhuslik väärtus. Kui Hääletaja loeb Kontrollrakenduse abil QR-koodi, siis saab Kontrollrakendus juurdepääsu vastavale infole. Sedeli unikaalse identifikaatori abil pärib Kontrollrakendus Kogumisteenuselt identifikaatorile vastava digiallkirjastatud ja krüpteeritud sedeli, Hääletaja allkirjasertifikaadi ja sedelit kvalifitseerivad elemendid, näiteks kehtivuskinnituse ja Registreerimisteenuse poolt väljastatud hääle registreerimist tõendava ajatempli. Selle info alusel kontrollib Kontrollrakendus, kas Hääletaja allkirjastamissertifikaadile on võetud nõuetele vastav kehtivuskinnitus ning kas sedel on korrektselt registreeritud. ElGamali krüptosüsteemi eripärast tulenevalt saab krüpteerimiseks kastutatud juhusliku väärtuse abil krüpteeritud hääle avada. Seeläbi kuvab Kontrollrakendus Hääletajale sedelis sisalduva valiku.

Hääletajal on võimalik eelhääletamisperioodi jooksul korduvalt e-hääletada. Protsess toimib analoogselt eelnevalt kirjeldatuga.

2.2.2.4 Hääletamisperioodile järgnev töötlusfaas

Pärast hääletamisperioodi lõppu edastab Registreerimisteenus Töötlejale kõik ajatemplipäringud ehk korraldused ja nendele päringute vastustena väljastatud ajatemplid. Kogumisteenus edastab Töötlejale e-urni, mis sisaldab krüpteeritud ja allkirjastatud sedeleid, ajatemplipäringuid ja nende päringute vastustena väljastatud ajatempleid.

Töötleja kontrollib Kogumisteenuse ja Registreerimisteenuse poolt edastatud info kooskõla. Lisaks kontrollib Töötleja iga sedeli juures, kas [21]

- sedeli allkirjastaja oli valiku tegemise hetkel valijate nimekirjas,
- allkirjastatud sedel on korrektses konteinervormingus,
- krüpteeritud sedelil on korrektne digitaalallkiri,
- kehtivuskinnituse alusel oli allkirjastaja sertifikaat sedeli vastuvõtmise ajahetkel kehtiv ja

- sedel on Registreerimisteenuse poolt korrektselt registreeritud.

Töötleja seab Hääletaja poolt antud sedelid ajalisse järjekorda ning väljastab elektrooniliselt hääletanute nimekirja. Iga Hääletaja viimasena antud sedel liigub töölemise järgmisse etappi. Seejärel kontrollib ja rakendab Töötleja sisendina saadud tühistusnimekirju ja ennistusnimekirju[19]. Tühistusnimekirjad koosnevad isikutest, kes andsid nii paberhääle kui e-hääle. Kuna paberhääl on ülimuslik, siis nende isikute e-hääled tühistatakse ning need ei lähe töötlemise järgmisesse etappi.

Järgnevalt Töötleja anonüümib sedelid, eemaldades krüpteeritud sedelitelt allkirjad. Selleks, et pärast häälte miksimist ja dekrüpteerimist oleks võimalik teha täiendav kontroll hääle pärinemise kohta õigest valimisringkonnast, lisatakse häälele algebraliselt ka ringkonna identifikaator. Sõltuvalt Korraldaja otsusest saab anonüümitud sedelid miksida või edastada need kokkulugemiseks [17].

Kui Korraldaja otsustab krüpteeritud kujul olevaid sedeleid miksida, siis kasutatakse Miksimisrakendust. Eesti e-hääletamise süsteem IVXV kasutab Miksimisrakendusena tarkvarapaketti Verificatum [20]. Vastavalt IVXV protokollide kirjeldusele [21] on vaja enne miksimist teisendada krüptogrammid Verificatumi jaoks sobivale kujule. Selle teisenduse korrektsuse kontrollimiseks kasutatakse Auditirakenduse tööriista *convert*[21].

Miksimisrakendus rekrüpteerib sedelid ja järjestab nad ümber. Tulemusena ei ole enam võimalik rekrüpteeritud sedeleid Hääletajate poolt allkirjastatud sedelitega kokku viia. Samas ei muutu miksimisel sedelites olevate häälte väärtus. Miksimisprotsessi teiseks väljundiks on miksimistõend, mida saab kasutada miksimise korrektsuse kontrollimiseks.

Audiitor saab kasutada Auditirakendust, et kontrollida miksimistõendi põhjal, kas miksimine toimus korrektselt nii, et hääli ei muudetud, sedeleid ei lisatud ega eemaldatud.

2.2.2.5 Lugemisfaas

Sedelite dekrüpteerimiseks kasutatakse Võtmerakendust, mis vajab tööks dekrüpteerimisvõtit. Dekrüpteerimisvõtme rekonstrueerimiseks läheb vaja vähemalt lävipiiriga võrdset arvu võtmeosakuid. Kuna võtmeosakuid sisaldavaid kiipkaarte haldavad võtmehaldurid, siis läheb dekrüpteerimisvõtme taastamiseks vaja vähemalt lävipiiriga võrdset arvu võtmehaldureid.

Pärast dekrüpteerimisvõtme taastamist dekrüpteeritakse sedelid koos ringkonna koodiga. Iga dekrüpteeritud sedeli kohta kontrollitakse, kas

- tegemist on korrektselt vormistatud häälega,
- kas valimiste identifikaator vastab hetkel käimasolevatele valimistele ja
- kas hääl on antud kandidaadile, kes kandideeris vastavas ringkonnas.

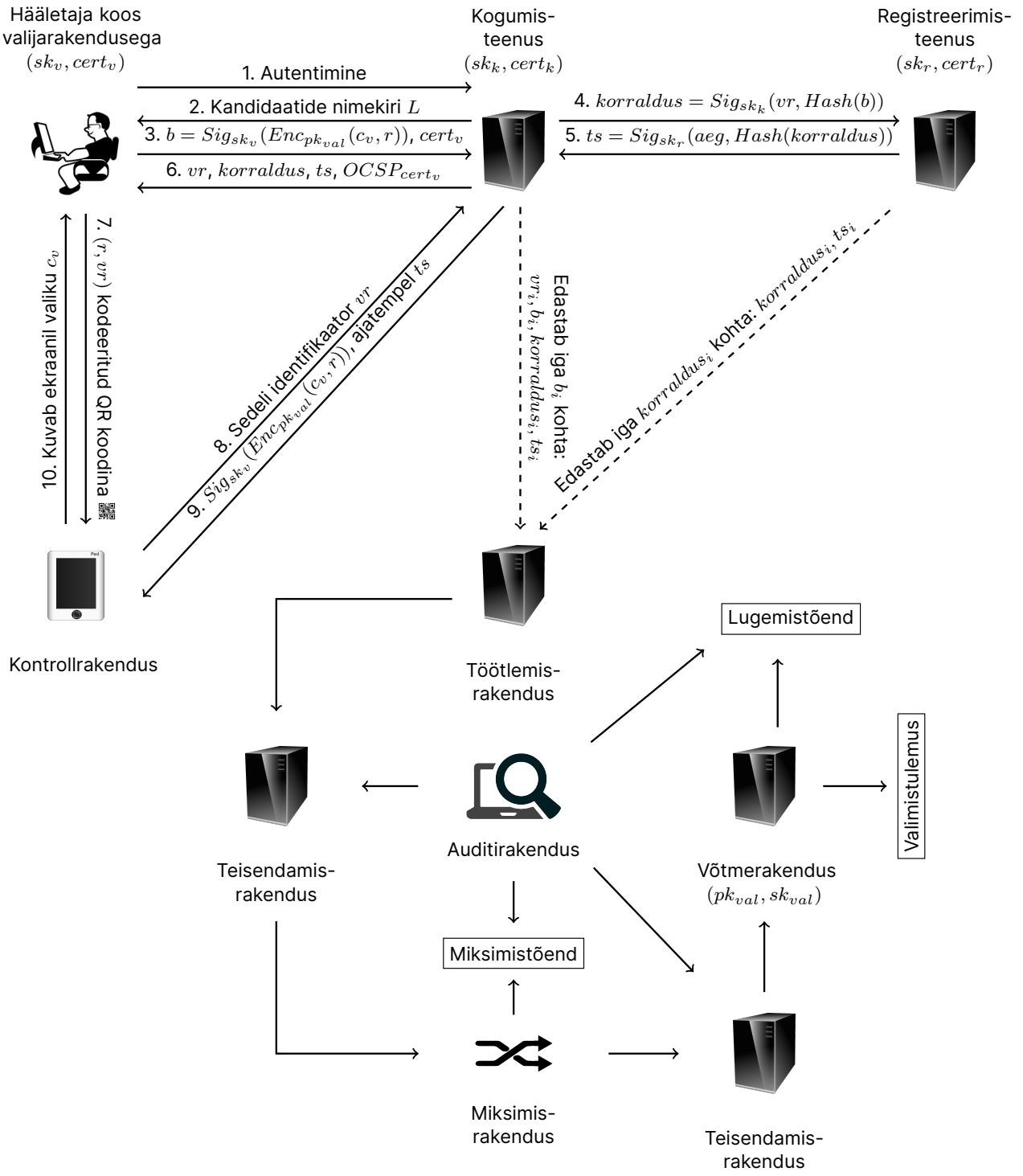
Iga sedeli kohta, mille dekrüpteerimisel saadakse korrektne hääl, antakse dekrüpteerimistõestus (lugemistõend), mille abil saab tõestada, et hääl dekrüpteeriti korrektselt. Järgnevalt loeb Võtmerakendus hääled kokku ning väljastab valimistulemuse.

Audiitor saab kasutada Auditirakenduse tööriista *decrypt*, et kontrollida lugemistõendi põhjal (seejuures ilma dekrüpteerimisvõtit omamata!), kas kõik hääled on korrektselt dekrüpteeritud.

[19] Ennistusnimekiri tekib, kui VISi poolt saadav tühistusnimekiri sisaldas mingil põhjusel valeandmeid. Sellisel juhul edastatakse ennistusnimekiri, mille abil taastatakse vääralt tühistatud sedelid.

[20] https://www.verificatum.org/

[21] https://github.com/vvk-ehk/ivxv/blob/49160800174473502e0bee4c8fa87b7ec75bd6f6/Documentation/et/seadistuste_koostejuhend/auditirakendus.rst



Joonis 1. Eesti elektroonilise hääletamise süsteem. Nummerdatud kirjed tähistavad hääletamisperioodi vältel toimuvaid tegevusi. Joonisel olev punktiirjoon eraldab hääletamisperioodi hääletamisperioodijärgsetest tegevustest.

3 Häälte töötlemise ja lugemise protsesside jõudluse parandamine

Jaotistes 2.2.2.4 ja 2.2.2.5 kirjeldatud häälte töötlemise ja lugemise protseduurid viiakse valdavalt läbi pärast hääletamisperioodi lõppu, st alates kella 20.00-st valimispäeva õhtul. Peamine põhjus, miks varem alustada ei saa, on vajadus eemaldada topelthääled, st need e-hääled, mis on muudetud jaoskonnas valimispäeval paberhääli andes. Valimiskasti terviklust kontrollida ja korduvhääli eemaldada saaks põhimõtteliselt ka enne, aga sel juhul peaks audiitorid ka nende varasemate protseduuride juurde organiseerima ning see poleks lihtsalt mõistlik. Valimispäeva õhtul on nad nagunii kohal ja esimesed protseduurisammud ei võta väga palju aega. Valimiskasti tervikluse kontroll, korduv- ja topelthäälte eemaldamine ning sedelite anonüümimine kestavad kokku umbes tund aega.

Ajaliselt kõige kulukam protseduur on siiani olnud anonüümitud häälte miksimine, mis on hinnanguliselt nõudnud ca 1,5 tundi. Sellele lisanduvad miksimitõendi kontroll ning lugemistõendi kontroll. Samas on ühiskonnal ootus e-hääled kiiresti kokku loetud saada. Seepärast on erinevatel aastatel miksimisele ja tõendite kontrollile lähenetud erinevalt.

Näiteks 2017. aastal ei kasutatud valimispäeval ei miksimist ega tõendite kontolli üldse ning täisprotseduur viidi läbi valimispäevale järgneval päeval. Niisugune lähenemine paneb aga kogu vastutuse häälte salajasuse säilitamise eest organisatoorsetele meetmetele. Sellepärast on alates 2019. aastast ka valimispäeval alati hääli enne lugemist miksitud. Protsessid on erinenud ainult tõestuste kontrollimise poolest, mida vahel on tehtud ka valimispäeval, vahel aga ainult valimispäevale järgneval päeval.

Kuidas saaks protseduure muuta nii, et ühiskondlikule ootusele paremini vastata? Selleks on kaks põhimõtteliselt erinevat (kusjuures teineteist mitte välistavat) võimalust.

- *Parema riistvara kasutamine*. Ülalmainitud 1,5-tunnine miksimisaeg saadi riistvarakonfiguratsiooniga, kus oli kasutusel 32-lõimeline AMD protsessor ja 16GB muutmälu (kuhu haagiti ka vajalik salvestusruum). Verificatumi autor Douglas Wikström väidab, et kasutades 13. põlvkonna Inteli i9-13900K 32-lõimelist protsessorit, 32GB muutmälu ja kiiret salvestusmeediat, on võimalik 300000 häält miksida ca 6 minutiga ja miksimistõendit kontrollida ca 2 minutiga.
- *Teise krüptosüsteemi kasutamine*. Täiendav kiirusevõit on võimalik saavutada, kui vahetada hetkel kasutuses olev 3072-bitine ElGamali krüptosüsteem elliptkõvera P-256 vastu. Kuna moodularvutused on üldiselt aeglasemad kui arvutused sama turvataset pakkuva elliptkõvera rühmas, on Eestis hetkel miksimine aeglasem kui Verificatum tehniliselt võimaldab. Kasutatava krüptosüsteemi väljavahetamine on samas mittetriviaalne. Ümber tuleb teha nii protokoll kui kõik rakendused (valijarakendus, kontrollrakendus, võtmerakendus, miksimistõendite kontroll, lugemistõendite genereerimine ja kontroll ning auditirakendused), aga piisava aja- ja ressursivaru korral on see teostatav. Üks positiivne muudatus, mida üleminek P-256 krüptosüsteemile endaga veel kaasa tooks, on kontrollimisel kasutatava QR-koodi mõõtmete vähenemise. See omakorda vähendaks võimalikke probleeme, mis võivad esineda QR-koodi skaneerimisel.

Ajalooliselt on jaotistes 2.2.2.4 ja 2.2.2.5 kirjeldatud protseduure väikeste variatsioonidega korratud ka valimispäevale järgneval päeval. Näiteks 2017. aastal, kui valimispäeval hääli aja kokku-

hoiu huvides ei miksitud ja tõestusi ei kontrollitud, kasutati teist päeva kogu protsessi täielikuks läbiviimiseks.

Viimastel aastatel on siiski võetud suund sellele, et kõik protseduurid valimispäeva õhtul täielikult läbi teha. Nagu eespool kirjeldatud, peaks parema riistvara kasutamine seejuures ka ajasurvet vähendama.

Samas kerkib loomulik küsimus, mis üldse on kogu protsessi kordamise mõte teisel päeval. Ühe võimaliku vastuse annab laiem auditeerimine. Jaotises 4 kirjeldame mitmeid ettepanekuid, kuidas on võimalik kaasata sõltumatult loodud auditirakendusi näiteks miksimis- ja lugemistõendite kontrollimiseks. Olenevalt sellest, kui palju niisuguseid rakendusi välja pakutakse ja kui hea on nende jõudlus, võib see protsess nõuda rohkem aega kui valimispäeva õhtul on. Sõltumatute auditirakenduste kaasamiseks sobibki valimispäevale järgnev päev seega tunduvalt paremini.

Paneme tähele, et esimesed protseduurid häälte töötlemisel (valimiskasti tervikluse kontroll, korduv- ja topelthäälte eemaldamine ning sedelite anonüümimine) on deterministlikud, st annavad sama sisendi korral alati sama väljundi. Need protseduurid on valimispäeva õhtul volitatud audiitorite poolt ka täielikult auditeeritud. Teisalt käsitlevad need protseduurid miksimata hääli, niisiis pole nende avalik auditeerimine potentsiaalsete mõjutusrünnete tõttu nagunii võimalik.

Kokkuvõttes ei anna teistkordne valimiskasti tervikluse kontroll, korduv- ja topelthäälte eemaldamine ning sedelite anonüümimine valimispäevale järgneval päeval sisuliselt midagi juurde. Teist päeva võib seega alustada anonüümitud e-urni kontrollsumma kontrollimisest, millele järgneb uus miksimine (koos vajalike vorminguteisendustega), miksimistõendi kontroll (sh sõltumatute kontrollrakendustega), miksitud häälte dekrüpteerimine ja lugemine võtmerakendusega ning lugemistõendi kontroll (sh sõltumatute kontrollrakendustega).

4 Võimalused protsesside täiendamiseks ja läbipaistvuse suurendamiseks

4.1 Miksimistõendi täiendav auditeerimine

Nagu eelpool kirjeldatud, kasutatakse Eesti e-hääletamise süsteemis häälte miksimiseks tarkvarapaketti Verificatum. Tegemist on ühe kõige küpsema ja võimalusterohkema miksimislahendusega maailmas.

Loomulikult kuulub paketi Verificatum enda koosseisu tõendite kontrollimise komponent ja seda Eesti e-hääletamise protsessis ka kasutatakse. Täiendavalt on miksimistõendi kontrollija arendatud välja IVXV tarkvara osana[1].

Tehniliselt võimaldab miksimistõend kontrollimist ka sõltumatute rakenduste poolt. Selliseid rakendusi on olemas mitmeid. Neist kõige kaugemale arendatuks võib pidada Hainesi jt loodud kontrollijat, mille korrektsus on muuhulgas formaalselt verifitseeritud [22]. On olemas ka mõned akadeemilisest keskkonnast pärit vähemtestitud lahendused[2][3].

Miksimitõendi täiendaval auditeerimisel tuleb arvesse võtta, et auditi sisendiks on muuhulgas valimistel antud häälte krüptogrammid. Kuigi krüptogrammid on anonüümsed, saab neid bitiesituse alusel endiselt signeeritud häältega kokku viia (ja selle seose murdmiseks miksimist ju üldse kasutataksegi). See tähendab, et miksimistõendi audiitor näeb, millised antud häältest läksid lugemisele. Seda teavet on põhimõtteliselt võimalik ära kasutada ühe sammuna mõjutusründest, kus ründaja saab kontrollida, kas tema mõjutuse all antud häält on hiljem muudetud või mitte.

Niisiis ei saa miksimistõendi kontrollimiseks vajalikke andmeid näiteks avalikult Internetti panna. Küll aga on mõeldav miksimistõendite kontrollimine laiema ringi usaldusväärsete audiitorite poolt (kusjuures audiitorit tuleb usaldada selles, et ta ei lekita miksimata hääli ega osale mõjutusründes). Hetkel puudub miksimistõendi kontrolli protseduuris samm, kus sõltumatud audiitorid võiksid oma auditirakendustega protsessis osaleda. Niisuguse sammu saab protseduuri lisada, aga see toob endaga kaasa vajaduse veel mitme täiendava sammu järele.

Kõigepealt tuleb arvesse võtta, et sõltumatult arendatud auditirakenduste kvaliteedikontrollimehhanismid ei pruugi olla piisaval tasemel. Selleks, et ennetada probleeme valimispäeval ja sellele järgneval päeval, tuleb ette valmistada ning avalikkusele kättesaadavaks teha testandmed, mille vastu arendajad oma rakendusi arendada ja testida saavad. Mõeldav on ka formaalne nõue, et rakendus peab need testid täielikult läbima enne kui ta lubatakse päris miksimistõendit auditeerima.

Teine mõeldav kvaliteedikontrollimehhanism on koodiaudit. Näiteks võib nõuda, et miksimistõendi kontrollrakendus peab olema avatud lähtekoodiga ning kättesaadav piisava aja vältel enne valimisi GitHubis vmt avalikus repositooriumis. Valimiste korraldaja peab siis kas ise läbi viima või organiseerima vastava koodiauditiprotsessi.

Isegi põhjalik testimine ja koodiaudit ei kindlusta seda, et kõik rakendused töötavad päris miksimistõendi peal alati sama moodi. Niisiis tuleb protsessis ette näha eeskiri ka juhuks, kui mõned rakendused annavad erineva tulemuse.

[1] https://github.com/vvk-ehk/ivxv/tree/master/auditor/src/main/java/ee/ivxv/audit/shuffle
[2] https://github.com/akels/Verificatum.jl
[3] https://github.com/ZetaTwo/sa104x-kexjobb

Nagu eespool nägime, on miksimistõendi auditeerimine seotud mõjutusriskiga juhul kui audiitor käitub pahatahtlikult. Selle riski minimeerimiseks võib kaaluda auditirakenduste töökeskkonna piiramist. Kuna rakendused peaksid juba koodiauditi võimaldamiseks olema avalikult kättesaadavad, pole otseselt põhjust, miks nad peaksid jooksma audiitori kontrolli all olevas arvutis. Valimiste korraldaja võib ette valmistada standardse töökeskkonna (näiteks stabiilse Ubuntu LTS versiooniga arvuti), kuhu tõmmatakse auditirakenduse lähtekood, vajadusel kompileeritakse see ja käivitatakse[4].

Audiitoril endal pole ideaalis vajadust sellesse protsessi sekkuda. Samas paneme tähele, et isegi juhul kui audiitor protsessis aktiivselt ei osale, peab ta suutma veenduda, et kasutusel on just tema poolt soovitav auditirakendus. Teisest küljest tuleb rakenduse kasutamisele eelneva koodiauditi käigus muuhulgas veenduda, et rakendus ei ürita lekitada miksimisele minevaid häälte krüptogramme. Lisaks tuleb muidugi veenduda, et pärast koodiauditit pole rakendust repositooriumis enam muudetud.

Kokkuvõttes võiks valimistele eelneva perioodi tegevused olla järgmised.

1. Valmistada ette ja avalikustada testandmed sõltumatute auditirakenduste arendamiseks.
2. Levitada infot sõltumatu auditeerimise võimaluse kohta.
3. Registreerida ja testida sõltumatult arendatud auditirakendused. Vajadusel viia läbi koodiaudit.
4. Valmistada auditirakenduste jaoks ette standardne töökeskkond.
5. Panna paika protseduurid olukorra jaoks, kus erinevad rakendused annavad erineva tulemuse.

Audit ise koosneb järgmistest sammudest.

1. Kontrollrakenduse lähtekoodi hankimine ning tervikluse kontroll (mh et hangitud on sama versioon lähtekoodist, mis on testitud ja auditeeritud).
2. Rakenduse käivitamine.
3. Tulemuse võrdlus ametliku miksimistõendi kontrollija poolt väljastatuga.
4. Vajadusel erisuste analüüs ning lahendamine.

4.2 Lugemistõendi täiendav auditeerimine

Teine oluline krüptograafiline auditeerimist vajav andmekogum on lugemistõend, mille häälte dekrüpteerimise ja kokkulugemise käigus väljastab Võtmerakendus. Erinevalt miksimistõendi kontrollimisest on hetkel olemas ainult üks IVXV tarkvarapaketti kuuluv vahend, mis lugemistõendeid auditeerida suudab[5].

Krüptograafilisest vaatest on aga ka lugemistõend mõeldud auditeerimiseks sõltumatutele osapooltele. Niisiis on võimalik korraldada lugemistõendi auditeerimist valimispäevale järgneval päeval sarnaselt miksimistõendiga. Enne valimisperioodi tuleks teha järgmised sammud.

1. Valmistada ette ja avalikustada lugemistõendi spetsifikatsioon, mis on piisavalt detailne sõltumatu auditirakenduse loomiseks. (Käesoleva kirjutamise hetkel novembris-detsembris 2022 sellist avalikku spetsifikatsiooni ei ole.)

[4] Senise praktika järgi on audiitor toonud kaasa oma kõvaketta, kuhu on installeeritud Ubuntu LTS ja audiitori poolt heaks kiidetud auditirakendus. Ka see lahendus töötab, aga vajab lisaks pärast audiitori kõvaketta puhastamist või hävitamist.

[5] https://github.com/vvk-ehk/ivxv/tree/master/auditor

2. Valmistada ette ja avalikustada testandmed sõltumatute auditirakenduste arendamiseks.
3. Levitada infot sõltumatu auditeerimise võimaluse kohta.
4. Registreerida ja testida sõltumatult arendatud auditirakendused. Vajadusel viia läbi koodiaudit.
5. Valmistada auditirakenduste jaoks ette standardne töökeskkond.
6. Panna paika protseduurid olukorra jaoks, kus erinevad rakendused annavad erineva tulemuse.

Audit ise koosneb järgmistest sammudest.

1. Kontrollrakenduse lähtekoodi hankimine ning tervikluse kontroll (mh et hangitud on sama versioon lähtekoodist, mis on testitud ja auditeeritud).
2. Rakenduse käivitamine.
3. Tulemuse võrdlus ametliku lugemistõendi kontrollija poolt väljastatuga.
4. Vajadusel erisuste analüüs ning lahendamine.

Lugemistõendi kontroll erineb miksimistõendi kontrollist selle poolest, et lugemistõendi kontrollimiseks vajalikud sisendid pole olemuselt privaatsed. See tähendab, et põhimõtteliselt võib kõik lugemistõendi auditiks vajalikud sisendid Internetis avalikustada. See annaks kõigile huvilistele võimaluse lugemistõendeid enda poolt usaldatavate vahenditega uurida.

Siiski tuleb IVXV protokolli enne sellise sammu astumist täiendada. Probleem algab sellest, et põhimõtteliselt on valijal võimalik anda hääl, mis ei kodeeri ühtegi võimalikku kandidaati, vaid mõne muu väärtuse. Hetkel niisuguste häälte kohta lugemistõendit ei väljastata. Teisest küljest tähendab selline käitumine, et Võtmerakendusel on voli mõne hääle kohta väita, et selle dekrüpteerimisel ei saadud kehtivat häält, aga tal pole kohustust seda väidet tõestada. Seeläbi saab pahatahtlik Võtmerakendus mõne hääle kokkulugemisest kõrvale hiilida.

Täieliku läbipaistvuse huvides tuleks anda tõestus ka kehtetute häälte kohta. Tehniliselt kõige lihtsam moodus selleks on anda samasugune lugemistõend nagu kehtivate häältegi korral, väljastades muuhulgas avalikuks auditeerimiseks ka selle kehtetu hääle.

Samas võib ka kehtetu hääl kanda endas informatsiooni ja seda informatsiooni saab kasutada ära erinevates rünnetes.

- Kõige lihtsamal juhul võib ründaja mõjutada valijat hoiduma kehtiva hääle andmisest. Selleks annab ründaja valijale ette enda poolt genereeritud väärtuse ning nõuab selle krüpteerimist kehtiva hääle asemel. Kui hiljem pannakse auditeerimiseks avalikult välja ka kehtetud e-hääled, võib ründaja kontrollida, kas mõjutatav valija tõepoolest allus mõjutusele või mitte.
- Kehtetu hääl võib endas kanda krüptovõtit, mille abil saab dekrüpteerida lekkinud riiklikke saladusi [23]. See rünne sunniks valimiste korraldajat valima valimiste läbipaistvuse ja konfidentsiaalse info lekitamise vahel. Samas hindame niisugust rünnet üsna teoreetiliseks – kui ründajal on ligipääs tundlikele riiklikele saladustele, siis on tal nendega arvatavasti muudki teha kui valimisi rünnata.
- Johannes Müller avaldas 2022. aastal ründe, mis kasutab ära Eesti e-häälte krüpteerimiseks kasutatava ElGamali krüptosüsteemi homomorfsust [24]. See omadus võimaldab ründajal mitu krüptogrammi üheks kombineerida (suutmata seejuures üksikuid krüptogramme dekrüpteerida!). Järgmiseks peab ründaja kombineeritud krüptogrammi mõne korrumpeerunud valija abil legitiimse hääle pähe ära esitama ja hiljem dekrüpteeritud väärtuse

auditifaasis kätte saama. Pärast seda võib ründaja näiteks kontrollida, kas kombineeritud krüptogrammi moodustanud väärtused vastasid tema poolt soovitutele. Niisugust võimekust saaks kasutada ära osana laiemast mõjutusründest.

Kui kehtetud hääled pandaks auditeerimiseks avalikult välja, kaitseks IVXV süsteemi viimasena mainitud ründe eest hetkeseadetes peamiselt kogumisteenuse füüsiline ja organisatsiooniline turve, mis teeb krüpteeritud häältele ligipääsemise ründaja jaoks keerukaks.

On olemas ka täiendav krüptograafiline meede Mülleri ründe neutraliseerimiseks. Nimelt saab hääle andmise sammul lisada nullteadmustõestuse selle kohta, et hääletaja ise teab oma hääle väärtust ja väärtuse krüpteerimisel kasutatud juhuarvu. Siis ei ole ründajal võimalik kombineeritud häält anda, sest ta ei tea kombineeritud hääle kohta vajalikke väärtusi (ja kui ta neid teab, siis tal on nagunii ohvrite üle täielik kontroll).

Esimese kahe ründe vastu sellisest nullteadmustõestusest ei piisa, vaja on tõestust selle kohta, et krüptogrammi alla on kodeeritud korrektne kandidaat. Niisugune tõestus on keerukam ja võib eeldata vajadust protokolli muuta.

Kõik toodud ründed eeldavad mitteametliku valijarakenduse kasutamist, kuid see on tehniliselt teostatav [25].

4.3 Korrektse teisendamise täiendav auditeerimine

Verificatumi ja IVXV andmevormingute vahel teisendamiseks on IVXV paketis olemas eraldi Teisendusrakendus. Selle komponendi töö korrektsust saab kontrollida Auditirakendusega, mis on samuti IVXV paketi osa. Ideaalis oleks vaja nende teisenduste korrektsust kontrollida ka sõltumatu osapoole loodud vahendiga.

Andmevormingute vahelise teisenduse auditeerimine erineb miksimis- ja lugemistõendi kontrollist, sest siin ei kasutata otseselt krüptograafilisi saladusi. Seega pole vaja genereerida ega verifitseerida nullteadmustõestusi. Tegemist on deterministliku protsessiga, mille sisendeid ja väljundeid saab lihtsalt võrrelda (näiteks kontrollsummade abil). Küll aga tuleb arvestada, et esimene teisendus toimub enne e-urni miksimist, niisiis ei saa teisendatavaid väärtusi avalikuks auditeerimiseks Internetti välja panna. Täiendavate auditirakenduste kaasamine, koodi auditeerimine, käivitamine jm peaks seega toimuma sama moodi nagu miksimistõendite korral. Teist teisendust, mis toimub pärast miksimist, võib põhimõtteliselt auditeerida ka avalikult.

4.4 Rahvusvahelise kogukonna kaasamine arendusse

Eesti e-hääletamise süsteemi on siiani arendatud poliitilise tellimuse alusel ja kohalike inseneride poolt. Mõlemail neist on protsessis oma koht, kuid meie hinnangul on edaspidi otstarbekas kaasta ka laiemat rahvusvahelist kogukonda. Kaaluda võib näiteks järgmisi samme.

- **Rahvusvahelise nõuandva kogu moodustamine.** Maailmas on veel riike, kus elektroonilise kaughääletamise kallal töötatud on (näiteks Šveits, Norra, Austraalia, Prantsusmaa jt). Nende maade ekspertide kogemus on väärtus, mida tasub ka meil arvesse võtta. Üheks võimalikuks viisiks on moodustada rahvusvaheline ekspertgrupp, mis teatava regulaarsusega kokku kutsutake ning mille liikmete käest vajadusel nõu küsida saab.
- **Protokollitäienduste kavandamine ja väljatöötamine rahvusvahelise kogukonna kaasabil.** Nagu ka siinsest aruandest nähtub, on Eesti e-hääletamise süsteem keerukas, koosnedes paljudest komponentidest ning nõudes põhjalikuks analüüsiks mittetriviaalset kompetentsi. Eriti kehtib see krüptograafiliste aspektide väljatöötamisel, kus tuleb kirjeldada formaalsed

turvaeesmärgid ning seejärel tõestada, et need turvaeesmärgid plaanitava lahendusega tõepoolest saavutatakse. Ka selles vallas oleks meil rahvusvahelise kogukonna kaasamisest palju võita.

- ***Bug bounty* tüüpi süsteemitestimiste regulaarne korraldamine.** Peale formaalselt tõestatud turvaomadustega krüptoprotokollistiku peab ka reaalne teostus vastama kõrgetele nõuetele. Eesti e-hääletamise süsteemi küll läbistustestitakse, kuid sedagi protsessi võiks laiendada rahvusvahelise kogukonna kaasamisega. *Bug bounty* tüüpi ettevõtmised on üks, kuigi muidugi mitte ainus võimalus selles vallas.

Viited

[1] John Stuart Mill. *Thoughts on parliamentary reform*. JW Parker, 1859.

[2] Thomas Mulligan. "Plural Voting for the Twenty-First Century". *The Philosophical Quarterly* 68.271 (september 2017), lk. 286–306. DOI: 10.1093/pq/pqx046.

[3] Paula Wasley. "Back When Everyone Knew How You Voted". *Humanities* 37.4 (2016).

[4] Peter Brent. "The Australian ballot: Not the secret ballot". *Australian Journal of Political Science* 41.1 (2006), lk. 39–50.

[5] Charlotte Reinisch ja John Parkinson. *Swiss Landsgemeinden: a deliberative democratic evaluation of two outdoor parliaments*. ECPR Joint Sessions, University of Helsinki. 2007.

[6] Silvano Moeckli. *Die schweizerischen Landsgemeinde-Demokratien*. Staat und Politik. Bern: Paul Haupt, 1987.

[7] Benoît Chevallier-Mames *et al*. "On Some Incompatible Properties of Voting Schemes". Teoses: *Towards Trustworthy Elections, New Directions in Electronic Voting*. Toim. David Chaum *et al*. Köide 6000. Lecture Notes in Computer Science. Springer, 2010, lk. 191–199. DOI: 10.1007/978-3-642-12980-3_11.

[8] Alisa Pankova ja Jan Willemson. "Relations Between Privacy, Verifiability, Accountability and Coercion-Resistance in Voting Protocols". Teoses: *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings*. Toim. Giuseppe Ateniese ja Daniele Venturi. Köide 13269. Lecture Notes in Computer Science. Springer, 2022, lk. 313–333. DOI: 10.1007/978-3-031-09234-3_16.

[9] Jan Willemson. "Bits or paper: Which should get to carry your vote?" *J. Inf. Secur. Appl.* 38 (2018), lk. 124–131. DOI: 10.1016/j.jisa.2017.11.007.

[10] Chad Cotti *et al*. "The relationship between in-person voting and COVID-19: Evidence from the Wisconsin primary". *Contemporary economic policy* 39.4 (2021), lk. 760–777.

[11] *Global overview of COVID-19: Impact on elections*. Institute for Democracy and Electoral Assistance, https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections. 2022.

[12] Robert Krimmer ja Melanie Volkamer. "Bits or Paper? Comparing Remote Electronic Voting to Postal Voting". Teoses: *Electronic Government - Workshop and Poster Proceedings of the Fourth International EGOV Conference 2005, August 22-26, 2005, Copenhagen, Denmark*. Toim. Kim Viborg Andersen *et al*. Köide 13. Schriftenreihe Informatik. Universitätsverlag Rudolf Trauner, Linz, Austria, 2005, lk. 225–232.

[13] Josh Benaloh, Peter Y. A. Ryan ja Vanessa Teague. "Verifiable Postal Voting". Teoses: *Security Protocols XXI - 21st International Workshop, Cambridge, UK, March 19-20, 2013, Revised Selected Papers*. Toim. Bruce Christianson *et al*. Köide 8263. Lecture Notes in Computer Science. Springer, 2013, lk. 54–65.

[14] Ari Juels, Dario Catalano ja Markus Jakobsson. "Coercion-resistant electronic elections". Teoses: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES 2005, Alexandria, VA, USA, November 7, 2005*. Toim. Vijay Atluri, Sabrina De Capitani di Vimercati ja Roger Dingledine. ACM, 2005, lk. 61–70. DOI: 10.1145/1102199.1102213.

[15] Roberto Araújo *et al*. “Towards Practical and Secure Coercion-Resistant Electronic Elections”. Teoses: *Cryptology and Network Security - 9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14, 2010. Proceedings*. Toim. Swee-Huay Heng, Rebecca N. Wright ja Bok-Min Goi. Köide 6467. Lecture Notes in Computer Science. Springer, 2010, lk. 278–297. DOI: 10.1007/978-3-642-17619-7_20.

[16] André Silva Neto *et al*. “Usability Considerations For Coercion-Resistant Election Systems”. Teoses: *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, Belém, Brazil, October 22-26, 2018*. Toim. Marcelle Mota *et al*. ACM, 2018, 40:1–40:10. DOI: 10.1145/3274192.3274232.

[17] *Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel*. Versioon 1.0. Dokumendi versioon IVXV-ÜK-1.0, 2017, https://www.valimised.ee/sites/default/files/2021-10/IVXV%20elektroonilise%20h%C3%A4%C3%A4letamise%20%C3%BCldraamistik.pdf.

[18] Riigi Valimisteenistus. *IVXV: E-hääletamise käsiraamat*. Versioon 0.6. Dokumendi versioon IVXV-KR-0.6, 2019, https://www.valimised.ee/sites/default/files/2021-10/IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat.pdf.

[19] *IVXV arhitektuur*. Versioon 1.7.6. Dokumendi versioon IVXV-AR-1.7.6, 2021, https://www.valimised.ee/sites/default/files/2021-10/IVXV%20arhitektuur.pdf.

[20] *IVXV võtmerakendus*. Versioon 1.4.0. Dokumendi versioon IVXV-SVR-1.4.0, 2019, https://www.valimised.ee/sites/default/files/2021-10/IVXV%20v%C3%B5tmerakendus.pdf.

[21] *IVXV protokollide kirjeldus*. Versioon 1.7.6. Dokumendi versioon IVXV-PR-1.7.6, 2021, https://www.valimised.ee/sites/default/files/2021-10/IVXV%20protokollide%20kirjeldus.pdf.

[22] Thomas Haines, Rajeev Goré ja Bhavesh Sharma. “Did you mix me? Formally Verifying Verifiable Mix Nets in Electronic Voting”. Teoses: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, lk. 1748–1765. DOI: 10.1109/SP40001.2021.00033.

[23] Douglas Wikström *et al*. “How Could Snowden Attack an Election?” Teoses: *Electronic Voting - Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings*. Toim. Robert Krimmer *et al*. Köide 10615. Lecture Notes in Computer Science. Springer, 2017, lk. 280–291. DOI: 10.1007/978-3-319-68687-5_17.

[24] Johannes Müller. “Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV”. Teoses: *Workshop on Advances in Secure Electronic Voting 2022*. https://orbilu.uni.lu/bitstream/10993/49442/1/main.pdf. 2022.

[25] Valeh Farzaliyev, Kristjan Krips ja Jan Willemson. “Developing a Personal Voting Machine for the Estonian Internet Voting System”. Teoses: *SAC ’21: The 36th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, Republic of Korea, March 22-26, 2021*. Toim. Chih-Cheng Hung *et al*. ACM, 2021, lk. 1607–1616. DOI: 10.1145/3412841.3442034.