TARTU ÜLIKOOL
Arvutiteaduse instituut
Infotehnoloogia mitteinformaatikutele õppekava

Lauri Ütsik

E-valimiste protsessid Riigikogu valimiste näitel

Magistritöö (15 EAP)

Juhendajad: Kristjan Krips, PhD
Jan Villemson, PhD

Tartu 2024

E-valimiste protsessid Riigikogu valimiste näitel

Lühikokkuvõte:

Käesolev magistritöö käsitleb on Eesti e-valimiste protsesside modelleerimist BPMN modelleerimiskeeles alates Eesti Vabariigi Põhiseadusest tulenevast valimiste korraldamise kohustusest kuni viimase alamprotsessini, milleks on e-valimiste protseduurideks kasutatud süsteemiketta, võtmeosakute ja e-häälte hävitamine. Töö täpsem fookus on suunatud e-valimiste auditeerimisele. Protsesside modelleerimisele järgneb analüüsi osa, milles tuuakse esile ebakõlad juhendmaterjali ja tegeliku olukorra vahel ning pakutakse parendusvõimalusi. Uuringus on läbivalt kasutatud Eesti Vabariigi Riigikogu valimiste näidet.

Võtmesõnad:

Protsesside modelleerimine, protsesside analüüs, e-valimised

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine

E-election processes on the example of the Parliamentary elections of the Republic of Estonia

Abstract:

The scope of this master's thesis is the modelling of the processes of Estonian e-elections in the BPMN modelling language, from the obligation to organise elections arising from the Constitution of the Republic of Estonia to the last sub-process, which is the destruction of the system disk, key shares and e-votes used for e-election procedures. The more precise focus of the work is aimed at auditing e-elections. The process modelling is followed by the analysis part, in which inconsistencies between the instructional material and the actual situation are pointed out, and opportunities for improvement are proposed. The research was carried out using the example of the Parliamentary elections of the Republic of Estonia.

Keywords:

Business process modelling, process analysis, e-voting

CERCS: P170 - Computer science, numerical analysis, systems, control

Sisukord

1. Sissejuhatus

Elektroonilised valimised, tuntud ka kui e-valimised, on Eestis kasutusel alates 2005. aastast ja nende populaarsus on ajas järjest kasvanud [1]. Elektroonilise hääletamise statistikast[1] selgub, et 2023. aasta Riigikogu valimistel ületas e-häälte arv esmakordselt valimisjaoskonnas antud häälte arvu, mis näitab ühiskonna kõrget usaldust e-hääletamise suhtes. Ometi on ühiskonnas hulk inimesi, kes kahtlevad e-valimiste korralduses ning see on üheks aspektiks, miks nad ei usalda e-valimiste tulemusi ega pea seda piisavalt turvaliseks. Seda usaldamatust külvavad ka ühe poliitilise partei esinumbrite põhjendusteta avaldused, justkui oleks 2023. aasta Riigikogu valimised varastatud e-hääletuse kaudu[2]. Ka on vanem generatsioon harjunud paberhääletusega. OSCE on 2023. aasta raportis [2] rõhutanud, et e-valimiste kohta avaldatud dokumentatsioon on kohati puudulik, mis raskendab valimiste protsessidest arusaamist ning mis omakorda võib pärssida avalikkuse usalduse kasvu elektroonilise hääletamise suhtes või koguni seda kahandada. Lisaks on vajalik informatsioon killustatud erinevate allikate vahel ning puudub ühtne allikas, kust oleks võimalik leida informatsiooni e-valimiste protsesside kohta tervikuna. Seetõttu soovitab OSCE oma raportis [2] valimiste korraldajal avaldada täielik, täpne ja ajakohastatud dokumentatsioon elektroonilise hääletamise kohta.

Käesoleva magistritöö eesmärgiks on e-valimiste olemasolevate protsesside tuvastamine avalikest allikatest leitava info põhjal ja protsesside modelleerimine, kasutades BPMN (*Business Process Model and Notation*) metoodikat. Suuremat tähelepanu pööratakse elektroonilise hääletamise auditeerimisele ja audiitorite rollile protsessis. Analüüsi osas tuuakse välja tähelepanekud leitud puuduste ja ebakõlade kohta ning pakutakse parendusettepanekuid. Protsesside tuvastamisel ja modelleerimisel jälgitakse tervet e-valimistsükli elukaart Riigikogu valimiste näitel: alates Eesti Vabariigi Põhiseaduse § 60 tulenevast kohustusest korraldada Riigikogu valimisi iga nelja aasta tagant kuni elektroonilise hääletamise viimase etapini, milleks on võtmeprotseduurideks kasutatud süsteemiketta, võtmeosakute ja e-häälte avalik hävitamine. Paralleelselt elektroonilise hääletamise korraldamisega toimub ka paberhääletamine jaoskondades, kuid käesoleva töö raames seda ei käsitleta, välja arvatud ühel juhul, kus e-hääletanud valijal on võimalik jaoskonnas oma valikut muuta.

[1] https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-haaletamise-statistika (18.04.2024)
[2] https://www.err.ee/1608909122/ekre-taotleb-riigikohtult-e-haaletuse-tulemuste-tuhistamist (18.04.2024)

Käesoleva magistritöö lõpptulemusena valmisid ülevaatlikud elektroonilise hääletamise protsesside mudelid koos kirjeldava dokumentatsiooniga.

Valminud lõputöö algab taustainfo peatükiga, mis annab ülevaate elektroonilise hääletamisega seotud osapooltest, valimiste korralduslikest etappidest ning varasematest e-hääletuse uuringutest. Neljandas peatükis on esile toodud valitud metoodika kirjeldus. Töö põhilise osa moodustavad e-valimiste protsesside mudelid koos detailse kirjeldusega kolmes järjestikus peatükis vastavalt e-valimiste korralduslikele etappidele. Viiendas peatükis vaadeldakse elektroonilise hääletamise ettevalmistavaid tegevusi, kuuendas peatükis kajastatakse vahetult e-hääletamise ajal ja häälte kogumisega seotud protsesse ning seitsmendas peatükis on toodud häälte kogumise perioodi järgsed protsessid. Kaheksandas peatükis on välja toodud tähelepanekud ja vastuolud e-valimiste juhendmaterjalis ning esitatud võimalikud parendusettepanekud. Üheksandas peatükis on analüüsitud audiitori rolli e-valimiste toimingute kontrollimisel ning välja toodud ettepanekud, mida peaks audiitor täiendavalt kontrollima ja kuidas muuta audiitori raportit nii, et see oleks valijale paremini arusaadav. Kokkuvõtte peatükis on kirjeldatud protsesside vastavust dokumentides toodud juhistele, magistritöö eesmärkide saavutamist ja võimalikke edasisi uurimisteemasid e-valimiste valdkonnas.

2. Mõisted, terminid ja lühendid

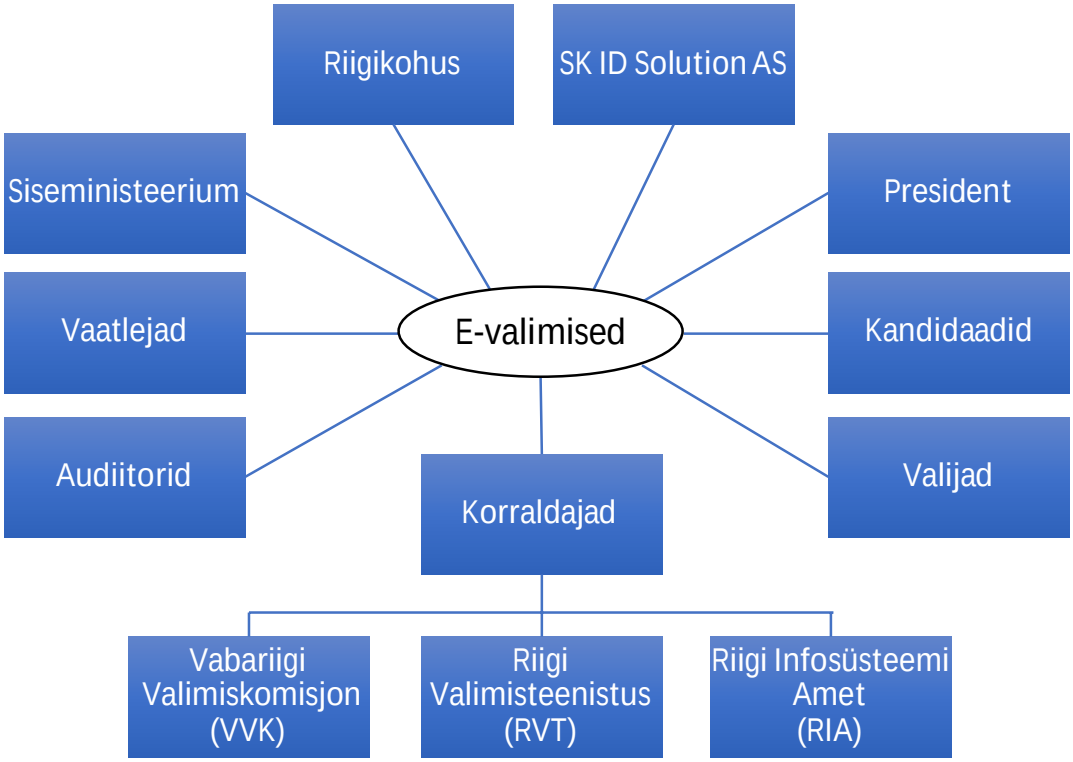
Allkirjastamisteenus	on allkirja andmise vahenditest (ID-kaart, Mobiil-ID) sõltuv teenus, mis abistab Hääletajat e-hääle allkirjastamisel ja mille abil Kogumisteenus küsib allkirja kehtivuskinnituse [3].
Auditirakendus	on audiitori põhitööriist, mille abil saab kontrollida häälte lugemise ja miksimise ning Verificatumi ja IVXV andmeformaatide teisenduste korrektsust [4, 5].
EHS	Elektroonilise hääletamise süsteem
E-hääletamine	Elektrooniline hääletamine ehk e-hääletamine on võimalus valida interneti vahendusel. Mujal maailmas on laialt levinud termin i-hääletamine (internet voting), kuna i-hääletamise termin ei ole Eestis laialdast kasutust leidnud, kasutab ka autor käesolevas töös läbivalt e-hääletamise terminit.
Kogumisteenus	on elektroonise hääletamise süsteemi keskne tarkvarakomponent, mis abistab Hääletajat Valijarakenduse vahendusel enda tuvastamisel ja e-hääle koostamisel ning registreerib selle Registreerimisteenuses enne hääle salvestamist e-valimiskasti [3]. Kogumisteenust haldab RVT ja majutab RIA.
Kontrollrakendus	on mobiilirakendus, mille abil saab Hääletaja veenduda, et tema antud e-hääl jõudis muutmata kujul Kogumisteenusesse [3].
Miksimisrakendus	on RVT põhitööriist, millega anonüümistatud krüpteeritud hääled segatakse nii, et neid ei ole võimalik sisendiga vastavusse viia; miksimisrakendus väljastab miksimistõendi [3].
PS	Eesti Vabariigi põhiseadus
Registreerimisteenus	on Kogumisteenusest eraldiseisev sõltumatu teenus, mille abil Koguja registreerib kõik Hääletajatelt laekunud e-hääled ning peale hääletusperioodi lõppu edastab kõik registreeringud e-valimiskasti Töötlejale [3].
RIA	Riigi Infosüsteemi Amet
RKVS	Riigikogu valimise seadus

RVT	Riigi Valimisteenistus
Tuvastusteenus	on Kogumisteenusest sõltumatu eraldiseisev teenus, mille abil tuvastatakse Hääletaja isik [3]. Hääletaja saab end tuvastada ID-kaardi või Mobiil-ID abil.
Töötlemisrakendus	on RVT põhitööriist, mille abil toimub häälte ja e-valimiskasti tervikluse kontrollimine ning selle abil tühistatakse korduvhääled ja topelthääled ning anonüümitakse e-hääled [3].
Usaldusjuur	määrab sertifitseerimishierarhiad, mille alusel IVXV komponendid verifitseerivad digitaalallkirju [4].
Valijarakendus	on tarkvarakomponent, mis võimaldab Hääletajal suhelda Kogumisteenusega enda tuvastamiseks, valiku tegemiseks, hääle krüpteerimiseks ja allkirjastamiseks. Peale hääletamist kuvab Valijarakendus QR-koodi, mille alusel on võimalik Kontrollrakendusega antud e-häält kontrollida [3].
VIS	Valimiste infosüsteem
VVK	Vabariigi Valimiskomisjon
Võtmerakendus	on RVT põhitööriist, mille abil genereeritakse e-häälte salastamise ja avamise võtmepaar ning mille abil toimub ka häälte lugemine [3].

3. Taustainfo

3.1 Elektroonilise valimise osapooled

Elektroonilise hääletamisega on seotud palju erinevaid osapooli, kuid põhiroll on siiski Korraldajate kanda, kellest sõltuvad ka kõik ülejäänud osapooled [3]. Joonisel 1 on toodud elektroonilise hääletamisega seotud osapooled.



Joonis 1. Elektroonilise hääletamise osapooled.

Alljärgnevalt on kirjeldatud seotud osapoolte ülesanded [3, 6, 7]:

1. Korraldajad – e-valimiste korraldamine jaguneb kolme institutsiooni vahel, milleks on:

- VVK – Vabariigi valimiskomisjoni pädevuses on elektroonilise hääletamise üldpõhimõtete tagamine, järelevalve tegemine RVT tegevuse üle, kandidaatide registreerimine ning valimiskaebuste lahendamine. Lisaks täidavad seitse VVK liiget ka häälte avamise võtmeosakute hoidja rolli.
- RVT – Riigi valimisteenistuse põhilisteks ülesanneteks on valimiste, sealhulgas elektroonilise hääletamise korraldamine ning selleks vajalike tehniliste lahenduste arendus ning haldus. RVT kanda on elektroonilise hääletamise Töötleja ja Lugeja roll. Kaks RVT liiget täidavad veel häälte avamise võtmeosakute hoidja rolli.

- RIA – Riigi Infosüsteemi amet täidab häälte Koguja rolli ehk nende vastutada on Kogumisteenuse serverisüsteemi toimimine. RIA vastutada on ka e-hääletamise küberturvalisuse tagamine. Hääletamise ja häälte kogumise perioodil pakub RIA klienditoe teenust, mis abistab hääletajat võimalike tekkivate probleemide korral.

2. SK ID Solutions AS – korraldajatest sõltumatu osapool, kes pakub nii Tuvastusteenust, Allkirjastamisteenust kui ka Registreerimisteenust.

3. Audiitor – sõltumatu osapool, kes kontrollib elektroonilise hääletamise süsteemi testimist, süsteemi terviklust ning RVT poolt läbi viidavate toimingute vastavust juhendmaterjalile ja küberturvalisuse üldtunnustatud reeglitele. Audiitori kohalolu on kohustuslik.

4. Vaatlejad – valimiste vaatlemine on vabatahtlik, igaühel on õigus vaadelda valimiste korraldajate toiminguid. Elektroonilise hääletamise vaatlejatele korraldab RVT enne igat perioodi vastava koolituse, et e-hääletamise süsteem ja korraldus oleks neile arusaadav. Tuleb arvestada asjaoluga, et kui vaatlemissooviga isikuid on väga palju, siis kõigile ei pruugi koolitusel kohti jaguda.

5. Kandidaadid – Riigikogu valimistel saavad kandideerida nii erakondade kandidaadid kui ka üksikkandidaadid. Kandideerida võib hääleõiguslik Eesti Vabariigi kodanik, kes hiljemalt kandidaatide registreerimise aja viimaseks päevaks on saanud 21-aastaseks.

6. Valijad – Riigikogu valimistel on hääletamisõigus igal Eesti Vabariigi kodanikul, kes hiljemalt valimispäevaks on vähemalt 18-aastane. Hääletada ei saa isikud, kes on tunnistatud teovõimetuks või kannavad vanglakaristust.

7. Siseministeerium – Rahvastikuregistri vastutav töötleja, kes vastutab valimiste teabelehe ja valijate nimekirja koostamise eest.

8. Riigikohus – tegeleb valimiskaebuste lahendamisega, kui huvitatud isik leiab, et valimiste korraldaja toiminguga või otsusega rikutakse tema õigusi. Kaebuse riigikohtule võib esitada alles peale kaebuse lahendamist Vabariigi Valimiskomisjonis.

9. Vabariigi President – kuulutab välja Riigikogu valimised vähemalt kolm kuud enne valimispäeva.

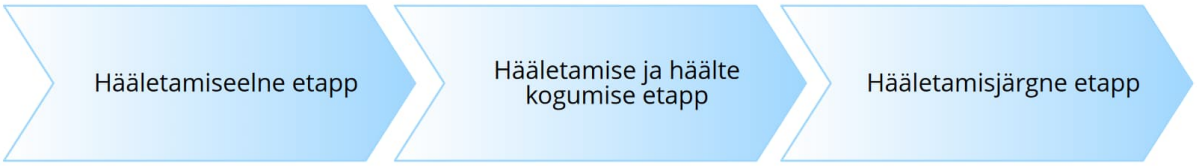
Lisaks põhirollidele on veel e-hääletamisega seotud osapooleks EHS-i (elektroonilise hääletamise süsteem) arendajad ja hooldajad, aga selleks ei ole kindlat institutsiooni, RVT valib igakordse partneri välja riigihanke korras.

3.2 Elektroonilise valimise etapid

Elektroonilise hääletamise üldraamistiku [3] alusel jagunevad e-valimised neljaks etapiks, milleks on:

1. Hääletamiseelne etapp;
2. Hääletamise ja häälte kogumise etapp;
3. Häälte töötlusetapp;
4. Häälte lugemisetapp.

Tinglikult võib kolmanda ja neljanda etapi lugeda üheks – hääletamisjärgseks etapiks, mille tegevused toimuvad peale hääletamist ja häälte kogumise lõppemist. Joonisel nr 2 on toodud elektroonilise hääletamise etappide väärtusahel.



Joonis 2. Elektroonise hääletamise etappide väärtusahel.

Esimeses etapis seatakse üles elektroonilise hääletamise süsteem, kuulutatakse välja lähenevad valimised, registreeritakse kandidaadid, koostatakse valijate esialgne nimekiri. Hääletamiseelne etapp lõpeb valijarakenduse avaldamisega vahetult enne e-hääletamise algust.

Teises etapis saavad kõik hääleõiguslikud isikud hääletada enda soovitud kandidaadi poolt. Taustal tegelevad valimiste Korraldajad häälte kogumisega. Lisaks e-hääletamisele käib ka paberhääletamine jaoskondades, kus on võimalik oma antud e-häält muuta, kui valija tunneb, et teda on senise valiku tegemisel mõjutatud.

Viimasel ehk hääletamisjärgsel etapil toimub häälte töötlemine ja lugemine ning e-valimistulemuste väljakuulutamine. Sellele järgneb valimiskaebuste lahendamine VVK ja Riigikohtu poolt ning elektroonilised valimised lõpevad e-valimiste süsteemiketta ja võtmeosakute avaliku hävitamisega. Iga etapi detailsed tegevused koos alamprotsesside kirjeldustega on toodud käesoleva töö peatükkides 5, 6 ja 7.

3.3 Varasemad uuringud

Järgnevalt on toodud valik varasematest uuringutest. Uuringute valiku kriteeriumiteks olid aspektid, et artikkel/raport käsitleks tervikuna Eesti e-valimiste protsessi, mitte ei keskenduks üksiku protseduuri, tarkvarakomponendi või turvalisuse aspektile ning võimalusel käsitleks e-valimiste korraldust aastate lõikes.

Michigani ülikooli abiprofessor J. Alex Halderman jt [8] uurisid 2013. aasta kohalike valimiste ajal elektroonilise hääletamise süsteemi turvalisust ja kontrollitavust. Nad lõid laboris e-hääletamise süsteemist oma koopia ja ründasid seda, uurimaks, kas süsteemiga manipuleerides on võimalik valimistulemusi mõjutada. Lisaks jälgisid nad e-valimiste protseduuride läbiviimist. Autorid tõid oma uurimuses välja mitmeid kitsaskohti, kus elektroonilise hääletamise süsteem ei olnud piisavalt kontrollitav, samuti alahinnati sisemise ründaja ohtu ning usaldati liialt valijate arvuteid, mis võisid olla häält muutva kahjurvara/pahavara sihtmärgiks. Uuringu tulemus oli üheks sisendiks, miks RVT muutis valimistega seotud protseduure ning 2017. aastal võeti kasutusele uus elektroonilise hääletamise süsteem – IVXV, seejärel muutus e-hääletamine otsast lõpuni kontrollitavaks [9].

Ehin ja teised [1] uurisid oma töös, kuidas on Eesti e-hääletus arenenud ja muutunud 15 aasta jooksul − vahemikus 2005-2019 korraldatud üheteistkümne elektroonilise hääletuse põhjal. Uuringus analüüsiti muutusi valimiste korralduses, valimiste statistikat ning usaldust elektroonilise hääletamise suhtes valimisjärgsete intervjuude põhjal. Artikli tulemustest selgub, et aasta-aastalt on e-hääletajate osakaal kasvanud: kui see 2005. aastal oli kõigest 0,9%, siis 2019. aastaks oli e-hääletajate osakaal jõudnud 46,9%-ni kõikidest antud häältest. Samas ei ole e-hääletamine valimisaktiivsuse hüppelist kasvu endaga kaasa toonud, pigem on valijate eelistus ajas muutunud e-hääletamise kasuks. Alates 2009 Euroopa Parlamendi valimistest on naiste osakaal e-hääletajate hulgas suurem, moodustades 2019. aastal 54% kogu e-hääletajate hulgast. Uuringust selgub, et elektroonilise hääletamise usaldusväärsus püsib kõrgel 70% juures ja viieteistkümne aastaga ei ole suuri muutusi toimunud.

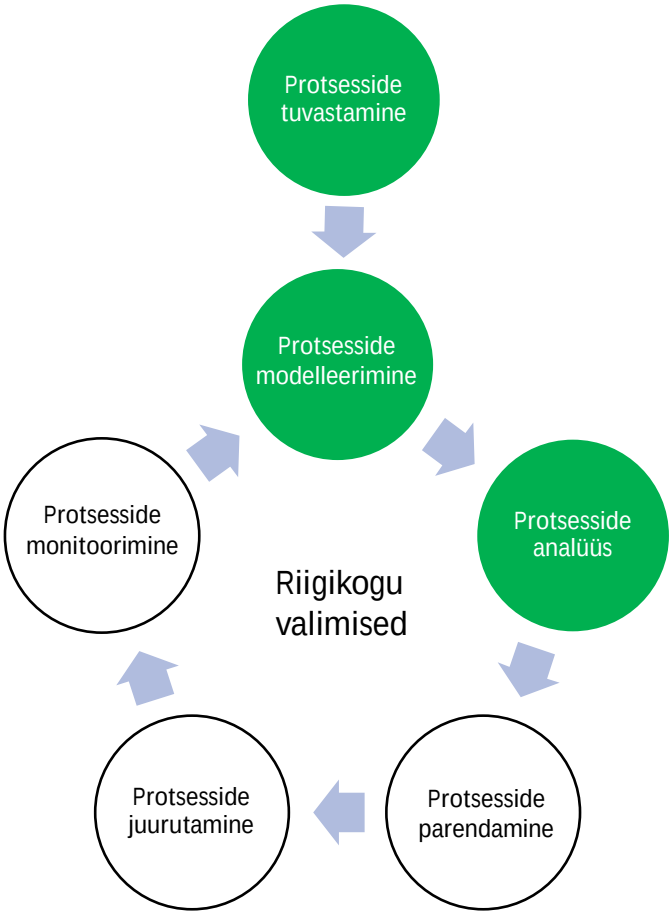
Alates elektroonilise hääletamise kasutuselevõtust 2005. aasta kohalike omavalitsuse valimistel, on Demokraatlike institutsioonide ja inimõiguste büroo (OSCE/ODIHR) esindajad käinud Riigikogu valimisi vaatlemas viiel järjestikul korral (2007, 2011, 2015, 2019, 2023). Nende raportitest [2, 10, 11, 12, 13] selgub, et juba 2007. aastal olid kaks poliitilist parteid, Eestimaa Rahvaliit ja Eesti Keskerakond, e-valimiste vastu ning kahtlesid selle usaldusväärsuses. 2023. aastal on suur pilt võrdlemisi sarnane − Eestimaa Konservatiivne Rahvaerakond väidab põhjendusteta, et 2023. a valimised on neilt e-hääletamise kaudu varastatud. Võrreldes vanemaid raporteid uutega, selgub, et esimestel kordadel esines probleeme elektroonilise hääletamise vaatlemisel, lisaks ei olnud häältelugemise protsess täielikult läbipaistev. 2023. aasta raportist selgub, et need puudused on valdavalt kõrvaldatud, kuid rõhutatakse, et VVK peab jätkuvalt selgitama e-valimiste protsessi ja tulemuste teavitamise ajakava. Samuti soovitatakse avaldada täielik, täpne ja ajakohastatud

dokumentatsioon e-hääletamise tehnoloogiate ja protsesside kohta. Nende nõuete täitmine aitab kõrvaldada kahtluse valimistulemuste usaldusväärsuses. Lisaks soovitatakse korraldajatel kaaluda meetodeid, kuidas saavutada läbiv kontrollitavus ning tagada, et kõik elektroonilise hääletamise tulemuste kindlaksmääramise etapid oleksid auditeeritavad.

Eelmainitud raportites [2, 10, 11, 12, 13] on välja toodud mitu probleemi, mis on jätkuvalt lahenduseta: üheks selliseks murekohaks on vangide absoluutne valimisõiguse piiramine, mis ei ole kooskõlas Euroopa standarditega. Vangide valimisõiguse piiramist saab kohandada üksnes raskete kuritegude eest, kus valimisõigusest ilmajätmine on kooskõlas määratud karistusega. Teise pikalt käsitlemata soovitusena tuuakse välja jätkuvalt suurt hulka kodakondsuseta isikuid, kes ei saa täiel määral teostada oma poliitilisi õigusi, näiteks hääletada Riigikogu valimistel või kuuluda erakonda.

4. Metoodika

Autor teostas uurimuse lähtudes M. Dumas jt [14] poolt soovitatud protsesside elukaare kontseptsioonist. Käesolevas magistritöös piirdutakse ainult kolme esimese etapi käsitlemisega, milleks on protsesside tuvastamine, protsesside modelleerimine ning protsesside analüüs. Ülejäänud etapid, milleks on protsesside parendamine, protsesside juurutamine ning monitoorimine jäävad käesoleva töö käsitlusalast välja. Joonisel 3 on toodud äriprotsesside elukaar, rohelisega on tähistatud käesolevas töös käsitletud etapid Riigikogu korraliste valimiste näitel.



Joonis 3. Äriprotsesside elukaar [14].

Töös kasutatud metoodika on jaotatud kolmeks mooduliks:

1. Töö avalikest allikatest pärit dokumentatsiooniga elektroonilise hääletamise protsesside tuvastamiseks.
2. Elektroonilise hääletamise protsesside modelleerimine lähtudes BPMN metoodikast.
3. Protsesside analüüs, mis sisaldab ebakõlade väljatoomist olemasoleva dokumentatsiooni ja protsesside tegeliku läbiviimise vahel ning parendusettepanekute tegemist.

4.1 Töö dokumentatsiooniga

Protsesside tuvastamiseks kasutas autor avalikest allikatest pärit elektroonilise hääletamisega seotud juhendmaterjale. Esimeseks sammuks oli sobivate dokumentide valik. 2017. aastal uuendati EHS põhjalikult ja seetõttu muutus osa juhendmaterjalist mitterelevantseks.

Töö läbiviimisel on kasutatud valikut alljärgnevatest allikatest leitud materjalist:

1. RVT avaldatud e-valimiste juhendid;
2. RVT avaldatud e-valimiste käsiraamatud;
3. RVT korraldused Riigikogu kantselei dokumendiregistris;
4. OSCE valimiste vaatlemise raportid;
5. EHS-i ja VIS-i arenduste hangete dokumentatsioon Riigihangete registris;
6. audiitorite raportid;
7. VVK otsused;
8. valimiste korraldust puudutavad seadused ja määrused;
9. elektroonilise hääletamise IVXV dokumentatsioon GitHub'i repositooriumis;
10. VVK ja Riigikohtu valimiskaebuste lahendid;
11. elektrooniliste hääletamiste protseduuride salvestised Youtube'i platvormil.

Peale materjaliga tutvumist viidi läbi dokumentatsiooni analüüs, tuvastamaks elektroonilise hääletamisega seotud alamprotsesse Riigikogu valimiste korraldamise näitel. E-hääletamist kasutatakse veel kohalike omavalitsuste volikogude (KOV) ja Euroopa Parlamendi (EP) valimistel, kuid need jäävad käesolevast uurimusest välja. Eletroonilist hääletamist on veel võimalik kasutada ka rahvahääletuse korral, aga kuna seda pole Eesti veel kordagi toimunud, siis käesolev töö seda ei käsitle.

4.2 Protsesside modelleerimine

Protsesside modelleerimisel on lähtutud BPMN metoodikast ja kasutatud SAP Signavio tarkvara. Modelleerimise tulemusena valmisid elektroonilise hääletamise mudelid Riigikogu valimiste näitel, alates protsessi käivitajast, milleks on PS § 60 tulenev kohustus korraldada Riigikogu valimisi iga nelja aasta tagant, kuni viimase alamprotsessini, milleks on elektroonilise hääletamise süsteemiketta, võtmeosakute ja e-häälte hävitamine. Valminud protsesside mudelid on toodud koos tegevuste kirjeldusega töö järgnevates peatükkides.

Kuna valimised on demokraatlike protsesside alustala, siis on suuremat tähelepanu pööratud elektroonilise hääletamise auditeerimisele ja audiitorite rollile protsessides. Ainult audiitoril on

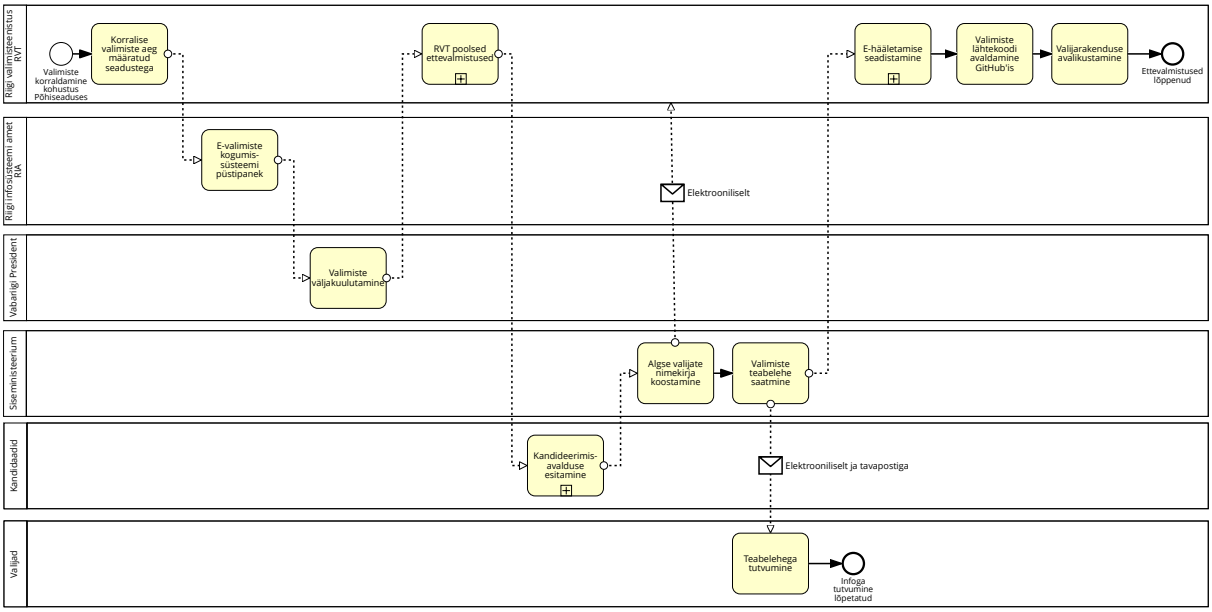
võimalik sõltumatult kontrollida, et e-valimiste Korraldaja on kõik häälte kogumise, töötlemise ja lugemise protseduurid viinud läbi korrektselt lähtuvalt juhenditest, seaduses sätestatust ja parimast küberturbe praktikast. Audiitor saab sõltumatu osapoolena kinnitada, et protseduuride läbiviimisel ei ole tuvastatud hääletamistulemusi mõjutavaid kõrvalekaldeid. Seetõttu saab väita, et audiitori töö korrektsusele ja läbipaistvusele võib taanduda e-valimiste usaldusväärsus.

4.3 Protsesside analüüs

Töö analüüsi osas tuuakse välja mitmed ebakõlad olemasoleva dokumentatsiooni ja tegelikkuses läbiviidud elektroonilise hääletamise toimingute vahel, mis on tuvastatud juhendmaterjali omavaheliste vastuolude ja e-hääletamise protseduuride videosalvestiste ning valimiskaebuste põhjal. Audiitori rolli analüüsimisel tuuakse välja mitmed protseduuride auditeerimise kitsaskohad, kus audiitori kontroll ei ole piisav või puudub sootuks. Välja on toodud audiitori raportis sisalduvad puudused. Kuid audiitori raport peaks tegelikult olema palju põhjalikum ja suunatud valijatele, kes saavad selle alusel kindluse, et valimistoimingud on läbi viidud korrektselt. Töö autor osales vaatlejana 2024. aasta Euroopa Parlamendi e-hääletamise protseduuridel, veendumaks käesolevas magistritöös esitatud informatsiooni õigsuses. Protsesside analüüsimisel lähtutakse M. Dumas jt [14] poolt soovitatud probleemide nimekirja ja juurpõhjuse analüüsi põhimõtetest ning antakse soovitusi puuduste kõrvaldamiseks.

5. E-valimiste ettevalmistavad protsessid

Valimisperioodi käivitajaks on PS § 60-st tulenev kohustus korraldada korralised Riigikogu valimised iga nelja aasta tagant. Riigikogu valimiste täpsemad nõuded ja reeglid on toodud Riigikogu valimise seaduses [7]. Käesoleva töö raames käsitletakse ainult korraliste Riigikogu valimiste korraldust puudutavat. E-valimiste ettevalmistused jagunevad eri institutsioonide vahel. Joonisel 4 on toodud elektroonilise valimise ettevalmistavad protsessid.



Joonis 4. E-valimiste ettevalmistavad protsessid.

E-valimiste ettevalmistavad tegevused lõpevad vahetult enne elektroonilise hääletamise perioodi algust, esmaspäeva hommikul, mil valimiste kodulehel avaldatakse Valijarakendus.

5.1 E-valimiste kogumissüsteemi käivitamine

Varasemast, 2023. aasta uuringust [15] selgub, et RIA kasutab elektroonilise hääletamise süsteemi teenuste tagamiseks pea 160 virtuaalserverit, mis käivitatakse umbes neli kuud enne valimispäeva ja on töös kuni e-valimiste häälte kogumise perioodi lõpuni. Enne igat valimisperioodi uuendatakse valimiste tarkvara ning viiakse läbi süsteemi koormus- ja läbistustestimine, kuid turvakaalutlustel RIA rohkem sellekohast infot ei avalda [5]. Valimiste infosüsteemi arendusse ja hooldusesse on kaasatud ka välised partnerid, Riigihangete registri alusel[3] on hetkel VIS-i arenduse (2022-2026) lepingupartner AS Nortal. RIA tellib raamlepingu alusel arendustöid ka AS Cyberneticalt[4].

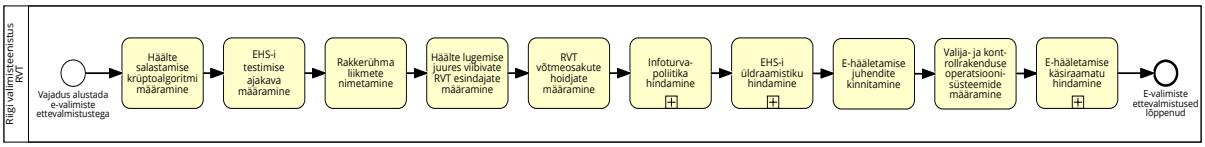
[3] https://riigihanked.riik.ee/rhr-web/#/procurement/4377089/general-info (20.04.2024)
[4] https://ria.ee/uudised/luuakse-pilootrakendus-e-haaletamiseks-nutiseadmes (20.04.2024)

5.2 Valimiste väljakuulutamine

Eesti Vabariigi põhiseaduse § 78 p 3 kohustab Vabariigi Presidenti välja kuulutama Riigikogu valimised, täpsemalt on antud nõue sätestatud RKVS § 2 lg 2, kus on esile toodud, et President kuulutab oma otsusega korralised valimised välja vähemalt kolm kuud enne valimispäeva. Valimiste väljakuulutamise pressiteade avaldatakse nii meedias kui ka Vabariigi Presidendi Kantselei kodulehel[5].

5.3 RVT-poolsed ettevalmistused

Umbes kaks kuud enne valimispäeva alustab omapoolseid ettevalmistusi RVT, nende läbi viidavad toimingud on toodud joonisel 5.



Joonis 5. RVT - poolsed e-valimiste ettevalmistused.

Antud toimingute läbiviimise järjekord võib valimisperioodiditi varieeruda, ülaltoodud näide on koostatud 2023. aasta Riigikogu valimiste näitel. Järgnevalt on kirjeldatud igal etapil toimuvat.

Krüptoalgoritmi valimine

RVT alustab elektroonilise hääletamise ettevalmistusi häälte salastamiseks kasutatava krüptoalgoritmi määramisega. Vastavalt VVK otsusele [16], mis sätestab, et elektroonilise häälte salastamiseks kasutatakse ElGamali krüptosüsteemi jäägiklassirühmas mooduli pikkusega vähemalt 2048 bitti. RVT hindab enne igat valimisperioodi arvutisüsteemide arengut, seal hulgas ka kvantarvutite arengut ning lähtuvalt sellest valib krüptosüsteemi mooduli pikkuse. RVT juhi korraldusega [17] määrati 2023. a Riigikogu valimistel kasutatavaks krüptosüsteemiks ElGamali jäägiklassirühm mooduli pikkusega 3072 bitti.

E-hääletamise pikaaegne juht Tarvi Martens on 2017. aastal selgitanud [18], et krüptosüsteemi mooduli pikkuse määramisel lähtutakse asjaolust, et e-hääle salajasus oleks tagatud kolmekümneks aastaks, kui krüpteeritud hääl peaks lekkima. Peale seda perioodi võiksid hinnangulised kahjud seoses valija poolt tehtud valiku avalikuks tulekuga, olla võimalikult väikesed. Kas sellest kriteeriumist lähtutakse ka tänasel päeval, ei ole teada.

Saksamaa riiklik infoturbe agentuur BSI (Bundesamt für Sicherheit in der Informationstechnik) annab oma 2024. aasta raportis [19] soovituse, et 3000-bitise mooduli pikkusega

[5] https://president.ee/et/ametitegevus/otsused/54335-208-riigikogu-korraliste-valimiste-valjakuulutamine (20.04.2024)

krüptosüsteemi võib kasutada kuni 2030+ aastani. Pluss aastaarvu järel tähendab seda, et krüptosüsteemi võib kasutada 2030. aastani ja peale seda tuleb jooksvalt hinnata, kas see on kasutatav ka edaspidi. Eespool mainitud raporti [19] põhjal võib väita, et Taavi Martensi selgitus, et krüptosüsteemi mooduli pikkuse määramisel lähtutakse asjaolust, et e-hääle salajasus oleks tagatud kolmekümneks aastaks, on ehk liialt optimistlik. Nii pikka krüptosüsteemi eluiga ei julge ükski agentuur ette ennustada.

Elektroonilise hääletamise süsteemi testimise ajakava määramine

Igal e-hääletamise ettevalmistusperioodil määrab RVT juht, RKVS § 48^2 lõike 4 punkti 3 alusel, oma korraldusega elektroonilise hääletamise süsteemi testimise ajakava ja ulatuse [20]. Antud korraldusega [20] määratakse täpne süsteemi testimise ehk prooviläbimise kuupäev, prooviläbimise korraldaja, kelleks on elektroonilise hääletamise rakkerühm. Samuti määratakse RVT ametiruumides viibivad isikud, kes saavad prooviläbimisel hääletada.

Elektroonilise hääletamise rakkerühma liikmete nimetamine

Lähtudes RKVS § 15 lõike 2 punkti 2 ja VVK otsusest [6], moodustab RVT juht oma korraldusega [21] elektroonilise hääletamise korraldamiseks, sh infoturbetegevuste koordineerimiseks, elektroonilise hääletamise rakkerühma, mille liikmeteks on [6]:

1. RVT elektroonilise hääletamise nõunik;
2. RVT elektroonilise hääletamise süsteemi operaator;
3. RIA nimetatud kogumisteenuse haldur;
4. RIA nimetatud võrguturbe juht;
5. RIA nimetatud elektroonilise hääletamise klienditeeninduse juht;
6. elektroonilise hääletamise süsteemi arendaja esindaja.

RVT elektroonilise hääletamise nõunik on ühtlasi ka rakkerühma juht.

Häälte lugemise juures viibivate RVT esindajate määramine

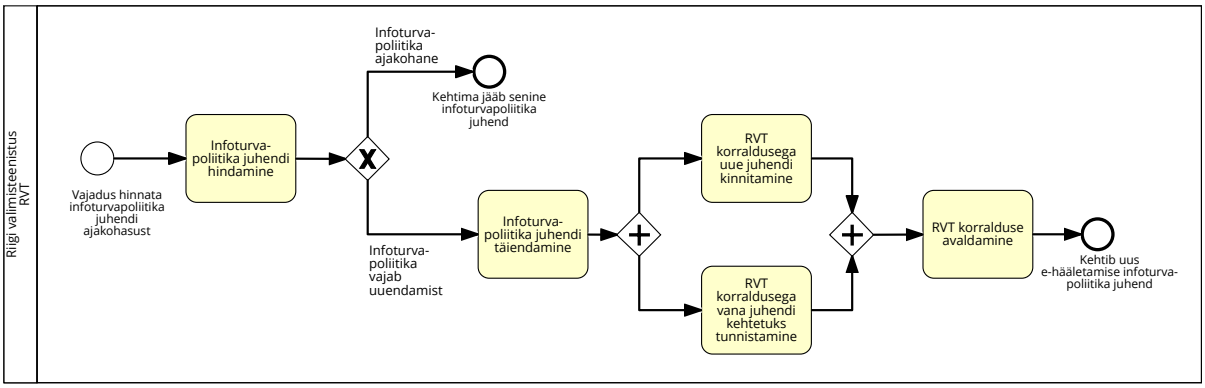
Lähtudes RKVS § 60^1 lõikest 2, määrab RVT juht oma korraldusega [22] vähemalt kolm Riigi Valimisteenistuse esindajat, kellel on kohustus viibida häälte avamise juures.

RVT võtmeosakute hoidjate määramine

RKVS § 48^3 lõike 3 alusel määrab RVT juht kaks Riigi Valimisteenistuse esindajat, kelle vahel jaotatakse ligipääsuvahendid elektrooniliste häälte avamise võtmele (ülejäänud seitse võtmeosakut jaotatakse VVK liikmete vahel).

Infoturvapoliitika hindamine

Enne igat valimisperioodi hindab RVT üle kehtiva „Riigi valimisteenistuse infoturvapoliitika“ juhendi [23] ja vajadusel uuendab seda (enne 2024. EP valimisi oli antud juhendi nimetus „Elektroonilise hääletamise süsteemi infoturbe poliitika“) [5]. Joonisel 6 on toodud infoturvapoliitika juhendi hindamise protsess.

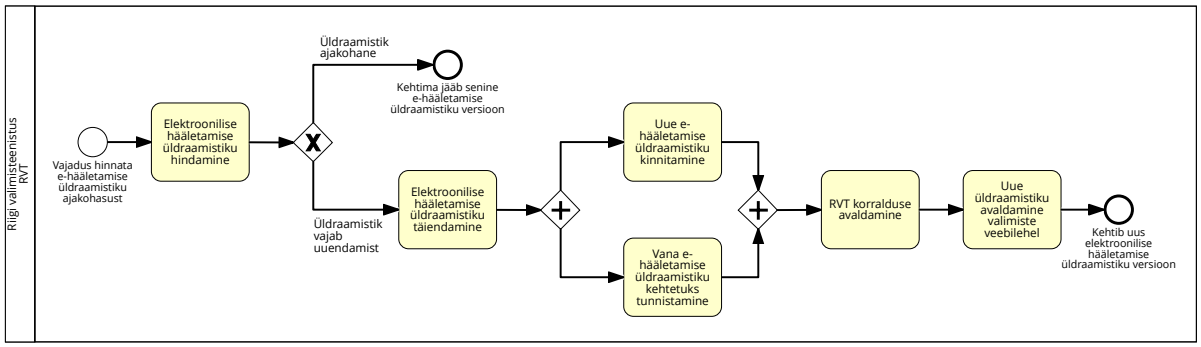


Joonis 6. Riigi valimisteenistuse infoturvapoliitika juhendi hindamise protsess.

Kui infoturvapoliitika juhend on ajakohane, siis muudatusi ei tehta ning kehtima jääb senine juhend. Kui hindamisel selgub, et juhend vajab uuendamist, siis RVT nõunik täiendab vastavaid juhendi peatükke. Seejärel, RVT juhi korraldusega [5], kinnitatakse uus juhend ning sama korraldusega tunnistatakse kehtetuks varasem korraldus. Vastav korraldus koos uue juhendiga avaldatakse Riigikogu kantselei dokumendiregistris[6] ja valimiste kodulehel.

Elektroonilise hääletamise süsteemi üldraamistiku hindamine

Enne igat valimisperioodi hindab RVT juhendmaterjali „Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel“ ajakohasust ja vajadusel uuendab teatud peatükke [3]. Joonisel 7 on toodud üldraamistiku hindamise protsess.



Joonis 7. Elektroonilise hääletamise üldraamistiku hindamise protsess.

RVT viib läbi kehtiva üldraamistiku hindamise ja kui see on jätkuvalt ajakohane, siis jääb kehtima olemasolev üldraamistik. Vastasel korral võtab RVT ette elektroonilise hääletamise

[6] https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/9717f73e-c9d0-4b29-b8af-40fc09b9b6b0 (20.04.2024)

üldraamistiku täiendamise ning RVT juhi korraldusega [3] kinnitatakse uus üldraamistik ja tunnistatakse kehtetuks varasem. Vastav korraldus avaldatakse Riigikogu kantselei dokumendiregistris[7] ja uus e-hääletamise üldraamistik avaldatakse ka valimiste veebilehel.

Elektroonilise hääletamise juhendite kinnitamine

Lähtudes RKVS § 48^2 lõike 4 punktist 1, kinnitab RVT oma korraldusega järgmised tehnilised juhendid elektroonilise hääletamise süsteemi opereerimiseks [24]:

1. IVXV − seadistuste koostamise juhend;
2. IVXV − valijarakenduse pakendamine;
3. IVXV − kogumisteenuse haldusteenuse kasutusjuhend;
4. IVXV − kogumisteenuse haldusjuhend.

Eespool mainitud korraldusega kinnitatakse ka järgmised elektroonilise hääletamise süsteemi spetsifikatsioonid [24]:

1. IVXV − arhitektuur;
2. IVXV − protokollide kirjeldus;
3. IVXV − võtmerakendus;
4. IVXV − xtee teenuse kirjeldus.

Eespool mainitud juhendid ja spetsifikatsioonid avaldatakse valimiste veebilehel[8] ning varasemad juhendid kaotavad kehtivuse.

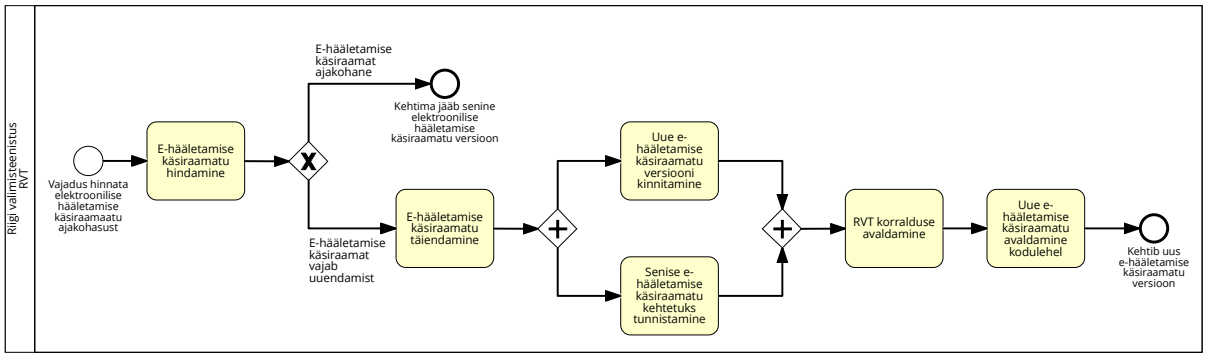
Valijarakenduse ja kontrollrakenduse operatsioonisüsteemide määramine

RKVS § 48^3 lõike 4 alusel määrab RVT oma korraldusega [25] enam levinud operatsioonisüsteemid ja nende versioonid, millele luuakse Valijarakendus; samuti määratakse mobiilseadmete operatsioonisüsteemid, millele luuakse hääle kontrollrakendus.

Elektroonilise hääletamise käsiraamatu hindamine

Elektroonilise valimise ettevalmistuse käigus hindab RVT elektroonilise hääletamise süsteemi käsiraamatu ajakohasust ja vajadusel uuendab seda. Joonisel 8 on toodud EHS-i käsiraamatu hindamise protsess.

[7] https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/314b409f-eeed-4ef5-8cf0-c862876c3857 (20.04.2024)
[8] https://www.valimised.ee/et/e-haaletamine/dokumendid (23.04.2024)



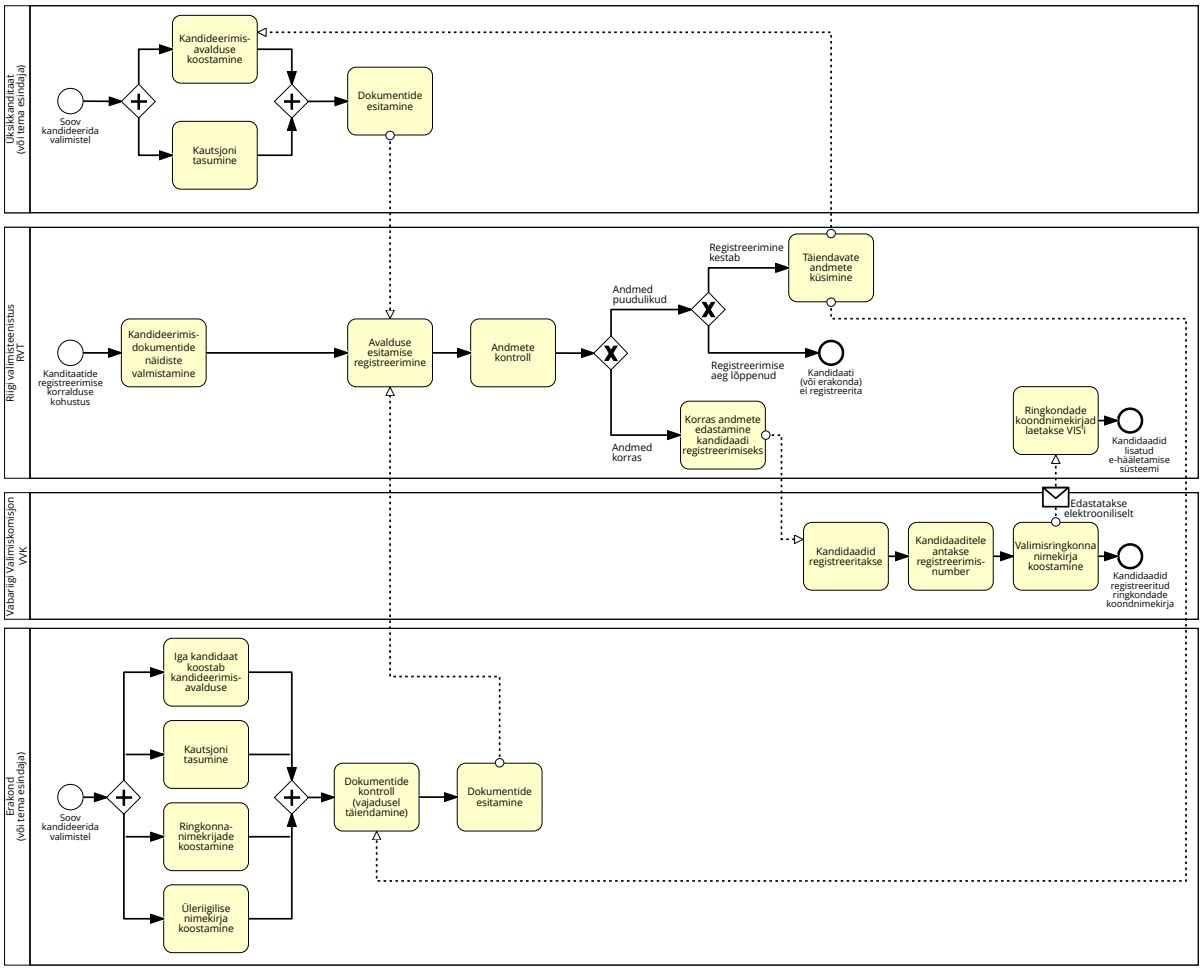
Joonis 8. Elektroonilise hääletamise süsteemi käsiraamatu hindamise protsess.

Kui hindamise tulemusel selgub, et EHS-i käsiraamat ei vaja uuendamist, siis jääb kehtima olemasolev käsiraamat. Kui hindamise tulemusel selgub, et teatud protseduurid on muutunud või tuleks neid detailsemalt lahti kirjutada, siis viiakse need muudatused juhendisse sisse. RVT korraldusega [26] kinnitatakse elektroonilise hääletamise uus versioon ja tunnistatakse kehtetuks varasem käsiraamat. Korraldus koos uue käsiraamatuga avaldatakse Riigikogu kantselei dokumendiregistris[9] ja valimiste veebilehel. Sellega on RVT- poolsed e-hääletamise ettevalmistused lõppenud.

5.4 Kandideerimisavalduse esitamine

Vastavalt RKVS § 4 p 4 on Riigikogu valimistel kandideerimisõigus igal Eesti kodanikul, kes on kandidaatide registreerimisaja viimaseks päevaks saanud 21-aastaseks. Kandideerida ei või tegevväelased ega vanglakaristust kandvad isikud. Kandideerimisõigus puudub ka teovõimetuks tunnistatud isikutel. Vastavalt RKVS § 26 ja § 27 võivad kandideerimisõiguslikud kodanikud kandideerida nii üksikkandidaadina kui ka erakonna nimekirjas. Riigi valimisteenistusel on kohustus vastavalt RKVS § $27^{1,}$ valmistada ette ja avaldada kandideerimisdokumentide näidised ning tagada võimalus nende elektrooniliseks esitamiseks. Dokumentide esitamine algab kolm kuud enne valimispäeva ja lõpeb 45. päeval kell 18.00 enne valimispäeva. Joonisel 9 on toodud kandidaatide registreerimise protsess.

[9] https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/4046ee65-26c1-498c-818e-c9b6c87a7634 (23.04.2024)



Joonis 9. Kandidaatide registreerimise protsess.

Nii üksikkandidaatide kui ka erakondade puhul on protsessi käivitajaks soov kandideerida Riigikogu valimistel, RVT puhul on selleks aga seadusest tulenev kohustus korraldada kandidaatide registreerimine [7]. Üksikkandidaadid on kohustatud täitma kandideerimis-avalduse vastavalt RVT avaldatud näidisele ning tasuma kautsjoni, mis Riigikogu valimistel vastab ühekordse kuutasu alammäärale [27]. Edasi registreerib RVT nende avalduse esitamise ja asub läbi viima avaldusel esitatud andmete kontrolli [7].

Vastavalt RKVS § 30 lg 3 peab iga valimistel kandideerida sooviv erakonna liige koostama kandideerimisavalduse, erakond tasub iga kandideeriva liikme kohta kautsjoni ning esitab tasumist tõendava maksekorralduse koopia koos kandideerimisdokumentidega. Erakond on kohustatud esitama ka kandidaatide ringkonnanimekirjad ja kandidaatide üleriigilise nimekirja [7]. Erakonna esindaja kontrollib seejärel ringkondadest saabunud dokumendid üle ja esitab need RVT-le, kes registreerib avalduse esitamise ja asub läbi viima dokumentide kontrolli [7].

Edasi kulgeb nii üksikkandidaatide kui ka erakondade jaoks protsess ühtemoodi. Kui RVT leiab esitatud dokumentides puudusi, siis nad võimaldavad lisaaega andmete parandamiseks

või puuduvate dokumentide esitamiseks. RKVS § 31 lg 6 alusel tuleb täiendavad dokumendid esitada hiljemalt 43. päeval enne valimispäeva kella 18.00. Vastasel juhul jäetakse erakond või üksikkandidaat registreerimata.

Kui kõik nõutavad dokumendid on esitatud ja need vastavad nõuetele, siis RVT edastab need VVK-le, kes vastavalt RKVS § 32 lg 1 registreerib kõik seadusest tulenevatele nõuetele vastavad isikud hiljemalt 40. päeval enne valimispäeva ning loosib kandidaatidele registreerimisnumbrid. Seejärel koostab VVK registreeritud kandidaatidest valimisringkondade nimekirjad, nimekirjad edastatakse elektrooniliselt RVT-le, kes sisestab ringkondade koondnimekirjad valimiste infosüsteemi [7]. Sellega on kandidaatide registreerimine lõppenud.

5.5 Algse valijate nimekirja koostamine

RKVS § 22 kohustab rahvastikuregistri vastutavat töötlejat, kelleks on Siseministeerium, koostama ja edastama valijate nimekirja RVT-le hiljemalt 25. päeval enne valimispäeva. Esialgne valijate nimekiri koostatakse valimispäevale eelneva 30. päeva seisuga [7]. Vähem kui 30 päeva enne valimispäeva tehtud elukoha muudatusi arvesse ei võeta. Valijate nimekirja ei kanta isikuid, kes valimispäevale eelneva kolmekümnenda päeva seisuga kannab valimispäevani vanglakaristust [7].

Vastavalt RKVS § 4 on Riigikogu valimistel hääleõigus Eesti kodanikul, kes on valimispäevaks saanud 18-aastaseks; hääleõigus puudub teovõimetuks tunnistatud isikul.

Lähtuvalt RKVS § 25 lg 1 uuendatakse valijate nimekirja, kui sellesse tuleb kanda isik, kellel on õigus hääletamisest osa võtta või tuleb sealt eemaldada isik, kellel ei ole õigus hääletamisest osa võtta. Hääletamisperioodil võib valijate nimekiri muutuda [3], Siseministeerium edastab valimisperioodil RVT-le uuendatud valijate nimekirja vähemalt kord ööpäevas [3].

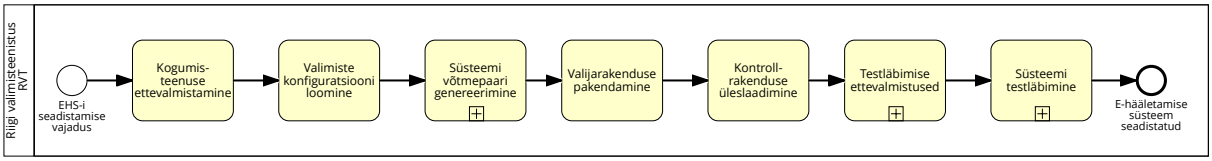
5.6 Valimiste teabelehe saatmine

Lähtudes RKVS § 21 lg 1 korraldab rahvastikuregistri vastutav töötleja, kelleks on Siseministeerium, valimiste teabelehe koostamise ja saatmise. Hiljemalt 10. päeval enne valimispäeva saadetakse valija rahvastikuregistri järgsele elukoha aadressile valimiste teabeleht. Kui valija on rahvastikuregistrile edastanud oma e-posti aadressi, saadetakse teabeleht ainult elektrooniliselt.

Valimiste infoleht on informatiivse sisuga, vastavalt RKVS § 21 lg 2 antakse sellel teave hääletamisõiguse tingimuste ja hääletamisvõimaluste kohta. Vajadusel lisatakse ka muud olulist teavet valimiste kohta.

5.7 E-hääletamise seadistamine

E-hääletamise ettevalmistusperioodi käigus on RVT-l vaja läbi viia elektroonilise hääletamise süsteemi seadistamise toimingud. Joonisel 10 on toodud e-hääletamise süsteemi seadistamise protsessid.



Joonis 10. Elektroonilise hääletamise süsteemi seadistamise protsess.

Hääletamise süsteemi seadistamine algab konfiguratsiooni ettevalmistamisega ja lõpeb süsteemi testläbimisega [26].

Kogumisteenuse ettevalmistamine

E-hääletamise käsiraamatu [26] alusel hõlmab Kogumisteenuse ettevalmistamine selle viimase tarkvaraversiooni installeerimist ja seadistamist ning süsteemi erinevate komponentide konfiguratsiooni jaoks vajalike mikroteenuste sertifikaatide hankimist.

Valimiste konfiguratsiooni loomine

E-hääletamise käsiraamat [26] sätestab, et järgmise etapina viiakse läbi valimiste konfiguratsiooni loomine, mille käigus koostatakse ja allkirjastatakse vajalikud konfiguratsioonifailid. Kogumisteenuse usaldusjuure konfiguratsioonifail saadetakse Kogujale käsurealt paigaldamiseks, ülejäänud konfiguratsioonifaile saab RVT paigaldada üle Koguja Haldusteenuse veebiliidese. Lisaks luuakse ja allkirjastatakse vajalikud konfiguratsioonifailid Korraldaja, Töötleja, Lugeja ja Audiitori funktsioonide täitmiseks; nende allkirjastaja ei ole rangelt määratud. Allkirjastaja nime näidatakse vastava rakenduse käivitamisel. Samuti luuakse Kontrollrakenduse konfiguratsioon, mis paigaldatakse veebiserverisse varasemalt arendajaga kokkulepitud asukohta.

Süsteemi võtmepaari genereerimine

Umbes kolm nädalat enne valimispäeva viib RVT läbi süsteemi võtmepaari genereerimise protseduuri, mille käigus luuakse e-hääletamisel kasutatav võtmepaar. Täpne krüptoalgoritmi spetsifikatsioon määratakse e-valimiste ettevalmistusel RVT korraldusega [17]. Võtmepaari genereerimine on auditeeritav protseduur, mille käigus võrgust lahti ühendatud arvutis, millel puuduvad sisemised salvestusseadmed, luuakse häälte salastamise võti ja häälte avamise võti [5, 26]. Võtmepaari genereerimine viiakse läbi välisel kõvakettal, kuhu on RVT poolt eelnevalt installeeritud operatsioonisüsteem ja vajalikud rakendused [26]. Kõvakettale operatsioonisüsteemi ja rakenduste paigaldamist ei auditeerita. Kõvakettast tehakse kaks koopiat, millest üks

jääb tagavaraks seifi [28]. Enne võtme genereerimise protseduuri algust on RVT poolt ette valmistatud võtmepaari loomiseks vajalik konfiguratsioon ning kirjutatud see DVD-plaadile. Joonisel 11 on toodud süsteemis võtmepaari genereerimise protsess.

RVT puhul on protsessi käivitajaks võtmepaari genereerimise vajadus, audiitoritel on kohustus protsessi jälgida. Vaatlejate osalemine on soovitatav ja sõltub huviliste olemasolust; audiitori raportist [29] järeldub, et protseduuri vaatlemise vastu on huvi olemas.

E-hääletamise süsteemi võtmepaari genereerimine koosneb kümnest etapist, mida jälgivad nii audiitorid kui ka vaatlejad [26]:

1. Konfiguratsiooni ettevalmistamine
Protseduur algab võtmepaari loomiseks vajaliku konfiguratsiooni ettevalmistamisega, mille käigus veendutakse rakenduste usaldusjuure ja võtmerakenduse konfiguratsiooni korrektsuses, digiallkirjastatakse need ning kirjutatakse koos võtmerakendusega DVD-plaadile.

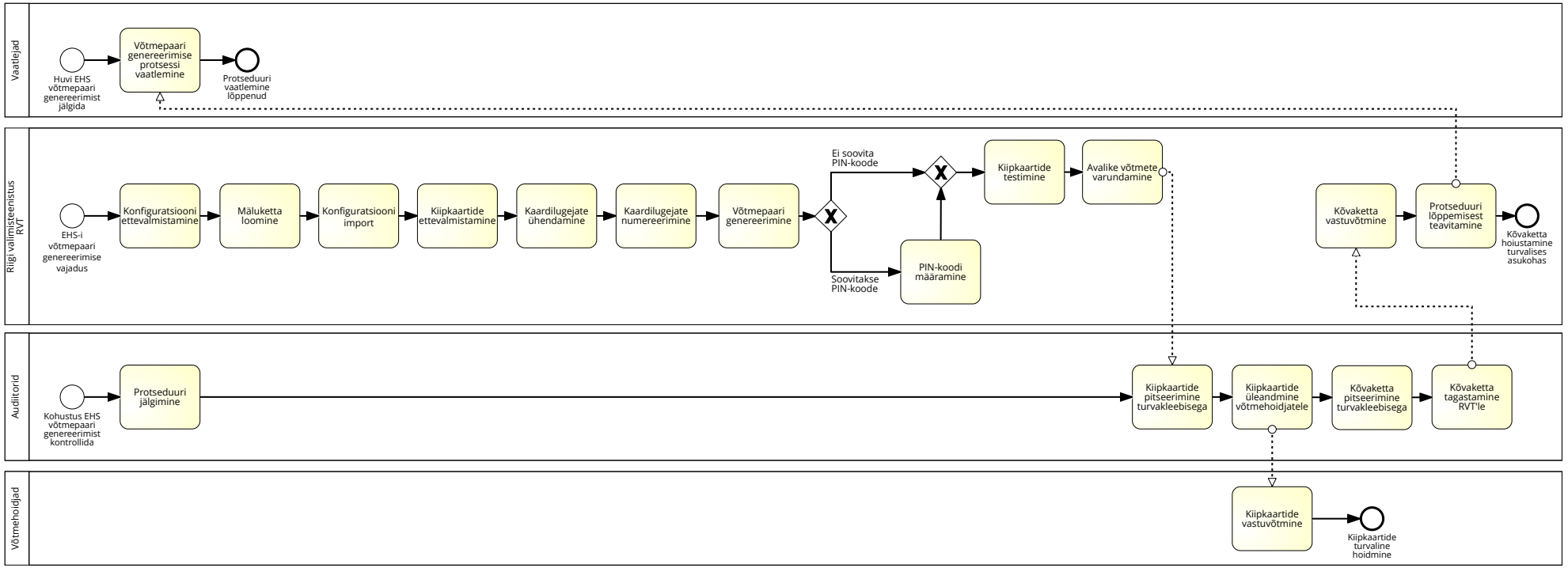
2. Mäluketta loomine
Järgnevalt luuakse, eelnevalt RVT poolt ettevalmistatud välisel kõvakettal, piisava suurusega virtuaalne mäluketas, millel hakatakse läbi viima võtme genereerimisega seotud protsesse.

3. Konfiguratsiooni import
Seejärel imporditakse DVD-plaadilt ettevalmistatud konfiguratsioon koos võtmerakendusega virtuaalsele mälukettale.

4. Kiipkaartide ettevalmistamine
Kiipkaartide ettevalmistuse käigus kasutatakse ainult ühte kaardilugejat, millega alglähtestatakse kasutusele võetavad kiipkaardid. Kiipkaartide ettevalmistamise käigus määratakse, kas kaartide kasutamise käigus küsitakse PIN-koode või mitte (RVT nõunik selgitas 16. mail 2024 toimunud e-valimiste vaatlemise koolitusel, et e-hääletamise ajaloo jooksul ei ole veel kordagi kiipkaartidel PIN-koode kasutatud, eelistatakse kasutada turvakleebiseid).

5. Kaardilugejate ühendamine
Peale kaartide alglähtestamist ühendatakse arvutiga ka ülejäänud 8 kaardilugejat.

6. Kaardilugejate numereerimine
Kaardilugejad nummerdatakse üksteise järel 0…8, kasutades ainult ühte kiipkaarti, tõstes seda ühest lugejast teise ja veendudes, mis numbriga lugejas kaart asub.



Joonis 11. Süsteemi võtmepaari genereerimise protsess.

7. Võtmepaari genereerimine

Võtmepaari genereerimiseks sisestatakse kaardilugejatesse kõik üheksa kiipkaarti. Kiipkaartidele kirjutakse peale kaardilugeja number, millesse nad sisestati. Seejärel genereeritakse häälte avamise privaatvõti ja jaotatakse see osakuteks üheksa kiipkaardi vahel. Lisaks genereeritakse ka vastavad avalikud võtmed, mis on vajalikud nii valijarakenduse kui ka kontrollrakenduse tööks ja valimistulemuste signatuuri kontrolliks.

8. PIN-koodide valik

Kui 4. punktis on PIN-koodide küsimine sisse lülitatud, siis määratakse kiipkaartidele PIN-koodid, vastasel juhul seda ei tehta (tegelikult PIN-koode ei kasutata, RVT eelistab kasutada turvakleebiseid).

9. Kiipkaartide testimine

Järgnevalt viiakse läbi proovi dekrüpteerimine mitme erineva kaardi kombinatsiooniga, veendumaks kiipkaartide korrektses töös. Dekrüpteerimiseks on vaja viit kiipkaarti ja kui eelnevalt on määratud PIN-koodid, siis küsitakse neid ka testimise käigus.

10. Avalike võtmete varundamine

Olles veendunud kiipkaartide toimivuses, kirjutatakse avalikud võtmed DVD-plaadile, turvakaalutlustel kirjutatakse kaks koopiat. Andmete loetavust kontrollitakse koheselt teises arvutis.

Sellega on võtmepaari genereerimine lõppenud, arvuti lülitatakse välja. Järgnevalt on kirjeldatud vahetult peale arvuti sulgemist läbiviidavaid tegevusi e-hääletamise käsiraamatu [26] ja võtmepaari genereerimise videosalvestise [30] põhjal.

Võtmeosakutega kiipkaardid antakse üle audiitoritele, kes pitseerib need turvakleebistega ning lisab turvakleebisele oma allkirja. Turvakleebiste paigaldamise käigus koostab audiitor akti, kuhu kirjutatakse kiipkaardi numbrid, turvakleebiste numbrid ning sulgemise kuupäev. Seejärel annab audiitor võtmeosakud üle võtmehoidjatele, fikseerides kirjalikult, kes millise numbriga kaardi sai ning võtmehoidjad kinnitavad kiipkaartide vastuvõtmist allkirjaga [29]. Seejärel e-valimiste juht pakendab Võtmerakendusega välise kõvaketta plastikkarpi ja annab selle üle audiitorile turvakleebiste paigaldamiseks, audiitor märgib kõvaketta seerianumbri ja turvakleebiste numbrid aktile. Kõvaketas tagastatakse RVT-le. Videosalvestisest [31] nähtub, et viimase tegevusena teavitab RVT esindaja vaatlejaid võtme genereerimise protseduuri lõppemisest, süsteemiketas viiakse RVT seifi ja kiipkaartide turvaline hoiustamine jääb võtmehoidjate vastutada.

Peale 2024. aasta EP valimiste võtmegenereerimise protseduuri lõppu lasi audiitor RVT esindajal võtmegenereerimiseks kasutataval arvutil eemaldada korpuse paneelid, mis võimaldas audiitoril visuaalselt veenduda, et arvutil puuduvad sisemised salvestusseadmed. Eelnevate e-valimiste audiitorite raportitest ei selgu, et sellist kontrolli oleks varasematel kordadel läbi viidud.

Valijarakenduse pakendamine

Vastavalt tehnilistele juhenditele [26, 32] pakendab RVT Valijarakenduse. Eelnevalt vaadatakse üle kõik rakenduse tekstid ja vajadusel uuendatakse neid ning seejärel rakendatakse antud konfiguratsioon kõikide operatsioonisüsteemide Valijarakendustele. Valijarakenduse pakendamisel lisatakse sellele vajalikud sertifikaadid, valimisringkondade ja valimisjaoskondade nimekiri ning häälte salastamiseks avalik võti, mis laetakse võtmepaari genereerimise käigus loodud DVD-plaadilt. Windows operatsioonisüsteemi rakenduse allkirjastab kas RIA või arendaja, MacOS rakendus saadetakse pakendamiseks ja allkirjastamiseks arendajale ning Linux Valijarakendust ei allkirjastata.

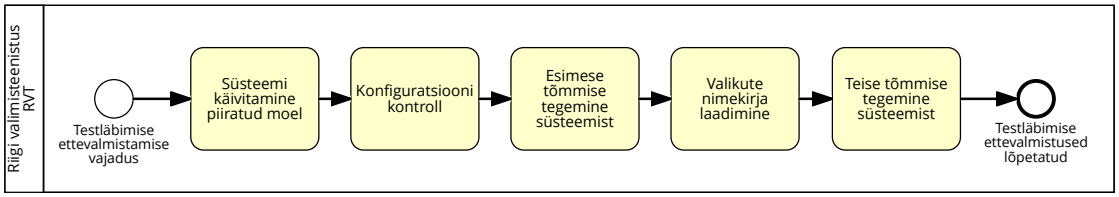
Kontrollrakenduse üleslaadimine

RVT-l on vaja Kontrollrakendus laadida Google'i ja Apple'i rakendusepoodidesse, et testhääletajatel oleks võimalik süsteemi testläbimise käigus seda kontrollida. Google'i tehnilises juhendis[10] on toodud, et rakenduse heakskiitmine ja avaldamine nende rakendusepoes võib võtta kuni seitse päeva ja teatud juhtudel isegi kauem. Apple'i puhul läheb rakenduse läbivaatamise ja avaldamise protsess kiiremini, nende tehnilises juhendis[11] väidetakse, et 90% rakendustest vaadatakse üle 24 tunni jooksul, põhjendatud juhtudel võib see võtta kauem aega. Vältimaks olukorda, kus Kontrollrakenduse jõudmine rakendusepoodidesse võtab liialt aega, on selle varasem versioon juba eelnevalt üles laetud ja enne valimisi uuendatakse rakendust. Uuenduse läbivaatamine ja heakskiitmine võtab rakendusepoodidel aega mõne tunni[12]. Kontrollrakenduse üleslaadimise võib RVT delegeerida ka rakenduse arendajale[13,14].

[10] https://support.google.com/googleplay/android-developer/answer/9859751?hl=en (25.04.2024)
[11] https://developer.apple.com/distribute/app-review/ (25.04.2024)
[12] https://www.quora.com/How-long-does-it-usually-take-for-new-updates-to-appear-in-the-App-Store-and-the-Google-Play-Store (25.04.2024)
[13] https://play.google.com/store/apps/details?id=ee.ivxv.ivotingverification (19.06.2024)
[14] https://apps.apple.com/us/app/eh-kontrollrakendus/id1265172086 (19.06.2024)

Testläbimise ettevalmistused

E-hääletamise käsiraamatust [26] selgub, et testläbimise ettevalmistamisel käivitab RVT elektroonilise hääletamise süsteemi piiratud moel. Testläbimise ettevalmistamise protsess on toodud joonisel 12.



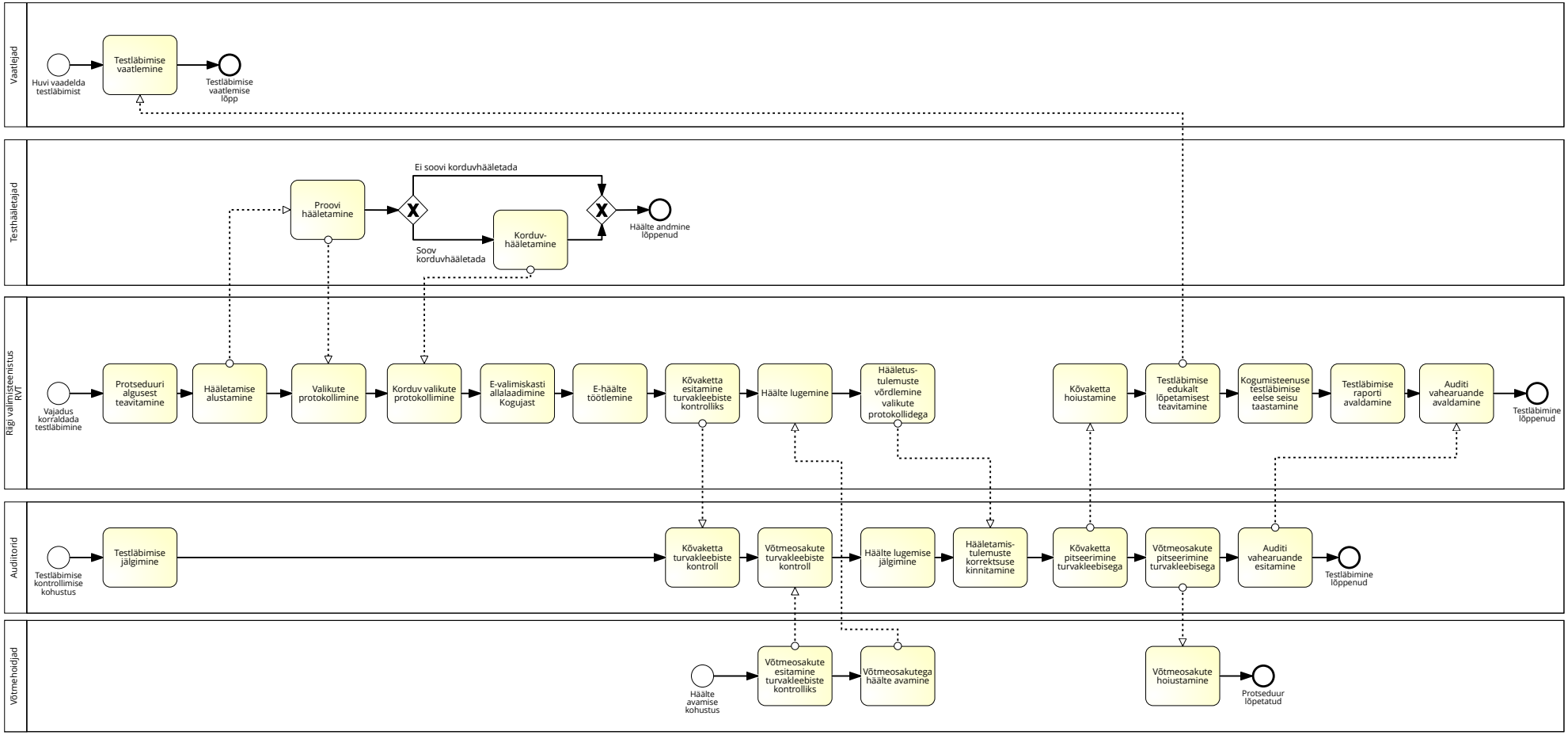
Joonis 12. Testläbimise ettevalmistused.

Testhääletamisel saab hääletada ainult RVT ametiruumides ja määrates hääletamise algus- ja lõpuajaks testläbimise aja. Seejärel viib RVT läbi konfiguratsiooni kontrolli ja teeb esimese tõmmise süsteemist ning laeb süsteemi valikute ehk kandidaatide nimekirja. Peale kandidaatide nimekirja sisestamist tehakse teine tõmmis süsteemist. Tõmmiste tegemine on vajalik, kuna testläbimise lõpus tuleb taastada Kogumisteenuse testläbimise eelne seis. Kui peale testläbimist kandidaatide nimekiri muutub, taastatakse Kogumisteenuse testläbimise eelne seisund 1. tõmmisest ning laetakse uus kandidaatide nimekiri. Kui kandidaatide hulgas muudatusi ei toimu, taastatakse Kogumisteenuse testläbimise eelne seisund 2. tõmmisest.

Süsteemi testläbimine

E-hääletamise süsteemi testläbimine viiakse reeglina läbi võtmepaari genereerimise järgsel päeval ja see on auditeeritav protseduur, vaatlejate osalemine on soovitatav [26].

RVT puhul on protsessi käivitajaks vajadus korraldada testläbimine ja veenduda e-hääletamise süsteemi tõrgeteta töös. Audiitoritel on kohustus veenduda protseduuri läbiviimise korrektsuses. Testläbimise protseduur on toodud joonisel 13.



Joonis 13. E-hääletamise süsteemi testläbimise protsess.

E-hääletamise testimise raportist [31] ja audiitori raportist [28] järeldub, et proovihääletamine viiakse läbi erinevatel operatsioonisüsteemidel ning kasutades valija isiku tuvastamiseks nii Mobiil-ID kui ka ID-kaarti. Hääletaja valik protokollitakse ja hääle jõudmist Kogumisteenusesse kontrollib hääle andja Kontrollrakendusega. Mõned testhääletajad hääletavad korduvalt, ka korduv valik protokollitakse ja audiitor kontrollib valikuid. Kui testhääletamine on lõppenud, viiakse läbi häälte töötlusetapid – krüpteeritud häälte digitaalallkirjade kontroll, korduvate häälte tühistamine, häälte anonüümine ja miksimine (testläbimise käigus häälte ajatempleid ei kontrollita). Häälte töötlusetappide detailsem kirjeldus on toodud töö 7. peatükis. Peale häälte töötlemist salvestatakse tulemused DVD-plaadile.

Testläbimise salvestisest [31] nähtub, et järgnevalt esitab RVT esindaja audiitorile kontrolliks ja avamiseks pitseeritud süsteemiketta ning viis võtmehoidjat esitavad audiitorile oma võtmeosakud turvakleebiste kontrolliks ja avamiseks. Seejärel käivitatakse süsteemikettalt võtmerakendus ning alustatakse võtmeosakutega häälte avamist ja lugemist. Häälte lugemise detailsem kirjeldus on toodud käesoleva töö 7. peatükis. Seejärel võrdleb RVT esindaja hääletustulemusi valikute protokolliga, veendumaks, et hääli said samad kandidaadid, kelle poolt hääletati. Audiitor kinnitab hääletustulemuse korrektsuse. Edasi pitseerib audiitor kasutatud süsteemiketta ja võtmeosakud turvakleebistega, protokollides turvakleebiste numbrid ning ta tagastab need võtmehoidjatele, süsteemiketta RVT esindajale. Lõpetuseks teavitab RVT esindaja vaatlejaid testläbimise edukast lõpetamist.

RVT kanda jääb veel Kogumisteenuse testläbimise eelse seisu taastamine [25] ja testläbimise raporti [31] avaldamine valimiste kodulehel. Ka audiitor esitab RVT-le oma vaheraporti [28], mis avaldatakse valimiste kodulehel. Sellega on testläbimine ka RVT ja audiitorite jaoks lõppenud. Testläbimise lõppemisega saab läbi ka e-hääletamise seadistamise protsess.

5.8 Valimiste lähtekoodi avaldamine GitHub'i koodihoidlas

Vastavalt VVK otsusele [16] on valimiste korraldajal kohustus avaldada elektroonilise hääletamise kesksüsteemi, kontrollrakenduse ja auditirakenduse lähtekood; valijarakenduse lähtekoodi turvakaalutlustel ei avaldata. E-hääletamise lähtekood avaldatakse GitHub'i koodihoidlas[15], RVT on lähtekoodi ja selle dokumentatsiooni üleslaadimise delegeerinud arendajale. Turvakaalutlustel avalikustatakse lähtekood võimalikul hilja, et ründajatel ei oleks

[15] https://github.com/valimised (25.04.2024)

palju aega võimalike ründevektorite leidmiseks. Teisalt pärsib lähtekoodi hiline avaldamine turvaekspertide ja teiste huviliste võimalust lähtekoodi enne valimisi testida.

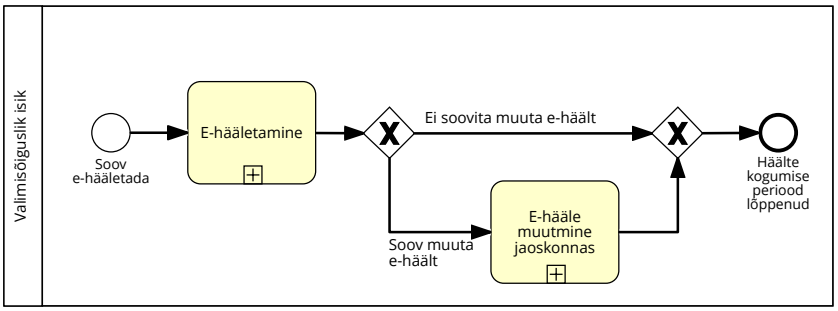
5.9 Valijarakenduse avalikustamine

E-hääletuse ettevalmistuse viimaseks etapiks on Valijarakenduse avaldamine. Vastavalt VVK otsusele [16] avaldab RVT Valijarakenduse valimiste veebilehel, vahetult enne e-hääletamise algust, esmaspäeva hommikul. Valijarakendus on loodud nii Windows'i, Linux'i kui ka MacOS'i operatsioonisüsteemidele ja koos rakendustega avaldatakse ka juhised[16], kuidas kontrollida rakenduse autentsust. Lisaks avaldatakse viited, kuidas alla laadida Kontrollrakendust. Sellega on elektroonilise hääletamise ettevalmistavad protsessid lõppenud.

[16] https://www.valimised.ee/et/e-haaletamine/e-haaletamise-juhised/valijarakendused-ja-usaldusvaarsuse-kontrollimine (25.04.2024)

6. Elektroonilise hääletamise ja häälte kogumise ajal toimuvad protsessid

Võrreldes e-hääletamise ettevalmistusperioodiga, mis kestab pea neli kuud, kestab hääletamisperiood ainult nädala. Elektrooniline hääletamine algab esmaspäeval kell 9.00 ja lõpeb sama nädala laupäeval kell 20.00. Hääletada saab ööpäev läbi, paralleelselt e-hääletamisega tegeleb Korraldaja häälte kogumisega. Pühapäevaks ehk valimispäevaks on e-hääletamine lõppenud, kuid valijal on võimalik oma antud e-häält jaoskonnas veel muuta.



Joonis 14. E-hääletamise ja häälte kogumise protsessid.

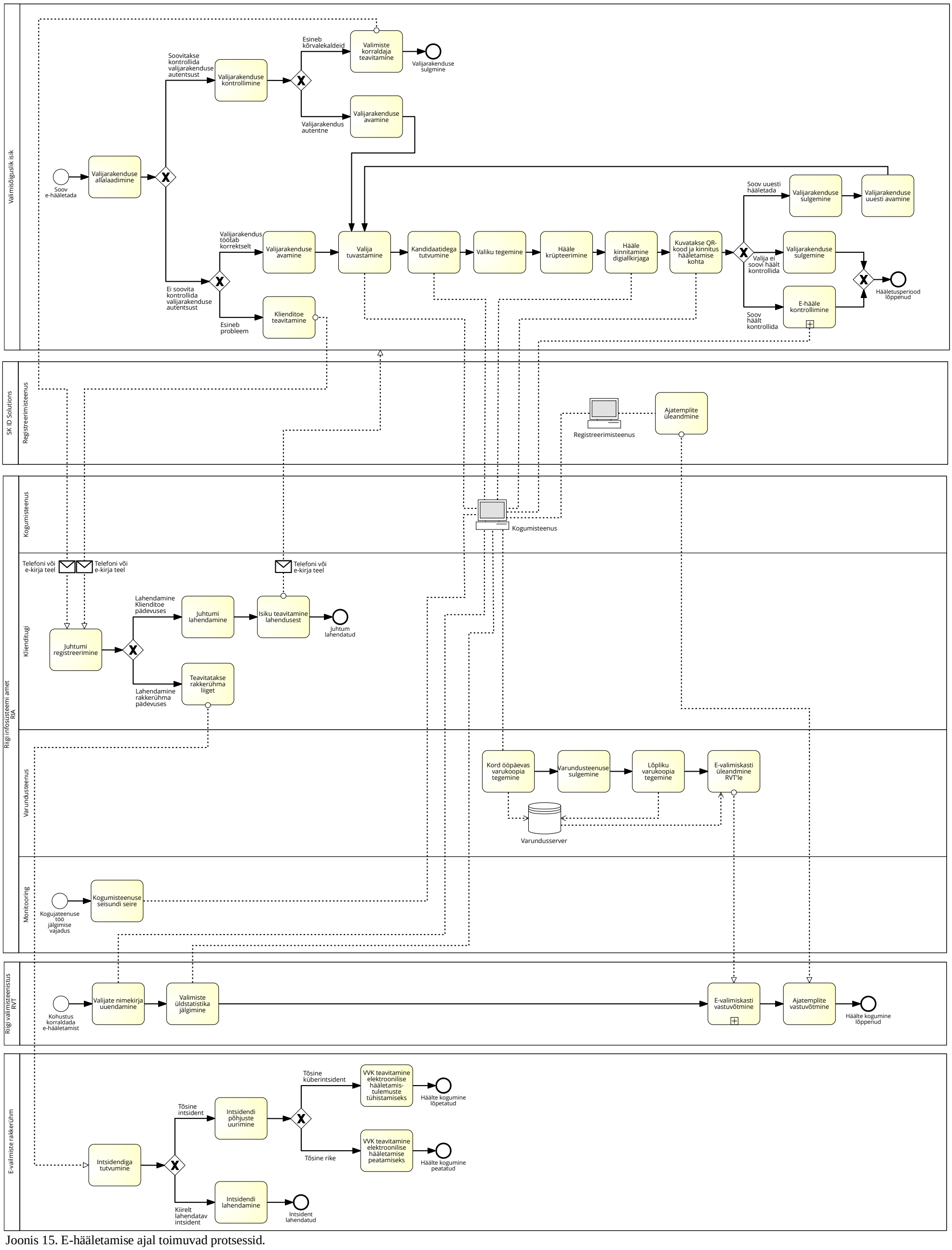
Joonisel 14 on toodud e-hääletamise protsessid, e-hääle muutmine ei ole kohustuslik, see on Korraldaja poolt loodud võimalus, kui valija tunneb, et ta ei olnud oma senise valiku tegemises vaba või otsustas oma valikut muuta.

6.1 E-hääletamine

Valija jaoks algab e-hääletamine Valijarakenduse allalaadimisega valimiste kodulehelt[17], seal on koos rakendusega toodud ka juhendmaterjal, mis kirjeldab, kuidas kontrollida Valijarakenduse autentsust. Valija jaoks on rakenduse autentsuse kontrollimine soovitatav ja kui esineb kõrvalekaldeid, siis tuleb sellest teavitada e-hääletamise klienditeenindust. Kui valijal esineb tehnilisi probleeme Valijarakenduse kasutamisel, siis saab ta pöörduda ööpäev läbi töötava klienditeeninduse poole kas telefoni või e-posti teel[18].

Elektroonilise hääletamise protsess ja sellega seotud osapooled on toodud joonisel 15.

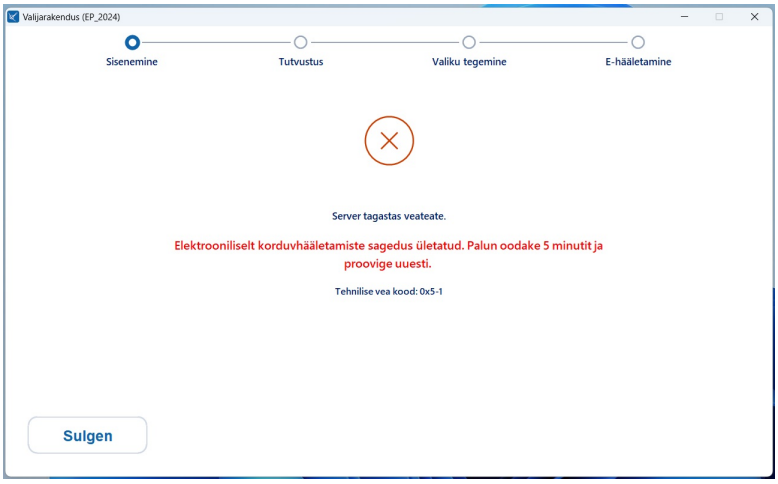
[17] https://www.valimised.ee/ (27.04.2024)
[18] https://www.valimised.ee/et/e-haaletamine/e-haaletamise-juhised/paigaldusjuhis-windowsi-kasutajale (27.04.2024)



Joonis 15. E-hääletamise ajal toimuvad protsessid.

Vastavalt e-hääletamise üldraamistikule [33] tuleb valijal rakendus käivitada ja end tuvastada kas ID-kaardi või Mobiil-ID vahendusel. Valijarakendus pöördub hääletaja tuvastamiseks Kogumisteenuse poole, mis kasutab hääletaja isiku tuvastamiseks välist Tuvastusteenust. Samuti kontrollib Kogumisteenus, ega valija ei ole juba e-häält andnud; kui on, kuvab sellekohase teatise ning kui valija soovib, saab ta oma valikut üle hääletades muuta. Kogumisteenus tuvastab valijate nimekirjas hääletaja hääleõiguse ning tema elukohaga seotud ringkonna. Juhul, kui isikul puudub hääleõigus, kuvatakse sellekohane veateade. Seejärel kuvatakse hääletajale tema ringkonna kandidaatide nimekiri, millega ta saab tutvuda ja endale sobiva valiku teha.

E-hääletamise üldraamistikus [3] on toodud, et peale kandidaatide seast valiku tegemist Valijarakendus krüpteerib hääle koos juhuarvu ja hääle salastamise võtmega, misjärel hääletaja digitaalallkirjastab tehtud valiku. Seejärel liigub allkirjastatud hääl Kogumisteenusesse, mis kontrollib hääletaja olemasolu valijate nimekirjas, küsib digiallkirjale kehtivuskinnituse ja ajatempli ning registreerib hääle välises Registreerimisteenuses. Kogumisteenus kuvab Valijarakenduse kaudu teate hääle edukast vastuvõtmisest ning veel kuvatakse Valijarakenduses QR-kood, mis sisaldab hääle krüpteerimisel kasutatud juhuarvu ning Kogumisteenuse poolt genereeritud ühekordset hääleidentifikaatorit. Seejärel on hääletajal olemas valikuvõimalus. Kui ta ei soovi häält kontrollida, siis ta sulgeb Valijarakenduse ja sellega on tema jaoks hääletamine lõppenud. Kui hääletaja soovib uuesti hääletada, siis tuleb Valijarakendus sulgeda ja uuesti avada ning kogu protsess algab otsast peale, hääletada on lubatud piiramatu arv kordi, kuni hääletamisperioodi lõpuni. Kuid peale 15. korduvhäält rakendub e-hääletamise süsteemi kaitsemehhanism, misjärel Valijarakendus kuvab veateate. Veateade on toodud joonisel 16.

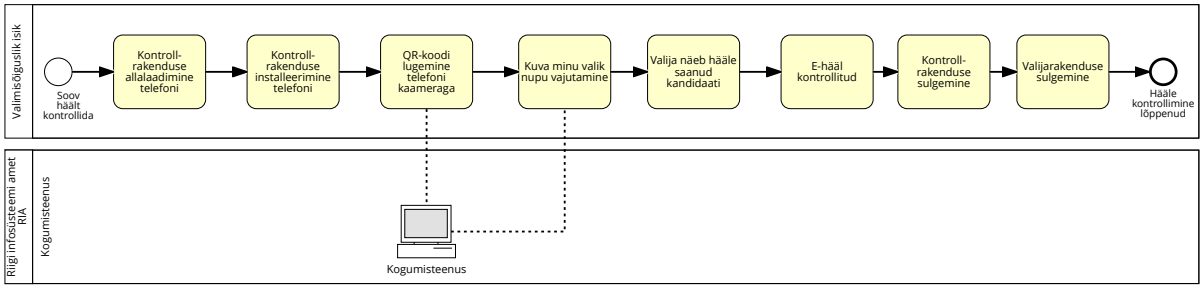


Joonis 16. Korduvhääletamise piirang.

Edaspidi saab valija oma e-häält muuta üks kord iga viie minuti järel kuni hääletamise lõpuni.

E-hääle kontrollimine

Kui hääletaja otsustab e-hääle kontrollimise kasuks, siis on selleks vaja internetiühendusega nutitelefoni, kuhu tuleb laadida ja installeerida Kontrollrakendus [33]. E-hääle kontrollimise protsess on toodud joonisel 17.



Joonis 17. E-hääle kontrollimise protsess.

E-hääletamise üldraamistikus [3] on hääle kohalejõudmise kontrolli protsessi kirjeldatud järgmiselt. Pärast rakenduse installeerimist tuleb see käivitada ja telefoni kaameraga skaneerida Valijarakenduse poolt kuvatav QR-kood. Seejärel tuleb vajutada „Kuva minu valik“ nuppu, peale mida teeb Kontrollrakendus päringu kogumisteenusele hääletaja antud e-hääle kohta, kasutades hääle tuvastamiseks QR-koodis sisalduvat ühekordset hääleidentifikaatorit. Kogumisteenus tagastab Kontrollrakendusele krüpteeritud ja signeeritud hääle, pärast mida Kontrollrakendus kontrollib hääle digitaalset allkirja ja ajatemplit. Seejärel arvutab Kontrollrakendus kandidaatide nimekirjast hääletaja poolt tehtud valiku, kasutades QR-koodis sisalduvat juhuarvu ja teades hääle salastamise võtit. Lõpuks kuvatakse hääletaja tehtud valik Kontrollrakenduse ekraanil, seejärel võib sulgeda nii Kontrollrakenduse kui ka Valijarakenduse ning sellega on hääle kohalejõudmise kontrollimine lõpetatud.

Hääletajal peab hääle kontrollimisel meeles pidama, et vastavalt VVK otsusele [16] sai 2023. aasta Riigikogu valimistel häält kontrollida ainult 30 minuti jooksul peale hääle andmist ning maksimaalselt kolm korda. Alates 2024. aasta EP valimistest lühendati hääle kontrollimise aega 15 minutini[19].

Klienditugi ja intsidentide lahendamine

Vastavalt e-hääletamise süsteemi infoturvapoliitikale [5, 23] pakub RIA terve valimiste perioodi kestel hääletajatele Klienditoe teenust, mille pädevuses on hääletajate teabepäringute, individuaalsete probleemide ning intsidentide lahendamine. Lisaks monitoorib RIA ööpäevaringselt Kogumisteenuse seisundit, sh. küberruumis toimuvat. Kõik Kogumisteenuse sündmused logitakse ja neid logisid saab kasutada juhtumi põhjuste tuvastamisel. Klienditugi

[19]https://www.valimised.ee/et/e-haaletamine/e-haaletamise-juhised/e-haale-kontrollimine (10.06.2024)

registreerib kõik laekunud juhtumid ja ka nende lahendamise käigu, kui lahendamine kuulub Klienditoe pädevusse. Tõsistest intsidentidest teavitatakse viivitamatult elektroonilise hääletamise rakkerühma liiget, kelle pädevusse vastava intsidendi lahendamine kuulub. Rakkerühma liige, kes vastutab intsidendi lahendamise eest, on kohustatud dokumenteerima kõik lahendamisega seotud otsused ja protsessid nii, et neid oleks võimalik tagantjärele tõendada. Kui intsidenti ei ole võimalik kohe lahendada, kuna tegemist on e-hääletamise süsteemi tõsise rikke või suure küberründega, siis rakkerühmal on õigus teha VVK-le ettepanek elektroonilise hääletamise peatamiseks või lõpetamiseks. VVK teavitab koheselt hääletajaid, milliseid hääletusviise on võimalik jätkuvalt kasutada. Tõsiseid rikkeid, mille korral oleks olnud VVK sunnitud e-hääletamist peatama või lõpetama, ei ole viimase 19 aasta jooksul esinenud.

Varundusteenus

RIA hallata on ka Varundusteenuse pakkumine häälte kogumise perioodiks. Vastavalt Riigi valimisteenistuse infoturvapoliitikale [23] on RIA-l kohustus teha e-valimiskastist varukoopiad vähemalt üks kord ööpäevas kogu hääletamisperioodi vältel. Viimane varukoopia tehakse vahetult peale häälte kogumise perioodi lõppu, laupäeva õhtul peale 20.15[20]. Varukoopiaid hoitakse originaalidest füüsiliselt eraldi, tagades nende säilimise originaali hävimise korral.

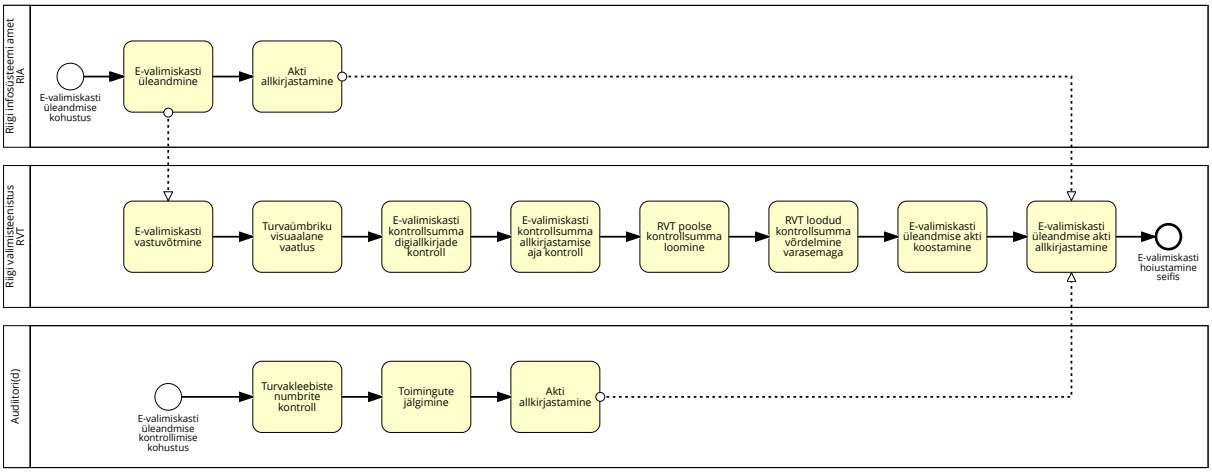
Riigi valimisteenistuse ülesanded hääletamise perioodil

RVT uuendab valijate nimekirja vähemalt kord ööpäevas vastavalt rahvastikuregistri vastutavalt töötlejalt saadud andmetele [3]. Näiteks üheks sagedasemaks põhjuseks valijate nimekirja uuendamiseks on isikute valimisikka jõudmine keset valimisperioodi. Teiseks sagedaseks põhjuseks aga inimese surm, misjärel lahkunu eemaldatakse valijate nimekirjast. Samuti jälgib RVT valimiste üldstatistikat valimiste kodulehel, mida Kogumisteenuse liides uuendab iga 15 minuti tagant. RVT jaoks lõpeb häälte kogumise periood e-valimiskasti vastuvõtmisega RIA-lt, kes komplekteerib e-valimiskasti kogutud hääled ning allkirjastab e-valimiskasti kontrollsumma [3]. Samuti annab Registreerimisteenus RVT-le üle ajatemplid, mis on nende poolt eelnevalt digitaalselt allkirjastatud [33].

[20] Kui valija on oma isiku enne kella 20.00 Valijarakenduses tuvastanud ja talle kuvatakse kandidaatide nimekiri, siis on valijal aega oma valiku tegemise lõpetamiseks kuni 20.15-ni, mil Kogumisteenus suletakse.

E-valimiskasti vastuvõtmine

E-valimiskasti vastuvõtmine on auditeeritav protseduur ning see leiab aset viimase e-hääletamise päeva ehk laupäeva hilisõhtul RVT ametiruumides [34]. E-valimiskasti vastuvõtmise protsess on toodud joonisel 18.



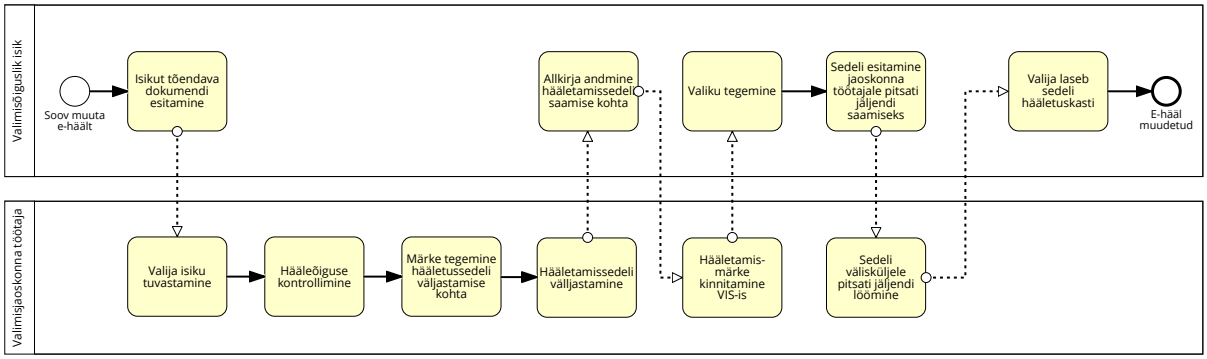
Joonis 18. E-valimiskasti vastuvõtmise protsess.

Vastavalt audiitori 2023. aasta raportis [34] toodud informatsioonile, annab RIA RVT-le üle turvaümbrikus e-valimiskasti, mis sisaldab kahte DVD-plaati. Esimese asjana viib RVT esindaja läbi turvaümbriku visuaalse vaatluse ja veendub, et pakend on rikkumata. Audiitor kontrollib turvaümbriku numbreid ning need kantakse ka vastavale aktile.

Seejärel kontrollib RVT esindaja üle e-valimiskasti kontrollsumma digiallkirjad ja allkirjastamise kellaaja ning need kantakse e-valimiskasti üleandmise-vastuvõtu aktile [34]. Seejärel genereerib RVT esindaja e-valimiskastile omapoolse kontrollsumma ja võrdleb seda RIA poolt allkirjastatud kontrollsummaga [3]. Kõiki toiminguid jälgib audiitor. Viimasena täidetakse e-valimistkasti üleandmise-vastuvõtmise akti vajalikud lahtrid ja see allkirjastatakse kõigi osapoolte poolt [34]. Sellega on ka RVT jaoks e-häälte kogumise periood lõppenud.

6.2 E-hääle muutmine jaoskonnas

Kui valija soovib, siis on tal võimalus oma antud e-häält muuta jaoskonnas, sellisel juhul tema e-hääl tühistatakse ja kehtima jääb jaoskonnas antud paberhääl. Valimisjaoskonnas saab e-häält muuta nii eelhääletamise perioodil kui ka valimispäeval kuni kella 20.00-ni õhtul [7]. Valija peab silmas pidama, et esmaspäevast kuni neljapäevani, eelhääletuse perioodil, saab oma e-häält muuta kõikides valimisjaoskondades; reedest kuni pühapäevani tuleb e-hääle muutmiseks siirduda oma elukohajärgse valimisringkonna valimisjaoskonda [7]. E-hääle muutmise protsess elukohajärgse valimisringkonna jaoskonnas on toodud joonisel 19.



Joonis 19. E-hääle muutmise protsess elukohajärgse valimisringkonna jaoskonnas.

Lähtudes RKVS-ist [7] ja hääletamise korraldamise juhendist [35], tuleb häält muuta soovival valijal siirduda valimisjaoskonda, esitada isikut tõendav dokument, mille alusel jaoskonnakomisjoni liige tuvastab hääletaja isiku ja hääletusõiguse olemasolu ning teeb märke hääletussedeli väljastamise kohta elektroonilisse valijate nimekirja. Valijate nimekiri kuvab valija järjekorranumbri, mille jaoskonna töötaja kirjutab hääletamissedeli saamise lehele ning seejärel väljastab valijale hääletussedeli (allkirjalehele on lubatud kirjutada valija järjekorranumbri asemel ka valija isikukood). Seejärel annab valija hääletamissedeli saamise lehele allkirja tema järjekorranumbri taga olevasse lahtrisse, peale mida jaoskonna töötaja kinnitab hääletamismärke VIS-i. Edasi suundub valija valimiskabiini, kus teeb oma valiku, murrab sedeli pooleks ning esitab selle jaoskonna töötajale pitsatijäljendi peale löömiseks. Lõpuks laseb valija oma sedeli isiklikult hääletuskasti ja sellega on e-hääle muutmine lõppenud.

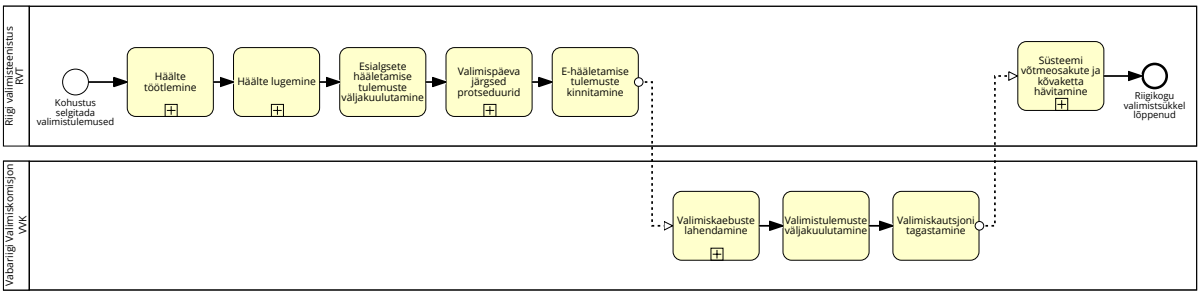
Kui valija soovib eelhääletuse esimestel päevadel e-häält muuta väljaspool elukohajärgset valimisjaoskonda, siis hääle muutmise protsess on analoogne eeltooduga, kuid koos valimissedeliga antakse valijale üle ka kaks ümbrikku, millest välimisele on VIS-st prinditud valija andmed [35]. Valija pakendab oma hääletussedeli pärast valiku tegemist topeltümbrikutesse ja laseb selle valimiskasti (hääletussedelile teist pitsatijäljendit ei lööda) [35].

Pühapäeva õhtul, kell 20.00 suletakse valimisjaoskonnad ning sellega on hääletamise ja häälte kogumise periood lõppenud[21] ning algavad hääletamisperioodi-järgsed protseduurid.

[21] Valimisjaoskonnas olevad valijad saavad hääletada ka pärast 20.00, kui nad on sisenenud sinna enne jaoskonna sulgemist. Jaoskonnakomisjon lubab valijatel hääle andmise lõpetada.

7. Häälte kogumise järgsed protsessid

Häälte kogumise järgsed protsessid hõlmavad endas häälte töötlemist ja lugemist ning esialgsete hääletamise tulemuste väljakuulutamist [26]. Valimisjärgsel päeval viiakse teist-kordselt läbi häälte töötlemine ja lugemine, misjärel kinnitatakse e-hääletamise tulemused [26]. Häälte kogumise järgsed protsessid on toodud joonisel 20.

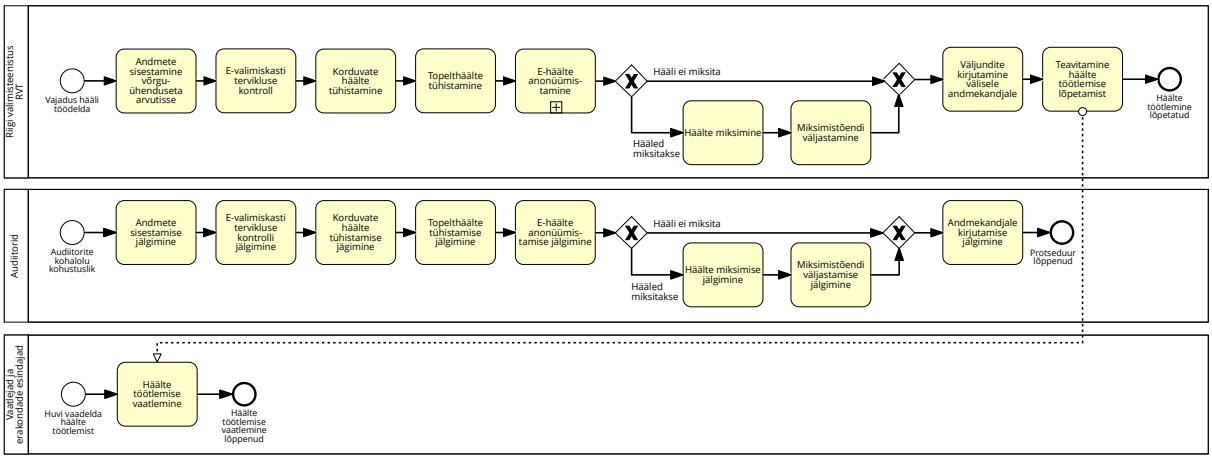


Joonis 20. Häälte kogumise järgsed protsessid.

Seejärel tegeleb VVK valimiskaebuste lahendamisega ja kui huvitatud isik ei ole nõus VVK otsusega, saab seda edasi kaevata Riigikohtusse [7]. Kui kõik valimiskaebused on oma lahendid leidnud, siis kuulutatakse välja lõplikud valimistulemused ning RKVS-is nõutud häältesaagi saanud kandidaadid saavad makstud valimiskautsjoni tagasi [7]. E-hääletamise viimaseks toiminguks on süsteemiketta ja häälte avamise võtmeosakute avalik hävitamine [26]. Sellega saab üks Riigikogu valimiste periood läbi.

7.1 Häälte töötlemine

Valimispäeva õhtul kella 19.00 paiku alustab RVT häälte töötlemise protseduuriga[22], kus osalevad audiitorid, registreeritud vaatlejad, ajakirjanikud, erakondade esindajad. E-häälte töötlemise protsess on näidatud joonisel 21.



Joonis 21. Häälte töötlemise protsess.

[22] https://www.valimised.ee/index.php/et/euroopa-parlament-2024/elektroonilise-haaletamise-vaatlemine (26.04.2024)

Esimese sammuna sisestatakse vajalikud andmed RVT võrguühenduseta arvutisse ning kontrollitakse, et kasutatav e-valimiskast koos selle kontrollsummaga vastaks eelmisel päeval RIA poolt üle antud e-valimiskasti ja selle kontrollsummale [34].

E-valimiskasti tervikluse kontroll

E-hääletamise üldraamistiku [3] alusel on töötlemise järgmiseks sammuks e-valimiskasti tervikluse kontroll, mille käigus RVT kontrollib iga hääle digitaalallkirja ja ajatemplit ning võrdleb ajatemplit Registreerimisteenuselt saadud ajamärgendiga. Töötlemisrakendus kontrollib üle ka hääle andnud isiku hääleõiguse olemasolu valijate nimekirjas. E-valimiskasti tervikluse kontrolli tulemusena on valimiskastis ainult need hääled, millel leiti vaste Registreerimisteenuse ajatemplite hulgast ning mille on andnud hääleõiguslikud isikud. Kui mõni antud e-hääl neile kriteeriumitele ei vasta, siis see tühistatakse. Peale tervikluse kontrolli on lubatud häältelt eemaldada digitaalallkirjad, säilitades samas seose krüpteeritud hääle ja selle andnud isiku ning hääletamise aja vahel.

Korduvate häälte tühistamine

Üldraamistik [3] sätestab, et järgnevalt tuleb läbi viia korduvate e-häälte tühistamine, mille käigus jäetakse alles vaid viimasena antud e-hääl. Käesoleva etapi lõpus võib e-häälelt eemaldada hääletamise aja, samas tuleb e-hääle juures säilitada isikuandmed. Väljundkataloogi tekkinud korduvhäältest puhastatud e-valimiskasti kontrollsumma allkirjastatakse.

Topelthäälte tühistamine

Peale korduvate e-häälte tühistamist koostatakse e-hääletajate nimekiri, mis laetakse VIS-i topelthääletanud isikute tuvastamiseks. Tuvastatud topelthäältest koostatakse tühistusnimekiri. Kuna jaoskonnas on võimalik e-häält muuta kuni valimispäeva õhtul kella 20.00-ni[23] [7], siis tuleb tühistusnimekirja saamiseks oodata, kuni kõik jaoskonnad on hääletanud isikud kandnud VIS-i. Tühistusnimekirja väljastab ja allkirjastab VIS-i operaator [26].

E-valimiste üldraamistik [3] sätestab, et nende isikute hääled, kelle nimi sisaldub tühistus-nimekirjas, tühistatakse. Lõpuks jäävad e-valimiskasti alles vaid unikaalsed isikustatud e-hääled.

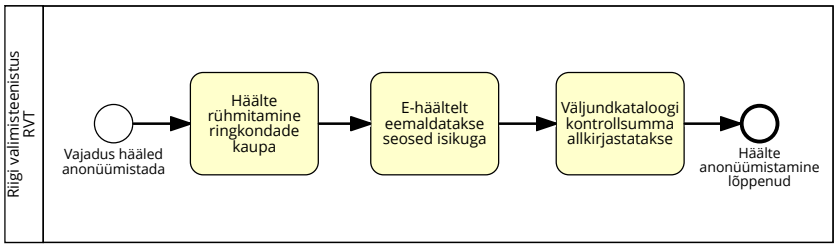
IVXV − seadistuste koostamise juhendis [4] on toodud, et valimisjaoskonna info põhjal on võimalik ka tühistatud e-hääli taastada, selleks kasutatakse ennistusnimekirja. Antud funktsionaalsust kasutatakse näiteks juhul, kui mõnes valimisjaoskonnas avastatakse, et mõni

[23] Valimisjaoskonnas olevad valijad saavad hääletada ka pärast 20.00, kui nad on sisenenud sinna enne jaoskonna sulgemist. Jaoskonnakomisjon lubab valijatel hääle andmise lõpetada ning seetõttu võib tühistusnimekirja loomine venida.

isik on ekslikult märgitud jaoskonnas hääle andnud valijate hulka, kuid tegelikult ta pole jaoskonnas hääletamas käinud. Sellisel juhul saab sellise isiku varasemalt tühistatud e-hääle lisada tagasi e-valimiskasti.

E-häälte anonüümistamine

E-hääletamise käsiraamat [26] määrab, et enne e-häälte kokku lugemist tuleb need anonüümistada. Häälte anonüümistamise protsess on toodud joonisel 22.



Joonis 22. E-häälte anonüümistamise protsess.

Esmalt tuleb e-hääled rühmitada valimisringkondade kaupa, seejärel eemaldatakse häältelt digiallkirjad [3]. Seejärel väljundkataloogi tekkinud anonüümistatud e-valimiskasti kontrollsumma allkirjastatakse RVT esindaja poolt ning väljundkataloogid kirjutatakse DVD-plaadile [26].

Häälte miksimine

Järgnevalt on RVT otsustada, kas valimispäeva õhtul hääled miksitakse või mitte. Vastavalt e-hääletamise käsiraamatule, on hääli lubatud kokku lugeda kahel viisil [26]:

1. Kui RVT leiab, et valimispäeva õhtul pole miksimiseks piisavalt aega, siis on lubatud kokku lugeda miksimata hääled, sellisel juhul lugemistõendit ei väljastada. Hääled miksitakse valimispäevale järgneval päeval ja kokku lugemisel väljastatakse ka lugemistõend.

2. Kui RVT otsustab valimispäeval hääled miksida, siis miksitud häälte kokkulugemise järel genereeritakse ka lugemistõend.

Elektroonilise hääletamise üldraamistik [3] selgitab, et miksimine on oma olemuselt häälte segamine ja krüptograafiline ümberjärjestamine, mille eelduseks on homomorfse krüptosüsteemi kasutamine hääle salastamisel. See tähendab, et nii miksimise sisendi kui väljundi dekrüpteerimine peab andma sama tulemuse.

Github'i koodihoidlast toodud juhendmaterjalist[24] selgub, et miksimiseks kasutatakse Vertificatum Mixnet rakendust, mis teisendab krüptogrammid miksimiseks sobivasse formaati, seejärel järjestab ümber sisendkrüptogrammid ning uuendab krüptogrammides olevat

[24] https://github.com/valimised/ivxv/blob/master/Documentation/et/audiitor/ylevaade.rst (28.04.2024)

juhuslikust ja lõpuks teisendab krüptogrammid tagasi IVXV protokollile sobivasse formaati. Kuna Miksimisrakendusse sisse ja sealt välja tulevad väliselt üksteisest sõltumatud krüptogrammid, siis protsessi lõpus väljastatakse ka miksimistõend, mis garanteerib, et Miksimisrakendus on töötanud korrektselt ja ühtegi häält pole asendatud. Miksimistõendit saab kontrollida auditirakendusega, seda teeb audiitor valimispäeva-järgsel päeval. Miksitud e-valimiskasti kontrollsumma allkirjastatakse ja kirjutatakse koos väljunditega DVD-plaadile [26]. Sellega on häälte töötlemisetapp lõppenud ning RVT esindaja teavitab sellest kohal viibivaid vaatlejaid ja erakondade esindajaid.

7.2 Häälte lugemine

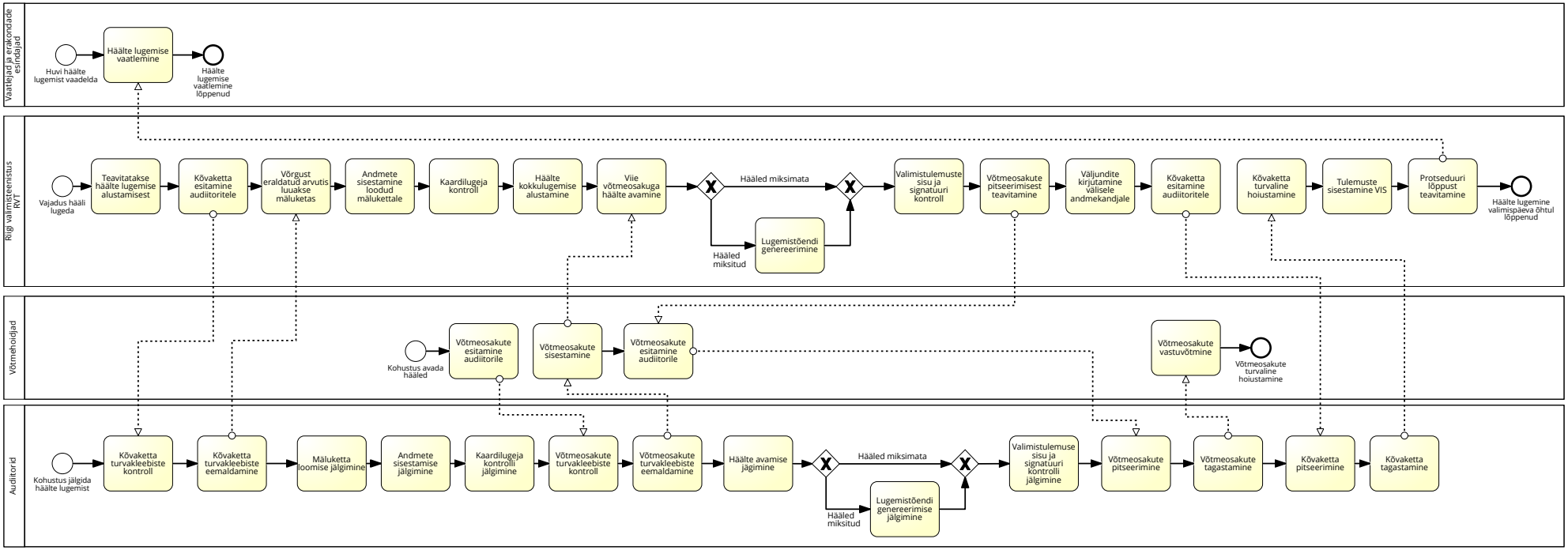
Järgnevalt viib RVT läbi häälte lugemise protseduuri. Häälte lugemine on auditeeritav protseduur, mida jälgivad ka vaatlejad ja erakondade esindajad ning see viiakse läbi võrgust eraldatud arvutis, kasutades sama süsteemiketast, mida kasutati võtmepaari genereerimise protseduuril [26]. Häälte lugemise protsess on toodud joonisel 23.

Häälte lugemise videosalvestiselt [36] selgub, et protseduuri alguses teavitab e-hääletamise juht kõiki kohalolijaid häälte lugemise algusest ja tutvustab põgusalt protsessi käiku. Seejärel esitab RVT esindaja audiitoritele välise süsteemiketta turvakleebiste kontrolliks ja eemaldamiseks. Audiitorid märgivad kleebiste numbrid ja avamise aja vastavasse akti [34]. Järgnevalt luuakse võrgust eraldatud arvutis virtuaalne mäluketas ning sisestatakse vajalikud andmed, milleks on [3]:

1. Kandidaatide ja ringkondade nimekiri.
2. Anonüümistatud e-hääled koos allkirjastatud kontrollsumma failiga või miksitud e-hääled koos allkirjastatud kontrollsummaga.

Seejärel kontrollib RVT esindaja kaardilugeja korrasolekut ning samal ajal esitavad viis võtmeosakute hoidjat oma kiipkaardid turvakleebiste kontrolliks ja avamiseks audiitorile [36].

Järgnevalt kontrollib RVT esindaja kaardilugeja korrasolekut ning samal ajal esitavad viis võtmeosakute hoidjat oma kiipkaardid audiitorile turvakleebiste kontrolliks ja avamiseks [36]. Audiitor fikseerib kirjalikult kleebiste numbrid ja kaartide avamise aja [34]. Seejärel käivitab RVT esindaja häälte kokkulugemise protsessi ning võtmeosakute hoidjad sisestavad üksteise järel oma kiipkaardid kaardilugejasse, kuni kõik viis võtmeosakut on sisestatud [36]. Seejärel algab häälte dekrüpteerimine ning kui e-hääled olid eelnevalt miksitud, väljastatakse lugemise käigus ka lugemistõend [26]. Lugemistõend kinnitab, et avakujul olev e-hääl ja sellele vastav krüptogramm on omavahel seoses, lähtudes häälte krüpteerimise avalikust võtmest [37].



Joonis 23. Häälte lugemise protsess.

Häälte dekrüpteerimise käigus kontrollib EHS hääle sisu ja kui see ei vasta valimistel kandideerinud kandidaadi numbrile, siis selline hääl tühistatakse. Kehtetuid sedeleid ei avata, kuna nende sisu ei ole teada ja tegemist võib olla ründega e-hääletamise süsteemi vastu [38]. Kehtivad hääled summeeritakse kandidaatide ja ringkondade kaupa [3].

Lõpetuseks kontrollitakse üle valimistulemuse sisu ja signatuur ning teavitatakse võtmehoidjaid, et nad võivad oma võtmeosakud esitada audiitorile turvakleebiste paigaldamiseks [39]. Pitseeritud kaardid tagastatakse võtmeosakute hoidjatele ning sellega on e-häälte lugemise protsess nende jaoks lõppenud. Samal ajal RVT esindaja allkirjastab ja kirjutab e-häälte lugemise protsessi väljundid ning logid kahes eksemplaris DVD-plaadile [3, 26]. Kui andmed on välistele andmekandjatele kirjutatud, sulgeb RVT esindaja arvuti, pakendab võtmerakendusega kõvaketta plastikarpi ning esitab selle audiitoritele turvakleebiste paigaldamiseks; seejärel tagastatakse pitseeritud kõvaketas RVT esindajale [40].

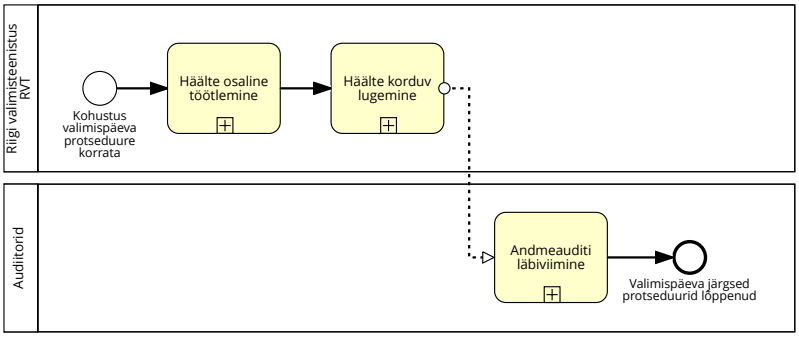
Vastavalt RKVS § 60^1 lg 9 alusel sisestab RVT esindaja koheselt hääletamistulemused VIS-i. Seejärel teavitab e-hääletamise korraldaja vaatlejaid ja erakondade esindajaid protseduuri lõppemisest [40].

7.3 Esialgsete hääletamise tulemuste väljakuulutamine

RVT avaldab valimispäeva õhtul esialgsed valimistulemused valimiste veebilehel.

7.4 Valimispäeva-järgsed protseduurid

Valimispäeva-järgsel päeval viiakse läbi häälte osaline töötlemine ning korduvlugemine, misjärel audiitor viib läbi andmeauditi. Valimispäeva-järgsed protsessid on toodud joonisel 24.

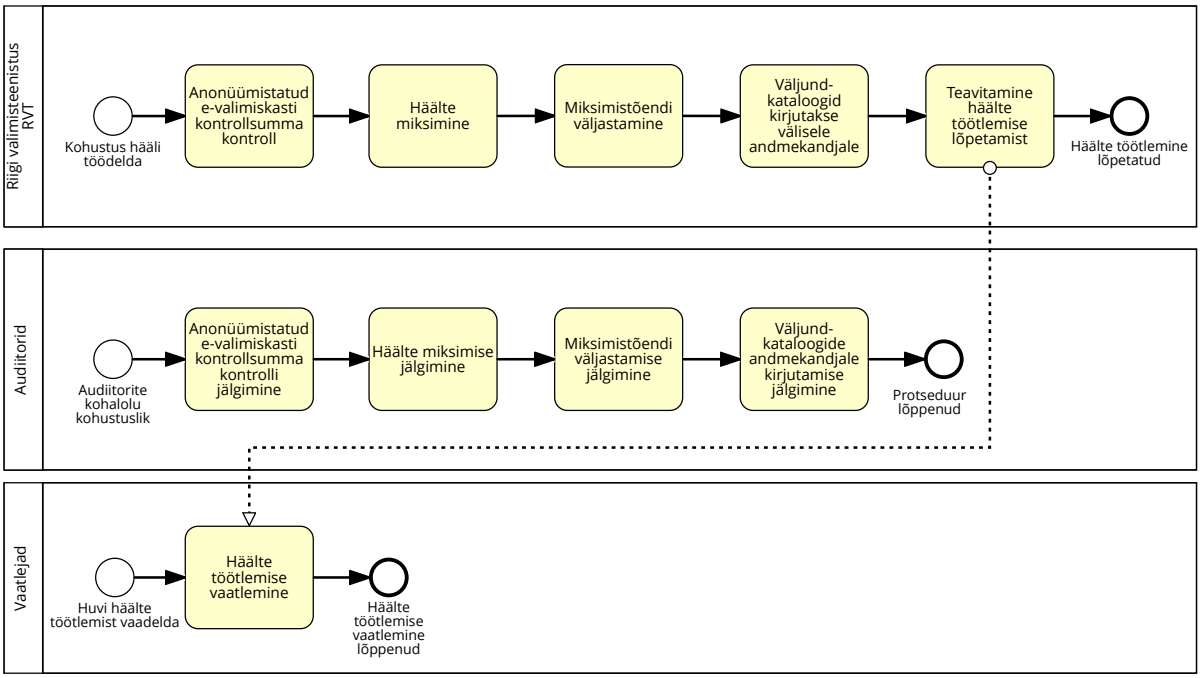


Joonis 24. Valimispäeva-järgsed protsessid.

Häälte osaline töötlemine

Valimispäeva-järgselt viib RVT läbi ainult häälte osalise töötlemise. Audiitori 2023. aasta vahearuandest [34] selgub, et häälte töötlemist alustatakse anonüümistatud e-valimiskasti kontrollsumma genereerimisega ning võrreldakse, kas see vastab valimispäeval genereeritud kontrollsummale. Seejärel viiakse läbi häälte miksimine koos miksimistõendi väljastamisega

ning miksitud e-valimiskasti kontrollsumma allkirjastatakse ja kirjutatakse koos väljunditega DVD-plaadile [15]. Häälte osalise töötlemise protsessid on toodud joonisel 25.



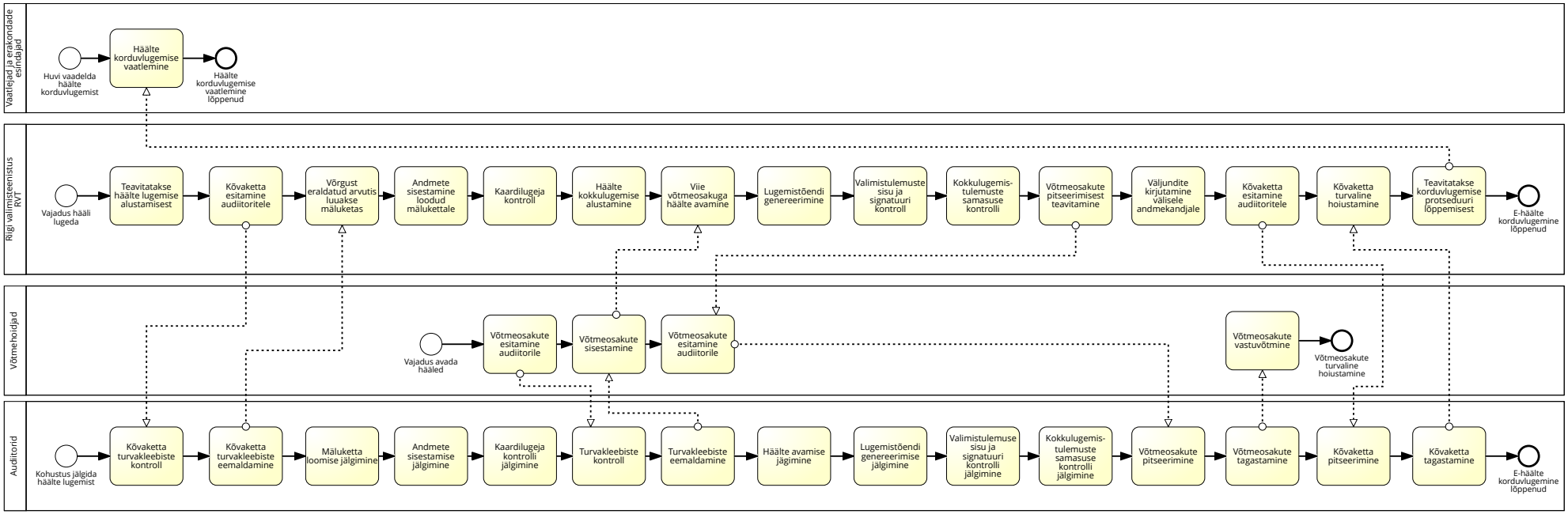
Joonis 25. Häälte osalise töötlemise protsessid.

Lõpetuseks teavitab e-hääletamise juht vaatlejaid häälte töötlemise protseduuri lõppemisest [41]. E-häälte töötlemisest on põhjalikult kirjutatud peatükis 7.1.

Häälte korduv lugemine

Järgnevalt viib RVT läbi häälte korduvlugemise protsessi. Kuna häälte lugemise protsessi on juba peatükis 7.2 detailselt kirjeldatud, siis korduvlugemise puhul on käesolevas uurimuses välja toodud ainult erandid võrreldes valimispäeva aegse häälte lugemisega. Korduvlugemine on auditeeritav protsess. Korduv häältelugemise protsess on toodud joonisel 26.

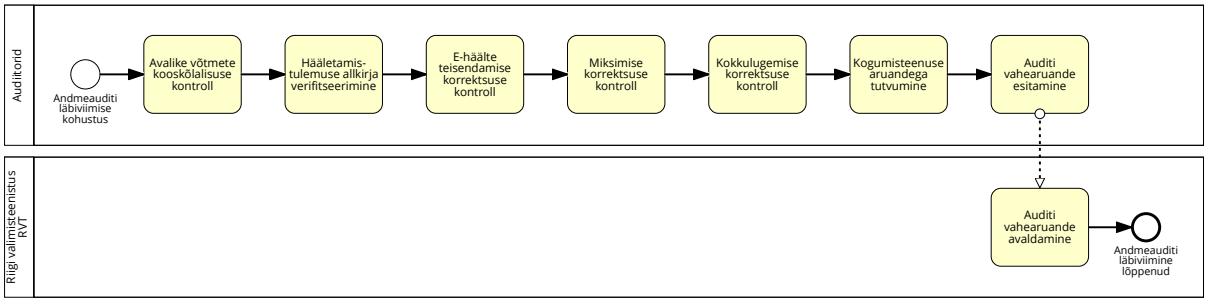
Kui e-valimiste käsiraamatus [26] oli valimispäeval lubatud lugeda ka hääli ilma miksimata, siis valimispäeva-järgsel päeval on kohustus e-hääled miksida ja sellest tulenevalt häälte lugemisel genereeritakse ka lugemistõend. Kui valimispäeval loeti hääled kokku miksimata kujul, siis nüüd võrreldakse miksimata häälte kokkulugemise tulemust miksitud häälte kokkulugemise tulemusega. Kui ka valimispäeval miksiti hääli, siis võrreldakse omavahel miksitud häälte kokkulugemise tulemusi. Mõlemal juhul peavad tulemused olema identsed.



Joonis 26. Häälte korduvlugemise protsess.

Andmeauditi läbiviimine

Pärast korduvlugemise protseduuri lõppu alustab audiitor andmeauditi läbiviimise protsessi, mis on toodud joonisel 27.



Joonis 27. Andmeauditi läbiviimise protsess.

Protsessi esimeseks sammuks on avalike võtmete kooskõlalisuse kontroll ning see lõpeb audiitori jaoks vahearuande esitamisega RVT-le, kes avaldab selle valimiste kodulehel [34]. Vastavalt audiitori soovile võib antud toimingute läbiviimise järjekord valimisperiooditi varieeruda.

Avalike võtmete kooskõlalisuse kontroll

Võtmepaari loomise käigus genereeriti privaatvõtme osakud, mis asuvad kiipkaartidel ning vastavad avalikud võtmed, mis kirjutati protseduuri lõpus DVD-plaadile [26]. Avalike võtmete kooskõlalisuse kontrolli käigus veendub audiitor, et sertifikaat, mis sisaldab tulemusfaili signeerimisvõtit, on korrektselt isesigneeritud[25] ning sertifikaat, mis sisaldas häälte salastamise võtit, on signeeritud tulemusfaili signeerimisvõtmega [4, 42]. Lisaks kontrollib audiitor, kas avaliku võtme eri kodeeringud (x509, *der*, *pem*) vastavad üksteisele [42].

Hääletamistulemuse allkirja verifitseerimine

Nii valimispäeva kui ka valimispäeva-järgse päeva e-häälte lugemise järel viib RVT läbi elektroonilise hääletamise tulemuse signatuuri kontrolli, olenemata sellest, kas valimispäeval hääled miksiti või mitte [26]. Andmeauditi käigus kontrollib hääletamistulemuste signatuuri ka audiitor, et veenduda allkirja korrektsuses, selle käigus eraldab ta signeerimisvõtme sertifikaadist avaliku võtme ning kasutab avalikku võtit häälte lugemise tulemusfaili kontrollimiseks [4]. Lisaks on võimalik audiitoril võrrelda omavahel valimispäeva ja valimispäeva-järgse päeva lugemistulemuste signatuuri, mis peavad olema identsed, olenemata sellest, kas valimispäeval hääled miksiti või mitte [42].

[25] Isesigneeritud sertifikaat on süsteemi võtmepaari genereerimise käigus loodud sertifikaat, mis sisaldab tulemusfaili signeerimisvõtit.

Häälte teisendamise kontroll

Kasutades auditirakendust, täpsemalt selle tööriista *convert*, kontrollib audiitor e-häälte teisenduste korrektsust keskkonnas, kus on tagatud sisendiks olevate miksimata krüptogrammide konfidentsiaalsus [4, 26].

Lähtuvalt IVXV seadistuste koostamise juhendis [4] toodust, selgub, et Verificatumi koostatud miksimistõendi formaat ei vasta IVXV kasutavale formaadile ning sama olukord on ka Vertificatumi ja IVXV krüpteeritud häälte formaatidega. Seetõttu on IVXV protokollil formaaditeisenduse adapterid, mis teisendavad faile ühest formaadist teise. Audiitor kontrollib, et Vertificatumi poolt koostatud miksimistõend vastaks IVXV vormingus olevatele failidele.

Miksimise korrektsuse kontroll

Nii nagu audiitor kontrollis häälte teisendamist keskkonnas, kus oli tagatud sisenditeks olevate krüptogrammide konfidentsiaalsus, tehakse seda ka miksimise korrektsuse kontrollil [26].

Vastavalt e-hääletamise käsiraamatule [26] saab audiitor protsessi läbiviimiseks valida kahe võimaluse hulgast – Auditirakenduse ja Verificatumi vahendi vahel. Lubatud on ka mõlema tööriista kasutamine, kuid Verificatumi vahend on ligi 18 korda kiirem kui Auditirakenduse tööriist *mixer*. 2023. aasta raportist [34] selgub, et audiitor kontrollis miksimistõendit mõlema vahendiga ning miksimistõend oli korrektne.

Kokkulugemise korrektsuse kontroll

Vastavalt e-hääletamise juhendmaterjalile [26] võib audiitor e-häälte kokkulugemise korrektsuse kontrolli läbi viia ükskõik millises arvutis, kuna kõik häälte krüptogrammid on miksitud ja seega ka anonüümitud ning lugemistõendi kontrolli väljund avalik. Protsessi käigus kopeeritakse kõik vajalikud sisendandmed, sh auditirakendus, audiitori poolt valitud arvutisse ning seejärel käivitatakse Auditirakenduse tööriist *decrypt*. Antud tööriist kontrollib iga krüptogrammi ja dekrüpteeritud hääle kohta eraldi, et dekrüpteerimine on toimunud korrektselt ehk iga hääle kohta on olemas dekrüpteerimise tõestus. Selle väljundi alusel saab audiitor veenduda, et hääled on kokku loetud korrektselt.

RVT edastab audiitoritele tutvumiseks Kogumisteenuse aruande, milles on välja toodud ka veateated. Viimasena esitab audiitor oma vahearuande RVT-le, kes avaldab selle valimiste kodulehel [34].

Lisaks audiitori poolt läbi viidud lugemistõendi kontrollile, viis üks Eesti arvutiteadlane 2023. aasta Riigikogu valimiste ajal läbi veel teisegi lugemistõendi kontrollimise, kasutades omakirjutatud kontrollrakendust [43].

7.5 E-hääletamise tulemuste kinnitamine

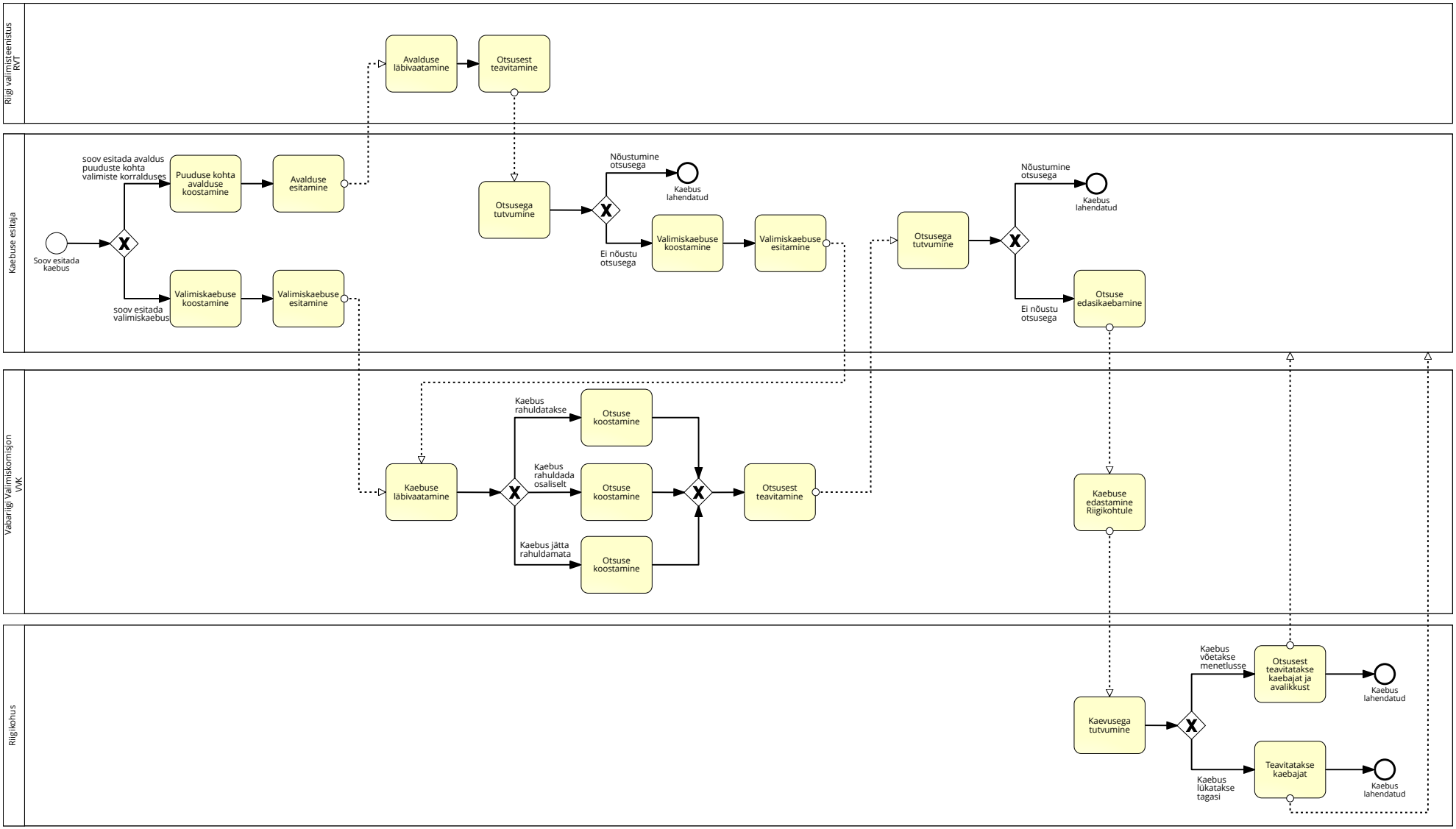
Vastavalt RKVS § 60^1 lg 10 alusel allkirjastab RVT juht e-hääletamise tulemused peale EHS-i andmete tervikluse kontrolli. Häälte teistkordsel kokkulugemisel saadud failid, milleks on hääletustulemused, signatuur, avalik võti ning „LOEMIND.txt“[26], avaldatakse allkirjastatuna valimiste kodulehel [26].

7.6 Valimiskaebuste lahendamine

Vastavalt RKVS § 68-le võib huvitatud isik, kes leiab, et valimiste korraldaja on tema õigusi rikkunud, esitada avalduse puuduste kohta valimiste korralduses. Avalduse läbivaatamine ja vastamine on RVT pädevuses. Avaldus puuduse kohta tuleb esitada hiljemalt kolmandal päeval puuduse avastamisest ja RVT peab selle läbi vaatama hiljemalt kolme päeva jooksul alates avalduse esitamisest. RVT-l tuleb läbivaatamise tulemusest teavitada avalduse esitajat. Kui avalduse esitaja ei nõustu RVT otsusega, on tal võimalus esitada valimiskaebus VVK-le. Lähtudes RKVS § 69-st selgub, et valimiskaebus on oma olemuselt VVK esitatav taotlus tunnistada seadusevastaseks valimiste korraldaja toiming. Valimiskaebuse lahendamise protsess on toodud joonisel 28.

Pärast valimiskaebuse saamist asub VVK kaebust läbi vaatama ning lähtuvalt kaebuse sisust, võib jätta kaebuse rahuldamata, rahuldada kaebuse osaliselt või rahuldada kaebuse [7]. Valimiskaebuse esitamisel tuleb jälgida, et kaebuse esitamise tähtaeg poleks möödunud; kaebus tuleb esitada kolme päeva jooksul vaidlustatava toimingu tegemisest või RVT-poolsest avalduse läbivaatamisest [7]. VVK-l on võimalik kaebus tagastada läbi vaatamata, kui kaebajal puudub kaebeõigus või kaebuse esitamise tähtaeg on möödas [7]. VVK peab kaebuse läbi vaatama ja otsuse tegema viie tööpäeva jooksul; peale otsuse tegemist tuleb viivitamata teavitada kaebuse esitajat [7]. Kui kaebuse esitaja ei nõustu VVK otsusega, on tal kolm päeva aega otsus edasi kaevata Riigikohtusse, ent seda saab teha ainult VVK kaudu [7]. Riigikohus tutvub kaebusega ja otsustab, kas lükkab kaebuse tagasi või võtab selle menetlusse, mõlemal juhul teavitatakse kaebuse esitajat [7]. Kui Riigikohus tuvastab tõsise rikkumise valimiste korralduses, siis on neil võimalik tühistada valimistulemused [7]; sellist rikkumist ei ole veel e-hääletamise ajaloo jooksul tuvastatud. Riigikohtu otsusega lõpeb valimiskaebuste läbivaatamine.

[26] Antud failis on toodud juhised, kuidas kontrollida valimistulemuse autentsust ja terviklust häälte lugemise käigus loodud signatuurfaili abil.



Joonis 28. Valimiskaebuste lahendamine.

7.7 Valimistulemuste väljakuulutamine

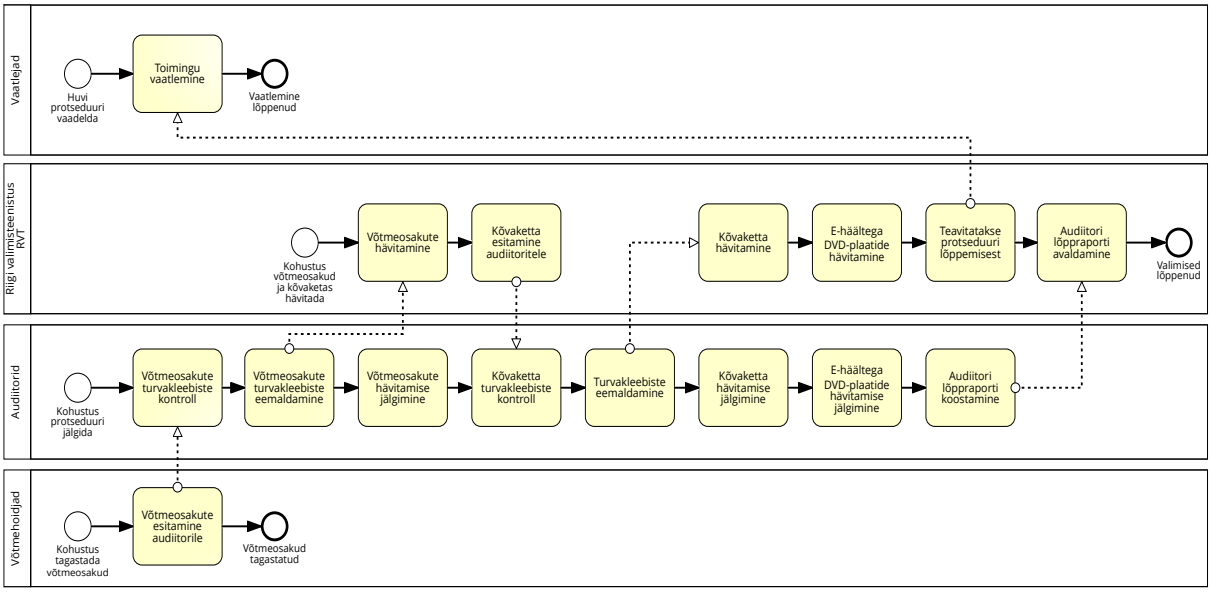
Pärast kõikide valimiskaebuste lahendamist kuulutab VVK välja lõplikud hääletamistulemused, registreerib mandaatide jagunemise Riigikogus ning kinnitab valimisringkondades valituks osutunud kandidaatide asendusliikmed [7].

7.8 Valimiskautsjoni tagastamine

Vastavalt RKVS § 77-le makstakse üksikkandidaadile või erakonnale tagasi valimiskautsjon, kui kandidaat osutub valituks või saab oma valimisringkonnas hääli vähemalt poole lihtkvoodi ulatuses. Erakonnale tagastatakse valimiskautsjon, kui nad on kogunud üleriigiliselt kokku vähemalt 5% häältest. VVK kannab tagastamata kautsjoni riigituludesse.

7.9 E-hääletamise süsteemi võtmeosakute ja kõvaketta hävitamine

E-hääletamise viimaseks protseduuriks on süsteemi võtmeosakute ja võtmetoiminguteks kasutatud kõvaketta hävitamine. Antud protsess on kajastatud joonisel 29.



Joonis 29. E-hääletamise süsteemi võtmeosakute ja kõvaketta hävitamise protsess.

Vastavalt e-hääletamise käsiraamatule [26] on süsteemi võtmepaari hävitamine auditeeritav protsess, kus võivad kohal viibida ka vaatlejad. Audiitor jälgib RVT poolt läbi viidavaid tegevusi.

E-häälte hävitamise salvestiselt [44] nähtub, et protsess algab võtmeosakute esitamisega audiitoritele, kes kontrollivad võtmehoidjate poolt esitatud kiipkaartide turvakleebiste terviklust, märgivad kleebiste numbrid ja avamise aja protokolli ning annavad kiipkaardid üle RVT esindajale nende hävitamiseks. Kiipkaardid hävitatakse füüsiliselt, kaartide kiibid puuritakse läbi. Seejärel esitab RVT esindaja audiitoritele süsteemi kõvaketta turvakleebiste

kontrolliks ja avamiseks. Peale kleebiste eemaldamist avab RVT esindaja kõvaketta korpuse ja puurib ükshaaval läbi kõik SSD (solid-state drive) kõvaketta kiibid. Seejärel söödetakse kõik e-hääletamise käigus kogunenud DVD - plaadid paberihunti ning RVT esindaja teavitab vaatlejaid protseduuri lõppemisest. Viimasena koostab audiitor oma lõppraporti ja edastab selle RVT-le, kes avaldab selle valimiste kodulehel. Ühes sellega on lõppenud ka kogu Riigikogu valimiste tsükkel.

8. Tähelepanekud ja vastuolud e-valimiste juhendmaterjalis

E-valimiste korraldust puudutavate materjalide analüüsimisel tuvastas autor mitmeid kitsaskohti valimiste korralduses, lisaks ilmnesid juhendmaterjalide omavahelised vastuolud. Järgnevalt on välja toodud leitud puudused ning soovitused, kuidas olukorda parendada.

1. Elektroonilise hääle salastamiseks kasutatava krüptoalgoritmi mooduli pikkuse määramise miinimumnõue on kehtestatud 2017. aasta VVK otsusega [16]. Autor ei suutnud leida ühtegi kirjaliku e-hääletamisega seotud juhendmaterjali, milles oleks toodud täpsed parameetrid, millest lähtub RVT krüptoalgoritmi mooduli pikkuse määramisel. 2017. aastast säilinud e-valimiste süsteemi salvestises [18] väidab endine e-hääletamise juht Tarvi Martens, et kasutatav krüptoalgoritm peab tagama hääle salajasuse vähemalt 30 aastaks. Kas sellest põhimõttest lähtub RVT ka tänasel päeval, pole teada.

RVT peab dokumentatsioonis kirjeldama krüptoalgoritmi mooduli pikkuse määramise täpsed parameetrid ning e-hääletajatele tuleb ka selgelt välja öelda, et juhul, kui nende krüpteeritud e-hääl peaks lekkima, on võib olla võimalik seda teatud ajaperioodi jooksul lahti murda. Sellele riskile peab RVT juhtima valijate tähelepanu, sest e-hääle avalikuks tulekuga võivad e-hääletajatele tekkida ebameeldivad tagajärjed.

2. Märt Põdra 2023. aasta Riigikogu valimiste valimiskaebusest [28] selgus, et vaatlejatel ja audiitoritel puudub võimalus tutvuda võtmepaari genereerimiseks kasutatavale välisele kõvakettale paigaldatud operatsioonisüsteemi ja rakendustega, veendumaks, ega need ei sisalda pahavara. RVT on kaebuse vastuses [28] selgitanud, et võtmetoimingud viiakse läbi võrguühenduseta arvutis, millel puuduvad sisemised salvestusseadmed ning võtmetoimingute välisel ajal on süsteemiketas turvakleebistega pitseeritud, ei saa sealt andmed lekkida. Riigikohus rahuldas Märt Põdra valimiskaebuse, misjärel RVT võimaldas M. Põdral süsteemiketta tagavarakoopiale paigaldatud tarkvaraga tutvuda.

Autor nendib, et ka 2024. aasta EP valimiste võtmepaari genereerimise protseduuril oli antud küsimus jätkuvalt lahendamata. Süsteemiketas oli RVT poolt eelnevalt ette valmistatud ja auditeerimata.

RVT-l tuleb igasuguste kahtluste hajutamiseks täiendada võtmepaari genereerimise protseduuri, kus audiitoritel (võimalusel ka vaatlejatel) oleks võimalik kontrollida võtmeprotseduurideks kasutatava kõvaketta operatsioonisüsteemi ja rakendusi ning auditeerida ka tarkvara paigaldamist. Praegu peavad nii audiitor, valijad kui ka vaatlejad pimesi usaldama

valimiste Korraldajat, et võtmeprotseduurideks kasutatava süsteemiketta tarkvara ei sisalda pahavara.

3. E-hääletamise käsiraamatu [26] peatükis 2.3 − „Süsteemi võtmepaari genereerimine“ on välja toodud, et see on auditeeritav protseduur. Protseduuri esimeseks etapiks on konfiguratsiooni ja võtmerakenduse ettevalmistamine. 2023. aasta audiitori vahearuandest [29] selgus, et protseduuri alustati hoopis teisest etapist; konfiguratsiooni ja võtmerakenduse ettevalmistamine oli RVT-l juba eelnevalt tehtud ning väljund DVD-plaadile kirjutatud. Seetõttu võib väita, et RVT ei lähtu samm-sammult e-valimiste käsiraamatus toodud juhendist ning konfiguratsiooni ja võtmerakenduse ettevalmistamine ei ole auditeeritav.

Autor nendib, et ka 2024. aasta EP valimiste süsteemi võtmepaari genereerimise protseduuril kordus tuttav muster: konfiguratsiooni ettevalmistamine ja DVD-plaadile kirjutamine oli RVT poolt juba eelnevalt tehtud. Konfiguratsiooni ja võtmerakenduse ettevalmistamist ei auditeeritud. Protseduuri alustati alates teisest alapunktist, milleks on mäluketta loomine. Pärast konfiguratsiooni importimist vaadati audiitori ja vaatlejate juuresolekul üle konfiguratsioonifailide allkirjastajad ja allkirjade sertifikaadid ning viidi läbi konfiguratsiooni kontrollsumma kontroll, mida ei ole e-valimiste käsiraamatus ette nähtud.

Vastuolu lahendamiseks tuleb RVT-l edaspidi protseduur läbi viia vastavalt juhendile [26] või uuendada juhendmaterjali, et protseduuri kirjeldus vastaks tegelikule olukorrale.

4. Vastavalt RVT infoturvapoliitika juhendile [23] rakendatakse EHS-i riskide vähendamiseks E-ITS’is kirjeldatud turvameetmeid. 2024. aasta EP valimiste süsteemi võtmepaari genereerimise protseduuril oli mõnesekundilise kestvusega elektrikatkestus, mis katkestas protseduuri ja seda tuli uuesti algusest peale läbi viia. RVT-l tuleb üle hinnata EHS-i käideldavusega seotud riskid ja tagada arvutitele puhvertoiteallikas (*Uninterruptable Power Supply*). Vastasel juhul võib juhtuda, et valimispäeva õhtul ei saa näiteks valimistulemusi kindlaks teha, kuna RVT ametiruumides on elektrikatkestus.

Autor nendib, et RVT reageeris probleemile operatiivselt. Juba järgmisel päeval (süsteemi testläbimisel) oli kasutusel puhvertoiteallikas ning e-valimiste juht kinnitas, et võimalik elektrikatkestus 2024. aasta EP valimiste protseduuride edasist läbiviimist ei mõjuta.

5. Elektroonilise hääletamise üldraamistiku [3] põhjal selgub, et Kontrollrakendus ei tuvasta hääle kontrollijat [37].

RVT-l tuleks kaaluda, kas Kontrollrakenduse peaks enne hääle kontrollimist tuvastama kasutaja isiku. Näiteks võib valija peale e-hääletamist Valijarakenduse lahti unustada ja ise

arvuti juurest eemale jalutada ning seetõttu võib realiseeruda risk, kus kõrvalisel isikul on võimalik Kontrollrakendusega kindlaks teha, kelle poolt hääletati. Siinkohal tuleb rõhutada asjaolu, et ka e-hääletajal on oma hääle salajasuse tagamise kohustus. Antud küsimus vajab täiendavat analüüsi, sest Kontrollrakenduse kasutaja tuvastamise nõue pärsib kasutamismugavust, lisaks tekib küsimus ID-kaardiga hääletajate korral, kellel puudub telefonis enda Mobiil-IDga tuvastamise võimalus.

6. E-hääletamise süsteemi infoturvapoliitika juhendmaterjalis [23] on toodud, et e-valimiskasti ja logide varundamine toimub vähemalt kord ööpäevas ning varukoopiate tegemiseks kasutatakse ühekordselt kirjutatavat irdmeediat [5]. Samas on GitHub'i koodihoidlas olevas e-hääletamise haldustoimingute dokumendis[27] kirjas, et varukoopiad talletatakse varundusserveris.

RVT nõunik selgitas 16. mail 2024 toimunud e-valimiste vaatlemise koolitusel, et RIA teeb häälte kogumise perioodil vähemalt kord päevas e-valimiskastist varukoopiad oma varundusserverisse ning vahetult peale hääletamisperioodi lõppu tehakse kaks identset koopiat DVD-plaadile, mis hiljem antakse üle RVT-le.

Siin on erinevate e-valimiste juhendmaterjalide omavaheline vastuolu, RVT-l on vaja avaldada täpne ja ajakohastatud info.

7. Audiitor ei kontrolli valijate nimekirjas olevate isikute valimisõigust.

Siin tuleks RVT kaaluda protseduuri muutmist nii, et audiitoril oleks täiendav tööriist, millega teha juhusliku valiku alusel mingi arv päringuid valijate nimekirja kohta, kontrollimaks, kas neil isikutel on õigus osaleda hääletamisel. See võimaldaks vähendada sisemise ründaja riski, kus pahatahtlik rahvastikuregistri vastutav töötleja saaks lisada valimisnimekirja valimisõigust mitteomavaid valijaid, et mõjutada valimistulemust. Hetkel peab audiitor pimesi usaldama valimiste nimekirja koostajat, kuna valimisnimekirjas olevate valijate valimisõigust ei ole võimalik kontrollida. Käesolev probleem ja selle lahendamine vajab täiendavat analüüsi.

8. Audiitori 2023. aasta vaheraportist [34] selgub, et valimisjärgsel päeval viiakse läbi ainult osaline häälte töötlemine − see algab anonüümitud häälte kontrollsumma kontrollist. Samas valimiste kodulehel[28] olevas infos, sh animatsioonides, on toodud, et valimispäeva-järgsel

[27] https://github.com/valimised/ivxv/blob/master/Documentation/et/kogumisteenuse_haldusjuhend/haldustoimingud.rst (03.05.2024)

[28] https://www.valimised.ee/et/e-haaletamine/e-haaletamisest-lahemalt/e-haaletamise-tutvustus (03.05.2024)

päeval viiakse läbi kõik protseduurid teistkordselt. Juhendmaterjal ei näe ette osalist häälte töötlemist.

Autor tuvastas vaatlejana, et EP valimiste valimisjärgsel päeval 10. juunil 2024 viidi läbi häälte täielik töötlemine alates e-valimiskasti kontrollsumma kontrollist. E-valimiste juhi selgituse kohaselt polnud valimisjärgsel päeval protseduuride läbiviimiseks ajalist piirangut ja seega viidi läbi häälte täielik töötlemine.

RVT-l on vaja avaldada valimispäeva-järgseid protseduure puudutav täpne ja ajakohastatud juhendmaterjal. Et kõikidele osapooltele oleks üheselt arusaadav, milliste kriteeriumite alusel RVT otsustab, kas viia läbi ainult osaline häälte töötlemine või täielik häälte töötlemine.

9. Valimispäeva õhtul on lubatud hääli kokku lugeda ilma miksimata. E-valimiste käsiraamatus on selle kohta toodud hägune selgitus, et hääli ei pea miksima, kui e-valimiste juht leiab, et valimisprotseduurid ei võimalda miksimiseks vajalikku ajaperioodi [26].

RVT nõunik selgitas 16. mail 2024 toimunud e-valimiste vaatlemise koolitusel, et valimispäeval ei miksita hääli juhul, kui tühistusnimekirja koostamine venib ning on risk, et valimistulemusi ei suudeta avaldada enne südaööd.

RVT-l on vaja juhendmaterjalis täpsustada valimispäeva häälte miksimise protseduuri kirjeldust, et kõikidele osapooltele oleks üheselt arusaadav, millistel asjaoludel võib hääled jätta miksimata.

10. 2023. aasta Riigikogu valimiste ajal viis üks Eesti arvutiteadlane läbi omakirjutatud tarkvaraga lugemistõendi kontrollimise [43].

RVT-l tuleks täiendada e-valimiste juhendmaterjali, et kõigile oleks üheselt arusaadav, kuidas ja millistel tingimustel sõltumatud osapooled saavad oma kontrolltarkvaraga miksimistõendit ja lugemistõendit kontrollida. Ning kuidas lahendada võimalike vaideid, kui kontrolli tulemused peaksid erinema audiitori poolt läbi viidud kontrollide tulemusest. Antud küsimus ja selle lahendamine vajab täiendavat analüüsi.

11. E-hääletamise viimase protseduurina hävitab RVT füüsiliselt võtmeosakute kiipkaardid, võtmetoiminguteks kasutatud kõvaketta ja valimiste käigus kasutatud DVD-plaadid [26]. E-hääletamise dokumentidest ei järeldu, millistel tingimustel ja kuidas hävitab RIA e-valimiskasti tagavarakoopiad ja Kogumisteenuse logid. Siin peavad audiitor ja vaatlejad usaldama RIA-t, et seda tehakse korrektselt, kuid kontrollida pole seda hetkel võimalik.

RVT-l on vaja täiendada süsteemi võtmepaari hävitamise protseduuri juhendmaterjali, kus oleks kajastatud ka tagavarakoopiate ja Kogumisteenuse logide hävitamise tingimused, ajakava ja kontrollmehhanismid.

Mitmes eespool viidatud punktis on välja toodud e-valimiste süsteemi puudutava dokumentatsiooni omavahelised vastuolud ja aegunud juhendmaterjali avaldamine, millele on oma 2023. aasta raportis viidanud ka OSCE [2]. E-valimistega seotud probleemide lahendamise venimise juurpõhjuseks on poliitilise tahte puudumine, sest Vabariigi Valitsus ei eralda RVT-le piisavalt rahalisi vahendeid, et e-hääletust puudutav juhendmaterjal korda teha. Elektroonilise hääletamise süsteemi arendatakse otsekui hoogtöö korras enne igat valimisperioodi, sel moel ei suuda RVT tagada e-hääletamise süsteemi ja selle juhendmaterjali jätkusuutlikku arendamist [37].

9. Tähelepanekuid audiitori rollist

Elektroonilise hääletamise materjalide analüüsimisel selgub, et valdav osa audiitori tööst on oma olemuselt passiivne – audiitor jälgib RVT poolt läbiviidavaid toiminguid (süsteemi võtmepaari genereerimist, testläbimist, e-valimiskasti üleandmist, häälte töötlemist, häälte lugemist) terminali ekraanilt ega sekku protseduuri. Ainult valimispäeva-järgsel päeval – pärast häälte korduvlugemist –, on audiitoril kohustus läbi viia andmeaudit (kirjeldatud käesoleva töö 7.4 peatükis). Autor on järgnevalt välja toonud mitmeid ettepanekuid, kuidas parendada audiitori tööd e-valimiste protsessis.

Audiitori raportiga seotud ettepanekud

1. Audiitori poolt koostatud raportid on suunatud auditi tellijale, kelleks on RVT. E-hääletamise käsiraamatut ja audiitorijuhendit tuleks täiendada selliselt, et audiitori raportid oleksid eelkõige suunatud valijale, kellel oleks võimalik raportite alusel kergesti veenduda, et e-valimised on läbi viidud korrektselt. Audiitori raport peab olema koostatud nii, et see oleks arusaadav keskmisele valijale, kes ei pruugi e-hääletamise protseduure peensusteni tunda.

2. Audiitori raportid peaksid kirjeldama ka e-valimiste protseduure, mida audiitor ei jälgi ega kontrolli ja tooma välja nende protseduuridega seotud kaitsemeetmed ning jääkriskid. See annab valijatele selge ülevaate elektroonilise hääletamise süsteemi kitsaskohtadest.

RVT-l tuleks täiendada audiitorijuhendit selliselt, et audiitoril oleks oma raportis kohustus välja tuua mitteauditeeritavate protseduuridega seotud kaitsemeetmed ning jääkriskid.

3. Audiitor peaks oma raportis selgitama, milliseid Korraldaja läbiviidud protseduure ja kontrolle ta jälgis ning millised on võimalikud ohud seoses sellega, et ta ei ole kontrolle ise läbi viinud.

Kuna e-valimiste protseduuridel terminali väljund vahetub võrdlemisi kiiresti, siis võib juhtuda, et audiitoril võib jääda midagi olulist märkamata, olles näiteks samal ajal hõivatud turvakleebiste kontrollimise ja avamisega.

4. Audiitor peaks oma raportites põhjalikumalt lahti seletama, milliseid kontrolle ta andmeauditi käigus ise läbi viis ning milliseid riske antud kontrollid maandasid. Siis oleks valijatele ka arusaadav, missuguseid ohte aitab audiitori poolt läbiviidav andmeaudit miinimumini viia.

RVT-l tuleks täiendada audiitorijuhendit selliselt, et audiitoril oleks oma raportis kohustus välja tuua EHS-i võimalikud riskid ning seostada need valitud kaitsemeetme ja audiitori poolt läbi viidud kontrollidega.

5. 2023. aasta Riigikogu valimiste audiitori raportis [34] on välja toodud, et valimiste korraldaja edastas audiitorile Kogumisteenuse aruande ning audiitor on tutvus aruandega ja selles välja toodud veateadetega. Audiitori raportit lugevale valijale ei anna see palju informatsiooni, pigem huvitaks valijat lühikokkuvõte tõsisematest veateadetest.

RVT võiks kaaluda audiitori juhendi täiendamist nii, et audiitoril oleks oma raportis kohustus anda väike ülevaade Kogumisteenuse tõsisematest veateadetest ja nende lahendamisest.

Audiitori poolt tehtavate kontrollidega seotud ettepanekud

1. Audiitor ei kontrolli võtmepaari genereerimiseks kasutatavale kõvakettale paigaldatud tarkvara. Seetõttu pole garanteeritud, et kõvakettale on paigaldatud autentne tarkvara. Kui võtmepaari genereerimiseks kasutatav tarkvara on kompromiteeritud, siis on võimalik luua nõrk või teadaolev privaatvõti, mille abil saaks rikkuda valimiste salajasust. Seetõttu on oluline, et audiitor auditeeriks võtmepaari genereerimiseks kasutatavat tarkvara ja selle paigaldamist.

RVT-l oleks süsteemikettale tarkvara paigaldamise auditeeritavaks muutmine võrdlemisi lihtne. E-hääletamise käsiraamatusse tuleb viia sisse muudatus, et süsteemikettale tarkvara ja rakenduste paigaldamine on auditeeritav protseduur ning tarkvara paigaldamise kohta tuleb koostada protokoll. Pärast operatsioonisüsteemi ja rakenduste paigaldamist tuleb audiitoril süsteemiketas ja selle tagavarakoopia pitseerida turvakleebistega, et valimiste Korraldajal ei oleks võimalik sinna ilma audiitori teadmata lisatarkvara paigaldada.

2. E-valimiste protseduuridel terminali väljund vahetub võrdlemisi kiiresti, siis võib juhtuda, et audiitoril võib jääda midagi olulist märkamata.

RVT võiks täiendada e-hääletamise käsiraamatut, mis kohustaks, et kõiki auditeeritavaid protseduure kontrolliks samaaegselt vähemalt kaks audiitorit.

Autor märgib, et 2024. aasta EP valimiste süsteemi võtmegenereerimise protsessi jälgis ainult üks audiitor, kuid teistel protseduuridel oli kohal kaks audiitorit.

3. RVT võiks kaaluda audiitorile täiendavate ülesannete andmist, kus valimispäeva-järgsel päeval on audiitoril e-valimiskasti töötlemise eri etappidel kohustus ise genereerida e-valimiskasti kontrollsummad ja võrrelda tulemusi valimispäeval saadud kontrollsummadega. Audiitori poolt läbi viidavate täiendavate kontrollide ajakulu oleks võrdlemisi marginaalne.

4. 2023. aasta Riigikogu valimiste audiitori vaheraportis [29] on toodud, et süsteemiketta ja võtmeosakute pitseerimiseks kasutatud turvakleebistel märgiti lisakontrollina audiitori allkiri. See asjaolu välistab olukorra, kus valimiste korraldajal võib olla kaks komplekti identsete numbritega turvakleepse ning audiitori teadmata on võimalik süsteemiketast või võtmeosakuid avada, viia läbi toiminguid ja hiljem sulgeda.

RVT-l tuleks e-hääletamise käsiraamatusse sisse viia täiendus, et audiitoril on kohustus lisakaitsemeetmena turvakleebised allkirjastada.

Enamik eespool mainitud kitsaskohti on RVT poolt võrdlemisi lihtsalt lahendatavad juhendmaterjali muutmisega ning audiitorile pandavad lisaülesanded ei too protseduuride läbiviimises suurt täiendavat ajakulu, kuid annab valijale kindluse ning selgema ülevaate, et e-valimised on läbi viidud korrektselt.

10. Kokkuvõte

Käesoleva magistritöö eesmärgiks oli e-valimiste protsesside tuvastamine avalikest allikatest leitavate dokumentide põhjal; e-valimiste protsesside modelleerimine Riigikogu korraliste valimiste näitel, pöörates suuremat tähelepanu audiitori rollile protsessis. Lisaeesmärgiks oli tuvastada läbiviidavate protsesside kitsaskohti ja vastuolusid elektroonilise hääletamise dokumentatsioonis ning teha parendusettepanekuid.

Töö raames valmisid elektroonilise hääletamise protsesside mudelid koos detailse kirjeldusega, kus on toodud esile, mida igas etapis tehakse. Töös on välja toodud juhendmaterjalide põhjal tuvastatud tähelepanekud ja vastuolud ning pakutakse soovitusi auditeerimisprotsessi täiustamiseks. Töö väärtus seisneb e-hääletamist puudutava info koondamise ühtsesse allikasse, kus lugejal on võimalik saada ülevaade tervest Riigikogu valimiste protsessist – alates selle esimesest sammust, Põhiseaduse § 60 tulenevast kohustusest korraldada korralisi Riigikogu valimisi iga nelja aasta tagant kuni e-hääletamise viimase protsessini, milleks on võtmeprotseduurideks kasutatud süsteemiketta ja võtmeosakute avalik hävitamine.

Töö edasiarendusena soovitab autor käsitleda erakorraliste Riigikogu valimistega seotud protsesse, veendumaks, kas erakorralistel valimistel on üldse võimalik elektroonilist hääletust kasutada. Siin tuleb silmas pidada asjaolu, et korraliste e-valimiste ettevalmistusperiood kestab pea neli kuud, aga erakorralised valimised tuleb korraldada hiljemalt 40 päeva pärast valimiste väljakuulutamist. Teise edasiarendusena soovitab autor uurida, milliseid muutusi toob e-valimiste protsessides endaga kaasa 1. oktoobril 2024 jõustuv RKVS muudatus, mis võimaldab tulevikus kasutusele võtta m-hääletuse ehk hääletamise mobiilseadmes.

Lähtudes eeltoodud infost võib väita, et lõputöö eesmärgid said täidetud. Töö tulemusena valmis terviklik ülevaade elektroonilise hääletamise protsessist Riigikogu korraliste valimiste näitel.

11. Viidatud kirjandus

[1] Ehin P, Solvak M, Willemson J, Vinkel P. Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*, 2022, kd. 39(4), nr 101718.

[2] OSCE/ODIHR. Eesti Riigikogu valimised 5. märts 2023 ODIHR valimiste eksperdirühma lõpparuanne, 2023. https://www.osce.org/files/f/documents/c/0/551671.pdf (18.03.2024)

[3] Riigi Valimisteenistus. Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/314b409f-eeed-4ef5-8cf0-c862876c3857/ (25.04.2024)

[4] Riigi Valimisteenistus. IVXV seadistuste koostamise juhend, 2023. https://www.riigikogu.ee/download/41609076-f53a-4d3d-b214-7a7409334795 (28.04.2024)

[5] Riigi Valimisteenistus. Elektroonilise hääletamise süsteemi infoturbe poliitika kinnitamine, 2022. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/9717f73e-c9d0-4b29-b8af-40fc09b9b6b0 (03.05.2024)

[6] Vabariigi Valimiskomisjon. Elektroonilise hääletamise organisatsiooni kirjeldus, 2021. https://www.riigiteataja.ee/akt/305022021001 (20.04.2024)

[7] Riigikogu valimise seadus, 2002. https://www.riigiteataja.ee/akt/124052024009 (03.08.2024)

[8] Springall D, Finkenauer T, Durumeric Z, Kitcat J, Hursti H, MacAlpine M, Halderman JA. Security Analysis of the Estonian Internet Voting System. *InProceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, 703-715.

[9] Heiberg S, Martens T, Vinkel P, Willemson J. Improving the verifiability of the Estonian Internet Voting scheme. *InInternational Joint Conference on Electronic Voting*, 2016, 92-107.

[10] OSCE/ODIHR. Eesti Vabariik Riigikogu Valimised 4. märts 2007. a. OSCE/ODIHR valimiste hindamise missiooni aruanne, 2007. https://www.osce.org/files/f/documents/3/c/25927.pdf (10.03.2024)

[11] OSCE/ODIHR. Eesti Riigikogu valimised 6. märts 2011 OSCE/ODIHR-i valimiste hindamise missiooni aruanne, 2011. https://www.osce.org/files/f/documents/2/7/81813.pdf (10.03.2024)

[12] OSCE/OHDIR. Eesti Riigikogu valimised 1. märts 2015 OSCE/ODIHR-I valimiste eksperdirühma aruanne, 2015. https://www.osce.org/files/f/documents/7/3/165836.pdf (10.03.2024)

[13] OSCE/OHDIR. Eesti Riigikogu valimised 3. märts 2019 ODIHR valimiste eksperdirühma aruanne, 2019. https://www.osce.org/files/f/documents/1/3/429065.pdf (10.03.2024)

[14] Dumas M, Rosa LM, Mendling J, Reijers AH. Fundamentals of business process management. Springer-Verlag. 2018.

[15] Willemson J, Krips K. Estimating Carbon Footprint of Paper and Internet Voting. *InInternational Joint Conference on Electronic Voting*, 2023, 140-155.

[16] Vabariigi Valimiskomisjon. Tehniliste nõuete kehtestamine elektroonilise hääletamise üldpõhimõtete tagamiseks, 2017. https://www.riigiteataja.ee/akt/306052017001 (05.08.2024)

[17] Riigi Valimisteenistus. Elektrooniliste häälte salastamiseks kasutatava krüptoalgoritmi määramine 2023. a Riigikogu valimistel, 2022. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/5ccbb266-2e6f-40b2-9ce6-8980e76db5f9 (24.04.2024)

[18] Riigi Valimisteenistus. Uue e-hääletamise süsteemi tutvutus (videosalvestis), 2017. https://www.youtube.com/watch?v=4UIiPmTBjWo (02.03.2024)

[19] Bundesamt für Sicherheit in der Informationstechnik. Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths, 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile (10.08.2024)

[20] Riigi Valimisteenistus. Elektroonilise hääletamise süsteemi testimise ajakava ja ulatus 2023. a Riigikogu valimistel, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/8126e170-9c9a-4d90-a0b3-4285ab156ac6 (20.04.2024)

[21] Riigi Valimisteenistus. Elektroonilise hääletamise rakkerühma liikmete nimetamine 2023. a Riigikogu valimisteks, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/52f63e58-9edb-42bd-8e17-0de56971e77d (20.04.2024)

[22] Riigi Valimisteenistus. Elektrooniliselt antud häälte lugemise juures viibivate riigi valimisteenistuse esindajate määramine ning elektrooniliste häälte avamise võtme ligipääsuvahendite jaotamine riigi valimisteenistuse esindajate vahel, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/63b7dedb-b4f6-4740-856f-43a4e4b24792 (20.04.2024)

[23] Riigi Valimisteenistus. Riigi valimisteenistuse infoturvapoliitika, 2024. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/e28d2604-8c22-429b-8090-436b0a77ade1/ (25.04.2024)

[24] Riigi Valimisteenistus. Elektroonilise hääletamise protokollistiku ja süsteemi tehniliste juhendite kinnitamine, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/191eacdb-a9f8-44fe-afb6-25184a82a83f (22.04.2024)

[25] Riigi Valimisteenistus. Operatsioonisüsteemide määramine valijarakendusele ja hääle kontrollrakendusele 2023. a Riigikogu valimistel, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/f3cf6b2b-9b95-4839-b299-9847ad2355b6 (23.04.2024)

[26] Riigi Valimisteenistus. IVXV: E-hääletamise käsiraamat, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/4046ee65-26c1-498c-818e-c9b6c87a7634/ (02.05.2024)

[27] Töötasu alammäära kehtestamine, 2023. https://www.riigiteataja.ee/akt/109122023005 (23.04.2024)

[28] Vabariigi Valimiskomisjon. Märt Põdra kaebuse läbivaatamine nr 54, 2023. https://www.riigiteataja.ee/akt/328022023004 (05.08.2024)

[29] KPMG Baltics OÜ. Elektroonilise hääletamise protsessi auditeerimine (1. vahearuanne), 2023. https://www.valimised.ee/sites/default/files/2023-02/2023%20Riigikogu%20valimiste%20e-h%C3%A4%C3%A4letamise%20auditi%20vahearuanne.asice (02.05.2024)

[30] Riigikogu valimiste süsteemi võtmepaari genereerimine (videosalvestis), 2019. https://www.facebook.com/watch/?v=255906565286300 (23.04.2024)

[31] E-valimiste testläbimine (videosalvestis), 2019. https://www.facebook.com/watch/?v=252736138995409 (23.04.2024)

[32] Riigi Valimisteenistus. IVXV valijarakenduse pakendamine, 2022. https://www.riigikogu.ee/download/63569a6c-9d3e-4769-b946-1ba1bed7eb48 (02.05.2024)

[33] Riigi Valimisteenistus. Elektroonilise hääletamise süsteemi testimise tulemuste kinnitamine 2023. a Riigikogu valimistel, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/faadb0cd-ecfa-4e6a-bad4-b07551cef010/ (10.06.2024)

[34] KPMG Baltics OÜ. Elektroonilise hääletamise protsessi auditeerimine (2. vahearuanne), 2023. https://www.valimised.ee/sites/default/files/2023-03/Vahearuanne%202%20RKV23%20EValimiste%20Audit.asice (05.08.2024)

[35] Riigi Valimisteenistus. Hääletamise korraldamise juhendi kinnitamine Riigikogu valimisteks 2023. aastal, 2023. https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/4cc6a5f3-fb3f-484f-8793-be6d868da798 (26.04.2024)

[36] Švilponis S. Tallying the e-votes of Estonian Parliament Elections 2019. Part 1, 2019. https://www.youtube.com/watch?v=LKqaFOz8Z_s&t=4s (28.04.2024)

[37] KPMG Baltics OÜ. Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse terviklik auditeerimine ja hindamine Majandus- ja Kommunikatsiooniministeeriumile, 2022. https://www.mkm.ee/media/7414/download (07.08.2024)

[38] Vabariigi Valimiskomisjon. Andres Alla kaebuse lahendamine, 2024. https://www.riigiteataja.ee/akt/322062024003 (01.08.2024)

[39] Švilponis S. Tallying the e-votes of Estonian Parliament Elections 2019. Part 4, 2019. https://www.youtube.com/watch?v=F8tso07aGiQ (28.04.2024)

[40] Švilponis S. Tallying the e-votes of Estonian Parliament Elections 2019. Part 5, 2019. https://www.youtube.com/watch?v=nVu4O_woUYU (28.04.2024)

[41] Šviponis S. Mixing of the votes of Estonian Parliament Election 2019. Part 3, 2019. https://www.youtube.com/watch?v=VCJZG7y2hRs (28.04.2024)

[42] Riigi Valimisteenistus. IVXV juhend audiitorile, 2023. https://github.com/valimised/ivxv/blob/published/Documentation/et/audiitor/audit.rst (08.08.2024)

[43] Willemson J. Creating a Decryption Proof Verifier for the Estonian Internet Voting System. *InProceedings of the 18th International Conference on Availability, Reliability and Security,* 2023, 1-7.

[44] Riigi Valimisteenistus. KOV valimiste e-häälte hävitamine, 2021. https://www.youtube.com/watch?v=qHFPsydaqhE (06.05.2024)

Lisad

I. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Lauri Ütsik,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „E-valimiste protsessid Riigikogu valimiste näitel, mille juhendajad on Kristjan Krips ja Jan Villemson, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Lauri Ütsik

09.08.2024