TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kristjan Düüna 204264IAPM

EESTI E-HÄÄLETAMISE USALDUSVÄÄRSUSE JA LÄBIPAISTVUSE TÕSTMINE

Magistritöö

Juhendaja: Tarvo Treier
MsC

Tallinn 2024

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Kristjan Düüna

20.05.2024

Annotatsioon

Magistritöö eesmärgiks on kontrollida, kas ebaausatel korraldajatel on võimalik keskserveris hääli nii välja vahetada, et vaatlejad ega audiitorid seda ei märka. Tulemused aitavad kaasa e-hääletamise turvalisemaks muutmisele.

Töö käigus viidi läbi e-hääletamise süsteemi samm-sammuline analüüs, leidmaks võimalikke ründekohti. Selle käigus leiti, et töötlemisetapi sees olevates alametappides ei ole lihtsat viisi kontrollimaks, ega häältega ei ole manipuleeritud.

Antud probleemile pakuti välja lahendus, mis lisab täiendavad kontrollmehhanismid veendumaks, et kõik hääled, mis olid olemas esialgses valimiskastis, oleks olemas kas tühistatud häälte hulgas või lugemisele minevate häälte hulgas. Pakutud lahendust tutvustati Valimiskomisjonile, kes kiitsid selle heaks, ning 2024. aasta valimistel peaks see olema lisatud auditrakendusse.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 30 leheküljel, 6 peatükki, 14 joonist, 1 tabel.

Abstract

Improving the Verifiability and Transparency of Estonian Internet Voting

The purpose of this thesis is to verify whether dishonest organizers can exchange votes in the central server without being detected by observers or auditors. The results contribute to making Estonian internet voting more secure.

To find possible weaknesses in the system, it is important to understand the system. For this purpose, the Estonian internet voting documentation was thoroughly studied and then voting test environment was set up.

Based on the gained knowledge, a step-by-step analysis of the e-voting system was conducted to find potential vulnerabilities. In the analysis, the preparing the votes for tabulation stage was reached and it was found that there is no simple way to check whether the votes have been manipulated or not.

A solution was proposed to address this issue, which adds comprehensive control mechanisms to ensure that all votes present in the original ballot box are accounted for, either among the cancelled votes or among those going to be counted. Finally, the validation of the solution was carried out, during which the correctness of the solution and the possibility of its use in real elections were verified. This proposed solution was presented to the Election Commission, who approved it, and it is expected to be included as part of the auditor application for the 2024 elections.

The thesis is written in Estonian and is 30 pages long, including 6 chapters, 14 figures and 1 table.

Lühendite ja mõistete sõnastik

Base64	Kodeerimisskeem, kus binaarandmetele pannakse vastavusse kuvatavad tähemärgid
JSON	*JavaScript Object Notation*, JavaScriptil põhinev andmevahetusvorming
Miksimine	Protsess, mille käigus hääled krüpteeritakse ringi, ilma et nende avakuju muutuks
OCSP	*Online Certificate Status Protocol*, kehtivuskinnitusteenus
PKI	*Public key infrastructure*, Avaliku võtme taristu
ZIP	Arhiveerimise failiformaat
Terviklus	Teabe omadus, mis näitab, et seda ei ole volituseta muudetud ega hävitatud

Sisukord

Jooniste loetelu

Tabelite loetelu

1. Sissejuhatus

Kodanikuks olemise osaks on võimalus osaleda valimistel, mis ikka ja jälle iga paari aasta tagant toimuvad. Olgu selleks siis Eesti mõistes Riigikogu valimised, kohaliku omavalitsuse volikogu valimised või Euroopa Parlamendi valimised. Traditsiooniliselt toimuvad valimised jaoskondades, kasutades pabersedeleid, kuid Eestis on alates aastast 2005 kasutusel selle kõrval e-hääletamine, kus hääle saab anda kodust lahkumata interneti teel [1].

Kuid vaatamata sellele, et Eestis on juba nii pikalt e-hääletamine kasutusel olnud, oleme ikkagi ainus riik maailmas, kus üleriigiliselt on kõigil kodanikel võimalik kõikidel valimistel anda enda hääl digitaalselt. Mitmed teisedki riigid on väiksemas mahus seda katsetanud, kuid üleriigilisel tasandil pole sellele püsima jäädud, põhjuseks on jäänud turvalisus ja vähene läbipaistvus. [1]

Paberhääletus on kasutusel olnud pikka aega ning selle käigus on välja kujunenud protsessid, kuidas tagada hääletamise salajasus ja auditeerimine, ning tavainimese jaoks on see arusaadav. E-hääletamise korral aga puudub traditsiooniline võimalus hääle liikumise jälgimiseks selle andmisest kuni lugemiseni. Seetõttu on oluline, et oleks paigas kindlad auditeerimise protsessid, mis tagaksid hääletamise korrektsuse ja läbipaistvuse. Üheks heaks näiteks on Helios, mis on sarnane Eestis kasutusel olevaga, ning selle puhul on tegemist avalikult otsast lõpuni auditeeritava valimiste süsteemiga [2]. Eesti e-hääletamise süsteemis pole keegi aga otsast lõpuni auditeeritavust tõestanud.

1.1 Eesmärk

Antud töö eesmärgiks on kontrollida, kas ebaausatel korraldajatel on võimalik keskserveris hääli nii välja vahetada, et vaatlejad ega audiitorid seda ei märka. Kindlasti ei soovi me antud tööga süüdistada kedagi ebaaususes või väita, et on toimunud valimispettus. Ideaalis võiks e-hääletamise süsteem olla nii tehtud, et ei peaks riistvara, tarkvara ega korraldajaid usaldama, vaid kõik oleks andmete põhjal hiljem piisavalt kontrollitav ja auditeeritav, et välistada kõik manipuleerimised. Selle viimaseni jõudmine ei ole antud töö eesmärgiks, töö eesmärgi täitmiseks võib juba lugeda seda, kui õnnestub viia olemasolev süsteem sellele sammu võrra lähemale. Kui töö tulemusena peaks leidma, et kõik juba on andmete põhjal kontrollitav ja auditeeritav, siis saab ka selle lugeda positiivseks tulemuseks.

Eesmärgi saavutamiseks tuleb lahendada järgmised alaeesmärgid:

1. Mõista Eestis kasutusel olevat e-hääletamise lahendust
2. Vaatama, mis on tehtud, varasemad leiud
3. Katsekeskkonna loomine
4. Kõikide sammude auditeeritavuse ja vaadeldavuse kontrollimine
5. Pakkuda lahendused leitud puudustele
6. Pakutud lahenduse valideerimine

1.2 Ülesehitus

Töö alguses antakse ülevaade Eestis kasutusel olevast e-hääletamise lahendusest. Seejärel pannakse püsti katsekeskkond, et lähemalt tutvuda antud süsteemiga ja et oleks olemas koht, kus katseid läbi viia.

Järgmiseks viiakse läbi hetkeseisu analüüs, tuginedes varasematele teiste poolt leitud tulemustele ja enda kogutud teadmistele. Valimiste süsteem võetakse samm-sammult ette, mille käigus vaadatakse, mis kaitsemehhanisme kasutatakse, kuidas auditeeritakse, ja üritatakse leida võimalikke ründekohti.

Edasises osas pakutakse leitud probleemile lahendus, mis lisaks täiendavaid kontrollmehhanisme süsteemi paremaks auditeerimiseks. Viimaks tuleb pakutud lahendus valideerida, veendumaks lahenduse töökindluses ja kiiruses.

2. Ülevaade e-hääletamise süsteemist IVXV

Antud peatükis luuakse ülevaade Eesti valimistel kasutusel olevast süsteemist IVXV. Selleks kasutatakse Elektroonilise hääletamise üldraamistikku [3], Sven Heibergi teadusartiklit "Improving the Verifiability of the Estonian Internet Voting Scheme" [4] ja e-hääletamise arhitektuuridokumenti "IVXV arhitektuur" [5].

Valimiste protsessi vaadatakse etappide kaupa, kuna see kirjeldab protsesse loogilises järjestuses ja teeb arusaadavamaks, milliseid ülesandeid vastavad komponendid süsteemis täidavad. Korralduslikult jaguneb e-hääletamine neljaks etapiks: hääletamiseelne etapp, hääletamisetapp, töötlusetapp ja lugemisetapp [3]. Enne praeguse süsteemi juurde jõudmist vaadatakse põgusalt otsa ajaloole, et mõista paremini algset loogikat ja kasutatud turvaelemente. Lisaks vaadatakse, mis on jäänud aastate jooksul samaks ja mis on hiljem juurde poogitud.

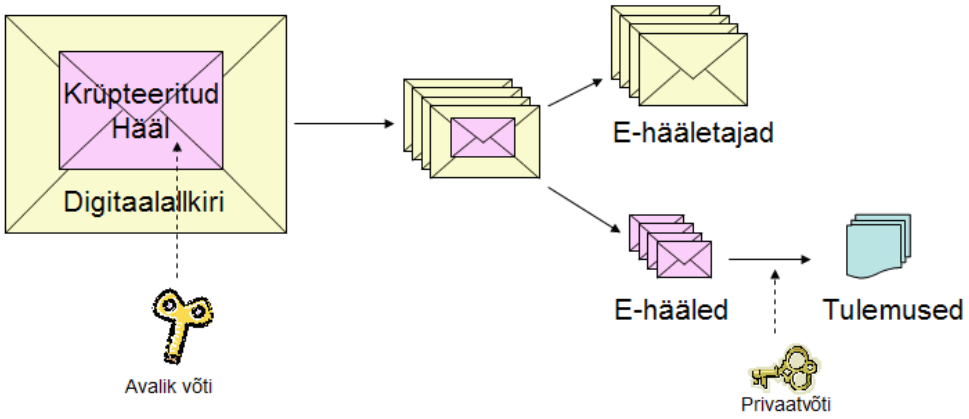
2.1 Ajalugu

Esmakordselt kasutati Eestis e-hääletamist 2005. aasta kohaliku omavalitsuse volikogu valimistel [1], millega sai Eestist esimene riik maailmas, kus interneti kaudu sai hääletada üleriigilistel valimistel [4].

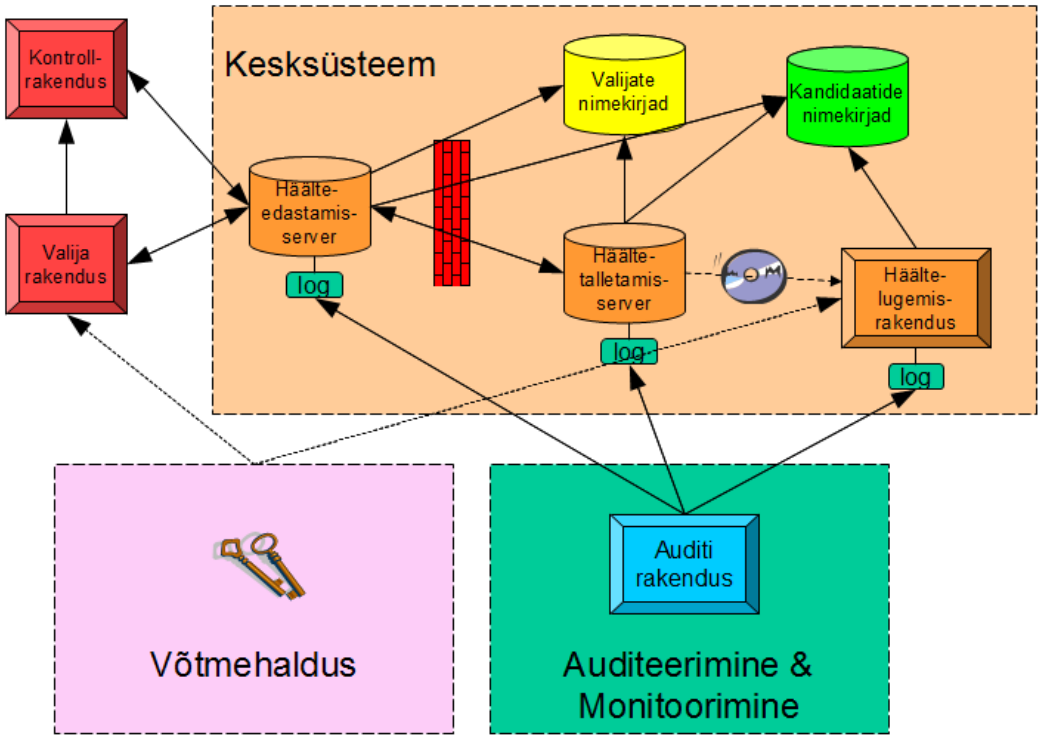
Süsteemi loomise aluseks võeti sarnane ümbrikuskeem, mida kasutati sellel ajal eelhääletamisel, kui kodanik soovis hääletada väljaspool enda elukoha järgset valimisringkonda. Esmalt identifitseerib hääletaja ennast dokumendi alusel valimiskomisjonile, seejärel täidab hääletaja valimissedeli ja paneb selle puhtasse ümbrikusse. See ümbrik pannakse omakorda teise ümbrikusse, kuhu peale kirjutatakse hääletaja andmed. Seejärel toimetatakse ümbrik hääletaja elukohajärgsesse valimisjaoskonda, kus veendutakse hääletaja hääleõiguses ja kui kõik on korras, eemaldatakse välimine ümbrik ning sisemine puhas ja anonüümne ümbrik pannakse valimiskasti. [6]

E-hääletamise puhul on tegemist valijarakendusega, kus kasutaja peab esmalt ennast ID-kaardiga identifitseerima ja saab seejärel teha enda valiku, kelle poolt hääletada. Tehtud valik krüpteeritakse ja tegemist on nii-öelda puhta ümbrikuga, kus hääletajaga seotud andmeid küljes ei ole. Seejärel antud krüpteeritud hääl allkirjastatakse, mille käigus pannakse külge hääletaja andmed. Nüüd on tegemist nii-öelda välimise ümbrikuga. Allkirjastatud hääl edastatakse valimiste serverisse, mis kogub kokku kõik antud hääled, kontrollib hääle-

tajate õigust hääletamiseks ning eemaldab hääled, mis korduvad või mida polnud õigus anda. Seejärel eemaldatakse välimine allkirjastatud ümbrik ja sisemised krüpteeritud hääled kogutakse kokku. Krüpteeritud hääled lähevad lugemisele, mille käigus need avatakse privaatvõtmega ja summeeritakse kokku. Saadud tulemus tehakse avalikkusele teatavaks. Kasutatud ümbrikuskeem on toodud Joonisel 1 ja süsteemi enda arhitektuur Joonisel 2, kuid tuleb välja tuua, et Kontrollrakendust ei olnud kohe alguses olemas, vaid see lisati juurde hiljem. [6, 7]



Joonis 1. 2005-2015 kasutusel olnud ümbrikuskeem. [7]



Joonis 2. 2005-2015 kasutusel olnud e-hääletamise süsteemi üldarhitektuur. Kontrollrakendus lisati 2013. [7]

Esialgses süsteemis oli eelduseks, et kasutaja arvuti turvalisuses saab kindel olla, seal ei eksisteeri midagi, mis võiks hääletamise protsessiga manipuleerida. Aastaks 2011 oli aga

selge, et see eeldus enam ei kehti. Nimelt oli üks tudeng valmis saanud prototüübi, mis oli võimeline manipuleerima hääletaja arvutis oleva valimisrakendusega, andes hääletaja poolt hääle kellelegi teisele, samal ajal jättes mulje, et hääl läks sellele, kellele see mõeldud oli [8]. Seetõttu lisati 2013. aasta valimisteks juurde võimalus hääletajal veenduda enda hääle korrektsest jõudmisest valimiste serverisse, kasutades selleks eraldiseisvat telefonirakendust hääle kontrollimiseks. [9]

Suuresti oli vanema süsteemi turvalisuse eelduseks usaldus kesksüsteemi vastu. Paigas olid kontrollmehhanismid selle tagamiseks, kuid jäid küsitavaks, kas need on ikka piisavad. 2013. aasta valimisi käis vaatlemas uurimisgrupp Michigani ülikoolist, kes leidsid hulga puudujääke protseduurides ja tõid välja hulganisti võimalikke ründekohti [10]. Eesmärgiks sai Eesti e-hääletamine ümber kujundada, et see sõltuks vähem inimfaktorist, teeks süsteemi rohkem sõltumatult auditeeritavaks ja võimaldaks süsteemi jagada erinevate organisatsioonide vahel laiali. [4]

Sellest sündis uus Eesti e-hääletamise süsteem koodnimega IVXV, mis on kasutusel valimistel alates aastast 2017. Lisati juurde eraldi audiitori roll, kes saab kontrollida, et kõik protseduurid on läbi viidud nõuetekohaselt. Häälte serverist kadumise vastu võeti juurde kolmas osapool, Registreerimisteenus, kelle ülesandeks on pidada arvet häälte üle, mis on keskserverile üle antud. Uus skeem peaks olema piisavalt kontrollitav ja väidetakse, et Eesti e-hääletamises on saavutatud otsast lõpuni kontrollitavus. Kui vastav väide paika peab, siis ei tohiks me antud töö käigus midagi leida. [4]

2.2 Hääletamiseelne etapp

Igaks valimiseks pannakse e-hääletamise süsteem püsti nullist lähtuvalt konkreetsetest valimistest. Seda tehakse enne e-hääletamise algust ning kogu protsessi nimetatakse hääletamiseelseks etapiks. Antud etapi põhiülesandeks on valmis seada kogu e-hääletamise süsteem, et kodanikel oleks võimalik hääletamisest osa võtta kasutades elektroonilist hääletamist interneti teel.

Hääletamiseelse etapi ajal koostatakse ringkondade, jaoskondade, kandidaatide ja valijate nimekirjad. Selle käigus genereeritakse konkreetse hääletuse tarbeks hääle salastamise võti (avalik võti) koos häälte avamise võtmega (privaatvõti) ning seadistatakse kogumisteenus, mille kaudu hääli kokku kogutakse, ja pakendatakse valijarakendus, mille kaudu saavad valijad e-hääletamisest osa võtta. Lisaks toimub antud etapis katsehääletus, mille käigus veendutakse, et kõik toimib nii nagu peab. [3], [5], [11]

2.2.1 Võtmehaldus

Võtmete genereerimine koos sinna juurde kuuluvaga on e-hääletamise süsteemi üks kriitilisemaid kohti, millest sõltub hääletamise salajasus, mis on üks valimiste põhinõuetest [3].

Hääletamise salajasus tagatakse asümmeetrilise krüptograafia vahendite abil, kus hääl krüpteeritakse kasutades häälte salastamise võtit ja hiljem avatakse kasutades häälte avamise võtit. Võtmed genereeritakse kasutades ElGamal krüptosüsteemi. Häälte salastamise võti on avalik ja see pakendatakse koos valimisrakendusega, mida hiljem valimisrakendus kasutab häälte krüpteerimiseks. Kuna häälte avamise võtmega on võimalik kõik hääled dekrüpteerida, jaotatakse see tükkideks kasutades Shamir osakujagamist. Iga tükk kirjutatakse eraldi kiipkaardile, mis jaotatakse määratud inimeste vahel laiali. Seda tehakse selleks, et häälte avamine oleks võimalik vaid siis, kui protseduur seda ette näeb, häälte lugemise faasis, ja selleks peavad osakute haldajad kokku tulema. See tagab hääletamise salajasuse, et ei oleks võimalik varasemalt hääli avada ja teada saada, kes kelle poolt hääletas. [3], [12]

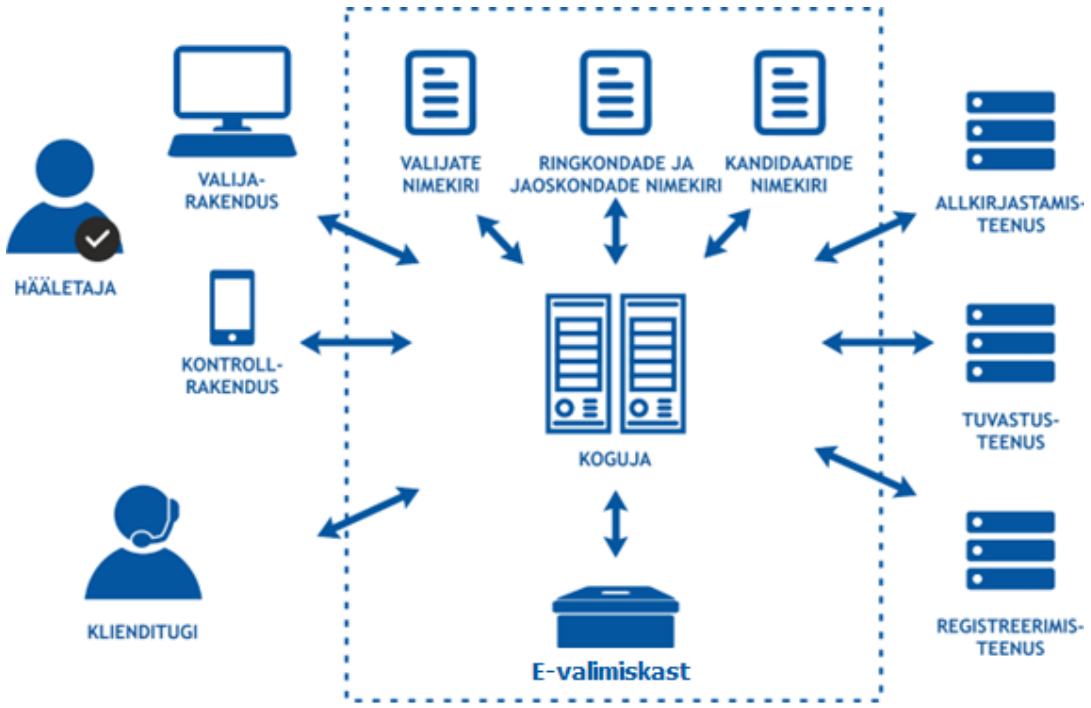
2.3 Hääletamisetapp

Hääletamisetapp toimub eelhääletamise ajal, millal on võimalik osa võtta e-hääletamisest. Valija saab hääletada korduvalt, nii palju, kui tahab, kuid arvesse läheb ainult viimasena antud hääl. Samal ajal toimub pabersedeliga hääletamine jaoskondades, tagamaks kõigile võimaluse hääletamiseks kasutada endale sobivat varianti. Kui hääletaja kasutab mõlemat valimise viisi, siis e-hääletamise teel antud hääl tühistatakse ja arvesse läheb vaid pabersedeliga antud hääl

E-hääletamise korral kasutavad hääletajad valijarakendust, mis suhtleb kogumisteenusega, vahetades informatsiooni nende vahel. Hääletamisetapi osapooled on toodud Joonisel 3. Edasi vaadatakse lähemalt ülesandeid, mida täidavad valijarakendus ja koguja.

2.3.1 Valijarakendus

Valijarakendust kasutades on võimalik hääletajale teha valik, kelle poolt enda hääl anda. Rakenduse kasutamiseks tuleb esmalt hääletajal ennast autentida, kasutades selleks kas ID-kaarti või mobiil-IDd. Seejärel saab valijarakendus koogumisteenuselt hääletaja elukohale vastava kandidaatide nimekirja, kelle vahel on võimalik enda valik teha. Hääletaja teeb võimalike kandidaatide seast valiku, mis seejärel krüpteeritakse valijarakenduse poolt. Krüpteerimiseks kasutatakse eelnevalt rakendusse kaasa pandud hääle salastamise võtit ja



Joonis 3. Hääletamisetapi osapooled. [3]

juhuarvu, mille valijarakendus genereerib iga krüpteerimise jaoks uue. Krüpteeritud hääl allkirjastatakse hääletaja poolt ja edastatakse koos allkirjastamise sertifikaadiga kogumisteenusele. Kui hääl on edukalt kogumisteenuse poolt vastu võetud, teavitatakse kasutajat ja hääletajale kuvatakse QR-kood, mis sisaldab krüpteerimisel kasutatud juhuarvu ja kogumisteenuse poolt genereeritud hääle identifikaatorit. Selle QR-koodi alusel on võimalik hääletajal, kasutades kontrollrakendust, kontrollida enda hääle jõudmist kogumisteenusesse ja veenduda, et hääles sisalduv valik on ikka see, mis seal olema peab. [3]

2.3.2 Kogumisteenus

Kogumisteenuse puhul on tegemist serverisüsteemiga, mis aitab valijarakenduse kaasabil hääletajal e-hääle moodustada [3]. Joonisel 3 on kogumisteenus välja toodud keskse komponendina Koguja nime all.

Hääletaja kasutab kogumisteenusega suhtlemiseks valijarakendust. Esmalt kasutaja tuvastatakse, selleks võib vajadusel kasutada välist tuvastusteenust, vajalik näiteks mobiil-IDga autentimise korral. Tuvastatud kasutaja hääleõigust kontrollitakse valijate nimekirjast ja sealt leitakse ka kasutaja valimisringkond, vastavalt millele edastatakse hääletajale vastava ringkonna kandidaadid. [3], [5]

Peale hääletajapoolseid toiminguid valijarakenduses, edastatakse kogumisteenusele krüp-

teeritud ja allkirjastatud hääl. Kogumisteenus kontrollib veelkord hääletaja eksisteerimist valijate nimekirjas, seejärel küsib allkirjastamisel kasutusel olnud sertifikaadile kehtivuskinnituse ja talletab selle koos häälega. Viimase eesmärgiks on kontrollida, et hääletaja sertifikaadid kehtivad hääle andmise hetkel. Edasi registreeritakse hääl välise Registreerimisteenuse juures ja sealt saadud kinnitus talletatakse samuti kogumisteenuses hääle juures. [3]

Lõpuks teavitab kogumisteenus valijarakendust hääletaja hääle edukast vastuvõtmisest ja talletamisest. Valijarakendusele edastatakse hääle identifikaator, mida saab kontrollrakendus kasutada hiljem hääle kontrollimise käigus. Selle alusel saab kontrollrakendus kogumisteenuse käest allkirjastatud hääle. Teades lisaks hääle salastamise võtit ja juhuarvu, millega hääl krüpteeriti, saab kontrollrakendus hääle avada ja hääletajale kuvada, kelle poolt on hääl antud. Hääletamisetapi lõpus edastab kogumisteenus kõik hääled koos sinna juurde kuuluvate kehtivuskinnituste ja registreerimistõenditega töötlemiseks. [3]

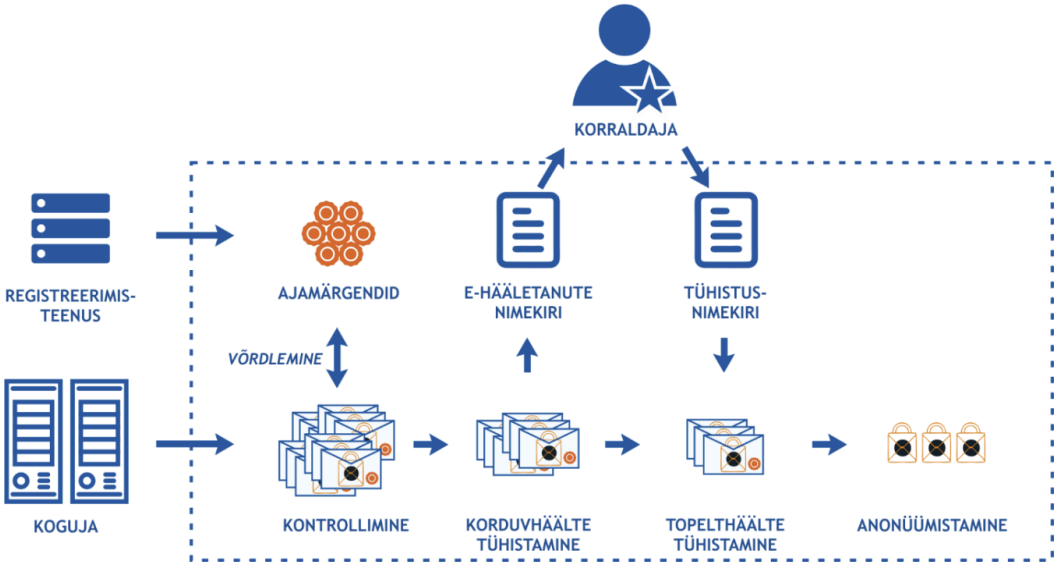
2.3.3 Registreerimisteenus

Registreerimisteenus on kolmas osapool, kelle juures registreeritakse kõik kogumisteenuse poolt vastu võetud hääled. Kinnituse jaoks, et registreerimispäring on kätte saadud, vastatakse päringuga, mis on omakorda allkirjastatud registreerimisteenuse sertifikaadiga. Registreerimisteenus on kohustatud hoidma kõik registreerimispäringud alles hilisemaks auditeerimiseks. Antud teenust peaks valimistel pakkuma kolmas sõltumatu osapool [5]. Teoorias on võimalik, et kogumisteenuse ja registreerimisteenuse koostöö korral oleks võimalik hääli ära unustada. Registreerimisteenus asendab niiöelda avalikku teadetetahvlit, mis on näiteks Heliosel [2] selleks, et saaksime kindlad olla, et kõik hääled jõudsid ikka valimiskasti, mis sinna teele pandi.

2.4 Töötlusetapp

Töötlusetapi eesmärgiks on kogumisteenuselt kõik saadud hääled üle kontrollida ja eemaldada korduvhääled, vigased hääled ja jaoskonnas pabersedeliga ülehääletanute hääled. Ülevaade töötlusetapist on toodud Joonisel 4. Lõplik väljund läheb edasi lugemisetappi. [3]

Töötlusetapi sisendiks on kogumisteenuselt saadud valimiskast, mis sisaldab endas kõiki hääli koos sinna juurde kuuluvate kehtivuskinnitustega ja registreerimistõenditega. Lisaks saadakse registreerimisteenuselt kõik registreerimistõendid (ajamärgendid). Esmalt kontrollitakse valimiskasti terviklust. Selle kõigus kontrollitakse allkirjade kehtivust ja selleks kasutataud sertifikaadi kehtivuskinnitust. Seejärel kontrollitakse, kas hääle küljes



Joonis 4. Häälte töötlemise etapid. [3]

olev registreerimistõend on olemas ja klapib sellega, mis saadi registreerimisteenuse käest. Vigased hääled logitakse ja nendega tegeletakse eraldi. [3]

Järgmisena sorteeritakse kõik ühe ja sama isiku poolt antud hääled ajalises järjestuses ja eemaldatakse kõik korduvad hääled peale viimase. Seejärel eemaldatakse valijate hääled, kes lisaks elektrooniliselt hääletamisele hääletasid ka jaoskonnas paberi peal. Viimase sammuna võetakse krüpteeritud häältelt ümbert ära allkirjastatud konteiner ja saadakse anonüümsed hääled. Lisaks on veel miksimine, mis on valikuline, kus hääled segatakse ja rekrüpteeritakse ringkondade kaupa, ilma et nende sisu muutuks. Vajalik on see selleks, et lugemisele läinud hääli ei oleks võimalik enam siduda esialgse häälega ja tagada sellega valimiste salajasus. [3]

2.5 Lugemisetapp

Lugemisetapp on e-hääletamise läbiviimise viimane etapp. Antud etapi sisendiks on töötlusetapis töödeldud anonüümistatud hääled. Esmalt hääled dekrüpteeritakse, selleks peavad kokku tulema eelnevalt määratud isikud, kellele jaotati kiipkaardid võtmeosakutega. Dekrüpteeritud hääled loetakse kokku ning summeeritakse kandidaatide ja ringkondade kaupa. Kombineerides need pabersedeliga hääletamise tulemustega, saadakse kokku lõplikud valimiste tulemused. [3]

3. Katsekeskkonna loomine

Käesoleva peatüki eesmärgiks on püsti panna töötav e-hääletamise katsesüsteem, saamaks parem ülevaade e-hääletamise süsteemist ja selle toimimisest. Lisaboonusena oleks olemas koht, kus viia läbi erinevaid katseid. Süsteemi püsti paneku aluseks on e-hääletamise tarkvara lähtekood, mis on tehtud avalikult kättesaadavaks GitHub repositooriumis[1]. Lisaks kasutatakse e-hääletamise dokumentatsiooni[2], et seda teha võimalikult täpselt, nagu valimiskomisjon on ette näinud.

3.1 Avaliku võtme taristu

Eesti e-hääletamine on ülesse ehitatud suuresti juba olemasolevale riiklikule avaliku võtme taristule (*Public Key Infrastructure*, PKI), mille juurde kuulub tugev krüptograafiline autentimistõend (*authentication token*), mida tuntakse kui ID-kaarti. Tegemist on dokumendiga, mis sisaldab sertifikaate enda elektrooniliseks autentimiseks ja digitaalse allkirja andmiseks. [1]

Kuna katsetamiseks on keeruline päris ID-kaarte kasutada, otsustati teha lihtsustatud variant riigis kasutusel olevast avaliku võtme taristust. E-hääletamise katsekeskkonna jaoks implementeeriti minimaalne osa avaliku võtme taristust, mis täidab vajalikud nõuded: sertifikaatide väljaandmine, sertifikaatide kehtivuse kontrollimine ja digiallkirjastamine.

PKI jaoks vajalike sertifikaatide väljaandmine ning sinna juurde kuuluvate teenuste lahendused said loodud kasutades Python[3] programmeerimise keelt. Keelevaliku aluseks sai töö autori varasem kogemus antud keelega ja laialdane teekide olemasolu, mis lihtsustavad PKI implementeerimist.

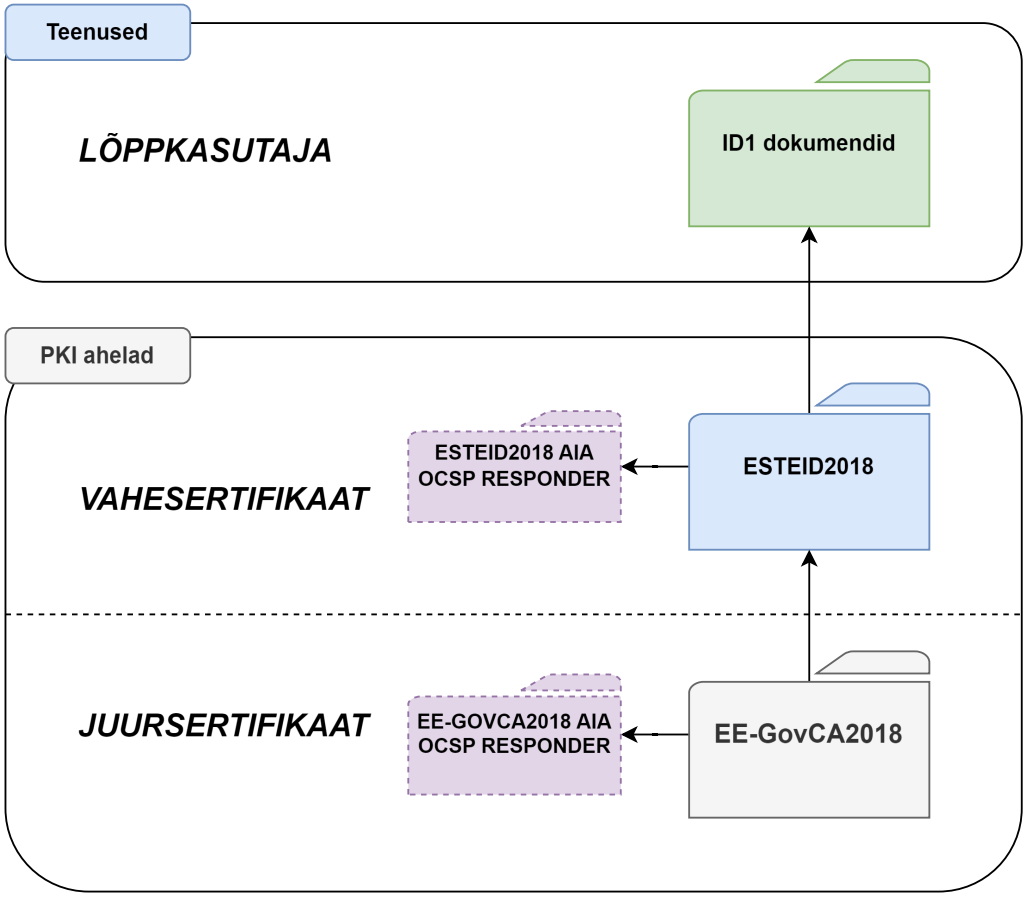
3.1.1 Sertifikaadid

Avaliku võtme taristu aluseks on sertifikaadid, mida kasutatakse erinevate toimingute jaoks nagu uute sertifikaatide väljaandmine, enda autentimine ja digitaalsete allkirjade andmine. Selleks, et kõik toimiks võimalikult sarnaselt riigis kasutusel oleva süsteemiga, võeti aluseks Eestis kasutusel olev sertifikaatide hierarhiline struktuur (Joonis 5).

[1] `https://github.com/valimised/ivxv`
[2] `https://www.valimised.ee/et/e-haaletamine/dokumendid`
[3] `https://www.python.org`

Vastavalt sellele luuakse juursertifikaat (EE-GovCA2018), mis on PKI sertifikaadi hierarhia aluseks, ja kõik sertifikaadid, mis välja antakse, tulenevad sellest. Juursertifikaadi poolt allkirjastatakse ID-kaardi sertifikaate välja andev sertifikaat (ESTEID2018), mis omakorda allkirjastab kõik inimestele välja antavad sertifikaadid (ID1 dokumendid). Kõik sertifikaadid on üritatud teha päris sertifikaatidega võimalikult sarnase konfiguratsiooniga.

Igale virtuaalsele inimesele luuakse kaks sertifikaati, esimene elektrooniliseks allkirjastamiseks ja teine autentimiseks, nagu on kasutusel ka ID-kaardi puhul. Sertifikaatide genereerimiseks on kasutatud Pythonit koos cryptography[1] teegiga.



Joonis 5. Sertifikaatide hierarhia (EE-GOVCA2018 CHAIN (2018 – 2033)).[2]

Kuna testkeskkonna puhul ei ole sertifikaatide turvalisus oluline, siis talletatakse salajane võti koos sertifikaadiga kasutaja arvutis. ID-kaardi puhul hoitakse salajane võti ID-kaardil ja seda sealt kätte saada ei ole võimalik.

[1] https://github.com/pyca/cryptography
[2] https://www.skidsolutions.eu/resources/certification-hierarchy

3.1.2 OCSP kehtivuskinnitus

Kui sertifikaadid välja antakse, on neil konkreetne kehtivuse aeg. Eestis kasutusel oleva ID-kaardi sertifikaadid kehtivad sama kaua kui dokument ise, milleks on viis aastat. Kui peaks juhtuma, et sertifikaate oleks vaja tühistada enne nende päris kehtivuse lõppu, näiteks ID-kaardi varguse korral, kasutatakse selleks OCSP (*Online Certificate Status Protocol*) teenust, mille käest saab küsida, kas vastav sertifikaat kehtib või on mingil põhjusel tühistatud.

E-hääletamise juures kasutab kogumisteenus OCSP teenust veendumaks, et hääl allkirjastati kehtiva sertifikaadiga. Seega tuleb teha vastav teenus ka katsekeskkonna jaoks.

OCSP teenuse jaoks genereeriti juursertifikaadi poolt allkirjastatud sertifikaat, mida OCSP server kasutab enda vastuste allkirjastamiseks. OCSP server sai autori poolt loodud kasutades Pythonit koos selle sama cryptography teegiga. Uuriti ka olemasolevaid lahendusi OCSP serveri jaoks, kuid need jäid kasutusest välja, kuna hääletamise ajal kasutatakse *nonce* veergu, mis on pikem, kui standard ette näeb, mistõttu ükski olemasolev vabavaraline OCSP server ei osanud vastata nendele päringutele. Ka cryptography teegis olevad OCSP meetodid ei toetanud pikemat *nonce* välja, kuid seal sai vähese vaevaga vastava toe juurde lisada. *Nonce* välja puhul on tegemist üldiselt juhusliku genereeritud arvuga, mis lisatakse sõnumile, et eristada kahte erinevat identset sõnumit. Lisaks kasutatakse seda näiteks taasesitus rünnete (*replay attack*) vastu, saamaks aru, et antud päringuga on juba tegeletud. E-hääletamise puhul pannakse *nonce* veerule krüpteeritud hääle allkirja räsi [13].

3.1.3 Digiallkirjastamine

E-hääletamise puhul tuleb kõik konfiguratsioonid, mis erinevatele programmidele ja teenustele ette antakse, digiallkirjastada. Kuna PKI on enda loodud, ei saa kasutada allkirjastamiseks olemasolevat DigiDoc4 klient[1] tarkvara, kuna see toimib ainult ID-kaardi, mobiil-ID ja Smart-IDga. Lahenduse loomiseks kasutati juba eelnevalt kasutusel olnud Pythonit koos cryptography teegiga, kuid juurde lisati pyasice[2] teek, mis lihtsustab allkirjastatud konteinerite loomist.

[1] `https://www.id.ee/rubriik/digidoc4-klient`
[2] `https://github.com/thorgate/pyasice`

3.2 Konfiguratsiooni genereerimine

Selleks, et valimiste süsteemi komponendid teaksid, mis tegema peavad, tuleb luua igale komponendile vastav konfiguratsioon. Seadistus koostatakse lähtuvalt IVXV seadistuste koostamise juhendile [12]. Kasutatav formaat seadistustes on YAML[1], näidis valimiste üldisest seadistusest kogumisteenusele on toodud Joonisel 6. Kõik loodud konfiguratsioonid tuleb digitaalselt allkirjastada, selleks kasutatakse eelnevalt loodud virtuaalse inimese allkirjastamise sertifikaati ja digiallkirjastamise lahendust.

```
identifier: TESTCONF
questions:
  - TESTQUESTION

period:
  servicestart:   2017-01-16T08:50:00+02:00
  electionstart:  2017-01-16T09:00:00+02:00
  electionstop:   2017-01-18T19:00:00+02:00
  servicestop:    2017-01-18T19:15:00+02:00

voting:
  ratelimitstart:   50
  ratelimitminutes: 5

verification:
  count:      3
  minutes:    30
  latestonly: false

voterlist:
  key: !container rr_pub.key
```

Joonis 6. Valimiste seadistuse yaml faili näide.

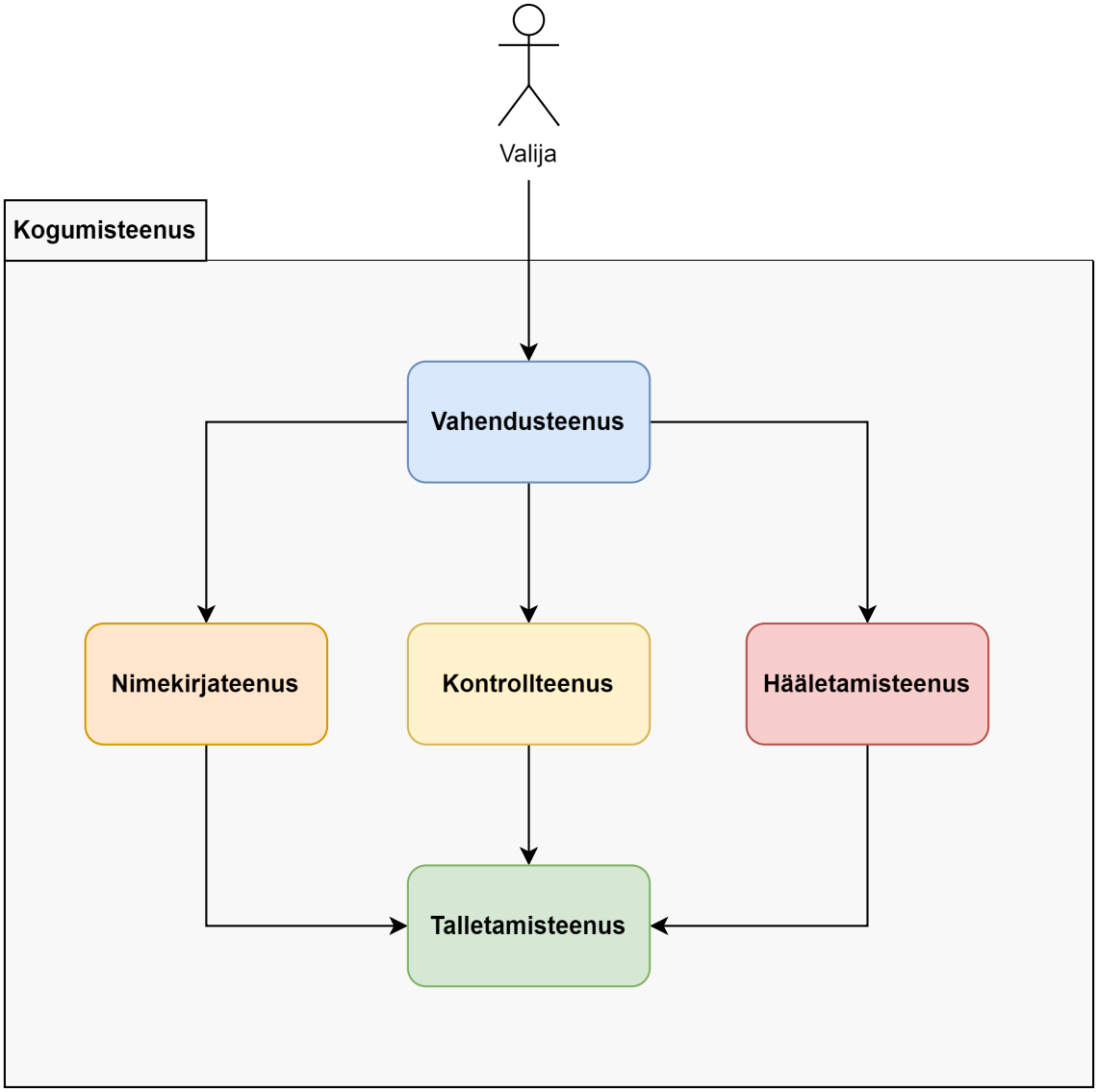
3.3 Kogumisteenuse püstitamine

Serverite püstitamine tehti vastavalt e-hääletamise käsiraamatule [11] ja kogumisteenuse haldusjuhendile [14]. Serveriteks kasutatakse operatsioonisüsteemi Ubuntu[2], mida näeb ette kogumisteenuse haldusjuhend. Serverite majutamiseks kasutatakse Hyper-V virtualiseerimise tarkvara, kuna töö autor kasutab Windows operatsioonisüsteemiga arvutit, mis juba sisaldab antud tarkvara. Tühjad serveri keskkonnad luuakse kasutades Vagrant[3] tarkvara, mis lihtsustab virtuaalserveri paigaldamist, pakkudes valmisolevaid keskkondi erinevate operatsioonisüsteemidega. Virtuaalservereid sai tehtud kaks, kuna üks neist peab vastavalt dokumentatsioonile olema haldusteenuse jaoks ja teine jääb kasutamiseks kogumisteenusele [14].

[1] https://yaml.org
[2] https://ubuntu.com
[3] https://www.vagrantup.com

Valimiste süsteem on loodud kasutades mikroteenuste arhitektuuri (Joonis 7). Mikroteenuste arhitektuur lihtsustab ressursi juurde andmist kohtadesse, mille koormus on valimiste ajal suurem.

Paigaldamiseks tuli kompileerida lähtekoodist haldusteenus ja kogumisteenus. Haldusteenust kasutatakse kogumisteenuse juhtimiseks ja paigaldamiseks [14]. Haldusteenus paigaldati neist ühte virtuaalmasinasse ja seejärel laaditi haldusteenusele peale seadistuste pakid. Selle põhjal paigaldab haldusteenus kogumisteenuse koos kõige sinna juurde kuuluvate mikroteenustega. Peale seadistuste ja vajalike nimekirjade peale laadimist on süsteem kasutusvalmis.



Joonis 7. Kogumisteenuse jaotus mikroteenusteks.

3.4 IVXV rakendused

E-hääletamise puhul kasutatatakse võtmete genereerimiseks, häälte töötlemiseks ja kokkulugemiseks ning auditeerimiseks erinevaid rakendusi. Nende puhul on tegemist käsurealiidesega programmidega, mis ei vaja töötamiseks serveri olemasolu. Kõik rakendused on kirjutatud Java[1] programmeerimise keeles. Rakendused kompileeriti avalikust lähtekoodist, mis asub IVXV repositooriumis.

3.4.1 Võtmerakendus

Võtmerakenduse ülesandeks on luua häälte salastamise võti ja häälte avamise võti. Originaalis jagatakse häälte avamise võti osakuteks ja need osakud kirjutatakse kiipkaartidele. Kuna käepärast ei olnud kiipkaarte, millele saaks neid osakuid kirjutada ning katsekeskkonnas pole häälte avamise võtme turvamine oluline, otsustati võtmerakenduse koodi vastavalt muuta, et kiipkaartide asemel kirjutatakse osakud arvuti kõvakettale.

3.5 Valijarakendus

Kuigi suures osas on valimiste lähtekood tehtud avalikuks, siis valijarakenduse kood ei ole avalik ja see tuleb ise implementeerida. Selle loomise aluseks võetakse IVXV protokollide kirjeldus [13].

Valijarakendus luuakse võimalikult lihtne, millega oleks võimalik hääl edastada kogumisteenusele. Kogumisteenus vajab kasutaja autentimist, selleks antakse valijarakendusele ette eelnevalt loodud virtuaalse kodaniku autentimise sertifikaat ja sellele vastav salajane võti, mis pannakse kaasa päringutesse, mis tehakse kogumisteenusele.

Esmalt küsitakse kogumisteenuselt valikute nimekiri, mis sisaldab kodaniku elukohale vastava valimisringkonna kandidaatide nimekirja. Kogu nimekiri trükitakse välja ja nende vahel saab teha valiku, kelle poolt hääletada. Vastavast valikust koostatakse valija tahteavaldus. Loodud tahteavaldus krüpteeritakse kasutades hääle salastamise võtit koos juhuslikult genereeritud arvuga. Krüpteeritud sedel allkirjastatakse virtuaalse kodaniku allkirjastamise sertifikaadiga. Valijarakenduses toimub allkirjastamine veidi teistmoodi kui tavaline digiallkirjastamine. Seetõttu ei saa kasutada PKI faasis loodud digiallkirjastamise loogikat. Allkirjastamisel ei võeta OCSP teenuse käest kinnitust sertifikaadi kehtivuse kohta ja see jääb allkirjast välja. Antud allkirjastamise sertifikaadi kehtivuse kinnitus võetakse alles kogumisteenuse poolt ja talletatakse allkirjastatud hääle juures.

[1] `https://www.java.com`

Viimaks saadetakse allkirjastatud konteiner kogumisteenusele. Hääle kontrollimiseks vajalikke tulemusi töö käigus loodud valimisrakendus ei kuva, kuna häälte kontrollimise rakendust ja sellega seonduvat käesoleva töö käigus ei uurita.

4. Hetkeseisu analüüs

Töö neljandas peatükis analüüsitakse praegu kasutusel olevat e-hääletamise süsteemi. Selleks võetakse samm-sammult ette e-hääletamise etapid ja vaadatakse, mis turvaelemendid häält kaitsevad, kuidas auditeeritakse ja kas on kohti, mida oleks võimalik potentsiaalseks ründeks ära kasutada. Kuna mitmed e-hääletamise komponendid said ise kirjutatud või muudeti olemasolevaid, siis nendega seotud võimalikke nõrkusi ei võetud arvesse võimalike rünnaku kohtadena. Enne omapoolse analüüsi juurde minekut vaadatakse, mida teised on leidnud ja e-hääletamise lahendusele ette heitnud. Seda selleks, et saada esialgne ülevaade võimalike probleemide kohta, mis võiks aidata leida uusi potentsiaalselt haavatavaid kohti.

4.1 Varasemad leiud

Esimene tõsisem uurimine Eesti e-valimiste turvalisuse kohta tehti Michigani ülikoolist pärit uurimisrühma poolt 2013. aasta kohaliku omavalitsuse volikogu valimiste ajal. Nende leidudest ja katsetest valmis turvaanalüüs [10]. Antud analüüs on tehtud küll e-hääletamise vanema süsteemi peal, mida enam ei kasutata, kuid enne enda analüüsi juurde minekut on hea vaadata, mida vanale süsteemile ette heideti ja kas need on praeguses parandatud. Läbi viidud katsed näitasid võimalikke kliendipoolseid rünnakute võimalusi, kus asendatakse valimisrakendus ja kontrollrakendus ning nende koosmõjul hääletatakse ründajale sobivalt. Serveripoolsete rünnetena toodi välja võimalikke serverite ründamist pahavaraga ja lugemisprotsessi käigus krüpteeritud häälte muutmist enne, kui need tagastatakse lugemisrakendusele kokkulugemiseks. Põhiliseks õppetunniks leiti, et ebaausa korraldaja puhul on väga raske veenduda serveris töötava koodi korrektsuses.

Praeguse valimiste süsteemi kasutuse ajal valmis väliskaubandus- ja infotehnoloogiaministri poolt kokku kutsutud turvalisuse töörühma poolt koondaruanne [15] ettepanekutest, mida võiks teha e-valimiste turvalisemaks muutmiseks. Olulisemateks ettepanekuteks oli viia e-hääletus vastavusse otsast lõpuni kontrollitavuse nõudega, kasutada dubleerivaid tarkvarakomponente häälte kokkulugemise protsessis ja muuta hääle liikumine audiitoritele ja vaatlejatele kogu tsükli ulatuses vaadeldavaks.

4.1.1 ODIHR valimiste eksperdirühma lõpparuanne

2023. aasta riigikogu valimiste kohta valmis ODIHR (Demokraatlike institutsioonide ja inimõiguste büroo) valimiste eksperdirühma lõpparuanne [16]. Antud aruanne vaatleb valimisi üldiselt, kuid selle lõputöö raames vaatame sealt seda osa, mis käsitleb e-hääletamisega seonduvat.

Ühe puudusena toodi välja, et häälte kogumise tarkvara ei kontrolli, kas saadud hääletussedel on kehtiv ja seetõttu on võimalik minna mööda ametlikust hääletamisrakendusest. Kasutades enda loodud lahendust, saab seega esitada valesti vormistatud hääletussedeli, mis võetakse hääletuskasti poolt vastu.

Teiseks toodi välja, et kuigi süsteemi lähtekood on avalikult kättesaadavaks tehtud, ei sisalda see piisavalt juhiseid, kuidas antud tarkvara püsti panna ja kuidas kontrollida, et valimistel kasutatav hääletusrakendus on see sama, mille kood on kättesaadav. Siinkohal töö autor nõustub, et süsteemi püstipanek on tõesti keeruline, kuna juhendites oli palju dokumenteerimata kohti, mis tegid süsteemi tööle saamise ajamahukaks.

Kolmandaks leiti kontrollitavusega seotud puuduseid. Individuaalse kontrollitavuse poole pealt väideti, et kui muuta valijarakendust sedasi, et peale hääletamist jookseks programm kokku täpselt peale hääle edastamist, kuid enne hääletajale kinnituse kuvamist. Kui nüüd kasutaja hääletab uuesti, arvates et esimene hääl ei läinud läbi, saaks programm hääletada endale sobiva kandidaadi poolt, aga kinnituse koha peal saaks näidata valija algse hääle koodi. Kontrollrakendusega häält kontrollides näeb hääletaja nüüd enda esialgset valikut ja saab eeldada, et kõik on korras, teadmata, et see ei ole tegelikult tema kõige uuem antud hääl.

Auditeerimise koha pealt leiti, et sammu, mille käigus eemaldati internetis või valimisjaoskonnas antud häälega ülekirjutatud hääled, ei kontrollitud. See võimaldaks siseringi kuuluval isikul, kes omab piisavalt vahendeid ja suudaks seda teha märkamatult, kontrollida, millised hääled eemaldatakse, ja selle kaudu osaliselt mõjutada tulemusi. Täpsemalt, kuidas seda teha, pole aruandes mainitud.

4.2 Süsteemi võtmepaari genereerimine

Hääletamise süsteemi üheks olulisemaks kriteeriumiks on hääletamise salajasus. Selle tagamiseks kasutatakse asümmeetrilist krüptograafiat. Igaks valimiseks luuakse süsteemi võtmepaar, mis koosneb häälte salastamise võtmest (avalik võti) ja häälte avamise võtmest

(privaatvõti). [3]

Võtmepaari genereerimise protseduuri juures on oluline, et häälte avamise võti peab olema genereeritud ja hoitud turvaliselt. Kui häälte avamise võti õnnestuks kellelgi oma valdusesse saada, saaks ta soovi korral avada kõigi hääletajate hääled enne nende anonümiseerimist, mis tooks kaasa teadmise, kes kelle poolt hääletas. Selle riski minimeerimiseks on süsteemi võtmepaari genereerimine auditeeritav protseduur [11]. Võtmepaar genereeritakse kasutades võtmerakendust, mille lähtekood on tehtud avalikuks. E-hääletamise käsiraamat [11] näeb ette, et võtmerakendust tuleb kasutada võrgust lahti ühendatud arvutis, millelt on eemaldatud sisemised salvestusseadmed, välja arvatud välisele andmekandjale kirjutamist võimaldav seade. Kusjuures mälupulga kasutamine andmevahetuseks on keelatud. Antud arvutis salvestatakse häälte salastamise võti ja võtmerakenduse logid välisele andmekandjale. Logisid saab hiljem kasutada auditeerimiseks ja häälte salastamise võti tuleb pakendada valijarakendusse häälte krüpteerimiseks.

Vastavalt auditile kasutati andmete salvestamiseks DVDd [17], kuid antud sõnastus jätab võimaluse kasutada seadmeid peale mälupulga, mille puhul oleks tegemist salvestusseadmega, kuid mis suudaks lisaks manipuleerida võtmepaari genereerimise süsteemiga. Kui aga järgida kõiki määratud protseduure, siis antud seade ühendatakse alles kõige lõpuks, kui häälte avamise võtmest ei tohiks süsteemis alles olla mitte mingit jälge, ning häälte salastamise võti on avalik informatsioon, mille lekkimine mingit ohtu ei kujuta. Kas seda oleks võimalik kuidagi ründeks ära kasutada jääb antud töö skoobist välja.

Arvuti alglaaditakse väliselt kõvakettalt, mis peaks tagama audiitoritele ja vaatlejatele võimaluse veenduda, et süsteem ei sisalda pahavara, mis võiks häälte avamise võtme kuhugi salvestada. Kõvaketast ennast hoitakse kasutamise välisel ajal pitseerituna, mis peaks tagama selle, et keegi ei saa manipuleerida kõvaketta sisuga. [11]

Häälte salastamise võti ise jagatakse osakuteks ja osakud säilitatakse kiipkaartidel, mis iga kasutamise järel pitseeritakse. Pitseerimine peaks tagama selle, et määratud isikud, kellele kiipkaardid on jagatud, ei saaks muul ajal võtme osakut kaardilt kätte kui viimaks häälte lugemise käigus, kus seda tehakse kontrollitud keskkonnas. [11]

Kõike eelnevat arvesse võttes võib väita, et kui jälgitakse kõiki protseduure korrektselt, siis häälte avamise võtit ei saa kasutada häälte avamiseks väljaspool häälte kokkulugemist.

4.3 Konfiguratsioonid

Hääletamise süsteemi toimimiseks tuleb süsteem ja sellega seotud rakendused seadistada [12]. Seadistamiseks kasutatakse konfiguratsioonifail, mis tuleb allkirjastada. Kogumisteenuse puhul määratakse esialgse seadistamise failiga ära, kelle allkirjaga seadistusi kogumisteenus vastu võtab. Seevastu rakenduste konfiguratsioonifailide allkirjastaja ei ole rangelt määratud, kuid allkirjastaja nime ja isikukoodi näidatakse rakenduse käivitamisel. Kui ette antakse allkirjastamata konfiguratsioonifail, siis rakendus ei tööta. [11]

Auditeerimise käigus on võimalik kontrollida, millised konfiguratsioonid kogumisteenusele peale laaditi ja mis konfiguratsioonidega rakendused käivitati. Samuti on näha, kelle poolt vastavad konfiguratsioonifailid allkirjastati. Vastavalt viimaste valimiste auditeerimise lõpparuandele [17] kontrolliti konfiguratsioonifailide allkirjade olemasolu.

Kuna kõik seadistused tuleb allkirjastada ja on hilisemalt auditeeritavad, siis on vähetõenäoline, et ründamiseks võiks kasutada konfiguratsioonifailidega manipuleerimist. Vastavad muudatused tuleks auditeerimise käigus välja ja allkirja järgi on konkreetselt näha, kes selle taga on.

4.4 Häälte kogumine

Häälte kogumise etapi põhilisteks komponentideks on valijarakendus ja kogumisteenus. Esmalt vaatame kodaniku tahteavalduse koostamist valijarakenduse kaudu ja pärast seda, kuidas tagatakse hääle turvaline hoidmine kogumisteenuse poolt.

Valijarakenduse lähtekood ei ole avalik, seetõttu ei saa veenduda, kas valijarakendus teeb täpselt seda, mida dokumentatsioon ette näeb. Seetõttu ei keskenduta võimalikele ründevõimalustele valijarakenduse kaudu, vaid vaadatakse, kuidas on turvatud valija tahteavaldus, mis koostatakse valijarakenduses ja talletatakse kogumisteenuses kuni töötlemiseni.

Valijarakenduse puhul on tegemist vahekihiga e-hääletaja ja kogumisteenuse vahel, mis aitab hääletajal häält koostada. Kogumisteenuse ja valijarakenduse vahelised päringud on autenditud. Selleks tuleb hääletajal esmalt ennast valijarakenduses autentida ja autentimise informatsioon pannakse päringutesse kaasa. Vastavalt sellele tuvastatakse hääletaja ja kuvatakse vaid talle ette nähtud andmed, kui tal on selleks õigus (peab olema valijate nimekirjas).

Esimese sammuna küsitakse valikute nimekiri, kogumisteenus tuvastab hääletaja ja vas-

tavalt elukohale tagastatakse valimisnimekiri. Saadud nimekirjast teeb hääletaja valiku ja sellest koostatakse valija tahteavaldus. Näidis võimalikust tahteavaldusest on toodud Joonisel 8. Esimesel real on valimisringkonna kood ja vastava valiku kood ringkonnas, joonisel toodud näites vastavalt 0064 ja 0821. Järgmisel real on valiku nimekirja nimi, antud näite puhul erakonna nimekiri, kus kandidaat kandideerib. Viimasel real on konkreetse kandidaadi nimi vastavast valikute nimekirjast. [13]

```
0  0  6  4  .  0  8  2  1
30 30 36 34 2E 30 38 32 31 1F

E  E  S  T  I     R  E  F  O  R  M  I  E  R  A  K  O  N  D
45 45 53 54 49 20 52 45 46 4F 52 4D 49 45 52 41 4B 4F 4E 44 1F

K  A  J  A     K  A  L  L  A  S
4B 41 4A 41 20 4B 41 4C 4C 41 53
```

Joonis 8. Valija tahteavaldus avakujul.

Seejärel krüpteerib valijarakenduse koostatud tahteavalduse. Esmalt genereeritakse juhuarv, mida krüptosüsteem krüpteerimiseks kasutab, ning koos valijarakendusse pakendatud häälte salastamise võtmega krüpteeritakse antud valija tahteavaldus. Oluline on, et juhuarv oleks täiesti juhuslik, kuna teades juhuarvu ja hääle salastamise võtit oleks võimalik hääl dekrüpteerida ilma häälte avamise võtmeta. Hääle avamise võtmega dekrüpteerimise korral ei ole juhuarvu teada vaja.

Krüpteerimine tagab, et enne ametlikku häälte lugemist ei oleks kellelgi võimalik häält lugeda ja juhuslik arv tagab kaitse jõurünnete (*brute-force attack*) vastu. Ilma juhuarvuta oleks valikute hulk väike ja kõigi võimalike valikute läbi katsetamisega oleks võimalik kiiresti teada saada, kelle poolt hääletati. Tuleks lihtsalt võrrelda kõikvõimalikke krüptogramme originaaliga. Kui leitakse vastavus, siis järelikult on tegemist valija tahteavaldusega.

Seejärel krüpteeritud hääl allkirjastatakse kasutaja poolt ja edastatakse kogumisteenusele. Kogumisteenuse kontrollib seejärel hääletaja olemasolu valijate nimekirjas. Järgmiseks kontrollitakse, kas allkirjastamise sertifikaat kehtib. Selleks tehakse päring OCSP teenuse poole ja kehtiva sertifikaadi korral lisatakse sealt saadud kehtivuskinnitus hääle juurde. Enne lõplikku hääle talletamist registreeritakse hääl registreerimisteenuse juures ja sealt saadud kinnitus lisatakse samuti hääle juurde. Kogumisteenus kinnitab valijarakendusele hääle talletamisest ja tagastab hääle unikaalse identifikaatori. Kasutajale kuvatakse QR-kood, mis võimaldab kasutajal kontrollrakenduse abil kontrollida, kas tema hääl on registreeritud ja sisaldab õiget valikut. QR-kood sisaldab hääle unikaalset identifikaatorit, mida kasutatakse hääle küsimiseks registreerimisteenuse käest ja juhuslikku arvu, mida valijarakendus kasutas hääle krüpteerimiseks. Teades krüpteeritud häält, hääle salastamise võtit ja krüpteerimisel kasutatud juhuarvu on võimalik krüpteeritud hääl dekrüpteerida ja

kuvada kasutajale hääle sisu.

Kogumisteenuse poolt häälte talletamine ja nende terviklus on tagatud registreerimisteenuse poolt. Teenuse pakkujaks on sõltumatu kolmas osapool, kelle juures registreeritakse kõik hääled, mis kogumisteenuse poolt vastu võetakse ja talletatakse. See võimaldab kontrollida, et kõik hääled, mis kogumisteenusel on, peavad seal olema ja et hääli ei oleks juurde tekkinud ega kaduma läinud.

Hääle salajasus on tagatud sellisel juhul, kui valijarakendus teeb ainult seda, mida tegema peab, ja ei edasta tehtud valikut või krüpteerimisel kasutusel olevat juhuslikult genereeritud arvu kellelegi kolmandale.

4.5 Häälte töötlemine

Häälte töötlemise etapi sisendiks on kogumisteenuse poolt kogutud hääled koos allkirjastamise sertifikaadi kehtivuskinnitusega ja registreerimisteenuse poolse vastusega. Lisaks tuleb registreerimisteenus käest nimekiri kõikidest nende juures registreeritud häältest, kus iga hääle kohta on see sama vastus, mis on valimiskastis registreerimistõendina.

4.5.1 Valimiskasti sisu

Kogumisteenuse käest saadud valimiskast sisaldab kõiki talletatud hääli koos nende juurde kuuluvate kehtivuskinnitustega ja registreerimistõenditega. Lisaks tuleb eraldi kogumisteenuse poolt kogu valimiskasti pealt arvutatud räsi, mis on digitaalselt allkirjastatud. Töötlusetapi alguses kontrollitakse selle räsi vastavust valimiskastiga. Kui need ei peaks klappima, on teada, et keegi on vahepeal valimiskasti sisuga manipuleerinud.

Valimiskasti enda puhul on tegemist ZIP-failiga, mille näitlikustatud struktuur on Joonisel 9. Antud näites hääletas kodanik isikukoodiga 60001019906 ühe korra ja kodanik 39901019992 kolm korda.

Nagu jooniselt näha, on iga hääle kohta valimiskastis neli faili. Neist .bdoc puhul on tegemist allkirjastatud konteineriga, mis sisaldab endas krüpteeritud häält. Olgu lisaks juurde mainitud, et kui avada antud allkirjastatud konteriner DigiDoc4 kliendiga, siis näidatakse, et allkiri ei ole kehtiv, kuna allkirjast on puudu sertifikaadi kehtivuskinnitus. Valimiskasti puhul hoitakse sertifikaadi kehtivuskinnitust eraldi .ocsp failina. Seejärel .tspreg sisaldab registreerimistõendit ja .version sisaldab hääle andmise ajal kogumisteenuses paikneva valijate nimekirja versiooni. [13]

```
votes.zip
└── votes/
    ├── 60001019906/
    │   ├── 20231104145812345+0200.bdoc
    │   ├── 20231104145812345+0200.ocsp
    │   ├── 20231104145812345+0200.tspreg
    │   └── 20231104145812345+0200.version
    ├── .../
    └── 39901019992/
        ├── 20231104132412345+0200.bdoc
        ├── 20231104132412345+0200.ocsp
        ├── 20231104132412345+0200.tspreg
        ├── 20231104132412345+0200.version
        ├── 20231104172912345+0200.bdoc
        ├── 20231104172912345+0200.ocsp
        ├── 20231104172912345+0200.tspreg
        ├── 20231104172912345+0200.version
        ├── 20231105124212345+0200.bdoc
        ├── 20231105124212345+0200.ocsp
        ├── 20231105124212345+0200.tspreg
        └── 20231105124212345+0200.version
```

Joonis 9. Valimiskasti sisu.

4.5.2 Häälte töötlemise sammud

Häälte töötlemise etapp koosneb neljast sammust, mis on toodud Joonisel 4. Häälte töötlemise esimeses sammus kontrollitakse häälte allkirjade kehtivust. Selleks lisatakse allkirjale juurde registreerimistõend ja seejärel kontrollitakse allkirja kehtivust Java teegiga DigiDoc4j[1]. Lisaks kontrollitakse iga hääle puhul, kas hääle juures olev registreerimistõend on olemas ka registreerimisteenuselt saadud nimekirjas ja vastupidi, kas kõigile nimekirjas olevatele kirjetele on olemas valimiskastis vastav hääl. Kõik hääled, mis ei läbi kontrolli, kirjutatakse logidesse hilisemaks auditeerimiseks. Järgmistes sammudes eemaldatakse korduvhääled ja seejärel jaoskonnas üle hääletanute hääled. Mõlemas sammus tühistatud hääled kirjutatakse eraldi logidesse hilisemaks auditeerimiseks. Kõikide etapi sammude väljundite pealt, mis lähevad sisendiks järgmisele sammule, arvutatakse räsi ja see allkirjastatakse. Seda räsi kontrollitakse sisendi lugemisel tagamaks selle, et andmeid ei oleks võimalik muuta töötlusetapi sammude vahepeal.

Kui nüüd aga oletada, et keegi on otsustanud manipuleerida töötlemisrakendusega sedasi, et tal õnnestub etapi sees häältega manipuleerida, neid juurde lisada, eemaldada ja välja vahetada. Hetkel puudub lihtne viis kontrollimaks, kas need hääled, mis anonüümistatud häälte hulka ei jõudnud, oleksid olemas kuskil logides koos põhjendustega, miks mingi konkreetne hääl tühistamisele läks. Samuti ei kontrollita seda, kas anonümiseeritud hääled olid olemas ka esialgses valimiskastis.

[1] https://github.com/open-eid/digidoc4j

Praegused meetmed selle vältimiseks on häälte töötlemise etappide uuesti läbi tegemine. Kui peaks saama teise tulemuse on arusaadav, et kuskil on mingi viga tehtud. Kuid seda peaks tegema erinevate sõltumatute osapoolte poolt loodud programmidega, mis on kirjutatud samade spetsifikatsioonide järgi, kuid võib oletada, et praegu viiakse korduslugemine läbi samades arvutites täpselt samade programmide poolt millega esimesel korral, kuna puuduvad nõuded, mis nõuaks vastupidist. Teiseks meetmeks on audiitorite poolt käsitsi häälte kontrollimine, kuid kuna viimastel valimistel anti umbes 300000 häält[1], siis on täiesti võimalik, et kui häältega manipuleerimist teha piisavalt väikse hulga häältega, siis ei tule see sellise kontrolli puhul välja. Kui seda strateegiliselt teha, oleks võimalik lõplike tulemusi endale sobivas suunas nihutada. Kuid uurides viimaste valimiste auditit [17], ei tule sealt välja, et selliseid kontrolle oleks üldse tehtud. Sarnasele probleemile viitas ka ODIHR valimiste eksperdirühma lõpparuanne [16]. Leidudest sai teavitatud ka Valimiskomisjoni, kust öeldi, et audiitoritel on praegu võimalus pisteliselt kontrollida, kus vastav hääl paikneb. Sellist kontrolli, mis kõik hääled üle kontrollib, ei ole.

4.6 Häälte kokku lugemine

Viimase etapina tuleb töödeldud hääled kokku lugeda. Seda tehakse samas keskkonnas, kus genereeriti süsteemi võtmepaar. Antud etapi sisendiks on töötlemisetapis saadud anonüümistatud hääled, mis võivad olla nii miksimata kui ka miksitud kujul. Antud etapi käigus peavad kokku tulema määratud isikud, kelle hoolde usaldati võtmeosakutega kiipkaardid. Kiipkaardid on varasemalt pitseeritud ja vastavalt auditeerimise lõpparuandele [17] neid ka kontrolliti. Pitseerimine välistab olukorra, et häälte avamise võtme oleks saanud taastada varasemalt ja kasutada häälte avamiseks väljaspool õiget aega. Hääled loetakse kokku võtmerakendusega ja selle käigus küsitakse eelnevalt mainitud kiipkaarte. Võtmerakendus kontrollib anonümiseeritud häälte sisu ja selle allkirjastatud räsi, millega veendutakse, et sisendiks on korrektsed hääled. Kui kokku loetakse miksitud hääled, väljastatakse selle kohta lugemistõend, mida kasutades on võimalik veenduda kokkulugemise korrektsuses. Miksimata lubatakse hääli kokku lugeda vaid valimispäeval, kui ajaliselt ei jõuta miksimist läbi viia. Sellisel juhul tehakse häälte miksimine ja kokkulugemine uuesti järgmisel päeval. [11]

Kui siingi jälgitakse kõiki määratud protseduure, on tagatud häälte salajasus ja korrektsus. Hääletamise tulemuse korrektsuses veendumisel on olulisel kohal miksimistõendi ja lugemistõendi kontroll.

[1] `https://rk2023.valimised.ee/et/detailed-voting-result/index.html`

5. Pakutud lahendus

Antud peatükis pakutakse välja lahendus, mis võiks aidata e-hääletamist turvalisemaks muuta. Pakutava lahenduse puhul ei tohiks panna eelduseks kaustatava tarkvara ja riistvara usaldusväärsust. Kõik peab olema kontrollitav ka sellisel juhul, kui kurjade kavatsusega isikul on ligipääs riistvarale.

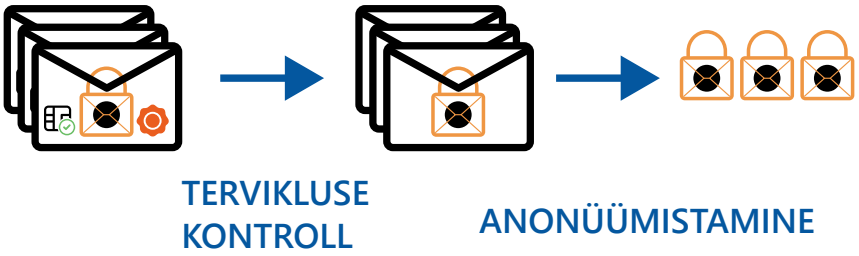
Analüüsi faasis leiti, et potentsiaalselt rünnatav koht on häälte töötlemise etapis ühe sammu sees. Sammude vahepealne manipuleerimine on kaitstud sellega, et väljundite tulemuste kontrollsumma digiallkirjastatakse ja järgmisel sammul sisendi lugemise käigus kontrollitakse selle vastavust allkirjastatud kontrollsummale. Samuti kontrollitakse, et see allkiri oleks kehtiv. Kui avastatakse vastuolu, antakse vastav hoiatus ja programm lõpetab andmete edasise töötlemise.

Pakutav lahendus lisab võimaluse kontrollida, et sammude sees ei läheks hääled kaduma ega tekiks neid juurde, ühesõnaga, et häältega ei manipuleeritaks. Lihtsustatult oleks pakutava lahenduse eesmärgiks kontrollida, kas kõik hääled, mis tulid sisse valmiskastist, oleksid ka lõpuks kuskil olemas, kas siis lugemisele läinud häälte hulgas või kuskil logides põhjendustega, miks mingi konkreetne hääl lugemisele ei läinud. Seda, kas logides olevad tühistatud hääled ka päriselt seal olema peavad, seda antud lõputöö raames ei vaadata, vaid oletatakse, et need vastavad tegelikkusele. Võib öelda, et seni on nende hulk olnud väike ja nende puhul on ka juba pistelise kontrolliga oluliselt suurem tõenäosus viga leida.

5.1 Võrreldava objekti leidmine

Töötlemisetapi käigus muutub järjest hääle kuju, kuna eemaldatakse turvaelemente, mida pole peale vastavat kontrolli enam vaja (Joonis 10). Peale tervikluse kontrolli eemaldatakse sertifikaadi kehtivuskinnitus ja registreerimisteenuse tõend ning peale anonüümistamist eemaldatakse valija isikuandmed. Seega tuli leida esmalt mingi viis, kuidas esitada häält sellisel kujul, et see oleks üks üheselt vastavusse viidav nii häälega, mis on esialgses valimiskastis, kui ka sellega, mis on häälest järgi peale anonümiseerimist. Lisaks kirjutatakse eemaldatud hääled logidesse, mis tuleb samuti vastavusse saada nende samade valimiskastis olevate häältega.

Hääle juures võrdlemiseks kasutada saavat infot hakati otsima kohast, kus hääle kohta on olemas kõige vähem informatsiooni. Esialgses valimiskastis on hääl olemas digiallkirjasta-



Joonis 10. Andmete järk-järguline eemaldamine.

tud konteineris koos sinna juurde kuuluvate turvaelementidega. Viimases faasis, kus hääled on anonümiseeritud, on eemaldatud kõik muu sealt juurest ja alles on jäänud vaid hääl json failis Base64 kodeeringus (Joonis 11). Kuid igas etapis kirjutatakse tühistatud hääled logidesse ja seal on häälest endast alles vaid hääle SHA-256 räsi Base64 kodeeringus. Lisaks räsile on logides veel rea tekkimise aeg, ringkonna kood, ringkonna number ja hääletaja isikukood (logi faili näidis Joonisel 12). Kuna logides on seega hääle kohta kõige vähem informatsiooni ning seal kasutatakse häälele viitamiseks krüpteeritud hääle räsi, siis võeti võrreldavaks objektiks hääle räsi. Räsi eelisteks on veel selle väiksus võrreldes hääle krüptogrammi endaga ning räsi ei avalda, mis hääles täpselt sisaldub. Lisaks kasutatakse failide räsisid ka näiteks allkirjastamise juures.

```
{
  "election" : "RK_2023",
  "districts" : {
    "0064.1" : {
      "0176" : {
        "RK_2023.question-1" : [ "MIIDGTALmnW3LUnx...",
                                 "MIIDGTALcYbjCkzA..." ]
      }
    },
    "0064.5" : {
      "0714" : {
        "RK_2023.question-1" : [ "MIIDGjALMJAoIBgE..." ]
      }
    }
  }
}
```

Joonis 11. Anonümiseeritud hääled json kujul.

```
1
RK_2023
2
20231104132412  n2+pSo38YH1t2WHLMNh4...  0064  1  39901019992
20231104172412  /lPmLd+2pqwVwhYXJnBT...  0064  1  39901019992
20231104182412  VHbvfwaxMTRRsgdBTDa0...  0064  1  39901019992
```

Joonis 12. Tühistatud häälte logi fail.

5.2 Esialgne häälte hulk

Töötlemisetapi sisendiks on valimiskast, kus iga hääletaja kohta on tema krüpteeritud hääl allkirjastatud konteineris koos sinna juurde kuuluvate allkirja sertifikaadi kehtivuskinnitustega ja registreerimisteenuse poolsete kinnitustega. Kuna meid huvitab konkreetse hääle enda räsi, siis tuleb see leida nende andmete pealt, mis meil olemas on.

Ette antud valimiskast ise on ZIP-konteiner, seega esmalt tuleb see lahti pakkida, et pääseks ligi allkirjastatud häältele. Iga krüpteeritud hääl asub omakorda .bdoc failis, mis tuleb sealt välja lugeda. Allkirjastatud konteineri puhul on tegemist tavalise ZIP-konteineriga, nagu seda oli ka valimiskast, kus lisaks allkirjastatud failidele on lisatud allkiri, millega need failid on allkirjastatud.[1] Kuna allkirja kontroll tehakse töötlusetapi sees esimeses sammus, siis eraldi allkirja kehtivuse kontrolli siin tegema ei hakata. Esmalt pakime allkirjastatud konteineri lahti ja loeme sealt seest krüpteeritud hääle välja. Saadud hääle faili laseme läbi räsifunktsiooni SHA-256 ja saame konkreetsele häälele vastavusse võrreldava objekti. Kõik saadud räsid hoiame alles nende edasiseks võrdlemiseks tühistatud häältega ja lugemisele minevate häältega. Viimaste all vaatame anonümiseeritud hääli enne miksimise protseduuri läbimist, kuna miksimise käigus häälte räsi muutub ja pole seega enam võrreldav. [18].

5.3 Tühistatud häälte hulk

Tühistatud hääled tulevad põhiliselt töötlemisetapi sees sammude väljunditest ja neid talletatakse .log2 failis. Faili sisu on täpsemalt nähtav Joonisel 12. Logifailist on juba olemas häälte räsid, kuid need on kodeeritud Base64 kodeeringusse. Võrdlemiseks tuleb need kõik logidest välja lugeda ja teisendada tagasi binaarkujule.

Kuid on üks erand, kus ei kasutata tühistatud häälte puhul vastavat logi formaati ja selleks on häälte tervikluse kontrolli samm. Siin kirjutatakse vigadega hääled eraldi töötlemisvigade raporti faili (näidis failist Joonisel 13). Antud failis on esmalt viide häälele valimiskastis, millega probleem oli. Viide vastab täpselt sellele, kuidas hääli hoitakse valimiskastis, puudu on vaid faililaiend. Seejärel on failis veateate viide ja inimesele loetaval kujul täpsem vea kirjeldus. Meid huvitab sealt ainult viide häälele.

```
39901019992/20230131153406332+0200 MISSING_FILE  <vea kirjeldus>
39901019992/20230202120946092+0200 REPEATED_FILE <vea kirjeldus>
```

Joonis 13. E-valimiskasti töötlemisvigade raporti faili näide.

Kuna antud failis ei ole piisavalt informatsiooni hääle räsi leidmiseks, tuleb vastav fail

[1] https://www.id.ee/wp-content/uploads/2020/01/bdoc-spec212-est.pdf

otsida ülesse esialgsest valimiskastist vastava viite alusel. Seejärel leiame hääle räsi samamoodi nagu seda tehti valimiskasti puhul. Antud juhul leiame vaid vigaste häälte räsid ja talletame need edasiseks võrdlemiseks.

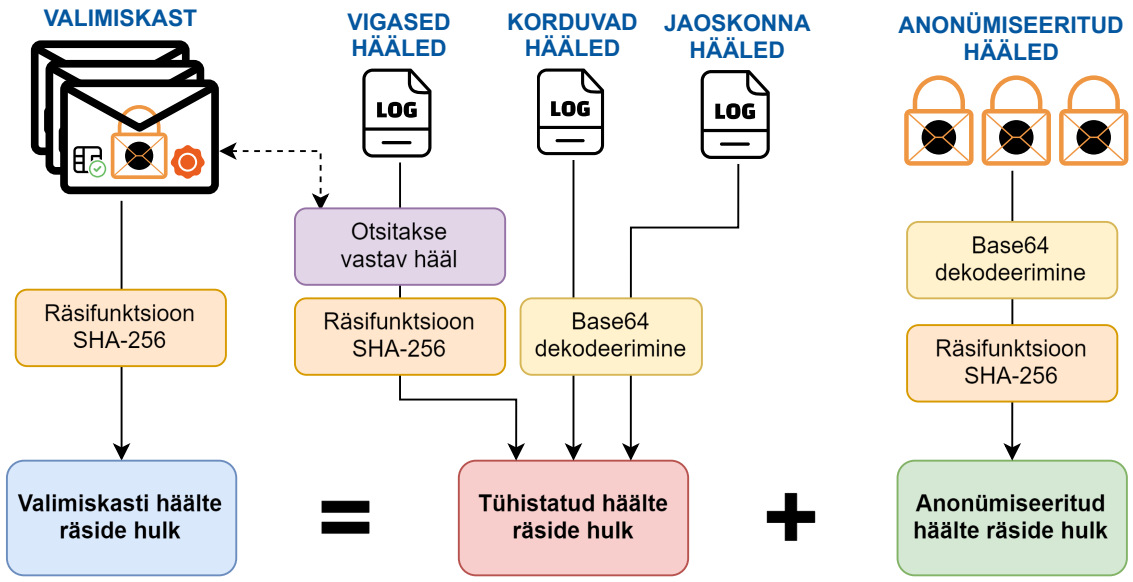
5.4 Anonümiseeritud häälte hulk

Töötlemisetapi anonüümistamise sammu lõpuks saame json faili, kus enam ühtegi viidet konkreetsele isikule ei ole, vaid hääled on jaotatud ringkondade kaupa ja talletatud json listis. Faili täpsem sisu on nähtav Joonisel 11.

Esmalt tuleb kõik listid läbi käia, kus hääli hoitakse, ja need sealt järjest välja lugeda. Kuna antud juhul on iga hääl Base64 kodeeringus, siis enne räsi arvutamist tuleb see teisendada tagasi binaarkujule. Seejärel saame lasta saadud bitid läbi räsifunktsiooni ning talletame need edasiseks võrdluseks.

5.5 Saadud hulkade võrdlemine

Kui on kätte saadud iga hääle räsi ja jaotatud hääled kolme hulka, jääb järele hulkade võrdlemine. Lahenduse üldine joonis on toodud Joonisel 14. Esimeseks hulgaks on kõik hääled, mis edastati töötlemisteenusele valimiskastina. Erinevates töötlemisetapi sammudes tühistati järjest hääli ja nende häälte räsid moodustavad teise hulga. Viimaks on anonümiseeritud hääled, mis lähevad lugemisele ja mille pealt saadakse e-hääletamise tullemus. Anonümiseeritud häältest moodustub kolmas hulk.



Joonis 14. Lahenduse visuaal.

Selleks, et iga hääl oleks kuskil olemas ja ühtegi lisahäält ei oleks juurde tekkinud, võrdle-

me lõpuks neid kolme hulka. Sissetulevate häälte hulk peab olema võrdne teise kahe hulga summaga, kuna lugemisele mitte läinud hääl peab olema tühistatud häälte hulgas. Kui viimase kahe hulga summa on võrdne esialgse hulgaga, saab kindel olla, et töötlusetapi sammude sees ei ole häältega manipuleeritud.

5.6 Valideerimine

Pakutud lahenduse valideerimiseks sai läbi viidud kahte tüüpi katseid. Esimeste puhul sai genereeritud valimiskast mis sisaldas nii korduvaid hääli, vigaseid hääli kui ka valiidseid hääli. Valimiskastiga sai läbi viidud töötlusetapp ja saadud väljundid said ette antud pakutud lahendusele ja veendutud, et kõik toimib korrektselt. Seejärel manipuleerisime veidi tulemustega ja vaatasime, kas keed tulevad välja. Katse tulemustena selgus, et kõik toimib nii nagu peab.

Teised katsed olid seotud mahtudega, mis Eestis e-hääletamisel olla võivad. Peamiseks valideerimise kohaks oli lahenduse toimimise kiirus. Selleks genereeriti erinevate suurustega valimiskastid ning sealt osad hääled kuulutati vigasteks ja jaotati erinevate logifailide vahel ära ning ülejäänud pandi anonümiseeritud häälte hulka. Täpsed tulemused on toodud Tabelis 1. Tulemustest selgub, et ka miljoni hääle puhul on kontroll piisavalt kiire, natuke üle minuti, seega on antud lahendus päris hääletamisel olevate mahtude korral kasutatav.

Tabel 1. Kontrollimiseks kuluv aeg.

Häälte kogus valimiskastis	**Ajakulu**
50000	4 sekundit
100000	7 sekundit
500000	36 sekundit
1000000	72 sekundit

Lisaks omapoolsele valideerimisele andsime loodud lahenduse prototüübi katsetamiseks Valimisteenistusele ja nemad kinnitasid, et loodud lahendus tõstaks läbipaistvust. Meile kinnitati, et 2024 aasta Euroopa parlamendi valimisteks on see lisatud auditrakendusse.

6. Kokkuvõte

Lõputöö eesmärgiks oli kontrollida, kas ebaausatel korraldajatel on võimalik keskserveris hääli nii välja vahetada, et vaatlejad ega audiitorid seda ei märka.

Eesmärgi saavutamiseks tuli esmalt mõista Eestis kasutusel olevat e-hääletamise süsteemi, selleks uuriti e-hääletamise dokumentatsiooni ja pandi püsti e-hääletamise süsteem. Viimase eesmärgiks oli ka katsete läbiviimine. Suure osa lõputöö mahust võttis katsekeskkonna püstitamine, sellest tulenevalt oleks soovitus, et sarnaste uuringute läbiviimiseks võiks olla olemas konteinerid näidis konfiguratsioonidega, mille abil saaks lihtsa vaevaga püsti panna keskkonna katsete läbiviimiseks. Kogutud teadmiste põhjal võeti ette süsteemi analüüs, selleks võeti e-hääletamise süsteem samm-sammult ette ja vaadati, mis turvaelemendid on kasutusel, kuidas auditeeritakse ja kas on võimalusi, kuidas sellest mööda minna.

Analüüsi käigus leiti, et häälte töötlemise etapis vahesammude sees on võimalik häältega manipuleerida, ilma et seda oleks lihtne kontrollida. Seejärel pakuti välja lahendus, mis selle kontrollitavaks teeks.

Antud puudustest teavitati Valimisteenistus, nende poolt anti teada, et audiitoritel on võimalik pisteliselt kontrollida, kas anonümiseeritud või tühistatud hääl on olemas ka algses valimiskastis, kuid puudub kontroll, mis kontrolliks kõiki hääli. Loodud kontrollimise lahenduse prototüüp edastati Valimisteenistusele katsetamiseks, kust kinnitati, et 2024 aasta Euroopa parlamendi valimisteks on see lisatud auditrakendusse.

Kasutatud kirjandus

[1] Piret Ehin *et al.* „Internet voting in Estonia 2005–2019: Evidence from eleven elections“. *Government Information Quarterly* 39.4 (2022), lk. 101718. ISSN: 0740-624X. DOI: https://doi.org/10.1016/j.giq.2022.101718. URL: https://www.sciencedirect.com/science/article/pii/S0740624X2200051X.

[2] Ben Adida. „Helios: web-based open-audit voting“. Teoses: *Proceedings of the 17th Conference on Security Symposium*. SS'08. San Jose, CA: USENIX Association, 2008, lk. 335–348.

[3] Riigi valimisteenistus. *Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel*. [Kasutatud: 01-04-2024]. 2023. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV%20elektroonilise%20h%C3%A4%C3%A4letamise%20%C3%BCldraamistik.pdf.

[4] Sven Heiberg *et al.* „Improving the Verifiability of the Estonian Internet Voting Scheme“. Teoses: *Electronic Voting*. Toim. Robert Krimmer *et al.* Cham: Springer International Publishing, 2017, lk. 92–107. ISBN: 978-3-319-52240-1.

[5] *IVXV arhitektuur*. [Kasutatud: 01-04-2024]. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV-arhitektuur.pdf.

[6] Estonian National Electoral Committee. *E-Voting System. General Overview*. [Kasutatud: 08-05-2024]. 2010. URL: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf.

[7] Vabariigi Valimiskomisjon. *Elektroonilise hääletamise süsteemi üldkirjeldus*. [Kasutatud: 08-05-2024]. 2013. URL: https://www.valimised.ee/sites/default/files/uploads/eh/elektroonilise-haaletamise-systeemi-yldkirjeldus-EH-03-03-1_2013.pdf.

[8] Sven Heiberg, Peeter Laud ja Jan Willemson. „The Application of I-Voting for Estonian Parliamentary Elections of 2011“. Teoses: *E-Voting and Identity*. Toim. Aggelos Kiayias ja Helger Lipmaa. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, lk. 208–223. ISBN: 978-3-642-32747-6.

[9] Sven Heiberg ja Jan Willemson. „Verifiable internet voting in Estonia“. Teoses: *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*. 2014, lk. 1–8. DOI: 10.1109/EVOTE.2014.7001135.

[10] Drew Springall *et al.* „Security Analysis of the Estonian Internet Voting System“. Teoses: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: Association for Computing Machinery, 2014, lk. 703–715. ISBN: 9781450329576. DOI: 10.1145/2660267.2660315. URL: https://doi.org/10.1145/2660267.2660315.

[11] Riigi valimisteenistus. *IVXV: E-hääletamise käsiraamat*. [Kasutatud: 01-04-2024]. 2023. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat.pdf.

[12] *IVXV seadistuste koostamise juhend*. [Kasutatud: 01-04-2024]. 2023. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV-seadistuste-koostejuhend.pdf.

[13] *IVXV protokollide kirjeldus*. [Kasutatud: 01-04-2024]. 2023. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV-protokollid.pdf.

[14] *IVXV kogumisteenuse haldusjuhend*. [Kasutatud: 01-04-2024]. 2022. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV-kogumisteenuse-haldusjuhend.pdf.

[15] Majandus- ja Kommunikatsiooniministeerium. *E-valimiste turvalisuse töörühma koondaruanne*. [Kasutatud: 16-05-2024]. 2019. URL: https://debriif.infoaed.ee/files/e-valimiste-tooruhma-koondaruanne-12122019-88361339.pdf.

[16] Demokraatlike institutsioonide ja inimõiguste büroo. *ODIHR valimiste eksperdirühma lõpparuanne*. [Kasutatud: 16-05-2024]. 2023. URL: https://www.osce.org/files/f/documents/c/0/551671.pdf.

[17] KPMG Baltics OÜ. *Elektroonilise hääletamise protsessi auditeerimine. Lõpparuanne*. [Kasutatud: 01-04-2024]. 2023. URL: https://www.valimised.ee/sites/default/files/2023-05/L%C3%B5pparuanne%20RKV23%20EValimiste%20Audit.asice.

[18] *IVXV raamistiku nõuded krüptosüsteemile*. [Kasutatud: 19-05-2024]. URL: https://www.valimised.ee/sites/default/files/2021-10/IVXV%20raamistiku%20n%C3%B5uded%20kr%C3%BCptos%C3%BCsteemile.pdf.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Kristjan Düüna

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Eesti e-hääletamise usaldusväärsuse ja läbipaistvuse tõstmine", mille juhendaja on Tarvo Treier
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

20.05.2024

[1] Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.