Riigi valimisteenistuse 06.02.2023 korralduse nr 11
LISA

Riigi valimisteenistus

Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel

Dokument: IVXV-ÜK-1.1
Kuupäev: 3.veebruar 2023.a.

Tallinn 2023

Annotatsioon

Antakse üldine, kuid terviklik ülevaade elektroonilise hääletamise raamistiku („IVXV”) tehnilisest ja organisatsioonilisest poolest ning selle rakendamisest Eesti riiklikel valimistel. Dokument on mõeldud avalikkusele ega eelda lugejailt põhjalikke tehnilisi eelteadmisi. Detailsemate nõuete ja kirjelduste saamiseks tuleb tutvuda tehniliste alusdokumentidega. Käesolev dokument kirjeldab süsteemi üldiselt; selle rakendamine Eestis on kirjeldatud eristuvate lõikudega.

Sisukord

1. Sissejuhatus

Elektroonilise hääletamise (*e-hääletamise*) all peetakse käesolevas dokumendis silmas hääletamisviisi, kus valija annab oma hääle **arvutiga interneti teel**. Nimetatud hääletamisviisi võib kutsuda ka „i-hääletamiseks" selleks, et rahvusvahelises kontekstis eristuda muudest infotehnoloogiat kasutatavatest hääletusviisidest, näiteks elektrooniliste valimismasinate kasutamine.

Kirjeldatav e-hääletamise raamistik on universaalne ning kohaldatav erinevate valimiste puhul. Selles dokumendis on siiski erilise tähelepanu all Eestis korraldatavad riiklikud valimised (Riigikogu, kohaliku omavalitsuse volikogu ja Euroopa Parlamendi) ja rahvahääletused. Seetõttu on edaspidises tekstis üldist raamistikku kirjeldava sisu kõrval eraldi ära toodud ka Eesti seadustest ja nende rakendusaktidest tulenevad asjaolud.

Käesolevas dokumendis:

- määratletakse e-hääletamise süsteemi ulatusala ehk piiritletakse e-hääletamise osa valimiste koguprotsessis;
- võetakse kokku e-hääletamise süsteemile esitatavad nõuded;
- määratletakse süsteemis osalevad osapooled ja kirjeldatakse nende tegevust;
- kirjeldatakse e-hääletamise põhiprotsesse;
- antakse ülevaade süsteemi korrektsuse ja põhinõuetele vastavuse kontrollimise võimalustest.

Käesolevas dokumendis ei määratleta süsteemi komponentide täpset turvataset, andmestruktuure, kasutatavaid tark- ja riistvaraplatvorme ega täpset tehnilist ülesehitust.

Dokumendi lugemisel tuleb arvestada, et detailirohkus kasvab järk-järgult nii, et alguses üldiselt kirjeldatu võib olla täpsemalt lahti seletatud tagapool.

Eestis on e-hääletamist kasutatud alates aastast 2005. Igal Eesti hääleõiguslikul isikul on võimalik valimistel ja rahvahääletustel anda turvalisel viisil oma hääl interneti teel, sest:

- on olemas õiguslik baas digitaalallkirja kasutamiseks ning kõigis valimisseadustes kajastuv õiguslik alus e-hääletamise läbiviimiseks,
- enamikul valimisõiguslikest isikutest on olemas nende turvalist elektroonilist identifitseerimist ja digitaalset allkirjastamist võimaldav ID-kaart, paljudel ka mõni täiendav seaduskohane elektrooniline isikutunnistus nagu Digi-ID või Mobiil-ID.

2. E-hääletamise süsteemi ulatusala

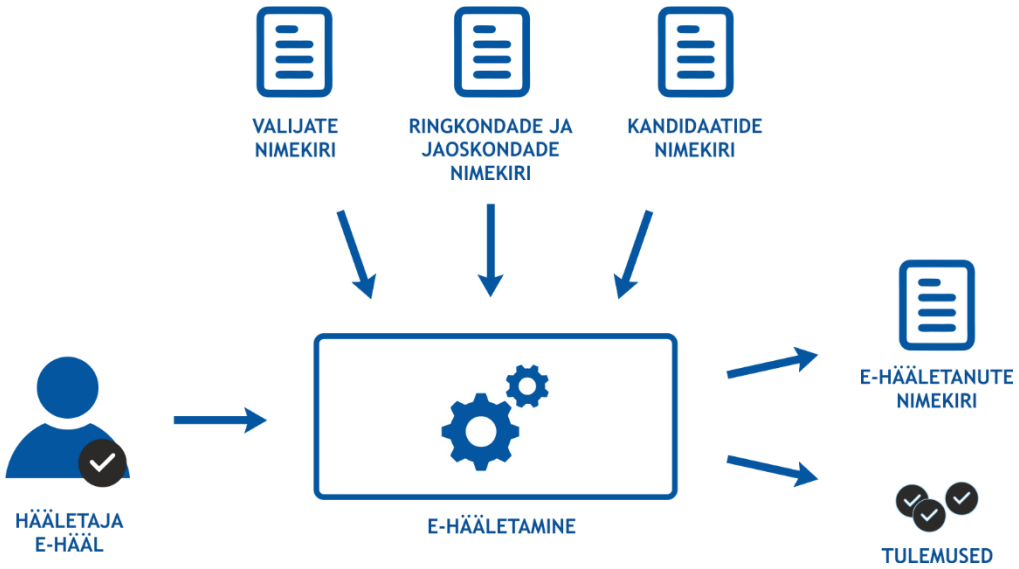
E-hääletamine on üks osa valimisprotsessist. Valimised koosnevad järgmistest põhietappidest:

- valimiste väljakuulutamine
- kandidaatide registreerimine
- valijate nimekirjade koostamine
- hääletamine
- häälte kokkulugemine
- valimistulemuste väljakuulutamine

E-hääletamise süsteem katab osaliselt vaid kolme viimast, st hääletamist interneti teel, häälte kokkulugemist ning e-häälte lugemiseks vajaliku võtme hävitamist peale tulemuste välja kuulutamist.

E-hääletamise süsteem eeldab, et:

1) valijate nimekirjad (koos valijaga seotud valimisjaoskonna ja valimisringkonnaga) on olemas ja sobival kujul kättesaadavad;
2) jaoskondade ja ringkondade nimekirjad on olemas ja sobival kujul kättesaadavad;
3) kandidaatide või valikute nimekirjad (edaspidi koos nimetatult *kandidaatide nimekiri)* on koostatud ja sobival kujul kättesaadavad (ringkondade kaupa);
4) e-hääled loetakse üle eraldi ning tulemused liidetakse hiljem paberhäälte lugemise tulemustele, arvestades, et ühegi isiku hääli (elektroonilist ja paberhäält) ei loendata topelt.



Joonis 1. E-hääletamise ulatusala

3. E-hääletamise põhinõuded

E-hääletamine peab järgima kõiki valimisseadusi ja -tavasid ning olema vähemalt sama turvaline kui tavahääletamine. Seega peab e-hääletamine olema ühetaoline ja salajane, (e-)hääletada peavad saama ainult valimisõiguslikud isikud, iga isik saab anda ainult ühe hääle ning hääletajad ei tohi saada tõestada, kas nende poolt antud hääl läks arvesse.

Põhiline e-hääletamise erinevus paberhääletamisest on see, et valija saab elektroonilisel teel hääletada korduvalt; arvesse läheb ainult viimasena antud hääl. See põhimõte võimaldab kaitsta e-hääletajaid mõjutamise vastu, sest surve all hääletanud ja hiljem surve alt vabanenud isik saab hääletada uuesti, muutes surve all antud hääle kehtetuks.

E-hääletamine toimub seadusega määratud **ajaperioodil enne valimispäeva**. Juhul, kui e-hääletamise süsteemiga juhtub midagi ootamatut (suuremahuline rünne, oluline tarkvaraviga vms), võib valimiste korraldaja äärmuslikul juhul e-hääled osaliselt või täielikult tühistada. Siis saavad e-hääletanud uuesti hääletada valimisjaoskonnas.

Kui paralleelselt e-hääletamisega toimub ka eelhääletamine jaoskondades (**paralleelhääletamine**), siis on võimalik, et valija hääletab kahel erineval moel. Sellisel juhul loetakse kehtivaks paberhääl ning kõik selle valija e-hääled tühistatakse. Ka see põhimõte kaitseb hääletajaid survestamise vastu.

Teiseks oluliseks e-hääletamise nõudeks on **digitaalallkirja kasutamine**. Hääletaja peab kinnitama oma valiku seadusekohase digitaalallkirjaga. Põhinemine digitaalallkirja seaduses toodud nõuetele tagab e-hääletamise keskse turvanõude: hääletaja isikusamasuse turvalise tuvastamise.

Hääletaja peab saama **kontrollida,** kas tema e-hääl on turvaliselt kohale jõudnud. Seda tehakse eraldi nutiseadme (mobiiltelefon, tahvelarvuti) abil. Kui e-hääletamiseks kasutatakse arvutit, siis e-hääle turvalise kohalejõudmise kontrolliks tuleks kasutada sellest erinevat seadet. Sellisel moel on võimalik suurendada e-hääletamise süsteemile (eelkõige hääletaja arvutile) suunatud rünnete tuvastamise tõenäosust.

E-hääletamise süsteemi ülesehitusel tuleb lisaks arvestada selle *auditeeritavusega* – süsteem peab olema tehniliselt piisavalt lihtne, et seda saaks auditeerida võimalikult lai ring spetsialiste.

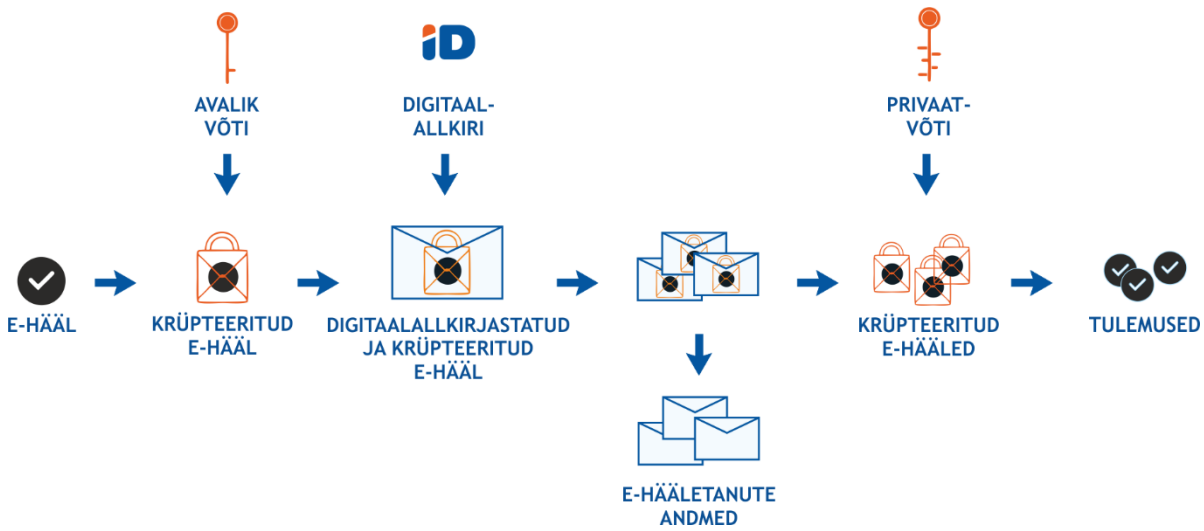
Eestis toimub e-hääletamine kuue päeva jooksul ja algab kuus päeva enne valimispäeva. Kasutatakse paralleelhääletamist. Digitaalse allkirja andmiste vahenditeks on kasutatavad isikutunnistus ehk ID-kaart, Mobiil-ID ja digitaalne isikutunnistus ehk Digi-ID. Alates 2015. aastast on valimiste korraldajal kohustus pakkuda hääletajale võimalust hääle kohalejõudmise kontrolliks.

4. Ümbrikuskeem

E-hääletamise süsteem rajaneb nn. „ümbrikuskeemile“, mis on tuntud posti teel hääletamisest, kus anonüümne kinnine ümbrik häälega asetatakse hääletaja nime ja allkirjaga varustatud välimisse ümbrikusse. E-hääletamiseks kasutatava programmi (nn. *valijarakenduse*) abil, e-hääletaja:

1) krüpteerib hääle ja arvuti poolt genereeritud juhuarvu hääletamiskohase avaliku võtmega – *häälte salastamise võtmega,* moodustades nii „sisemise ümbriku“;
2) allkirjastab krüpteeritud hääle digitaalallkirjastamise vahendiga, moodustades nii “välimise ümbriku”.

Häälte salastamise võtmega krüpteeritud häält saab dekrüpteerida üksnes privaatvõtmega – *häälte avamise võtmega*.



Joonis 2. Ümbrikuskeem

Krüpteeritud ja allkirjastatud hääled kogutakse kokku, sorteeritakse, kontrollitakse isikute valimisõigust ning eemaldatakse korduvad e-hääled ning isikute e-hääled, kes andsid oma hääle ka valimisjaoskonnas eelhääletamise ajal.

Enne e-häälte kokku lugemist sorteeritakse need ringkondade kaupa, moodustatakse e-hääletanute nimekiri ning seejärel eemaldatakse digitaalallkirjad.

Häälte lugemise käigus dekrüpteeritakse anonüümsed ja segatud hääled hääletamiskohase privaatvõtmega – *häälte avamise võtmega* ja väljastatakse summaarsed e-hääletamise tulemused.

5. E-hääletamise etapid

E-hääletamine jaguneb korralduslikult neljaks etapiks.

1) **Hääletamiseelsel etapil** leiab aset süsteemi kasutusvalmiks seadmine, mille käigus:

- koostatakse ringkondade, jaoskondade, kandidaatide ja valijate nimekirjad;
- luuakse iga hääletuse tarbeks häälte salastamise võti ja häälte avamise võti;
- avaldatakse valijarakendus, kontrollrakendus ja vastavad juhendmaterjalid ning eraldi infokanalis nende autentsuse ja tervikluse kontrolliks vajalikud andmed.

2) **Hääletamisetapil** toimub e-hääletamine. Paralleelhääletamise korral toimub hääletamine samaaegselt ka valimisjaoskondades.

3) **Töötlusetapil**:

- Kontrollitakse e-häälte terviklust ja autentsust (digitaalallkirja) ning seda, et kõik antud e-hääled on endiselt olemas.
- Hääled sorteeritakse, ühe ja sama isiku korduvad e-hääled tühistatakse.
- Paralleelhääletamise kasutamise puhul laetakse elektrooniliselt hääletanute nimekiri valimiste infosüsteemi, mis omakorda tagastab nimekirja nendest paberhääletajatest, kes on andnud ka elektroonilise hääle, ehk topelthääletajate nimekirja.
- Topelthääletanute e-hääled tühistatakse, lugemisele minevad hääled anonüümistatakse.

4) **Lugemisetapil** avatakse hääletamistulemuse kindlaks tegemiseks anonüümistatud hääled häälte avamise võtmega ning summeeritakse.

Eestis avatakse e-hääletamise võimalus kuus päeva enne valimispäeva esmaspäeva hommikul kell 9.00 ning suletakse üks päev enne valimispäeva ehk valimisnädala laupäeval kell 20.00. Hääletada on võimalik ööpäevaringselt veebileheküljel www.valimised.ee avaldatud valijarakendusega. Valijate nimekirja võimalikke muudatusi kantakse e-hääletamise süsteemi vähemalt üks kord ööpäevas vastavalt valimiste infosüsteemist saadud andmetele.

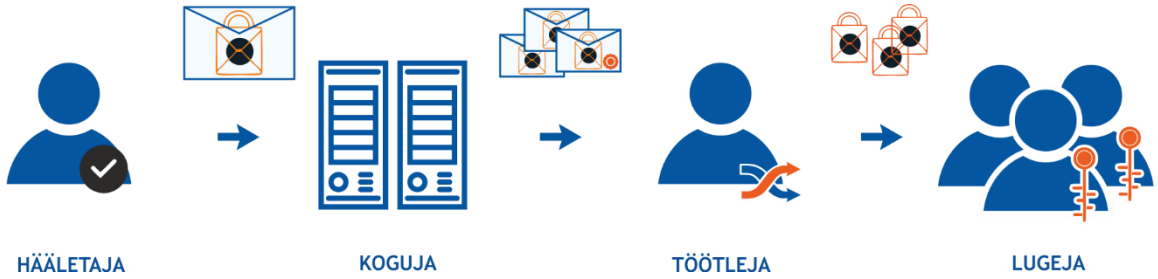
Kasutatakse paralleelhääletamist, topelthääletanute e-hääled tühistatakse vahetult enne e-häälte kokkulugemist.

E-hääletamise tulemusi ei tohi avaldada enne seaduses sätestatud aega.

6. Süsteemi osapooled ja komponendid

E-hääletamise põhiroll on **Korraldajal**, kes määrab kõik ülejäänud rollitäitjad. Korraldaja hoiab tavajuhtumitel ka e-hääletamise süsteemi põhisaladust – häälte avamise võtit ning seega täidab ta ka häälte avaja ja summeerija ehk **Lugeja** rolli.

Süsteemi põhirolle illustreerib alljärgnev joonis.



Joonis 3. E-hääletamise süsteemi peamised osapooled

Süsteemi osapooled on:

- **Hääletaja** – e-hääletaja teeb arvutis paikneva valijarakenduse abil valiku, krüpteerib selle, allkirjastab digitaalselt ning saadab valiku Kogujale. Hääletaja saab kontrollida oma valiku terviklikku kohalejõudmist hääletamiseks kasutatud arvutist erineva seadmega.
- **Koguja –** serverisüsteem, mis aitab hääletajal e-häält moodustada (väljastab valijale kandidaatide nimekirja, abistab digiallkirjastamisel) ning võtab vastu e-hääli. Koguja vastab ka Hääletaja poolt tehtud hääle tervikluse kontrollpäringutele. Kogumisteenuse osutaja digiallkirjastab hääletamisperioodi lõpul elektroonilise valimiskasti kontrollsumma ja annab töötlejale üle e-hääled, e-häälte allkirjastatud kontrollsumma ning logid.
- **Töötleja** – töötleb hääletamisperioodil kogutud e-hääli:
  - kontrollib digitaalallkirju ja Kogujalt saadud andmete terviklikkust,
  - tühistab korduvad e-hääled ning paralleelhääletamise kasutamisel ka nende e-hääled, kes hääletasid jaoskonnas eelhääletamise ajal,
  - anonüümistab e-hääled, eemaldades nendelt isikulised digitaalallkirjad, olles eelnevalt need sorteerinud ringkondade kaupa ja jättes alles ringkonna identifikaatori,
  - segab anonüümistatud hääled sobival moel ning saadab lugemisele. Seda võib käsitleda ka alamrollina, sellisel juhul nimetame rollitäitjat **Miksijaks**.
- **Lugeja** rolli täidab Korraldaja, kelle käes on häälte avamise võti. Lugeja avab anonüümsed ja miksitud hääled ning summeerib need e-hääletamise tulemusteks.

Lisaks põhirollidele on süsteemis olemas:

- **Audiitor** – kontrollib süsteemi Korraldaja poolt avaldatud andmete ja kesksete osapoolte vahel liikuvate andmete terviklust ning kooskõlalisust.
- **Klienditugi** - osapool, kelle poole pöördub Hääletaja probleemide korral. Klienditugi abistab Kogumisteenusest saadud info abil Hääletajat probleemide lahendamisel. Klienditugi registreerib kõik laekunud probleemid ning nende lahendamise käigu.
- **Valijate nimekirja koostaja ja täiendaja –** nimekirjad koostatakse hääleõiguslikest

isikutest vastavalt valimise liigile. Hääletamisperioodil võib nimekiri muutuda.

Süsteemivälised kriitilised teenused on järgnevad:

- **Tuvastusteenus** – teenus mida kasutatakse vajadusel hääletaja identiteedi tuvastamiseks;
- **Allkirjastamisteenus** – allkirja andmise vahendist sõltuv teenus, mis abistab Hääletajat allkirjastamisel ja sellele kehtivuskinnituse saamisel;
- **Registreerimisteenus** – teenus, mille abil Koguja peab registreerima kõik Hääletajatelt saadud hääled. Pärast hääletamisperioodi lõppu edastab teenuseosutaja kõik registreeringud Töötlejale.

Ülal nimetatud rollide täitmiseks on vajalikud vahendid, mida rollitäitjad oma protseduurides kasutavad. Järgnevalt defineerime süsteemi tarkvarakomponendid.

- **Valijarakendus** töötab Hääletaja arvutis, suhtleb Kogujaga ning võimaldab Hääletajal teha valikut, seda krüpteerida ja digitaalselt allkirjastada. Valijarakendus kuvab QR-koodi, mille alusel saab Hääletaja Kontrollirakendusega kontrollida e-hääle korrektset jõudmist Kogujani.
- **Kontrollrakendus** võimaldab Hääletajal arvutist erineval nutiseadme platvormil veenduda, et tema e-hääl jõudis Kogujani ning väljendas tema tahet korrektselt.
- **Võtmerakendus** – Korraldaja põhitööriist, millega genereeritakse iga hääletamise jaoks häälte salastamise ja häälte avamise võti. Võtmerakenduse abil toimub ka häälte lugemine ja tulemuse väljastamine.
- **Kogumisteenus** – süsteemi keskne komponent, mida käitab Koguja. Teenus abistab Hääletajat e-hääle koostamisel ning registreerib selle enne salvestamist *e-valimiskasti*. Kogumisteenus kasutab väliseid teenuseid (tuvastamine, allkirjastamine, registreerimine). Kogumisteenusel on peale Koguja enda teisigi haldureid (Korraldaja, Klienditugi), kelle jaoks on Kogumisteenusel eraldi haldusliidesed.
- **Töötlemisrakendus –** Töötleja põhitööriist, mille abil kontrollitakse häälte individuaalset terviklust ja e-valimiskasti terviklust, tühistatakse korduvaid ja topelthääli, väljastatakse hääletanute nimekirju ning ringkondade kaupa rühmitatud anonüümistatud hääli. Töötlemisrakenduse sisendi annavad Koguja, Registreerimisteenus ja Korraldaja. Töötlemisrakendust võib käitada ka Audiitor Töötleja töötulemuste kontrollimiseks.
- **Miksimisrakendus –** Töötleja või Miksija tööriist, mille sisendiks on ringkondade kaupa rühmitatud anonüümistatud krüpteeritud hääled ning mis väljastab segatud hääled nii, et neid ei ole võimalik sisendiga vastavusse viia. Miksimine peab toimuma sellisel moel, et nii sisend- kui ka väljundhäälte dekrüpteerimine ja tulemi summeerimine annaks sama resultaadi. Miksimirakendus väljastab lisaks *miksimistõendi*.
- **Auditirakendus –** Audiitori tööriist, mis võimaldab kontrollida Lugeja ja Miksija töö korrektsust. Lugeja töö korrektsust on võimalik kontrollida ka avalikult.

7. Põhiprotsessid

Käesolevas peatükis kirjeldatakse süsteemi osapoolte tegevust, mille käigus selgub süsteemi komponentide üldine funktsionaalsus ning välistele osapooltele esitatavad üldnõuded.

7.1. Võtmehaldus

Võtmehalduse protseduurid ja kasutatav turvaskeem on e-hääletamise süsteemi üks kriitilisemaid kohti, millest sõltub valimiste põhinõuete - hääletamise salajasus ja korrektsus, hääletaja sõltumatus - täitmine.

Salajasus tagatakse *asümmeetrilise krüptograafia* vahendite abil häälte krüpteerimisega. Igaks hääletamiseks luuakse Võtmerakenduse abil süsteemi võtmepaar – häälte salastamise võti (avalik võti) ja häälte avamise võti (privaatvõti).

Häälte salastamise võtit kasutab Valijarakendus häälte krüpteerimiseks. Häälte avamise võtit kasutatakse Võtmerakenduses häälte dekrüpteerimiseks. Seaduses sätestatud tähtajal häälte avamise võti hävitatakse.

Võtmepaari genereerimist ja avamisvõtme kasutamist korraldavad mitu *võtmehaldur*it koos. Võtmehaldurite arv ja koosseis määratakse vastavalt kehtestatud reeglitele. Häälte avamise võtme aktiveerimine on võimalik ainult siis, kui kohal on eelnevalt kokkulepitud hulk võtmehaldureid. Võtmehalduritele antakse häälte avamise võtme aktiveerimiseks füüsilised ja teadmuslikud **võtmeosakud** (näiteks kiipkaart ja/või parool).

Võtmehalduse toiminguid, sealhulgas võtmepaari ja paroolide genereerimist, häälte avamise võtme säilitamist, dubleerimist ning kasutamist Võtmerakenduses, auditeerib Audiitor.

7.2. Hääletaja tuvastamine

Hääletaja tuvastamine Koguja poolt on vajalik hääleõiguse esmaseks kontrolliks ning ringkonna kandidaatide nimekirja saamiseks. Hääletaja tuvastamine võib toimuda tema käest isikukoodi küsides, kuid otstarbekam[1] on nõuda tuvastamist autentimisvahendi abil.

Selleks toetab Koguja mitmeid *autentimismeetodeid*, mille vahel saab Hääletaja valida sõltuvalt tema valduses olevast *autentimisvahendist.* Nimetatud vahend võib olla lihtsalt teadmuspõhine (kasutajanimi/parool, PIN), kuid tugevama tuvastuskindluse tagab füüsilise autentimisvahendi (näiteks: kiipkaart, SIM-kaart vms) olemasolu kombineerituna teadmuspõhisega.

Sõltuvalt valimistel kasutatavast autentimismeetodist võib osutada vajalikuks välise **Tuvastusteenuse** kasutamine, mis kinnitab kas kasutatava autentimisvahendi kehtivust (kehtivusteenus) või siis tegeleb ise Hääletajalt autentimisvahendi küsimisega. Valijarakendus ja Kogumisteenus vahendavad Hääletajat ja Tuvastusteenust sobival moel. Protsessi tulemusena saab Kogumisteenus teada Hääletaja identiteedi.

Kasutatavad autentimisvahendid ja nendele vastavad Tuvastusteenused määrab Korraldaja.

7.3. Hääle allkirjastamine

Hääletaja allkirjastab krüpteeritud hääle, et tagada selle autentsus ja terviklus. Digitaalallkirjast tulenev isikuidentiteet on aluseks e-hääle arvesse võtmisel. See tähendab, et Hääletaja tuvastamisel

1 Tavaliselt on elektrooniline autentimisvahend ühitatud allkirjastamisvahendiga samal kandjal (näiteks: ID-kaart). Otstarbekus avaldub sellisel juhul sama kandja kasutamises mõlemaks otstarbeks.

saadud identiteeti ei arvestata digiallkirjastatud hääle edasisel käitlemisel.

Hääletaja kasutab digiallkirja andmiseks *allkirja andmise vahendit*, mis on kombinatsioon füüsilisest (näiteks: kiipkaart, SIM-kaart) ja teadmuslikust (PIN) osast.

Digitaalallkirja loomine koosneb:

- Signeerimisest ehk krüptograafilise signatuuri loomisest Hääletaja allkirja andmise vahendis sisalduva privaatvõtmega – Hääletaja kasutab selleks vastavat PIN-koodi. Valijarakendus kontrollib loodud signatuuri terviklust.
- Kehtivuskinnituse hankimisest, mis tõestab signatuuri loomisel kasutatud privaatvõtmele vastava sertifikaadi kehtivust küsimise ajahetkel. Kehtivuskinnituse päring ja vastus võivad sisaldada ka loodud signatuuri sõnumilühendit.

Allkirjastamisteenuse kasutamine toimub Valijarakenduse ja Kogumisteenuse poolt moel, mis sõltub kasutatavast allkirja andmise vahendist. Allkirjastamisteenuse üht osa – kehtivuskinnitusteenust – tuleb kasutada alati.

Protsessi tulemusena moodustab Kogumisteenus digitaalallkirja, milles sisaldub Hääletaja signatuur, tema sertifikaat ning allkirja kehtivuskinnitus.

Kasutatavad allkirja andmise vahendid ja nendele vastavad Allkirjastamisteenused määrab Korraldaja lähtudes digitaalallkirja käsitlevast seadusandlusest.

7.4. Hääle registreerimine

Kõik Kogujale saadetud e-hääled tuleb registreerida. **Registreerimisteenus** on sõltumatu osapool, mis registreerib ning kinnitab iga Kogumisteenusesse jõudnud krüpteeritud ja allkirjastatud hääle (selle sõnumilühendi) – toodab *ajamärgendi* koos omalt poolt lisatud ajaga.

Registreerimisteenus identifitseerib turvaliselt kõik Koguja päringud. Hääletamise lõppedes annab Registreerimisteenus kõik ajamärgendid üle Töötlejale.

Registreerimisteenus võib olla kombineeritud digitaalallkirja moodustamiseks kasutatava kehtivuskinnituse teenusega.

Registreerimisteenuse osutaja valib Korraldaja, pidades silmas, et teenus järgiks usaldusteenuse osutamiseks esitatud nõudeid eIDAS[2] 3. peatüki mõistes.

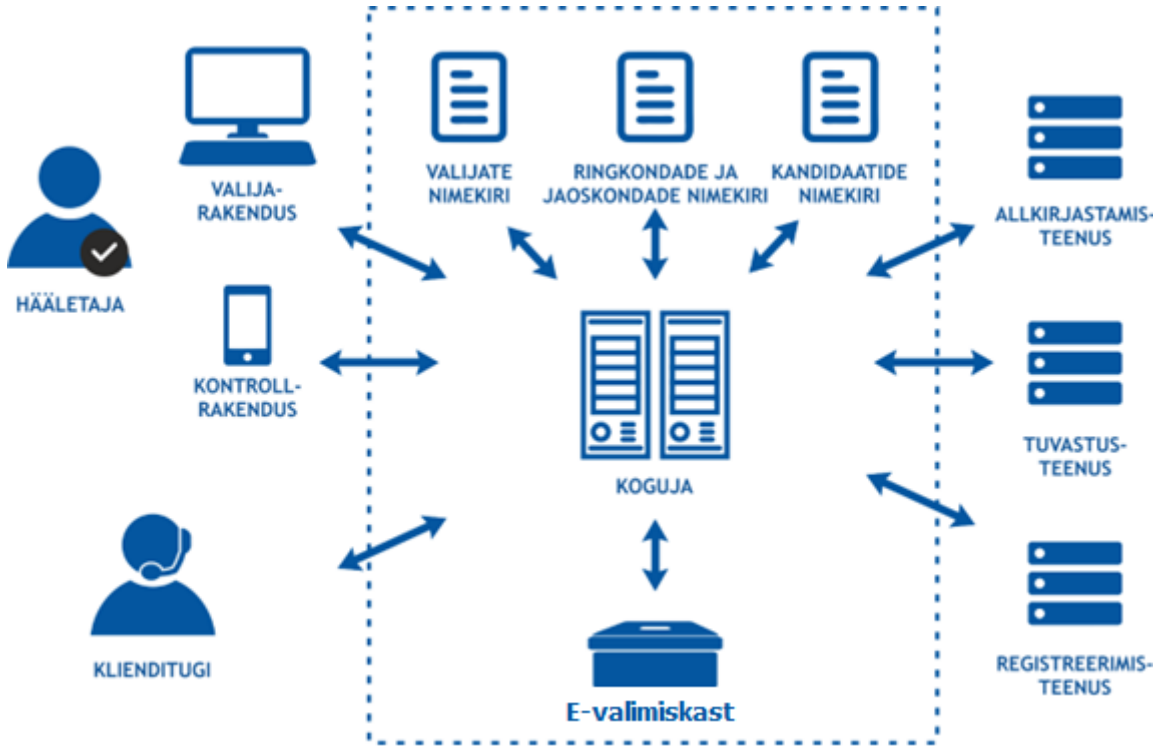
7.5. Hääletamine ja hääle kontrollimine

Hääletaja kasutab hääletamiseks arvutisse paigaldatud Valijarakendust, mis suhtleb Kogumisteenusega. Kogumisteenus kasutab oma töös valijate nimekirja, kandidaatide nimekirja ning jaoskondade ja ringkondade nimekirja. Hääletaja identifitseerimiseks võib Kogumisteenus kasutada Tuvastusteenust; krüpteeritud häälele digitaalse allkirja andmisel aitab Kogumisteenus Hääletajat, kasutades välist Allkirjastamisteenust. Kogumisteenus registreerib digitaalselt allkirjastatud hääle Registreerimisteenuses. Valijarakendus teavitab Hääletajat hääle õnnestunud talletamisest, väljastades asjakohase QR-koodi.

Hääle kontrollimiseks kasutab Hääletaja nutiseadmesse laetud Kontrollrakendust, mis suhtleb samuti Kogumisteenusega. Kontrollrakendus saab oma tööks vajalikud andmed Valijarakendusest, lugedes QR-koodi nutiseadme kaamera abil. Kontrollrakendus teavitab Hääletajat

2 Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014 , e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul, http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014R0910

Kogumisteenusesse talletatud valikust.



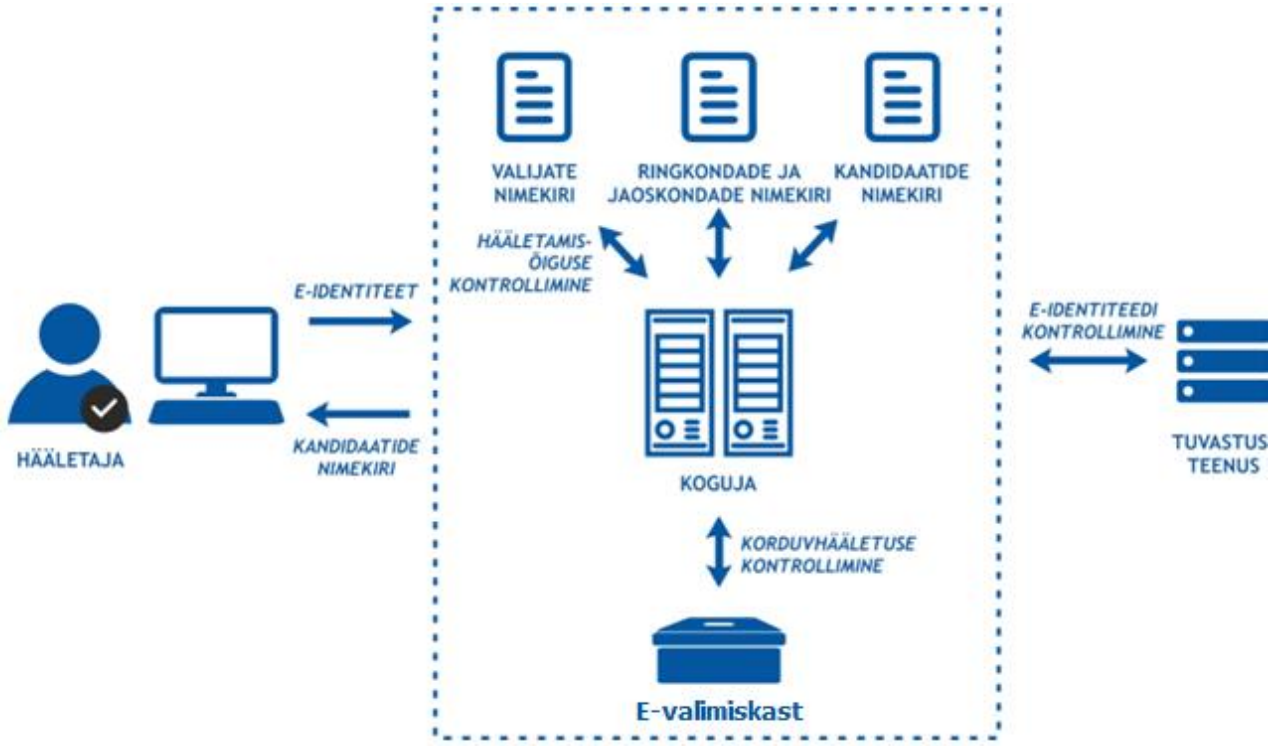
Joonis 4. Osapooled hääletamisel

Valijarakenduse laeb Hääletaja alla Korraldaja poolt hallatavalt veebilehelt. Kontrollrakendust saab paigaldada nutiseadmesse vastava rakenduste poe kaudu, paigaldamisjuhised on samuti veebilehel. Nii veebilehe kui ka Valijarakenduse autentsust ja terviklust saab kontrollida andmete abil, mille Korraldaja on turvaliselt avaldanud.

Hääletamine toimub kahes faasis, tuvastamis- ja hääletamisfaasis.

Tuvastamisfaasis tuvastatakse hääletaja ning saadetakse talle valikud.

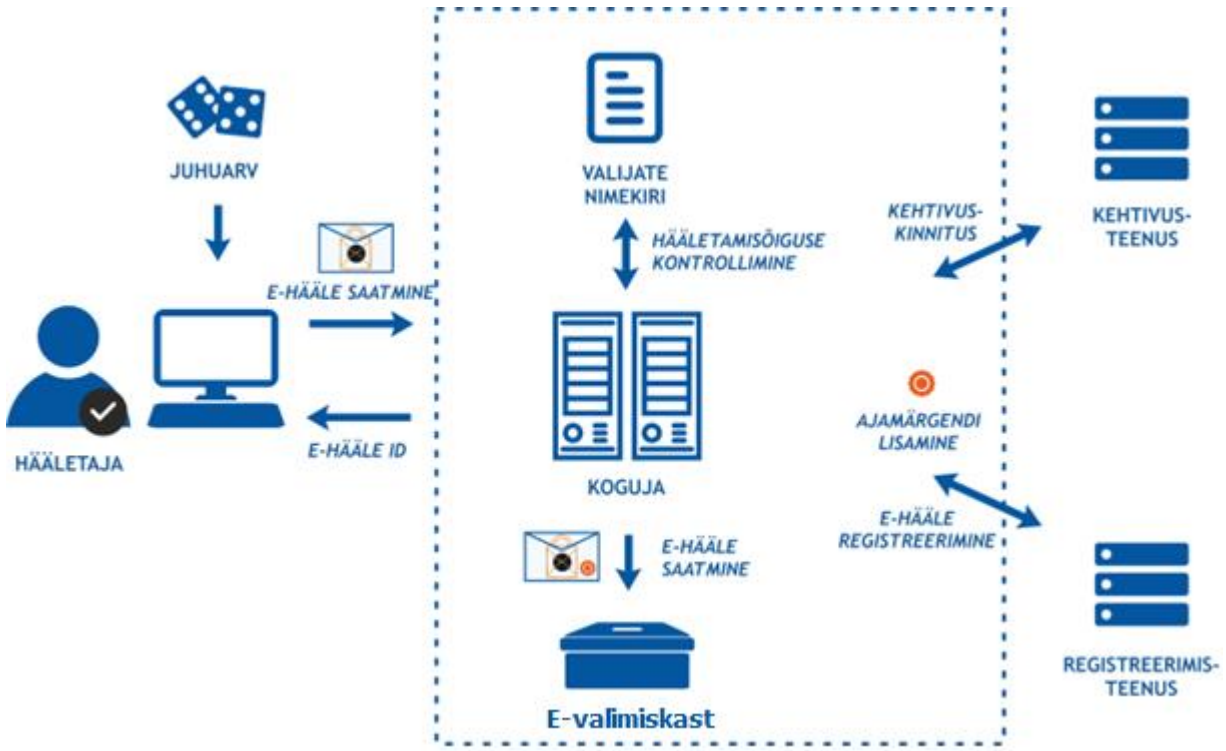
1. Hääletaja valib endale sobiliku autentimisvahendi.
2. Valijarakendus pöördub turvatud andmesideprotokolli abil Kogumisteenuse poole, toimub Hääletaja tuvastamine vastavalt valitud autentimisvahendile. Kogumisteenus kasutab vajadusel välist Tuvastusteenust.
3. Kogumisteenus kontrollib, kas valija on juba e-hääletanud. Positiivsel juhul informeeritakse sellest Hääletajat, kes võib siiski jätkata ja anda uue, eelmist asendava, hääle.
4. Kogumisteenus tuvastab valijate nimekirjast Hääletaja hääleõiguse ja tema valimisringkonna. Kui hääleõigus puudub, kuvatakse veateade.
5. Kogumisteenus saadab Valijarakendusele kuvamiseks Hääletaja ringkonnas kandideerivad kandidaadid või rahvahääletuse küsimuse vastusevariandid.



Joonis 5. Hääletaja identifitseerimine

Tuvastamisfaasile järgneb **Hääletamisfaas**, kui Hääletaja hääletamist ei katkesta. Hääletamisfaas kulgeb järgnevalt:

1. Hääletaja teeb kuvatud kandidaatide seast valiku. Valijarakendus krüpteerib valiku koos *juhuarvuga* ja häälte salastamise võtmega.
2. Hääletaja signeerib oma krüpteeritud valiku allkirjaga vastavalt jaotisele 7.3 ning saadab selle koos oma sertifikaadiga Kogumisteenusele. Kogumisteenus kontrollib Hääletaja olemasolu valijate nimekirjas ning varustab hääle kehtivuskinnitusega.
3. Krüpteeritud ja allkirjastatud hääl tuleb registreerida. Selleks kasutab Kogumisteenus eraldi Registreerimisteenust või kasutab võimalusel ära kehtivuskinnituses leiduvat ajamärgendit.
4. Kogumisteenus teavitab Valijarakenduse vahendusel Hääletajat hääle edukast vastuvõtmisest ning talletamisest. Hääletajale väljastatakse QR-kood, mis sisaldab krüpteerimisel kasutatud *juhuarvu* ja Kogumisteenuse poolt hääle registreerimisel genereeritud ühekordset *hääleidentifikaatorit*.

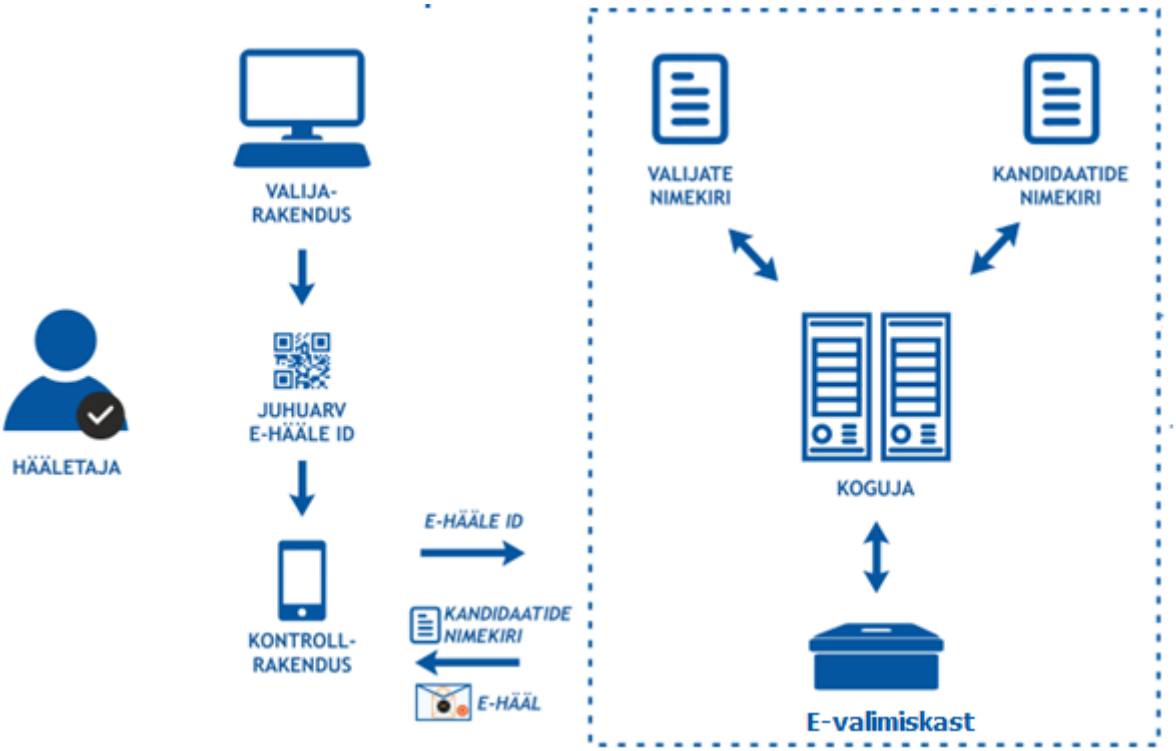


Joonis 6. Hääletamisfaas: valiku teele saatmine

Kontrollimisfaas. Selleks, et veenduda oma valiku terviklikus kohalejõudmises Kogujani, saab Hääletaja kasutada hääletamiseks kasutatud arvutist erinevat nutiseadet. Nutiseade peab olema varustatud kaamera ja internetiühendusega ning sellesse peab olema paigaldatud Kontrollrakendus, mis varustatakse kontrolli teostamiseks vajalike parameetrite ja usaldusankrutega.

Hääle kohalejõudmise kontroll toimub järgnevalt:

1. Hääletaja käivitab elektroonilise hääletamise kontrollrakenduse ning skaneerib Valijarakenduse poolt kuvatud QR-koodi.
2. Kontrollrakendus teeb päringu Kogumisteenusele e-hääle kohta, kasutades hääle identifitseerimiseks QR-koodis sisalduvat *hääleidentifikaatorit*. Päringuga tagastatakse nutiseadmesse elektrooniline hääl.
3. Kontrollrakendus kontrollib Kogumisteenuse autentsust, hääle digitaalset allkirja ning selles sisalduvat, registreerimisel saadud, ajamärgendit.
4. Kontrollrakendus arvutab hääle krüpteerimisel kasutatud *juhuarvu* ja häälte salastamise võtit teades hääletaja poolt tehtud valiku.
5. Kontrollrakendus kuvab hääletaja andmed ja tehtud valiku.



Joonis 7. Hääle kontrollimine

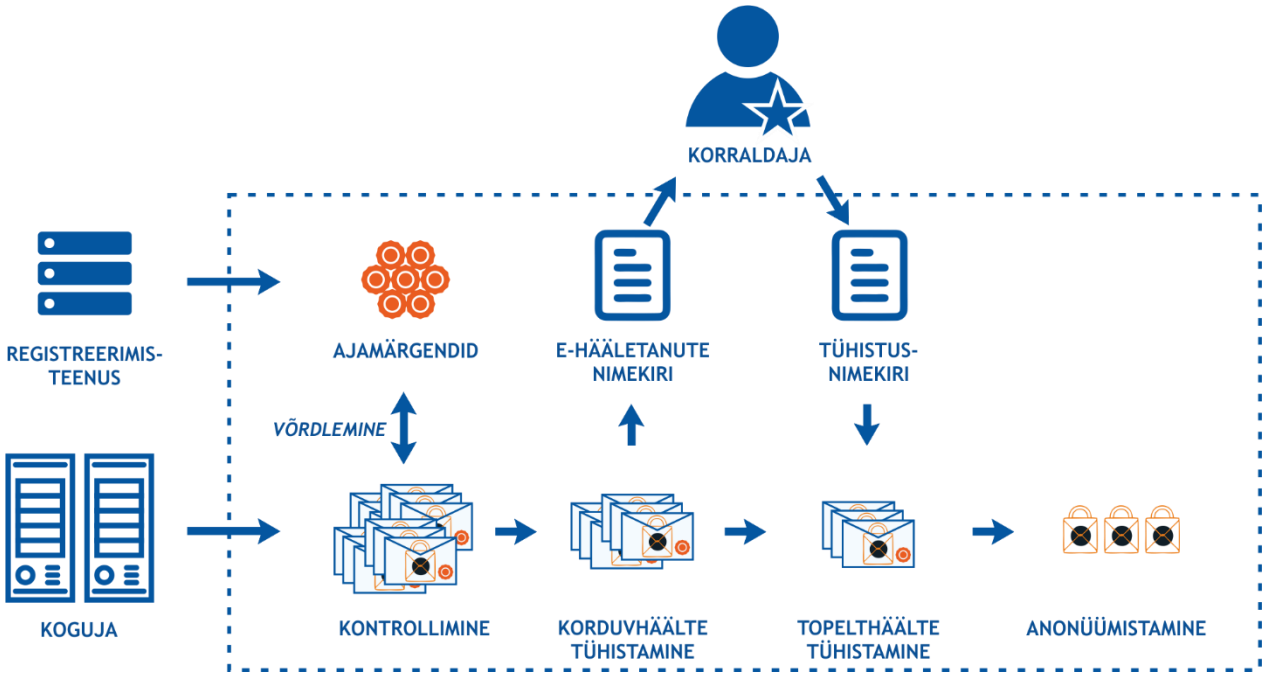
Hääle kohalejõudmist saab kontrollida piiratud aja jooksul teatav arv kordi. Piirangud kehtestab Korraldaja.

Pärast Hääletamisperioodi lõppu komplekteerib Koguja e-valimiskasti kogutud hääled ning allkirjastab e-valimiskasti kontrollsumma. Allkirjastatud e-valimiskasti kontrollsumma ja e-valimiskast edastatakse Töötlejale. Hääletamisprotsessi käigus tekkinud tehnilised logid antakse üle Korraldajale, kes võib nende kontrollimiseks kasutada Audiitori abi.

Registreerimisteenuse osutaja annab Töötlejale üle kõik ajamärgendid, lisades omapoolse digitaalse allkirja.

7.6. Häälte töötlemine

Häälte töötlemine toimub pärast hääletamisperioodi lõppu ja enne kokkulugemist. Töötlemise etappe viib läbi Töötleja, nendest viimast – miksimist, võib läbi viia ka eraldi osapool: Miksija. Töötleja allkirjastatab kõikide etappide tulemid. Häälte töötlemine toimub andmesidevõrgust lahtiühendatud keskkonnas.



Joonis 8. Häälte töötlemise etapid

Töötlemise põhietapid:

I: e-valimiskasti tervikluse kontroll.

1. Töötleja kontrollib iga individuaalse hääle digitaalallkirja ning selles leiduva ajamärgendi olemasolu Registreerimisteenuselt saadud infos.
2. Töötleja kontrollib kõikide Registreerimisteenuselt saadud ajamärgendite olemasolu häälte kogumis.

Etapi tulemuseks on need e-valimiskasti hääled, millele leiti vaste Registreerimisteenuselt saadud andmekogumis. Selle etapi lõpus *võib* häältelt eemaldada digitaalallkirjad, säilitades samas terviklikul moel seose krüpteeritud hääle, selle andnud isiku ja hääle andmise aja vahel.

II: korduvate e-häälte tühistamine. Eemaldatakse Hääletaja antud korduvad hääled, jättes alles vaid ühe, viimasena antud e-hääle. Etapi lõpus *võib* eemaldada hääle andmise aja, säilitades seose krüpteeritud hääle ja selle andnud isiku vahel.

Paralleelhääletamise kasutamisel koostatakse etapi lõpuks nimekiri e-hääletanud isikutest, mis laetakse valimiste infosüsteemi topelthääletamise (e-hääl ja paberhääl) tuvastamiseks. Tuvastatud topelthäältest koostatakse *tühistusnimekiri* isikutest, kelle e-hääl tuleb tühistada. Nimekirja allkirjastab Korraldaja.

III: topelthääletanute häälte tühistamine (ainult paralleelhääletamise korral).

Eemaldatakse e-hääled Hääletajatelt, kelle nimi sisaldub *tühistusnimekirjas*.

Alles jäävad unikaalsed isikustatud e-hääled. Enne nende kokkulugemist tuleb need anonüümistada, samas säilitades seose hääle ja ringkonna vahel.

IV: e-häälte anonüümistamine.

1. Töötleja rühmitab e-hääled ringkondade kaupa.
2. Töötleja eemaldab e-häältelt seosed neid andnud isikutega.

Etapi tulemuseks on ringkonniti rühmitatud anonüümsed e-hääled (krüptogrammid valitud

kandidaatidest).

Selleks, et häälte kokkulugemine oleks avalikult kontrollitav, võib kasutada häälte krüptograafilist segamist ehk **miksimist**.

V (valikuline): miksimine. Töötleja (või selleks volitatud Miksija) miksib anonüümsed e-hääled ringkondade kaupa kasutades Miksimisrakendust. Miksimine koosneb häälte segamisest ja krüptograafilisest permuteerimisest ehk ümberjärjestamisest. Viimati nimetatud tehnika kasutamise eelduseks on *homomorfse krüptosüsteemi* kasutamine hääle salastamisel. Miksimine peab toimuma nii, et tema nii sisendi kui ka väljundi dekrüpteerimine annaks sama tulemuse. Protsessi kõrvaltulemusena väljastatakse *miksimistõend,* mida saab Auditirakenduse abil kasutada protsessi korrektsuse tõestamiseks.

Kokkulugemisele võib saata nii miksitud kui ka miksimata hääled. Kui Korraldaja tahab tõestada kõigile oma valduses oleva häälte avamise võtme kasutuse korrektsust kokkulugemisprotsessis, on vajalik läbida ka miksimisetapp.

7.7. Häälte kokkulugemine

Häälte avamine ja kokkulugemine toimub andmesidevõrgust lahti ühendatud keskkonnas kasutades Võtmerakendust. Kokkulugemist korraldab Lugeja koos *võtmehalduritega,* kelle vahel on jagatud häälte avamise võti.

1. Võtmerakendusse laetakse kandidaatide ja ringkondade nimekiri.
2. Võtmerakendusse laetakse anonüümistatud (ja miksitud) hääled ning häälte allkirjastatud kontrollsumma.
3. Võtmehaldurid kasutavad häälte avamise võtme aktiveerimiseks neile võtmepaari genereerimise käigus jagatud autentimisvahendeid.
4. Hääled dekrüpteeritakse. Kui hääle dekrüpteerimise tulemus ei kuulu selles ringkonnas kandideerivate kandidaatide hulka, loetakse hääl kehtetuks.
5. Arvesse minevad hääled summeeritakse kandidaatide ja ringkondade kaupa. Kokkulugemise protsess väljastab ka *lugemistõendi,* mida saab kasutada häälte avamise korrektsuse tõestamiseks.
6. Protsessi lõpus deaktiveeritakse häälte avamise võti.

Protsessi jälgib audiitor. Lugemistõend võimaldab Auditirakenduse abil kontrollida protsessi matemaatilist korrektsust. Juhul, kui lugemisele läinud hääled olid miksitud, saab kokkulugemise korrektsust kontrollida ka avalikult.

Lugeja allkirjastab kokkulugemise tulemused digitaalselt.

8. Turvalisus ja auditeerimine

Käesolevas dokumendis kirjeldatud e-hääletamise süsteem tagab valimistele esitavad põhinõuded täielikult ning on lisaks **täielikult verifitseeritav** - kõikide protsesside sisendit ja väljundit saab omavahel matemaatiliselt kõrvutada.

Reaalsel rakendamisel sõltub süsteemi turvalisus selle kasutuskeskkonnast, infotehnoloogilise süsteemi kvaliteedist, protseduuride läbiviimise korrektsusest jms.

8.1. Krüptograafiline turvalisus

Krüptograafilises mõttes on e-hääletamise süsteemi omapäraks see, et ühel hääletamisel kogutud häälte enamik turvaomadusi peavad säilima seaduses sätestatud tähtajani. Peale seda häälte avamise võti hävitatakse, isikustatud ja krüpteeritud hääled muutuvad kasutuskõlbmatuteks.

Samas säilib teoreetiline oht, et keegi suudab süsteemist kopeerida isikustatud e-hääli ning üritab ajapikku häälte avamise võtit ära arvata, kasutades märkimisväärset arvutiressurssi pika aja vältel.

Korraldaja peab häälte salastamise krüptoalgoritmi ja võtmepikkuse valikul lähtuma ülalnimetatud ohust, võttes aluseks ajakohased krüptoalgoritmide turvalisusuuringud.

Digitaalallkirja meetodite ja -vahendite valikul piisab igapäevasest praktikast lähtumisest, pidades silmas, et allkirjastamisvahendid oleksid kasutusel ka teistes olulistes eluvaldkondades.

8.2. Põhinõuete täitmine

Hääletamise salajasus tagatakse häälte krüpteerimisega Hääletaja poolt. Kasutatakse asümmeetrilist krüptoalgoritmi nii, et häälte salastamise võtmega krüpteeritud hääli ei saa selle sama võtmega dekrüpteerida. Juhuarvu häälele lisamine on otseselt vajalik häälte salajasuse tagamiseks, et sama kandidaadi poolt antud häälte krüptogrammid oleksid erinevad.

Dekrüpteerimiseks on vaja häälte avamise võtit, mida aga ei saa enne häälte lugemise protsessi kasutada. Lugeja dekrüpteerib ainult anonüümseid hääli, kust on eemaldatud isikuandmed. Häälte avamise võtme aktiviseerimiseks on vaja mitme võtmehalduri koostööd.

Kirjeldatav süsteem toetab mitmekordset hääletamist , s.t. Hääletaja saab hääletada korduvalt, arvesse läheb ainult viimasena antud hääl. Seega sisaldab endas teatavat valimissaladust viimasena antud hääle aeg. Hääletaja viimase hääletamise aega teadvatel isikutel avaneb võimalus kontrollida, kas Hääletajalt ostetud hääl läks lugemisel arvesse või mitte. Seetõttu tuleb piiritleda isikute ring, kes arvesse minevate isikustatud häältega kokku puutuvad (Koguja, Töötleja, Audiitor, Registreerimisteenus, Allkirjastamisteenus).

Hääletamise korrektsus (hääleõiguse arvestamine, „üks isik - üks hääl" põhimõte) tagatakse hääletaja isiku tuvastamisega turvalist ja laialt kasutuses olevat allkirjastamisvahendit kasutades.

Hääletaja sõltumatus (vaba tahte arvestamine) tagatakse korduvhääletamise võimalusega, s.t. surve all hääletanu saab surve alt vabanedes uuesti hääletada, muutes surve all antud varasemad hääled kehtetuks. Täiendavalt saab Hääletaja valimisjaoskonnas hääletada eelhääletamise ajal või valimispäeval, mille tulemusena tühistatakse kõik Hääletaja antud e-hääled.

8.3. Verifitseeritavus

E-hääletamine koosneb mitmest põhiprotsessist, mis on kirjeldatud 7. peatükis. Protsesse saab verifitseerida, kontrollides matemaatiliselt protsessi sisendi ja väljundi kooskõlalisust.

Verifitseerimine on sõltuvalt selle läbiviijast kas:

a) individuaalne – Hääletaja kontrollib ise,

b) delegeeritud – kontrollijaks on Audiitor,

c) avalik/universaalne – kontrollida saavad kõik soovijad.

Hääletaja saab individuaalselt verifitseerida oma isikliku hääle kohale jõudmist Koguja e-valimiskasti ja selle registreeritust Registreerimisteenuse juures.

Audiitor saab protsesside kordamise teel verifitseerida kõiki Töötleja ja Lugeja protsesse, välja arvatud miksimine ja kokkulugemine. Viimaste jaoks kasutab Audiitor nende protsesside poolt väljastatud spetsiaalset tõendit ning Auditirakendust.

Juhul, kui anonüümistatud hääli enne kokkulugemist täiendavalt miksiti, on võimalik avalikustada ka lugemisele läinud krüptogrammid ning vastavaid abivahendeid ja -andmeid kasutades verifitseerida Lugeja tööd avalikul moel.

8.4. Auditeerimine ja vaatlemine

Audiitor on Korraldaja määratud osapool, kes teostab süsteemi tervikluse kontrollimiseks protsessi- ja andmeauditeid.

Audiitor käitleb isikustatud krüpteeritud hääli mille üks komponent on hääle andmise aeg. Neil on võimalik saada teada Hääletaja hääletamise fakt ja aeg. Neid andmeid ei tohi kopeerida ega kasutada muuks kui auditiprotsesside läbiviimiseks Korraldaja kontrollitud keskkonnas.

Protsessiauditeid kohaldatakse toimingutele, mis on seotud häälte avamise võtmega. Need toimingud viiakse läbi Võtmerakendusega, välja arvatud häälte avamise võtme hävitamine (selle kasutamise võimatuks muutmine).

Andmeauditite käigus kontrollitakse protsesside sisendi ja väljundi omavahelist kooskõla ning protsesside käigus digitaalselt allkirjastatud andmete terviklust ja autentsust. Protsesside peamised sisendid ja väljundid on:

- Koguja sisend: valijate, ringkondade ja kandidaatide nimekiri, kasutatavad autentimis- ja allkirjastamisvahendid, häälte salastamise võti ja kasutatava krüptoalgoritmi parameetrid jm.
- Koguja väljund: e-valimiskasti kogutud hääled.
- Registreerimisteenuse väljund: Kogujale väljastatud ajamärgendid.
- Väljundid Töötleja tööetappidest: e-valimiskasti tervikluse kontroll, korduvate häälte tühistamine, topelthäälte tühistamine, häälte anonüümistamine, miksimine.
- Kokkulugemisprotsessi väljund: hääletamistulemused.

Andmeauditi käigus veendub Audiitor e-valimiskasti tervikluse, korduvate häälte tühistamise ja häälte anonüümistamise korrektsuses.

Miksimise ja kokkulugemise verifitseerimiseks kasutab Audiitor lisaks sisendile ja väljundile ka miksimis- või lugemistõendit. Nende andmekogumite omavahelist kooskõla kontrollitakse Auditirakenduse abil, mille usaldatavuse tagamine on Audiitori ülesanne.