Vabariigi Valimiskomisjon

Elektroonilise hääletamise süsteemi üldkirjeldus

Dokument: EH-03-03-1
Kuupäev: 18.09.2013.a.

Tallinn
2004-2013

Annotatsioon

Antakse üldine, kuid terviklik ülevaade Eesti elektroonilise hääletamise süsteemi tehnilisest ja organisatsioonilisest poolest. Dokument on mõeldud avalikkusele ega eelda lugejailt põhjalikke tehnilisi eelteadmisi. Detailsemate nõuete ja kirjelduste saamiseks tuleb tutvuda elektroonilise hääletamise alusdokumentidega. Teksti on viimati täiendatud ja parandatud septembris 2013.

Sisukord

1 Sissejuhatus

Elektroonilise hääletamise (e-hääletamise) temaatikaga on Eestis erinevatel tasanditel aktiivsemalt tegeletud alates aastast 2001. Täna on igal hääleõiguslikul kodanikul võimalik valimistel ja rahvahääletustel anda turvalisel viisil oma hääl elektrooniliselt, sest:

- on olemas kõigis valimisseadustes kajastuv õiguslik baas e-hääletamise läbiviimiseks,
- enamikul valimisõiguslikest isikutest on olemas nende turvalist elektroonilist identifitseerimist võimaldav ID-kaart, paljudel ka mõni täiendav elektrooniline isikutunnistus nagu Digi-ID või Mobiil-ID,
- aastail 2011-2013 loodud häälte lisakontrolli mehhanism võimaldab e-hääletanutel mobiilseadme abil usaldusväärsel viisil kontrollida, kas nende hääled registreeriti süsteemi poolt korrektselt, ja sellega sisuliselt elimineeritakse e-hääletajate arvutite võimalikust ebaturvalisusest lähtuvad ohud.

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 süsteemi arhitektuuri ja tööpõhimõtteid, sealhulgas andmete liikumist ja algoritme;
- analüüsitakse ja kirjeldatakse võimalikke turvaohte ja põhjendatakse süsteemi vastavust turvanõuetele.

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

2 E-hääletamise süsteemi ulatusala

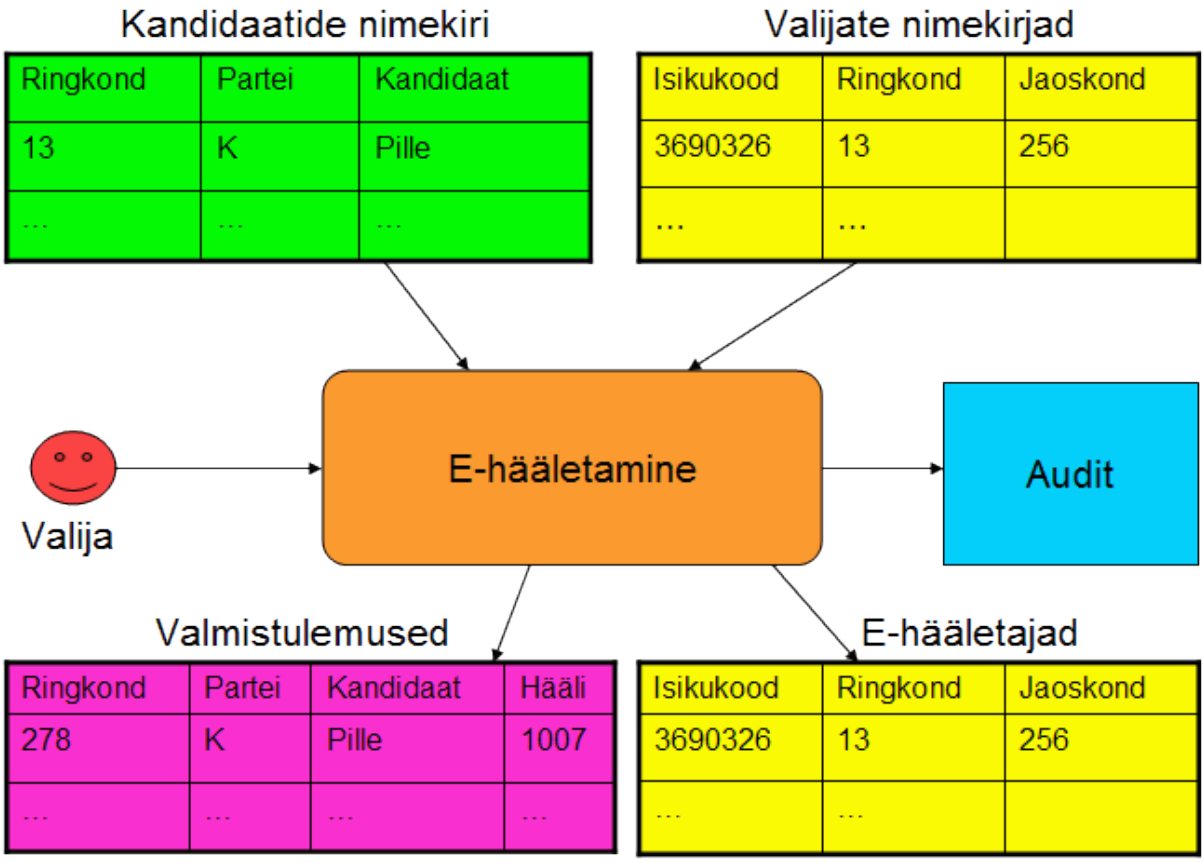
Eesti e-hääletamise süsteem katab suhteliselt väikese osa kogu valimisprotsessist. Valimised koosnevad järgmistest põhietappidest:

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

E-hääletamise süsteem katab osaliselt vaid kahte viimast, st hääletamist ja häälte kokkulugemist.

Eesti e-hääletamise süsteem eeldab, et:

1) valijate nimekirjad (koos valijaga seotud valimisjaoskonna ja valimisringkonnaga) on olemas ja sobival kujul kättesaadavad;
2) kandidaatide nimekirjad (ringkondade kaupa) on koostatud ja sobival kujul kättesaadavad;
3) 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: sisendid ja väljundid

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, kellele nad hääle andsid. Samuti peab (e-)häälte kogumine olema turvaline, usaldusväärne ja kontrollitav.

Eesti valimisseadused sätestavad järgmised nõuded:

(1) Valija saab 10. – 4. päeval enne valimispäeva hääletada elektrooniliselt.

1. Hääletamine algab 10. päeval enne valimispäeva kell 9.00 ja kestab ööpäevaringselt kuni hääletamise lõpuni 4. päeval enne valimispäeva kell 18.00.
2. Valija tõendab oma isikut digitaalset tuvastamist võimaldava sertifikaadiga, mis on välja antud isikut tõendavate dokumentide seaduse alusel.
3. Pärast valija isiku tuvastamist kuvatakse valijale tema elukohajärgse valimisringkonna kandidaatide koondnimekiri.
4. Valija märgistab oma elukohajärgse valimisringkonna selle kandidaadi, kelle poolt ta hääletab. Elektrooniliseks hääletamiseks kasutatav rakendus salastab valija hääle häälte salastamise võtmega. Valija kinnitab hääletamist digitaalallkirja seaduse nõuete kohase digitaalallkirjaga.
5. Valija saab pärast hääletamise kinnitamist teate hääle vastuvõtmise kohta.

(2) Valijal on õigus oma elektrooniliselt antud häält muuta:

1. hääletades uuesti elektrooniliselt 10. – 4. päevani enne valimispäeva;
2. hääletades hääletamissedeliga 10. – 4. päevani enne valimispäeva.

(3) Valijal on võimalik kontrollida, kas tema antud hääle on elektrooniliseks hääletamiseks kasutatud rakendus valija tahte kohaselt elektroonilise hääletamise süsteemile edastanud.

1. Elektroonilise hääle kontrollimise korra kehtestab määrusega Vabariigi Valimiskomisjon

Järgmised põhinõuded on e-hääletamise spetsiifilised:

- *Hääletaja tuvastamiseks ja hääle andmiseks kasutatakse Eestis kehtivaid elektroonilisi isikutunnistusi.* Valdaval enamusel valimisõiguslikest isikutest on ID-kaart olemas ja puudub vajadus täiendava isiku füüsilist kohalolu nõudva registreerimisprotseduuri järele.
- *Elektroonilise ülehääletamise võimalus* – e-hääletajal on võimalus uuesti e-hääletada, kusjuures vana hääl kustutatakse. Põhimõte võimaldab kaitsta e-hääletajaid survestamise vastu, sest surve all hääletanud ja hiljem surve alt vabanenud isik saab hääletada uuesti, muutes surve all antud hääle kehtetuks.
- *Tavahääletamise ülimuslikkus* – kui hääletaja läheb eelhääletamise ajal valimisjaoskonda ning hääletab tavameetodil (olles eelnevalt e-hääletanud), siis e-hääl kustutatakse. Ka see põhimõte kaitseb hääletajaid survestamise vastu.
- *Hääle registreerimise kontrollitavus* – e-hääletaja peab saama sõltumatust allikast kontrollida oma e-hääle korrektset registreerimist.
- *Tehniline auditeeritavus* – süsteem peab olema tehniliselt piisavalt lihtne, et seda saaks auditeerida võimalikult lai ring spetsialiste.
- *Taaskasutatavus* – süsteem peab katma kõik Eestis kasutatavad olulisemad hääletamisviisid, nii et igaks uueks hääletamiseks ei oleks vaja luua uut süsteemi.

4 E-hääletamise etapid

E-hääletamise läbiviimiseks luuakse elektroonilise hääletamise komisjon, mille ülesandeks on ette valmistada ja korraldada elektrooniline hääletamine. Komisjoni ülesandeks on teha kindlaks e-hääletamise tulemus.

E-hääletamine viiakse läbi neljas etapis.

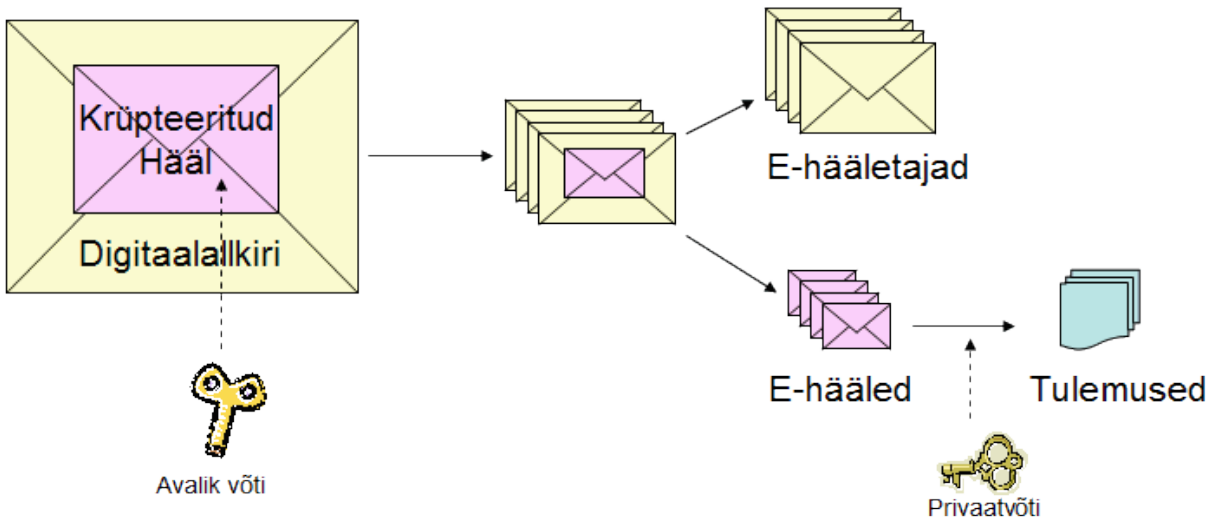
- **Hääletamiseelsel etapil** leiab aset e-hääletamise süsteemi seadistamine ning nimekirjade koostamine.
    - Kandidaatide nimekirjad ja valijate elektroonilised nimekirjad fikseeritakse hiljemalt 13. päevaks enne valimispäeva. Valijate nimekiri võib e-hääletamise ajal muutuda.
- **Hääletamisetapil** toimub hääletamine.
    - E-hääletamise võimalus avatakse 10 päeva enne valimispäeva neljapäeva hommikul kell 9 ning suletakse 4 päeva enne valimispäeva ehk valimisnädala kolmapäeval kell 18. Hääletada on võimalik ööpäevaringselt.
    - Valijate nimekirja võimalikke muudatusi kantakse e-hääletamise süsteemi kord päevas.
- Hääletamisetapile järgneb **tühistusetapp**. Sel etapil kontrollitakse, et igalt valimas käinult läheks arvesse ülimalt üks hääl.
    - E-hääled sorteeritakse, korduvad hääled tühistatakse.
    - E-hääletamise komisjon koostab valimisjaoskondade kaupa e-hääletanute nimekirja.
    - E-hääletanute nimekiri edastatakse maakonna valimiskomisjonidele hiljemalt teisel päeval enne valimispäeva. Maakonna valimiskomisjon edastab nimekirja jaoskonnakomisjonidele hiljemalt valimispäevale eelneval päeval.
    - Kui valija on e-hääletanud, teeb jaoskonnakomisjoni liige valijate nimekirja märke elektroonilise hääletamise kohta.
    - Kui valija on hääletanud nii elektrooniliselt kui ka hääletamissedeliga, arvestatakse valija hääletamissedelit. Jaoskonnakomisjon saadab e-hääletamise komisjonile asjakohase teatise, mille alusel jäetakse valija e-hääl arvestamata.
- **Lugemisetapp**
    - E-hääletamise tulemus tehakse kindlaks valimispäeval pärast kella 19.00.
    - Häälte lugemise juures peab viibima vähemalt pool e-hääletamise komisjoni ning VVK koosseisust, sealhulgas komisjonide esimehed või aseesimehed.
    - Enne hääletamistulemuse kindlaks tegemist tühistatakse jaoskonnakomisjonide poolt viidatud hääled, seejärel eraldatakse e-hääled valijate isikuandmetest.
    - Hääletamistulemuse kindlakstegemiseks avab VVK e-hääled häälte avamise võtmega.
    - E-hääletamise komisjoni esimees allkirjastab hääletamistulemuse, tulemus sisestatakse valimiste infosüsteemi.

5 E-hääletamise süsteemi üldskeem

E-hääletamise skeem rajaneb nn. „ümbrikuskeemile“, mis sarnaneb posti teel hääletamisele tavavalimistel, kus anonüümne kinnine ümbrik häälega asetatakse hääletaja nime ja allkirjaga välimisse ümbrikusse. E-hääletamiseks kasutatava programmi (nn. *valijarakenduse*) abil, e-hääletaja:

1) krüpteerib hääle ja juhuslikult arvuti poolt valitud *kontrollkoodi* süsteemi *häälte salastamise võtmega* (moodustades nii „sisemise ümbriku“), ja
2) digitaalallkirjastab krüpteeritud hääle digitaalallkirjastamise vahendiga (moodustades nii “välimise ümbriku”).

Häälte salastamise võtmega krüpteeritud häält saab dekrüpteerida üksnes häälte avamise võtmega, mida “teab” ainult Häältelugemisrakendus – elektroonilise hääletamise komisjoni valduses turvalises keskkonnas hoitav ja Internetist täielikult eraldatud arvuti, millele antakse ligipääs vaid VVK otsusega.



Joonis 2. Ümbrikuskeem

Juhusliku kontrollkoodi saab iga hääletaja laadida oma mobiilseadmesse ja selle abil kontrollida, kas tema hääl registreeriti süsteemi poolt korrektselt.

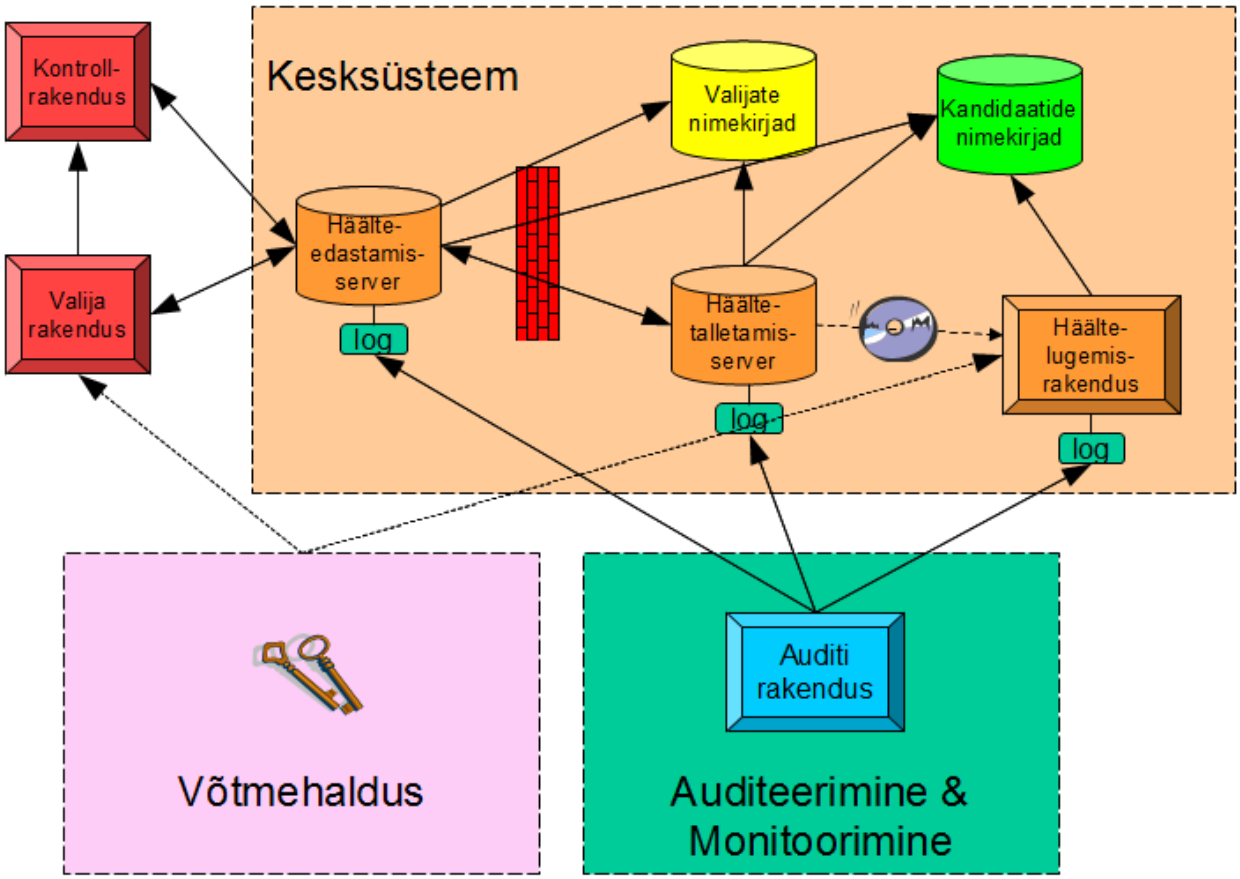
Krüpteeritud ja digitaalallkirjastatud hääled kogutakse kokku, sorteeritakse, kontrollitakse isikute valimisõigust ning eemaldatakse üleliigsed hääled (korduvad hääled, valimisõiguseta isikute hääled).

Enne e-häälte kokku lugemist eemaldatakse krüpteeritud häältelt digitaalallkirjad. Krüpteeritud hääled, mis enam ei seostu hääletanud isikutega, edastatakse turvalisel viisil häältelugemisrakendusele. Digitaalallkirjade põhjal moodustatakse e-hääletanute nimekiri.

Häältelugemisserver dekrüpteerib hääled häälte avamise võtmega, loeb üle ja väljastab summaarsed e-hääletamise tulemused.

6 Süsteemi arhitektuur ja osapooled

Elektroonilise hääletamise süsteemi arhitektuuri kirjeldab Joonis 3.



Joonis 3. E-hääletamise süsteemi üldarhitektuur

Süsteemi osapooled (Joonisel 3 tähistatud kastidena) on:

- **Valija** – e-hääletaja arvutis krüpteeritakse hääl, allkirjastatakse digitaalselt ja saadetakse Kesksüsteemi.
- **Kesksüsteem –** e-hääletamise komisjoni vastutuse all olev süsteemiosa, mis võtab vastu ja töötleb hääli ning väljastab lõpuks koondtulemuse.
- **Võtmehaldur –** tegeleb süsteemi võtmepaari genereerimise ja haldamisega. Häälte salastamise võti integreeritakse Valijarakendusesse, häälte avamise võti salvestatakse turvaliselt ja antakse sobival hetkel Häältelugemisrakendusele.
- **Auditeerimine –** Lahendab e-hääletamisega seotud kaebusi Kesksüsteemi logide abil.

Kesksüsteem sõltub Rahvastikuregistrist, kes koostab valijate nimekirjad. Kandidaatide nimekirjad koostab Vabariigi Valmiskomisjon.

Valija poolt kasutatavad komponendid on järgmised:

- **Valijarakendus** vahendab valija ja Kesksüsteemi vahelist suhtlust ning võimaldab valijal valikut krüpteerida ja digitaalselt allkirjastada. Valijarakendus kuvab kontrollkoodi, mille alusel saab kontrollida e-hääle korrektset jõudmist Kesksüsteemi.

- **Kontrollrakendus** võimaldab valijal Valijarakendusest erineval platvormil veenduda, et tema e-hääl jõudis Kesksüsteemi ning väljendas tema tahet korrektselt.

Kesksüsteemi põhikomponendid on järgmised:

- **Häälteedastamisserver (HES)** tuvastab elektroonilise identiteedi abil hääletaja isiku, tema valimisõiguse, edastab hääletajale tema piirkonna kandidaadid, võtab vastu krüpteeritud ja digitaalselt allkirjastatud e-hääle, mille edastab koheselt Häältetalletamisserverile ja edastab sealt saadud positiivse kättesaamisteate hääletajale. HES lõpetab töö pärast e-hääletamise lõppu. HES-s hoitakse ka Valijate nimekirjade andmebaasi, mis on e-hääletamise perioodil dünaamiline tagamaks näiteks e-hääletamise võimaluse andmist ka isikutele, kes registreerivad oma elukoha „viimasel minutil“. E-hääletamise perioodi lõppedes nimekirjade andmebaas fikseeritakse, kuid e-hääletamise perioodi vältel uuendatakse Valijate nimekirja regulaarselt. HES on ainus Interneti vahendusel kättesaadav kesksüsteemi komponent. Kõik ülejäänud Kesksüsteemi komponendid on Internetist eraldatud ning neisse on võimaldatud juurdepääs ainult HES-st.
- **Häältetalletamisserver (HTS)** võtab HES-lt vastu ja talletab e-hääli. Pärast e-hääletamise lõppu eemaldab HTS korduvad hääled ning võtab vastu ja täidab e-häälte tühistusi. Lõpuks eemaldab HTS krüpteeritud häältelt digitaalallkirjad ja valmistab need ülelugemiseks ette.
- **Häältelugemisrakendus (HLR)** on vallasrežiimis komponent, kuhu kantakse üle krüpteeritud hääled, millelt on eemaldatud digitaalallkiri. HLR dekrüpteerib hääled häälte avamise võtme abil, summeerib kehtivad hääled ja väljastab e-hääletamise tulemused.
- **Auditirakendus** on komponent, mille abil kontrollitakse HES, HTS ja HLR logide kooskõlalisust.

7 E-hääletamise protseduurid

7.1 Võtmehaldus

Võtmehalduse protseduurid ja kasutatav turvaskeem on e-hääletamise süsteemi üks kriitilisemaid kohti, millest sõltub süsteemi põhinõuete (valimiste privaatsus ja salajasus) täitmine.

Valimiste salajasus tagatakse häälte krüpteerimisega. Luuakse süsteemi võtmepaar (häälte salastamise ja avamise võti).

Häälte salastamise võti integreeritakse valijarakenduse tarkvarasse ja seda kasutatakse häälte krüpteerimiseks.

Häälte avamisvõtit kasutatakse Häältelugemisrakenduses häälte dekrüpteerimiseks. Avamisvõtme kasutamine on võimalik vaid häälte kokkulugemise ajal, st valimispäeval kell 19.00. Pärast kaebuste lahendamise perioodi lõppu häälte avamisvõti hävitatakse.

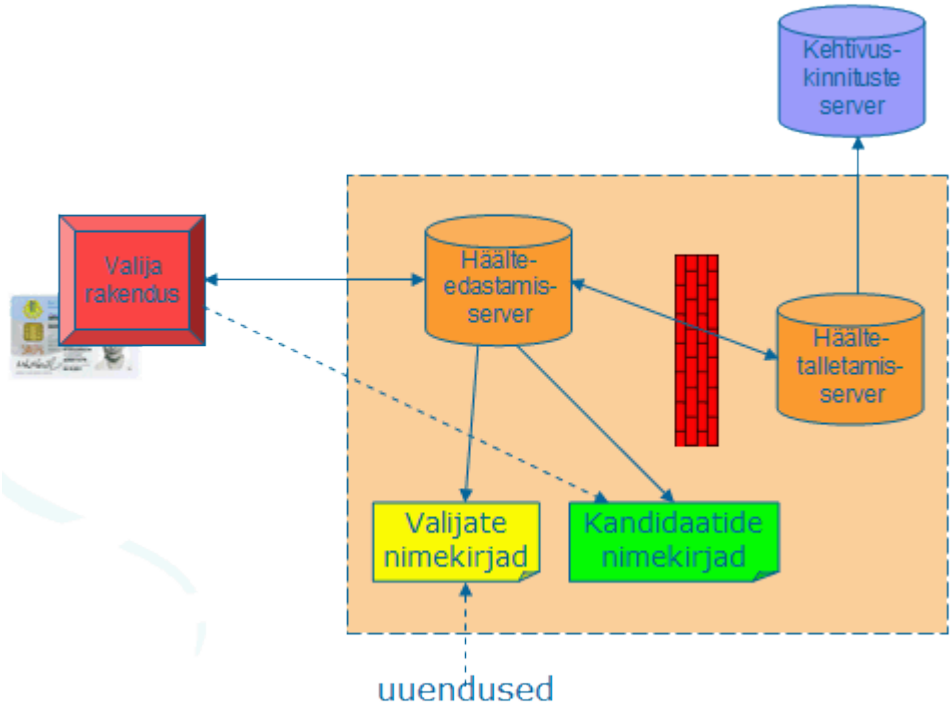
Võtmepaar genereeritakse riistvaralises turvamoodulis (HSM – *Hardware Security Module*). Häälte avamisvõtit talletatakse turvamoodulis kogu valimise vältel.

Võtmepaari genereerimist ja avamisvõtme kasutamist korraldavad seitse *võtmehaldurit*, kelleks on VVK liikmed. Turvamooduli aktiveerimine on võimalik ainult siis kui kohal on vähemalt neli VVK liiget seitsmest. Võtmehalduritel on füüsilised ja teadmuslikud autentimisvahendid (kiipkaart ja parool) turvamooduliga suhtlemiseks.

Võtmehalduse protseduure auditeeritakse, sealhulgas võtmepaari ja paroolide genereerimist, häälte salastamise võtme integratsiooni valijarakendusse, häälte avamise võtme säilitamist, dubleerimist ning kasutamist HLRs.

7.2 Hääletamine, häälte talletamine ja kontrollimine

Hääletamine toimub Valija, Valimisrakenduse ja HES vahelise transaktsioonina. HES teeb päringuid Valijate nimekirjade ja Kandidaatide nimekirjade lokaalsesse andmebaasi ning saadab lõpuks hääle HTS-i.



Joonis 4. Hääletamise protsessis osalevad komponendid

Valija laadib oma brauseri abil alla signeeritud Valijarakenduse, mis töötab veebikeskkonnast sõltumatult ja mis küsib valijalt tema valiku, genereerib juhusliku kontrollkoodi, krüpteerib hääle koos kontrollkoodiga ja digitaalallkirjastab krüptogrammi.

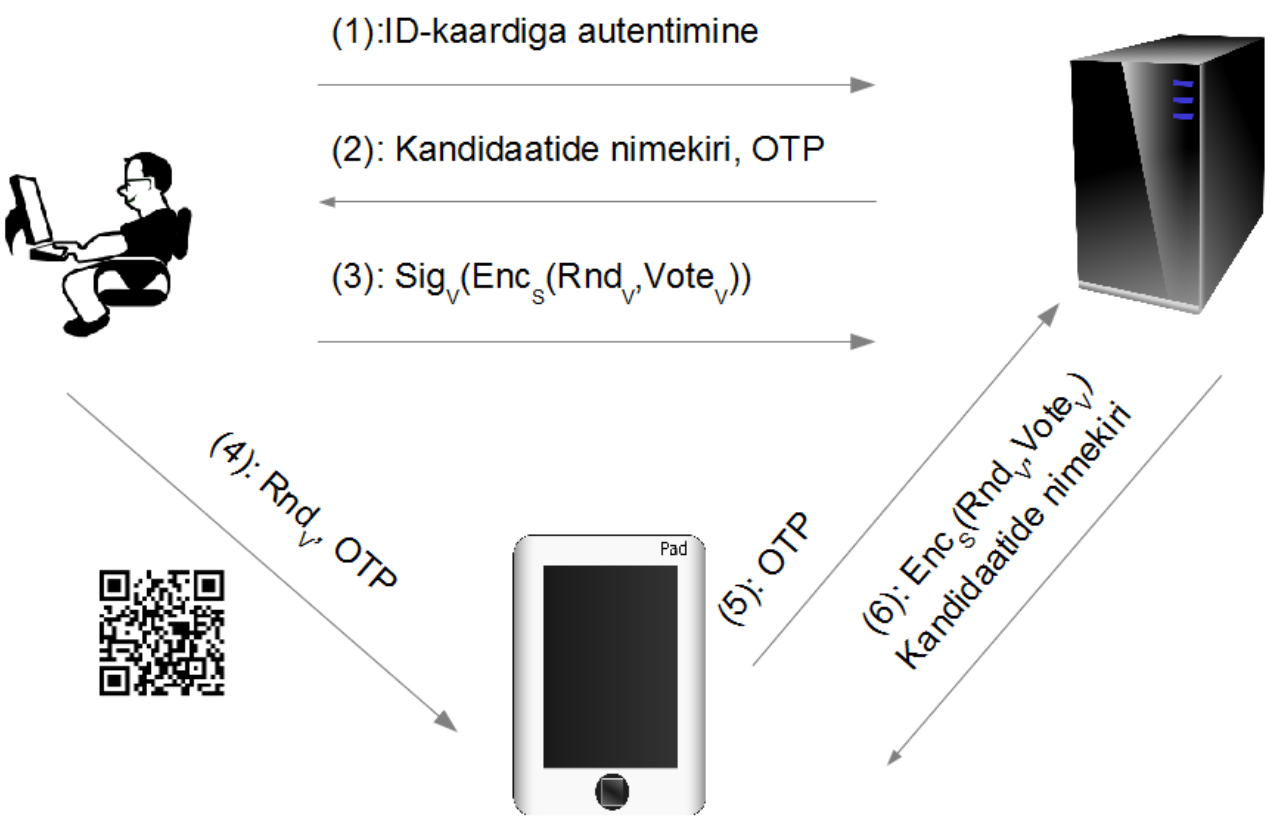
Hääle talletamise protseduur toimub järgmiselt:

1. Valijarakendus pöördub HTTPS-protokolli abil HES-i poole. Valijat autenditakse ID-kaardi või Mobiil-ID abil.
2. HES teeb päringu Valija isikukoodi (IK) abil Valijate nimekirjade andmebaasi ning tuvastab valimisõiguse ja valimisringkonna. Kui valimisõigus puudub, kuvatakse veateade.
3. HES teeb päringu HTS-i ja kontrollib, kas valija on juba e-hääletanud. Positiivsel juhul informeeritakse valijat.
4. HES teeb ringkonna järgi päringu Kandidaatide nimekirjade andmebaasi ning kuvab Valijale päringuvastuseks saadud ringkonnas kandideerivad isikud.
5. Valija valib meelepärase kandidaadi.
6. Valijarakendus küsib kasutajalt kinnitust tehtud valiku kohta, kuvades valitud kandidaadi nime.
7. Valijarakendus krüpteerib valiku ja juhusliku kontrollkoodi häälte salastamise võtmega. Valija allkirjastab krüptogrammi oma ID-kaardi või mobiil-ID abil.
8. Valijarakendus saadab allkirjastatud krüptogrammi HES-le. HES kontrollib sõnumi vormingut ning digiallkirja andnud isiku vastavust sessiooni alguses autenditud isikuga.
9. HES saadab krüpteeritud ja digitaalallkirjastatud hääle edasi HTS-le. HTS kontrollib digitaalallkirja kehtivust, pöördub kehtivuskinnituste serveri poole ning hangib sealt tõendi sertifikaadi kehtivuse kohta, mis lisatakse allkirjastatud häälele. HTS kinnitab hääle vastuvõtmist omapoolse digitaalallkirjaga. Logisse 1 kantakse kirje hääle vastuvõtmise kohta, mis sisaldab isikukoodi ja krüpteeritud hääle räsiväärtust.
10. Positiivsel juhul saadab HTS HES-ile teate hääle vastuvõtmise kohta ning hääle identifikaatori kontrollrakendusele edastamiseks. Vastav teade edastatakse ka Valijarakendusele, mis kuvab Valijale nii kontrollkoodi kui hääle identifikaatorit ühes QR koodis.
11. Valija võib hääletada mitu korda. Kõik hääled edastatakse läbi HES-i HTS-le. Korduva hääle andmisel tühistatakse eelnevalt antud hääl ning logisse 2 kantakse tühistuskirje, mis sisaldab lisaks isikukoodile ja krüpteeritud hääle räsiväärtusele ka tühistamise põhjust.
12. Pärast e-hääletamise lõppu HES seiskub.

Peale hääletamist on Valijal võimalik kontrollida oma häält kasutades Valijarakendusele saadetud kontrollkoodi, mis kuvatakse ekraanile QR-koodina. Valija skaneerib kontrollkoodi oma mobiilseadmesse kasutades Kontrollrakendust, mis on eelnevalt mobiilseadmesse laaditud kas mingist platvormi-põhisest avalikust rakenduste baasist või Vabariigi Valimiskomisjoni koduleheküljelt. Põhimõtteliselt on võimalik ka kontrollrakendus ise luua, sest kõik vastavad tehnilised liidesed on avalikud.

Kontrollrakendus küsib Kesksüsteemilt krüpteeritud hääle, leiab kandidaadi numbri, kelle poolt hääletati, ja kuvab selle mobiilseadme ekraanile. Kandidaadi leidmine on võimalik, kuna kontrollrakendusel on kontrollkood. Osapooled, kellel kontrollkoodi ei ole – näiteks kesksüsteem või kolmandad osapooled – ei saa krüpteeritud häälest kandidaati ilma dekrüpteerimata tuvastada. Seega on hääle salajasus jätkuvalt kaitstud, kuid valija saab ise kontrollida, kas ekraanile kuvatud

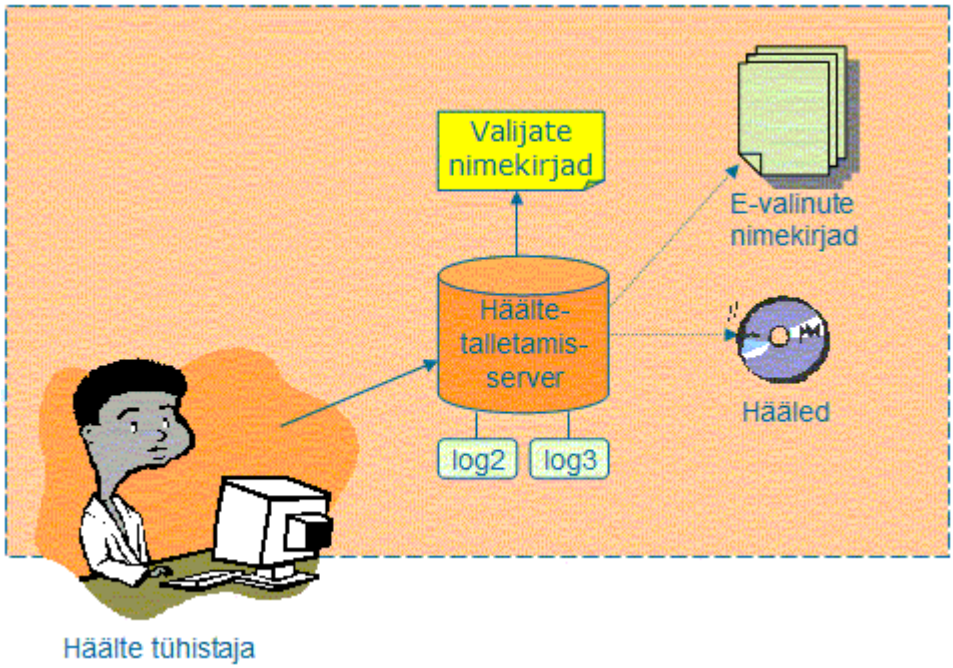
number vastab tema poolt tegelikult valitud kandidaadile.



Joonis 5. Hääle kontrollimine

7.3 Häälte tühistamine ja sorteerimine

Pärast hääletusperioodi lõppu eraldatakse Häältetalletamisserver arvutivõrgust ning koostatakse valimisjaoskondade kaupa nimekirjad e-hääletanud isikutest (nimi, isikukood ja rea number valimisjaoskonna valijate nimekirjas). Nimekirjad saadetakse koos eelhääletanud isikute ümbrikega valimisjaoskondadesse. See protseduur hoiab ära ühe isiku hääle (e-hääle ja tavahääle) kahekordse lugemise.



Joonis 6. Tühistamine ja sorteerimine

Jaoskonnakomisjonid märgivad valijate nimekirja elektrooniliselt hääletanud isikud. Nemad enam valimispäeval hääletada ei saa. Seejärel koostavad jaoskonnakomisjonid avalduse e-häälte tühistamiseks. Sinna kantakse isikud, kes on andnud e-hääle ja ka eelhääletanud valimisjaoskonnas.

E-hääletamise komisjon koostab üle-eestilise tühistamise koondnimekirja, allkirjastab selle digitaalselt ning edastab selle HTS-le. Viimane kontrollib digitaalallkirja, talletab tühistusavalduse ning tühistab e-hääled, kandes need logisse 2.

VVK volitatud tühistajal on võimalik esitada HTS-ile digitaalselt allkirjastatud tühistusavaldusi kui ka tühistamise ennistamisavaldusi, juhul kui selgub, et tühistamine oli inimlik eksimus.

Tühistamiste perioodi lõppedes, vahetult enne häälte kokkulugemist, eraldatakse digitaalallkirjad häältest järgmiste etappidena.

1. Hääled sorteeritakse valimisringkondade kaupa. Digitaalallkirjast saadud isikukoodi järgi tehakse päring valijate nimekirjade baasi ja tehakse kindlaks ringkond.
2. Digitaalallkirjad eemaldatakse, järele jäävad häälte salastamise võtmega krüpteeritud hääled.
3. Hääled valmistatakse ette üle kandmiseks HLR-i välisel andmekandjal (mälupulk vms.).

Kõik HLR-le saadetavad (isikukoodi ja krüpteeritud hääle räsiväärtust sisaldavad) kirjed kantakse logisse 3.

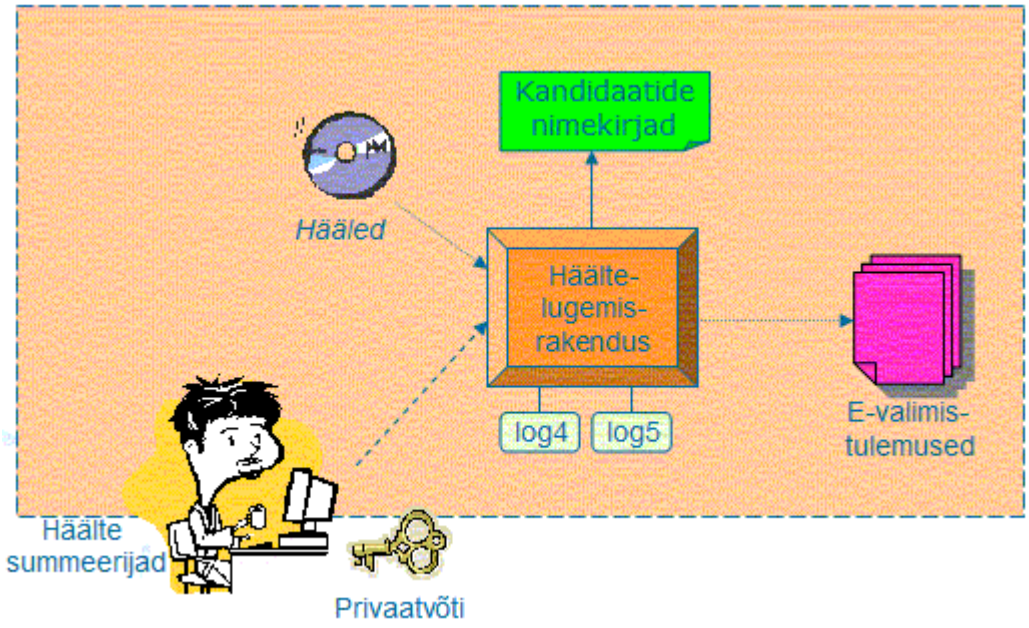
7.4 Häälte kokkulugemine

Häälte summeerimine toimub võrgust eraldiseisvas Häältelugemisrakenduses (HLR), kus on olemas ka lokaalne Kandidaatide nimekirja koopia.

Häälte kokkulugemise toiming on korratav, s.t. võimalik on kontroll-lugemine teises arvutis HLR riistvaratõrgete puhuks.

Häälte summeerimiseks aktiveerivad võtmehaldurid häälte avamise võtme.

Ringkondade kaupa sorteeritud hääled transporditakse HTS-st HLR-i välisel andmekandjal.



Joonis 7. Häälte kokkulugemine.

Hääled dekrüpteeritakse ringkondade kaupa häälte avamise võtme abil. Ka krüpteeritud hääled jäetakse esialgu alles. Pärast dekrüpteerimist kontrollitakse kandidaatide nimekirja abil, kas ringkonnas on valitud kandidaadi poolt võimalik hääletada. Kui kandidaadi number ei klapi ringkonnaga või kui dekrüpteeritud hääl ei vastanud e-hääle vormistusnõuetele, tunnistatakse hääl kehtetuks ja hääle räsiväärtus kantakse logisse 4. Ametlik Valijarakendus garanteerib e-hääle vastavuse vormistusnõuetele.

Arvesse minevad hääled summeeritakse kandidaatide ja ringkondade kaupa. Iga arvesse mineva krüpteeritud hääle räsiväärtus kantakse logisse 5.

E-hääletamise tulemused liidetakse tavavalimiste tulemustele.

7.5 Auditirakenduse funktsioonid

E-hääletamise süsteem toodab oma erinevates etappides erinevaid logisid, täpsemalt:

Logi 1: vastvõetud hääled kujul: *isikukood, räsiväärtus*

Logi 2: tühistatud hääled kujul: *isikukood, räsiväärtus, põhjus*

Logi 3: lugemisse läinud hääled kujul: *isikukood, räsiväärtus*

Logi 4: kehtetud sedelid (vale kandidaadi nr.) kujul: *räsiväärtus*

Logi 5: arvestatud hääled kujul: *räsiväärtus*

Krüpteeritud hääle räsiväärtus on räsifunktsiooni kollisioonikindluse tõttu hääle unikaalne tunnus, kuid samas ei võimalda kindlaks teha, kuidas on hääletatud. Seda isegi juhul, kui häälte avamise võti on teada.

Auditirakendus võimaldab logisid omavahel võrreldes tuvastada, mis sai igale konkreetsele isikukoodile vastavast häälest.

- Võeti vastu – sisaldub logis 1.
- Tühistati selle tõttu, et isik käis eelvalimistel – vastav kirje logis 2.
- Tühistati selle tõttu, et isik korduvhääletas elektrooniliselt – vastav kirje logis 2.

- Tühistati selle tõttu, et „valimissedelis” oli kandidaadi number, kes ei kandideerinud vastavas ringkonnas – vastavad kirjed logis 3 ja logis 4.
- Läks arvesse: vastavad kirjed logis 3 ja logis 5.

Peale selle on auditirakendusel võimalik kontrollida logide terviklust – logide 2 ja 3 ühisosa peab vastama logile 1, logide 4 ja 5 ühisosa peab vastama logile 3.

Kõik logikirjed sisaldavad ka kirje logimise aega.

8 Turvalisus

E-hääletamise süsteem, piisavate organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete rakendamise korral, loob aluse e-hääletamise läbiviimiseks vähemalt sama turvaliselt, kui seda on tavahääletamine. Lisainformatsiooni saab e-hääletamise turvaanalüüsi dokumendist.

8.1 Põhinõuete täitmine

Hääletamise faasis tagatakse *hääletamise salajasus* häälte krüpteerimisega. Kasutatakse asümmeetrilist krüptoalgoritmi, nii et häälte salastamise võtmega krüpteeritud hääli ei saa selle sama võtmega dekrüpteerida. Dekrüpteerimiseks on vaja häälte avamise võtit, mida aga ei saa enne häälte lugemise protseduuri kasutada. Häälte avamise võtme aktiviseerimiseks on vaja mitme isiku (võtmehalduri) koostööd. Juhusliku kontrollkoodi häälele lisamine on otseselt vajalik häälte salajasuse tagamiseks, sest vastasel korral oleks krüpteeritud hääle abil võimalik häälte salastamise võtit kasutades proovimise teel kindlaks teha, kelle või mille poolt hääletati.

Häälte lugemise faasis tagatakse *hääletamise salajasus* organisatsiooniliste meetmetega: mitte ühelgi isikul ei ole samaaegselt juurdepääsu digitaalallkirjastatud häälte krüptogrammidele ja dekrüpteeritud häältele.

Hääletamise korrektsus (hääleõiguse arvestamine, üks isik-üks hääl printsiip) tagatakse hääletaja isiku tuvastamise abil elektroonilise identiteedi põhjal.

Hääletaja sõltumatus (vaba tahte arvestamine) tagatakse korduvhääletamise võimalusega, s.t. surve all hääletanu saab surve alt vabanedes uuesti hääletada muutes nii surve all antud hääled kehtetuks.

8.2 Tarkvara ja integratsioon

E-hääletamiseks kasutatav tarkvara on välja töötatud Eestis. Välismaise päritoluga programmvara (operatsioonisüsteemid, komponendid, teegid, jne.) on kasutatud nii, et nende komponentide võimaliku kompromiteerituse mõju e-hääletamise süsteemi turvaloogikale on minimeeritud.

Tarkvara lähtekood auditeeritakse, kompileeritakse sõltumatus keskkonnas ning testitakse selle funktsionaalsust. Auditi läbinud tarkvara käivituskood signeeritakse, signatuur publitseeritakse.

Süsteemsete komponentide (operatsioonisüsteem, veebiserver, tugiteegid) valikul, paigaldamisel ja konfigureerimisel peetakse silmas järgmisi punkte.

- Aluseks võetakse võimalikult stabiilsed (s.t. pikemalt ekspluatatsioonis olnud ja testitud) komponendid. Komponentide tunnusinfo (allikad, kontrollsummad, jne.) dokumenteeritakse.
- Komponendid võetakse algallikast, **kõik** muudatused (süsteemiosade kustutamised, konfiguratsioon) dokumenteeritakse.
- Pärast e-hääletamist teostatav järelkontroll peab olema suuteline samasuguse süsteemi oleku saavutama tuginedes algallikast mahalaaditavale tarkvarale ning järgides dokumentatsioonis fikseeritud muudatusi.

8.3 Hääle kohalejõudmise kontrollitavus

Iga e-hääletaja hääletamise turvalisus sõltub otseselt tema koduarvuti (kui eeldatavalt enimkasutatava e-hääletuskeskkonna) turvalisusest. Viirused ja ründetarkvara võivad koduarvutis sihilikult mõjutada hääletamistulemust.

Eesti e-hääletamise süsteemis on igal hääletajal võimalik oma isikliku mobiilseadme (nutitelefon,

tahvelarvuti vms) abil usaldusväärselt kontrollida, kas tema hääl jõudis modifitseerimata kujul Kesksüsteemi.

Kontrollitavuse olemasolu ei aita mitte üksnes oluliselt tõsta iga hääletaja isiklikku turvalisust. Kontrollitavuse olulisim efekt on hääletajate koduarvutitele suunatud ulatuslike (ja valimistulemusi oluliselt mõjutavate) rünnete avastamine. Kui kasvõi 5% e-hääletajatest oma häält kontrollib, muutub ulatuslike rünnete märkamatu teostamine võimatuks.