

Vabariigi Valimiskomisjon

# **E-hääletamise organisatsiooniline ja tehniline kontseptsioon**

Autor: Tarvi Martens

Dokument: EH-01-03  
Kuupäev: 11.11.2003.a.

- Tallinn 2003 -

## **Annotatsioon**

Dokument pakub kontseptsiooni tasemel välja e-hääletamise süsteemi eesmärgiga anda valijatele võimalus esmakordselt valida Eestis 2005.a. kohalike omavalitsuste valimistel ka elektrooniliselt ehk Interneti vahendusel ja ID-kaardi abil. Dokumendi klass „kontseptsioon“ tähistab, et ta peaks olema piisavaks aluseks nii tehniliste detailprojektide koostamiseks, organisatsioonilise mudeli kokkuleppimiseks ning samas olema ka piisavalt arusaadav otsustajatele ja rahvavalgustajatele. Tegemist on esimese etapi tulemusega 2003.a. augustis käivitatud e-hääletamise projektist.

## Sisukord

Annotatsioon .....	1
Sisukord.....	2
Sissejuhatus .....	3
1. E-hääletamise süsteemi ulatusala .....	4
2. Nõuded, eeldused ja mööndused e-hääletamisele .....	7
3. E-hääletamise protsessi etapid .....	10
4. E-hääletamise süsteemi üldkontseptsioon.....	12
5. Süsteemi arhitektuur ja osapooled.....	14
6. E-hääletamise protseduurid .....	16
6.1. Võtmehaldus.....	16
6.2. Hääletamine ja häälte talletamine .....	17
6.3. Häälte sorteerimine ja tühistamine .....	18
6.4. Häälte kokkulugemine.....	20
6.5. Auditirakenduse võimalused .....	21
7. Tarkvara arendusest, keskkondadest ja integratsioonist .....	23
8. Süsteemi vastavus nõuetele, võimalikud ohud .....	25
9. Kokkuvõte .....	27
10. Viited.....	28

## Sissejuhatus

E-hääletamise teemaga on Eestis erinevatel tasanditel aktiivsemalt tegeletud selle sajandi algusest peale. Nüüdseks on aga võimalus ja põhjus e-hääletamise projekt ka ellu viia eesmärgiga pakkuda valijatele 2005.a. kohalike omavalitsuse valimistel e-hääletamise võimalust kuna:

- On olemas seadusandlik baas e-hääletamise läbiviimiseks, mis kajastub järgmistes seadustes:
  - Kohaliku omavalitsuse volikogu valimise seadus §50
  - Riigikogu valimise seadus §44
  - Euroopa Parlamendi valimise seadus §43
  - Rahvahääletuse seadus §37
- On loodud turvalist elektroonilist isiku tuvastust ja digitaalallkirja andmist võimaldav avaliku võtme infrastruktuur ID-kaardi näol – hetkeks (oktoober 2003) on väljastatud üle 310 000 ID-kaardi, 2005. aasta valimisteks peaks see arv olemasoleva väljaandmise graafiku kohaselt liginema 800 000 ID-kaardile ehk katma valdava enamiku valimisõiguslikest isikutest.
- Võimuoleva valitsuse koalitsioonilepingus seisab: “Koalitsioon seab eesmärgiks luua tingimused, et 2005. aasta kohalikel valimistel oleks võimalik rakendada e-valimisi.”

Käesolev kontseptsioonidokument on esimene üldkirjeldus planeeritava e-hääletamise tehnilisest ja organisatsioonilisest süsteemist, mille põhjal peaksid valmima täpsustavad dokumendid. See dokument:

- määratleb e-hääletamise süsteemi ulatusala (skoobi) ehk piiritleb teema valimiste koguprotsessis;
- sätestab süsteemile esitatavad nõuded;
- määratleb süsteemis osalevad osapooled ja kirjeldab nende tegevuse;
- annab e-hääletamise süsteemi arhitektuuri, toimimise üldkirjelduse ning kirjeldab andmete liikumist ja algoritme;
- analüüsib ja kirjeldab võimalikke turvaote ja vaatleb süsteemi vastavust püstitatud turvanõuetele.

Selles dokumendis on paiguti juttu kuid põhirõhu alt jäävad välja:

- süsteemi komponentide turvaseme täpne määratlemine;
- täpsete andmestruktuuride spetsifitseerimine;
- tark- ja riistvaraplatvormide valik;
- süsteemi võrgutehniline skeem – serverite dubleerimine, rakendatavad võrguturbevahendid (tulemüürid, ründetuvastussüsteemid), võrguühenduste arhitektuur.

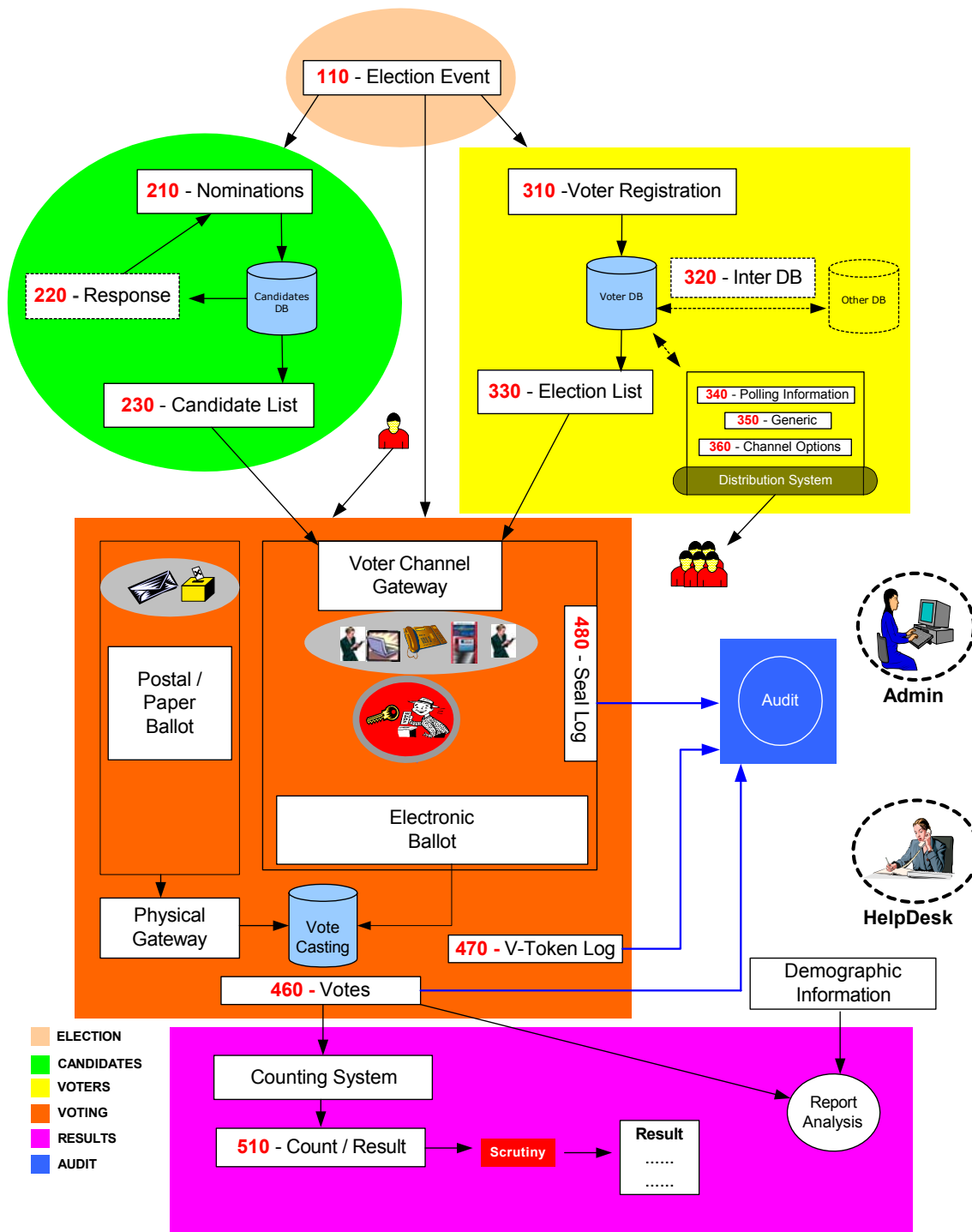
*Autor on tänulik paljude kolleegide tõhusa sisendi eest kontseptsiooni koostamiseks. Eraldi soovin ära märkida Arne Ansperi abistav-kritiseerivat rolli dokumendi valmimisel.*

## **1. E-hääletamise süsteemi ulatusala**

Käsitletav e-hääletamise süsteem on suhteliselt väikene osa kogu valimisprotsessist. Tehnilise vaatenähtena koosnevad valimised järgmistest allosadest:

- Valimiste väljakuulutamine
- Kandidaatide registreerimine
- Valijate nimekirjade koostamine
- Hääletamine (siia kuulub ühe alamhulgana ka e-hääletamine)
- Häälte kokkulugemine

Kõrvalosadena võib veel ära märkida auditeerimist, protestide lahendamist jm. tugitegevust. Ülal kirjeldatud illustreerib järgmine EML mudelist [EML] laenatud skeem:



Joonis 1. Valimiste tehniline vaade.

Selles dokumendis käsitletav e-hääletamise süsteem eeldab, et:

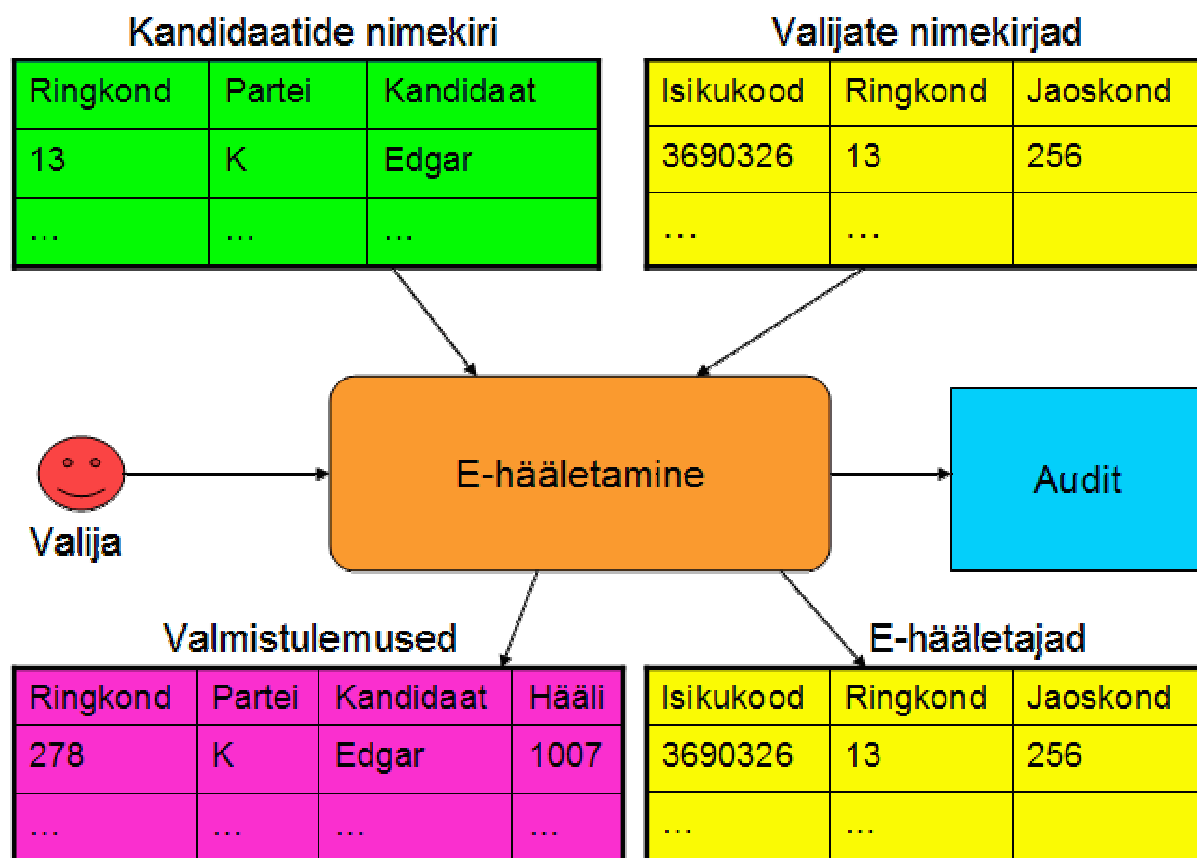
- valijate nimekirjad on olemas ja sobival kujul kättesaadavad,
- kandidaatide nimekiri on koostatud ja sobival kujul kättesaadav,
- e-hääled summeeritakse eraldi ning liidetakse pärast teiste hääletega (see on erinevus ülaltoodud joonisest).

Teisiti väljendudes on e-hääletamise süsteemi sisenditeks:

- valijate nimekirjad (koos valijale omistatud valimisjaoskonna ja valimisringkonnaga)

- kandidaatide nimekirjad (ringkondade kaupa)
  - valijate tahteavaldused
- ning väljunditeks:
- summeeritud valimistulemused e-hääletanute kohta
  - e-hääletanud isikute nimekiri

E-hääletamise süsteemi ulatusala ning sisend-väljundparameetreid piltlikustab alljärgnev joonis:



Joonis 2. E-hääletamise ulatusala: sisendid ja väljundid

## 2. Nõuded, eeldused ja mööndused e-hääletamisele

Käesolevas jaotises sedastame nõuetekogumi, millele e-hääletamise süsteem peab vastama. Alustame üldistest põhimõtetest, seejärel kitsendame nõudeid Eesti keskkonna jaoks. Seejärel teeme mõningad eeldused keskkondade turvalisusele ja osapoolte usaldatavusele. Mõningaid nõudeid on kommenteeritud, sellisel juhul on tekst *kursiivis*.

Alustame üldiste nõuetega, mis kajastavad nii lokaalseid kui rahvusvahelisi valmisseadusi ja –praktikat.

Põhinõuded:

- Valimiste salajasus:
  - Valija poolt antud hääл peab jääma salajaseks kuni hääлte kokkulugemise hetkeni;
  - Keegi ei tohi mingilgi hetkel teada saada, kelle poolt on valija hääлетanud;
  - Valija tuvastamine peab olema võimalik ilma valija poolt antud hääлe salajasust rikkumata.
- Sunnitamatus (*uncoercibility*) – valijad ei tohi saada hiljem tõestada, kelle poolt nad on valinud.
- Kontrollitavus – igal soovijal peab olema võimalik kontrollida, et tema hääл on hääлte kokkulugemisel arvesse võetud.
- „Üks isik – üks hääл“ – iga valija poolt antud hääлtest peab arvesse minema ainult üks hääл.

*Üldiseks printsiibiks turvanõuete järgmisel tuleb silmas pidada seda, et süsteem oleks vähemalt sama turvaline kui tavaline valimissüsteem. Kui e-hääletamissüsteem pakub veelgi paremaid turvaomadusi, on see plussiks.*

*Näiteks „Kontrollitavuse“ nõuet ei ole realistlik realiseerida tavavalimiste puhul, küll on aga see võimalik e-hääletamise puhul, mistõttu selle nõude edukas realiseerimine teeks e-hääletamise tavahääletamisest turvalisemaks.*

Järgmised põhimõtted on Eesti-spetsiifilised:

- Hääлетaja autentimiseks kasutatakse ID-kaarti, hääлетada võivad ainult hääлеõiguslikud ja tuvastatud valijad (eeldus on, et hääлеõiguslikest isikutest on olemas andmebaas)

*Kuigi võiks kaaluda ka näiteks pankade autentimisteenuseid, oleks see liialt suur risk. Autentimisteenuse osutajal on võimalik suhteliselt lihtsasti valimistulemusi mõjutada. Peale selle näevad e-hääletamisel seadused ette digitaalallkirja kasutamist, see on aga võimalik praktilises plaanis ainult ID-kaardi abil. E-hääletamise projekteeritava süsteemi ja pankade infosüsteemi vahel on veel üks põhimõtteline vahe – e-hääletamise süsteemi turvalisus põhineb tema avalikkusele ja auditeeritavusele. Süsteemi toimimise alused ja tarkvara on sõltumatuks hindamiseks kättesaadavad kõigile osapooltele ja pideva avaliku järelevalve all. Pankade infosüsteeme, vastupidi, iseloomustab salajasuse nõue – nad ei tohi tulenevalt seadusandlusest jm põhjustest avalikustada oma kasutatavate süsteemide detaile. Kui hakata pankade süsteeme*



*kasvõi osaliselt e-hääletamises kasutama, tähendaks see teatud süsteemide kirjelduse avalikustamist, mis ei pruugi olla pankade huvidega kooskõlas.*

- Elektroonilise ülehääletamise võimalus – e-hääletajal peab olema võimalus uuesti hääletada, vana hääle selle peale kustutatakse

*Kuigi tavaliselt käsitletakse mitmekordset hääletamist kuriteona (Karistusseadustik, §165), siis antud juhul on tegu meetmetega hääle ostmise vastu – surve all olnud hääletaja saab üle hääletada peale seda kui ta surve alt vabaneb. Seega ei ole elektrooniline „ülehääletamine“ käsitletav „mitmekordse hääletamisena“ kuna süsteem annab väljundiks ainult ühe (viimasena antud) hääle.*

- Tavahääletamise ülimuslikkus – kui hääletaja läheb valimispäeval valimisjaoskonda ning hääletab tavameetodil (olles eelnevalt e-hääletanud), siis e-hääle kustutatakse

*Sarnaneb eelmise nõude põhjendusega. Vajalik ka üldisemaks puhuks – kui näiteks ilmneb, et eelhääletamise ajal toimunud e-hääletamise süsteem on põhjalikult kompromiteeritud või halvatud ning kõik või osa e-hääli tuleb tühistada, siis annavad hääletajad oma hääle traditsioonilisel viisil.*

- Silmas peaks pidama neljas Eesti seaduses esinevat e-hääletamise punkti (seaduste muutmise on võimalik, kuid komplitseeritud):
  - (1) Valija, kellel on digitaalallkirja sertifikaat, saab eelhääletamise päevadel hääletada elektrooniliselt Vabariigi Valimiskomisjoni veebilehel. Valija hääletab ise.
  - (2) Valija tõendab oma isikut digitaalallkirja andmisega.
  - (3) Pärast valija isiku tuvastamist kuvatakse veebilehel valijale tema elukohajärgse valimisringkonna kandidaatide koondnimekiri.
  - (4) Valija märgistab veebilehel selle oma elukohajärgse valimisringkonna kandidaadi, kelle poolt ta hääletab, ning kinnitab hääletamist.
  - (5) Valija saab veebilehel teate hääle arvestamise kohta.

*Käesolev kontseptsioon lähtub toodud piirangutest.*

Tehnilised nõuded:

- Skeem peab olema võimalikult lihtne ning kasutama võimalikult standardseid krüptoalgoritme (RSA, AES, SHA-1)

*Igasuguste keeruliste ja vähe läbi uuritud krüptoalgoritmide kasutamine teeb süsteemi keerulisemaks, raskemini auditeeritavaks ning tõstab turvariski.*

- Kõik e-hääletamise süsteemi sisulist loogikat realiseerivad komponendid peavad olema lähtekoodi tasemel võimalikult lihtsasti auditeeritavad.

*Süsteemi tarkvarakomponendid võib tinglikult jagada „mustadeks kastideks“ ja „valgeteks kastideks“. Mustad kastid on need süsteemsed komponendid (operatsioonisüsteem, veebiserver, keele kompilaator/interpretaator), mille lähtekoodi ei auditeerita. Mustade kastide puhul on tähtis terviklus ja töökindlus. „Valged kastid“ on need, mis tegelevad süsteemis sisuliste andmete töötlusega, sealhulgas*

*krüptograafiliste operatsioonidega. Valged kastid peavad olema lähtekoodi tasemel auditeeritavad.*

- Taaskasutatavus – süsteem peab olema taaskasutatav ka järgmiste e-hääletamiste korraldamisel, võimaldades kulusid kokku hoida selle kaudu, et iga kord ei ole tarvis uut süsteemi projekteerida ja teostada, vaid võib taaskasutada juba olemasolevat.

*Käesolev kontseptsioon käsitleb KOV e-hääletamise süsteemi, kus sarnaselt Riigikogu valimistega on oma osa ringkondadel. Rahvahääletustel ja Europarlamendi valimistel on ainult üks ringkond ning kogu skeem seega lihtsam. Seetõttu on KOV e-hääletamist võimaldav süsteem lihtsa kohaldamisega rakendatav ka muudel juhtudel.*

Nõuete, õigemini – soovitude kirjeldamisega on tegelema asunud ka Euroopa Nõukogu juurde moodustatud IP1-S-EE töörühm [IP1]. Nende soovitusel on jagatud juriidilisteks, eksploatatsioonilisteks ja tehnilisteks. Nende töö on alles algusjärgus ja põhineb vähestel kogemustel (Inglise ja Šveitsi pilootprojektid ja –süsteemid) ja antavad soovitusel on ühelt poolt liialt üldised ja teiselt poolt liialt kitsendavad (näiteks EML kasutamine). Sellegi poolest on kasulik nende töödokumentides toodud soovitude arvesse võtmine süsteemi projekteerimise käigus.

Kogu süsteemi 100% turvalisuse tagamine on teoreetiliselt lahendamatu ülesanne. Et piiritleda lahendamist vajavaid turvaküsimusi eeltoodud nõuete täitmiseks, teeme järgnevalt mõningad eeldused keskkonnale:

- keskserveri(te) turvalisus tagatakse tehniliste ja organisatsiooniliste meetmete abil – skeem ei pea ette nägema „ebaosaldatavaid“ servereid
- Vabariigi Valimiskomisjon (VVK) on piisav ja vajalik neutraalne keskne usaldatav osapool

*Kui hakata skeemis ette nägema usaldatava osapoole (VVK) kontrolli all olevaid „ebaosaldatavaid“ servereid, siis tõuseks skeemi keerukus suurusjärkude võrra. Lihtsam on tagada töökorralduse ja audiitorkontrolli läbi see, et kesksüsteemid töötaksid nii nagu ette nähtud. Kindlasti tuleb sellest eeldusest tulenevad ohud kaardistada ja vastavad meetmed kavandada.*

- Valija arvuti turvalisus on tehnilise lahenduse ulatusalast väljas.

*Skeemi valija-poolne komponent peab tagama parima võimaliku turvalisuse (signeeritud rakendus, tervikluskontrollid jne.). Samas on täieliku turvalisuse tagamine valija arvutis on praktiliselt võimatu ülesanne – ei saa eeldada, et valijate arvutid on trooja- ja viirusevabad (ja selle vastu ei anna keskselt ka midagi ette võtta). Parim, mis keskselt teha saab, on teavitustöö, soovitades valijatel paigaldada viimased operatsioonisüsteemi paigald, kasutada antiviiirusprogramme jne.*

*Jällegi – sellest eeldusest tulenevad ohud tuleb kaardistada.*

### 3. E-hääletamise protsessi etapid

Valimisseadused sätestavad, et e-hääletamine toimub eelhääletamise päevadel. See annab aega koostada valimispäevaks valijate nimekirjad nii, et nendel oleks näha, kes on juba eelnevalt e-hääletamise abil hääletanud.

Eraldi tuleb käsitleda olukorda, kus hääletaja on käinud eelhääletamas ja andnud ka e-hääle. Praeguse seadusandluse järgi sellisel juhul e-hääl kindlasti tühistatakse, eelhääl aga tühistatakse vastavalt sellele kus ta antud on – kui see on antud elukohajärgses valimisjaoskonnas, siis seda ei tühistata (kastist enam häält kätte ei saa), kui aga elukohavälises jaoskonnas (hääletamine ümbrikusse), siis see tühistatakse. **Nimetatud vastuolu tuleb seadusandlusest kõrvaldada, st võrdsustada erinevates jaoskondades antud eelhääled ning neid mitte tühistada.**

Kuna nõuetes on sätestatud ka tavavalimiste ülimuslikkus, siis tuleb ette näha ka protseduur, millega **turvaliselt** teatatakse eelhääletanud valijate ja valimispäeval valimisjaoskonnas käinute e-hääle tühistamisest enne hääle kokkulugemist. Siin on oluline moment, et e-hääletamise süsteem peab ette nägema e-hääle tühistamise meetodi, samas tagades selle e-hääle salastatuse.

Sellised piirangud annavad järgmise ajakava:

- Kandidaatide elektroonilised nimekirjad ja valijate nimekirjad peavad olema fikseeritud hiljemalt valimiseelse nädala pühapäevaks. Valijate nimekiri muutub dünaamiliselt e-hääletamise perioodi jooksul.
- Üheaegselt eelhääletamisega avatakse e-hääletamise võimalus, tavaliselt valimiste nädala esmaspäevast kuni kolmapäevani. Ööpäevaringse e-hääletamise võimaluse kõrval võib kaaluda ka e-hääletamise võimaluse andmist ainult päevasel ajal (8.00..24.00), et tagada süsteemide reaal-aja monitooring rünnete vastu.
- E-hääletamise lõppedes fikseeritakse lõplikult (e-hääletamise süsteemi jaoks vajalik) valijate nimekiri.
- E-hääled sorteeritakse, korduvad hääled ja valimisõigust mitte omavate isikute hääled tühistatakse.
- Peale eelmist sammu saadetakse valimisjaoskondadesse nimekirjad e-hääletanud isikutest (ja ka eelhääletajatest koos ümbrikusse pandud häälega), mille peale teevad valimisjaoskonnad valijate nimekirjadesse vastavad märkmed. See tegevus peab olema lõppenud valimispäevale eelneva päeva õhtuks. **E-hääletanute nimekirjade kohalejõudmine ja töötlemine valimisjaoskondades on protsessi kriitiline etapp – kui see informatsioon ei jõua jaoskonda, siis saab isik anda kaks häält.**
- **Valimispäeval saavad e-hääletanud ümber hääletada kuni kella 17.00-ni.** Nendest valijatest, kelle e-hääl läheb tühistamisele (tänu sellele, et nad eelvalimistel või valimispäeval kohal käisid), koostatakse nimekiri ning saadetakse maakondade valimiskomisjonide kaudu Vabariigi Valimiskomisjonile, kes vastavad e-hääled tühistab. **Kella 19.00-ks peavad kõik vastavad nimekirjad VVK-sse laekunud olema!**
- 20.00 avatakse „e-hääle kast“ ning loetakse e-hääled kokku. Saadud e-hääle summa sisestatakse valimiste infosüsteemi (automaatselt, vajalik on vastav liides)

Kirjeldatud skeemis on mitmeid turvakriitilisi infoliigutamisi (jaoskondade avaldused e-hääle tühistamiseks jne.). Sellise andmevahetuse automatiseerimisel tuleb arvestada elementaarsete turvanõuetega tagamaks info terviklust ja autentsust (turvaline e-post, digitaallkiri jne.). Silmas peab pidama, et infovahetus ja toimingute registreerimine oleks vähemalt sama turvaline või turvalisem kui tavavalimiste puhul.

## 4. E-hääletamise süsteemi üldkontseptsioon

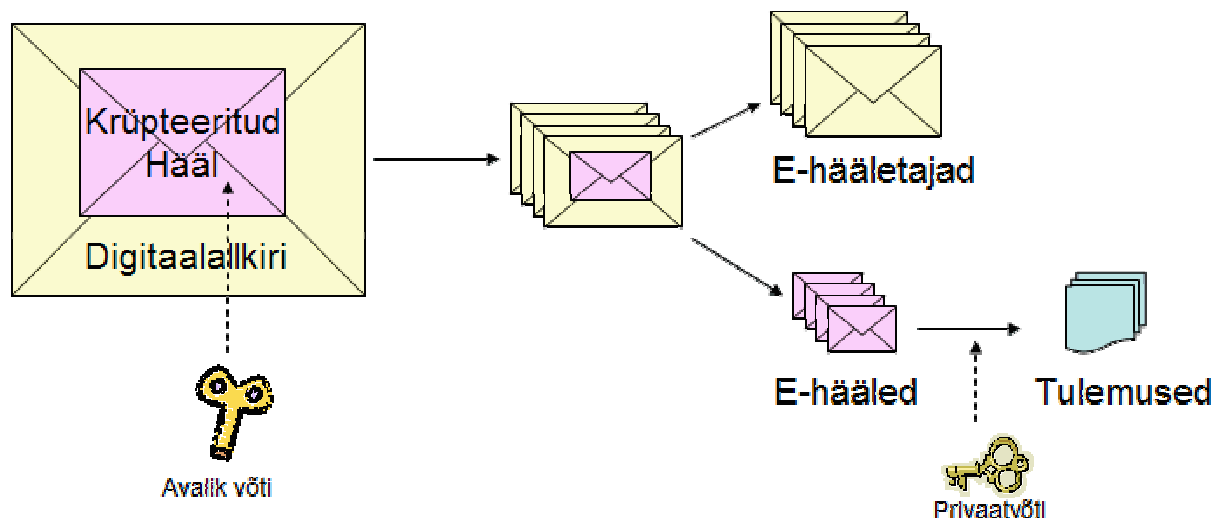
Väljapakutav kontseptsioon rajaneb nõuete ja eelduste jaotises toodud põhimõtetele – lihtsus, krüptoalgoritmide järgiproovitus ning kesksüsteemi usaldatavus.

Kontseptsioon rajaneb nn. „ümbrikuskeemile“, mis sarnaneb ümbrikusse hääletamisele tavavalimiste puhul. Selles skeemis moodustab e-hääletaja sisemise ümbriku, (mis kujutab endast krüpteeritud häält) ja välimise ümbriku (mis kujutab endast e-hääletaja digitaalallkirja).

Ümbrikuskeemi kasuks räägivad järgmised asjaolud:

- kontseptsiooni arusaadavus ja lihtsus ning paralleeli võimalus tavavalimistega
- süsteemi arhitektuuri lihtsus – minimiseeritud komponentide ja osapoolte hulk
- maksimaalne kasulõikamine digitaalallkirjast

Ümbrikuskeemi illustreerib alljärgnev joonis:



Joonis 3. Ümbrikuskeem

Skeemis kasutatakse avaliku võtmega krüptograafiat\*. E-hääletaja (rakendus) šifreerib tehtud valiku (kandidaadi numbr) süsteemi avaliku võtmega ning allkirjastab tulemi digitaalselt. Hääled kogutakse kokku, sorteeritakse, kontrollitakse isiku valimisõigust ning eemaldatakse üleliigsed hääled (korduvhääletamised, valimisõigust mitteomavate isikute hääled). Seejärel eraldatakse välised ümbrikud (digitaalallkirjad) sisemistest (krüpteeritud hääled). Välisest ümbrikutest moodustatakse e-hääletanute nimekiri. Sisemised ümbrikud (kus ei ole enam mingit seost hääle andja isikuga) antakse üle häälte kokkulugejale. Viimasel on kasutada süsteemi privaativõti. Häälte kokkulugeja (rakendus) väljastab summaarsed e-hääletamise tulemused.

\* Avaliku võtmega krüptograafia puhul on mängus võtmepaar – avalik võti ja privaativõti. Kui lähtetekst šifreerida privaativõtmega, siis sellest saadavat krüptogrammi saab dešifreerida ainult vastava avaliku võtmega. Ja vastupidi – kui lähtetekst šifreerida avaliku võtmega, siis resulteeruvat krüptogrammi saab dešifreerida ainult vastava privaativõtmega.

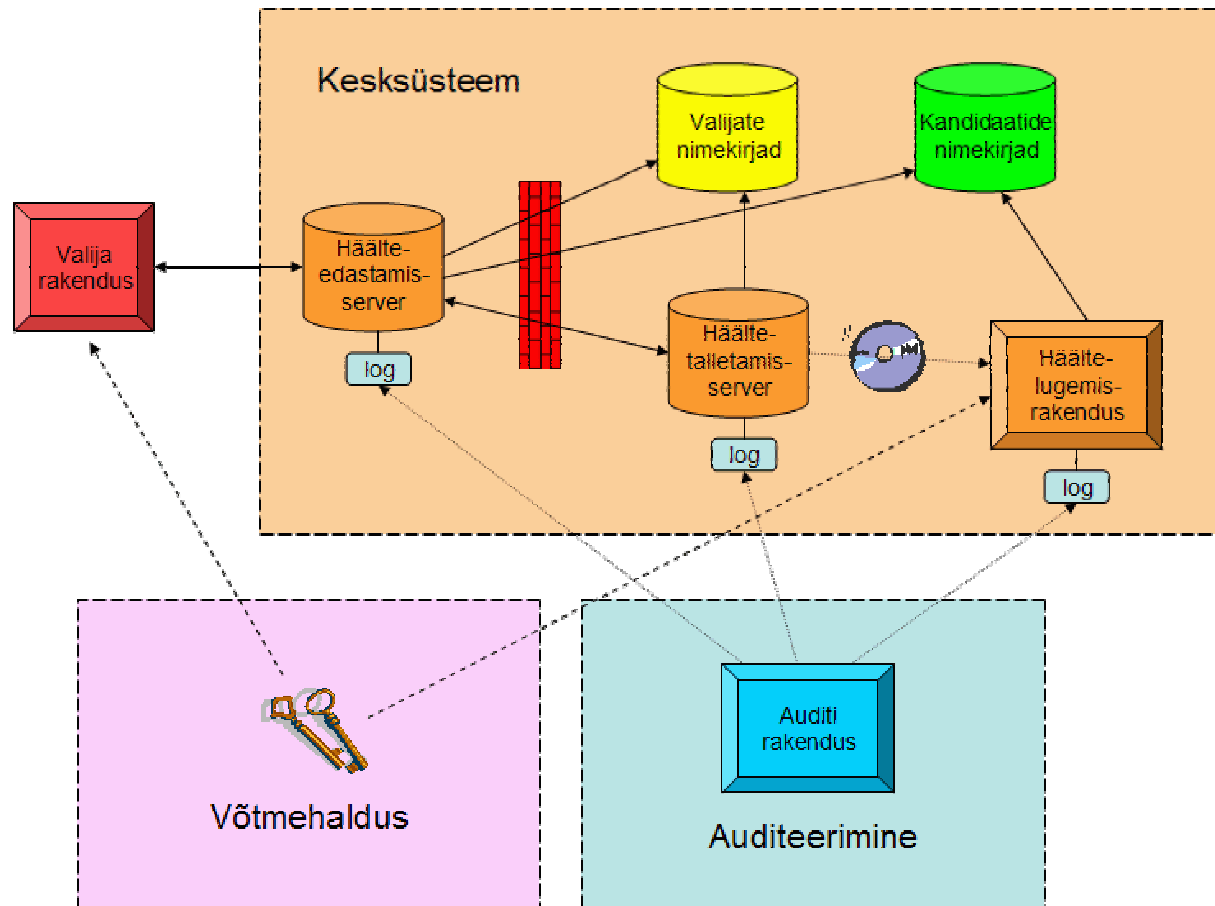
Selles skeemis tagab e-hääletajate privaatsuse järgmise nõude täitmine: **süsteemi ühelgi osapoolel ei tohi ühelgi ajahetkel olla kasutada digitaalallkirjaga varustatud e-hääli ja süsteemi privaatvõti.**

Selline on valitud ümbrikuskeemi üldpõhimõte. Loomulikult on reaalselt kogu skeem keerukam, pakkudes lisaks e-hääle tühistamise turvalist võimalust, hõlmates süsteemi täpsustatud arhitektuurilisi komponente, erinevaid organisatsioonilisi osapooli jne. Sellest tuleb juttu järgnevates jaotistes.

## 5. Süsteemi arhitektuur ja osapooled

Selles jaotises täpsustame süsteemi komponente ning kirjeldame nende funktsionaalsust ja liideseid. Määratleme süsteemis esinevad osapooled ja toome ära ka võimaliku komponentide jaotumise eri osapoolte vahel.

Süsteemi arhitektuuri kirjeldab järgmine joonis:



Joonis 4. Valimissüsteemi arhitektuur

Alustame osapoolte kirjeldamisest – viimased on joonisel esitatud erinevat värvi ruudukujuliste aladena:

- **Valija** – e-hääletaja oma personaalarvutiga. Tegeleb krüpteeritud ja digitaalallkirjastatud hääle moodustamisega ja saatmisega Kesküsteemi;
- **Kesküsteem** – Vabariigi Valimiskomisjoni vastutuse all olev süsteemiosa. Tegeleb hääle vastuvõtmisega ja töötlemisega kuni e-hääletamise koondtulemuse väljastamiseni;
- **Võtmehaldus** – Osapool, kes tegeleb süsteemi võtmepaari(de) genereerimisega ja haldamisega. Avalik võti (avalik võtmed) integreeritakse Valija rakendusesse, privaativõti (privaativõtmed) antakse õigel ajal kasutamiseks Häätelugemisrakendusele;

- **Auditeerimine** – Lahendab e-hääletamisega seotud kaebusi, kasutades Kesküsteemist pärit logi-informatsiooni.

Kesküsteem on sõltuvuses veel kahest osapooldest –

- valijate nimekirjade genereerija (hetkel AS Andmevara)
- kandidaatide nimekirjade koostaja (hetkel VVK ise)

Järgnevalt Kesküsteemi komponentidest lähemalt:

- **Häälteedastamisserver (HES)** – autendib hääletaja ID-kaardi abil, tuvastab tema valimisõiguse, kuvab hääletajale tema piirkonna kandidaadid ning võtab vastu krüpteeritud ja digitaalselt allkirjastatud e-hääle. Selle e-hääle edastab ta kohe Häältetalletamisserverisse ja edastab sealt saadud positiivse kättesaamisteate hääletajale. Lõpetab töö peale eelhääletamise lõppu.
- **Häältetalletamisserver (HTS)** – võtab vastu e-hääli HES-lt ja talletab neid. Peale eelhääletamise lõppu eemaldab korduvad hääled, tühistab valimisõigust mitte omavate isikute hääled ning võtab vastu ja täidab e-hääle tühistusi. Lõpuks eraldab sisemised ümbrikud välimistest ning paneb need valmis Häältelugemisrakenduse jaoks
- **Häältelugemisrakendus (HLR)** – vallasrežiimis komponent, kuhu kantakse üle krüpteeritud hääled, millelt on eemaldatud digitaalallkiri. HLR kasutab süsteemi privaativõtit, summeerib hääled ning väljastab e-hääletamise tulemused.



## 6. E-hääletamise protseduurid

Käesolevas jaotises kirjeldame täpsemalt süsteemi üldarhitektuuris toodud komponentide käitumist erinevate e-hääletamise etappide puhul.

### 6.1. Võtmehaldus

Võtmehalduse protseduurid ja kasutatav turvaskeem on e-hääletamise süsteemi üks kriitilisemaid kohti, millest sõltub süsteemi põhiomaduste (valimiste privaatsus ja salajasus) täitmine. Siinkohal ei anna me sellel teemal lõplikku meetmete ja protseduuride kirjeldust, vaid toome ära teema põhiolemuse, põhiohud ja võimalikud meetmete variandid.

Valimiste salajasuse tagamise põhimootoriks süsteemis on asümmeetrilise krüptograafia. Genereeritakse **süsteemi võtmepaar**, mille avalik komponent integreeritakse kliendi tarkvara sisse ning mida kasutatakse hääle šifreerimiseks. Võtmepaari privaatkomponenti kasutatakse Häältelugemisrakenduses hääle dešifreerimiseks. On ülimalt oluline, et privaatvõtme kasutamine oleks võimalik ainult hääle kokkulugemiseks HLR-s (valimispäeval kell 20.00 ja, kui osutub vajalikuks, siis kordu lugemisel). Pärast kaebuste lahendamise perioodi lõppu privaatvõti hävitatakse.

E-hääletaja privaatsuse ja salajasuse võivad ohtu panna kahe turvariski samaaegne realiseerumine: süsteemi (või süsteemist välja) tekib osapool, kellel on ühtaegu kasutada nii süsteemi privaatvõti kui ka digitaalallkirjaga varustatud hääled. Kuigi mõlemad infohulgad on süsteemis eraldatud, jääb risk ikkagi alles. Ühte ja ainsat privaatvõtit on ilmselt oluliselt lihtsam kaitsta kui digitaalallkirjaga varustatud e-hääli - need liiguvad läbi mitmete süsteemi komponentide (Valija, HES, HTS) ja andmesidekanalite, mistõttu nende lekkimise oht on suurem. Seetõttu tuleks turvalisuse tagamise põhirõhk panna võtmehaldusele.

Privaatvõtit ähvardab kaks ohtu:

- **Kompromiteerumine ehk avalikuks tulek.** Selle ohu realiseerumine võimaldab digitaalallkirjastatud e-hääli omavatel osapooltel teha kindlaks, kes kelle poolt hääletas, seades ohtu hääletaja privaatsuse.
- **Riknemine.** Privaatvõtme kandja võib hävineda, kaduda või rikneda tehnilise vea tõttu. Selle ohu realiseerumisel osutub võimatuks šifreeritud e-hääli dešifreerida ning kõik elektrooniliselt antud hääled lähevad tühja. Selline oht on kriitiline ning seetõttu tuleks **süsteemis kasutada paralleelselt kahte võtmepaari**. See tähendab, et kõik edaspidi kirjeldatavad algoritmilised tegevused privaat- ja avaliku võtmega tuleb dubleerida mõlema võtmepaari jaoks.

Turvalise võtmehalduse skeemi projekteerimisel tuleb teha veel järgmisi valikuid:

1. **Privaatvõtme kandja.** Kindlasti tuleb võtmepaaride salajasi komponente säilitada riistvaraliselt kas kiipkaardis või HSM-s (*Hardware Security Module*) kopeerimist välistaval viisil ning nende käivitamine peab olema võimalik ainult vastava PIN-koodi sisestamise abil.

Valik kiipkaardi või HSM vahel tuleb teha, lähtudes mitte ainult turvalisusest, vaid ka töökiirusest – kiipkaart teeb keskmiselt kaks operatsiooni sekundis. Kui meil on

miljon häält, siis kulub 500000 sekundit, mis on peaaegu 6 päeva. 30000 hääle korral kulub 4 tundi. Selles mõttes võib HSM möödapääsmatuseks osutuda.

2. **Topeltkrüpteerimise võimalus.** Sel juhul kasutaja häält krüpteeritakse mitu korda erinevate võtmega. See võimaldab vastutamise hajutamist kahe erineva isiku (privaatvõtme hoidja) vahel nii, et üks nendest ei saa üksinda midagi teha.
3. **Võtmehaldusorganisatsioon.** Võtmehaldust võib teostada Kesküsteemis või kolmanda osapoole poolt. Kuigi tehniliselt nendel võimalustel vahet pole, võib organisatsioonilisest ja ka psühholoogilisest vaatevinklist olla kolmas osapool parem valik – kolmas osapool poleks mingil moel ülejäänud valimiste protseduuridega seotud ning süsteemi privaativõti (-võtmed) oleks (kiusatuse vältimiseks) „kaugemal“ HES ja HTS operaatoritest.

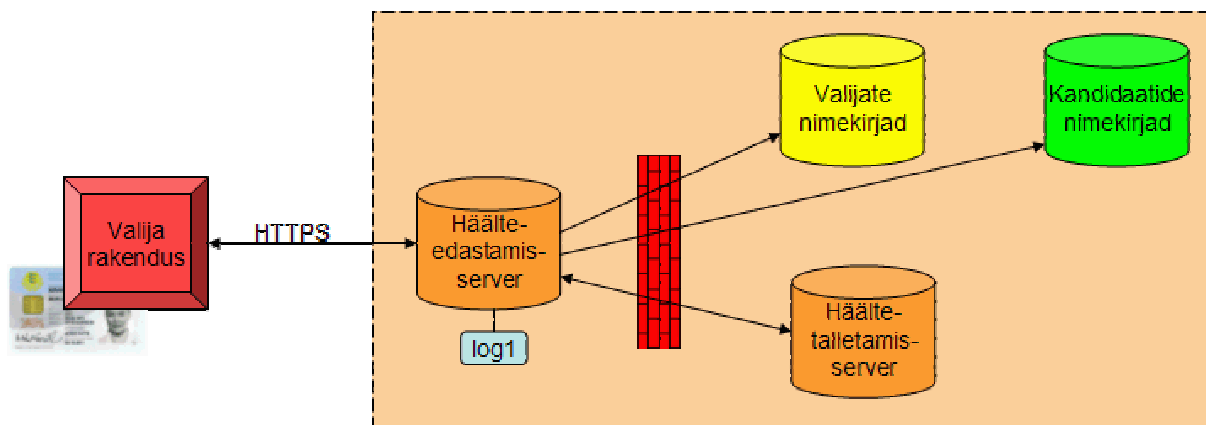
Vastavalt valitud võtmehaldusskeemile (liiasus privaativõtme riknemise kaitseks, topeltkrüpteerimine vastutuse hajutamiseks), tuleb edasistes kirjeldustes „võtmepaari“ ja „avaliku- ja privaativõtme“ mõistete puhul mõista ühte, kahte või koguni nelja võtmepaari.

Võtmehalduse protseduurid (võtmepaari ja PIN-ide genereerimine, avaliku komponendi transport kliendirakenduse loojani, privaatse komponendi säilitamine ning kasutada andmine HLR-le) tuleb kirjeldada **eraldi dokumendis** ning peavad olema audiitorjärelvalve objektiks.

## 6.2. Hääletamine ja häälte talletamine

Hääletamine toimub hääletamispäeva esmaspäevast kolmapäevani, eelhääletamise ajal. Koos eelhääletamise lõppemisega lõpetab välismaailmaga suhtlemise ka Kesküsteem.

Hääletaja toimub Valija ja HES vahelise transaktsioonina. HES kasutab oma tööks päringuid Valijate nimekirjade ja Kandidaatide nimekirjade andmebaasi ning saadab lõpuks hääle HTS-sse. Selle etapi arhitektuuri peegeldab järgmine joonis:



Joonis 5. Hääletamise protsessis osalevad komponendid

Valija rakendus töötab veebikeskkonnas. HTML-lehtede kõrval laetakse Valija brauserisse signeeritud ActiveX või Java rakendus, mis võimaldab häält šifreerida ning moodustunud krüptogrammide digitaalallkirja anda.

HES-s töötab veebiserver koos oma rakendusega. HES on ainukene Kesküsteemi komponent, mis on otseselt kätte saadav Internetist – kõik ülejäänud Kesküsteemi komponendid on (sisemise) tule müüri taga ning neisse on võimaldatud juurdepääs ainult HES-st. HES võib olla (korduvalt) dubleeritud.

Valijate nimekirjade andmebaas on e-hääletamise perioodil dünaamiline tagamaks e-hääletamise võimaluse andmist ka isikutele, kes registreerivad oma elukoha „viimasel minutil“. E-hääletamise perioodi lõppedes nimekirjade andmebaas fikseeritakse. Reaalselt tähendab see, et e-hääletamise perioodi vältel omab Valijate nimekirja pidaja (AS Andmevara) operatiivset juurdepääsu sellele baasile, e-hääletamise perioodi lõppedes kantakse aga fikseeritud seis üle Kesküsteemi edasiseks töötamiseks.

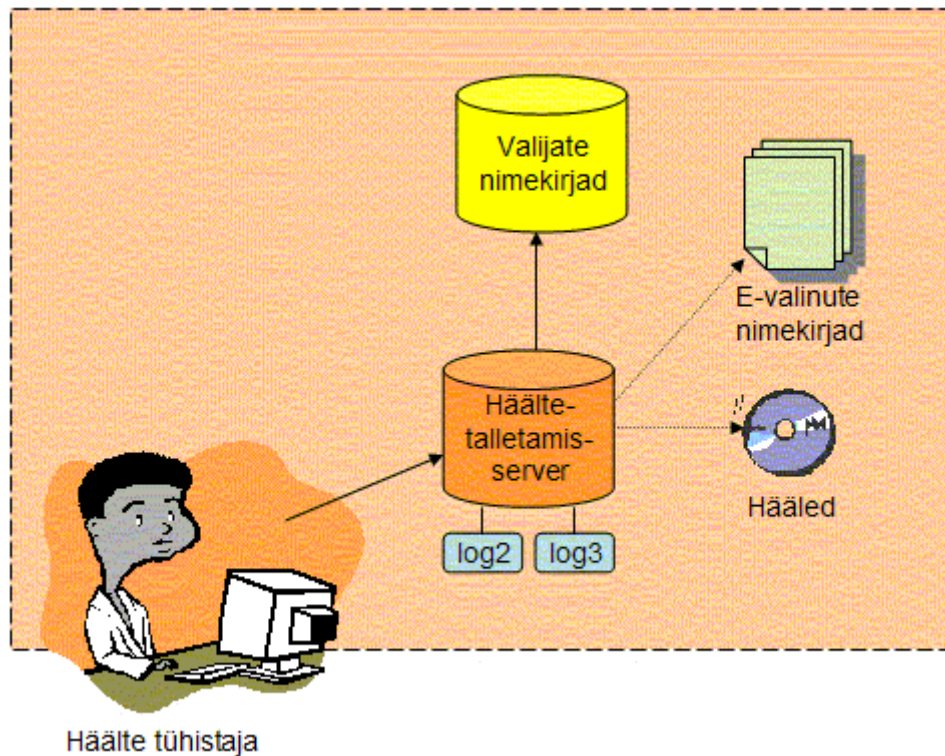
Hääletamise protseduur toimub järgmiselt:

1. Valija pöördub HTTPS-protokolli abil HES poole ning autendib ennast ID-kaardiga.
2. HES teeb päringu Valija isikukoodi (IK) abil Valijate nimekirjade andmebaasi ning tuvastab Valija valimisõiguse ning tema valimisringkonna. Kui Valijal puudub valimisõigus, siis väljastatakse sellekohane teade ning töö lõpeb.
3. HES teeb ringkonna järgi päringu Kandidaatide nimekirjade andmebaasi ning saab vastuseks selles ringkonnas kandideerivad isikud. Nimekiri kuvatakse Valijale.
4. Valija selekteerib meelepärase kandidaadi ning sisestab selle kandidaadi numbrit brauserisse laetud rakenduse sisendvälja (kui on võimalik, siis tekib see number lahtrisse hiireklõpsuga automaatselt (JavaScript vms. vahendeid kasutades) – samas ei tohi serveri veebirakendus mingil juhul teada saada isiku tehtud valikut).
5. Rakendus šifreerib valiku ja juhuarvu HLR avaliku võtmega (avalike võtmetega, kui kasutuses on mitu võtmepaari). Valija allkirjastab selle krüptogrammi (edaspidi: *hääl*) oma digitaalallkirjaga.
6. Valija rakendus saadab oma allkirjastatud ümbriku häälteedastamisserverile. HES-e võib olla palju, nad ei pea olema usaldatavad. Nende ainus funktsioon on korjata kokku välimised ümbrikud ning pidada meeles ümbriku kättesaamise aeg.
7. HES saadab saadud hääle edasi Häältetalletamisserverile (HTS) ning saab sealt kinnituse hääle salvestamise kohta. Vastav teade edastatakse ka Valijale. Logifaili (LOG1) kantakse kirje hääle vastuvõtmise kohta kujul [*IK, hash(hääl)*].
8. Valija võib hääletada palju kordi. Kõik hääled edastatakse läbi HES-i HTS-le.
9. Pärast e-hääletamise lõppu lõpetab HES suhtlemise.

Paneme tähele, et ID-kaardiga autentimine sessiooni alguses ei taga veel seda, et Valija rakenduse poolt moodustatud *hääl* oleks digitaalselt allkirjastatud sama ID-kaardi alusel. Teisiti öeldes – valimisõigust mitte omav ründaja võib sessiooni alustada valimisõigusliku isiku ID-kaardiga ning hääle allkirjastada oma ID-kaardiga. Seega tuleb digitaalallkirjastatud hääli valimisõiguse seisukohalt täiendavalt kontrollida.

### **6.3. Häälte sorteerimine ja tühistamine**

Häälte sorteerimise ja tühistamise etapis osaleb keske komponendina Häältetalletusserveri (HTS) rakendus. Viimasel peab olema juurdepääs Valijate nimekirjadele. Antud protsessi tulemiteks on *hääled* (krüpteeritud kandidaatide numbrid, millelt on eemaldatud digitaalallkiri) ning nimekiri e-hääletanud isikutest. Protsessi illustreerib alljärgnev joonis:



Joonis 6. Sorteerimine ja tühistamine

Eelvalimiste lõpu järel tühistatakse koheselt korduvad hääled. Arvesse läheb iga Valija puhul ainult viimasena antud e-hää. Aega kontrollitakse digitaalallkirja kehtivuskinnituse aja järgi.

Seejärel tühistatakse valimisõigust mitte omavate isikute antud hääled, kontrollides digitaalallkirjast saadud isikukoodi kaudu selle olemasolu Valijate nimekirjades.

Kõik tühistatud hääled logitakse logisse LOG2 kujul:

*IK, hash(hää), põhjus*

Kus põhjus võib olla:

- korduv hää, viide arvesse läinud häälele
- valimisõiguse mitteomamine
- eelhääletamisel osalemine, viide tühistusavaldusele
- ümbervalimine valimispäeval, viide tühistusavaldusele

Nende tegevuste järel koostatakse valimisjaoskondade kaupa nimekirjad e-hääletanud isikutest ning saadetakse need koos eelhääletanute ümbrikutega sama protseduuri kaudu valimisjaoskondadesse laiali. Selle informatsiooni terviklus, autentsus ja kättesaamise tõesus on kriitiline – vastasel korral on isikul võimalik anda kaks häält (e-häält ja tavahäält). Kuna hetkel ei saa arvestada arvutite olemasoluga valimisjaoskondades, siis peame siinkohal silmas paberdokumendi vastavat käsitlust.

Järgmine etapp, mis kestab valimispäeva kuni 20.00-ni ongi e-häälte tühistamise etapp.

Valimisjaoskonnad hakkavad koostama avaldusi e-häälte tühistamiseks. Esimeses järjekorras kantakse sinna isikud, kes on andnud e-hääle ja samal ajal ka eelhääletanud. See tegevus peaks olema lõppenud hiljemalt valimispäevaks.

Järgmine tühistuste etapp toimub valimispäeval. E-hääletanud saavad soovi korral ümber valida valimisjaoskondades kuni kella 17.00-ni. Peale seda lõpetavad valimisjaoskonnad e-häälte tühistusavaldusesse kannete lisamise, allkirjastavad selle dokumendina ning saadavad maakondlikku valimiskomisjoni (informatsioon võib sinna liikuda ka muid kanaleid kaudu, tähtis on, et e-häälte tühistamise aluseks tekiks allkirjastatud dokument).

Maakondlikku valimiskomisjoni peavad kõik jaoskondade e-häälte tühistusavaldused olema laekunud kella 18.00-ks (isegi kui ühtegi tühistust pole, peab tekkima sellekohane informatsioon ja dokument!). Peale seda koostab maakondlik valimiskomisjon elektroonilise nimekirja kõikide oma maakonna valimisjaoskondade kohta, allkirjastab selle digitaalselt (komisjonis peaks olema vähemalt kaks digitaalallkirja-võimelist isikut) ning saadab VVK-le hiljemalt kella 19.00-ks.

VVK summeerib saadud koondnimekirjad omakorda, allkirjastab selle digitaalselt (jällegi on vajalik vähemalt kaks isikut-tühistajat) ning söötab HTS rakendusele. Viimane kontrollib digitaalallkirja, talletab tühistusavalduse ning viib tühistused täide (logides need logisse LOG2). VVK volitatud tühistaja(te)l on võimalik esitada HTS-ile digitaalselt allkirjastatud tühistusavaldusi kui ka tühistamise ennistamisavaldusi (viimased on vajalikud juhuks, kui tuvastatakse töö käigus, et mingi tühistamine oli teostatud inimliku eksimuse tõttu) ühe või mitme hääle kohta.

Tühistamiste perioodi lõppedes eraldatakse välimised ümbrikud sisemistest s.t. digitaalallkirjad allkirjastatud sisust (*häälest*). Algoritm ise on järgmine:

1. Ümbrikud sorteeritakse valimisringkondade kaupa. Digitaalallkirjast saab teada hääletanute isikukoodi, tehes selle järgi päringu Valijate nimekirjade baasi, on võimalik tuvastada konkreetne ringkond.
2. Välised ümbrikud avatakse. S.t. digitaalallkirjad eemaldatakse, järgi jäävad häältelugemiskanduse (HLR) avaliku võtmega krüpteeritud krüptogrammid ehk *hääled*.
3. Digitaalallkirjad säilitatakse eraldi ilma sisuta. Nimetagem seda e-hääletajate nimekirjaks (kui on seda vaja säilitada) – tegelikult piisab kui säilitada nimekiri isikukoodidest ja ringkondadest-jaoskondadest.
4. *Hääled* valmistatakse ette üle kandmiseks HLR-i välisel andmekandjal (CD vms.). Ülekandmise protseduuris tuleb kontrollitult säilitada *häälte* kogumi terviklus.

Kõik HLR-le saadetavad kirjed logitakse logifaili LOG3 kujul *IK,hash(hääl)*.

#### **6.4. Häälte kokkulugemine**

Häälte summeerimine toimub võrgust eraldiseisvas Häältelugemiskanduses (HLR). Samas peab HLR-l olema kasutada Kandidaatide nimekirjaga andmebaas. Seda võib realiseerida kas:

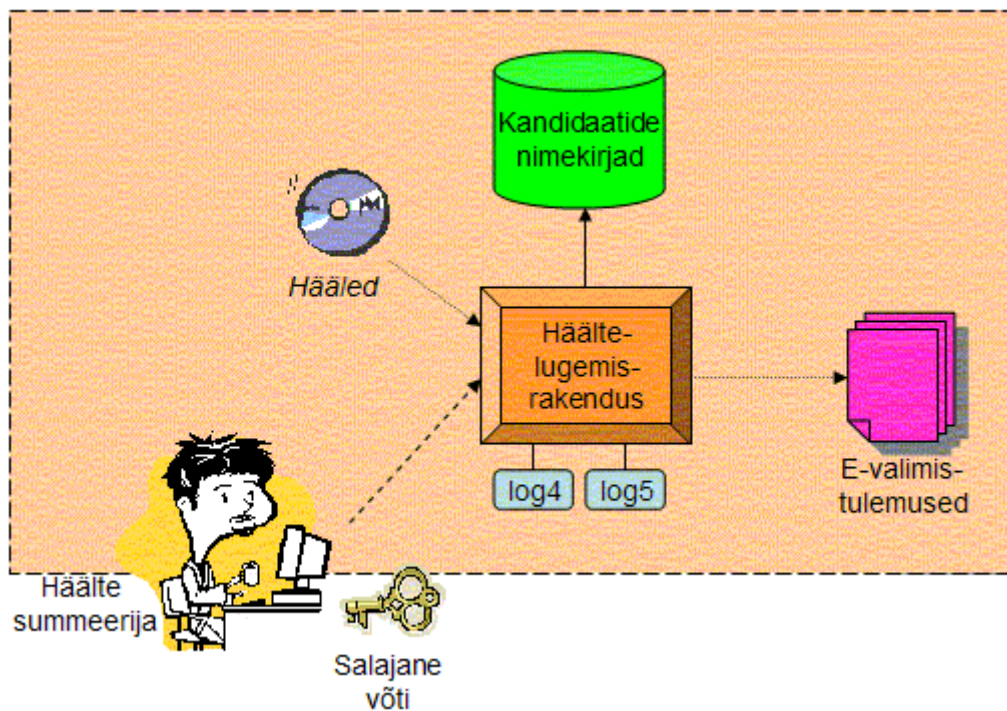
- a) piiratud võrguühenduse loomisega baasiga
- b) baasi kopeerimisega HLR arvutisse (ilmselt kõige otstarbekam kuna sealne info on staatiline)

Nõudeks on, et häälte kokkulugemise toiming peab olema korratav. See annab kindluse HLR arvuti riistvara tõrgete puhuks, võimaldab kontroll-lugemist teises arvutis jne.

Häälte summeerimiseks aktiveeritakse vastavalt sätestatud võtmehaldusprotseduuridele süsteemi privaatvõti (privaatvõtmed mitme võtmepaari puhul) koos PIN-koodidega ning antakse üle HLR operaatori(te)le.

Häälte kokkulugemise sisendiks on HTS-st välisel andmekandjal toodud *hääled*, mis on sorteeritud ringkondade kaupa.

Häälte kokkulugemise keskkonda visualiseerib järgmine joonis:



Joonis 7. Häälte kokkulugemine.

Hääled dešifreeritakse ringkondade kaupa privaatvõtme(te) abil. Esialgne *hää* jäetakse esialgu alles. Peale dešifreerimist kontrollitakse Kandidaatide nimekirja abil, kas antud ringkonnas on valitud kandidaadi poolt võimalik hääletada. Kui kandidaadi number on vale, siis see hää tunnistatakse kehtetuks. Vastav märg kirjutatakse logisse LOG4 kujul *hash(hää)*.

Arvesse minevad hääled summeeritakse kandidaatide ja ringkondade kaupa. Iga arvesse minev hää logitakse logisse LOG5 kujul *hash(hää)*.

E-hääletamise tulemused liidetakse tavavalimiste tulemusega.

## 6.5. Auditirakenduse võimalused

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

LOG1: vastvõetud hääled kujul:	<i>IK, hash(hää)</i>
LOG2: tühistatud hääled kujul:	<i>IK, hash(hää), põhjus</i>
LOG3: lugemisesse läinud hääled kujul:	<i>IK, hash(hää)</i>
LOG4: kehtetud sedelid – vale kandidaadi nr. kujul:	<i>hash(hää)</i>

LOG5: arvestatud hääled kujul:

*hash(hää)*

Krüpteeritud kandidaadi numbrist ja juhuarvust (*hää*) sõnumilühendi (*hash*) moodustamise põhjus on lihtne – sõnumilühendist pole võimalik esialgset *hää*lt tuletada, samas tagab sõnumilühendi algoritmi (SHA-1 vms.) kollisioonikindlus tema unikaalsuse. Kokkuvõttes on auditeeri jaoks *hash(hää)* unikaalne väärtus, mille abil üht häält teisest eraldada, küll aga puuduvad tal igasugused vahendid selle hääle tegeliku väärtuse rekonstrueerimiseks (isegi mitte süsteemi privaatvõtme abil).

Auditirakendus võimaldab tuvastada, mis sai konkreetse IK-ga antud häälest. Variandid on:

- Võeti vastu – sisaldub LOG1-s
- Tühistati selle tõttu, et isik ei oma valimisõigust – vastav kirje LOG2-s
- Tühistati selle tõttu, et isiku käis eelvalimistel – vastav kirje LOG2-s
- Tühistati selle tõttu, et isik käis valimispäeval valimas – vastav kirje LOG2-s
- Tühistati selle tõttu, et „valimisedelisse“ oli kirjutatud kandidaadi number, kes ei kandideerinud vastavas ringkonnas – vastav kirje LOG3-s ning sellele omakorda vastav *hash(hää)* LOG4-s
- Hää läks arvesse: vastav kirje LOG3-s ning sellele omakorda vastav *hash(hää)* LOG5-s

Põhiliseks auditirakenduse kasutamise põhjuseks on vaidluste lahendamine. Põhimõtteliselt on aga võimalik e-hääletajale pakkuda välja ka selline veebirakendus, kus ta saab oma ID-kaardi abil autentimise järel teada oma antud hääle(t)e staatusest.

Peale selle on auditirakendusel võimalik kontrollida logide terviklust – LOG2 ja LOG3 ühisosa peab andma LOG1 sisu, LOG4 ja LOG5 ühisosa peab andma LOG3 sisu.

Kõik logikirjed peavad kandma ajainformatsiooni ja võiksid olla omavahel krüptograafiliselt lingitud, et tagada logide terviklus ja võltsimiskindlus.



## 7. Tarkvara arendusest, keskkondadest ja integratsioonist

Üldise printsiibina – kõik „valged kastid“ valmistatakse kodumaise väljatöötlusena. „Mustade kastidena“ kasutatav välismaise päritoluga programmvara (operatsioonisüsteemid, komponendid, teegid, jne.) kasutus tuleb projekteerida nii, et nende komponentide võimaliku kompromiteerituse mõju e-hääletamise süsteemi turvaloogikale oleks minimeeritud.

Süsteemi arhitektuurilises vaates toodud komponendid on eraldi käsitletavat, s.t. põhimõtteliselt võib arendada igat tarkvara moodulit (arhitektuurilisel vaatel kujutatud komponentidena) erinev osapool. Tehnilises projektis tuleb ära kirjeldada täpsed andmevahetusprotokollid ja andmestruktuurid.

Komponentidevaheliste andmestruktuuride spetsifitseerimisel tuleks eelistada XML-keelseid konstruktsioone, võimalusel kasutades EML vorminguid. Digitaallkirja vorminguks peaks olema DigiDoc vorming, mis annab võimaluse kasutada olemasolevat programmvara ning tagab digitaallkirjastatud informatsiooni ühilduvuse olemasolevate, DigiDoc-vormingul põhinevate, digitaallkirja süsteemidega.

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

Valmiste rakendus ja vastav veebikeskkond võib olla ainult eestikeelne. Äärmiselt soovitatav oleks keskkonda toetava abiinfo kättesaadavus ka teistes keeltes.

Süsteemsete komponentide (operatsioonisüsteem, veebiserver, tugiteegid) ehk „mustade kastide“ valikul, paigaldamisel ja konfigureerimisel tuleb silmas pidada, et:

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

Keskkondade valikul ja arenduses tuleb lähtuda järgmistest printsiipidest:

- Tuleb eeldada, et Valija keskkond on kodu- või kontoriarvuti, mille operatsioonisüsteemi ja seadistust Valija muutma ei hakka. Seega võib 95% tõenäosusega arvestada Windows-keskkonnaga. **Näitena** võib sätestada piirangu, mis eeldab vähemalt Windows 98 või uuema (Windows 95 pole enam Microsofti poolt toetatud) ja Internet Explorer 5.0 või uuema olemasolu. Kõikvõimalike kasutajaplatvormide toetamine on tehniliselt ülikeerukas ja seega kulukas.
- Keskstüsteemi HES ja HTS komponendid platvormideks võiks olla FreeBSD või Linux, kust on eemaldatud kõik ebavajalik. Rakendused tuleks kirjutada soovitatavalt C keeles, igasuguse *middleware* kasutamist (teegid, utiliidid) tuleks minimeerida. Komponentide sisemiseks tööks ja omavaheliseks andmevahetuseks kasutatavad andmehoidlad peaksid olema „inimloetava“ vorminguga (tekst, CSV, XML).



- Kesküsteemi Häältelugemisrakenduse keskkonna valikul tuleb lähtuda eelkõige alussüsteemi tervikluse ja turvalisuse printsiibist – peab olema välistatud igasuguste protsessi häirivate või halvavate kõrvalprogrammide mõju.
- Audiitorrakendus võib olla suhteliselt spartalik, UNIX-i käsoreal toimiv utiliidikomplekt.

## 8. Süsteemi vastavus nõuetele, võimalikud ohud.

Järgnevalt vaatleme süsteemi vastavust esitatud põhinõuetele – salajasus, sundimatus, kontrollitavus ja üks-isik-üks-hääl ning toome esile võimalikud ohud.

See alajaotis ei ole süstemaatiline ja täielik ohtude analüüs – selle tarbeks väärib koostamist eraldi dokument. Pigem tuleb allolevalt toodud ohujuhte vaadelda indikatiivsetena süstemaatilise turvaanalüüsi teostamisel.

**Salajasus ja valija tahte terviklus.** Valija valik šifreeritakse süsteemi avaliku võtmega Valija rakenduses ning dešifreeritakse HLR-s alles häälte kokkulugemise ajal. Võimalikud ohud on:

- **HES saab teada valija eelistuse** – HES veebisüsteem identifitseerib Valija ID-kaardi abil ning seega teab tema isikukoodi, kuvab talle kandidaadid jne. Samas ei tohi Valija rakendus midagi teada teda kasutava isiku identiteedist. Valija veebisüsteemi ja rakenduse kombineerimisel tuleb hoolega silmas pidada, et seda nõuet ei rikutaks (näiteks „kargab“ kandidaadi pildi peale vajutades Valija rakenduse lahtrisse õige number, samas saab aga HES veebisüsteem sellest teada).
- **Valija rakenduse korrumpeerumine** – kuna Valija rakendus töötab ebaturvalises keskkonnas (viiruse- ja trooja-altis Windowsi keskkonnas), siis on see nõrk lüli. Parim, mis on võimalik tehniliselt teha, on Valija rakenduse tervikluse ja autentsuse tagamine digitaalsignatuuri abil. Valija arvutit on võimalik kompromiteerida, arendades välja spetsiaalse viiruse, mille detailse kirjeldamisega me selles dokumendis pikemalt ei tegele. Lühidalt asendaks selline viirus märkamatuvalt Valija rakenduse, selle tervikluskontrolli mehhanismid ning suunaks Valija veebiühenduse ümber oma serverile. Siin aitaksid täiendavad turvakontrollid (võtmete sõnumilühendite jms. parameetrite) Valija poolt, seda ei saa aga me eeldada. Sellise ründe tulemusena saadaks võlts Valija rakendus tee kandidaadi numbri, mis ei vasta valija tahte.

Reaalselt on sellise ründeprogrammi koostamine ja levitamine küllaltki komplitseeritud. Sellist rünnet saab suure tõenäosusega võimalik avastada (spetsialist suudab tuvastada Valija arvuti kompromiteerituse, kui ründeprogramm pole ennast ja oma olemasolu tundemärke enda järel veel hävitanud) kuid mitte lõpuni ära hoida. Eraldi mõtteaineks on siin – kui väidetavalt selline olukord mingis Valija arvutis juhtus, kes siis peab kellele mida ja kuidas tõestama?

- **Süsteemi privaativõtme korrumpeerumine** – süsteemi privaativõti ja digitaalselt allkirjastatud *hääled* saavad samal ajal teatavaks mingile osapoolele. See paneb löögi alla valija hääle privaatsuse. Selline risk on madal juhul, kui võtmehalduse protseduurid on korrektselt järgitud ja auditeeritud. Vt. ka arutlust alajaotises „Võtmehaldus“.
- **Väikene arv e-hääletajaid ühes valimisringkonnas** – Häätelugemisrakendusse kantakse anonüümseks tehtud hääled valimisringkondade kaupa. Kui näiteks mingis valimisringkonnas e-hääletas ainult üks Valija, siis on võimalik HTS sisemisest andmebaasist või valimisjaoskonda saadetud e-hääletanute nimekirjast kindlaks teha selle valija isik.

Sellele probleemile pole head lahendust. Ilmselt on ainukeseks leevendavaks vahendiks siin see, et e-hääletamise tulemust ei avaldataks eraldi vaid tavahäältega konsolideerituna. E-hääletamise tulemit võib avaldada ainult statistiliste näitajate kaudu.

**Sunnitamatus** – valijad ei tohi saada hiljem tõestada, kelle poolt nad on valinud. Kirjeldatud süsteemis puudub valijal **väliste liideste** abil igasugune võimalus näidata, kelle poolt nad on hääletanud.

Siin on võimalik üks huvitav rünne: Valija moodustab oma digitaalselt allkirjastatud e-hääle oma rakendusega, mis on modifitseeritud nii, et juhuarvu asemel pannakse krüptogrammi sisse kindel arv. Selline e-hääle ei erine millegi poolest „ametliku“ Valija rakendusega moodustatud e-häälest. Kui Valija tahab tõestada Kontrollijale, et just see hääle läks arvesse, on vajalik, et Kontrollija pääseks ligi LOG5-s sisalduvale logikirjele *hash(hääle)* ning kõrvutades seda Valija poolt teele saadetud e-häälega (rakendades vastavaid operatsioone), saab ta veenduda, et just see Valija hääle läks arvesse.

**Kontrollitavus** – igal soovijal peab olema võimalik kontrollida, et tema hääle on hääle kokkulugemisel arvesse võetud. Auditirakendus annab selleks täieliku võimaluse. Eraldi otsustuseks jääb, kas seda kontrolli pakkuda kõigile automaatse veebisüsteemi kaudu, või käib see läbi teistsuguse menetlusprotsessi. Veebisüsteemi puhul tuleb silmas pidada, et e-hääletanule väljastatakse tulemuseks ainult e-hääle arvesseminemise või –mitteminemise fakt, mitte mingil juhul ei tohi väljastada kuupäevi/kellaegu ega *hääle* tunnuseid (vt ka eelmine punkt).

**Üks-isik-üks-hääle** – nõude täitmine on mh. kirjeldatud alajaotises „Hääle sorteerimine ja tühistamine“.

## 9. Kokkuvõte

**E-hääletamine on võimalik läbi viia piisava turvataseme juures.** Kirjeldatud tehniline ja organisatsiooniline kontseptsioon tagab vähemalt sama turvataseme (ja paljudes nüanssides isegi suurema), kui seda on tavavalimiste puhul. Kuigi skeemis on komponente, mille turvalisuse hindamine on ebatäpne (Valija personaalarvuti), on nendest komponentidest lähtuvad ohud piisavalt väikese tõenäosusega. Väljapakutud skeemile turvataseme andmise täpsem hinnang jääb siiski detailse turvaanalüüsi tulemusi ootama.

Käesoleva kontseptsiooni koostamisel on lähtutud ID-kaardi ja digitaalallkirja kasutamise nõuetest. Kahtlemata tagavad sellised nõuded parima turvalisuse Valija identiteedi tuvastamise ja tahteavalduse tervikluse koha pealt. Samas võib e-hääletamise komistuskiviks saada vähene valmisolek ID-kaardi elektroonilise kasutamiseks (kiipkaardilugejate vähene levik). 2005.a. KOV valimisteni on aga hetkel päris palju aega – raske on öelda, milline on valmisolek ID-kaardi kasutamiseks siis.

Põhimõtteliselt on olemas piisava turvalisusega skeeme, mis võimaldavad e-hääletamist läbi viia ka ilma ID-kaardi ja digitaalallkirjata. Selleks tuleks aga kahjuks muuta kõiki olemasolevaid valimisseadusi, mis hetkel näevad kohustusliku komponendina ette digitaalallkirja kasutamist. Samuti suureneks sellises süsteemis osalevate osapoolte arv ja mitmekordistuks süsteemi keerukus ja sellest tulenevad ohud. Plussiks oleks aga hinnanguliselt suurusjärg suurem potentsiaalsete e-hääletajate hulk.

Mainitud dilemma lahendamine jääb käesoleva dokumendi ulatusalast välja. Kui asjaomased töörühmad ja komisjonid otsustavad valida ID-kaardile alternatiivse tee, siis jääb käesolev kirjatükk siiski kehtima oma põhipunktides (ulatusala, nõuded, protseduurid).

Edasises töös tuleb:

- viia läbi skeemi detailiseeritud turvaanalüüs.
- kokku leppida organisatsioonilised struktuurid ja vastutusalad,
- täpsustada tehnilise projekti näol e-hääletamise süsteemi tehnilist poolt - platvormi, andmevahetusprotokolle ja –struktuure,
- detailselt fikseerida Võtmehalduse meetmed ja protseduurid,

## 10. Viited

[EML] *OASIS Election and Voter Services TC* poolt välja töötatud „Election Markup Language“ vt [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=election](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election)

[IP1] Euroopa Nõukogu Ministrite Komitee poolt moodustatud töörühm IP1-S-EE  
<http://www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/>