Vabariigi Valimiskomisjon

E-hääletamise kontseptsiooni turve: analüüs ja meetmed

Töö täitjad:
Arne Ansper
Ahto Buldas
Aivo Jürgenson
Mart Oruaas
Jaan Priisalu
Kaido Raiend
Anto Veldre
Jan Willemson
Kaur Virunurm

Dokument: EH-02-02
Kuupäev: 27.12.2010.a.

- Tallinn 2010 -

Sisukord

1.SISSEJUHATUS **3**

2.E-HÄÄLETAMISE PROTSESSI NÕUDED JA EELDUSED **4**

2.1.Nõuete vastandlikkuse probleem 4
2.2.Esitatavad nõuded 4
2.3.Tehnilised eeldused 6
2.4.Süsteemi arhitektuursed komponendid 6

3.TUVASTATUD RISKID **8**

3.1.Fundamentaalsed probleemid 8
3.2.Tehnilise riskianalüüsi kokkuvõte 12

4.NÕUTAVAD JA SOOVITATAVAD TURVAMEETMED **14**

4.1.Üldised nõuded kesksüsteemile 14
4.2.Nõuded süsteemi komponentidele 17
4.3.Nõuded valimiste korraldusele 22
4.4.Võtmehaldus 24
4.5.Meetmete kokkuvõte 28
4.6.Aktsepteerimist vajavad riskid 30

5.ÜLDHINNANG KONTSEPTSIOONILE **32**

6.KOKKUVÕTE **34**

7.LISA 1 - SÜSTEEMIS TÖÖDELDAVAD ANDMED **35**

8.LISA 2 - ANDMEKANALID SÜSTEEMI JA SÜSTEEMIST VÄLJA **36**

9.LISA 3 - TEHNILINE RISKIANALÜÜS **37**

9.1.Riskide klassifikatsioon 37
9.2.Tervikluse riskid 37
9.3.Privaatsuse riskid 42
9.4.Töökindluse riskid 44
9.5.Võtmehalduse riskid 45
9.6.Usaldusväärsuse riskid 47

10.LISA 4 - RISKIDE KOONDTABEL **48**

11.LISA 5 - EBAVAJALIKUKS TUNNISTATUD TURVAMEETMED **51**

12.LISA 6 - VIITED **53**

1. SISSEJUHATUS

Käesolev analüüs on tellitud Vabariigi Valimiskomisjoni poolt eesmärgiga käsitleda turvariske Vabariigi Valimiskomisjoni poolt välja kasutatavas e-hääletamise tehnilises kontseptsioonis. Ülesandeks on hinnata lahenduse turvalisuse üldist sobivust, esitada tehniliste ja organisatoorsete riskide võimalikult põhjalik kaardistus ning vajadusel täiendada süsteemi esitatud turvanõudeid.

Dokumendi esimene versioon valmis 2003. aastal ning siis analüüsiti tollal alles planeeritava e-hääletuse lahenduse riske. Seitsme aasta jooksul on e-hääletamine muutunud igapäevaseks reaalseks ning selle aja jooksul on esialgsele kontseptsioonile vastavat tehnilist lahendust kasutatud kokku viie e-hääletamise läbiviimiseks. Senine praktika näitab, et valimiste turvaline läbiviimine on võimalik ning esialgne kontseptsioon on ajaproovile vastu pidanud. 2010. aastal värskendati dokument, tuginedes vahepeal läbiviidud e-hääletuste käigus saadud kogemustele ning uuenenud teadmistele IT ja interneti turvariskide kohta.

Kuna analüüsitav hääletusskeem on iseenesest võrdlemisi lihtne, on suuremate riskide leidmine tegelikult intuitiivne. Ka kontseptsioon ise sisaldab nii turvaanalüüsi kui meetmeid enamiku suuremate ohtude vastu – digitaalallkiri, hääle krüpteerimine, kesksüsteemi jagamine mitmeks serveriks. Käesolev analüüs on süstemaatilisem, vaatleb riske põhjalikumalt ning esitab rohkem konkreetseid tehnilisi nõudeid.

Meie töö ulatus piirdub tehnilise turbe ja töökorralduse protsessidega. Me ei hinda poliitilisi riske ega anna hinnangut elektroonilise hääletuse sotsiaalsetele või politoloogilistele aspektidele. Küll aga toome me välja turvalisust puudutavad momendid, mis on sisult tehnilised, kuid vajavad kas otsustamist või aktsepteerimist just kõrgemal, poliitilisel tasemel. Sellisteks aspektideks on vastuolu hääletusprotsessi privaatsuse ja kontrollitavuse vahel, hääletuse tsentraliseerumisega seotud riskid, usaldusväärsusega seotud ohud ning tehniliselt pädeva auditi vajadus.

2. E-HÄÄLETAMISE PROTSESSI NÕUDED JA EELDUSED

2.1. Nõuete vastandlikkuse probleem

Salajase hääletamise teeb keerukaks vastuolu kontrollitavuse ja salajasuse nõuete vahel. Ühelt poolt tuleb tagada tulemuste õigsus; selleks peab protsess olema algusest lõpuni auditeeritav, igast tegevusest peab jääma jälg. Teiselt poolt tuleb tagada häälte salajasus, muidu kaob protsessi demokraatlik olemus; seetõttu ei tohi mitte kusagil, mitte iialgi tekkida seost hääletaja ja antud hääle vahel. Need kaks nõuet – kontrollitavus ja salajasus – on sisuliselt vastandid. Lisanõuded – vajadus kontrollida hääletaja õigust valida, korduva hääletamise keeld, hääletusviiside paljusus jne – tekitavad probleeme veelgi juurde.

Perfektset lahendust siin ei ole, tuleb leppida kompromissiga.

Tava-valimistel on kompromissiks mitmekordsesse ümbrikusse hääletamine ning hulk keerukaid kontrollprotseduure selle ümber. Kaasnevaid riske on palju – jaoskonnatöötajate usaldamise vajadus, võimatus proteste lõplikult lahendada jne –, kuid neid aktsepteeritakse lootuses, et protsess kajastab ühiskonna tahet piisava, ehkki mitte absoluutse täpsusega.

E-hääletamise kui infotehnoloogilise ülesande jaoks tähendab see, et süsteemile kehtestatavad *nõuded* tuleb kokku leppida poliitilisel tasemel ja teadlikult. Auditeeritavus ja salajasus, veakindlus ja mitte-tõestatavus, turvalisus ja mugavus ei käi käsikäes; kuhugi tuleb tõmmata joon ja teha otsus. Seda ülesandesse sisseehitatud vastuolu käsitlevad pea kõik e-hääletamiste turva-uuringud, siiani parim lahtiseletus on ilmselt Peter Neumann'i töös [Neumann].

2.2. Esitatavad nõuded

Järgnevas toome süstemaatiliselt ja koos selgitustega välja süsteemi turvalisuse nõuded. Enamik neist on otseselt kirjas ka e-hääletuse kontseptsioonis, teised tulenevad meie Põhiseadusest ja valimisseadustest, kolmandad on lihtsalt "klassikalised", e-hääletamise süsteemidelt nõutavad turvaomadused.

2.2.1. Hääletuse korrektsuse nõuded

Hääletuse korrektsuse ehk tervikluse alla kuuluvad funktsionaalsed nõuded, mille täidetus tagab, et hääletuse tulemus on õige, väljendab valijate tahet ning vastab seadustele. Neid nõudeid on väga palju – sisuliselt on kogu valimisi reguleerivate seaduste tekst selliste nõuete loetelu – ning nende täitmisega tegeleb kogu hääletusskeemi disain. Siinkohal loeme üles vaid turvalisuse jaoks kõige olulisemad nõuded.

Hääletajate autoriseeritus – hääletada tohivad vaid valijate nimekirjas olevad hääletajad ning hääletada tohib vaid oma valimisringkonna kandidaatide poolt. Autoriseerimise nõue tingib omakorda vajaduse hääletaja *autentida*.

"Üks isik – üks hääl" – kõikidest ühe valija poolt mistahes viisidel antud häältest peab arvesse minema ainult üks hääl.

Häälte võltsimise keeld – mitte keegi ei tohi saada muuta valijate antud hääli ega lisada süsteemi võltsitud hääli (näiteks hääletada valimistel mitte osalenud valijate eest).

Hääletuse ühetaolisus – kõikidele hääletajatele peab olema tagatud sarnane võimalus valida.

Elektroonilise ülehääletuse võimalus – valijal peab olema võimalus uuesti hääletada.

Tavahääletamise ülimuslikkus – mistahes muul viisil hääletamine tühistab kõik valija antud e-hääled.

Järgnevad kaks funktsionaalset nõuet, mida e-hääletamise süsteemidele tihti esitatakse, kuid mida Eesti seadused ei tunnista ning mida e-hääletamise tehniline lahendus otseselt ei toeta.

Hääle tühistatavus valija poolt – võimalus enda poolt juba antud e-hääl tühistada.

Tühja hääle andmise võimalus – võimalus hääletada "mitte kellegi poolt" ehk anda tühi hääl.

Tühja hääle andmise funktsioonil on kaks põhjendust – tehniline ja poliitiline.

Tehniline põhjendus on anda valida mitte soovivatele valijatele võimalus oma meelerahuks kindlustada, et keegi teine ei saaks nende nime all hääletada. Poliitiline on anda kodanikele võimalus "demokraatlikuks protestiks" oma kodanikuõiguste demonstratiivse mittekasutamise kaudu.

Tegelikult on mõlemad nõuded tavahääletuse ülimuslikkuse kaudu realiseeritud. Valija saab alati peale e-hääletamist minna valimispäeval füüsiliselt valimispunkti ning seal valimiskasti panna tühja hääletussedeli.

2.2.2. Hääletuse salajasuse nõuded

Hääle salajasus – mitte keegi ei tohi mingilgi hetkel teada saada, kelle poolt valija hääletas.

Hääletamise fakti privaatsus – ei tohi saada tuvastada seda, kas, millal ja millisest arvutist hääletaja hääletas.

Hääletamise fakt ei ole ei e- ega tava-hääletamise puhul kunagi täiesti salajane. Võrgu-ühenduse pakkuja (ISP) näeb oma klientide pöördumisi VVK veebiserveri poole, valimis-jaoskonna välisust jälgiv vaatleja näeb jaoskonda sisenejaid. Samas ei tea ei kumbki seda, kas valija ka tegelikult hääletas. E-hääletamisel on vaja samasugust "nõrka" privaatsust.

Hääletamise tõestamatus – hääletaja ei tohi saada tõestada, kelle poolt, millal või mis viisil ta hääletas.

Tõestamatus on vahend hääletuse *sundimatuse* (sunnitamatus, hääletamisvabadus, *uncoercibility*) kaitseks. Sundimatus nõuab, et hääletaja oleks oma valikus vaba. Kui hääletaja ei saa tõestada, kuidas ta hääletas, siis ei ole võimalik ka häälte kontrollitav müümine / ostmine ega muu (näiteks tööandja-poolne) sund.

Hääletustulemuse salajasus – e-hääletamise tulemused ei tohi mitte kellelegi olla teatavad enne tavahääletuse lõppemist; üldisest hääletustulemusest eraldiseisvat e-häälte jaotust valimiskomisjon ei avalikusta.

2.2.3. Hääletuse töökindluse nõue

Hääletussüsteemi käideldavus – e-hääletamise tehniline süsteem peab olema töökindel, valijatele ning valimiste korraldajatele ettenähtud ajal kättesaadav, töötama piisavalt kiiresti, tagama andmete säilivuse ja hääletustulemuse õigeaegse väljastamise.

2.2.4. Hääletuse usaldusväärsuse nõuded

Ühiskond ja asjaosalised peavad nii enne kui pärast hääletuse toimumist uskuma, et e-hääletamine on (oli) usaldusväärne hääletusviis. Tehniliselt väljendub see järgnevates nõuetes.

Läbipaistvus – hääletuse protsess ja mehhanismid peavad olema avalikud ning arusaadavad.

Auditeeritavus – volitatud isikutel peab olema võimalus veenduda, et hääletusprotsess oli kogu ulatuses korrektselt läbi viidud.

Hääle arvestamise kontrollitavus – igal hääletajal peab olema võimalik soovi korral kontrollida, et tema hääl on häälte kokkulugemisel arvesse võetud.

Üleloetavuse korratavus – e-häälte ülelugemisprotsess peab olema korratav.

2.2.5. Teoreetilised nõuded

Täielikkuse huvides toome ära veel kaks hääletusprotokollidele esitatavat nõuet. Need on *universaalne verifitseeritavus*, mille korral kõikide häälte lõpptulemuses arvesse võtmist peab saama tõestada iga soovija (ka iga täiesti süsteemiväline osapool), ning *hääle absoluutne ("fail-safe") salajasus* ehk nõue, et hääletaja hääl ei saaks avalikuks mitte mingitel tingimustel, ka mitte kõikide teiste osapoolte (sh valimiste korraldajate) kokkumängu korral.

Me arvame, et selliseid nõudeid täitvat reaalset hääletamisskeemi ei ole olemas ning ei saagi kunagi olema.

2.3. Tehnilised eeldused

Tehnilised eeldused, millele esitatud kontseptsioon ja meie analüüs tuginevad, on järgmised.

Kesksüsteemi serverid on turvalised ja usaldatavad. See tähendab, et kesksüsteemi serveri kompromiteerumine võib e-hääletamise turvalisust mõjutada nii suurel määral, et tulemused tuleb tühistada.

Samas on kesksüsteem siiski jagatud mitme serveri vahel. Kas see on ülalnimetatud eelduse korral üldse vajalik? Vastus on kindlasti jah, selline modulaarsus võimaldab süsteemi tehnilist turvalisust oluliselt tõsta.

Kesksüsteem koos *sisevõrguga* on terviklik ja käideldav ning tema füüsiline turve on korras. Me ei analüüsi näiteks sisevõrgus toimuvaid vahendusründeid, side- ega toitekatkestusi.

E-hääletamise infosüsteem on muust valimiste infosüsteemist *võrgutasemel eraldatud*, kogu suhtlus välismaailmaga toimub läbi piiratud liideste.

Hääletajal on tugeva autentimise ning digiallkirja andmise vahend, näiteks ID-kaart, DigiID või Mobiil-ID, millel on kehtivad *autentimissertifikaat* ja *digitaalallkirja sertifikaat.*

Digitaalallkiri on võltsimatu, ID-kaart, Mobiil-ID ning nende kasutamisega seotud baastarkvara on turvalised ja veatud.

Hääletaja keskkond (arvuti, brauser) on turvaline. Samas ei ole see keskkond valimiskomisjoni poolt kontrollitav ning selle turvalisuse eest peab hoolitsema keskkonna omanik ja sellega seotud riske tuleb hallata kodanike teavituse ja infoturbealase teadlikkuse tõstmise kaudu.

Süsteemi *sisendandmed* – kandidaatide ja valijate nimekirjad – on korrektsed.

2.4. Süsteemi arhitektuursed komponendid

Me ei kirjelda selles analüüsis süsteemi ennast, kuna seda teeb analüüsitav kontseptsioon niigi, kuid ühise arusaamise huvides tuleb anda nimed süsteemi komponentidele ja selles

töödeldavatele andmetele. See nimekiri ei ole täielik – enamik mõisteid on niigi kas intuitiivsed või siis kirjeldatud analüüsitavas kontseptsioonis.

Hääletaja rakendus, HR – häält hääletaja arvutis krüpteeriv ja allkirjastav rakendus. Hääletaja rakendus töötab *hääletaja arvutis*.

Häälteedastusserver, *HES* – server, mis annab hääletajale rakenduse ja selle jaoks vajalikud andmed, võtab vastu antud hääle ja edastab selle HTS-ile. Kuna HES on ka seaduses defineeritud "Vabariigi Valimiskomisjoni veebilehe" rolli, siis nimetame teda tihti ka *Veebiserveriks*.

Häältetalletamisserver, *HTS* – server, mis talletab hääletajate antud krüpteeritud e-hääli, võimaldab neid sorteerida, tühistada ning kokkulugemiseks HLR-ile edastada. HRL-ile edastamisel eemaldatakse krüpteeritud e-häältelt valija digitaalallkiri ning e-hääled muutuvad anonüümseks.

Häältelugemisrakendus, *HLR* – eraldiasuv rakendus, mis krüpteerib digiallkirjadeta e-hääled lahti, summeerib need ning väljastab e-hääletamise tulemused. Arvuti, milles HLR töötab, kannab nime *HLR server*.

Kehtivuskinnitusteenus – väline teenus, mis tõendab häälte digitaalallkirjade andmise aega ning hääletaja allkirjasertifikaadi kehtivust.

Internet – võrguühendus HR ja kesksüsteemi vahel.

Sisevõrk – ühendused kesksüsteemi komponentide vahel. Sisevõrgu alla kuulub ka *tulemüür* ja muud võimalikud võrgutasemel pääsukontrolli mehhanismid ning vallasandmekandjatel andmekanal HTS ja HLR vahel.

Auditisüsteem – auditiandmete kogumiseks ja *auditirakenduse* tööks mõeldud Kesksüsteemi osa.

Lisaks on süsteemis *Andmebaas* ning hulgaliselt *rakendusi* – häälte sorteerimise rakendus, auditirakendus, valija tagasiside rakendus jne. Andmebaas asub HTS-is, ehkki tegelikult on ta iseseisev loogiline komponent ja vajadusel võiks paikneda ka eraldi serveris.

Kaudselt on e-hääletamise süsteemi osaks ka *valimiste infosüsteem*, mis annab e-hääletamise jaoks vajalikke andmeid, millest saadakse tühistusi ja ennistusi ning kuhu sisestatakse valimiskomisjoni poolt kinnitatud e-häälte lugemise tulemused.

3. TUVASTATUD RISKID

Detailne, süsteemi arhitektuurist ja riskide kategooriatest lähtuv tehniline riskianalüüs on toodud Lisas 3. Selles peatükis analüüsime vaid e-hääletamisega seotud põhimõttelisi probleeme ning toome ära tehnilise analüüsi koondtulemuse.

3.1. Fundamentaalsed probleemid

3.1.1. Vajadus usaldada hääletaja arvutit

Tänapäeva personaalarvuti on sedavõrd komplitseeritud, et valija seisukohalt on tegemist "musta kastiga", mille tööd ta kontrollida ei oska ega suuda. Arvuti võib hääletaja nimel, kuid tema eest salaja, teha praktiliselt kõike – hääletada teise kandidaadi poolt, signeerida lisaks häälele veel midagi muud, saata valija hääl lahtiselt ajakirjandusele ja nii edasi.

Põhiliselt on hääletaja arvuti rünnatav nelja vektori kaudu:
- võrk / operatsioonisüsteem (näiteks Microsoft Windowsi võrguteekide vead, USB mälu-seadmete kasutamise ohud, jne),
- e-post, kiirsuhtlusprogrammid ning sotsiaalvõrgustikud, kui kõige enam ära-kasutatavamad Interneti-teenused,
- veebibrauserite turvavead (igas brauseris ning tema lisades on piisavalt vigu, et võimaldada ründekoodi sisaldavate veebisaitide külastamise käigus arvutit rünnata),
- füüsiline juurdepääs.

Nende kanalite kaudu saab arvutisse installeerida tarkvara, mis kas:
- jälgib kasutaja tööd – saab teada tema antud hääle ja/või ID-kaardi PIN-koodi; või
- asendab Hääletaja Rakenduse teisega ning annab vale (kasutaja tahtest erineva) hääle; või
- kuritarvitab ID-kaarti ning annab hääletajale teadmata digitaalallkirju; või
- blokeerib hääletamise.

Samad riskid olid olemas 2003. aastal, selle analüüsi esimese versiooni kirjutamise ajal ning need riskid eksisteerivad ka 2010. aastal. Selles osas on olukord muutumatu. Tõsi küll, ründeid tehakse tihedamini, ründed võivad olla paremini ettevalmistatud ning enamik ründeid tehakse kuritegelikel eesmärkidel.

Praeguseks ajaks on teada üks rünne välisriigis, kus kasutati ära arvutiga ühendatud kiipkaarti ning kus kasutaja nimel tehti pangas rahalisi tehinguid, ilma et kasutaja seda ise tähele oleks pannud. Varemalt teadaolevat ning varemgi tehniliselt võimalikuks peetud rünnet on nüüd praktikas demonstreeritud, kuid asjaoludel, mis seni oluliselt ei muuda e-hääletuse riskihinnangut.

Eestis on praeguseks ajaks tekkinud ka teoreetiliselt huvitav olukord, kus ID-kaardi draiveritest on loodud kaks versiooni, millest ühe lähtekood on avalik ning kõigile soovijatele kättesaadav. Baastarkvarade paljususe tõttu on lõppkasutajad sunnitud tegema nende vahel valiku ning pahaaimamatu arvutikasutaja ei suuda tihti vahet teha, millisest allikast pärit ID-kaardi draiverid on ohutud ning millised mitte.

Samal ajal on ka rünnete avastamine, nende käsitlemine kuritegudena, nende uurimine ning kurjategijate väljaselgitamine nii Eestis kui mujal maailmas oluliselt edasi arenenud. Ka

arvutite kaitsmisele pööratakse oluliselt enam tähelepanu ning kokkuvõtteks ei ole praktiline olukord lõppkasutaja keskkonna riskide osas palju muutunud.

Pikemalt on hääletaja arvutiga seotud põhimõttelised probleemid lahti kirjutatud Avi Rubini töös [Rubin] ning konkreetselt Eesti e-valimiste süsteemi riske on käsitletud ka Buldase ja Mägi artiklis [BM]. Kahjuks on tegemist selliste riskidega, mida e-hääletamise kesksüsteem ei saa kontrollida ega vältida.

Leiame siiski, et hääletaja arvuti usaldamine, hoolimata teadaolevatest rünnetest tema vastu, on hääletamise läbiviimisel aktsepteeritav risk.

Põhjused on järgmised:

- Ühe hääletaja arvuti või võrguühenduse ründamine tema hääle võltsimise eesmärgil ei ole mõistlik. Kogu hääletuse tulemust saab mõjutada ainult massilise ründega.
- Ühe hääletaja arvuti ründamine tema paroolide/PIN-koodide saamise eesmärgil ei ole seotud e-hääletamisega sündmusega – seda võib teha ka igal muul ajal.
- Ühe hääletaja arvuti sihitud ründamine, eeldades, et seda arvutit kasutab see või teine konkreetne isik, ei ole tänapäeval praktiline. Enamik ründeid on automatiseeritud ning mõeldud massiliseks kasutamiseks.
- Massilise arvutite vastase ründe salajane läbiviimine on praktiliselt võimatu. Seda on näidanud kurivara levik – ka kuitahes kavalalt kirjutatud ja *stealthy* kurivara ilmutab ennast mingit tüüpi arvutites ikka, kui mitte muul põhjusel, siis arvuti (Windowsi, brauseri, Outlooki...) enda vigade tõttu. Ka viimase aja kõige edukam kurivara Stuxnet, mis oli loodud ennast levitama väga märkamatult ning avaldas enda mõju ainult väga üksikutes olukordades, avastati sellest hoolimata. Hääletajate arvutite konfiguratsiooni erinevused ning operatsioonisüsteemi, brauseri, viirusetõrjetarkvara jm paljusus tingib olukorra, kus osad hääletajad panevad rünnet tähele ning see avastatakse ning blokeeritakse.

  E-hääletamine ise võib säärase ründe tulemusel isegi ebaõnnestuda, kuid väga tõenäoliselt tuvastatakse ründaja ja ründe ulatus. On selge, et ründe edukus jääb piiratuks ning ründaja esialgne eesmärk ei täitu. Seetõttu ei ole sellise ründe tellimine poliitilise tellimustööna kuigi reaalne.
- Massilise veebiserveri võltsimise ründe läbiviimine on võimalik, kui valijate teavitamine e-valimiste veebiserveri aadressist ei ole piisavalt aktiivne.
- Kuna hääle andmine toimub veebi mõttes "ebastandardse" tehnoloogia abil (kasutatakse eraldi rakendust), on hääle võltsimiseks vajalik teadmus võrdlemisi suur. Ükskõik millise Interneti-panga ründamine on vähemalt suurusjärk-kaks kergem, sellest saadav kasu on aga palju reaalsem.

3.1.2. Vajadus usaldada avalikke internetipunkte

Eraldi tuleb vaadata arvuteid, mida kasutab palju inimesi: AIP-d ja internetikohvikud, koolide arvutiklassid, suurte ettevõtete tsentraalselt hallatud arvutid ning ka spetsiaalsed valimiste ajaks püsti pandud nö „valimistelgid“, mis pakuvad samuti e-valimise võimalust.

Selliste arvutite ja võrkude administraatoritel on võimalik rünnata kõiki sealtkaudu hääletajaid, lastes hääletada näiteks vaid oma lemmikerakonna poolt. Kooli arvutiklassi võib muidugi kompromiteerida ka lihtsalt nutikas koolijüts.

Interneti-pankade vastu on maailmas selliseid ründeid tehtud, ehkki (teadaolevalt) vaid paar korda. Leiame siiski, et ka see risk on väike ning ei saa mõjutada suurt hulka e-hääletajaid.

Pigem juhime tähelepanu oluliselt suuremale ja üldsegi mitte tehnilise iseloomuga riskile, et AIP haldajal on keskmisest suurem võimalus kohapeal hääletajate otsuseid suunata või mõjutada. Selles kontekstis tuleb inimesi hoiatada, et nad võimalusel väldiksid (eriti just parteipoliitiliste) internetipunktide kasutamist.

3.1.3. Vajadus usaldada avalikku võrku

Lisaks oma arvutile peab võrgukasutaja usaldama avalikku Internetti kogu selle keerukuses.

Valija ***peab*** hääletamist alustama õigelt veebilehelt. See on kogu hääletusprotsessi turvalisuse alus. Kui keegi suudab meelitada valija alustama "hääletamist" valelt veebilehelt, siis ei saa edasise tegevuse kohta mingeid piire seada: talle võidakse saata vale rakendus, anda vale kandidaatide nimekiri, kogu tema arvuti kontrolli alla võtta. Täpsemalt on neid riske analüüsitud riskianalüüsi peatükis 9.2.2, "Interneti kasutusega seotud riskid".

3.1.4. Vajadus usaldada Kesksüsteemi arvuteid

Kesksüsteemi arvutite süsteemne kiht – operatsioonisüsteemid ja standardtarkvara ehk kontseptsioonis kirjeldatud "mustad kastid" – on meie jaoks komponendid, mida lihtsalt tuleb usaldada. Selle usaldusvajaduse saab viia miinimumini, hankides neid komponente vaid usaldusväärsetest allikatest, kes seejuures ei tohiks teada nende kavatsetavat kasutusviisi. Põhimõtteline probleem jääb aga alles.

3.1.5. Võimatus toetada kõiki valijaid

Igasuguse tehnika kasutamine välistab mingi osa inimestest, kes seda kasutada ei saa, kas siis seetõttu, et tal pole juurdepääsu arvutile, tal puuduvad vajalikud arvutioskused, arvuti kasutamist takistab füüsiline või vaimne puue, inimesel pole soovi arvutit kasutada või siis lihtsalt kasutab inimene sellist platvormi, mis ei ole üldlevinud. Ka HR ei hakka kindlasti töötama kõikidel Eesti Vabariigi kodanike käsutuses olevatel arvutitel. Kuigi rakendus luuakse nii Windows, Linux kui ka MacOSX platvormile, jääb siiski teatud hulk platvorme ja operatsioonisüsteemide versioone toetamata. Eestis ei ole ka mingit ametlikku standardit, mis kinnitaks riigis legaalselt "lubatud" arvutiplatvormid, mida e-hääletamine siis toetada saaks.

3.1.6. E-hääletamise ja tavahääletuse protsesside konfliktid

E-hääletamine toimub samal ajal tava-hääletusega; selle eest vastutavad ning seda viivad tõenäoliselt läbi samad inimesed.

See tähendab, et e- ja tava-hääletuse protsesside vahel võib tekkida konflikte. Inimesed peavad tegema mitut asja korraga, teadma senisest rohkem ning jagama oma tähelepanu mitme süsteemi vahel.

Näitena toome jaoskondade prioriteedikonflikti. E-häälte lugemise alustamiseks peavad olema *kõikidest* jaoskondadest laekunud *kõik* e-häälte tühistusavaldused, need peavad olema ringkondade komisjonide kaudu VVK-sse ja sealt Kesksüsteemi jõudnud. Viivitus kasvõi ühe jaoskonna töös blokeerib kogu e-hääletamise lõpetamise protsessi. Samas on jaoskondade jaoks nende nimekirjade tegemine ja saatmine väga ebaoluline töö, kuna jaoskonna enda hääletustulemus sellest ei sõltu.

3.1.7. Protsesside tsentraliseerimise riskid

Kontseptsioon kirjeldab tsentraliseeritud lugemisega hääletamis- ja lugemisskeemi.

Tsentraliseerimine annab efektiivsuse, kuid toob kaasa riskide kontsentreerumise. Seda nii tehnilisel kui inimeste tasemel – üksainus programmeerija viga või ühe hääli lugeva isiku ebaausus annavad siin palju suurema efekti kui tavalisel, jagatud protsessil põhineval hääletamisel.

3.1.8. Protsesside formaliseerumisega kaasnevad riskid

Füüsilise maailma reeglid on alati "pehmed", kuna inimestevahelisi suhteid saab igal erijuhul muuta. Infosüsteemidesse valatuna muutuvad reeglid aga rangeteks, enam neid eirata ega "nurki lõigata" ei saa.

Tulemusena võivad liigformaalsed protseduurid töö täielikult blokeerida, või kaovad ära mõned siiani toiminud ja sisuliselt mõistlikud erandite tegemise viisid.

Toome näiteks valija isiku tuvastamine. Tavavalimistel lubatakse naise ja lastega valima tulnud pereisa hääletama ka siis, kui tal pass koju on jäänud; usutakse abikaasa sõna, vaadatakse töötõendit või spordiklubi liikmekaarti ning võetakse valesti autentimise risk. E-hääletamisel sellist võimalust ei ole; kuna HR ↔ HES protokollis "nurumise" sõnumeid ei ole, siis ilma ID-kaardita e-häält anda ei saa.

Drastilisemaks näiteks on Londoni kiirabi dispetšersüsteemi realiseerimine IT vahenditega. Ekipaažide senine mitteformaalne juhtimine lakkas töötamast ning muutuse otsese tagajärjena suri kolme päevaga 26 inimest, kelleni abi ei jõudnud.

Tuleb läbi mõelda need valimiste käigus läbiviidavad protseduurid, kus praegu kiputakse reegleid rikkuma, ning mõelda, kas e-hääletamine tekitab nendes kohtades probleeme või ei. Siin tuleb saada sisend tava-hääletuse töökorralduse võimalikult madalatelt tasemetelt.

3.1.9. Süsteemi sisend- ja väljundandmete volitamatu muutmine

E-hääletamise süsteemi võib vaadata masinana, mis saab sisendiks kandidaatide ja valijate andmed ja hääletajate valikud ning annab väljundiks hääletustulemuse ja seda kinnitavad kontrollandmed.

Kõikide nende sisendite ja väljundite korrektsus on kriitiline. Igasugune tehniline turvalisus kaotab mõtte, kui keegi ei kontrolli, kas VVK valimiste infosüsteemi sisestatud numbrid klapivad HLR poolt kokku loetutega.

3.1.10. Arendus- ja haldusprotsessi probleemid

Iga infosüsteemi kaks tegelikult kõige ohtlikumat riski on *arenduse kvaliteet* ehk *tarkvara vead* ja *halduse kvaliteet* ehk *süsteemi konfigureerimise vead*. Nii testimata tarkvara kui ka hooletu haldus tekitavad lisaks lihtsalt vigadele ka turvaprobleeme. E-hääletamise süsteem on sellistele vigadele eriti avatud, kuna ta on hajussüsteem (koosnedes mitmes eri keskkonnas töötavast komponendist), harva kasutatav, raskesti testitav ja aegkriitilise valmimistähtajaga.

Krüptograafia kasutamisega kaasnevad rakenduse kvaliteediprobleemid
Hääletusskeem kasutab avaliku võtme tehnoloogiat (PKI) nii serverite poolel kui ka HR-is, tehtavad operatsioonid on seejuures võrdlemisi lihtsad. Praktika näitab aga, et detailide keerukuse tõttu tehakse PKI realiseerimisel väga tihti vigu, kusjuures pisivea efekt võib olla

turvalisuse täielik kadu. Näiteks Microsofti PKI-väljatöötlustes on olnud väga drastilisi vigu (signeerimisahelate kontrolli puudulikkus).

E-hääletamises on krüptograafiast tekkinud probleeme oodata eeskätt HR töökindluses (kontrollimatu keskkond) ning häälte kokkulugemisel (keerukas võtmehaldus).

Lihtsat rohtu ei ole. Rakenduste korrektsus tuleb tagada hoolika analüüsi ja testimisega. PKI-rakenduste loomiseks tuleb varuda rohkem aega ja raha kui sarnase funktsionaalse keerukusega, kuid krüptograafiat mitte kasutava tarkvara jaoks. Hoolimata sellest, et missioonikriitilise tarkvara väljatöötamine ning kasutamine on väga kulukas ja keerukas, suudetakse seda näiteks kosmose, energia jms valdkondades siiski edukalt teha. Senised kogemused Eesti e-hääletamise lahenduse realiseerimisel näitavad, et seda on võimalik teha ka meil.

3.2. Tehnilise riskianalüüsi kokkuvõte

Olulisemad tehnilised riskid jagunevad laias laastus nelja kategooriasse:

- Interneti kui avatud ja avaliku keskkonna riskid;
- hääletamisel juhtuvad vead, mida võimendab hääletaja jaoks tundmatu rakenduse kasutamine;
- hääli salvestava/sorteeriva serveri kui süsteemi kõige keerukama komponendi vead;
- häälte kokkulugemise probleemid, mida võimendavad kõrged nõuded protsessi organisatoorsele turbele.

Detailne analüüs on toodud peatükis "Lisa 3 - tehniline riskianalüüs", siinkohal anname nimekirja kümnest meie arvates kõige olulisemast (suurema mõju ja tõenäosusega) riskist.

Risk	**Rakendumise koht**
Kasutaja arvuti ründamine ja kontrolli alla võtmine	OS, rakendused
Hääletaja rakenduse tõrked ja kvaliteediprobleemid	HR
Vahendusründed veebiserveri ja hääletaja arvuti vahel, võlts-veebilehed	Internet
Hääletaja rakenduse või selle sisendandmete kompromiteerumine	HR, HES
Veebiserveri näotustamine või selle sisu volitamatu muutmine	HES
Hääle salajasuse rikkumine veebiserveris hääle andmise jooksul	HES
Klassikalised veebirakenduse / veebiserveri halduse ja turvalisuse vead	HES
Kesksüsteemi (HTS) tarkvara tõrked ja kvaliteediprobleemid	HTS
HLR rakenduse funktsionaalsed vead	HLR
HLR salajase võtme häving / juurdepääsu võimatus	võtmehaldus

Kõige kõrgem turvarisk on veebiserveri sisu ja rakenduste turvalisus. Siin kombineeruvad vigade suur tõenäosus ja rünnete kerge teostatavus kogu hääletusprotsessi mõjutava efektiga.

Mitte ühtegi varem teadvustamata põhimõttelist probleemi, millega kontseptsioonis arvestatud ei ole, me ei leidnud: skeemi lihtsus tingib ka vigade lihtsuse, intuitiivne tulemus ei ole palju halvem kui tehniliselt süstemaatiline riskianalüüs.

Kokkuvõtteks võib aga öelda, et e-hääletamise riskid on tegelikult väga sarnased tava-hääletuse riskidele, enamikul tehnilistel rünnetel ja ohtudel on tava-maailmas analoogid. IT-süsteemide asemel on inimesed ja organisatsioonid, aga skeem ja protsessid on samad.

Hääletaja rakenduse vigade asemel on tava-hääletusel valed/vigased nimekirjad ("*Florida butterfly*", [Florida]), häälte kontrollimisel ja kokkulugemisel teevad vigu nii tarkvara kui inimesed, on olemas käideldavuse probleemid (järjekorrad valimisjaoskondades) ja ründed usaldusväärsuse vastu (protestid).

E-hääletamine lisab siia vaid sõltuvuse tehnikast. Lisaks kehtib üldine tehnoloogiast tekkiv probleemide võimendumise efekt: vigade sagedus väheneb, nende ulatus aga suureneb.

4. NÕUTAVAD JA SOOVITATAVAD TURVAMEETMED

Me ei hakka kirja panema tavalisi turvaliste süsteemide ehitamise nõudeid – neid võib lugeda paljudest asjakohastest infoturbe raamatutest või -standarditest. Eeldame, et kasutatakse pääsukontrolli, haldustegevused on dokumenteeritud, operatsioonisüsteemid (kontseptsiooni "mustad kastid") on turvavigade suhtes uuendatud, rakendused kontrollivad oma sisendit ja logivad tehtud tegevusi ja nii edasi.

Soovitame süsteemi üldturbes tugineda ISKE turvatasemele H.

Samas ei saa ühegi üliolulise süsteemi turvalisus piirduda etalonturbega. Siin loeme me seega üles turvanõuded, mis tulenevad e-hääletamise süsteemi spetsiifilistest iseärasustest.

4.1. Üldised nõuded kesksüsteemile

4.1.1. Nõuded Kesksüsteemi arhitektuurile

Kesksüsteemi operatsioonisüsteemide ja andmebaasi valiku printsiibid on kontseptsioonis kirjas ning neid tuleb järgida. Eesmärgiks on lihtsus ja kontrollitavus.

Kesksüsteemi eraldatus
E-hääletamise Kesksüsteem peab olema eraldiseisev infosüsteem eraldiseisvate serverite ja nendevahelise võrguühendusega.

Võrgu tsoneerimine
Veebiserver / HES peab asuma eraldi võrguosas, kuid mitte tulemüüri ja avaliku võrgu vahel.

Süsteemsete platvormide funktsionaalsuse piiramine
Kõikide serverite ja muude süsteemi osade funktsionaalsus peab olema absoluutselt minimaalne etteantud teenuste ja rakenduste tööks vajalik. Serverites ei tohi olla arendusvahendeid (kompilaatorid, mittevajalike programmeerimiskeelte tugi), andmebaasi juurdepääsu vahendeid, jne. Mittevajalikud rakendused ja teenused ei tohi olla installeeritud, tulemüürides tohib olla lubatud vaid minimaalne hulk absoluutselt vajalikke võrguprotokolle, jne.

Võrgutasemel ründetuvastus ja süsteemide tervikluse tagamine
Süsteem peab tuvastama reaalajas enda vastu võrgutasemel sooritatud ründed (võrgutasemel IDS). Serverid peavad tuvastama operatsioonisüsteemi ning e-hääletamise jaoks oluliste failide tervikluse rikkumise. Selleks võib kasutada näiteks mõnda Tripwire sarnast vahendit.

Serverite oleku salvestamine
Enne e-hääletamise algust tuleb Kesksüsteemi serveritest teha nn "puhtad" koopiad, mis sisaldavad kogu serverite konfiguratsiooni ja tarkvara. Seejärel on võimalik hääletuse käigus tõrke andnud server taastada töötavasse konfiguratsiooni maksimaalselt kiiresti.

Pärast häälte andmise perioodi lõppu tuleb luua kõikide HES ja HTS serverite kõvaketastest ning nendes olevatest andmetest "külmutatud" auditikoopia.

Teine auditikoopia tuleb luua tulemuste lõpliku fikseerimise eel.

Auditikoopiaid tuleb hoida turvaliselt – turvaümbrikus ja lukustatud seifis – ning nendele ligipääsu faktid peavad olema fikseeritud.

Keskse andmebaasi kasutamine
Kandidaatide ja valijate andmebaas peab olema üks ja ühine kõigi süsteemi komponentide jaoks ning paiknema HTS-is (või eraldi andmebaasiserveris). Erand on muidugi HLR, millele tuleb kõik andmed ette anda staatiliste failidena.

4.1.2. Nõuded Kesksüsteemi rakendustele

Kasutajaliideste mitte-graafilisus
Kuna kõik sooritatavad operatsioonid on äärmiselt lihtsad, siis soovitame kogu Kesksüsteemi ulatuses kasutada ainult tekstilise või pseudograafilise liidesega rakendusi. See võimaldab kasutada lihtsamaid arendusvahendeid, suurendada rakenduste läbipaistvust, loobuda graafiliste liideste installeerimisest Kesksüsteemi serveritele jne. Negatiivseks küljeks on rakenduste spartalikum (tehnilisem, vähem atraktiivne) väljanägemine. Lisaks tekib vajadus nende kasutamine täpselt dokumenteerida, kuid see on voorus, mitte puudus.

Tehniliste vigade logimine
Kõik Kesksüsteemi rakendused peavad nende töö jooksul juhtunud tehnilised vead ja loogilised vastuolud registreerima ja Auditisüsteemile edastama.

4.1.3. Töökindluse tagamine

Siin kirjeldame ära töökindluse tagamise arhitektuursed ja puhttehnilised meetmed. Ei tohi aga ära unustada riskianalüüsi väidet – kõige suuremad töökindluse riskid seisnevad halduse vigades ning vigases tarkvaras.

Süsteemi käideldavuse nõuete spetsifitseerimine
Süsteemi käideldavuse nõuded peavad olema fikseeritud. Peab teadma, kui kiiresti peab hääletajale vastuse andma, kui kaua tohib aega võtta häälte sorteerimine ja lugemine, jne. Need on sisendandmed süsteemi tehnilise disaini jaoks.

Koormustestid
Süsteemile tuleb teha koormustest (*load test*) ja ülekoormustest (*stress test*).

Monitoorimine
Peab eksisteerima kogu süsteemi kui terviku tööd monitooriv rakendus, mis salvestaks kõik kogutavad jõudlusandmed. Vigade korral tuleb süsteemi haldajale tuleb saata veateavitus.

Andmekadude piiratus, andmete taastatavus
Tuleb ära piirata andmete hulk, mis Kesksüsteemi vigade korral kaotsi minna võib. Selleks on kaks meetodit – kõikide sisendandmete dubleerimise ja taasesitamise võimalus või andmete tarkvaraline peegeldus teise süsteemi.

Lihtsam meetod on teha sagedasi varukoopiaid e-hääletamise käigus tekkivate andmetest (andmebaasi *redo*-logidest). Kuna andmete maht on väike, siis võib selle varukoopiate tegemise sageduse valida sobilikult väikese (näiteks iga viie minuti tagant).

Taasteplaanide olemasolu
Peavad valmis olema protseduurid kogu süsteemi või andmebaasi uuendamiseks olukorras, kus mõni komponent või andmebaas on mingil põhjusel (riistvara rike, haldusviga vms) hävinud.

4.1.4. Nõuded andmeformaatidele

Andmeformaadid peavad olema nii lihtsad kui võimalik.

Eelistatud on “inimloetavad” formaadid.

XML ei ole iseenesest eelis, välja arvatud väliste kanalite jaoks (tühistused / ennistused).

Transporditavate andmete tervikluse tagamine
Andmete transpordil HES-HTS ning HTS-HLR vahel tuleb rakendada meetmeid, mis tagaksid ülekantavate andmete tervikluse. Terviklust tuleb kontrollida nii andmete transpordi hetkel kui hiljem, auditeerimise käigus.

Auditeerimise käigus nõutavad kontrollid on kirjeldatud vastavas sektsioonis.
Transpordil tuleb rakendada lihtsamaid meetodeid, näiteks kontrollsummade arvutamist.

HLR sisend ja väljund lihtteksti
Kogu HLR sisend ja väljund peavad olema lihttekstis (näiteks CSV formaat).
XML (või ükskõik milline SGML-põhine vorming) lisaks HLR rakendusele liialt keerukust.

Võltsimiskindel, lihttekstis logimine
Auditeeritavate logide jaoks tuleb kasutada võltsimiskindlat logimist.
Logid peavad olema lihttekstis loetavad.

Hääle krüptogrammi formaat
Lahtisel kujul hääl peaks olema võimalikult lihtsas formaadis, soovitavalt ASCII tekst.

Hääle krüpteerimiseks soovitame standardi PKCS#1 2.1 krüpteerimisskeemi RSAES-OAEP, abifunktsioonidena kasutada standardis toodud vaikefunktsioone [PKCS]. Sisuliselt tähendab see hääle krüpteerimist otse RSA algoritmi abil, ilma vahepealse sümmeetrilise krüpteerimiseta. See piirab küll ära hääle pikkuse ja ei sobi keerukate (mitme valikuga, vabateksti võimalusega) hääletusskeemide jaoks, kuid on Eesti skeemi puhul parim valik.

Hääle võib signeerida ükskõik millise digitaalallkirja sertifikaadi abil, millel ei ole e-hääletamist keelavat kasutusvaldkonna piirangut. Praegusel hetkel sobivad nendeks ID-kaart, DigiID ning Mobiil-ID. Tulevikus võib olla olemas ka teisi digitaalallkirja sertifikaate, siis võib kasutada ka neid.

4.1.5. Nõuded välistele andmekanalitele

Kandidaatide nimekirjade avalikkus
Igal soovijal peab olema võimalus saada koopia kandidaatide täielikust nimekirjast.
VVK peab eraldi sõltumatu kanali kaudu avalikustama selle nimekirja kontrollsumma.

Sisendandmete tervikluse kontroll

Süsteemis olevat valijate nimekirja ja kandidaatide nimekirja peab saama võrrelda AS Andmevara ja VVK originaalidega.
Näiteks võib nii Kesksüsteemi kui VVK andmebaasis olla päring, mis arvutab kontrollsumma üle valijate nimekirja kantud hääletajate isikukoodide.

Väljundandmete tervikluse kontroll
Süsteemist lahkuvad failid (hääletustulemused, e-hääletanute nimekirjad) peavad olema mingil viisil süsteemis olevate andmetega võrreldavad.

Tühistuste ja ennistuste nimekirjade allkirjastamine
VVK-st lähtuvad tühistuste ja kinnituste nimekirjad peavad olema digitaalselt allkirjastatud. HTS tühistus/ennistusrakendus peab seda allkirja kontrollima HTS-is oleva volitatud allkirjastajate nimekirja vastu, milles peab olema vähemalt kaks isikut.

4.2. Nõuded süsteemi komponentidele

4.2.1. Nõuded HR-ile

Hääletaja autentimiseks tuleb kasutada autentimisvahendil paiknevat ametlikku **autentimis-sertifikaati,** mitte muid sertifikaate, mis võivad samuti autentimisvahendil olla.

Rakendus ei tohi puhverdada hääletaja kiipkaardi sertifikaatide pääsukoode ning võimaluste piirides tagama, et ka operatsioonisüsteemi teegid ning muu baastarkvara ei lubaks puhverdamist.

Hääletaja valiku ja vaadatavate andmete peitmine veebiserveri eest
Brauseris / HR-is toimuv kandidaatide andmete vaatamine peab olema veebiserverist täiesti sõltumatu. Kogu hääle andmiseks vajalik informatsioon tuleb brauserisse saata ühe päringuga, nii et veebiserveril ei oleks teadmist, milliste kandidaatide andmeid hääletaja täpselt vaatas.

4.2.2. Nõuded HES-ile / Veebiserverile

Veebiserveri autentimine hääletaja poolt, HTTPS
Suhtlus veebiserveri ja hääletaja arvuti / HR vahel ***peab*** olema turvatud.
Oluline on serveri autentimine, kanali krüpteeritus on sekundaarne.

See on kõige olulisem hääletamisprotsessi nõue üldse. Kui hääletaja satub valele veebiserverile, on see võrdne valimisjaoskonna asemel mõne partei peakorteris hääletama hakkamisega: tagada ei saa mitte midagi, tulemus ei pruugi omada valija tahtega mingit seost.

Server peab töötama turvatud režiimis, s.t. kasutama HTTPS protokolli.

Hääletajal saab veebiserveri autentsust kontrollida selle *sertifikaadi* kaudu.
Sertifikaat *ei pea* seejuures tingimata olema signeeritud hääletaja arvuti poolt usaldatava sertifitseerimisserveri poolt; tegeliku turvalisuse loob see, kui valija kontrollib serveri sertifikaadi kontrollsummat ("sõrmejälge"). Vastav võimalus on igas Interneti-brauseris olemas.

Serveri sertifikaadi kontrollimise kirjeldus ja õige kontrollsumma tuleb teavitusprotsessi käigus valijatele teadvustada ja selle täitmist nõuda (või vähemalt tungivalt soovitada).

Minimaalne funktsionaalsus
Kuna tegemist on avalikus internetis oleva serveriga, mida saab kõikide seal töötavate rakenduste ning kõigi avatud teenuste/protokollide kaudu rünnata, siis tohivad veebiserveris olemas olla (mitte ainult töötada, vaid ka installeeritud olla!) vaid need komponendid, mida on vaja.

Hääletaja autentimine autentimisvahendi autentimissertifikaadiga
Hääletaja tuleb autentida autentimissertifikaadiga ning mitte mingil muul viisil. Lisaks tuleb kontrollida, et antud hääl oleks digitaalselt allkirjastatud sama isiku poolt, kes ennast veebiserverile autentis.

HTTP veebiserveri ainus funktsioon olgu HTTP ümbersuunamine
Hääletajate mugavuse jaoks võidakse siiski otsustada hoida üleval ka HTTP teenust.
Sellisel puhul peab selle serveri ainus funktsioon olema HTTP ümbersuunamine tegeliku turvalise HTTPS veebilehe peale.

E-hääletamise kasutatav domeen peab asuma .ee tippdomeenis.
Soovitame e-hääletamise jaoks reserveerida eraldi serverinime (FQDN), mida kasutatakse ainult e-hääletamise läbiviimiseks.

Veebiserveri poolt kuvatavate kandidaatide andmete piiramine
E-hääletamise lehel või HR-is tohib kandidaatide kohta olla ainult ametlikult vajalikuks tunnistatud, kõikide jaoks ühetaoline informatsioon.
Seal ei tohi olla viiteid reklaammaterjalidele, näiteks kandidaatide kodulehekülgedele.

Veebiserveri sisu peab olema võimaluste piires staatiline
Kandidaatide andmete näitamise, HR laadimise ning abiinfo andmise veebilehed ei tohi olla andmebaasis. Kui kandidaatide arvukuse tõttu või muul põhjusel tuleb andmeid hoida andmebaasis, siis tuleb veebiserveri jaoks ikkagi genereerida staatiline koopia.

Staatiline, standardne, valideeritud HTML
Hääletajale näidatavad veebilehed peavad olema kirjutatud staatilises HTML-is, mis ei kasutaks brauseris ega serveris käivitatavaid aktiivseid skripte.
Veebilehed tuleb valideerida võimalikult vähenõudliku (minimalistliku) HTML standardi järgi.

Korrektsete häälte logimine
HES peab HTS-ile edastatud, korrektseid hääli logima (Log1).
See on sisuliselt ainus võimalus auditeerida HTS tööd.

Vigaste häälte mitte-logimine
Kui HES tuvastab, et hääletajalt saadud e-hääl on tehniliselt vigane, siis selliseid hääli ei tohi salvestada. On võimalik, et viga oli krüpteerimises ning salvestamine rikuks hääle salajasuse. See on probleem hoolimata sellest, et konkreetne hääl jäi hääletusel arvesse võtmata.

Tava-turvalisuses vastab sellele nõudele keeld logida ebaõnnestunud autentimiskatsete andmeid ("vigaseid paroole").

Küll aga tuleb logida vigase hääle saamise fakt.

Tehniliste vigade logimine
HES peab logima kõik hääle andmise protsessi vead. Autenditud isiku ja hääle signeerija mittevastavus, poolelijäänud sessioonid (näiteks hääletajale tagasi saatmata jäänud kinnitus hääle arvestamise kohta) jne peavad saama registreeritud.

***Reverse proxy* kasutamine**
Veebiserveri kõik hääletajale tagastatavad vastused peavad läbima *reverse proxy*, mis teeb nende sisule elementaarse turvakontrolli.

HES rakenduse multitegumilisus
HES peab olema võimeline teenindama mitut hääletajat paralleelselt.
Tuleb arvestada, et hääle edastamine HTS-ile ning HTS vastuse ootamine võib võtta aega.

HES → HTS ühenduste loomine
HES ja HTS vaheliseks andmevahetuseks peavad olema loodud püsikanalid.
Nende arv peab olema piiratud nii alt kui ülaltpoolt. Maksimaalse ühenduste arvu piiramine hoiab ära HTS ülekoormamise HES poolt (hääle kümnekordse saatmise risk). Sisuliselt tähendab see, et rakendustasemel teenustõkestusründed ei pääse HES-ist kaugemale.
Kanalid peab looma HTS, s.t. ühendused võetakse sisevõrgust väljapoole.

Hääle vastuvõtmise / tagasilükkamise kinnitus
HES peab HR-ile või brauserile tagastama HTS-ist saadud kinnituse saadud hääle aktsepteerimise või tagasilükkamise kohta. Kinnitus peab olema lõplik, positiivse kinnituse saanud hääl peab olema tõesti HTS-is salvestatud. See ei välista muidugi hääle hilisemat tühistamist kontseptsioonis toodud põhjusel (tava-hääletusel osalemine vms).

Rakendustasemel rünnete tuvastus
Vajalik on monitoorida ning analüüsida hääle andmisel rakendustasemel tekkivaid vigu ning ründeid.

See tegevus ei ole kerge, kuna nõuab võimalike ründemallide ette ennustamist ja äratundmist. Tavaliste süsteemide puhul annavad igapäevase kasutuse logid selleks võimaluse, e-hääletamisel neid andmeid pole. Kui monitoorimine ei ole võimalik, tuleb see analüüs teha hiljem, auditisüsteemi abil.

Näidisreeglid monitoorimiseks on järgnevad:
- rohkem kui N autentimist ühe hääletaja jaoks;
- rohkem kui N ühe hääletaja poolt antud häält,
- rohkem kui N autentimist ühe hääletaja jaoks, millele ei järgne hääle andmist;
- rohkem kui N autentimist väga lühikese ajavahemiku jooksul;
- lahknevus autenditud valija ja hääle signeerija vahel,
- tehniliselt vigaste (vales formaadis, signeerimata, ...) häälte andmine,

jne.

4.2.3. Nõuded HTS-ile

HTS on e-hääletamise süsteemi kõige keerukam komponent.
Just HTS kaudu sooritatakse enamik vajalikke administratiivseid tegevusi – häälte sorteerimine, e-hääletanute nimekirjade tekitamine, tühistusnimekirjade ja ennistuste sisestamine jne.

HTS rakenduste turvalisus
Kõige lihtsam ja kõige olulisem nõue on HTS-is töötavate rakenduste "klassikaline" turvalisus.

Mingit nimekirja siinkohal anda ei ole mõtet – tähtis on, et HTS rakendused töötaksid vastavalt spetsifikatsioonile ja jälgiksid tavalisi turvareegleid. Kasutajaid peab autentima, iga tegevuse kohta peab tekkima logi, paroole (kui neid kasutatakse) peab hoidma ja edastama krüpteeritult, rakendused ega kasutajad ei tohi omada rohkem õigusi kui vajalik, ja nii edasi.

HTS rakenduste korrektus
Kui hääletuse ajal leitakse HTS sorteerimis-rakendustes vigu, siis tingib see ilmselt vajaduse erakorraliseks otsejuurdepääsuks e-häälte andmetele. Iga selline juurdepääs on tõenäoline turvanõuete ja protseduuride rikkumine. Seepärast on HTS rakenduste töökindluse korralik testimine ühtlasi ka turvameede.

HTS rakenduste ja kasutajate õiguste piiramine
Rakendused ei tohi omada ega kasutajatele anda rohkem õigusi kui vajalik – näiteks ei tohi hääli sorteeriv protsess saada muuta kandidaatide nimekirja.

See on realiseeritav operatsioonisüsteemi juurdepääsukontrollidega, andmebaasi disainiga ning erinevatele rakendustele minimaalsete vajalike andmebaasiõiguste andmisega.

Andmebaasi olek igal ajahetkel peab olema tagantjärele tuvastatav
Selleks peavad kõik andmebaasi tekitatud kirjed omama ajatemplit, muudatuste tegemisel tuleb kirje eelnev olek arhiveerida, jne.

Andmebaasi parameetertabelite ja konstantsete andmete külmutamine
HTS andmebaas sisaldab andmeid, mida ei tohi e-hääletamise jooksul muuta: kandidaatide ja ringkondade nimekirjad, parameetertabelid, antud häälte informatsioon jne. Andmebaasi õigustega tuleb tagada, et neid tõesti ***ei saaks*** muuta.

Kuna mõnede andmebaasiosade seis fikseerub lõplikult häälte andmise perioodi lõpul, siis tuleb vastavad tabelid mitte-kirjutatavaks märkida alles siis.

HTS rakenduste lisakontrollid
HTS rakendused mõjutavad hääletustulemust nii otseselt, et nende võimalike vigade vältimiseks tuleb ilmselt rakendada mitmekordseid kontrolle.

Näiteks häälte tühistusprotseduur (tavaliste ja digitaalallkirjadega varustatud andmete liikumine) on kontseptsioonis kirjeldatud. Sellele tuleks lisada programse järelkontrolli nõue: pärast tühistusnimekirja "söötmist" süsteemi tuleb kontrollida, kas HTS rakendus kavatseb tühistada sama palju (ja pisteliselt ka seda, kas samu) hääli, nagu VVK tühistusnimekirjas kirjas.

4.2.4. Nõuded HLR-ile ja HLR serverile

HLR serveri eraldatus Kesksüsteemi võrgust
HLR ei tohi omada võrguühendust. Kogu suhtlus välise maailmaga tohib toimuda vaid irdmeedia (CD, flopiketas, USB mälu, printeripaber) vahendusel.

HLR sisend ja väljund lihtteksti
Kogu HLR sisend ja väljund, k.a. kandidaatide nimekiri, peavad olema lihttekstis (näiteks CSV formaat). XML või ükskõik milline muu SGML-põhine vorming lisaks HLR rakendusele liialt keerukust.

HLR mälu kaitsmise nõuded
Andmetöötlus peab toimuma operatiivmälus. HLR ei tohi vahetulemusi (loetud hääled, hetkeseis) ei kuvada ega salvestada – kogu andmetöötlus peab toimuma ainult rakenduse mälus.

Pärast häälte lugemist ja eksporti tuleb sooritada HLR serveri alglaadimine ning hoida serverit vähemalt 3 minutit vooluvõrgust väljas.

Hääle formaadikontrollid
Lahtikrüpteeritud häälele tuleb teha enne kõiki teisi kontrolle teha tüübi- ja formaadikontroll. Kontseptsioonis kirjeldatud loogilisi kontrolle (kas sellise numbriga kandidaat on olemas, jne) tohib teha alles pärast seda.
Põhjuseks on fakt, et hääl on otsene ja kontrollimatu andmekanal välismaailmast HLR-i. Mitte keegi enne HLR-i ei saa vaadata krüpteeritud hääle sisse ega vaadata, kas krüptogrammis sisaldub tegelikult kandidaadi number või käivitatav programmikood.

Hääletustulemuse väljatrükk otse HLR-ist
Soovitame hääletustulemuse kohe pärast häälte kokkulugemist otse HLR-ist välja trükkida ja kõigi komisjoni liikmete poolt allkirjastada. See on hääletustulemuse nn "originaal".

4.2.5. Nõuded auditisüsteemile

Auditisüsteemi poolt kokku kogutavad andmed
Auditisüsteem peab koguma kokku:
- funktsionaalsed logid - LogWeb, Log1 .. Log5;
- HES, HTS ja HLR rakenduste tehnilised logid;
- IDS logid, tripwire logid;
- süsteemi serverite konsoolilogid;
- süsteemi serverite kasutajate sisselogimiste logid (utmp), jne
- vabatekstis vearaportid (kui neid tekib; sisestatakse käsitsi);
- tegevuste aktid (võtmehaldus, häälte lugemine).

Auditisüsteem peab olema turvatud samal tasemel teiste Kesksüsteemi komponentidega.

4.2.6. Nõuded süsteemi haldusprotsessile

Etalonturbe meetmestik käsitleb haldusprotsessi nõudeid võrdlemisi põhjalikult. Kordame üle vaid vajaduse haldustegevus **dokumenteerida** ning süsteemi kõikide serverite **konsoolilogid salvestada**.

Igaks uueks e-hääletamiseks tuleb kõik Kesksüsteemi serverid uuesti installeerida ja konfigureerida. Alustama peab puhtast ja võimalikult uuest operatsioonisüsteemist, ka kogu muu tarkvara tuleb installeerida ja konfigureerida alates nullist, ei tohi kasutada eelmise hääletuse serveri konfiguratsiooni. Sama tuleb teha ka peale avalikku test-perioodi.

HES ja HTS funktsionaalsuse külmutamine häälte andmise lõppedes
E-hääletamise lõppemise hetkel tuleb sulgeda Kesksüsteemi hääli vastu võttev funktsioon. E-hääletamise ajal avatud andmefailidesse (logid) ja andmebaasitabelitesse kirjutamine tuleb blokeerida, nii HES kui HTS hääli vastuvõtvad rakendused peavad lõpetama töö.

Soovitav on HES/HTS täielik eraldamine avalikust võrgust. Hääle kontrollimise rakenduse jaoks võib neist luua piiratud andmete (ainult häälte digitaalallkirjad) ja funktsionaalsusega koopia.

Häälte hävitamine pärast valimistulemuste lõplikku kinnitamist
Me ei saa olla kindlad selles, kas praegused krüpteerimismeetodid peavad vastu ka 30 aasta pärast. Seega tuleb pärast valimistulemuste lõplikku kinnitamist antud hääled kõikidelt andmekandjatelt kustutada või need andmekandjad hävitada.

Hääled asuvad selleks hetkeks:
- HTS-is (Andmebaasis);
- HLR serveris,
- serverite auditikoopiates,
- HTS - HLR transpordi-CD-des,
- auditisüsteemis.

Digitaalallkirjad, logid jne võivad säilida. Kustutada tuleb vaid häälte krüptogrammid.

Süsteemi tehnilised haldajad peavad e-hääletamise perioodil olema pidevalt kättesaadavad.

Valimiste infoliin olgu hääletajate tehnilise toe funktsiooniks valmis ning osaku lahendada sagedasemaid ID-kaardi ja HR-iga seotud probleeme.

4.3. Nõuded valimiste korraldusele

4.3.1. E-hääletamise ja tavahääletuse protsesside integratsioon

Tava- ja e-hääletamise protsessid tuleb lõimida ühtsesse töökorraldusse.

Tuleb läbi mõelda need valimiste käigus tehtavad protseduurid, kus praegu kiputakse reegleid rikkuma, ning mõelda, kas e-hääletamine tekitab nendes kohtades probleeme või ei.

E-hääletamise tühistusnimekirjade kiire ärasaatmine jaoskondades peab olema kuidagi motiveeritud.

4.3.2. Protseduuride kirjeldamise nõuded

Kõik e-hääletamise jaoks vajalikud protseduurid peavad olema eelnevalt kirjeldatud ja nende kirjelduste järgi testitud.

Dokumentatsioon peab sisaldama:
- protsessi alustamiseks vajalikke tingimusi;
- saavutatavat lõpptulemust;
- protsessi algatajaid ja osalisi;
- teostatavaid tehnilisi tegevusi;
- vajalikke protsessi käigus tekkivaid dokumente ja protsessi läbiviimise akte;
- protsessi edukuse kriteeriumite loetelu.

VVK peab määrama täitjad ja vastutajad järgmistele tegevustele:
- süsteemi arenduse koordineerimine;
- hääletusprotseduuride kirjeldamine;
- süsteemi dokumentatsiooni haldus ja avalikustamine;
- andmevahetuse korraldamine e-hääletamise süsteemi ning VVK, Andmevara jne vahel;
- Kesksüsteemi haldamine ja halduse koordineerimine;
- Kesksüsteemi monitoorimine e-hääletamise ajal;
- süsteemi varukoopiate ja auditi-informatsiooni hoidmine;
- hilisem digitaalallkirjade, audititulemuste ja protseduuride aktide arhiveerimine;
- võtmehaldus;
- valijatele tehnilise toe tagamine;
- tehniliste protestide lahendamine;
- hääletuseelse tehnilise eel-ekspertiisi tegemine;
- hääletusaegse vaheauditi tegemine;
- hääletusjärgse protseduuride auditi tegemine;
- eriolukordade lahendamine;
- avalik suhtlus.

Seejuures tuleb järgida klassikalist rollijaotuse põhimõtet, mille kohaselt süsteemi arenduse, tehnilise halduse, kasutamise ja kontrolliga peavad tegelema erinevad isikud.

Eriolukordade lahendamiseks peavad olema määratud vastutajad, kommunikatsioonikanalid ning probleemide eskaleerimise reeglid.

4.3.3. Nõuded süsteemi dokumentatsiooni avalikustamisele

Võimalikult suur osa süsteemi dokumentatsioonist peab olema avalik.

Süsteemi põhimõtteskeemid ja disainiotsused, sh käesolev turvaanalüüs, peaksid olema avalikud.

Hääletaja rakendus peab olema avalik ja kontrollitava autentsusega.

HLR avalik võti peab olema avalik ja kontrollitava autentsusega.

Kandidaatide nimekirjad peavad olema autentsel viisil kättesaadavad. See ei tähenda automaatselt nende (veebis) avalikustamist – tähtis on, et huvitatud isikul oleks olemas täisnimekirja saamise võimalus.

Avalikus võrgus kasutatavad protokollid (protokoll HES ja HR vahel) peavad olema avalikud. Põhimõtteliselt peab igal soovijal olema võimalus avalikele spetsifikatsioonidele toetudes oma isiklik hääletusrakendus kirjutada.

Kõikide süsteemi jaoks kirjutatud tarkvarakomponentide lähtekood peab olema auditeerimiseks kättesaadav; juurdepääsu tingimused selleks määrab VVK.

Valijate teavitamine e-valimiste veebilehest peab olema hästi korraldatud. E-hääletamise veebilehe aadress peab olema avaldatud avalikus meedias ning trükitud valija valijakaardile. Levitama peab otse e-valimiste veebilehe URL-i, mitte VVK veebilehe üldaadressi.
Lisaks tuleb avaldada serveri sertifikaadi kontrollimise kirjeldus ja õige kontrollsumma.

4.3.4. Teenuse kvaliteedi lepingud

E-hääletamise süsteemi haldajal peavad olema sõlmitud teenuse kvaliteedi lepingud:
- Internetiühenduse pakkujatega;
- sertifitseerimisteenuse pakkujatega (praegu AS Sertifitseerimiskeskusega) sertifikaatide tühistusnimekirjade saamise osas;
- AS Andmevaraga valijate nimekirjade uuendamise osas;
- kehtivuskinnitusteenuse pakkujaga teenuse käideldavuse osas.

Lisaks peaks olemas olema kasvõi mitteformaalsed kooskõlastused suuremate ISP-dega, kelledest samuti sõltub nende klientide ehk valijate juurdepääs e-hääletuse veebiserverile.

4.3.5. Turvakontroll süsteemi arenduse käigus

Lisaks käesolev eelanalüüsile, mis hindab kontseptsiooni, tuleb analüüsida ja testida ka süsteemi komponentide tegelike realisatsioonide turvalisust.

4.3.6. Hääletuseelne turvalisuse eksperthinnang

E-hääletamise eel tuleb hinnata, kas tehniline keskkond on e-hääletamise läbiviimiseks piisavalt turvaline. 21. sajandi algusaastad on eriti ilmekalt näidanud, kui kiiresti võib Interneti turvalisus langeda. Turvaprobleemide ilmnemisel seoses mõne konkreetse kasutatava tehnoloogiaga tuleb e-hääletamisest loobuda või, kui võimalik, turvaauk paigata (näiteks asendada tulemüüri platvorm teisega).

4.3.7. Valimisaegne vaheaudit

Pärast häälte esmast kokkulugemist, kuid enne valimistulemuste kinnitamist peab toimuma e-hääletamise *vaheaudit*. Selle eesmärk on kiirete testidega välja selgitada, kas hääletuse käigus on toimunud jämedaid turvarikkumisi ja milliseid.

Vaheauditi käigus peab tegema vähemalt järgmist:

- Võrdlema jaoskondadele saadetud nimekirju, tühistatud hääli ja VVK tühistusnimekirja.
- Võrdlema ennistatud hääli ja VVK ennistusnimekirja.
- Kontrollima IDS ja muude turvasüsteemide logisid.
- Kontrollima kõikide Kesksüsteemi serverite terviklust vastava rakenduse abil.
- Kontrollima, kas igale HES logi (Log1) kirjele leidub vaste HTS logides (Log2, Log3).
- Kontrollima, kas igale HTS logide (Log2, Log3) kirjele leidub vaste HES logis Log1.
- Kontrollima, kas igale HLR logide (Log4, Log5) kirjele leidub Log3 vaste.
- Kontrollima, kas igale HLR logide (Log4, Log5) kirjele leidub HTS-is digiallkiri.
- Kontrollima, kas häälte summa on võrdne Log5 ridade arvuga.

Soovitame lisaks ka e-häälte kontroll-ülelugemist. See sarnaneb häälte kokkulugemisega, kuid seda viivad läbi teised isikud, kasutatakse (soovitavalt) teist turvamoodulit ning tulemusi tuleb võrrelda eelmiste kokkulugemiste tulemustega.

Vaheauditi jaoks peavad olema valmis tehniliselt pädevad inimesed, kes
- ei ole seotud e-valimiste lõpptulemuse väljaselgitamisega;
- ei ole seotud süsteemi arendus- ega haldusprotsessiga.

Auditi tulemuste kohta vormistatakse kirjalik, allkirjastatud akt.

4.3.8. Valimisjärgne audit

Auditi põhiline funktsioon on kontrollida, kas kõik hääletusprotsessis ette nähtud tegevused on täidetud ning kas selle kohta on dokumendid olemas.

Turvalisuse vaatepunktist on hääletusjärgne audit võimalus hinnata süsteemi turvet ning vajadusel teha ettepanekuid süsteemi, turvameetmete ja turbeprotsesside muutmiseks järgmiste valimiste tarbeks.

4.4. Võtmehaldus

Kõikide valimiste kulminatsioon on häälte kokkulugemine. Seda toimetatakse pidulikult, mitmeliikmeliste komisjonidega, vaatlejate ning terve ühiskonna valvsa pilgu all.

E-hääletamisel on selleks tipphetkeks häältelugemisrakenduse käivitamine. Valimiskasti piduliku avamise asemel on HLR privaatvõtme aktiveerimise protseduur, kus patsiga tehnikud ja kikilipsus komisjoniliikmed veerivad kõrvuti ekraanilt numbreid lugeda.

Aga nii nagu valimiskasti turvalisus saab alguse selle ehitanud tisleri töötoast, saab ka e-hääletamise turva alguse võtmehalduse protseduuridest, mis tehakse ammu enne seda, kui hääletajad VVK veebiserverile kokku kutsutakse. Võtmehalduse protseduurid on aga esmapilgul ülimalt keerukad, nende tulemus ei ole käega katsutav ning vähimgi eksimus tekitab veaolukorra või muudab nad ebaturvaliseks. Seepärast tuleb nende protseduuride kirjeldamisel, täitmisel ja auditeerimisel olla hoolikas ja põhjalik ning – mis kõige tähtsam – saada igal hetkel aru, mida tehakse.

4.4.1. Üldised nõuded

HLR võtmehaldusele on kolm absoluutset nõuet, millest tulenevad kõik ülejäänud.
Nende nõuete rikkumisel e-hääletamine ebaõnnestub.

HLR avaliku võtme autentsuse nõue:
HR-is peab olema HLR õige avalik võti.

HLR privaatvõtme absoluutse käideldavuse nõue:
HLR privaatvõti ei tohi mitte mingitel tingimustel hävida või muutuda kasutuskõlbmatuks.

HLR privaatvõtme absoluutse salajasuse nõue:
HLR privaatvõti ei tohi mitte mingitel tingimustel saada avalikuks.

4.4.2. Nõuded võtmehaldusprotseduuridele

Võtmehaldusprotseduuride läbiviimiseks peavad kohal viibima mitu selleks volitatud isikut. Nimetame neid edaspidi *võtmehalduriteks*.

Võtmehaldurid kinnitab nimeliselt Vabariigi Valimiskomisjoni esimees.

Peab olema tehniliselt tagatud, et HLR privaatvõtit ei saaks ilma võtmehaldurite osaluseta luua, kasutada, transportida ega hävitada (neid operatsioone nimetame edaspidi *võtme kasutamiseks*).

Samas ei tohi ühe (ega ka mitme) võtmehalduri puudumine võtme kasutamist takistada, vastasel korral oleks võtmehaldurite isikutega seotud riskid liiga suured. Ehk:
Võtme kasutamiseks peab vaja olema mitut võtmehaldurit, kuid ei tohi vaja olla kõiki.

Hea tava kohaselt peavad võtmehaldurid olema sõltumatud, s.t. kuuluma erinevatesse organisatsioonidesse. Kindlasti peab võtmehaldurite hulka kuuluma VVK esindaja (või mitu), kuid ainult VVK esindajate abil ei tohi saada võtit kasutada.

Lisaks võtmehalduritele peavad võtme kasutamisel osalema vaatlejad.

Iga võtmete kasutamise operatsiooni kohta tuleb luua kirjalik, osalenud võtmehaldurite poolt allkirjastatud akt. See peab sisaldama vähemalt järgmist infot:
- osalejad;
- kellaaeg (vahemik) ja toimumise koht;
- mida sooviti teha;
- mida tegelikult tehti;
- tegevuse lõpptulemus;
- tekkinud probleemid.

Akte arhiveerib VVK.

Test- ja arendussüsteemides tuleb kasutada tegelikust e-hääletamise süsteemist erinevaid võtmeid.

HLR võtmepaar peab olema RSA võtmepaar pikkusega 2048 bitti. Lühem võti ei ole praegusel ajal enam turvaline, pikem võti muudab operatsioonid liiga aeglaseks.

HLR privaatvõti ega selle komponendid ei tohi mitte kunagi eksisteerida lahtisel (krüpteerimata) kujul.

HLR privaatvõtmest peab olema tehtud varukoopia (või kaks).
Varukoopia(te) jaoks kehtivad privaatvõtmega identsed nõuded.

Kui hääletustulemused on kinnitatud, tuleb HLR privaatvõti ja selle koopiad hävitada.

HLR avalikku võtit tuleb levitada isesigneeritud sertifikaadi kujul.
Sertifikaat ja selle kontrollimiseks vajalik info peavad olema avalikud.

Sisuliselt tähendavad eelnevad nõuded seda, et HLR võtmehalduseks peab kasutama riistvaralist turvamoodulit (HSM, *Hardware Security Module*). Selle korral hoitakse HLR

privaatvõtit ainult turvamooduli staatilises mälus. Privaatvõtme kasutamiseks tuleb turvamoodul autoriseerida mitme spetsiaalse kiipkaardi ja PIN-koodi abil. Võtmehaldurid on nende kiipkaartide omanikud ja PIN-koodide teadjad.

4.4.3. Võtmehaldurite määramise skeemid

HLR privaatvõtme juurdepääsu kontrollimiseks on mitu võimalikku skeemi. Nad kõik realiseerivad nõuet "privaatvõtme kasutamiseks vajatakse mitut võtmehaldurit, kuid mitte kõiki".

Üldiselt eeldame siin ja edaspidi, et kõik võtmehaldurid valdavad kiipkaarte ja vastavaid PIN-koode, millega nad oma õigust võtit kasutada tehniliselt realiseerivad.

Mitu mitmest (M-of-N) skeem
Võtmehaldureid on kokku `N` isikut.
Võtme kasutamiseks on vaja nendest `M` isiku kohalolu, kusjuures `M < N`.

Näiteks: kui `N=5`, `M=3`, siis on võtmehaldureid on kokku viis, võtme kasutamiseks on vaja nendest kolme kokkulepet ja kohalolekut (muidugi koos kiipkaartide ja PIN-koodidega).

Selle skeemi eeliseks on loogilisus, efektiivsus (vajaminevaid isikuid ja kaarte on vähe) ning suhteline töökindlus: 3/5 puhul võivad ükskõik millised kaks võtmehaldurit puududa, võtit saab kasutada ikka.

Komplektide skeem
HLR privaatvõtme kasutamiseks on vaja komplekti `N` erinevast kiipkaardist.
Igast erinevast kiipkaardist on `K` koopiat, igaüks neist erineva võtmehalduri käes.
Seega on süsteemis kokku `N * K` kiipkaarti ja võtmehaldurit.
Võib ka öelda, et on olemas `N` põhilist võtmehaldurit, kellest igaühel on `(K-1)` asendusisikut.

Näiteks: `N=3`, `K=3`, võtmehaldureid on kokku `3*3=9`.

Skeemi on sarnane tavalise mitme lukuga ukse avamisega: ukse igal lukul on erinev võti, igast võtmest on mitu koopiat; ukse avamiseks on vaja ühte võtit iga luku jaoks.

4.4.4. Võtmehaldusprotseduurid

Me ei saa selles analüüsis anda võtmehaldusprotseduuride kirjeldusi, kuna need sõltuvad kasutatava turvamooduli mudelist ning täpsete protseduuride esitamine oleks sisuliselt turvamooduli margi valik. Seetõttu on esitatud protseduurid mõnevõrra tinglikud, pakkudes välja ühe võimaluse ülaldefineeritud nõuete täitmiseks.

HLR võtmepaari loomine

HLR võtmepaari loomine tuleb teostada enne e-hääletamise algust. Üks selle tulemus – HLR avalik võti – tuleb integreerida HR-i ning see võtab aega.

- Võtmehaldurid autoriseerivad turvamooduli, kasutades kiipkaarte ja PIN-koode.
- Võtmehaldurid annavad turvamoodulile käsu luua HLR võtmepaar.
- Turvamoodul genereerib privaatvõtme ning avaliku võtme.
- Turvamoodul salvestab privaatvõtme oma staatilisse mällu.
- Turvamoodul genereerib HLR avaliku võtme sertifikaadi.
- Turvamoodul trükib sertifikaadi või avaliku võtme välja.
  Vastav printer on ühendatud turvamooduliga otse, ilma arvuti vahenduseta.
  Väljatrükk signeeritakse. See on HLR avaliku võtme nn "originaal".

- Turvamoodul salvestab avaliku võtme faili.
  Alternatiiv on võtme käsitsi ümbertrükkimine turvamooduli konsoolilt.
- Turvamoodul viiakse tavalisse, autoriseerimata režiimi.
- Failis olev sertifikaat trükitakse välja ning seda võrreldakse originaaliga.
- Sertifikaadile arvutatakse kontrollsumma.
- Sertifikaat ja selle kontrollsumma avalikustatakse.

HLR võtmepaari varukoopia loomine

See protseduur loob HLR privaatvõtmest koopia teise turvamooduli mällu.
Turvamoodul tohib privaatvõtit eksportida ainult nii, et selle osad (komponendid) kirjutatakse eraldi kiipkaartidele. Need kiipkaardid on mõeldud ainult selle võtme transportimiseks ning nad hävitakse pärast protseduuri.

- Võtmehaldurid autoriseerivad turvamooduli.
- Võtmehaldurid annavad turvamoodulile käsu eksportida HLR privaatvõti.
- Turvamoodul ekspordib võtme komponentide kaupa kiipkaartidele.
- Turvamoodul viiakse tavalisse, autoriseerimata režiimi.
- Kiipkaardid viiakse teise, samas ruumis paikneva turvamooduli juurde.
- Võtmehaldurid autoriseerivad teise turvamooduli.
- Võtmehaldurid annavad turvamoodulile käsu importida HLR võtmepaar.
- Turvamoodul loeb kiipkaartidelt HLR privaatvõtme komponendid, küsides iga kiipkaardi PIN koodi.
- Turvamoodul arvutab loetud privaatvõtmele vastava avaliku võtme.
- Turvamoodul viiakse tavalisse, autoriseerimata režiimi.
- Turvamoodul trükib arvutatud avaliku võtme välja.
  Vastav printer on ühendatud turvamooduliga otse, ilma arvuti vahenduseta.
- Väljatrükki võrreldakse HLR avaliku võtme originaaliga.
- Kiipkaardid hävitatakse füüsiliselt.

Kui väljatrükk ja originaal kattuvad, siis on nüüd mõlemas turvamoodulis sama HLR võtmepaar. Lisaks on olemas digitaalselt signeeritud fail HLR avaliku võtmega.

Nende protseduuride järel võib turvamoodulid vooluvõrgust lahti ühendada ning šeifi paigutada; järgmine kord on neid vaja alles tulemuste kokkulugemisel.

HLR võtmepaari testimine

Hääle krüpteerimine on e-hääletamise kõige läbipaistmatum osa. Kui iga muud operatsiooni – veebilehe kuvamist, hääle signeerimist, HTS-is toimuvaid tegevusi – saab mitmesugusel viisil kontrollida, siis häälte krüpteerimise korrektsus on peidetud kuni häälte kokkulugemise hetkeni.

Seetõttu tuleb pärast HR-i lõplikku valmimist eraldi üle kontrollida, kas kogu protsess toimib ning kas HR sisaldab õiget avalikku võtit. Selleks tuleb anda HR abil üks või mitu häält ning kontrollida, kas need on HLR poolt avatavad ning kas tulemus on õige.

- HLR abil moodustatakse üks või mitu korrektset test-häält.
- Lisaks moodustatakse mitu valehäält, millest mõned sisaldavad mittelubatud andmeid ning mõned ei ole krüpteeritud õige võtmega.
- Test-hääled kopeeritakse HLR serverisse.
- Turvamoodul ühendatakse HLR serveriga.
- Käivitatakse HLR rakendus.
- Võtmehaldurid autoriseerivad turvamooduli, kasutades kiipkaarte ja PIN-koode

- HLR rakendus avab hääled (arvutab välja e-hääletamise tulemuse).
- Turvamoodul viiakse tavalisse, autoriseerimata režiimi ning lahutatakse HLR serveri küljest.
- HLR server algkäivitatakse.
- HLR kokkuloetud tulemust võrreldakse moodustatud häältega.

Häälte kokkulugemine – HLR privaatvõtme kasutamine

Selleks hetkeks peab HLR serveris olema fail, milles on krüptitud, kuid enam mitte allkirjastatud e-hääled (nn "sisemised ümbrikud"). Faili autentsus ning terviklus peavad olema tagatud – faili transport HTS-ist HLR-i serverisse peab olema olnud protseduuriliselt korrektne ning faili peab olema võrreldud HTS väljundiga näiteks kontrollsumma abil.

- Turvamoodul ühendatakse HLR serveriga.
- Käivitatakse HLR rakendus, selle sisendiks on HTS-i e-häälte väljundfail.
- Võtmehaldurid autoriseerivad turvamooduli.
- HLR rakendus avab hääled ning arvutab välja e-hääletamise tulemuse.
- Turvamoodul viiakse tavalisse, autoriseerimata režiimi ning lahutatakse HLR serveri küljest.
- HLR server algkäivitatakse.
- Häälte fail kustutatakse HLR serverist.
- Kontrollitakse tulemuste faili, Log4 ja Log5 sisu.

Nagu näeme, on tulemuste kokkulugemine võtmete loomisega võrreldes suhteliselt lihtne protseduur. Nii see ongi: võtmehalduse juures on enamik keerukust seotud võtmete loomise ja levitamisega, mitte nende kasutamisega.

HLR privaatvõtme hävitamine

Kui hääletustulemused on kinnitatud, tuleb HLR privaatvõti hävitada.

Vastavad protseduurid on antud turvamooduli juhendis. Turvamooduli tootja vastutab, et turvamoodulis asunud võtmed hävivad taastamatult.

HLR avaliku võtme (sertifikaadi) integreerimine HR-iga

HLR avalik võti on HR osa. Riskid, mis kaasnevad sellega, et HR on vale avalik võti, on võtmehalduse riskide all kirjeldatud.

Pärast HR lõplikku valmimist, kuid enne Veebiserverisse asetamist peab eraldi üle kontrollima, kas HR sisaldab õiget HLR avalikku võtit. Selleks võib kasutada ülalkirjeldatud protseduuri "HLR võtmepaari testimine".

4.5. Meetmete kokkuvõte

Võtame esitatud turvameetmed lühidalt kokku.

4.5.1. Tehnilised turvameetmed

Üldise turvalisuse tagamiseks soovitame kasutada ISKE turvatasemele H vastavaid meetmeid.

Läbipaistvuse tagamiseks peab süsteemi disain ja dokumentatsioon olema võimalikult avalik.

Kesksüsteem peab olema eraldiasuv, tsoneeritud võrgu, tulemüüri ja ründetuvastusega süsteem, mis ei sõltu eluliselt ühestki välisest andmeallikast peale hääletajate endi; siin pakutud kontseptsiooni muudatuste realiseerumisel ei ole ei valijate andmebaasi uuendamine

ega ajatemplite saamine enam aegkriitilised. Kõikide komponentide puhul on disainieesmärgiks lihtsus, omaduste piiramine ja funktsioonide lahusus. Kontrollitavus on eesmärk; logida ja salvestada tuleb kõike, mis ei ohusta antud häälte privaatsust; logimist tuleb eri serverites dubleerida; nii võrgu- kui rakendustasemel vigade ja rünnete monitoorimine on range soovitus.

Tarkvara ja haldustegevuse korrektsusele tuleb panna rohkem rõhku kui funktsionaalsusele ja võimsusele. Teenustõkestusrünnete vastu kaitse ei ole kuulu süsteemi funktsionaalsuse hulka, selliste rünnete tõrje tagatakse süsteemiväliste vahenditega.

Andmekadude ulatuse piiramine ja süsteemi kiire taastatavus on tänu andmete ja süsteemi väikesele mahule saavutatav üsna lihtsate abinõude abil. Nõudeks on ka süsteemi haldajate pidev kättesaadavus.

Andmete formaadid tuleb hoida lihtsatena, alati peab aga olema võimalus kontrollida süsteemis olevate või liikuvate andmete korrektsust. Eriti hoolikalt tuleb tervikluse kontrolli teha süsteemiväliste andmeallikate ja -saajate korral. Osa andmeid tuleb kontrollitaval viisil avalikustada (vt "Lisa 2 - andmekanalid süsteemi ja süsteemist välja"). Häälte krüptogrammid tuleb pärast valimistulemuste kinnitamist hävitada.

Hääletaja rakenduse omadused tulenevad tavalistest signeerimis-rakenduse nõuetest. Keerukaim on autonoomse kontrollteavituse vajadus – selleks peab rakendus kas serverist või iseendast saama omama lubatud kandidaatide andmed. Lisaks peab kandidaatide andmete näitamine toimima veebiservist sõltumatult, nii et veebiserver ei teaks, kelle andmeid vaadati.

Hääleedastusserveri / Veebiserveri kui avaliku ja seega kõige rünnatavama serveri turvalisusele tuleb pöörata erilist rõhku. Võtmesõnad on taas lihtsus, omaduste piiramine ja konservatiivne programmeerimine. Erinõueteks on vajadus siduda SSL-kasutaja ja hääle andja isik ning vajadus piirata kandidaatide kohta näidatavat infot. HES peab andma kasutaja rakendusele tagasisidet saadetud hääle arvestatuse kohta.

Hääletalletamisserver kui kõige keerukam komponent jaguneb sisuliselt kaheks: häälte andmise ajal toimiv andmehõive-mootor ning hilisem sorteerija/tühistaja. Need funktsioonid tasub võimaluse piires lahutada. Lisaks asub siin andmebaas, mille turvamiseks tuleb kasutada tavalisi meetmeid (juurdepääsupiirangud, adekvaatsed õigused, logimine jne).

HTS andmebaasirakenduste vead võivad anda juurdepääsu andmetele ja piirangute eiramise, seetõttu on HTS rakenduste korrektsus ühtlasi ka turvanõue.

Häälelugemisrakendus, milles paiknevad hääled lahtisel kujul ja mis hääletuse tulemuse tegelikult kokku arvutab, on kaitstud põhiliselt füüsilise turvalisusega ning võtmehaldusega. Lisaks mõnedele HLR tehnilise kaitse meetmetele soovitame HLR väljundi – hääletustulemuse – otse HLR-ist välja trükkida.

Lugesime üles *Auditisüsteemi* kogutavad andmed ja panime kirja mõned vajalikud kontroll-tegevused, mida kindlasti sooritama peaks. Lisaks rõhutame, et auditisüsteemi andmeid peab kaitsma samamoodi nagu töötavates serverites olevaid andmeid.

Võtmehaldus on esmapilgul harjumatult keerukas teema, mis seob omavahel organisatoorse turbe ja krüptograafia ning mille kirjeldamisele tuleb seetõttu keskmisest enam tähelepanu pöörata. Analüüs pakub välja turvamoodulitel põhineva võtmehaldusskeemi, loeb üles võtmehaldusega seotud protseduurid ning nende käigus tehtavad tegevused.

4.5.2. Organisatsioonilised turvameetmed

Kõige tähtsam organisatsiooniline meede on e-hääletamise protsesside *täitjate ja vastutajate määramine*. Seejuures tuleb järgida *rollijaotuse põhimõtet* ning jagada vastutus osalistele kooskõlas tava-hääletuse rollidega ning riigi infosüsteemide halduse tavadega.

Peavad olema määratud reeglid *eriolukordade lahendamiseks*, *teavituseks* ning *probleemide eskaleerumise puhuks*.

Tuleb analüüsida e-hääletamise ja tava-hääletuse töövoogu ning tagada, et nad üksteist täiendaksid, mitte ei segaks. Protseduurid tuleb eelnevalt kirjeldada ja testida, samas tuleb vältida protsesside üleformaliseerimise ohtu.

E-hääletamisega peab kaasnema *valijate teavitamine e-hääletamise turvalisusest* rõhuga veebilehe autentsuse kontrollil ning omaenda arvuti turvalisuse hoidmisel.

Tuleb tagada *pidev turvakontroll* e-hääletamise süsteemi arenduse ja juurutamise üle.

Enne igat e-hääletamist tuleb läbi viia *hääletuseelne turvalisuse eksperthinnang*.

Enne valimistulemuste kinnitamist tuleb läbi viia *valimisaegne vaheaudit*.

Soovitame läbi viia e-häälte *kontroll-ülelugemise*.

Pärast valimistulemuste kinnitamist tuleb läbi viia *valimisjärgne protsessiaudit*.

Oluliste väliste osapooltega tuleb sõlmida *teenuse kvaliteedi lepingud*.

Hääletuse ajal peab töötama *hääletajate tehnilise toe infoliin*.

4.6. Aktsepteerimist vajavad riskid

4.6.1. Vajadus kulutada ressursse organisatoorse ja tehnilise turvalisuse peale

Turvalisus on kulu. Ta vastandub efektiivsusele, mugavusele ja lihtsusele; operatsioone tuleb dubleerida, tegevustele lisada jälgimine ja järelkontrollimine, arendusele turvaanalüüs, haldusele audit. See kõik kulutab tööjõudu ja raha.

Tuleb ette aktsepteerida, et need ressursid leitakse.

4.6.2. Hääletajate arvutite võimalik ebaturvalisus

Arvame, et teatud hulga hääletaja arvutite võimalik ebaturvalisus on e-hääletamise seisukohalt aktsepteeritav risk. Põhiline argument on siin asjaolu, et osapooltel, kellel oleks suure arvu hääletajate arvutite ründamise jaoks vajalik teadmus, ressurss ja juurdepääs, ei ole selleks motivatsiooni; ning poliitilised jõud, kellel on motivatsioon, ei saa võtta ründamisega seotud riske.

Arvuti teel oma äri- ja rahaasju ajavad inimesed on iga päev palju ”suuremas ohus" kui e-hääletamise ajal.

AIP-dega seotud riskide maandamiseks ei ole häid meetodeid ning need riskid tuleb lihtsalt aksepteerida.

4.6.3. Vajadus usaldada Kesksüsteemi arvuteid

Tuleb aktsepteerida asjaolu, et Kesksüsteemi arvutite süsteemse kihi komponente lihtsalt tuleb usaldada. Riski vähendab nende komponentide hankimine usaldusväärsetest allikatest.

4.6.4. Võimatus toetada kõiki valijaid

Tuleb aktsepteerida fakti, et e-hääletada saavad vaid levinumate personaalarvutite kasutajad. HR suudetakse hetkel arendada Windows, Linux ja MacOSX platvormidele, kuid mitte kõigile võimalikele versioonidele ning operatsioonisüsteemidele. Lisaks seab omad piirangud ka ID-kaardi baastarkvara toetatud platvormide nimekiri.

4.6.5. Riskide kontsentreerumine ja negatiivse meediakajastuse võimalus

Tuleb aktsepteerida riskide kontsentreerumist. Inim-protseduuride sagedaste pisivigade asemel tekivad tehnilises süsteemis harvad, kuid ulatuslikud ja kardetavasti kõrge meediaväärtusega vead.

4.6.6. Protsesside formaliseerumisega kaasnevad riskid

Füüsilise maailma reeglid on alati "pehmed", kuna inimestevahelisi suhteid saab igal erijuhul muuta. Infosüsteemidesse valatuna muutuvad reeglid aga rangeteks, enam neid eirata ega "nurki lõigata" ei saa.

Tulemusena võivad liigformaalsed protseduurid hakata tööd takistama nii, et seda ei tehta enam üldse, või kaovad ära mõned siiani toiminud ja sisuliselt mõistlikud erandite tegemise viisid.

5. ÜLDHINNANG KONTSEPTSIOONILE

Vastavus valimistele esitatavatele nõuetele

"Nõuete" peatükis kirjeldasime vastuolusid valimistele esitatavate nõuete vahel ning ütlesime, et nende vahel tuleb leida kompromiss, kus kõik põhilised nõuded on täidetud ning seejuures võetud riskid on poliitilisel tasandil aktsepteeritud.

Arvestades praeguseid riske ning infoturbealast olukorda maailmas, leiame, et e-valimiste lahendus on jätkuvalt turvaline ning maandab need riskid mõistlikult.

Toome siin ära lahenduse vastavuse peatükis 2.2, "Esitatavad nõuded" toodud nõuetele.

Nõue	Tagamise viis
Hääletajate autoriseeritus ja autenditus	Tagatud süsteemi disainiga. ID-kaart või Mobiil-ID on paberdokumendi näitamisest kindlasti tugevam autentimis-viis.
"Üks isik – üks hääl"	Tagatud süsteemi disainiga.
Häälte võltsimise keeld	Tagatud süsteemi disaini ja auditeerimisega. Digitaalallkirja võltsimine on võimatu, muud vead tuvastab vaheaudit.
Hääletuse ühetaolisus	Hinnang sellele, kas arvuti abil hääletamise võimaluse olemasolu rikub ühetaolisust või parandab seda, jääb meie analüüsi ulatusest välja.
Elektroonilise ülehääletuse võimalus	Tagatud süsteemi disainiga.
Tavahääletamise ülimuslikkus	Tagatud seadustega ja valimiste üldise töökorraldusega.
Hääle tühistatavus valija poolt	Ei ole nõue, kuid kaudselt tagatakse tavalisel teel ülehääletamise võimalusega.
Tühja hääle andmise võimalus	Ei ole nõue, ei tagata.
Hääle salajasus	Tagatakse tugeva krüptograafia ja võtmehaldusega.
Hääletamise fakti privaatsus	Tagatakse pehmelt – võrguühenduste jälgimine nende pakkujate poolt on teoreetiliselt võimalik.
Hääletuse tõestamatus	Tagatud HES / HTS rakenduse omadustega ning tavalisel teel ülehääletamise võimalusega.
Hääletussüsteemi töökindlus	Skeem on maksimaalselt lihtne ja modulaarne. Tehniline töökindlus ei ole probleem, tarkvara tõrkeid tuleb vältida testimisega.
Läbipaistvus	Tagatud disaini lihtsusega, süsteemi põhimõtete avalik-kusega ning rakenduste lähtekoodi kontrollitavusega
Auditeeritavus	Tagatud süsteemi disainiga. Tehniline realisatsioon on loodud logimise, auditisüsteemi ja auditirakenduse kaudu.
Hääle arvestamise kontrol-litavus	Tagatud hääletaja tagasiside võimaluse ja auditi-rakendusega.
Üleloetavuse korratavus	Tagatud süsteemi disainiga.

Süsteemi arhitektuur ja lahenduse lihtsus

Turvalisuse esimeseks nõudeks on analüüsitava süsteemi või protsessi lihtsus. Keerukas, suure hulga rakenduste ja nendevaheliste seostega hajussüsteem infosüsteem sisaldab alati rohkem vigu kui lihtne ja hõlmatav lahendus.

Leiame, et süsteemi arhitektuur on mõistlik ning just parasjagu modulaarne. Analüüsi käigus pakuti välja mitmeid võimalusi seda muuta, kuid diskussiooni käigus otsustati nad kõik kõrvale jätta või kasutada neid ainult kui analüüsi kergendavat abstraktsiooni.

Rõhutame, et analüüs on tehtud eeldusel, et e-hääletamise infosüsteem on muust valimiste infosüsteemist eraldatud ning kogu e-hääletamise süsteemi suhtlus välismaailmaga toimub vaid läbi väga piiratud liideste. Kui tekivad kontrollimatud infokanalid e-hääletamise süsteemi ja muu maailma vahel (näiteks kasutatakse kulude kokkuhoiu mõttes tava-valimiste rakendusega ühiseid servereid), siis on kontrollimatud ka sellega seotud turvaohud.

Realiseeritavus

E-hääletamise tehniline lahendus on Eestis kohaliku IT teadmise abil realiseeritud ning seda on praktikas kasutatud kokku viiel korral. Seega on e-hääletamine praeguseks muutunud juba igapäevaseks reaalsuses, olles mitte enam lihtsalt kontseptsiooniks.

Ühilduvus Euroopa Liidu soovitustega

Kontseptsioon on heas kooskõlas Euroopa Liidu tulevaste e-hääletamise nõuetega ehk IP1-S-EE töögrupi soovitusliku dokumendiga [IP1-S-EE].

6. KOKKUVÕTE

Elektroonilise hääletamise vastuolulise ülesande lahendamine oli 2003. aastal huvitav väljakutse. Praeguseks saab öelda, et väljakutse on lahendatud ning praktikas realiseeritud.

Olemasolev lahendus on üsna lihtne. Matemaatiliselt turvalisem, kuid realisatsioonilt keerukam skeem muudab ka lahenduse keerukamaks, suurendab komponentide ja nendevaheliste seoste arvu ning lõppkokkuvõtteks vähendab turvalisust. Ilmselt on valikus hääletusskeemi teoreetilise turvalisuse ja selle realisatsiooni keerukuse vahel olemas optimum, millele vastav tehniline lahendus annab parima kompromissi esitatud nõuete vahel.

Eesti hääletusskeemi tugevateks külgedeks on:
- hoomatavus ja sarnasus tava-hääletusega;
- maksimaalne Eestis olemasoleva digiallkirjalahenduse (ID-kaart, DigiID, Mobiil-ID) ärakasutamine;
- ainult lihtsate krüptoalgoritmide kasutamine,

ning mis kõige tähtsam
- see on Eestis kohapealse IT-teadmuse abil tehtav.

Kompromissi teiseks pooleks ehk skeemi põhimõtteliselt nõrgaks kohaks on aga vajadus usaldada keskservereid ja valijate arvuteid.

Kas selline kompromiss on mõistlik?

Meie arvates – jah.

Usume, et kirjeldatud hääletusskeemi riskid on maandatud sedaviisi, et ohtude realiseerumise võimalus või tekkiv kahju on vastuvõetavalt väike. Võib öelda, et pannes süsteemi eri osad üksteist umbusaldama ja monitoorima ning lisades vajalikesse kohtadesse inimese-poolse kontrolli, oleme saavutanud piisava turvalisusega e-hääletamise süsteemi.

Muidugi tuleb tehnilistele vahenditele (krüptograafia, ründetuvastus, andmete topeltkontrollid jne) kasutada ka organisatsioonilisi meetmeid: tööülesannete ja vastutuse jagamine, formaalsed protseduurid, riskide teadvustamine ja juhtimine VVK poolt, väljamõeldud tegevusplaanid eriolukordade lahendamiseks, sõltumatu audit.

Usume, et loodud e-hääletamise mehhanism, mille turvalisus on tavalise, paberil hääletamise omast kõrgem. See vajab ka tulevikus läbimõeldud tehnilist lahendust, hoolikat arendustööd ning – mis kõige tähtsam – vastutustundlikku kasutamist, aga eks seda nõuab iga sellise kriitilisusega süsteem.

7. LISA 1 - SÜSTEEMIS TÖÖDELDAVAD ANDMED

Loeme üles e-hääletamise käigus töödeldavad andmed.

Muidugi on süsteemis veel hulk sekundaarset infot, mis siin ei kajastu: kasutajate paroolid, rakenduste lähtekood ja süsteemi dokumentatsioon, võtmehaldurite kiipkaardid jne.

'Asukoht' tähendab allolevas tabelis seda, et need andmed on süsteemi sellele komponendile mingil hetkel kättesaadavad. 'A' tähendab hääletaja arvutit, 'audit' auditisüsteemi, 'paber' paberkujul väljastatavaid või saadavaid andmeid. Internet ei ole komponent, kuna andmed liiguvad krüpteeritult ning ei ole sidekanali poolt loetavad.

Andmed	**A**	**HES**	**HTS**	**HLR**	**audit**	**paber**
Sisendandmed						
valijate nimekiri		x	x			
kandidaatide nimekiri ja avalik lisainfo	x	x		x		
HR	x	x				
hääletaja / digitaalallkirja andja isikuandmed	x	x	x		x	
hääletaja ID-kaardi PIN-kood	x					
Hääletuse protsesside käigus tekkivad andmed						
HLR salajane võti				x[1]		
HLR avalik võti	x	x		x		x
signeeritud, krüpteeritud hääled	x	x	x			
krüpteeritud, signeerimata hääled	x	x	x	x		
digitaalallkirjad	x	x	x		x	
krüpteerimata hääled	x			x		
hääle vastuvõetuse kinnitused	x	x	x			
hääletaja hääletatuse staatus	x	x	x			
e-hääletanute nimekirjad jaoskondadele			x		x	x
komisjonide tühistusavaldused			x		x	x
VVK tühistamise ennistamisavaldused			x		x	x
hääletustulemus				x	x	x
Logid						
LogWeb - veebiserveri access-log		x			x	
Rakenduste tehnilised vealogid		x	x	x	x	
Log1 - antud hääled		x			x	
Log2 - sorteerimisel tühistatud hääled			x		x	
Log3 - arvestatud, lugemisele saadetud hääled			x		x	
Log4 - kokkulugemisel vigaseks osutunud hääled				x	x	
Log5 - hääletustulemuses arvestatud hääled				x	x	

1) HLR salajane võti asub tegelikult turvamoodulis ning on rakendusele avatud vaid kasutamiseks, HLR serveri kaudu seda kopeerida ei saa.

8. LISA 2 - ANDMEKANALID SÜSTEEMI JA SÜSTEEMIST VÄLJA

Sisendandmed

kandidaatide nimekiri	VVK	→ HTS
valijate nimekiri	Andmevara	→ HTS
valijate nimekirja uuendused	Andmevara	→ HTS
tühistused ja ennistused	VVK	→ HTS
hääl	hääletaja	→ HR

Väljundandmed

tagasiside	HR	→ hääletaja
hääletaja hääletatuse staatus	HR	→ hääletaja
e-hääletanute nimekirjad	HTS	→ valimisjaoskonnad
e-hääletamise tulemused	HLR	→ VVK
monitooringu tulemused	jälgimisrakendus	→ VVK, süsteemi haldajad
logid, auditi tulemused	auditisüsteem	→ VVK, arhiiv
arhiveeritud digiallkirjad	HTS	→ arhiiv
e-hääled	HTS, HLR	→ hävitamisele

Avalikustatavad andmed

Järgnevad andmed peavad olema avalikud ja tagatud autentsuse ning terviklusega:

kandidaatide nimekiri ja lisainfo
e-hääletamise veebiserveri URL (aadress)
HR, selle signatuur või kontrollsumma ja kontrollimise viis
veebiserveri avalik võti, selle kontrollsumma ja kontrollimise viis
HLR avalik võti, selle kontrollsumma ja kontrollimise viis

VVK poolt määratud tingimustel peavad olema soovijatele kättesaadavad:

HR – HES vaheline suhtlusprotokoll
süsteemi tehniline dokumentatsioon
süsteemi komponentide lähtekood

9. Lisa 3 - tehniline riskianalüüs

Formaalselt võib öelda, et tervikluse ja salajasuse riskid on defineeritud kõikide süsteemis olevate andmete tervikluse ja salajasusega üle süsteemi kõikide komponentide. Samuti on käideldavuse riskid lihtsalt ülesloetavad iga komponendi, rakenduse ja andmesalvesti töökindluse / töökiiruse kaupa. Järgneva riskianalüüsi eesmärk ei ole aga mitte kõikide selliste variantide loetlemine – selleks piisaks lihtsast süsteemi andmete ja komponentide risttabelist, tulemusel ei oleks aga suuremat praktilist väärtust –, vaid olulisematele kohtadele tähelepanu pööramine.

9.1. Riskide klassifikatsioon

Riske on võimalik klassifitseerida ja esitada mitmel moel: ründe sooritaja järgi (rollikeskne vaade); mõjutatava süsteemi osa järgi (arhitektuurne vaade); tekkeviisi järgi (viga, rünne, keskkonna mõju); turvalisust kaotava andmehulga järgi (andmekeskne vaade); ajalises järjestuses (protsessikeskne vaade); kriitilisuse järgi; jne.

Meie riskide kaardistus põhineb süsteemile esitatud nõuetel.

Võib ka öelda, et me jagame riskid klassidesse rünnatava turvaatribuudi kaupa:
- *Tervikluse riskid* ohustavad hääletustulemuse korrektsust.
- *Salajasuse riskid* ohustavad hääletuse salajasust.
- *Käideldavuse riskid* ohustavad süsteemi töökindlust ja kasutatavust.
- *Usaldusväärsuse riskid* seavad kahtluse alla e-hääletamise protsessi korrektsuse.
- Lisaks toome eraldi välja *võtmehalduse riskid*, mis moodustavad ühe loogilise terviku.

Kõik riskihinnangud on kvalitatiivsed.

9.2. Tervikluse riskid

9.2.1. Diskrimineerimisvead

Diskrimineerimisvead on vead, kus e-hääletamise süsteem käitub osade hääletajate suhtes teisiti kui teiste suhtes. Võib ka öelda, et tegemist on valikulise käideldavusega, aga kuna ta ohustab hääletuse ühetaolisuse nõuet, siis on ta korrektsuse (tervikluse) risk.

Sellist sorti viga võib esineda süsteemi ükskõik millises komponendis. Diskrimineerimine võib olla juhuslik (sel puhul on ta lihtsalt kvaliteedi viga) või süsteemi meelega sisse viidud.

Võimalikud näited:
- Veebiserver ei luba ühendusi mõnest maakonnast, näiteks Virumaalt.
- Kesksüsteem HES logib valesti mõnede häälte räsisid, hilisem kontroll tühistab need hääled.
- Kesksüsteem ei suuda kontrollida digiallkirja, mille andja nimes on ‘õ’, ja lükkab sellised hääled tagasi.
- Hääletaja rakendus ei tööta venekeelse Windowsiga, mitte-eestlased ei saa hääletada.
- Hääletaja rakendus ei tööta Kunstiinstituudi Mac-tüüpi arvutites, kunstiüliõpilased ei saa hääletada.

Diskrimineerimisrisk ei ole iseenesest väga suur oht, kuna valimiste korraldus arvestab sellega ning võimaldab kõigil valijatel hääletada ka tavalisel teel. Samas võib diskrimineerimine endaga kaasa tuua mitmesuguseid usaldusväärsuse riske.

9.2.2. Interneti kasutusega seotud riskid

Normaalset andmevahetust Kesksüsteemi ja hääletaja brauseri või HR vahel Interneti kaudu rünnata ei saa. Küll võib aga valija sattuda (või suunatud saada) sellisele veebilehele, mis kas imiteerib e-hääletamise lehte ja petab valijat, või mis ründab valija arvutit, saades seeläbi kontrolli ka e-hääletamise protsessi üle.

Hääletaja suunamine võltsitud veebilehele
Hääletaja võib valele lehele sattuda:
- vale teavituse tõttu,
- sisestusvea tõttu (sisestades aadressiks nt. `ww.wvvk.ee`),
- tehnilistel põhjustel (DNS vead/ründed, hääletaja arvuti vale konfiguratsioon, ...).

Viimase aasta edukad ründed interneti-pankade vastu on toimunud just veebilehtede võltsimise ja massilise valeteavituse kaudu, üks selline (vaid häkkerite keelelise küündimatuse tõttu ebaõnnestunud) rünne on toimunud ka Eestis.

Vahendusründed veebiserveri ja HR vahel
Vahendusründed on erijuht, mille korral võlts-veebileht vahendab kogu HR ja veebiserveri vahelist suhtlust. Sisuliselt on sidekanali vahendusründed võrdsed veebiserveri rünnetega: keegi loob mingi võrguosa jaoks võlts-veebiserveri, mille kaudu siis on võimalik anda hääletajale ette vale rakendus, saada teada tema tehtud valik jne.

Üldjuhul ei ole vahendusrünnete vastu head rohtu olemas. Klassikaline meetod – veebiserveri autentimine serveri sertifikaadi abil – nõuab kasutajate-poolset teadlikkust ja hoolikust. Õnneks on Eesti Vabariik siin ülejäänud maailma ees eelisseisus, kuna tänu kiipkaartide olemasolule saame me veebiserveris nõuda ka kliendi autentimist, see aga välistab vahendusründed täiesti. Mobiil-ID puhul ei saa SSL kanali mõlemapoolset autentimist samal tasemel teha, kuid Mobiil-ID abil hääletajad ei ole praegusel hetkel enamuses.

Kasutaja arvuti ründamine ja kontrolli alla võtmine on teine Interneti kasutamisega paratamatult kaasnev risk. Viimaste kuude jooksul avalikustatud turvavead Microsofti tarkvaras (nii operatsioonisüsteemides kui brauseris) on teinud selle veel teravamaks. Kuna hääletuse hetkel on arvutis kättesaadav ka hääletaja ID-kaart, võib e-hääletamise hetk olla ründamiseks kõige huvipakkuvam.

Internet saab hääletusprotsessi ühetaolist rikkuda veel *diskrimineerimise* ehk hääletajate valikulise takistamise kaudu. On näiteks võimalik, et just e-hääletamise päevadel on Ida-Virumaa võrguühendus katki.

9.2.3. Veebiserver / HES

Veebiserveri sisu (nimekirjad, HR programmikood, staatiline info) on e-hääletamise algushetkel korrektsed. Need andmed on sarnased valimisjaoskonnas olevate nimekirjade, valimissedelite ja tegevusjuhistega ning nende terviklus tuleb enne valimiste algust üle kontrollida.

Seda sisu võidakse aga volitamatult muuta – kas serverisse sisse murdes või serveri tehnilise administraatori poolt. Kuna seeläbi muutuvad valeks hääletusprotsessi kõige olulisemad sisendandmed, siis muutub paratamatult valeks hääletusprotsessi tulemus ehk hääl.

Hääletaja rakenduse kompromiteerumine
Veebiserveris asuva hääletajate poolt alla laetava hääletamisrakenduse. Selle volitamatu muutmise tulemus on e-hääletamise turvalisuse massiline kadu. Võimalikud on häälte võltsimine, hääle ja hääletaja privaatsuse kadu, osade kandidaatide valimise võimatus jne.

Kandidaatide nimekirja volitamatu muutmine
Veebiserveris asub hääletajale näidatav kandidaatide nimekiri. Kui see ei ole korrektne, ei saa seda olla ka antud hääl. Andmete volitamatul muutmisel (kandidaatide eemaldamine, lisamine, omavahel vahetamine, ringkondade info muutmine jne) muutub kõikide muudetud nimekirja saanud hääletajate hääl potentsiaalselt valeks. Hääletaja ei saanud valida soovitud kandidaati, signeeris oma tahtest erineva valiku, vms.

Sama tulemuseni viib veebiserveri programmi selline muutmine, et hääletajale väljastatakse päringu peale vale nimekiri.

Veebiserveri staatilise sisu kompromiteerumine
Veebiserveris asub e-hääletamise jaoks vajalik staatiline teavitusinfo ("e-hääletamiseks klikka punasele nupule"). Selle info volitamatu muutmine (nt. mõne partei reklaami lisamine) tekitab probleeme, kuid reaalset ohtu hääletustulemuse terviklusele siin ilmselt ei ole.

Kandidaatide andmete ühetaolise kuvamise vead
Süsteem peab kuvama kõikide kandidaatide või nimekirjade andmeid sarnaselt ja tagama, et rakenduse visuaalne pool ei mõjutaks valikuprotsessi. Kõige teravamaks probleemiks on ilmselt ekraani "ääre taha" jäävad kandidaadid. Raskusi võib tekitada ka eesti tähestiku tähtede kuvamine mõnede hääletajate arvutites. Jällegi võimendab riski asjaolu, et hääletajale pilti näitav keskkond, tema arvuti ja brauser, on ennustamatud.

Andmeid muutuva suurusega ekraanile kuvades on väga lihtne luua ka nn "Florida liblika" efekt, kus kandidaadid ja valikukastid ei ole kohakuti ja segaduses hääletajad valivad teise kandidaadi kui tegelikult soovitud.

Klassikalised veebirakenduse ja veebiserveri vead
Nimekirjas viimased on nad seetõttu, et nad on tuntud ja tüüpilised, mitte seetõttu, et nad oleksid ohutud. *Cross-site scripting*, *session fixation attacks*, sisendandmete kontrollimise vead, *code/SQL injection*, konfiguratsioonandmete väljastamine läbi veateadete jne – veebirakendustel on suur hulk vigu, mida alalõpmata uuesti ja uuesti tehakse. Vastava nimekirja leiab näiteks [OWASP] lehelt. Nende sageduse põhjus on lihtne – selliste vigade vältimiseks on programmeerimisel vaja tüütuseni minevat hoolikust, aga see on meie kiirustavas e-maailmas harv külaline.

Ka veebiserverit ennast on võimalik sajal viisil valesti hallata nii, et tema sisu oleks rünnatav. Näiteks võib ründaja saada enda valdusesse veebiserveri HTTPS sertifikaadi salajase võtme ning seeläbi teha palju raskemini tuvastatavaid vahendusründeid.

9.2.4. Hääletaja arvuti, veebibrauser, HR

Kandidaatide nimekirja kompromiteerumine
Kui hääletaja poolt nähtav kandidaatide nimekiri ei ole korrektne, ei saa korrektne olla ka tema poolt antud hääl. Kui vahetada nimekirjas ära kahe poliitiku numbrid või eemaldada sealt mõni kanditaat hoopiski, on hääletustulemus selgelt vale.

Hääletaja rakenduse kompromiteerumine
Rakenduse kompromiteerumine muudab hääle andmise protsessi, tagajärjed ükskõik millised (hääle võltsimine, hääle salajasuse kadu, osade kandidaatide valimise võimatus jne).

Milline on vahe nimekirja (andmete) ja rakenduse ründamise vahel? Andmete ründamine on enamasti oluliselt lihtsam. Veebibrauseris HTML-lehena nähtavad andmed on brauseri turvaauke ära kasutades väga lihtsalt muudetavad, selleks ei pea saama täiskontrolli hääletaja arvuti üle. Rakenduse (või rakenduse-siseste vahenditega kuvatava info) modifitseerimine on vähemalt suurusjärgu võrra keerukam.

Hääletaja rakenduses oleva HLR avaliku võtme asendamine
See on tegelikult HR kompromiteerumise erijuht, mis on kirjeldatud võtmehalduse riskide juures.

Hääletaja rakenduse funktsionaalsed vead
Rakendus võib sisaldada nii disainivigu, tahtmatuid vigu kui tahtlikke trooja hobuse laadseid omadusi. Näiteks võib HR

- asendada hääletaja tehtud valiku millegi muuga;
- mitte kuvada teatud kandidaatide nimesid;
- mingitel tingimustel lihtsalt "mitte töötada".

Tegelikult on kindel, et HR jaoks "toetatud" arvuti/OS/brauseri kombinatsioonid ei kata kõiki hääletajaid. Funktsionaalsete vigade esinemise tõenäosus on seega ligi 100% ning küsimus on vaid selles, kas neid esineb piisavalt vähe ning kas nad rikuvad ainult valimiste ühetaolisust (ei toetata venekeelseid Windowsi versioone) või ka otseselt tulemuse terviklust (ei kuvata teatud partei kandidaate; muudetakse häält).

Eksitavate andmete kasutamine hääletaja poolt
See, et hääletaja hääletab oma tava-keskkonnast lahkumata, tekitab juurde valereklaami riski. Sel puhul saadetakse valijale kuidagi (e-postiga, tavapostiga, ...) eksitav reklaam – näiteks saadetakse kiri "vali P.P, number 666!", kuid tegelikult on kandidaatide nimekirjas number 666 all hoopis T.T.

Tava-valimistel saab hääletaja valimisjaoskonnas defineeritult õiged andmed ja seega ei sõltu ta muust reklaamist sellisel kombel. E-hääletamisel on see risk suurem.

Tahtlik mittekorrektse hääle saatmine hääletaja poolt
HR töötab hääletaja arvutis ning on seega hääletaja kontrolli all. See tähendab, et hääletaja võib – piisava tehnilise teadmise olemasolul – selle käitumist oma suva järgi muuta. Põhimõtteliselt on võimalik, et hääletaja (või keegi teine) kirjutab ametliku rakenduse asemele teise, alternatiivse rakenduse. Iseenesest ei ole sellest midagi halba, nii nagu ei ole midagi halba sellest, et inimesed kasutavad erinevaid veebibrausereid – tähtis on vaid, et toetatakse samu standardeid (HTTP, HTML, CSS, ...).

See tähendab aga, et me ei tohi teha mingeid eeldusi hääletaja poole HES-ile saadetava hääle korrektsuse osas. Hääl võib olla krüpteerimata või signeerimata; olla krüpteeritud vale võtmega või olla signeeritud mitte-ametliku sertifikaadiga; sisaldada valeandmeid (mitte kandidaadi numbrit, vaid näiteks tema nime, või siis poliitilist manifesti); olla tehniliselt valesti formaaditud või muul viisil mittekorrektne.

Jätkates analoogiat veebibrauseritega – ka HTTP päring on täiesti selle saatja kontrolli all ning selle sisu ega formaadi suhtes ei tohi teha mingeid eeldusi. Valed HTTP päised, HTML-vormide andmete mitteusaldamine, puhvri ületäitumised ning muud ründed on asjaolud, mida iga veebirakendus peab arvestama; e-hääletamise serveripoolne rakendus peab samamoodi umbusaldama saadetud hääle vormingut.

Hääle allkirjastamine kehtetu (tühistatud või peatatud) sertifikaadiga
On võimalik, et hääletaja signeerib hääle tühistatud sertifikaadiga (näiteks varastatud kaardiga) või tühistab sertifikaadi pärast hääle saatmist.

Üldised allkirjarakenduse riskid
Hääletaja rakendusel olemas kõik klassikalised allkirjarakenduse riskid, mis tulenevad asjaolust, et ta saab juurdepääsu hääletaja ID-kaardile. Näiteks võib rakendus lisaks signeerida häälele veel midagi muud, või siis hääletaja ID-kaardi PIN-koodi häkkerile meilida.

Kui muudel juhtudel saaks selliseid vigu osaliselt tuvastada serveripoolse tagasiside abil ("Signeerisite laenulepingu summas 1 miljon dollarit. Täname!"), siis hääle salajasuse nõue kaotab selle võimaluse – HES ei tohi valijale öelda, et "valisite kandidaadi nr. 666".

9.2.5. Sisevõrk

Võrk (või tulemüür) saab hääletustulemuste terviklust rikkuda *diskrimineerimise* kaudu hääli valikuliselt edastades.

Signeerimata häälte nimekirja muutmine
Kõige ohtlikum tervikluse risk on HTS-ist HLR-i transporditava signeerimata häälte nimekirja muutmine. Siin on võimalik hääli piiramatus ulatuses juurde lisada ning autentseid hääli kustutada.

9.2.6. HTS

HTS kui funktsionaalselt kõige keerukam komponent omab kõige paremat kontrolli antud häälte üle, seega ka kõige rohkem võimalusi nendega manipuleerida. HTS võib hääli kustutada ja juurde lisada, alusetult tühistada, modifitseerida jne.

HTS-is saavad kokku kõik e-hääletamise süsteemi sisendandmed: valijate ja kandidaatide nimekiri, antud hääled koos staatusega (kehtiv, vigane, koheselt tühistatud), tühistus- ja ennistusavaldused. Neist tekib lõpuks HLR-ile edastatav "anonüümsete" häälte fail.

HTS asuvate sisendandmete vead
On selge, et iga andmeallika vead mõjutavad otseselt tulemuse terviklust. Kui kandidaatide nimekirjas on kasvõi üheks päevaks üks kandidaat puudu, siis ei olnud hääletajatel tol päeval võimalik selle kandidaadi poolt hääletada. Kui valijate nimekirjas on keegi puudu või üle, siis ta kas ei saa legaalne valija hääletada või saab hääletada isik, kes ei ole valija.

HTS rakenduste funktsionaalsed vead
HTS rakenduste (hääle vastuvõtmine ning sellel tehtavad kontrollid, häälte tühistamine ja ennistamine, sorteerimine) vead võivad hääletustulemuse terviklust mõjustada nii mitmel viisil, et ei ole isegi vajadust neid üles lugema hakata. Kui andmete vigasus on tõenäoliselt väikese ulatusega (ei ole tõenäoline, et valijate nimekirjast puuduvad pooled valijad), siis rakenduse vigade ulatus ja tagajärjed on piiramatud.

Lahenduseks on HTS tegevuse mitmekordne kontrollimine; selleks tuleb kasutada HES logisid, auditirakendust jne.

Digitaalallkirjade kontrollimise vead
HTS poolt kasutatav hääle digiallkirja kontrollimise algoritm peab olema absoluutselt veatu, muidu saab võimalikuks häälte võltsimine suures mahus (valede allkirjade aktsepteerimisel) või valimiste ühetaolisuse rikkumine (tegelikult korrektsete allkirjade tagasilükkamine).

Näiteks võib HTS vastu võtta hääled, mis on signeeritud ükskõik millise sertifikaadiga, mille vorm (väljaandja ja subjekti *Distinguished Name*) on ametliku allkirjasertifikaadiga sarnane.

See on üks HTS rakenduse funktsionaalsete vigade liik.

HTS kompromiteerumine
HTS kompromiteerimine kas ründe või selle administraatori(te) pahatahtliku tegevuse läbi võib hääletustulemusi muuta sarnaselt HTS rakenduse vigadega.

Samas on HTS tehniline turvalisus Veebiserveriga võrreldes parem, kuna ta ei ole avalikust võrgust kättesaadav.

9.2.7. HLR

Häältelugemisrakendus on see e-hääletamise süsteemi komponent, mis hääli loeb ja tegeliku tulemuse väljastab. Seetõttu on paratamatu, et iga *HLR rakenduse funktsionaalne viga* on otseselt e-hääletamise tulemuste tervikluse viga.

9.2.8. Kehtivuskinnituse teenus

Kehtivuskinnituse teenus ei suuda valimiste korrektsust mõjutada muul viisil kui *diskrimineerimise* kaudu ning ka sellisel juhul ei saa ta kehtivuskinnitusest keelduda näiteks hääle sisu alusel, kuna teenuseosutaja näeb vaid digitaalallkirja räsi, millest ei saa tuletada mitte mingit informatsiooni ei hääle ega selle andja kohta.

9.2.9. Auditisüsteem ja auditirakendus

See kontrolliva funktsiooniga alamsüsteem tulemuse terviklust mõjutada ei suuda.

9.3. Privaatsuse riskid

9.3.1. Veebiserver / HES

Hääletamise fakti privaatsuse rikkumine
Veebiserveris asuv juurdepääsulogi sisaldab rakenduse laadimise aegu, IP-sid ja brauseri versioone. Kui kasutatakse autentimist ID-kaardiga, siis teab Veebiserver automaatselt ka hääletaja isikukoodi ja nime. Kui logitakse isikukoodi alusel ringkonnakoodi küsimist, siis jääb veebiserveri logisse ka isikukoodi ja ringkonna seos. Sarnast infot sisaldab ka HES logi.

Kasutaja arvuti rünnete ajastamine
Veebiserveri või kasutaja võrguühenduse jälgimine võimaldab rünnata hääletaja arvutit reaalajas, hääletamise hetkel.

Häälte salajasuse rikkumine
On võimalik, et Veebiserver saab teada hääletaja valiku. See võib juhtuda näiteks siis, kui veebirakenduse disain on vigane ning kandidaadi valikul HR-is päritakse Veebiserverilt tema kohta mingit lisainfot (näiteks pilti).

9.3.2. Hääletaja arvuti, veebibrauser, HR

Hääle salajasuse rikkumine
Hääletamise fakti privaatsuse rikkumine
Hääletaja arvuti on esimene ja kõige tõenäolisem koht nii hääletaja tehtud valiku kui muude hääletaja andmete lekkimiseks. Lisaks eelpool kirjeldatud hääletaja arvuti turvaprobleemidele

hääletusprotsessi ajal jääb märk hääletamas käimisest (Veebiserveri poole pöördumisest) ka kasutaja veebibrauseri logisse.

9.3.3. Sidekanal (Internet) HR ja Kesksüsteemi vahel

Hääletamise fakti privaatsuse rikkumine
Liikluse jälgimine võimaldab tuvastada, millisest arvutist Kesksüsteemi poole pöördutakse.

See on võimalik ka siis, kui side HR ja Kesksüsteemi vahel on krüpteeritud. Fakti, et keegi esitab Veebiserverile päringu ja saab sellelt umbes HR pikkuse vastuse, on raske peita. Kui sellele järgneb suhtlus "hääl – HES kinnitus", siis on hääletamise fakt üsna ilmne.

9.3.4. HTS, sisevõrk

HTS ja Kesksüsteemi sidevõrgu kaudu võivad *lekkida sisuliselt kõik e-hääletamise süsteemis olevad andmed* peale tegelike antud häälte, mis on HTS-ile kättesaadavad vaid krüptituna.

Ka *häälte täieliku andmebaasi lekkimine* on kõige võimalikum just HTS-ist, kuna seal on see tervikuna olemas (teised komponendid vahendavad seda infot oma tööea jooksul). Oht on siin see, et hääle krüpteerimiseks kasutatav tehnika ei pruugi 30 aasta pärast enam toimida ning siis on andmebaasi omaniku võimuses kõikide häälte salajasuse rikkumine.

9.3.5. HLR

HLR sisaldab alates mingist hetkest hääletustulemust.

Kuna HLR teab nii iga krüptitud hääle väärtust kui selle hääle räsi, siis on võimalik selle kaudu *siduda hääle räsi ja antud hääle väärtus*. Hääle räsi kaudu saaks HTS-ist omakorda teada hääle andja.

Selleks peaks ründaja monitoorima HLR kasutatavat mälu või kasutama ära HLR enda vigu.

9.3.6. Kehtivuskinnituse või ajatembelduse teenus

Kehtivuskinnituse teenus kontrollib hääle andja sertifikaadi kehtivust, seega tekib temasse *nimekiri e-hääletanutest* ja häälte andmise kellaaegadest.

Kehtivuskinnituse või ajatembelduse teenuse serveri kaudu *võib lekkida e-hääletamise kasutusintensiivsuse informatsioon.*

9.3.7. Süsteemi väljund

E-hääletamise tulemuste piiratud salajasus

Iga ringkond võib iga kandidaadi jaoks teha tehte: e-hääletamisel antud häälte hulk võrdub lõplikust valimistulemusest lahutatud tavalisel teel antud hääled.

Seega – e-hääletamise tulemus ei ole saladus neile isikutele, kes näevad ringkondade tava-valimise teel antud häälte alusel koostatud valimisprotokolle. Vähese hääletajate arvu korral on see probleem, kuid komisjoni liikme korrumpteerumist ei saa lahendada tehniliste vahenditega.

9.3.8. Auditisüsteem ja auditirakendus

Logid on klassikaline andmete lekke koht. Auditisüsteemi sisaldab logisid, mis sisaldavad antud häälte informatsiooni ning suurt hulka tehnilist infot süsteemi toimimise kohta. Seda informatsiooni tuleb kaitsta sama hoolikalt kui HTS-is ja HES-is sisalduvaid andmeid.

9.4. Töökindluse riskid

Tavaliste süsteemide käideldavuse probleemid jagunevad umbes suhtes 4:2:1 halduse vigade, tarkvara vigade ning riistvara tehniliste tõrgete vahel. E-hääletamise süsteemis on halduse ja tarkvara vead ilmselt veel suurema osakaaluga, kuna süsteemi kasutusaeg on suhteliselt väike.

Seega on töökindluse probleemide tekitajaks eelkõige *haldustegevuse vead* ning *testimata tarkvara*, alles seejärel tulevad *riistvara tõrked* ning *vajalike süsteemiressursside vale planeerimine*.

Töökindluse rikkumisi on kõige lihtsam tuvastada, kuna töökindlusele esitatavad nõuded on kvantitatiivselt defineeritavad ning süsteemi vastavus nendele on mõõdetav.

9.4.1. Hääletaja rakendus, hääletaja arvuti, veebibrauser

Hääletaja arvuti ja selles töötava tarkvara töökindlus on hääletaja, mitte kesksüsteemi haldajate kontrolli all, seega ei käsitle käesolev analüüs neid e-hääletamise süsteemi riskidena.

Hääletaja rakenduse töökindlus on aga tõenäoliselt kogu e-hääletamise süsteemi valulaps. Kvaliteediprobleeme tekib pea kindlasti – ei ole kerge kirjutada rakendust, mis toimib ühetaoliselt kõikides Internetis kasutatavates kliendiarvutites.

9.4.2. Sidekanal (Internet) HR ja Kesksüsteemi vahel

Üldiselt on sidekanali käideldavuse probleemid hääletaja kanda, nii nagu valimisjaoskonda kohale tuleku raskused on tava-hääletaja mured.

Probleemiks võib osutada *HR suur maht*, mis ei võimalda aeglase Interneti-ühendusega hääletajatel seda alla laadida või mille käivitamine muudab kogu hääletusprotsessi liiga pikaks.

9.4.3. Veebiserver / HES, tulemüür, sisevõrk, HTS

Need komponendid osalevad hääletusprotsessis otseselt ning seega on nad süsteemi töökindluse seisukohalt kõige kriitilisemad. Nende mittetöötamine tingib e-hääletamise ebaõnnestumise.

Serverite ja sidevõrgu käideldavuse riskid ei ole e-hääletamise spetsiifilised. Nendega puutub kokku iga töökindlat infosüsteemi vajav organisatsioon ning nende maandamiseks on olemas klassikalised meetodid (riistvara ja võrguühenduste dubleerimine, andmete peegeldamine, monitooring jne).

Tarkvara tõrked – Küll aga on riski allikaks e-hääletamise jaoks loodud tarkvara, mille tõrked, veataluvus, juhuslikud programmeerimisvead ei pruugi olla korralikult läbi testitud.

Andmebaasi vead (tabelite ja indeksite riknemine) mõjutavad korraga kogu e-hääletamise süsteemi ning on raskesti parandatavad.

Kehtivuskinnituse / ajatembelduse teenuse mitte-kättesaadavuse risk on käsitletud peatükis 4, „Nõutavad ja soovitatavad turvameetmed“.

Teenustõkestusründed (“Denial of Service”)
Julgeme öelda, et kuni e-hääletamisel antud häälte arv ei ületa tavahäälte arvu, ei ole pahatahtlikud DoS ründed hääletamise läbiviimise jaoks tõsine risk. Risk ei kasva oluliselt ka sellisel juhul, kui kui e-hääletamine peaks muutuma valdavaks hääletamise viisiks.

Arvamuse aluseks on suur lahknevus ründaja riski ja motivatsiooni vahel. Me ei usu, et Eesti sees oleks osapooli, kes julgeks sooritada avalikku, kõrge profiiliga rünnet riigi infosüsteemide vastu. Eestist väljaspool võib motivatsioon ja julgus olemas olla, samas on välise ründe blokeerimine kergem.

E-hääletamise kestus – seitse päeva – on piisavalt pikk aeg selleks, et nii Eestist kui väljastpoolt tulevate rünnete vastu meetmed kasutusele võtta, seega on piiratud ka sellise ründe ajaline ulatus.

Hääletaja / HR vigade mõju kesksüsteemile
Lihtne hääletaja või HR poolne viga, näiteks ühe hääle saatmine sada korda järjest, võib kogu Kesksüsteemi üle koormata.

9.4.4. HLR

HLR käideldavus on kriitiline ainult hääletuse lõppfaasis. Kuna HLR server ei sisalda dünaamilisi andmeid, on ta on tõrke korral väga kiiresti taastatav, seega ei ole tema tehniline käideldavus oluline risk.

HLR rakenduse tõrked – HLR rakendus on nii lihtne, et tõenäosus selles juhuslike vigade ilmnemiseks küllalt väike. Kõige tõenäolisemalt tekivad probleemid rakenduse ja turvamooduli vahelises suhtluses.

HLR privaatvõtmete käideldavus võib olla probleem. RSA krüpteerimisoperatsioonid on väga aeglased ning privaatvõtmeid kasutava riistvara (turvamooduli) valikul peab seda arvestama.

9.4.5. Auditisüsteem ja auditirakendus

Auditirakendus peab e-häälte kokkulugemise ja valimistulemuste avalikustamise vahel talle pandud vaheauditi funktsioonid (logide võrdlemine jne) läbi tegema. Kuna logide maht on tõenäoliselt väike, ei tohiks see probleemiks olla.

9.5. Võtmehalduse riskid

9.5.1. HLR privaatvõtme haldus

Kogu e-hääletamise salajasus põhineb häälelugemisrakenduse salajase võtme turvalisusel.

Kui *salajane võti hävib*, siis ei ole võimalik e-hääli lahti krüptida – e-hääletamine ebaõnnestub.
Kui *salajasele võtmele puudub juurdepääs*, siis lükkub e-häälte kokkulugemine edasi. Kui juurdepääs on permanentselt kadunud, on see võrdne võtme hävimisega.

Võtme hävimise/kadumise põhjused on vead võtmehaldusprotseduuride läbiviimisel, turvamoodulite rikked, kiipkaartide rikked ning võtmehalduritega seotud probleemid alates haigestumisest, PIN-koodi unustamisest ja ajapuudusest kuni suunatud ründeni.

Kui *salajane võti saab avalikuks*, siis on kõikide antud häälte salajasus rikutud.
Vastavad ohud on kirjeldatud ka kontseptsioonis.

Võtme avalikuks saamise põhjused on vead võtmehaldusprotseduuride läbiviimisel, võtmehaldurite kokkumäng ja turvamoodulite vead.

Seega peavad süsteemis olema meetmed
- salajase võtme käideldavuse tagamiseks,
- salajase võtme juurdepääsu ja kasutamise piiramiseks.

9.5.2. HLR avaliku võtme haldus

Tegelikkuses on avaliku võtme autentsuse tagamine raskem ülesanne kui salajase võtme turvamine. Kõikide avaliku võtme krüptograafiat kasutavate skeemide valupunkt on just avalike võtmete levitamine, mitte salajaste kaitsmine.

Avalike võtmete levitamiseks kasutatakse tavaliselt sertifikaate, mis võimaldavad usaldusest ühe osapoole (sertifikaadiserveri, CA) vastu tuletada usalduse sertifikaadiomanike ja nende avalike võtmete vastu. Tavamaailmas on analoogiaks pass, kus isiku tuvastamine põhineb usaldusel riigi kui isikut tõendava dokumendi väljaandja vastu. Samasugust skeemi tuleb kasutada ka e-hääletamisel.

HLR avaliku võtme asendusrünne

Hääletaja rakenduses asuv hääle krüpteerimiseks kasutatav HLR avalik võti ***peab*** vastama HLR privaatvõtmele. Kui rakenduses on vale võti, siis
- saab uue võtme salajase poole omanik hääled avada, häälte salajasus kaob;
- ei suuda HLR neid hääli enam avada, hääled lähevad kaotsi.

Võimalik on ka *vahendusrünne*, kus ründaja krüpteerib need hääled uuesti, seekord juba õige võtmega, ning edastab HES-i kaudu hääletussüsteemile. Tavavalimistel oleks võrreldav situatsioon see, kui valimiskastid oleks kaheosalised (vahelaega): hääletajad lasevad ümbrikud ülemisse poolde, loetakse üle aga hoopis alumisest poolest pärit võltsitud hääled.

Vahendusründe riski kaotab digiallkirja nõue – ründaja ei saa imiteerida hääletaja digiallkirja ning seega saab ta nii vahendada vaid ühe hääle (enda allkirja abil).

Probleem oleks *HLR võtme vahendusrünne HTS enda poolt* (veebiserver annab hääletajale rakenduse, mis krüpteerib hääle HTS-ile teadaoleva võtmega; HTS annab hääletaja valikust ründe organiseerijale teada, hääle aga muudab ära ja krüpteerib uuesti), kuna sel puhul saab "ründaja" ignoreerida digiallkirja kontrolli nõuet. Selle vastu aitab audit, mis kontrollib, kas HLR-i saadetud häältele on HTS-is olemas kehtivad digiallkirjad. Tegelikult on aga veebiserveril hääletaja hääle teadasaamiseks ja muutmiseks ka teisi, lihtsamaid viise, näiteks HR modifitseerimine.

Ründed võtmehaldurite vastu
On võimalik, et e-hääletamise ebaõnnestumiseks või häälte väärtuste teadasaamiseks püütakse HLR privaatvõtmele juurdepääsu omavaid isikuid mõjutada või kõrvaldada. Selle riski maandamiseks peab neid isikuid olema piisavalt palju, juurdepääs võtmetele peab olema jagatud (nn. mitu-mitmest skeemid) ning nad peavad olema organisatoorselt üksteisest sõltumatud.

9.6. Usaldusväärsuse riskid

E-hääletamine erineb tavalistest Interneti-teenustest oma poliitilise atraktiivsuse poolest. Selle protsessi ja süsteemi suhtes algatatakse peaaegu kindlasti mittesisulisi proteste ja vaidlusi, ning arvestama peab ka rünnetega, mis selliste protestide jaoks algmaterjali toodavad.

Seetõttu tuleb olla valmis selleks, et süsteemi kas püütakse kujutada ebausaldusväärsena, või tehakse midagi, et süsteem näiks ebausaldusväärne.

Poliitilisi riske meie analüüs ei kajasta, aga vastavad tehnilised võimalused kirjeldame ära.

Süüdistus – süsteemi sobimatus avalikuks hääletuseks
Võib väita, et e-hääletamine ei täida mõnda avalikule hääletusele esitatavat nõuet – näiteks ei taga hääle salajasust, tulemuse korrektsust või hääletuse ühetaolisust.

Süüdistus – süsteemi mittekontrollitavus
Võib väita, et e-hääletamise tehniline lahendus on kas ehitatud salajase, suletud lahendusena või on nii keerukas, et teda ei ole välistel vaatlejatel võimalik kontrollida.

Süsteemi avalike komponentide ründamine
Süsteemi avalikke komponente saab suure kära saatel ja kaugele nähtavalt rünnata.
Siia alla kuuluvad teenustõkestusründed, veebiserveri näotustamine (*defacement*), HR modifitseerimine jne.
Rünne ei pruugi olla sisuline. VVK veebiserveri näotustamine, näiteks selle esilehele mõne ebasündsa pildi panemine, võib kaasa tuua suure meediakära, omamata mingit efekti hääletuse tegelikule protsessile.

Ründe imiteerimine, pettused
Avalikkust saab ka petta väitega, et rünne on toimunud, ja esitada võltsitud tõendusmaterjali.
Igaüks võib oma arvutis lisada eelnimetatud VVK veebiserveri esilehele ükskõik milliseid pilte ja saata tulemuse ajakirjandusele väitega, et selline pilt veebis oligi. Või öelda, et HR tema arvutis tööle ei hakanud.

Samasuguseid ründeid saab muidugi teha ka tava-valimiste vastu: valija saab öelda, et "jaoskonnas ei küsitud minu passi", ja sellest ajaleheartikli tellida.

Auditisüsteemi ja auditirakenduse vead
Kui süsteemi kontrollimise vahendid on vigased või ebapiisavad, siis saa süsteem töö korrektsuses veenduda ning selle usaldusväärsus kannatab.

10. Lisa 4 - riskide koondtabel

Loetleme leitud riskid tabeli kujul üles ning lisame neile tõenäosus ja mõju hinnangud. Kontseptsiooni faasis oleva süsteemi korral on need muidugi väga umbkaudsed.

Nii tõenäosuse kui mõju hinnangud on skaalal 1 .. 3. Tõenäosuse korral on 1 tähendus "seda ei juhtu niikuinii" ja 3 "see risk realiseerub peaaegu kindlasti". Mõju lahtris olev 1 tähendab, et ohustatud on üks hääletajat või tema hääl, 2 taseme risk on kas ajalises või häälte arvu ulatuses piiratud, ning 3 mõjutab suurel määral kogu hääletustulemust või kogu e-hääletamise protsessi.

Riskihinnangud on antud eeldusel, et rakendatakse käesolevas analüüsis soovitatud meetmeid ja kontseptsiooni parandusi.

Risk	**Toimimise koht**	**Tõe-näosus**	**Mõju**
Fundamentaalsed ja protsessijuhtimise probleemid			
Protsesside formaliseerumisega kaasnevad riskid			
Protsesside tsentraliseerimisega kaasnevad riskid			
Süsteemi projekteerimise kvaliteet - disaini vead			
Süsteemi arenduse kvaliteet - tarkvara vead			
Süsteemi halduse kvaliteet - konfigureerimise ja haldamise vead			
Krüptograafia kasutamisest tingitud tarkvara probleemid			
Hääletaja arvuti kui kontrollimatu keskkonna riskid			
AIP-de kasutamisega seotud riskid			
Võimalikud tava- ja e-hääletamise protsesside konfliktid			
Ründed võtmehaldurite vastu			
E-hääletamise tulemuste piiratud salajasus			
Usaldusväärsuse riskid			
Süüdistus - süsteemi sobimatus avalikuks hääletuseks			
Süüdistus - süsteemi mittekontrollitavus			
Süsteemi avalike komponentide ründamine, näiteks veebiserveri näotustamine			
Ründe imiteerimine ja muud pettused			
Auditisüsteemi ja auditirakenduse vead			
Hääletustulemuse korrektsust mõjutavad riskid			
Hääletaja suunamine võltsitud veebilehele	net	xx	xx
Vahendusründed veebiserveri ja HR vahel	net	x	xx
Kasutaja arvuti ründamine ja kontrolli alla võtmine	net	xx	xx
Hääletaja rakenduse funktsionaalsed vead	HR	xxx	x
Eksitavate andmete kasutamine hääletaja poolt	HR	xx	x
Tahtlik mittekorrektse hääle saatmine hääletaja poolt	HR	xx	x
Kehtetu sertifikaadiga allkirjastatud hääle arvestamine tulemuses	HR	x	xx

Üldised allkirjarakenduse riskid	HR	xx	x
Süsteemi sisend- ja väljundandmete volitamatu muutmine	Kesksüsteem	x	xxx
Hääletaja rakenduse kompromiteerumine	HES, HR	x	xxx
Hääletaja rakenduses asuva HLR avaliku võtme asendamine	HES, HR, võtmehaldus	x	xxx
Kandidaatide nimekirja vead / volitamatu muutmine	HES, HR	x	xxx
Veebiserveri staatilise sisu kompromiteerumine	HES	xx	xxx
Klassikalised veebirakenduse ja veebiserveri halduse vead	HES	xxx	xx
HTS-is asuvate sisendandmete vead	andmebaas	xx	xx
HTS-is asuvate sisendandmete volitamatu muutmine	andmebaas	x	xx
Andmebaasis asuvate muude andmete volitamatu muutmine	andmebaas	x	xx
Signeerimata häälte nimekirja muutmine	Sisevõrk	x	xxx
HTS rakenduste funktsionaalsed vead	HTS	xx	xx
Digitaalallkirjade kontrollimise vead	HTS	x	xx
HLR rakenduse funktsionaalsed vead	HLR	x	xxx
Diskrimineerimisvead	kõik komponendid	xx	x
Häälte või hääletustulemuse salajasust mõjutavad riskid			
Hääletamise fakti privaatsuse rikkumine hääletaja arvutis	HR	xx	x
Hääle salajasuse rikkumine hääletaja arvutis	HR	x	x
Hääletamise fakti privaatsuse rikkumine Internetis	net	xxx	x
Hääletamise fakti privaatsuse rikkumine Kesksüsteemis	HES	x	x
Hääle salajasuse rikkumine veebiserveris	HES	xx	xxx
Häälte salajasuse rikkumine HTS-is	HTS	x	x
Häälte täieliku andmebaasi lekkimine	HES, HTS, sisevõrk	x	xx
Antud häälte väärtuse lekkimine häältelugemisrakendusest	HLR	x	xxx
E-hääletanute nimekirja lekkimine Kehtivuskinnituse teenuse pakkuja kaudu	KKT	(xx)	(x)
E-hääletamise kasutusintensiivsuse informatsiooni lekkimine	net	xx	x
HLR salajase võtme avalikuks tulek	HLR, võtmehaldus	x	xxx
Logide lekkimine auditisüsteemist	audit	xx	xx
Hääletamise töökindlust mõjutavad riskid			
Süsteemi haldustegevuse vead	kesksüsteem	xx	xx
Serverite ja sidevõrgu käideldavuse riskid	kesksüsteem	x	xx
Kesksüsteemi tarkvara tõrked ja kvaliteediprobleemid	kesksüsteem	xx	xxx
Kesksüsteemi riistvara tõrked	kesksüsteem	x	xx
Vajalike süsteemiressursside vale planeerimine	kesksüsteem	x	xx
Hääletaja rakenduse tõrked ja kvaliteediprobleemid	HR	xxx	x

Hääletaja rakenduse suur maht (hääletajate võrguühenduse suhtes)	HR	xx	xx
Andmebaasi töökindluse vead	HTS	x	xxx
Kehtivuskinnituse / ajatembelduse teenuse mitte-käideldavus	KKT	x	xx
Teenustõkestusründed	võrk, HES	x	xx
Hääletaja / HR tekitatud Kesksüsteemi ülekoormus	HES, HTS	x	x
HLR rakenduse tõrked	HLR	xx	xx
HLR salajase võtme häving / juurdepääsu võimatus	võtmehaldus	x	xxx
HLR privaatvõtmete käideldavus (dekrüptimise töökiirus)	HLR	xx	x

11. Lisa 5 - ebavajalikuks tunnistatud turvameetmed

Toome siinkohal ära turvameetmed, mille töögrupp 2003. aastal läbi arutas, kuid mille nõudmist vajalikuks ei peetud. Nende juurutamine ei ole muidugi endiselt keelatud ka 2010. aastal.

HR - HES suhtluse lisaturve

HR ja HES vahelisele suhtlusele saab lisad veel ühe kihi turvalisust:

- HR võib kontrollida, kas veebileht omab õiget sertifikaati
- lisaks HTTPS-ile võib kasutada täiendavat sõnumite ja andmete autentsuse ja tervikluse kontrolli: kandidaatide nimekirjad võiksid olla eelnevalt digitaalselt allkirjastatud, jne.

Kahjuks ei aita see näivalt kasulik vahend ei rakenduse kompromiteerumise ega vahendusrünnete vastu. Rakendustasemel turvalisuse lisamine ei aita selle vastu, kui rakendust ennast võltsitakse.

See meetod suurendaks küll ründeks vajalikku teadmist (ründama peab rakendust ennast, lihtsalt andmete võltsimisest ei piisa), kuid samas lisaks HR-ile keerukust veelgi juurde.

HTS jagamine kaheks eraldiseisvaks komponendiks

Võimalik on HTS jagamine kaheks lihtsamaks komponendiks: e-häälte andmise ajal töötavaks serveriks ning hilisemaks andmete töötlejaks. Neid komponente ühendaks ainult andmebaas.

Sisuliselt on see andmehõive ja andmetöötluse lahutamine.

Online paber-tally sissetulevate häälte tagatud "salvestamise" ja auditi jaoks

Võimalik on Kesksüsteemile saadetud hääled koheselt välja trükkida. Nii tekiks paberkujul häälte kontrolljälg. Alternatiivina võib trükkida hääle saamise fakti ja hääle räsi, sisuliselt oleks see siis Log1 paberkoopia.

Pea kõigi lääne-maailma valimismasinate analüüsis on väga tugevalt sees soovitus tekitada ka paberil kontrolljälg.

Leiame siiski, et häälte säilimise tagamine ning süsteemi auditeerimine on võimalik ka ilma antiikseid tehnoloogiaid kasutamata. Paber-väljatrükil oleks vaid kunstiline väärtus.

Lokaalsed andmebaasid erinevates komponentides

Arutati varianti valijate andmebaasi ka veebiserveris (HES-is) hoida.

Kahjuks tekivad seejuures nii suured sünkroniseerimisprobleemid, et võimalik lisa-turvalisus ei kompenseeri neid kuidagi.

Kesksüsteemi komponentide dubleerimine ning koormuse jaotumine

Süsteemi arhitektuur on selline, et kõiki kesksüsteemi komponente, v.a. andmebaas, võib olla piiramatu hulk.

Samas ei näe me hetkel vajadust dubleeritavust kasutada.

E-hääletamise infosüsteem erineb "tavalisest" e-teenuse infosüsteemist oluliselt:

- tema eluiga on lühike – füüsilise tõrke tõenäosus väike;
- koormus väike – koormusejagamist (*load-balancing*) pole vaja;
- testimiseks ja häälestamiseks on võimalusi võrdlemisi vähe.

Lisaks nimetatud erisustele näitavad seniläbiviidud e-valimised, et suur osa kasutajate koormusest langeb e-hääletamise perioodi esimesele ning viimasele tunnile. Selline olukord on omane kõigile süsteemidele, mille kasutamine on seotud mingi konkreetse tähtaja ning ajapiiranguga, näiteks e-maksuamet. Siiski ei ole mõistlik süsteemi võimsust dimensioneerida tipp-hetkede järgi. E-valimistel on püütud seda probleemi vähendada sellega, et valimisperiood pikendataks kolmelt päevalt seitsmele.

See tähendab, et dubleerimisega vähendatavate vigade (riistvara tõrked, ülekoormus) tõenäosus on väga väike, halduse ja tarkvara vigade tõenäosus on väga suur. Komponentide dubleerimine lisab keerukust ja kokkuvõttes mitte ei suurenda, vaid vähendab töökindlust.

Dubleeritud RSA võtmed

Käideldavuse huvides võib HLR-i kasutada kaht erinevat RSA võtmepaari. HR-is sisalduvad mõlemad, HES-ile saadetakse kaks eri võtmetega krüptitud häält. Sellele mehhanismile viidati ka kontseptsioonis.

See ei ole hea lahendus kahel põhjusel:

- Hääletamise tulemuse terviklus pole tagatud – me ei tea, kas mõlemas krüptogrammis on sama info. Tekib olukord, kus 1. või 2. võtmega üle lugedes saame eri tulemuse
- Me ei tea, kas 2. hääl krüptiti õige võtmega. Keegi võib HR-is ühe võtme teisega asendada ja kõikide häälte turvalisust rikkuda ilma et Kesksüsteem seda tuvastaks.

Topeltvõtmete võtmehaldus on piisavalt palju keerukam, et seda mitte teha.

Tagasiteavitus kolmanda osapoole kaudu (SMS: täname valimast!)

Maandab mitmesuguseid väärkasutuse riske, kuid tekitab neid veel rohkem juurde, ning selleks ei ole ka ühtegi üldkasutatavat kanalit.

Kesksüsteemi võrgu ja operatsioonisüsteemi kasutajate autentimine

Arutasime mitmeid viise Kesksüsteemi kasutajate paremaks autentimiseks ja võrgu tsoneerimiseks. Näiteks võib kasutajad panna tööle eraldi võrku ning lubada juurdepääs serveritele vaid läbi tulemüüri. See tagaks konsoolilogid, protokollide piiramise jne.

Leiti, et süsteemi haldajatele juurdepääsu piiramine ei ole tegelikkuses võimalik ega efektiivne. Mõnede tegevuste jaoks on niikuinii vaja füüsiliselt arvuti juurde pääseda.

HLR-i liikuva häälte faili juhuslikku järjekorda seadmine

See oleks olnud vahend häälte ja häälte andjate HLR-poolse sidumise vältimiseks.
Sisuliselt oleks see mix-net skeemi rakendamine Kesksüsteemi sees.

Hääletuse intensiivsuse läviväärtused

Vähese antud e-häälte arvu korral (vt peatükk 9.3.7, "Süsteemi väljund") võib hääle väärtus välistamismeetodil avalikuks saada. Selle ärahoidmiseks võib nõuda, et vähese antud häälte arvu korral loetakse e-hääletamine ebaõnnestunuks.
Tuleks defineerida:

- minimaalne antud häälte arv, millest alates tulemust kokku lugema hakatakse.
- minimaalne arvestatud häälte arv, millest alates tulemus arvesse võetakse.

Leiti siiski, et see ei ole vajalik.

12. Lisa 6 - viited

[BM] „Practical Security Analysis of E-voting Systems“, Ahto Buldas, Triin Mägi, IWSEC 2007
http://dx.doi.org/10.1007/978-3-540-75651-4_22

[Florida] The Butterfly Ballot: Anatomy of a Disaster
Ask Tog veebiajakiri, jaanuar 2001
http://www.asktog.com/columns/042ButterflyBallot.html

[IP1-S-EE] “Recommendation on legal and operational standards for e-enabled voting (Second Draft)"
IP1-S-EE töögrupp, juuli 2003
www.coe.int

[ISKE] Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE,
Riigi Infosüsteemide Arenduskeskus, juuni 2010
http://ria.ee/iske

[Neumann] Security Criteria for Electronic Voting
Peter G. Neumann, september 1993
http://www.csl.sri.com/users/neumann/ncs93.html

[OWASP] The OWASP Top 10 for 2010
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[PKCS] PKCS #1 v2.1 RSA Cryptography Standard
RSA Laboratories, juuni 2002
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/

[Rubin] Security Considerations for Remote Electronic Voting over the Internet
Avi Rubin, AT&T Labs – Research, juuli 2003
http://avirubin.com/e-voting.security.html