

Vabariigi Valimiskomisjon

E-hääletamise käsiraamat

Version 1.9

Dokument: EHA-03-02-1.9

Kuupäev: 29.01.2015.a.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Redaktsioonide ajalugu

| Kuupäev | Versioon | Kirjeldus ja muudatused | Autor |
|------------|----------|---|----------------------------------|
| 01.08.2005 | 1.0 | Koostatud ja vastu võetud dokument. | Jaak Tepandi |
| 22.09.2005 | 1.1 | Parandatud veebiserveri ja koodisigneerimise võtmepaari genereerimise ja sertifitseerimise kirjeldust | Tarvi Martens |
| 09.11.2006 | 1.2 | Parandatud koodisigneerimise võtmepaari genereerimise ja sertifitseerimise kirjeldust. Lisatud digitaalse templi sertifikaadi hankimise kirjeldus | Tarvi Martens |
| 31.01.2007 | 1.3 | Süsteemi, HES, HTS, HLR paigaldamise protseduurid muudetud. Konsolideeritud HSM initsialiseerimise ja võtmepaari genereerimise protseduurid. Läbivalt tehtud redaktsioonilisi ja sisulisi parandusi | Uve Lokk, Tarvi Martens |
| 08.05.2009 | 1.4 | Redaktsioonilised parandused, kustutatud ebakohaseid kohti. Lisatud valijarakenduse kontrollsummade avaldamise kord. Täiendatud koodisigneerimisega seonduvat. Lisatud e-hääletanute nimekirja printimise ja VIS-i ülekandmise protseduur. Eemaldatud süsteemi prooviläbimisega seotud protseduurid. Täiendused HES/HTS seadistamist. Lisatud proovihälte andmine. | Tarvi Martens |
| 17.09.2009 | 1.5 | Redaktsioonilised parandused. Eemaldatud akteerimisnõuded võtmete jms. hävitamisel. Eemaldatud auditeerimisnõue peatükis 2 kirjeldatult. Lisatud viimase HTS varukoopia eraldi transportimise ja säilitamise nõue. | Tarvi Martens |
| 13.01.2011 | 1.6 | Korrigeeritud viiteid teistele dokumentidele nende muutumise tõttu. Eemaldatud individuaalsete tühistusnimekirjade allkirjastamise nõue. | Tarvi Martens |
| 01.06.2012 | 1.61 | Kogu tekst toimetatud ja lisatud uued protseduurid 3.3 Majutusteenuse lepingu sõlmimine 5.4 ***Serverite avariijärgne taaste 6.8 ***Krüpteeritud e-hälte hävitamine 6.9 ***SSL serveri ja koodisigneerimise salajaste võtmete hävitamine 6.10. ***Isikuandmeid sisaldavate valijate nimekirjade ja nende koopiade hävitamine Protseduur „Lepingute lõpetamine ja süsteemi arhiveerimine“ kustutati. | Cybernetica AS (Ahto Buldas) |
| 01.12.2012 | 1.62 | Täiendatud vastavalt Tarvi Martensi ja Priit Vinkeli märkustele | Cybernetica AS (Sven Heiberg) |

| | |
|--------------------------|---------------------|
| E-hääletamise süsteem | Versioon: 1.9 |
| E-hääletamise käsiraamat | Kuupäev: 29.01.2015 |

| | | | |
|------------|-----|---|---------------|
| 23.09.2013 | 1.7 | Viidud vastavusse uue versiooniga „süsteemiülevaht juhend“-ist. Eemaldatud protseduurid, mida ei kasutata (DNS muutmine, tembeldussertifikaadi hankimine jms). Täpsustatud süsteemi prooviläbimist. | Tarvi Martens |
| 28.04.2013 | 1.8 | Minimaalsed korrektsioonid | Tarvi Martens |
| 28.01.2015 | 1.9 | Viited viidud vastavusse „süsteemiülevaht juhendi“ ver. 1.22-ga. Jaotised „Valimisjaoskondade ja valikute/kandidaatide failide tekitamine“ ja „Valijate esialgse nimekirja tekitamine“ asendatud jaotisega „Andmete komplekteerimine“. Lisatud protseduur „Logifailide kontrollimine“ Väiksemad täpsustused. | Tarvi Martens |

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Sisukord

| | |
|---|-----------|
| 1. Sissejuhatus ja taust | 6 |
| 1.1. Eesmärgid ja põhimõtted | 6 |
| 1.2. Lisamaterjalid ning -nõudmised | 6 |
| 1.3. Kriitilised protseduurid | 7 |
| 1.4. Kasutatud mõisted ja lühendid | 7 |
| 2. E-hääletamise süsteemi halduse ja edasiarenduse protseduurid | 9 |
| 2.1. E-hääletamise süsteemi konfiguratsioonihaldus..... | 9 |
| 2.2. E-hääletamise süsteemi tarkvara haldus..... | 11 |
| 3. Hääletamiseeelse perioodi protseduurid (enne kandidaatide registreerimist) | 12 |
| 3.1. Riistvara kontroll/hange | 12 |
| 3.2. Kehtivuskinnituse teenuse lepingu sõlmimine | 12 |
| 3.3. Mobiil-ID teenuse lepingu sõlmimine | 13 |
| 3.4. Majutusteenuse lepingu sõlmimine..... | 13 |
| 3.5. Valimiste veebisaidi uue sisu tekitamine ja haldamine..... | 14 |
| 3.6. ***E-hääletamise seadmetele baassüsteemide paigaldamine..... | 15 |
| 3.7. Veebiserverite TLS-sertifikaadi hankimine..... | 15 |
| 3.8. Valijarakenduse koodi signeerimise sertifikaadi hankimine | 16 |
| 4. Hääletamise-eelse perioodi protseduurid (pärast kandidaatide registreerimisotsust)..... | 18 |
| 4.1. Valimisjaoskondade ja valikute/kandidaatide failide tekitamine...Error! | |
| Bookmark not defined. | |
| 4.2. Valijate esialgse nimekirja tekitamine.....Error! Bookmark not defined. | |
| 4.3. ***Süsteemi võtmepaari loomine ja varundamine..... | 18 |
| 4.4. ***HES häälestus | 20 |
| 4.5. ***HTS häälestus | 20 |
| 4.6. ***HLR häälestus..... | 21 |
| 4.7. ***Jälgimisjaama häälestus | 19 |
| 4.8. ***Valijarakenduse pakendamine ja kontrollrakenduse seadistuse loomine | 22 |

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

| | | |
|-------|---|----|
| 4.9. | ***Serverite ülespanek majutuskohta..... | 24 |
| 4.10. | Rünnete jälgimine ja vastumeetmed..... | 25 |
| 5. | <i>Hääletamiseperioodi protseduurid.....</i> | 27 |
| 5.1. | ***E-hääletamise alustamine | 27 |
| 5.2. | ***Valijate nimekirja täiendamine, varukoopiate tegemine..... | 27 |
| 5.3. | ***E-hääletamise lõpetamine | 28 |
| 5.4. | ***Serverite avariijärgne taaste..... | 28 |
| 6. | <i>Hääletamisejärgse perioodi protseduurid.....</i> | 30 |
| 6.1. | ***Serverite tagasitoomine | 30 |
| 6.2. | ***E-hääletanute nimekirja printimine | 30 |
| 6.3. | ***E-häälte tühistuste kogumine ja e-häälte tühistamine | 31 |
| 6.4. | ***Häälte kokkulugemine | 32 |
| 6.5. | ***E-hääletamise tulemuse failide ülekanne valimiste infosüsteemi... .. | 32 |
| 6.6. | ***Võtmepaari hävitamine..... | 33 |
| 6.7. | ***Krüpteeritud e-häälte hävitamine..... | 34 |
| 6.8. | ***SSL serverite ja koodisigneerimise salajaste võtmete hävitamine. .. | 34 |

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

1. Sissejuhatus ja taust

1.1. Eesmärgid ja põhimõtted

Käesolev käsiraamat on loodud eesmärgiga vähendada e-hääletamise süsteemi haldusega seotud riske, pakkudes tuge süsteemi haldamisel ja turvalisuse tagamisel. Turvaprobleeme käsitletakse süvitsi dokumendis "E-hääletamise süsteemi infoturbe poliitika". E-hääletamise süsteemi ülesehitust kirjeldatakse täpsemalt dokumendis "E-hääletamise organisatsioon ja infrastruktuur".

Mõnede käsiraamatus kirjeldatud protseduuride täpsem sisu on lahtiseks jäetud. Neile fikseeritakse vajalikud välistingimused ning viidatakse juhenditele, mis protseduure täpsemalt kirjeldavad. Osad protseduurid sisaldavad suhtlust kolmandate osapooltega, vastutusrikkaid siseprotseduure vms. Neid kirjeldatakse käsiraamatus pikemalt.

Protseduuride detailsuse astme valik eeldab, et nende täitjail on ülevaade kasutatavatest keskkondadest, baassüsteemidest ja infoturbe meetoditest. Eeldatakse ka, et täitjad on tuttavad või tutvuvad vastavalt vajadusele muu e-hääletamise süsteemi dokumentatsiooniga, mida käsiraamatus ei dubleerita. Süsteemihalduse hõlbustamiseks on mõned keerukamad üldprotseduurid e-hääletamise süsteemi parameetritega detailsemalt lahti kirjutatud.

1.2. Lisamaterjalid ning -nõudmised

Järgnevates jaotistes on kirjeldatud e-hääletamise etappidega seotud protseduurid. Protseduurides viidatakse vajadusel teistele dokumentidele. Mitmete protseduuride detailsem esitus on toodud järgmistes materjalides:

1. "E-valimised. Süsteemiülevaade juhend" (EHA-03-03-*).
2. "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhise" (EHA-03-06-*). Käsiraamatus on viidatud põhiliselt tegevusjuhisele. Protseduuride läbiviimisel võib olla kasulik ka dokument "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Üldosa(EHA-03-05-*).".
3. "Valijarakenduse pakendamine" (EHA-03-04-*).
4. "E-hääletamise organisatsioon ja infrastruktuur" (EHA-02-01-*), kus on esitatud e-hääletamisega seotud organisatsioonid, rollid, töötajad ja allkirjaõiguslikud isikud.
5. "E-hääletamise süsteemi infoturbe poliitika" (EHA-02-03-*), kus on esitatud täiendavad nõudmised protseduuride läbiviimisele, näiteks sündmuste logimisele, insidentide haldusele, seadmete ja informatsiooni turbele jne.

Vastavalt vajadusele lähtutakse Riigikogu Kantselei sisekorraeeskirjast, asjaajamiskorrast, asutusesisese teabe kasutamise korrast ja Toompea lossis viibivate isikute ohuolukorras tegutsemise korrast.

| | |
|--------------------------|---------------------|
| E-hääletamise süsteem | Versioon: 1.9 |
| E-hääletamise käsiraamat | Kuupäev: 29.01.2015 |

VVK ja Elektroonilise Hääletamise Komisjoni (EHK) esimees kontrollivad kõikide protseduuride täitmist vastavalt vajadusele. Kriitiliste protseduuride juures on kontrollimine kohustuslik, vastav roll ning kontrolli määr on toodud jaotises "Kontrollib".

Jaotises E-hääletamise süsteemi halduse ja edasiarenduse protseduurid toodud süsteemihalduse protseduurid on pidevad ja ei ole seotud konkreetsete valimistega. Teisi protseduure täidetakse uute valimiste ajal uuesti.

1.3. Kriitilised protseduurid

Olulisimad elektroonilise hääletamisega seotud riskid on:

- tulemuste ebakorrektsus,
- tulemuste ebausaldusväarsus,
- hääle salajasuse rikkumine,
- hääletamise katkemine.

Põhiriskide realiseerumine võib toimuda näiteks läbi häälte ebakorrekse loendamise, ühe valija mitme hääle arvestamise või vale inimese hääle arvestamise kaudu. Loetelu ei ole lõplik.

Kriitilisteks loetakse neid protseduure, mille ebakorrekne täitmine võib viia nimetatud põhiriskide realiseerumiseni. Kriitilised on näiteks protseduurid, mille väärtäitmine võib viia süsteemi koodi volitamatu muutmiseni või oluliste võtmete lekkeni. Kriitilised protseduurid on tähistatud kolme tärniga protseduuri nimetuse alguses.

Kriitilisi protseduure täidetakse vähemalt kahe sõltumatu inimese koostöös ja täitjaid roteeritakse regulaarselt valimiste lõikes. Võimalusel täidetakse kriitilisi protseduure väljaspool hääletusperioodi.

Kriitilisteks ei loeta neid protseduure, mille valesti täitmine võib põhjustada probleeme kuid mis ei vii põhiriskide realiseerumiseni. Näiteks protseduur, mille ebaõnnestumine võib viia e-hääletamise ärajätmiseni olukorras, kus seda saab asendada tavahääletamisega, ei ole kriitiline protseduur.

1.4. Kasutatud mõisted ja lühendid

| Mõiste/lühend | Seletus |
|----------------------|---|
| HES | Häälteedastusserver |
| HTS | Häältetalletamisserver |
| HLR | Häältelugemisrakendus |
| AR | Auditirakendus |
| HSM | riistvaraline turvamoodul (<i>Hardware Security Module</i>) |

| | |
|--------------------------|---------------------|
| E-hääletamise süsteem | Version: 1.9 |
| E-hääletamise käsiraamat | Kuupäev: 29.01.2015 |

| | |
|-------------|--|
| VIS | valimiste infosüsteem |
| Kesksüsteem | Vabariigi Valimiskomisjoni vastutuse all olev süsteemiosa. Tegeleb hääle vastuvõtmisega, töötlemisega ja koondtulemuse väljastamisega. |

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

2. E-hääletamise süsteemi halduse ja edasiarenduse protseduurid

Süsteemi halduse ja edasiarenduse protseduuride põhieesmärk on süsteemi korrektse funktsionaalsuse säilitamine muudatuste käigus. Kuna muudatused on tihti vaid lokaalsed, ei ole enamasti otstarbekas pärast iga muudatust kogu süsteemi uuesti verifitseerida. Seetõttu kasutatakse konfiguratsiooni- ja muudatuste haldust.

E-hääletamisel on kriitilised nii tarkvara kui riistvara, kuid süsteem ise on väikesemahuline. Seepärast on e-hääletamise süsteemi konfiguratsioonihalduse kord esitatud ühiselt tarkvarale ja riistvarale.

2.1. E-hääletamise süsteemi konfiguratsioonihaldus

Konfiguratsioonihalduse eesmärk on luua ja säilitada e-hääletamise süsteemi kõigi komponentide terviklus ning tagada, et süsteemihaldureil oleks alati õige ja täpne teave süsteemi ja selle komponentide oleku kohta.

Tulemusena on kõigi süsteemi versioonide kõik komponendid identifitseeritavad, verifitseeritud ning nende ajalugu on jälgitav alates baasversioonist, st on võimalik

- üheselt identifitseerida iga süsteemi elemendi versioone,
- identifitseerida kõigi e-hääletamise süsteemi konkreetseks tarkvaraversiooniks ühendatavate tarkvaraelementide versioone,
- identifitseerida väljatöötamisel olevate, üleantud või installeeritud tarkvaratoodete arendusseisundit,
- ohjata kahe või mitme sõltumatult töötava isiku tööd mingi tarkvaraelemendi üheaegsel uuendamisel,
- identifitseerida ja jälgida kõiki muudatuse taotlusest või probleemist tulenevaid toiminguid ja muudatusi nende algatamisest kuni üleandmiseni.

Konfiguratsioonihalduses osalevad järgmised osapooled:

- *e-hääletamise kesksüsteemi haldaja* – kehtestab konfiguratsioonihalduse korra, loob süsteemi konfiguratsiooni identifitseerimise põhimõtted, kehtestab süsteemi konfiguratsiooni baasversiooni, vastutab selle eest, et tarkvara konfiguratsioonihalduse nõudmised oleksid kajastatud arendajaga sõlmitavates lepingutes, jälgib tarkvara konfiguratsioonihalduse korrektsust ja nõuab vajadusel täiendusi,
- *e-hääletamise tarkvara arendaja* – identifitseerib ja haldab e-hääletamise süsteemi tarkvara konfiguratsiooni.

E-hääletamise kesksüsteemi haldaja loob ja hoiab käigus konfiguratsiooniseisundi arvestust, kus kajastuvad ka kasutatavad konfiguratsioonihalduse vahendid ja meetodid.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitja (Roll): EHK

Partner: e-hääletamise tarkvara arendaja

Toimingud

E-hääletamise kesksüsteemi haldaja

- 1) identifitseerib esialgse verifitseeritud süsteemi baasversiooni ja kõik selle komponendid,
- 2) registreerib iga muudatuse põhjused, sisu, muudetud komponendid ning nende uued identifikaatorid,
- 3) verifitseerib vajadusel kõik komponentide muudatused analoogiliselt baasversiooni komponentidega.

Konfiguratsiooniseisundi arvestus kajastab

- 1) süsteemi struktuuri ja konfiguratsioonielementide valikut,
- 2) dokumentatsiooni ja faile,
- 3) nimereegleid sh versioonide identifitseerimist,
- 4) süsteemi konfiguratsiooni baasversiooni kehtestamist.

E-hääletamise süsteemi konfiguratsioonihaldusega hallatavate toodete hulka kuuluvad

- 1) protsessi, plaanimist, lepinguid ja tooteid puudutavad dokumendid (võivad olla osaliselt hallatud eraldi logides),
- 2) riistvara ja sidevahendid,
- 3) andmed (võivad olla hallatud eraldi logides),
- 4) tarkvara (haldab tarkvara arendaja).

Tarkvara arendaja identifitseerib tarkvara konfiguratsiooni

- 1) tarkvara struktuuri ja konfiguratsioonielementide valikuga,
- 2) dokumentatsiooni ja failidega,
- 3) nimereeglitega (sealhulgas versioonide identifitseerimine),
- 4) tarkvara konfiguratsiooni baasversiooni kehtestamisega.

Versioonide identifitseerimisel jälgitakse põhimõtet, et iga muudatuse tegemine praktilisse kasutusse minevas koodis peab kaasa tooma koodi versiooni muutumise.

Tarkvara konfiguratsioonihalduse süsteemiga hallatavate toodete hulka kuuluvad

- 1) lepingut, protsessi, plaanimist ja toodet puudutavad dokumendid,
- 2) arendaja loodud lähte-, objekt- ja täitmiskood,
- 3) kolmandate osapoolte tarkvara nagu operatsioonisüsteemid, teegid jne.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Iga tarkvaraelemendi või elementide kogumi kohta identifitseeritakse

- 1) dokumentatsioon,
- 2) kõik tootega seotud arendusinstrumendid,
- 3) liidestus teiste tarkvaraelementide ja riistvaraga,
- 4) riistvara- ja tarkvarakeskkond.

2.2. E-hääletamise süsteemi tarkvara haldus

Tarkvara halduses osalevad e-hääletamise kesksüsteemi haldaja ja e-hääletamise tarkvara arendaja.

E-hääletamise süsteemi tarkvarana käsitletakse: baastarkvara (operatsioonisüsteemid jne), e-hääletamise süsteemi tarkvara, kompileeritud mooduleid, dokumentatsiooni, muid komponente (näiteks testide protokollid või tulemused).

Organisatsioon: E-hääletamise kesksüsteemi haldaja

Täitjad (rollid): EHK, EHK esimees

Partner: E-hääletamise tarkvara arendaja (tarkvara arendaja)

Toimingud

1. EHK esimees täpsustab probleemi või tööülesande ja organiseerib nõudmiste/muudatuste spetsifikatsiooni koostamise.
2. EHK esimees tellib tarkvara arendajalt spetsifikatsiooni alusel vajaliku arendustöö.
3. EHK esimees korraldab tarkvara arendaja töö jälgimise (vastavus ülesandele, kvaliteedi- ja turvanõuetest kinnipidamine).
4. EHK esimees reguleerib ja auditeerib kõiki juurdepääse ohutus- ja turvakriitilisi funktsioone käsitlevatele tarkvaraelementidele.
5. EHK esimees võtab vastu tulemused (lähtekood, kompileeritud kood, dokumentatsioon, nõudmised riistvarale jne), ja säilitab neid vastavalt talitluspidevuse plaanis ettenähtule.
6. EHK esimees organiseerib tulemuste testimise ja nõuab vajadusel tarkvara arendajalt parandusi.
7. EHK esimees korraldab nõudmiste riistvarale esitamise dokumendis "E-hääletamise süsteem. Tehnilised nõudmised riistvarale".

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

3. Hääletamiseelse perioodi protseduurid (enne kandidaatide registreerimist)

Selle jaotise protseduuridega võib alustada kuitahes vara. Protseduurid tuleb aga lõpetada enne konkreetse valimise hääletamisperioodi algust.

Kui protseduuri teostamise asukohta ei ole antud, siis eeldatakse, et protseduur teostatakse e-hääletamise kesksüsteemi haldaja keskkonnas.

3.1. Riistvara kontroll/hange

Kontrollitakse riistvara olemasolu, vajadusel hangitakse riistvara usaldusväärsetl partnerilt.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): EHK esimees, kesksüsteemi peaoperaator

Partner: riistvara tarnija

Toimingud

1. Peaoperaator täpsustab, millist riistvara on e-hääletamise läbiviimiseks vaja. Vajalik konfiguratsioon on toodud dokumendis "E-hääletamise organisatsioon ja infrastruktuur"
2. Peaoperaator kontrollib vajaliku riistvara olemasolu. Nõuded riistvarale on esitatud dokumendis "E-hääletamise süsteem. Tehnilised nõudmised riistvarale".
3. Kui riistvara on vaja juurde hankida, sätestab peaoperaator nõuete põhjal tehnilised hanketingimused. EHK esimees korraldab riistvara hanke ning tarnitava riistvara vastuvõtmise ja turvalise ladustamise.

Märkus: Riistvara hankena käsitletakse ka Riigi Infosüsteemi Ameti (RIA) ressursside kasutamist.

3.2. Kehtivuskinnituse teenuse lepingu sõlmimine

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi peaoperaator, EHK esimees, VVK esimees

Partner: kehtivuskinnituse teenuse osutaja

Toimingud

1. Peaoperaator teeb kindlaks kehtivuskinnituse teenuse vajadused ning sellest tulenevalt kehtivuskinnituse teenusepaketi.
2. EHK esimees valmistab ette lepingu kehtivuskinnituse teenuse osutajaga.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

3. VVK esimees sõlmib lepingu kehtivuskinnituse teenuse osutajaga.
4. EHK esimees jälgib, et lepinguga võetud kohustused oleks täidetud.

Märkus: Kehtivuskinnituse teenust sidusrežiimis kasutab ainult HTS.

3.3. Mobiil-ID teenuse lepingu sõlmimine

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi peaoperaator, EHK esimees, VVK esimees

Partner: Mobiil-ID teenuse osutaja

Toimingud

1. Peaoperaator teeb kindlaks Mobiil-ID teenuse vajadustest tuleneva teenusepaketi.
2. EHK esimees valmistab ette lepingu Mobiil-ID teenuse osutajaga.
3. VVK esimees sõlmib lepingu Mobiil-ID teenuse osutajaga.
4. EHK esimees jälgib, et lepinguga võetud kohustused oleks täidetud.

Märkus: Mobiil-ID teenust sidusrežiimis kasutab ainult HES.

3.4. Majutusteenuse lepingu sõlmimine

Majutusteenuselt eeldatakse, et e-hääletamisega seotud serverid paigaldatakse eraldi seadmekappi, mille tellija kinni pitseerib. Samuti eeldatakse, et teenusepakkuja kaitseb servereid välisvõrgu eest tulemüüri abil.

E-hääletamise majutus erineb seetõttu standardsest majutusteenusest, leping peab olema hästi ette valmistatud, teenusepakkujale tutvustatud ning selle korrektset täitmist tuleb kontrollida.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi peaoperaator, EHK, VVK esimees, EHK esimees

Partner: häälteedastamis- ja häältetalletamisserverite majutaja (majutusteenuse pakkuja)

Kontrollib: audiitor vaatab vajadusel kohapeal üle majutusteenuse olukorra ja kontrollib nõuetele vastavust

Toimingud

1. Peaoperaator hindab serverimajutuse vajadusi (serverite mõõdud, võimsustarve, täiendava elektritoite vajadused, ühenduse kiirus, IP-aadresside arv, erinõudmised, telehotelli klass jne), arvestades m.h. dokumendiga "Nõudmised e-hääletamise majutusteenusele".

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

2. EHK hindab majutusteenuse pakkuja vastavust vajalikule turvastandardile, nõudes kehtivat auditeerimisaruannet, milles kinnitatakse majutusteenuse pakkuja vastavust ISKE H-taseme nõuetele.
3. EHK esimees hindab teenuse majutuseks vajalikku ajavahemikku.
4. EHK esimees ja teenusepakkuja valmistavad lepingu ette ja räägivad läbi tingimustes.
5. VVK esimees ja majutusteenuse pakkuja sõlmivad kokkuleppe majutusteenuse osutamiseks.
6. EHK esimees jälgib, et kokkuleppega võetud kohustused oleks täidetud.

3.5. Valimiste veebisaidi uue sisu tekitamine ja haldamine

Valimiste veebisaidil olev info võib oluliselt parandada e-hääletajate turvakäitumist, seetõttu töötab EHK välja valimiste veebisaidi www.valimised.ee elektroonilise hääletamise spetsiifilise sisu ning haldab seda vastavalt hääletamise käigus tekkivatele võimalikele probleemidele.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): EHK, Valijatele tehnilise toe tagaja

Partner: puudub

Kontrollija ja kontrolli tase: audiitor hindab tulemusi omal valikul

Aeg: enne e-hääletamise algust ja kogu hääletamisperioodil

Toimingud

1. EHK analüüsib, milline on minimaalne vajalik oluline turvainfo e-hääletamise läbiviimiseks, kuid annab edasi vähemalt järgmised soovitused: kasutada tulemüüri; installeerida oma operatsioonisüsteemile ja rakendustele turvauendused; teha viirusekontroll ja kasutada nuhkvara tõrjet; ise sisestada veebiaadress; kontrollida serveri sertifikaati; kontrollida valija rakenduse digitaalselt allkirjastatud kontrollsummasid; kasutada kontrollrakendust hääle kontrollimiseks; teavitada kõigist probleemidest valimise tehnilist tuge.
2. EHK analüüsib, milline on minimaalne vajalik tehniline informatsioon e-hääletamise läbiviimiseks, kuid annab edasi vähemalt järgmise informatsiooni: toetatud operatsioonisüsteemid, ID-kaardi tarkvara toimimise kontroll, internetiühenduse toimimise kontroll.
3. Valijatele tehnilise toe tagaja koostab tekstide tehnilise sisu.
4. EHK esimees korraldab valimiste veebisaidi sisu avalikustamise

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

3.6. *E-hääletamise seadmete baassüsteemide paigaldamine**

Paigaldatakse HES, HTS, HLR ja jälgimisjaama baassüsteemid ning üks varuserver.

Operatsioonisüsteemi ja turvapaikade laadimisel ning arvutite Internetti ühendamisel tuleb jälgida dokumendis "E-hääletamise organisatsioon ja infrastruktuur" toodud nõudmisi.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

Kontrollija: audiitor

Asukoht/infrastruktuur (vajadusel): e-hääletamise kesksüsteemi haldaja ruumid

Eeldused: Protseduur Riistvara kontroll/hange on toimunud, e-hääletamise kesksüsteemi haldaja valduses on reserveeritud nõuetekohane riistvara.

Toimingud

1. Operaatorid paigaldavad ja seadistavad HES, HTS, HLR, jälgimisjaama ja varuserveri vastavalt dokumendile „E-hääletamise süsteem. Operatsioonisüsteemi paigaldus“.
2. Operaatorid kaitsevad arvutid parooliga vastavalt paroolihalduse eeskirjale.
3. Operaatorid pitseerivad seadistatud serverid turvakleebistega.
4. Pitseeritud arvutid ladustatakse turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

3.7. Veebiserverite TLS-sertifikaadi hankimine

Hangitakse TLS-sertifikaadid serveritele:

- Valijarakenduse ja kontrollrakenduse jagamiseks seatud www.valimised.ee
- HES
- Jälgimisjaam (selle jaoks võib kasutada ka isegenereeritud sertifikaati)

Märkus: Toiming viiakse läbi ainult siis, kui on vaja hankida uus sertifikaat. Mitmetel järjestikustel valimistel võib kasutada sama sertifikaati. Sellisel juhul tuleb kindlustada vastava privaatsvõtme ja seda kaitsvate paroolide turvaline säilimine.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Kesksüsteemi operaatorid.

Partner: sertifitseerimisteenuse osutaja

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Kontrollija ja kontrolli tase: audiitor hindab tulemusi omal valikul

Toimingud

1. EHK esindaja veendub, et sertifitseerimisteenuse osutaja on valmis teenust osutama.
2. Operaatorid veenduvad, et serverarvuti, milles genereeritakse võtmepaar on arvutivõrgust eraldatud. Operaatorid veenduvad, et serverarvutisse on paigaldatud openssl.
3. Operaatorid loovad veebiserveri salajase võtme käsuga

openssl genrsa -des3 -out hes.pem 2048

4. Operaatorid kaitsevad võtme parooliga.
5. Operaatorid teevad salajasest võtmest varukoopia. Juurdepääsuõigus salajasele võtmele ja selle varukoopiale on EHK esimehel ning kesksüsteemi operaatoritel Op1 ja Op2.
6. Operaatorid hoiavad salajast võtit turvaliselt ja haldavad selle parooli vastavalt paroolihalduse reeglitele.
7. Operaatorid loovad sertifikaadipäringu:

openssl req -new -sha1 -key hes.pem -out hes.csr

Parameeter `challenge password` jääb määramata.

8. Operaatorid kontrollivad sertifikaadipäringu sisu käsuga
- openssl req -in hes.csr -text
9. Operaatorid saadavad sertifikaadipäringu sertifitseerimisteenuse osutajale.
 10. EHK esimees korraldab sertifitseerimisteenuse osutajalt laekunud arve tasumise.
 11. Operaatorid saavad kätte sertifikaadi ning salvestavad selle.

3.8. Valijarakenduse koodi signeerimise sertifikaadi hankimine

Genereeritakse valijarakenduse koodi genereerimise võti ning hangitakse sertifikaat.

Märkus: Toiming viiakse läbi ainult siis, kui on vaja hankida uus sertifikaat. Mitmetel järjestikustel valimistel võib kasutada sama sertifikaati. Sellisel juhul tuleb kindlustada vastava privaatvõtme ja seda kaitsvate paroolide turvaline säilimine.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Kesksüsteemi operaatorid.

Partner: sertifitseerimisteenuse osutaja

| | | |
|--------------------------|----------|------------|
| E-hääletamise süsteem | Version: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Toimingud

1. Operaatorid tuvastavad valijarakenduse signeerimiseks vajaliku krüptopulga tehnilised nõudmised.
2. Operaatorid soetavad krüptopulga valimise eelarvest.
3. Kui pulgal puudub eelgenereeritud võtmepaar, siis operaatorid genereerivad selle valides sobiva(d) parooli(d).
4. Operaatorid genereerivad sertifitseerimispäringu.
5. Operaatorid pitseerivad krüptopulga ja parooli(d) turvaümbrikusse ning tähistavad selle.
6. Operaatorid esitavad sertifitseerimisteenuse osutajale avalduse koodisigneerimise sertifikaadi saamiseks ning sertifikaadipäringu.
7. EHK esimees korraldab sertifitseerimisteenuse osutajalt saadud arve tasumise.
8. Sertifikaadi laekumisel avavad operaatorid turvaümbriku ning paigaldavad sertifikaadi krüptopulgale. Operaatorid veenduvad koodisigneerimise toimimises. Seejärel pitseeritakse krüptopulk ning parool(id) uude turvaümbrikusse ning tähistatakse see.
9. EHK esimees vastutab krüptopulka sisaldava turvaümbriku hoidmise eest.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

4. Hääletamise-eelse perioodi protseduurid (pärast kandidaatide registreerimisotsust)

Selle jaotise protseduuridega on võimalik alustada pärast kandidaatide registreerimisotsust.

4.1. ***Süsteemi võtmepaari loomine ja varundamine

Lähtestatakse HSM ning selle partitsioon, misjärel genereeritakse süsteemi võtmepaar. Avalik komponent integreeritakse valija rakendusse. Privaatvõtit kasutatakse häältelugemise rakenduses hääle dešifreerimiseks ("E-hääletamise süsteemi üldkirjeldus", jaotis 6).

Võetakse HSM server ning töötatakse sellega vastavalt dokumentides "E-hääletamise organisatsioon ja infrastruktuur", "E-hääletamise süsteemi infoturbe poliitika" ja "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Üldosa" ettenähtule.

VVK otsustab eelnevalt, mitme liikme kohalolu on vajalik süsteemi privaativõtme aktiveerimiseks.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kõik turvamooduliga seotud rollid

Partner: VVK

Kontrollija ja kontrolli tase: audiitor teeb koos operaatoritega läbi vähemalt osa sooritavatest protseduuridest, aga kõik võtmepaari loomist kitsamas mõistes puudutavad punktid.

Aeg: enne valijarakenduse pakendamist

Toimingud

Operaatorid teevad läbi protseduuri 1.1 juhendist "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhised" (dokument EHA-03-06-*). Sealhulgas genereeritakse süsteemi avalikust võtmest autoallkirjastatud sertifikaat. Võtmepaariga seotud täpsemad protseduurid on kirjeldatud juhendi punktides 1.1.99-1.1.141.

Vajadusel taastatakse HSM server või võtmepaar vastavalt protseduurile 1.3 juhendist "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhised".

4.2. Andmete komplekteerimine

Enne serverite häälestust tuleb kokku koguda ning vormindada seadistuseks vajalikud andmed ning konfiguratsioonid. Need on (sulgudes andmete andja ja viide andmestruktuuri spetsifikatsioonile):

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

- Kandidaatide nimekiri (Valimiste Osakond, „Elektroonilise hääletamise protokollistik IV: Kesküsteemi protokollid“)
- Ringkondade ja jaoskondade nimekiri (Valimiste Osakond, „Elektroonilise hääletamise protokollistik IV: Kesküsteemi protokollid“)
- Valijate nimekiri (AS Andmevara, „Elektroonilise hääletamise protokollistik IV: Kesküsteemi protokollid“)

Märkus1: AS Andmevara poolt toodetavad valijate nimekirjad on signeeritud. Vastava signeerimisvõtme on digitaalselt allkirjastanud organisatsiooni vastutav isik. Juhul, kui allkirjastatud on avaliku võtme asemel autosigneeritud sertifikaat, tuleb sellest eraldada avalik võti käsuga:

```
openssl x509 -noout -pubkey -in andmevara.der -inform DER
```

- Sertifikaatide konfiguratsioon (EHK, vt dokument "E-valimised. Süsteemiülevaade juhend" jaotis 3.2.1)
- Kontrollrakenduse konfiguratsioon (EHK, „Elektroonilise hääletamise protokollistik III: Kontrollprotokoll“)

Märkus2: Viimase koostamiseks on vajalik käesoleva dokumendi jaotise 4.1 järgi genereeritud autoallkirjatatud sertifikaat. Vajaliku avaliku võtme saab sellest käsuga:

```
openssl x509 -noout -pubkey -in vvk.der -inform DER
```

Kontrollrakenduse konfiguratsiooni võib juba enne järgmise etappe juba paigaldada aadressile <https://www.valimised.ee/config.json>.

4.3. ***Jälgimisjaama häälestus

Selle protseduuri käigus häälestatakse jälgimisjaam.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): e-hääletamise kesksüsteemi haldaja ruumid

Eeldused: Protseduur ***E-hääletamise seadmetele baassüsteemide paigaldamine on toimunud.

Toimingud

1. Operaatorid võtavad jälgimisjaama jaoks reserveeritud arvuti koos installeeritud baassüsteemi ja jälgimisjaam tarkvaraga.
2. Audiitor kontrollib, et riistvara on nõuetekohaselt turvakleebistega kaitstud.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

3. Operaatorid seadistavad jälgimisjaama vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 2.4.
4. Operaatorid pitseerivad seadistatud arvuti turvakleebistega.
5. Pitseeritud arvuti ladustatakse kuni majutusteenusesse viimiseni turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

4.4. *HES häälestus**

HES häälestatakse algavateks valimisteks.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): e-hääletamise kesksüsteemi haldaja ruumid

Eeldused: Protseduur ***E-hääletamise seadmetele baassüsteemide paigaldamine on toimunud.

Toimingud

1. Operaatorid võtavad HES jaoks reserveeritud arvuti koos installeeritud baassüsteemi ja HES tarkvaraga.
2. Audiitor kontrollib, et riistvara on nõuetekohaselt turvakleebistega kaitstud.
3. Operaatorid teevad läbi ühised seadistusperioodi tegevused vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 3.
4. Operaatorid seadistavad HESi vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 4.1.
5. Vajadusel muudavad operaatorid süsteemseid teateid vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 8.6.
6. Operaatorid pitseerivad seadistatud arvuti turvakleebistega.
7. Pitseeritud arvuti ladustatakse kuni majutusteenusesse viimiseni turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

4.5. *HTS häälestus**

HTS häälestatakse konkreetseteks valimisteks.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): e-hääletamise kesksüsteemi haldaja ruumid

Eeldused: Protseduur ***E-hääletamise seadmetele baassüsteemide paigaldamine on toimunud.

Toimingud

1. Operaatorid võtavad HTS jaoks reserveeritud arvuti koos installeeritud baassüsteemi ja HTS tarkvaraga.
2. Audiitor kontrollib, et riistvara on nõuetekohaselt turvakleebistega kaitstud.
3. Operaatorid teevad läbi ühised seadistusperioodi tegevused vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 3.
4. Operaatorid seadistavad HTSi vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 5.1.
5. Vajadusel muudavad operaatorid süsteemseid seadeid vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 8.6.
6. Operaatorid kontrollivad serverite ühtsust vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 4.1.6.
7. Operaatorid pitseerivad seadistatud arvuti turvakleebistega.
8. Pitseeritud arvuti ladustatakse kuni majutusteenusesse viimiseni turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

4.6. *HLR häälestus**

HLR häälestatakse konkreetseteks valimisteks.

HLR on riistvaralise turvamooduliga ühendatud kahes režiimis: (1) kui terminal, juhendis "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhend" punases kirjas käsud ja (2) võrgu kaudu, juhendis "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhend" sinises kirjas käsud. Häälestamine toimub mõlemas režiimis.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): e-hääletamise kesksüsteemi haldaja ruumid

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Eeldused: Protseduur ***E-hääletamise seadmetele baassüsteemide paigaldamine on toimunud.

Toimingud

1. Operaatorid võtavad HLR jaoks reserveeritud arvuti koos installeeritud baassüsteemi ja HLR tarkvaraga.
2. Audiitor kontrollib, et riistvara on nõuetekohaselt turvakleebistega kaitstud.
3. Operaatorid teevad läbi ühised seadistusperioodi tegevused vastavalt dokumendi "E-valimised. Süsteemiülema juhend" jaotisele 3.
4. Operaatorid seadistavad HLRi vastavalt dokumendi "E-valimised. Süsteemiülema juhend" jaotisele 6.1
5. Operaatorid pitseerivad seadistatud arvuti turvakleebistega.
6. Pitseeritud arvuti ladustatakse turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

4.7. *Valijarakenduse pakendamine ja süsteemi prooviläbimine**

Luuakse valijarakendus konkreetsete valimiste jaoks.

Protseduuri eeltingimused on järgmised:

- e-hääletamise arvutitele on paigaldatud baassüsteemid,
- süsteemi võtmepaar on loodud,
- valijarakenduse koodi signeerimise sertifikaat ning vajalikud väljaandja sertifikaadid on paigaldatud sertifikaadihoidlasse,
- valikute / kandidaatide nimekiri on olemas,
- hes.valimised.ee TLS-sertifikaat on olemas.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: sertifitseerimisteenuse osutaja

Kontrollib: audiitor


Toimingud

1. Operaatorid teevad läbi tegevused juhendist "Valijarakenduse pakendamine".
2. Operaatorid veenduvad, et valimiste veebiserverisse on paigaldatud sobiva konfiguratsiooniga seadistusfail, mille vorming on kirjeldatud dokumendis „Elektroonilise hääletamise protokollistik III: Kontrollprotokoll“ jaotises 5.
3. Operaatorid võtavad HES, HTS ja jälgimisjaama jaoks seadistatud arvutid.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

4. Audiitor kontrollib, et HES, HTS ja jälgimisjaama riistvara on nõuetekohaselt turvakleebistega kaitstud.
5. Operaatorid viivad läbi testid, et veenduda süsteemi toimivuses.
 - 5.1.Operaatorid alustavad HES-is ja HTS-s hääletusperioodi
 - 5.2.Operaatorid, audiitor(id) ja soovi korral ka vaatlejad saavad anda proovihääli. Audiitor dokumenteerib antud hääled. Veendutakse kontrollrakenduse toimimises.
 - 5.3.Hääletusperiood lõpetatakse, HTS-is minnakse üle lugemisperioodi.
 - 5.4.Hääled loetakse kokku vastavalt käesoleva dokumendi jaotisele 6.4. Audiitor kontrollib hääletustulemuse vastavust antud häältega.
 - 5.5.Operaatorid viivad HES tagasi algolekusse vastavalt dokumendi "E-valimised. Süsteemiülema juhend" jaotisele 7.3.
 - 5.6.Operaatorid kustutavad logid jälgimisjaamast.
 - 5.7.Operaatorid lõpetavad HTS-i valimised ning seadistavad selle uuesti vastavalt käesoleva dokumendi jaotisele 4.5.
6. Operaatorid arvutavad valijarakenduste kontrollsummad, koodisigneerimise ja veebiserveri sertifikaadi sõnumilühendid ning koostavad kuulutuse avaldamiseks üleriigilises ajalehes vastavalt Joonisel 1 toodud näitele. Lisaks publitseerivad operaatorid EHK esimehe poolt digitaalselt allkirjastatud kuulutuse veebilehel.
7. Operaatorid pitseerivad HES, HTS ja jälgimisjaama arvutid turvakleebistega
8. Pitseeritud arvutid ladustatakse turvaalal vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika"

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |



Vabariigi Valimiskomisjon

Andmed 2011. a Riigikogu valimiste e-hääletamise süsteemi tervikluse kontrollimiseks

Veebiserveri <https://www.valimised.ee> sertifikaadi sõnumilühend:
14 9e 6f c4 c7 59 39 16 40 dc a5 f0 dd 00 4f 07 c9 72 be c9

Valijarakenduse Windowsi versiooni signeeritud sertifikaadi sõnumilühend:
4c ad a1 bb af 26 f2 74 b8 53 a3 5f 82 72 30 d8 d5 77 c1 04

Valijarakenduse Linuxi versiooni kontrollsumma:
SHA1: 73534440bd0ccab15de5113db9581dc353db471b

Valijarakenduse Linuxi 64-bitise versiooni kontrollsumma:
SHA1: 4e5056dcc65de8045ea39c575e27d562f7969df4

Valijarakenduse Mac OS X versiooni kontrollsumma:
MD5: f9c9fc8cb2d1ad7fab981033d6b34ad4

Andmete kasutamise kohta saab lisateavet aadressilt:
www.valimised.ee/kontroll.html

Vabariigi Valimiskomisjon

Joonis 1. Näide publitseeritud kontrollsummadest

4.8. *Serverite ülespanek majutuskohta**

HES, HTS ja jälgimisjaam viiakse majutuskohta, paigaldatakse ja ühendatakse.

Transpordi turvalisuse ja usaldusväärsuse tagamiseks pitseeritakse transporditavad serverid kinni audiitori kontrolli all. Kasutatakse turvakotte ja turvakleebiseid, mis on nummerdatud ja mida ei saa kasutada kaks korda, jätmata kergesti tuvastatavaid jälgi.

Enne transporti registreerib audiitor pitseerimisel kasutatud turvakleebiste numbrid ja kontrollib nende õigsust pärast transporti.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid, Riigikogu Valveteenistus või Politsei- ja Piirivalveamet

Partner: majutusteenuse pakkuja

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): kesksüsteemi haldaja ning teenusepakkuja

Toimingud

1. Operaatorid kontrollivad teenusepakkuja valmisolekut ning asjakohasel juhul lepingute kehtivust ja teenustasude maksmist.
2. Vähemalt kaks päeva enne ülespanekut käivad operaatorid teenusepakkuja juures ja kontrollivad andmesideühenduse vastavust nõudmistele. Operaatorid kontrollivad ka turvameetmete (sealhulgas tulemüüri sätete) vastavust nõudmistele.
3. Riigikogu Valveteenistuse Vanem korraldab HES, HTS ja jälgimisjaama transpordi majutuskoha.
4. Audiitor kontrollib serverite pitseeritust ja turvakleebiste/kottide numbrite vastavust registreeritud numbritele.
5. Operaatorid paigaldavad serverid ja ühendavad vastavalt vajadusele.
6. Operaatorid katsetavad võimalust mööda kõiki lepingus sätestatud teenuse parameetreid, sealhulgas andmeside ühendust, tulemüüri sätteid jne.
7. Operaatorid eemaldavad HES veebiserveri privaatvõtmelt parooli, kasutades käsku

```
openssl rsa -in hes.key -out uus_hes.key
```

8. Operaatorid muudavad võrgu ümberhäälestuseks faile:

```
/etc/default/ntpdate
/etc/hosts
/etc/network/if-pre-up.d/iptables
/etc/network/interfaces
/etc/rsyslog.d/*-syslog.conf
```

9. Operaatorid korraldavad süsteemi prooviläbimise majutuskohas alustades HES-is ja HTS-s hääletusperioodi, andes ühe hääle, veendudes selle kontrollitavuses ning seejärel viivad HES-i ja HTS-i tagasi algolekusse.

4.9. Rünnete jälgimine ja vastumeetmed

Partnerite abiga jälgitakse võimalikke ründeid kasutajate arvutitele ja kesksüsteemile, pöörates eriti tähelepanu massilistele rünnete kasutajate arvutite vastu. Kasutusele võetakse vastumeetmed; kui need ei ole enam võimalikud, peatatakse e-hääletamine.

Luuakse formaalsed ja mitteformaalsed suhted ekspertide ja huvilistega, kes jälgiksid ründeid "ründelõksude" – tavalist valijaarvutit imiteerivate ebapiisavalt kaitstud arvutite abiga, millelt perioodiliselt tehakse e-hääletamise tegevusi.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Ründelõksude abil on soovitatav teha kõiki e-hääletamise tegevusi, näiteks ühenduse võtmine valimiste veebisaidiga, e-hääletamise perioodil rakenduse laadimine ja hääletamine, korduvhääletamine jne. Märkus: kui rünne on korraldatud spetsiifiliselt konkreetse e-hääletamise jaoks, siis pole tulemüürist, viirusetõrje vahenditest või nuhkvara tõrjest tõenäoliselt abi.

Eriti hoolikalt tuleb jälgida ründeid ja võimalikke kasutajate arvutite hõivamisi e-hääletamise toimumise ajal. Märkus: suuremahuline rünne, mille jooksul hõivatakse suurem osa halvasti kaitstud arvutitest, võib toimuda päevadega või tundidega, seepärast on soovitatav teha kontrolle mitu korda päevas.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Kesksüsteemi monitoorija, kesksüsteemi operaatorid, EHK

Partnerid: CERT-EE, teenusepakkuja, välised eksperdid ja huvilised

Kontrollija ja kontrolli tase: audiitor hindab tegevusi ja tulemusi omal valikul.

Aeg: enne e-hääletamise starti ja kogu e-hääletamise perioodil

Toimingud

1. Kesksüsteemi monitoorija jälgib ründeid CERT-EE, teenusepakkuja ja teiste allikate abiga.
2. Rünnete, vigade või kõrvalekaldumiste korral tegutsevad operaatorid vastavalt intsidentide halduse põhimõtetele (vt dokument "E-hääletamise süsteemi infoturbe poliitika").
3. Kui suuremahuline rünne kasutajate arvutitele on olnud edukas ja võib prognoosida, et suur osa e-hääletajate arvutitest on hõivatud, informeerivad operaatorid kohe EHK-i, et vajadusel katkestada e-hääletamine.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

5. Hääletamiseperioodi protseduurid

5.1. ***E-hääletamise alustamine

Alustatakse e-hääletamisega.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: majutusteenuse pakkuja

Kontrollija ja kontrolli tase: audiitor teeb koos operaatoritega läbi tegevused omal valikul.

Asukoht/infrastruktuur: majutusteenuse pakkuja ruumid

Toimingud

1. HES võimaldab e-hääletamise alustamist automaatselt, kui see on seadistatud vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 4.1.5. Käsitsi on võimalik e-hääletamist alustada lõpetades HES seadistusperioodi vastavalt dokumendi "E-valimised. Süsteemiülevaade juhend" jaotisele 4.2.1.
2. Operaatorid lõpetavad HTS seadistusperioodi vastavalt dokumendi "E-valimised. Süsteemi ülevaade juhend" jaotisele 5.2.1. Selle toiminguga võib teha ka enne hääletamisperioodi algust.
3. Veebilehed www.valimised.ee serveris muudetakse nii, et tekib link allalaaditavatele valijarakendustele.

5.2. ***Valijate nimekirja täiendamine, varukoopiate tegemine

Pärast e-hääletamise algust saab valijate nimekirja isikuid lisada ja ka kustutada, kui põhjuseks on kas tõkendi rakendamine või jaoskonna vahetus.

Tekitatakse valijate täiendava nimekirja fail koos kontrollsummaga. Faili tekitamine toimub AS Andmevaraga kokku lepitud veebipõhise postkasti kaudu.

Nimekirja täiendamine algab vastavalt AS Andmevaraga sõlmitud kokkuleppele hetkest, mil kokkulepidud töötajale on laekunud teade nimekirja ülespaneku kohta.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Kesksüsteemi operaatorid, andmevahetuse korraldaja

Partnerid: Rahvastikuregistri volitatud töötaja, majutusteenuse pakkuja

Kontrollija ja kontrolli tase: audiitor.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Toimingud

1. Andmevahetuse korraldaja laeb alla täiendava nimekirja ning kirjutab välisele andmekandjale koos kontrollsummaga.
2. Operaatorid uuendavad valijate nimekirja vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotistele 4.1.4 ja 5.1.1.
3. Operaatorid varundavad HES ja HTS vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 7.3.
4. Operaatorid säilitavad varukoopiaid turvalises kohas.

5.3. *E-hääletamise lõpetamine**

Lõpetatakse e-hääletamine.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: teenusepakkuja

Kontrollija ja kontrolli tase: audiitor.

Asukoht/infrastruktuur (vajadusel): teenusepakkuja ruumid

Toimingud

1. HES võimaldab e-hääletamise lõpetamist automaatselt, kui see on seadistatud vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 4.1.5. Manuaalseks lõpetamiseks toimitakse järgmiselt:
 - 1.1.E-hääletamiseks seadusega ette nähtud perioodi lõppemisel alustavad operaatorid hääletamisperioodi lõpetamisega vastavalt "E-valimised. Süsteemiülevaht juhend" jaotisele 4.2.1. Seejärel oodatakse mõistku ajaperioodi vältel (10-15 minutit).
 - 1.2.Operaatorid lõpetavad HES hääletusperioodi vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 4.2.2.
2. Operaatorid lõpetavad HTS hääletusperioodi vastavalt dokumendi "E-valimised. Süsteemiülevaht juhend" jaotisele 5.2.1.

5.4. *Serverite avarijärgne taaste**

E-hääletamisega seotud serveritest tehakse regulaarselt varukoopiaid. Serveri rikke korral paigaldatakse ja ühendatakse uus server ja seejärel taastatakse andmed (sealhulgas vastuvõetud hääled) varukoopiast. Üldsust teavitatakse kaotatud häälest.

Taaste kiiremaks toimumiseks on valmis pandud varuserver, mille töövalmis seadmiseks on vaja paigaldada asendatav süsteem (HES/HTS). Seejärel tuleb paigaldada varukoopiast seadistus ja HTS korral ka talletatud hääled.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Kesksüsteemi operaatorid, Avaliku suhtluse korraldaja, EHK, EHK esimees, VVK

Partnerid: majutusteenuse pakkuja

Kontrollija ja kontrolli tase: audiitor.

Asukoht/infrastruktuur (vajadusel): majutusteenuse pakkuja ruumid

Toimingud

1. Operaatorid võtavad varuserveri
2. Audiitor veendub varuserveri turvakleebiste korrektsuses
3. Operaatorid paigaldavad varuserverile asendatava süsteemi tarkvara (HES / HTS)
4. Operaatorid taastavad varukoopiatelt süsteemi konfiguratsiooni ja e-hääletamise andmed varuserverile vastavalt dokumendi "E-valimised. Süsteemiülema juhend" jaotisele 8.3.
5. Operaatorid ühendavad varuserveri süsteemi riknenud serveri asemele.
6. Operaatorid teevad proovihääletamise teel kindlaks, kas server töötab korrektselt.
7. Operaatorid selgitavad välja ajavahemiku, mille jooksul võisid e-hääled kaotsi minna ja teavitavad sellest EHKi esimeest.
8. Avaliku suhtluse korraldaja valmistab VVK'le ette selgituse toimunu kohta
9. EHK teeb ettepaneku antud olukorras e-hääletamisega jätkamiseks või peatamiseks

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

6. Hääletamisejärgse perioodi protseduurid

6.1. ***Serverite tagasitoomine

HES ja HTS serverarvutid tuuakse majutuskohast tagasi VVK halduses olevatesse ruumidesse.

Transpordi turvalisuse ja usaldusväarsuse tagamiseks pitseeritakse transporditavad serverid kinni audiitori kontrolli all. Kasutatakse turvakotte ja turvakleebiseid, mis on nummerdatud ja mida ei saa kasutada kaks korda, jätmata kergesti tuvastatavaid jälgi.

Enne transporti registreerib audiitor pitseerimisel kasutatud turvakleebiste numbrid ja kontrollib nende õigsust pärast transporti.

HES enam tööle ei panda, HTS kasutatakse e-hääletanute nimekirja printimiseks, e-häälte tühistamiseks ja e-häälte lugemisele viimiseks. HTSi ei ühendata enam Internetiga.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid, Riigikogu Valveteenistus või Politsei- ja Piirivalveamet

Partner: majutusteenuse pakkuja

Kontrollib: audiitor

Asukoht/infrastruktuur (vajadusel): kesksüsteemi haldaja ning teenusepakkuja

Aeg: kohe pärast e-hääletamise perioodi lõppu, peale protseduuri ***E-hääletamise lõpetamine.

Toimingud

1. Operaatorid teevad varukoopia HTS olekupuust. Varukoopia transporditakse ja säilitatakse turvaliselt eraldi HTS serverarvutist.
2. Audiitor pitseerib varukoopia, HES, HTS ja jälgimisjaama serverid ning registreerib kasutatud turvakleebised/kotid.
3. Riigikogu Valveteenistuse Vanem organiseerib HES, HTS ja jälgimisjaama transpordi majutuskohast VVKsse.
4. Audiitor kontrollib serverite pitseeritust ja turvakleebiste/kottide numbrite vastavust registreeritud numbritele.

6.2. E-hääletanute nimekirja eksportimine

Organisatsioon: e-hääletamise kesksüsteemi haldaja

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Täitjad (rollid): kesksüsteemi operaatorid

Partner: Valimiste Infosüsteem

Kontrollija ja kontrolli tase: audiitor teeb koos operaatoritega läbi tegevused omal valikul.

Toimingud

1. Operaatorid ekspordivad e-hääletanute nimekirja vastavalt juhistele dokumendis "E-valimised. Süsteemiülevaht juhend" p.5.2.3.
2. EHK esimees allkirjastab nimekirja digitaalselt.
3. VIS administraator kannab andmed üle valimiste infosüsteemi.

6.3. *E-häälte tühistuste kogumine ja e-häälte tühistamine**

Organisatsioon: E-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid, VVK, VVK volitatud tühistaja

Partner: Valimiste Infosüsteem

Kontrollib: audiitor

Aeg: valimispäeval pärast kella 16.00

Eeltingimused: Volituste andmine tühistus- ja ennistusnimekirjade laadijatele vt "E-valimised. Süsteemiülevaht juhend" jaotis 5.3.1 on tehtud. E-hääletanute nimekiri on prinditud ning saadetud valimisjaoskondadesse.

Toimingud

1. VVK annab jaoskonnakomisjonidele korralduse, et hiljemalt kell 12:00-ks on kõigi jaoskondade kohta tühistusinfo VISi sisestatud.
2. VVK volitatud tühistaja kogub VIS vahendusel kõigi jaoskondade tühistusinfo ning allkirjastab selle digitaalselt e-hääletamise süsteemi importimiseks.
3. Operaatorid impordivad tühistusavalduste ja tühistamise ennistusavalduste failid HTSi ning teostavad tühistamised ja ennistamised vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotistele 5.3.2 ja 5.3.3.
4. Operaatorid ja audiitor viivad läbi vaheauditi vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotisele 5.3.4.
5. Operaatorid lõpetavad tühistusperioodi vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotisele 5.3.5.

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

6. Operaatorid ekspordivad loendamisele minevad hääled DVD-kettale vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotisele 5.3.6.

6.4. *Hääle kokkulugemine**

Hääle lugemine toimub võrgust eraldatult ehk vallasrežiimis. Hääled pärinevad HTSist ja imporditakse välisel andmekandjal. Lugemine eeldab, et turvamoodul (HSM) on ühendatud serveriga ning serverisse on sisestatud turvamooduli konfiguratsioon.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid, turvamooduliga seotud rollid, EHK esimees

Partner: puudub

Kontrollib: audiitor

Aeg: pärast tühistamisi ja ennistamisi

Toimingud

1. Kesksüsteemi operaatorid impordivad e-hääled vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotistele 6.2.1 ja 6.2.2, kasutades hääle tühistamise protseduuri tulemusena saadud DVD ketast.
2. Kesksüsteemi operaatorid loevad e-hääled kokku vastavalt juhendi "E-valimised. Süsteemiülevaht juhend" jaotisele 6.2.3.
3. Kesksüsteemi operaatorid sirvivad hääletamistulemust vastavalt vajadusele, jälgides juhendi "E-valimised. Süsteemiülevaht juhend" jaotist 6.2.4.
4. EHK esimees allkirjastab hääletamistulemuse faili digitaalselt.

6.5. *E-hääletamise tulemuse failide ülekanne valimiste infosüsteemi**

VVK poolt kokku loetud e-hääled tuleb lisada kõigile teistele häälele. Protseduur teostatakse valimispäeval kella 19.00–20.00 vahel (Euroopa Parlamendi valimistel 23.00–24.00 vahel), et valla- ja linnakomisjonid (kui tegu on kohalike valimistega, arvutatakse tulemus valla/linna tasandil) saaksid VISi abil välja arvutada oma valla või linna valimistulemuse ja selle avalikustada veebis pärast kella 20.00 (Euroopa Parlamendi valimistel pärast kella 24.00)

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid, VIS administraator

Partner: Valimiste Infosüsteem

Kontrollib: audiitor

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Aeg: valimispäeval pärast häälte kokkulugemist

Toimingud

1. Operaatorid ekspordivad andmed häältelugemisrakendusest välisele andmekandjale.
2. VIS administraator impordib tekitatud valimistulemuste failid Valimiste Infosüsteemi, andes ette tulemuste ja kontrollsummafailide nimed.

6. 6. *Logifailide kontrollimine**

Valimispäevale järgneval päeval kontrollitakse logifailide terviklust ning vajadusel analüüsitakse muid serverites sisalduvaid andmeid.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: Valimiste Infosüsteem

Kontrollib: audiitor

Aeg: valimispäevale järgnev päev

Toimingud

1. Operaatorid ekspordivad logifailid log4 ja log 5 HLR-st välisele andmekandjale.
2. Operaatorid ekspordivad logifailid log1, log2 ja log 3 HTS-st välisele andmekandjale.
3. Operaatorid kontrollivad logide kooskõllalisust auditirakenduse abil
4. Vajadusel analüüsitakse muid serveris olevaid andmeid.
5. Kontrolli tulemuste kohta koostab komisjon akti, mille allkirjastab komisjoni esimees. Akt esitatakse Vabariigi Valimiskomisjonile.

6. 7. *Võtmepaari hävitamine**

Võtmepaari hävitamine toimub uue tühja partitsiooni loomise ja selle varundamise teel.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): turvamooduliga seotud rollid

Partner: Vabariigi Valimiskomisjon

Kontrollib: audiitor

Aeg: pärast vaidlustusperioodi lõppu

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Toimingud

Täitjad järgivad juhendi "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhhis" jaotist 1.4.

6.8. *Krüpteeritud e-häälte hävitamine**

Krüpteeritud e-hääled ja nende kõik koopiad tuleb turvaliselt kustutada, et neid ei saaks taastada ega kasutada tulevikus. Selleks tuleb koguda kokku ning kustutada turvaliselt kõik koopiad (nii kõvakettad kui välised andmekandjad) kõigist e-hääletamisel antud krüpteeritud häälest vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika".

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): Vabariigi Valimiskomisjoni esindaja, EHK esimees, kesksüsteemi operaatorid

Partner: Vabariigi Valimiskomisjon

Kontrollib: audiitor

Aeg: pärast vaidlustusperioodi lõppu

Toimingud

1. Operaatorid koguvad kokku kõik registreeritud koopiad.
2. Operaatorid hävitavad koopiad füüsiliselt. Kõvakettal olevad andmed tuleb esmalt kustutada, kirjutades nende iga sektori viis korda üle juhuslike andmetega, seejärel kõvaketas sobilike seadmetega hävitada.

6.9. *SSL serverite ja koodisigneerimise salajaste võtmete hävitamine**

Valimiste veebisaidi SSL serveri ja koodisigneerimise salajaste võtmete kõik koopiad hävitatakse. Selleks tuleb vastavalt dokumendile "E-hääletamise süsteemi infoturbe poliitika" koguda kokku ning kustutada turvaliselt kõik koopiad SSL serveri ja valijarakenduse koodi signeerimise salajastest võtmetest.

Märkus: Teatavatel juhtudel (järjestikused valimised jne) võib osutada otstarbekaks nimetatud salajaste võtmete säilitamine. Sellisel juhul tuleb salajased võtmed säilitada vastavalt e-hääletamise infoturbe poliitikale.

Organisatsioon: e-hääletamise kesksüsteemi haldaja

Täitjad (rollid): kesksüsteemi operaatorid

Partner: puudub

| | | |
|--------------------------|-----------|------------|
| E-hääletamise süsteem | Versioon: | 1.9 |
| E-hääletamise käsiraamat | Kuupäev: | 29.01.2015 |

Kontrollib: audiitor

Aeg: vaidlustusperioodi lõppemisel

Toimingud

1. Operaatorid kogub kokku kõik võtmete ja nende osade registreeritud koopiad.
2. Operaatorid hävitavad koopiad füüsiliselt.