Riigi valimisteenistuse 13.09.2017 korralduse nr 10 LISA

Riigi Valimisteenistus

E-hääletamise süsteemi infoturbe poliitika

Versioon 1.0

Dokument: IVXV-TP-1.0

Kuupäev: 13.09.2017.a.

Redaktsioonide ajalugu

Kuupäev	Versioon	Kirjeldus ja muudatused	Autor
13.09.2017	1.0	Koostatud ja vastu võetud dokument	Epp Maaten

Sisukord

1. Sissejuhatus

1.1 Käesolev infoturbe poliitika määratleb e-hääletamise süsteemi infoturbe eesmärgid ning üldised kaitsepõhimõtted. Poliitika eesmärk on anda infoturbele juhtkonnapoolne suunamine ja tugi vastavalt õigusaktidele ja muudele eeskirjadele ning tagada süsteemi turvalisus e-hääletamise käigus.

1.2 Infoturbe poliitika rakendusala on e-hääletamise organisatsioon ja e-hääletamisega seotud infotehnoloogilised süsteemid. Poliitika lähtub järgmistest dokumentidest:

- elektroonilise hääletamise raamistik „IVXV“;
- Vabariigi Valimiskomisjoni (edaspidi VVK) otsus nr 28 "Tehniliste nõuete kehtestamine elektroonilise hääletamise üldpõhimõtete tagamiseks";
- VVK otsus nr 25 "Elektroonilise hääletamise organisatsiooni kirjeldus".

2. Mõisted

- e-hääletamise süsteem – süsteem interneti teel hääletamiseks ja häälte kokku lugemiseks. E-hääletamise süsteemiga on hääletamisperioodil seotud süsteemi välised tuvastus-, allkirjastamis- ja registreerimisteenused ning klienditugi .
- Korraldaja, Koguja, Töötleja, Lugeja ja Klienditoe rollid on kirjeldatud elektroonilise hääletamise raamistikus „IVXV“ ning rollide täitjad on määratud punktis 2 VVK otsuses nr 28.
- kriitilised riskid on e-hääletamise tulemuste ebakorrektsus, e-hääletamise tulemuste ebausaldusväärsus, hääletamise katkemine, hääle salajasuse rikkumine, sh võtmerakenduse salajase võtme avalikuks saamine või sellele juurdepääsu kaotamine.
- kriitilised andmed –andmed, mille volitamatu muutmine või hävinemine võib viia e-hääletamise kriitiliste riskide realiseerumiseni. Andmete allikat peab saama tõestada kolmandale osapoolele ja nende tervikluse turvaosaklass ISKE järgi on T3 (vt Lisa 2).
- kriitilised seadmed – seadmed, mis töötlevad kriitilisi andmeid.
- intsident – sündmus, millega kaasneb andmete või muude infovarade käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib oht nende kadumiseks.
- kogumisteenus - serveriteenus, mis aitab hääletajal e-häält moodustada (väljastab hääletajale kandidaatide nimekirja, abistab digiallkirjastamisel), võtab vastu e-hääli ning registreerib e-hääled enne salvestamist e-urni.
- e-urn – Koguja kokku kogutud e-hääled, mille põhjal tehakse kindlaks hääletamistulemus.
- töötlemisrakendus – tarkvara, mille abil Töötleja kontrollib häälte individuaalset terviklust ja e-urni terviklust, tühistab hääli, väljastab hääletanute nimekirjad ning ringkondade kaupa rühmitatud anonüümistatud hääled.

- miksimisrakendus – tarkvara, mille sisendiks on ringkondade kaupa rühmitatud anonüümistatud krüpteeritud hääled ning mis väljastab segatud hääled nii, et neid ei ole võimalik sisendiga vastavusse viia.
- auditirakendus – tarkvara, mis võimaldab Audiitoril kontrollida Lugeja ja miksimisrakenduse töö korrektsust.
- võtmerakendus – tarkvara, millega Korraldaja genereerib iga hääletamiskorra jaoks häälte salastamise ja häälte avamise võtme. Võtmerakenduse abil toimub ka häälte lugemine ja tulemuse väljastamine.
- valijarakendus - tarkvara, mis töötab hääletaja arvutis, suhtleb kogumisteenusega ning võimaldab hääletajal luua e-hääle, seda krüpteerida ja digitaalselt allkirjastada.
- kontrollrakendus - tarkvara, mis võimaldab hääletajal nutiseadet kasutades veenduda, et tema e-hääl jõudis e-urni ning väljendas tema tahet korrektselt.

3. Turvaeesmärgid

3.1 E-hääletamise turvaeesmärk on tagada valimiste üldpõhimõtete täitmine:

- valimiste vabaduse tagamine;
- valimiste üldisuse tagamine;
- valimiste ühetaolisuse tagamine;
- valimiste salajasuse tagamine.

Üldpõhimõtted ja nende tagamismeetodid on kirjeldatud VVK otsuse nr 25 punktides 1-23 ja IVXV raamistikus.

3.2 Lisaks üldpõhimõtetele kehtivad järgmised turvaeesmärgid:

- e-hääletamise süsteem peab vastama Eestis kehtiva ISKE turvastandardi H-taseme nõuetele (vt Lisa 1. ISKE turvaklassi määramine e-hääletamise süsteemile ning Lisa 2. Infovarade spetsifikatsioon). Süsteemi turvaklass on K2T3S3. E-hääletamise organisatsiooni kuuluvad osapooled lähtuvad oma rolli täitmiseks vajalike e-hääletamise infovarade haldamisel Lisas 2 toodud turvaklassist.
- e-hääletamise süsteemis teostatavad protsessid peavad olema täielikult verifitseeritavad - protsesside sisendit ja väljundit saab omavahel matemaatiliselt kõrvutada.
- Korraldaja peab avalikustama e-hääletamise kesksüsteemi, kontrollrakenduse ja auditirakenduse lähtekoodi. Valijarakenduse lähtekoodi ei avalikustata (p 29 VVK otsus nr 25).
- e-hääletamise süsteem peab kasutama sobivat ja ajakohast krüptograafiat, võttes aluseks ajakohased krüptoalgoritmide turvalisusuuringud.
- auditeerimise- ja vaatlemisvõimalused peavad olema tagatud ning süsteem peab olema tehniliselt piisavalt lihtne, et seda saaks auditeerida võimalikult lai ring spetsialiste. Audiitor teostab süsteemi tervikluse kontrollimiseks protsessi- ja andmeauditeid. Audiitoriga samadel alustel võivad vabatahtlikkuse alusel sarnaseid kontrolliprotseduure võivad läbi viia ka vaatlejad. Korraldaja

avalikustab enne e-hääletamise algust valijarakenduse, kontrollrakenduse ning valimiste veebilehe autentsuse ja tervikluse tagamiseks vajalikud andmed.

- kriitiliste seadmete ja andmete kaitse peab olema rakendatud sõltumatult nende asukohast. Kriitilistele seadmetele ja andmetele tuleb anda juurdepääs ainult tõendatud vajaduse alusel. E-hääletamise kesksüsteemi riistvara ja tarkvara kasutatakse hääletamisperioodil ainult otseselt e-hääletamise läbiviimiseks vajalike ülesannete täitmiseks, kõik muud kasutusviisid on keelatud.

4. Turbe organisatsioon

4.1 E-hääletamise organisatsiooni üleüldine turvapoliitika, e-hääletamise infoturbe poliitika ja e-hääletamise süsteemi turvapoliitika on koondatud käesolevasse dokumenti. Muud infoturbega seotud dokumendid vormistatakse vajadusel eraldi dokumentidena ning dokumentidega saab tutvuda põhjendatud vajadusel.

4.2 E-hääletamise organisatsiooni kuuluvad osapooled on sätestatud VVK otsuse nr 28 punktides 2 kuni 5. Osapoolte vahelised kohustused fikseeritakse soovitavalt täiendava lepinguga või mõnel muul Korraldaja poolt sätestatud moel. Kui osapooled kasutavad Lisas 2 loetletud infovarasid, jälgivad nad, et infovarale rakendatavad turvameetmed on kooskõlas Korraldaja kehtestatud nõuetega ja ISKE standardiga. Osapoolte vaheline suhtluskanal peab olema turvaline.

4.3 Infoturbe eest vastutab e-hääletamise juht. Vajadusel asendab juhti kohusetäitja, kes kinnitatakse Korraldaja otsusega. E-hääletamise juht määrab vajadusel teised infoturbega tegelevad rollid.

4.4 E-hääletamise korraldamiseks, sh infoturbetegevuste koordineerimiseks, moodustab Korraldaja rakkerühma. Rakkerühma juhib e-hääletamise juht, kelle ülesandeks on teavitada e-hääletamise rollide täitjaid õigusaktidest ja muudest Korraldaja poolt vastuvõetud dokumentidest tulenevatest turvanõuetest. Korraldaja korraldab seadusekohast e-hääletamist takistavate juhtumite lahendamise (vt 9 ptk).

4.5 Häälte avamise võtmega seotud protsesse sooritatakse vähemalt kahe rakkerühma liikme koostöös ning nende toimingute juures viibib audiitor. E-häälte kokkulugemise juures peab viibima vähemalt kolm Korraldaja määratud isikut ja vähemalt pool VVK koosseisust.

4.6 Korraldaja hoolitseb selle eest, et e-hääletamise süsteemi teabele või infotöötlusvahenditele juurdepääsu või nende töötlust või haldamist sisaldavad lepped hõlmavad kõiki asjassepuutuvaid turva- ja konfidentsiaalsusnõudeid. Koguja peab igaks hääletamiskorraks ette valmistama infoturbega seotud tehnilise dokumentatsiooni.

4.7 Korraldaja annab VVK-le infoturbe ülevaateid. Regulaarne ülevaade antakse iga hääletamiskorra lõpus. Ootamatult tekkivate infoturbeprobleemide korral või riskide tõttu, mis tulenevad uutest tehnilistest arengutest, võib tekkida vajadus lisaks regulaarsetele infoturbearuannetele anda vajadusepõhine infoturbe ülevaade. Ülevaated on infoturbele antava hinnangu andmiseks vajalike otsuste tegemise aluseks.

4.8 Turvameetmete pideva asjakohasuse tagamiseks on vajalik turvameetmete ja nõuete perioodilised läbivaatused, igapäevane töökeskkonna seire, infoturbe perioodiline

vastavusekontroll, muudatustele reageerimine ja intsidentide käsitlus. Personal peab olema teadlik turvapoliitika sätetest ning muudest turvanõuete rikkumise tagajärgedest.

4.9 Iga hääletamiskorra tarbeks määrab Korraldaja audiitori, kes teostab protsessi- ja andmeauditeid. Protsessiauditeid kohaldatakse toimingutele, mis on seotud häälte avamise võtme loomise, kasutamise ja hävitamisega. Andmeauditiga kontrollitakse valimispäevale järgneval päeval protsesside sisendi ja väljundi omavahelist kooskõla ning protsesside käigus digitaalselt allkirjastatud andmete terviklust ja autentsust. Audiitoril on õigus saada Klienditoelt ülevaade hääletajate probleemidest. Koguja võimaldab audiitori ligipääsu süsteemile, füüsilistele objektidele ning auditeerimiseks vajalikule dokumentatsioonile.

5. Riskianalüüsi strateegia ja turbe vastavuse kontroll

5.1 Riigi valimisteenistus tagab e-hääletamise süsteemi riskide halduse ning määratleb riskide juhtimise metoodika, aruandekohustuse ja kontrollmehhanismid. Riskide hindamine peab kaasnema iga olulise muudatusega e-hääletamise infosüsteemis või protsessides.

5.2 E-hääletamise süsteemile rakendatakse ISKEt, mis on kohustuslik etalonturbe standard riigiasutustele.

5.3 Punktis 3 nimetatud e-hääletamise süsteemi turvaeesmärke peab arvesse võtma e-hääletamise süsteemi arendamisel ja tarkvaras muudatuste tegemisel.

5.4 Kogumisteenus rajatakse igaks hääletamiskorraks lähtudes asjakohastest ISKE H-taseme meetmetest.

5.5 Korraldaja koostab igaks hääletamiskorraks e-hääletamise süsteemi testimise ajakava ja ulatuse ning testimise tulemused ja avalikustab tulemuste raporti. Testimise läbivad soovitavalt kogumisteenus, valijarakendus, valimiste veebileht ja kriitilised seadmed ja varukoopiad kriitiliste andmetega.

6. Võtmehaldus

6.1 Võtmehaldusest sõltub valimiste põhinõuete - valimise salajasuse, ühetaolisuse ja vabaduse - täitmine. Vastavalt VVK otsusele nr 25 kasutatakse e-häälte salastamisel ElGamali krüptosüsteemi jäägiklassirühmas mooduli pikkusega vähemalt 2048 bitti või sama turvataset pakkuvas elliptkõverate rühmas.

6.2 Enne elektroonilise hääletamise algust loob Korraldaja koos VVK-ga e-häälte salastamise võtme ja häälte avamise võtme. Võtmepaari genereerimist korraldavad mitu võtmehaldurit koos.

6.3 Ligipääsuvahendid häälte avamise võtmele jaotatakse VVK liikmete ja Korraldaja vahel. Võtmehalduritele antakse häälte avamise võtme aktiveerimiseks võtmeosakud (näiteks kiipkaardid).

6.4 Häälte avamise võtme aktiviseerimiseks on vaja mitme võtmehalduri koostööd. Häälte avamise võtme aktiveerimise ja häälte lugemise juures peab viibima vähemalt kolm Korraldaja määratud isikut ja vähemalt pool VVK koosseisust. Võtmehaldurid

kasutavad häälte avamise võtme aktiveerimiseks neile võtmepaari genereerimise käigus jagatud autentimisvahendeid. Võtmerakendus dekrüpteerib ainult anonüümseid e-hääli, kust on eemaldatud isikuandmed.

6.5 Pärast ebavajalikuks muutumist, st vähemalt üks kuu pärast hääletamise lõppu või pärast kaebuste menetluse lõppu, hävitatakse häälte avamise võti.

6.6 Võtmehalduse toiminguid, sealhulgas võtmepaari ja paroolide genereerimist, häälte avamise võtme säilitamist, kasutamist võtmerakenduses ning hävitamist, auditeerib audiitor.

7. Pääsu reguleerimine ja seadmete turve

7.1 Tagamaks juurdepääs tõestatud vajaduse alusel, rakendatakse füüsilisi (pääsu reguleerimine, turvakleebiste kasutamine, füüsiline volitustõend, nt kiipkaart) ja loogilisi piiranguid (turvaline sidekanal, autentimine). Kriitilisi andmeid ja seadmeid tuleb kaitsta nii füüsiliste kui loogiliste piirangutega. Muid andmeid tuleb kaitsta kas füüsiliselt või loogiliselt.

7.2 Hääletaja tuvastamiseks e-hääletamise süsteemis kasutatakse isikutunnistust ja digitaalset isikutunnistust, sealhulgas mobiil-ID vormis digitaalset isikutunnistust.

7.3 E-hääletamise operaatorite, rakenduste ja veebilehe administraatorite tuvastamiseks kasutatakse virtuaalset privaatvõrku ja juurdepääsutõendeid.

7.4 Kõigilt operaatoritelt, administraatoritelt ja kolmandatelt isikutelt tuleb nende töösuhte, lepingu või kokkuleppe lõppemisel võtta infovarale ja töötlusvahenditele juurdepääsu õigused, töösuhte, lepingu või kokkuleppe muutumisel aga need õigused kohandada.

7.5 Hääletamisperioodil paikneb H-taseme serverite süsteem andmekeskuseks mõeldud sihtotstarbelistes ruumides, mille turvameetmete valikul on lähtutud ISKE moodulist 2.4 Serveriruum või samaväärsest standardist.

7.6 Korraldaja säilitab tõendid e-hääletamise süsteemi rakenduste lähtekoodi tervikluse kohta. Lisaks avaldab Korraldaja juhendmaterjalid, mille abil hääletajal on võimalik valijarakenduse ja kontrollrakenduse autentsust ja terviklust kontrollida.

7.7 Võrku kasutavate süsteemide ja rakenduste kaitseks tuleb võrke adekvaatselt hallata. Et vähendada võrkudest tulenevaid riske, on võrguhalduse turbe põhimõte "kõik, mis pole e-hääletamise protseduuride läbiviimiseks otseselt vajalik, on keelatud". E-hääletamise süsteem on kaitstud eraldi tulemüüriga. Võrguühenduse ja tulemüüri konfiguratsioonid lubavad ainult spetsifitseeritud tegevusi, võimalusel kitsendades IP-aadressid, protokollid ja pordid.

7.8 E-hääletamise arvutitele baassüsteemide paigaldamisel, operatsioonisüsteemide turvapaikade laadimisel ja muude teenindusprotseduuride käigus tuleb tagada, et teave pärineb usaldusväärsest ja kontrollitud allikast.

7.9 E-hääletamise süsteemi seadmetevahelise andmevahetuse turvamiseks irdmeedial tuleb kasutada asjakohaseid meetmeid nagu failide digitaalne allkirjastamine või krüpteerimine.

7.10 Andmekandjaid, millel säilitatakse tõendeid või varukoopiaid, tuleb säilitada turvalises keskkonnas, näiteks seifis. Andmekandjad tuleb markeerida ja registreerida, et ei toimuks nende ekslikku kasutamist muude funktsioonide täitmiseks.

8. Varundamine, intsidentide haldus ja logide töötlemise põhimõtted

8.1 Hääletajate allkirjastatud ning krüpteeritud hääled kopeeritakse varundamiseks hääletamisperioodi jooksul. Varukoopiate tegemise sagedus e-hääletamise ajal on vähemalt üks kord päevas. E-hääletamise viimasel päeval tehakse lõplik varukoopia vahetult pärast hääletamisperioodi lõppu.

8.2 Varukoopiate tegemiseks kasutatakse ühekordselt kirjutatavat irdmeediat.

8.3 Varukoopiad ladustatakse turvaliselt originaalandmekandjatest kaugemal.

8.4 Intsidentiks ei loeta hääletajate teabepäringuid ja individuaalseid probleeme, mille lahendamine on Klienditoe pädevuses. Klienditugi registreerib oma andmebaasis kõik laekunud päringud ja probleemid ning nende lahendamise käigu.

8.5 Intsidendist tuleb teavitada rakkerühma liiget, kelle vastutusalasse intsident kuulub, nii kiiresti kui võimalik. Rakkerühma liige on hääletamisperioodil valmis reageerima teadetele viivitamata.

8.6 Intsidendi käsitleja, kelle vastutusalasse intsident kuulub, dokumenteerib intsidendi nii, et kõiki sellega seotud protsesse ja otsuseid oleks võimalik tagantjärele tõendada.

8.7 Intsidentide haldamise põhimõtted ja osapoolte täpsemad rollid sätestatakse eraldi dokumendis.

8.8 Korraldajal on õigus teha VVK-le ettepanek elektroonilise hääletamise mittealustamiseks, peatamiseks või lõpetamiseks kui elektroonilise hääletamise süsteemi turvalisust või töökindlust ei ole võimalik tagada selliselt, et elektroonilist hääletamist saaks läbi viia valimisseaduste nõuete kohaselt. Hääletamise peatamise korral teavitab VVK viivitamata hääletajaid elektroonilise hääletamise peatamisest või uuesti alustamisest. Hääletamise mittealustamise või lõpetamise korral teavitab VVK viivitamata hääletajaid sellest, milliseid hääletamisviise on võimalik e-hääletamise asemel kasutada.

8.9 Kõik tegevused e-häältega registreeritakse logis. E-häältega seotud logisid hallatakse vastavalt asjakohasetele ISKE M-taseme nõuetele.

8.10 Hääletamisprotsessi käigus tekkinud tehnilised logid annab Koguja koos e-urniga üle Korraldajale. Korraldaja võib logide kontrollimiseks kasutada audiitori abi.

8.11 Kolmandatele isikutele võib teaduslikul otstarbel väljastada e-hääletamise süsteemi logisid. Logisid väljastatakse kujul, mis ei võimalda identifitseerida hääletajat.

8.12 Lisaks e-häältega seotud tegevustele logitakse süsteemis muud olulised sündmused nagu veasituatsioonid ja rikked.

8.13 Korraldaja säilitab e-häältega seotud logisid vähemalt ühe kuu jooksul pärast hääletamise lõppu või kuni kaebuste menetluse lõpuni.

LISA 1. ISKE turvaklassi määramine e-hääletamise süsteemile

E-hääletamise eesmärk on võimaldada valijal osaleda valimistel ja rahvahääletusel Interneti teel. Selleks kasutatakse e-hääletamise süsteemi, mis kasutatakse kolmel valimisetapil: hääletamine Interneti teel, e-häälte kokkulugemine ning e-häälte lugemiseks vajaliku võtme hävitamine peale valimistulemuste välja kuulutamist.

Lähtudes ISKE rakendusjuhendist 8.0 on e-hääletamise süsteemi turvaklassid määratud kolmel erineval alusel:

1. seadustest ja lepingutest tulenevad nõuded (vt punkt 1) ;
2. põhitegevuse protsessidest tulenevad nõuded (vt punkt 2);
3. tagajärgede kaalukuse hindamine (kirjeldatud, kui muudab või toetab oluliselt turvaosaklassi).

Õiguslik regulatsioon:

- valimisseadused
  - Riigikogu valimise seadus
  - Kohaliku omavalitsuse volikogu valimise seadus
  - Euroopa Parlamendi valimise seadus
  - Rahvahääletuse seadus
- Avaliku teabe seadus (andmekogude pidamise regulatsioon)
- Isikuandmete kaitse seadus (isikuandmete töötlemise nõuded)
- Vabariigi Valimiskomisjoni (VVK) otsused, sh
  - otsus nr 28 Elektroonilise hääletamise organisatsiooni kirjeldus
  - otsus nr 25 Tehniliste nõuete kehtestamine elektroonilise hääletamise üldpõhimõtete tagamiseks
  - otsus nr 26 Hääletamissedeli ja elektroonilise hääle vormi kehtestamine kohaliku omavalitsuse volikogu valimistel
- VVK 4.mai 2017 otsuses nr 25 sätestatud e-hääletamise raamistik „IVXV“.

	K	T	S
e-hääletamise infosüsteem[1]	2	3	3

[1] Infosüsteemi turvaklass tuleneb komponentide kõrgeimatest turvaosaklassidest.

	ISKE turvaklassid(1+2)			Seadusandlus(1)			Töökorraldus(2)			Tagajärjed		
	K	T	S	K	T	S	K	T	S	K	T	S
e-hääletamise infosüsteem	K2	T3	S3	K2	T3	S3	K2	T3	S3	R2	R3	R3

1. Seadustest ja alamaktidest tulenevad nõuded

a) **Käideldavus**

Valimisseaduste kohaselt algab e-hääletamine 10. päeval enne valimispäeva kell 9.00 ja kestab ööpäevaringselt kuni hääletamise lõpuni 4. päeval enne valimispäeva kell 18.00 (tööaeg 6*24+9=153h). E-hääletamise süsteem peab olema kasutusvalmis hiljemalt 13. päevaks enne valimispäeva. Seadused näevad ette võimaluse e-hääletamise peatamiseks, ennetähtaegseks lõpetamiseks ja mittealustamiseks. E-hääletamise tulemused tehakse kindlaks valimispäeval pärast kella 19.00 ning tulemusi ei avalikustata enne kella 20.00. Seaduse sellise sõnastuse korral võib lugeda piisavaks käideldavuse turvaosaklassiks **K2** (käideldavus suurem või võrdne kui 99% ja väiksem kui 99,9% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 4 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 4 tunniga ja suurem kui 1 tund);

b) **Terviklus**

E-hääletamise süsteem kuvab valijale korrektse kandidaatide nimekirja ja hääletamissedeli. E-hääletamise süsteem peab tagama, et hääletamistulemuste kindlakstegemisel läheb arvesse iga valija kohta üks hääl. Valijal on võimalik elektrooniliselt antud häält muuta. E-hääl koosneb valimiste identifikaatorist ja valija tahteavaldusest, mittevormikohane hääl on kehtetu. Valija kinnitab hääletamist digitaalallkirjaga. Valijarakendus kontrollib kontrollib loodud signatuuri terviklust. Valijal on Kontrollrakendusega võimalik kontrollida, kas tema antud hääle on e-hääletamiseks kasutatud rakendus valija tahte kohaselt e-hääletamise süsteemile edastanud. Valija- ja Kontrollrakenduse autentsust ja terviklust saab kontrollida andmete abil, mille Korraldaja on turvaliselt avaldanud. Kõik Kogujale saadetud e-hääled tuleb registreerida, mille käigus lisatakse häälele ajamärgend. Pärast hääletamise lõppu allkirjastab Koguja e-urni kogutud hääled ning need digitaalselt. Töötleja kontrollib kõikide registreerimise käigus tekkinud ajamärgendite olemasolu e-urni kogutud häälte kogumis.

Lähtudes seaduse nõuetest ning e-hääletamise raamistikus kirjeldatud täiendavatest kontrolliprotseduuritest on tervikluse turvaosaklass **T3** (T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse, ajakohasuse kontroll reaalajas);

c) **Salajasus**

Valija hääletab ise. Valijarakendus salastab valija hääle selliselt, et hääle edastamisel ei ole võimalik näha, kelle poolt valija hääletab. E-hääletamise süsteem peab tagama, et enne e-häälte lugemist eraldatakse valija isikuandmed e-häälest selliselt, et ei ole võimalik tuvastada, milline oli selle valija antud e-hääl. Kui valija e-hääletab mitu korda, tagatakse kõigile e-häältele salajasus. Salajasus tagatakse asümmeetrilise krüptograafia

vahendite abil häälte krüpteerimisega. Igaks hääletamiseks luuakse e-hääletamise süsteemi võtmepaar: e-häälte salastamise võtme ja avamise võtme. Ligipääsuvahendid häälte avamise võtmele jaotatakse Vabariigi Valimiskomisjoni liikmete ja riigi valimisteenistuse vahel. Võtmehalduse protseduuride korrektsusest sõltub hääletamise salajasus ja valija sõltumatus. E-hääletamise süsteemis kasutatvatele valijate nimekirjadele saab ligipääsu vaid Vabariigi Valimiskomisjoni nimetatud vastavaid õigusi omav hääletamise korraldaja.

Lähtudes seadustes kirjeldatud nõuetest on konfidentsiaalsuse turvaosaklass **S3** (salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral).

2. Põhitegevuse protsessidest tulenevad nõuded ei erine seadustest tulenevatest nõuetest.

3. Tagajärgede kaalukuse hindamine

a) Käideldavus - **R2** (intsidendiga kaasnevad olulised kahjud, intsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt olulise takistuse asutuse funktsiooni täitmisele või olulisi rahalisi kaotusi);

b) Terviklus **R3** - kaasnevad väga olulised (missioonikriitilised) kahjud, intsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise või märkimisväärseid häireid riigikorralduses või väga olulisi rahalisi kaotusi.

c) Konfidentsiaalsus **R3** - kaasnevad väga olulised (missioonikriitilised) kahjud, intsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise või märkimisväärseid häireid riigikorralduses või väga olulisi rahalisi kaotusi.

LISA 2. Infovarade spetsifitseerimine

Turvaklass	Infovara	Looja/kasutaja	Kommentaar
K1 T2 S2 (M)	valijate nimekiri ning selle muudatused, e-hääletanute nimekiri, tühistusnimekiri	väline partner (valijate nimekirjad) ja Korraldaja	sisendandmed kogumisteenusele
K1 T2 S0 (M)	ringkondade ja jaoskondade nimekiri, kandidaatide nimekiri	Korraldaja	sisendandmed kogumisteenusele ja võtmerakendusele
K1T3S3 (H(HT HS))	e-urn ehk digiallkirjastatud e-hääled	Koguja/Korraldaja	iga e-hääl digiallkirjastatud hääletaja poolt, e-urn kogumina on digiallkirjastatud ja on kogumisteenuse väljund, e-urn on sisend töötlemisrakendusele
K1T3S3 (H(HT HS))	anonüümsed miksimata e-hääled	Korraldaja	töötlemisrakenduse väljund, sisend miksimisrakendusele.
K1T3S1 (H(HT))	anonüümsed miksitud e-hääled	Korraldaja	miksimisrakenduse väljund, sisend võtmerakendusele
K1T3S1 (H(HT))	registreerimisteenuse väljund	Koguja/Korraldaja	registreerimisteenuse ajamärgendid
K2 T3 S0 (H(HT))	hääletamistulemus	Korraldaja	võtmerakenduse väljund. Lugeja, st Korraldaja ja VVK allkirjastavad kokkulugemise tulemused digitaalselt. Erandlik infovara, mis liigub klassist S2 klassi S0 valimispäeval kell 20:00. (EP valimistel 23:00)
K1 T2 S0 (L)	kesksüsteemi tarkvara (kogumisteenus, kontrollrakendus, töötlemisrakendus, miksimisrakendus, võtmerakendus, auditeerimisrakendus)	Korraldaja/Koguja	Rakenduste kirjeldus saadaval ptk 6 elektroonilise hääletamise raamistikus „IVXV“

Turvaklass	Infovara	Looja/kasutaja	Kommentaar
K1 T2 S2 (M)	valijarakenduse tarkvara	Korraldaja/Koguja	võimaldab hääletajal teha valikut, seda krüpteerida ja digitaalselt allkirjastada. Valijarakendus kuvab QR-koodi.
K2T3S0 (H(HT))	Häälte salastamise võti	Korraldaja/Koguja	Salastamise võti on sisend kogumisteenusele.
K2T3S3 (H(HT HS))	Häälte avamise võti	Korraldaja/Korraldaja	Avamise võtit kasutatakse võtmerakenduses häälte dekrüpteerimiseks. Ligipääsuvahendid häälte avamise võtmele jaotatakse VVK liikmete ja Korraldaja vahel.
K1T3S3 (H(HT))	valimiste kodulehe TLS serveri privaatvõti	Korraldaja	veebileht www.valimised.ee on esmane pöörduspunkt hääletajale valijarakenduse saamiseks
K1T2S2 (M)	e-hääletamise logid	Koguja/Korraldaja	kogumisteenuse logid, digiallkirjastatud Koguja poolt, sisend Korraldajale, kes võib logide kontrollimiseks kasutada Audiitori abi
K0T0S0	anonüümsed e-hääletamise logid	Korraldaja/väline partner	Tagantjärele võib kolmandatele isikutele teaduslikul otstarbel väljastada elektroonilise hääletamise süsteemi logisid. Logid väljastatakse kujul, mis ei võimalda identifitseerida hääletajat.