Riigikogu Kantselei riigi valimisteenistus

Euroopa parlamendi elektroonilise hääletuse toimingute audit

ARUANNE

Jaan Oruaas CISA, ISO27001 juhtiv audiitor
Hillar Põldmaa, CISA, CISM

juuli 2024

Vastavalt FocusIT OÜ ja Riigikogu Kantselei riigi valimisteenistuse vahel 16. mail 2024 sõlmitud lepingule viis FocusIT OÜ läbi 2024. aasta Euroopa parlamendi valimiste elektroonilise hääletuse toimingute auditi.

1 Auditeeritavad toimingud

Juhindudes Riigikogu valimise seadusest ja audit ülesandest jälgisid audiitorid elektroonilise valimise järgmisi tegevusi:
- võtmepaari genereerimine;
- elektrooniliste häälte (edaspidi häälte) avamise võtme kasutamine prooviläbimisel;
- elektroonilise valimiskasti sulgemine koos autentsustõendi loomisega;
- elektroonilise valimiskasti üleandmine RVT-le ja autentsuses veendumine;
- häälte avamise võtme kasutamine esmasel häälte lugemisel;
- häälte avamise võtme kasutamine teistkordsel häälte lugemisel;
- korduvate häälte eemaldamine;
- topelthääletanute häälte eemaldamine;
- häälte anonümiseerimine;
- häälte krüptograafiline segamine;
- häälte lugemine;
- häälte avamise võtme hävitamine.

1.1 Ettevalmistavate toimingute jälgimine

Elektroonilise hääletuse ettevalmistust jälgisid audiitorid vastavalt kinnitatud ja avaldatud juhenditele sealhulgas audiitoritele ja vaatlejatele edastatud juhendile IVXV: E-hääletamise käsiraamat Versioon 0.8[1].

Protsessi käigus kontrolliti:
- kas töötlusprotsesse tehti juhendites ettenähtud ulatuses võrgust lahti ühendatud arvutites ja mälukettal. Kontrolliti arvuti BIOSi, kontrolliti väliste seadmetega WiFi ja Sinihamba ühenduste puudumist ning vaatlusega võimalike lisaseadmete puudumist;
- kas töötlusprotsessid tehti mälukettal;
- kas sisendite laadimine ja väljundite salvestamine tehti DVD-plaadil;
- kas sisendandmed, konfiguratsioonifailid ja väljundid olid kinnitud allkirjadega;
- kas toimingud logiti vastavalt nõuetele.

1.1.1 Võtmepaari loomine

Protsessi käigus jälgiti järgmisi tegevusi:
- mäluketta loomine;
- konfiguratsiooni ja rakenduste import;
- kiipkaartide ettevalmistamine;
- kaardilugejate ühendamine ja nummerdamine;
- võtmepaari genereerimine;
- võtmeosakute kirjutamine kiipkaartidele;
- kiipkaartide toimivuse kontroll;
- avaliku võtme varundamine.

[1] https://www.valimised.ee/sites/default/files/2024-05/RVT%20Korraldus%20nr%2010%20lisa%20%28IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat%2008%29-1.pdf

Loodud võtmeosakute kiipkaardid ja võtme loomiseks kasutatud süsteemiketta sulges audiitor turvakleebistega ning märkis üles turvakleebiste numbrid ja signeeris turvakleebised.

Võtmeosakute loomiseks elektroonilise valimise ettevalmistamisel ja häälte lugemiseks kasutati ainult selleks otstarbeks komplekteeritud arvuteid. Arvutite soetamiseks on RVT-s koostatud juhend „Suure kaitsetarbega arvuti komplekteerimise kord". Arvutite kasutamise riskid on hinnatud ning sellel alusel komplekteerimise peamisteks põhimõteteks on:
- hankida riistvara, mille juhtmevabade ühenduste loomiseks komponendid puuduvad või need on võimalik eemaldada;
- püsivara (BIOS) kontrollsummade kontroll, uuendamine usaldusväärsest allikast;
- kasutada maandatud metallkorpust signaalide summutamiseks;
- kahtluse korral teostada 3-nda osapoole audit riistvarale;
- tarkvara võtta ainult usaldusväärsest allikast, kontrollida sertifikaadi usaldusväärsust ja kontrollsummasid.

1.1.2 Proovihääletus

Euroopa parlamendi valimiste elektroonilise hääletamise prooviläbimine toimus 22. mail 2024 Riigikogu hoones.

Audiitorid jälgisid proovihääletuse käiku. Hääletuseks kasutasid proovihääletajad kolme valijarakendusega arvutit, millel olid erinevad operatsioonisüsteemid ja kasutati erinevaid autentimisvahendeid. Kasutati kontrollrakendust. Proovihääletusel hääletas kaheksa isikut, nendest mitmed testimise eesmärgil korduvalt erinevate autentimisvahenditega. Urni avamisel oli selles 20 häält. Seitse neist olid antud enne proovihääletuse algust ja tühistati. Ühe proovihääletaja hääl tunnistati kunstlikult loodud tühistusnimekirja alusel kehtetuks. Kehtivaid hääli loeti kokku seitse. Audiitor kinnitab, et hääli said samad kandidaadid, kelle poolt testi käigus hääletati. Proovihääletajad veendusid selles ka ise kontrollrakendusega.
Urn avati viie privaatvõtme osakuga. Audiitor tuvastas eelnevalt, et kõigi osalenud võtmeosakute kiipkaartide ja süsteemiketta turvakleebised olid terved. Kasutatud võtmeosakute kiipkaardid ja süsteemiketta sulges audiitor peale kasutamist turvakleebistega ning märkis üles ja signeeris turvakleebiste numbrid.

2 Hääletuse järgsete tegevuste jälgimine

Auditi käigus jälgiti Euroopa parlamendi valimiste elektroonilise hääletuse elektroonilise valimiskasti Riigi valimisteenistusele (RVT) üleandmise protsessi, häälte avamise võtme kasutamist esmasel ja teisel lugemisel ning krüptograafilise segamise toiminguid.

2.1 Auditeeritavad toimingud

Juhindudes Riigikogu valimise seadusest ja audit ülesandest jälgisid audiitorid elektroonilise valimise järgmisi tegevusi:
- elektroonilise valimiskasti sulgemine;
- elektroonilise valimiskasti üleandmine RVT-le;
- häälte avamise võtme kasutamine esmasel häälte lugemisel;
- häälte avamise võtme kasutamine teistkordsel häälte lugemisel;
- korduvate elektrooniliste häälte eemaldamine;
- topelthääletanute elektrooniliste häälte eemaldamine;
- häälte anonümiseerimine;
- häälte krüptograafiline segamine;
- häälte lugemine;
- võtmeosakute ja välise kõvaketta hävitamine.

Protsessi käigus kontrolliti:

- kas elektroonilise valmiskast suleti ja anti üle vastavalt juhenditele,
- kas töötlusprotsesse tehti juhendites ettenähtud ulatuses võrgust lahti ühendatud arvutites ja mälukettal. Kontrolliti arvuti BIOSi, väliste seadmetega WiFi ja Sinihamba ühenduste puudumist ning vaatlusega võimalike lisaseadmete puudumist;
- kas töötlusprotsessid tehti mälukettal;
- kas sisendite laadimine ja väljundite salvestamine tehti DVD/BR-plaatidel;
- kas sisendandmed, konfiguratsioonifailid ja väljundid olid kinnitud allkirjadega;
- kas toimingud logiti vastavalt nõuetele.

2.2 Koguja tegevused

Protsessi käigus jälgiti järgmisi tegevusi:

- elektroonilise valimiskastile juurdepääsu sulgemine ja teenuste sulgemine;
- valmistulemuste kontrollsumma arvutamine;
- valimistulemuste kopeerimine.

Kasutatud arvuti ja irdkandjad suleti audiitor juuresolekul turvakleebistega turvaümbrikutesse.

Valimistulemused anti RVT-le üle nõuetekohaselt irdkandjatel ja turvaümbrikutes. Andmekandjate transporti turvas politsei.

2.3 Elektroonilise valimisskasti vastuvõtmine

Elektroonilise valimiskasti vastuvõtmisel RVT-s kontrolliti järgmist:

- üle antud elektroonilise valimiskasti ja logide sõnumilühendeid, mis olid allkirjastatud RIA esindaja poolt audiitori juuresolekul;
- registreerija poolt kogutud ajatempleid koos allkirjastatud sõnumilühendiga;
- elektroonilise valimiskasti ja ajatemplite kontrollsummade allkirjastajate sertifikaatide õigusust;
- üle antud andmete loetavust, autentsust ja töödeldavust.

2.4 Häälte lugemine

Euroopa parlamendi valimiste elektrooniliste häälte lugemine toimus 9. mail 2024 Riigikogu hoones.

Elektrooniliste häälte lugemisel jälgisid audiitorid vastavalt kinnitatud ja avaldatud juhenditele, sealhulgas audiitoritele ja vaatlejatele edastatud juhendile IVXV: E-hääletamise käsiraamat Versioon 0.8[2] ja IVXV kogumisteenuse haldusjuhend[3].

Häälte lugemiseks valmistati ette kontrollitud konfiguratsiooniga arvuti mäluketas.
Audiitorid jälgisid häälte lugemise käiku.
Elektrooniline valimiskast avati viie privaatvõtme osakuga. Audiitor tuvastas eelnevalt, et kõigi osalenud võtmeosakute kiipkaartide ja süsteemiketta turvakleebised olid terved. Kasutatud

[2] https://www.valimised.ee/sites/default/files/2024-05/RVT%20Korraldus%20nr%2010%20lisa%20%28IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat%2008%29-1.pdf
[3] https://www.valimised.ee/sites/default/files/2024-05/RVT%20korraldus%20nr%2012%20lisa%20%28IVXV-kogumisteenuse%20haldusjuhend%29.pdf

võtmeosakute kiipkaardid ja süsteemiketta sulges ja signeeris audiitor uuesti turvakleebistega ning märkis üles turvakleebiste numbrid.

Elektroonilises valimiskastis avamisel tuvastati selles 157487 elektroonilist häält. 12 häält oli antud enne valimisperioodi ja eemaldati. Järele jäänutest 157 475 oli topelt elektrooniliselt hääletanuid 3627 ehk hääli oli antud 153 848 isiku poolt. Korduvhääletajaid, kes hääletasid nii elektrooniliselt kui ka pabersedeliga oli 578 ehk häälte tühistamise protseduuridega muutusid kehtetuks 578 paberhääletanud elektroonilist häält. Ühe hääletaja elektrooniline hääl ei olnud vormistatud vastavalt nõuetele ja eemaldati. Elektrooniliste häälte lugemisele minevate häälte arv oli 153 269. Häälte lugemisel tuvastati üks elektroonilise hääle vormile mittevastav hääl ja eemaldati. Kokku said kõik kandidaadid 153268 elektroonilist häält.

Korduvate elektrooniliste häälte tühistamine, anonümiseerimine ja elektrooniliste häälte krüptograafiline segamine tehti vastavalt juhendile IVXV: E-hääletamise käsiraamat Versioon 0.8.

2.5 Häälte lugemise kontroll

Euroopa parlamendi valimiste elektroonilise häälte korduslugemine toimus 10. mail 2024 Riigikogu hoones. Korduslugemise käigus kontrolliti juhuvalimiga, kas jaoskondades hääletanute elektroonilised hääled tühistati ja kas kohapeal olnud elektrooniliste hääletajate isikukoode ei olnud tühistusnimekirjades.

Audiitor kontrollis oma kompileeritud audiitorrakendusega oma loodud mälukettal häälte lugemise korrektsust vastavalt auditeerimise suunistele. Eelnevalt vaatas audiitor üle audiitorrakenduse lähtekoodi. Lahknevusi häälte lugemise ja audiitorrakendusega saadud tulemustes ei tuvastatud.

Andmeauditi käigus kontrolliti punktis 1.2 kirjeldatud RVT-s vastuvõetud andmete terviklikkust ja töödeldavust. Kõiki andmeid kasutati andmeauditi sisendina. Audiitorrakendusega kontrolliti elektrooniliste häälte krüptograafilise segamise ja lugemise tõendeid.

3 Krüptograafilise võtme hävitamine

Audiitor jälgis IVXV: E-hääletamise käsiraamatu juhiste täitmist elektrooniliste häälte avamise võtme hävitamisel.

Kõik üheksa võtmeosakute kaarti ja võtme osakute loomiseks ning häälte lugemisel kasutatud väline kõvaketas hävitati füüsiliselt.

Riigi Infosüsteemi Amet esitas aktid kasutatud arvuti kõvaketta ja BR-plaatide hävitamise kohta.

4 Tähelepanekud

Elektrooniliste häälte töötlemisel vajalikud allkirjastamised tuleks samuti kuvada vaatlejatele ja audiitori jaoks suurel ekraanil.

Töötleja juhendis ei olnud eraldi välja toodud täpseid juhiseid, mis on olemas valimiste korraldamise põhimõtetes, elektrooniliste häälte nõuetele mittevastavate „sedelite“ tühistamiseks.

Valimisteenistus järgis elektrooniliste häälte töötlemiseks kasutatavate arvutite soetamise juhendit „Suure kaitsetarbega arvuti komplekteerimise kord“. Kord ei olnud pädeva ametniku poolt kinnitatud. Dokumendi avalikustamisel kaaluda riskide loetelu mitteavalikustamist.

Koos elektrooniliste häälte avamise võtmeosakute hävitamisega hävitati ka kõik häälte lugemisel kasutuses olnud DVD/BR plaadid. Kaaluda tuleks kasutusele võetavate plaatide nimekirja koostamist seejuures arvestades, kas tekkiv halduskoormus on asjakohane.

5 Kokkuvõte

Audiitorid ei tuvastanud võtmepaari loomisel ega proovihääletusel puudusi, mis võiksid takistada elektroonilise hääletamise läbiviimist. Proovihääletuse läbiviijad järgisid toimingutes andmete terviklikkuse ja konfidentsiaalsuse tagamiseks vajalikke turvalisuse nõudeid.

Audiitorid ei tuvastanud elektroonilise valimiskasti sulgemisel ega häälte lugemisel puudusi, mis võiksid kuidagigi mõjutada elektroonilise hääletamise tulemusi. Häälte lugemisel ja järgnevates toimingutes järgiti andmete autentsuse, terviklikkuse ja konfidentsiaalsuse tagamiseks vajalikke turvalisuse nõudeid.

Audiitorid
Jaan Oruaas
CISA, ISO27001 juhtaudiitor

Hillar Põldmaa
CISA, CISM