



Elektroonilise hääletamise protsessi auditeerimine

Tellijä: Riigikogu Kantselei riigi valimisteenistus
Valimised: 2023. aasta riigikogu valimised

LÖPPARUANNE

KPMG Baltics OÜ
16.05.2023



KPMG Baltics OÜ
Narva mnt 5
Tallinn 10117
Estonia

Telephone	+372 6 268 700
Fax	+372 6 268 777
Internet	www.kpmg.ee

Riigikogu Kantselei riigi valimisteenistus
Lossi plats 1a
15165 Tallinn

16. mai 2023

Lp Arne Koitmäe

Vastavalt KPMG Baltics OÜ ja Riigikogu Kantselei riigi valimisteenistuse vahel 10.02.2023 sõlmitud lepingule teostas KPMG Baltics OÜ 2023. aasta riigikogu valimiste elektroonilise hääletuse protsessi auditeerimist.

Edastame Teile 2023. aasta riigikogu valimiste e-hääletuse auditeerimise lõpparuande. Aruanne sisaldab auditeeritud toimingute ülevaadet ja auditi tulemusi.

Auditi käigus juhendasid audiitorid kehtivatest õigusaktidest, kinnitatud ja avaldatud juhendmaterjalidest, audiitoritele ja vaatlejatele edastatud juhendist IVXV: E-hääletamise käsiraamat (versioon 0.7). Samuti küberturvalisuse üldtunnustatud põhimõtetest ja parimatest praktikatest.

Käesolev lõpparuanne on koostatud pärast 2023. aasta riigikogu valimiste elektroonilise hääletuse komisjoni hääletusjärgse perioodi toimingute teostamist. Viimased toimingud viidi läbi 12. mai 2023.

Auditeerimise tulemusena ei tuvastanud audiitorid olulisi kõrvalekaldeid kehtivatest nõuetest.

Lugupidamisega

(allkirjastatud digitaalselt)

Tarmo Toiger
Partner, juhtimisoostamise ja
tehnoloogia valdkonna juht
KPMG Baltics OÜ

(allkirjastatud digitaalselt)

Risto Jürisson, CISA
IT-audiitor
KPMG Baltics OÜ



Sisukord

1	Auditeerimise tehniline korraldus	4
2	Testlõbimine ja proovihääletus	5
3	Elektroonilise hääletamise protsessi auditeerimine 04.03.2023 – 06.03.2023	6
4	Võtmeosakute ja süsteemiketta hävitamine	8

1 Auditeerimise tehniline korraldus

Juhindudes õigusaktidest ja asjakohastest juhendmaterjalidest pöörasid audiitorid tähelepanu eeskätt järgnevale:

- ✓ töötlusprotsessid toimusid juhendites reguleeritud ulatuses võrgust lahti ühendatud arvutis ja mälukettal;
- ✓ töötlusprotsesside läbiviimine toimus juhendites reguleeritud mälukettal;
- ✓ töötlusprotsesside sisendite ja väljundite salvestamine ning kasutamine toimusid juhendites reguleeritud ulatuses DVD-plaadil;
- ✓ olemas olid sisendandmeid kinnitavad allkirjad, konfiguratsioonifailide sisu kinnitavad allkirjad ja väljundite sisu kinnitavad allkirjad;
- ✓ toimingud logiti vastavalt juhendites esitatud nõuetele;
- ✓ võtmeprotseduurid viidi läbi juhendmaterjalidele vastavalt. Võtmeprotseduurideks kasutatud riistvara (võtmeosakud ja süsteemiketas) pitseeriti kinni ja turvakleebised olid terved;
- ✓ juhendites nimetatud ulatuses koostati aruandeid, nende sisu tutvustati vajalikul määral asjasse puutuvatele isikutele;
- ✓ töötlusprotseduuride tulemused olid auditeeritavad auditeerimisvahenditega;
- ✓ järgiti küberturvalisuse üldtunnustatud reegleid.

2 Testlõbimine ja proovihääletus

Riigikogu valimiste (RKV) elektroonilise hääletamise proovilõbimine toimus 15.02.2023-16.02.2023 (aadressil Lossi plats 1a, Tallinn).

E-hääletuse protsessi kontrollisid audiitorid vastavalt kinnitatud ja avaldatud juhenditele sealhulgas audiitoritele ja vaatlejatele edastatud juhendile [IVXV: E-hääletamise käsiraamat \(versioon 0.7\)](#)¹

E-hääletamise seadistamise ja testimise käigus kontrolliti järgmisi tegevusi:

- ✓ süsteemi võtmepaari genereerimine;
 - mäluketta loomine
 - konfiguratsiooni import
 - kiipkaartide ettevalmistamine
 - kaardilugejate ühendamine ja numereerimine
 - võtmepaari genereerimine
 - kiipkaartide testimine
 - avalike võtmete varundamine
- ✓ süsteemi testlõbimine.

Audiitorid jälgisid proovihääletuse käiku, millele eelnevalt olid loodud valijarakendused (erinevate operatsioonisüsteemide jaoks) ja seadistatud kontrollrakendus. Proovihääletusel hääletas viis isikut, nendest kaks korduvalt testimise eesmärgil. Kehtetuid hääli ei olnud, kehtivaid hääli loeti kokku viis (5). Audiitor kinnitas, et hääli said samad kandidaadid, kelle poolt testi käigus hääletati.

Audiitorid ei tuvastanud olulisi puuduseid, mis võiksid takistada e-hääletamise läbiviimist testimise perioodil. Protseduuride käigus kasutati andmete terviklikkuse ja konfidentsiaalsuse tagamiseks turvakleebiseid, mille rikkumatust audiitorid kontrollisid kõikide hääletamisprotseduuride käigus. Süsteemi testlõbimise kohta koostati audiitoripoolne vahearuanne, mis edastati riigi valimisteenusele (RVT).

¹ <https://www.valimised.ee/sites/default/files/2023-02/IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat.pdf>

3 Elektroonilise hääletamise protsessi auditeerimine 04.03.2023 – 06.03.2023

Audiitorid kontrollisid e-hääletuse protsessi vahemikus 04.03 - 06.03.2023 vastavalt kinnitatud ja avaldatud juhenditele sealhulgas audiitoritele ja vaatlejatele edastatud juhendile IVXV: E-hääletamise käsiraamat (versioon 0.7).

04.03.2023 toimus audiitorite juuresolekul koguja poolt töötlejale e-valimiskasti üleandmine. Üleandmise käigus jälgiti, et:

- ✓ koguja poolt töötlejale DVD plaadil üle antud häältega e-valimiskast koos allkirjastatud sõnumilühendiga on kinni pitseeritud ning pakend on terve;
- ✓ sõnumilühendiga failil on kehtiv allkiri ning üleandmise kellaaeg on korrektne;
- ✓ allkirjastatud sõnumilühend on identne häältega e-valimiskastile genereeritud sõnumilühendiga.

05.03.2023 esimese sessiooni ajal toimunud e-häälte tervikluse kontrolli ja korduvhäälte tühistamise käigus jälgiti, et:

- ✓ koguja poolt töötlejale üle antud häältega e-valimiskast koos allkirjastatud sõnumilühendiga on DVD-plaadil ja e-valimiskastile genereeritud lühisõnum on identne eelmisel päeval koguja poolt töötlejale üle antud e-valimiskasti lühisõnumiga;
- ✓ registreerimisteenuse poolt on töötlejale üle antud ajatemplid koos allkirjastatud lühisõnumiga;
- ✓ kogumisteenuses salvestatud e-hääli võrreldi registreerimisteenuses fikseeritud e-häältega ja kontrolliti e-häälte digitaalallkirjade terviklust;
- ✓ e-hääletuse käigus antud korduvad e-hääled ja kehtetu e-sedel tühistati;
- ✓ kordumatute häältega e-valimiskastile genereeritud kontrollsumma digiallkirjastati.

05.03.2023 teise sessiooni ajal toimunud topelthäälte tühistamise, anonüümistamise, miksimise ja kokkulugemise käigus jälgiti:

- ✓ e-häälte hulgast valimispäeval hääletanud valijate e-häälte tühistamist;
- ✓ e-häälte anonüümistamist;
- ✓ e-häälte miksimist koos miksimistõendi genereerimisega;
- ✓ e-häälte kokkulugemist.

06.03.2023 toimunud teistkordse e-häälte kokkulugemise käigus läbiti osaliselt eelmisel päeval toimunud protsess uuesti. Protsessi käigus jälgiti:

- ✓ e-valimiskasti tervikluse kontrolli. Kontrolli käigus võrreldi eelmisel päeval anonüümistatud e-valimiskasti digitaalselt allkirjastatud kontrollsummat uue genereeritud kontrollsummaga;
- ✓ e-häälte miksimist koos miksimistõendi genereerimisega;
- ✓ e-häälte kokkulugemist koos lugemistõendi genereerimisega;
- ✓ kahel päeval loodud kokkulugemistulemuste samasuse kontrolli vastavust.

Audiitorid on teostanud järgnevaid kontrolliprotseduure:

- ✓ avalike võtmete kooskõllalisuse kontroll;
- ✓ hääletamistulemuse allkirja verifitseerimine;
- ✓ e-häälte teisendamise korrektsuse kontroll;
- ✓ e-häälte miksimise korrektsuse kontrollimine IVXV auditirakenduse ja Verificatum'i rakendusega;
- ✓ e-häälte lugemise korrektsuse kontrollimine.

Audiitorid teostasid kontrolliprotseduure sõltumatult kompileeritud vahendite abil, kasutades töötleja poolt antud sisendeid. Audiitorite poolse kontrollimise tulemusena veateateid ei tuvastatud.

Töötleja on audiitoritele edastanud kogumisteenuse aruande ning audiitorid tutvusid aruande ja aruandes välja toodud veateadetega.

4 Võtmeosakute ja süsteemiketta hävitamine

12.05.2023 toimus võtmeosakute, süsteemiketta ja teiste e-valimistega seotud väliste andmekandjate (DVD'de) füüsiline hävitamine. Audiitorid kontrollisid võtmeosakute ja süsteemiketta turvakleebiste terviklust ning jälgisid nende hävitamist.

Teave auditi käigus kasutatud turvakleebiste kohta on toodud aruande Lisas 1.

Lisa 1 Turvakleebiste kasutus

Võtmepaari genereerimise järgselt vahendite sulgemine ja väljastamine (15.02.2023)

Objekt	Kleebis nr	Sulgemise kuupäev	Väljastatud isiku nimi
Kaart 0	6183	15.02.2023	Oliver Kask
Kaart 1	6184	15.02.2023	Olari Koppel
Kaart 2	6185	15.02.2023	Airi Mikli
Kaart 3	6186	15.02.2023	Janek Laidvee
Kaart 4	6187	15.02.2023	Epp Hannus
Kaart 5	6188	15.02.2023	Teet Raidma
Kaart 6	6189	15.02.2023	Dilaila Nahkur-Tammiksaar
Kaart 7	6190	15.02.2023	Indrek Leesi
Kaart 8	6191	15.02.2023	Sandra Elken
Süsteemiketas (SSD)	6192, 6193	15.02.2023	Indrek Leesi
Avaliku võtmega DVD	6195, 6196	15.02.2023	Indrek Leesi

Turvakleebistega vahendite järelevalveahel:

Objekt	Kleebis nr	Sulgemise kuupäev	Kontroll enne avamist	Avamise kuupäev
Kaart 0	6183	15.02.2023	Kleebis terve	16.02.2023
Kaart 1	6184	15.02.2023	Kleebis terve	16.02.2023
Kaart 2	6185	15.02.2023	Kleebis terve	12.05.2023
Kaart 3	6186	15.02.2023	Kleebis terve	05.03.2023
Kaart 4	6187	15.02.2023	Kleebis terve	16.02.2023
Kaart 5	6188	15.02.2023	Kleebis terve	05.03.2023
Kaart 6	6189	15.02.2023	Kleebis terve	06.03.2023
Kaart 7	6190	15.02.2023	Kleebis terve	16.02.2023
Kaart 8	6191	15.02.2023	Kleebis terve	16.02.2023
Süsteemiketas (SSD)	6192, 6193	15.02.2023	Kleebised terved	16.02.2023
Avaliku võtmega DVD	6195, 6196	15.02.2023	Kleebised terved	12.05.2023
Kaart 0	6197	16.02.2023	Kleebis terve	05.03.2023

Kaart 7	6198	16.02.2023	Kleebis terve	06.03.2023
Kaart 8	6199	16.02.2023	Kleebis terve	06.03.2023
Kaart 1	6200	16.02.2023	Kleebis terve	05.03.2023
Kaart 4	6201	16.02.2023	Kleebis terve	05.03.2023
Süsteemiketas (SSD)	6202, 6203	16.02.2023	Kleebised terved	05.03.2023
Kaart 0	6204	05.03.2023	Kleebis terve	12.05.2023
Kaart 1	6205	05.03.2023	Kleebis terve	12.05.2023
Kaart 5	6206	05.03.2023	Kleebis terve	12.05.2023
Kaart 4	6207	05.03.2023	Kleebis terve	06.03.2023
Kaart 3	6208	05.03.2023	Kleebis terve	06.03.2023
Süsteemiketas (SSD)	6209, 6210	05.03.2023	Kleebised terved	06.03.2023
Kaart 7	6211	06.03.2023	Kleebis terve	12.05.2023
Kaart 8	6212	06.03.2023	Kleebis terve	12.05.2023
Kaart 4	6213	06.03.2023	Kleebis terve	12.05.2023
Kaart 6	6214	06.03.2023	Kleebis terve	12.05.2023
Kaart 3	6215	06.03.2023	Kleebis terve	12.05.2023
Süsteemiketas (SSD)	6216, 6217	06.03.2023	Kleebised terved	12.05.2023

12.05.2023 kuupäeval toimunud kiipkaartide avamise hetkel tagastas kaardi nr 8 Arne Koitmäe. Antud kiipkaardi üleandmine Sandra Elkeni hoiult Arne Koitmäele oli vormistatud digitaalselt allkirjastatud avalduse alusel. Korrektselt vormistatud üleandmise-vastuvõtmise akt on esitatud audiitoritele. Teised turvakleebistega suletud vahendid tagastati algselt väljastatud isikute poolt.

Kontakt

Risto Jürisson

IT-audiitor

+372 626 8700

rjurisson@kpmg.com

KPMG Baltics OÜ

Narva mnt 5

10117 Tallinn

Estonia

www.kpmg.com

© 2023 KPMG Baltics OÜ, Eesti osaühing ja Šveitsi ühinguga KPMG International Cooperative ("KPMG International") lepinguliselt seotud sõltumatute ettevõtjate võrgustiku liige. Kõik õigused kaitstud.

KPMG nimi ja logo on registreeritud kaubamärgid või ühingu KPMG International Cooperative ("KPMG International") kaubamärgid.