

Riigi Valimisteenistus
Vabariigi Valimiskomisjon

.10.2026 nr 2-7/26-295/1

Elektroonilise valimise turvalisuse tagamisest

Riigikogu korruptsioonivastase erikomisjoni 26. jaanuari 2026 päevakorras oli e-hääletamise auditeerimise süsteemi lünkade ja turvaohutude arutelu¹. Komisjoni liikmed kuulasid vabas vormis Tarvo Treieri ülevaadet tema teadustöodes kirjeldatud siserünnetest², mille abil sai siseründaja 2025. aasta kohalike omavalitsuste volikogude (KOV) valimistel muuta audiitorile avastamatult hääletustulemusi. Arutelu käigus jäi ebaselgeks kas, kuidas või millal edastati audiitorile Treieri kirjeldatud ründestsenaariumid. Nende edastamise või käsitlemise kohta ei leia viiteid ka audiitori aruannetest³. Samuti ei kajasta aruanded ega auditeerimise ametlik video⁴ audiitori samme nende konkreetsete ja valimistulemuse korrektsuse aspektist kriitilise tähtsusega rünnete välistamiseks.

Valmistudes Riigikogu valimisteks peame oluliseks saada ülevaade elektroonilise valimise turvalisuse tagamisest ja ootame 9. novembriks 2026 vastuseid alljärgnevatele küsimustele:

1. Kuidas ja millal edastati audiitorile Tarvo Treieri kirjeldatud ründestsenaariumid? Palun edastada vastav kirjavahetus.
2. Missuguste konkreetsete sammudega ja millises auditeerimise etapis välistas audiitor 2025. aasta KOV valimistel Treieri teadustöös kirjeldatud ja korruptsioonivastase erikomisjoni liikmetele tutvustatud siseründed, mille abil sai töötusfaasis mõjutada seda, millised elektroonilises valimiskastis olevad sedelid loetakse kokku, tühistatakse või tunnistatakse korduvhäälteks, ning seeläbi seadusevastaselt mõjutatakse valimistulemust? Kui audiitor selliseid kontrole tegi, siis palun osutada täpselt, kus on need dokumenteeritud olemasolevates auditaruannetes või ametlikus videos.

¹<https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/3cf2b10c-2d3e-41b3-af9d-ca0ac9b83d91/>

²<https://ieeexplore.ieee.org/document/11271237>, <https://geenius.delfi.ee/artikkel/120450950/teadlane-pani-eesti-e-haaletuse-proovile-ja-leidis-12-kriitilist-viga-kui-susteemi-ei-parandata-voib-e-haaletus-kinni-minna>

³<https://www.valimised.ee/sites/default/files/2025-10/Vahearuanne%20KOV2025%20e-valimiste%20audit.asice>, <https://www.valimised.ee/sites/default/files/2025-10/Vahearuanne%20KOV2025%20e-valimiste%20audit%20II.asice>, <https://www.valimised.ee/sites/default/files/2025-12/L%C3%B5pparuanne%20KOV2025%20e-h%C3%A4%C3%A4letuse%20audit%2022.12%20I.asice>

⁴<https://youtu.be/c9LAOCCr3UQ>

Tarvo Treier ja Kristjan Düüna kirjeldasid töötlusfaasi siseründeid Riigi valimisteenistusele (RVT) juba 2024. aastal⁵ ja nendest lähtuvalt täiendas RVT internetihääletuse süsteemi 2024. aasta Euroopa Parlamendi valimisteks auditeerimisrakendusega⁶. 26. jaanuari 2026 kohtumisel korruptsioonivastase erikomisjoni liikmetega selgus, et auditeerimisrakendus ei välistanud töötlusfaasi siseründeid ja Tarvo Treier edastas RVT-le 2025. aasta 18. veebruaril ja 12. juunil täpsustatud nimekirja töötlusfaasi siserünnetest. Seda hoidis RVT üle poole aasta enda teada ja avaldas nende kohta avalikult teabe alles 9. detsembril 2025, st üks päev pärast elektroonilise hääletuse andmekandjate hävitamist, mistõttu ei olnud pärast andmekandjate hävitamist enam võimalik nendele talletatud andmete põhjal veenduda, et kirjeldatud siseründeid aset ei leidnud. Kuigi RVT lubas oma teavituses⁷, et siseründeid välistava tarkvaralahenduse töötab RVT välja 2027. aasta valimisteks, ei ole avaldatud lubatud tarkvaralahendust ega testandmeid, mille abil peaks saama "iga IT-teadmistega inimene" veenduda, et hääled loetakse kokku korrektselt.

3. Arvestades, et töötlusfaasi siseründed olid RVT-le teada juba 2024. aastal, kuid 2025. aasta KOV valimistel kasutatud auditirakendus ei kõrvaldanud kirjeldatud riske ning samal ajal ilmnis auditirakenduses ka tarkvaraviga⁸, siis kuidas tagab RVT, et need riskid on 2027. aasta Riigikogu valimisteks tegelikult kõrvaldatud või piisavalt maandatud ning et kõigi teadaolevate asjakohaste ründestsenaariumide avastatavus on sõltumatult kontrollitud? Ootame sellele küsimusele ammendavat vastust koos selgitava dokumentatsiooniga, sh lubatud tarkvaralahenduse lähtekood ja testandmed, probleemi algpõhjuse analüüs ja täiendatud ohumudel, parandusmeetmete tegevuskava ning võetud meetmete sõltumatu hindamise tulemused.
Juhul, kui niisuguseid dokumente ei ole koostatud või vastav teave sisaldub muudes dokumentides, palume esitada olemasolevad asjakohased dokumendid, mis võimaldavad sõltumatult hinnata tuvastatud probleemide algpõhjuseid, nende lahendamiseks kavandatud ja rakendatud meetmeid ning nende tulemuslikkust. Kui vajalik dokumentatsioon või analüüs puudub, palun seda selgesõnaliselt märkida ning selgitada, milliste tegevustega ja mis tähtjaks tagatakse vajaliku analüüsi tegemine, dokumenteerimine ja meetmete tulemuslikkuse kontroll.
4. Kuidas on tagatud, et avastatavad on ka Tarvo Treieri teadustöös kirjeldamata töötlusfaasi või muude faaside siseründed, mida on käsitlenud nt Anto Veldre⁹? Kas RVT on kõnealuste juhtumite põhjal hinnanud ka oma turvariskide tuvastamise, käsitlemise ja eskaleerimise protsessi toimivust ning kas hindamise käigus tuvastati puudusi riskijuhtimises, arenduse ja auditeerimise korralduses või vastutuse jaotuses? Palume edastada vastava hindamise tulemused ning otsused protsesside

⁵<https://digikogu.taltech.ee/et/Item/50cabbbc-37e7-47f9-9711-940054bd2bfe>,
<https://ieeexplore.ieee.org/document/10811882>

⁶<https://github.com/valimised/ivxv/blob/v1.9.10-EP2024/auditor/src/main/java/ee/ivxv/audit/tools/IntegrityTool.java>

⁷<https://www.valimised.ee/et/e-haaletamise-auditeerimine-saab-koostoos-teadlastega-taas-taienduse>,
<https://www.valimised.ee/et/e-haaletamine-turvaline-ning-pohjalikult-auditeeritud>

⁸<https://github.com/infoaed/korduva-kryptogrammi-juhtum>

⁹<https://www.riigikogu.ee/tegevus/dokumendiregister/toimik/70208eba-fb7a-4524-9438-03ceb224f924/>

parandamiseks. Kui niisugust hindamist ei ole tehtud, siis ootame selgitusi, miks ei ole peetud vajalikuks analüüsida probleemi kordumise põhjuseid ka organisatsiooni tegevuse ja juhtimise tasandil ning milliste meetmetega tagatakse, et samalaadsed puudused ei kordu.

5. Tarvo Treier on oma 2025. aasta septembris avaldatud teadustöös¹⁰ näidanud, et Eesti elektroonilise hääletuse süsteemis saab valija oma hääle metaandmete, ID-tehingute logide ja valijate nimekirja päringu abil välistele osapooltele tõendada, milline elektrooniline hääle oli tema viimane ehk kehtiv hääle. See võimaldab valijale survet avaldada ja tema hääletamisvalikut kontrollida ega ole kooskõlas demokraatlike valimiste põhimõtetega. T. Treier pakub oma teadusartiklis lahenduseks logikirjete peitmist koos vastavate seadusemuudatustega, hääle allkirjastamist ID-kaardiga võrguühenduseta režiimis või valimistel eraldiseisva digitaalse identiteedi kasutamist, millega ei kaasneks valijasundi võimaldavat hääle salajasuse riivet. Kuna valimistel alates 2023. aastast on eri valijad seda meetodit oma hääle tõendamiseks praktiliselt demonstreerinud¹¹, siis ei ole tegu hüpoteetilise, vaid tegeliku turvariskiga, mis vajab lahendamist.
6. Millise T. Treieri pakutud või muu lahenduse on RVT otsustanud 2027. aasta Riigikogu valimisteks kasutusele võtta välistamaks elektroonilise hääle kehtivuse tõendamise abil valijale surve avaldamine ja tema hääletamisvaliku kontrollimine? Palume esitada lahenduse valiku põhjendused, asjakohane riskianalüüs, rakendamise ajakava ja tehniline dokumentatsioon ning kirjeldatud riski käsitlemise tulemuslikkuse sõltumatu hindamise tulemused, mis võimaldavad veenduda, et risk on piisavalt maandatud või kõrvaldatud. Kui lahendust ei ole valitud või selle rakendamist otsustatud, siis palume seda selgesõnaliselt märkida, põhjendada otsuse puudumist ning esitada tegevuskava koos konkreetsete tähtaegade ja vastutajatega riski käsitlemiseks ning rakendatavate meetmete tulemuslikkuse sõltumatuks hindamiseks.

Lugupidamisega

(allkirjastatud digitaalselt)
Anastassia Kovalenko-Kõlvart
esimees

¹⁰https://link.springer.com/chapter/10.1007/978-3-032-05036-6_12

¹¹<https://docs.google.com/document/d/1AxsiAnCnLUQTm8VXdBBG1Ym2Hr6F53BEaac0DTFWM8>