OTSUS

Tallinn 23.02.2023 nr 54

Märt Põdra kaebuse läbivaatamine

Kaebuse asjaolud

Elektroonilise hääletamise (edaspidi *e-hääletamise*) ettevalmistavad toimingud ja e-hääletamise vaatlemine 2023. a Riigikogu valimisteks toimus järgmiselt:
14.02 kl 10.00 – elektroonilise hääletamise koolitus,
15.02 kl 10.00 – e-hääletamise süsteemi (edaspidi EHS) hääle salastamise võtme (avaliku võtme) ja häälte avamise võtme (privaatvõtme) loomine,
16.02 kl 10.00 – e-hääletamise prooviläbimine.

Vaatlejad osalesid kõigi toimingute juures, osa vaatlejaid kohapeal, osa vaatlejaid jälgis toiminguid MS Teamsi ülekande kaudu. 15.02 alustati EHS-i avaliku ja privaatvõtme loomist. Süsteemi alglaadimiseks ning privaatvõtme salvestamiseks kasutatakse eelnevalt ettevalmistatud kõvaketast. Kell 10.34 küsis Märt Põder Teamsi vestluses, et kas on võimalik uurida lähemalt kõvakettal olevat operatsioonisüsteemi ja tarkvara. Kaebaja tegi ettepaneku teha kõvakettast tõmmise ja teha see kättesaadavaks, et kõik saaksid veenduda süsteemi korrektsuses. Seejuures viitas Märt Põder e-hääletamise käsiraamatu punktile 2.3 „Süsteemi võtmepaari genereerimine“. Seda talle ei võimaldatud.

Kaebuse sisu

Märt Põder esitas 17.02.2023 kaebuse Vabariigi Valimiskomisjonile. Kaebaja vaidlustab süsteemi võtmepaari genereerimise usaldusväärsuse valimiste korraldaja poolt 15.02.2023, kuna vaatlejatele ja audiitoritele ei antud vastavalt e-hääletamise käsiraamatus nõutule võimalust veenduda, et süsteemis ei sisaldu pahavara, mis häälte avamise võtit salvestab või kasutab. Tema palvet eirati kommentaarideta 15.02.2023 ja alles 16.02.2023 sai ta vastuse enne prooviläbimist. Vastuse põhisisuks oli, et pahavara puudumise tuvastamiseks piisab kasutatava kõvaketta pitseerimisprotseduuride visuaalsest vaatlusest ja pitseerimise tõttu ei saa andmed kettalt lekkida. Pahavara võis olla kettale jõudnud juba enne pitseerimist ja esimest kasutamist ametlike valimisprotseduuride käigus. Kuna ketta vormindamise ja tarkvara paigaldamise vaatlemist pole ette nähtud, on võimalik pahavara olemasolu või puudumist elementaarsel tasemel tuvastada vaid kõvakettale juba paigaldatud operatsioonisüsteemi ja rakendustarkvara analüüsides. Ekslik on eeldus, et pahavara eesmärk saab piirduda andmete lekitamisega kettalt – näiteks võib eelnevalt paigaldatud pahavara anda ette genereeritavate võtmete pähe varem ettevalmistatud võtmepaari, mis on n-ö lekkinud juba enne protseduuride algust ning simuleerida kogu protsessi üksnes kasutajaliideses. Ülepea ei ole põhjust piirata pahavara eeldatavat funktsionaalsust lekitamisega, vaid selle eesmärk võib olla manipuleerida võtmepaari genereerimist mõnel muul viisil, nt muutes krüptograafilisi parameetreid selle nõrgestamise eesmärgil. Kui käsiraamatus on sõnaselgelt

öeldud, et pahavara puudumises peab audiitoritel ja vaatlejatel olema võimalik veenduda, siis peab leidma selleks ka võimaluse, eriti kuna võtmepaari genereerimine on valimiste turvalisuse vaatenurgast eriti kriitiline protseduur. Tõenduseks lisas kaebaja kuvatõmmised vaatlemiskeskkonnast.

Riigi valimisteenistuse selgitus

Kaebaja küsimusele vastas Indrek Leesi 16.02 enne prooviläbimise algust (videosalvestuse 0:10:28 – 00:11:50), et seda kõvaketast, mis pitseeritakse, ei ühendata enam ühegi teise seadme külge ega üritata sealt mingeid andmeid kätte saada ja ning see on ka käsiraamatu selle punkti mõte.

E-hääletamise käsiraamatu punkti 2.3 esimene lõik on: „Süsteemi võtmepaari genereerimine on auditeeritav protseduur. Süsteemi võtmepaar genereeritakse eraldi võrgust lahti ühendatud arvutis, millel on eemaldatud sisemised salvestusvahendid (v.a. andmete välisele andmekandjale kirjutamist võimaldav seade) ning mis alglaaditakse väliselt kõvakettalt. Sellisel moel on võimalik audiitoritel ja vaatlejatel veenduda, et süsteemis ei sisaldu pahavara, mis häälte avamise võtit salvestab või kasutab. Kui välist kõvaketast ei kasutata, säilitakse seda turvakleebisega või turvakotis pitseerituna. Mälupulga kasutamine andmevahetuseks selle arvutiga, milles genereeriti süsteemi võtmepaar, on keelatud.“

Kaebaja lähtub lausest, „Sellisel moel on võimalik audiitoritel ja vaatlejatel veenduda, et süsteemis ei sisaldu pahavara, mis häälte avamise võtit salvestab või kasutab“ ning et sellest tulenevalt pidanuks pakkuma vaatlejatele võimalust kõvaketta sisu kontrollida.

Kaebaja viidatud lause ei näe ette toimingu kohustusliku osana vaatlejate poolt kõvaketta kontrollimist, vaid selgitab, miks süsteemi võtmepaar luuakse eraldi võrgust lahti ühendatud arvutis. Seda tehakse süsteemile väljastpoolt ligipääsu välistamiseks, et poleks võimalik süsteemi privaatvõtmest koopiat teha. Seda, et privaatvõti ja avalik võti on moodustatud korrektselt, saab kontrollida kohe prooviläbimisel. Valimistel näitab seda ka lugemistõend. Kui avalik võti on avaldatud, ei saa privaatvõtit enam muuta. Viidatud lõik kirjeldab ka arvutile ligipääsu tingimusi, mis privaatvõtme kaitseks on piiratud.

Märt Põdra taotluse esitamise ajal ei olnud tema taotlust enam võimalik rahuldada, sest võtmete loomise protseduuriga oli 15.02 juba alustatud. Võimalik oleks olnud esitleda taotlus varem. E-hääletamise protseduure ei saa katkestada määramata ajaks vaatlejate soovil, arvestades ka, et kogu e-hääletamise protsess on ajaliselt raamistatud (järgmisel päeval 16.02 oli ette nähtud prooviläbimise läbiviimine).

Kõvakettast lisatõmmise tegemine vaatlejatele tutvumiseks oleks võimalik, kuid seda saab teha enne e-hääletamise toimingute (antud juhul võtmete loomise) algust, mitte selle käigus. Samas ei anna ka kõvaketta tõmmise tegemine vaatlejale täit kindlust, et võtme loomise ajal ei ole arvuti mälus pahavara, mis kas kopeeriks võtit või nõrgestaks seda. Teoorias saab pahavara tekkida ka arvutisse pärast kettakoopia loomist. Et vaatleja saaks olla kindel, tuleks ühendada võtme loomise masina külge ka vaatleja arvuti, mis paralleelselt skaneerib arvutis toimuvat ja jälgib mälu protsesse. Lisaks oleks võimalik teha pärast võtmete loomist privaatvõtmetest koopia ja anda selle vaatlejatele analüüsimiseks, kuid privaatvõtme ja süsteemi rikkumatuse kaitseks ei ole see mõeldav. Teoretiseerides võib olla pahavara peidetud ka DVD lugejasse, kõvaketta kontrollerisse, arvuti emaplaadile jms riistvarasse. Kui keegi väidab, et võti oli loodud nõrgalt, ehk ei kasutanud

piisavat juhuslikkust ja on loodud paralleelne privaatvõti, saab ta seda demonstreerida testhääle avamisega.

Võtmete loomisel kasutatud kõvakettale on installeeritud Microsofti repositooriumist alla laaditud Windows 10 operatsioonisüsteem. Seejärel käivitati arvuti Riigikogu Kantselei arvutivõrgus ning installeeriti saada olevad uuendused**,** kaasa arvatud aktiivse viirusetõrje tarkvara Windows Defender. Arvuti valmistas ette e-hääletamise süsteemi operaator, Riigikogu Kantselei töötaja. Alglaadimisketas ei ole olnud EHS-i penetratsioonitesti skoobis, kuna test hõlmas ainult komponente, millele on ligipääs internetist. Töötlus- ja võtmeloomise arvutitele puudub võrgust ligipääs, mistõttu neid ei pen-testitud. Olemas on varukõvaketas, millest on võimalik kontrollimiseks tõmmis teha, kuid mida ei saa võrrelda juba pitseeritud kettaga, sest sellele ligipääs tuleb välistada.

Tulevikku vaadates saab protseduuri täiendada, kuid sel juhul tuleb määratleda, mida, millal, kuidas ja mis ulatuses kontrollitakse. See maandab riski, et rakendus püüab teha nõrka võtit, manipuleerides juhuarvugeneraatorit. Tagada tuleb, et tulemus oleks usaldusväärne, et tehtud tõmmis vastab võtmeloomise arvutis kasutatavale kõvakettale ja et tõmmise tegemine ei mõjutaks alglaadimisketast ennast.

Vabariigi Valimiskomisjoni seisukoht

1. Vabariigi Valimiskomisjon leiab, et e-hääletamise võtmete genereerimine viidi läbi korrektselt, tehnilisi nõudeid järgides ja käsiraamatus kirjeldatule vastavalt ning nõustub selles osas riigi valimisteenistuse selgitusega.

2. Kaebaja taotlus, mida ta kinnitas ka valimiskomisjoni koosolekul, on tutvuda alglaadimiseks kasutatud kõvaketta sisu koopiaga. Koosolekul selgitas kaebaja täiendavalt, et on nõus ka kõvaketta varukoopiast tehtud tõmmise analüüsimisega. Kuna alglaadimiskettast on loodud varukoopia, tuleb riigi valimisteenistusel teha sellest tõmmis ja võimaldada kaebajal tutvuda selle sisuga riigi valimisteenistuse ruumides kuni võtmetoimingutega seotud andmekandjate hävitamiseni.

Arvestades ülaltoodut ja lähtudes Riigikogu valimise seaduse § 72 lõike 3 punktist 3, Vabariigi Valimiskomisjon otsustab:

1. Rahuldada kaebus osaliselt ning võimaldada kaebajal tutvuda EHS-i privaatvõtme loomiseks kasutatud alglaadimisketta varukoopia tõmmise sisuga valimisteenistuse ruumides kuni võtmetoimingutega seotud andmekandjate hävitamiseni.

2. Muus osas jätta kaebus rahuldamata.

Vastavalt RKVS §-le 72^1 võib huvitatud isik, kes leiab, et Vabariigi Valimiskomisjoni otsusega rikutakse tema õigusi, esitada otsuse peale kaebuse põhiseaduslikkuse järelevalve kohtumenetluse seaduses ettenähtud korras Riigikohtule. Kaebus esitatakse Riigikohtule kolme päeva jooksul Vabariigi Valimiskomisjoni otsuse teatavakstegemisest arvates Vabariigi Valimiskomisjoni kaudu.

(allkirjastatud digitaalselt)
Oliver Kask
Vabariigi Valimiskomisjoni esimees