KPMG

cutting through complexity™

Riigikogu valimiste e-hääletamise protseduuride hindamine

Vabariigi Valimiskomisjon

Heiki Sibul
Riigikogu Kantselei
Lossi plats 1a
15165 Tallinn

Tallinn, 20.04.2011

Lugupeetud Heiki Sibul

Vastavalt KPMG Baltics OÜ ja Vabariigi Valimiskomisjoni vahel 03.02.2011 sõlmitud lepingule viis KPMG Baltics OÜ ajavahemikus 15.02.2011–11.04.2011 läbi Vabariigi Valimiskomisjoni poolt Riigikogu valimiste raames korraldatud e-hääletuse hindamise.

Hindamise läbiviimise eesmärgiks oli kontrollida e-hääletuse läbiviimist vastavalt e-hääletamist reguleerivale dokumentatsioonile. Töö ulatuse ja töö käigus tehtud tähelepanekute ja soovituste kohta esitame Vabariigi Valimiskomisjonile juhtkonnale käesoleva aruande. See aruanne põhineb informatsioonil, mis on saadud kuni 11.04.2011. Aruandes ei kajastata sündmusi ja muudatusi, mis on toimunud pärast antud kuupäeva.

Antud aruanne on suunatud Vabariigi Valimiskomisjonile andmaks kindlust, et Riigikogu valimiste e-hääletus on läbi viidud vastavalt e-hääletamist reguleerivale dokumentatsioonile. Lõpparuanne on mõeldud käsitlemiseks tervikuna, kuna üksikute lõikude avaldamine või edastamine võib moonutada aruande sõnumit.

Lugupidamisega,

(allkirjastatud digitaalselt)

Taivo Epner
Partner

Sisukord

1 Kokkuvõte

Ajavahemikus 15.02.2011–11.04.2011 viis KPMG Baltics OÜ läbi Vabariigi Valimiskomisjoni poolt Riigikogu valimiste raames korraldatud e-hääletuse hindamise. Hindamise läbiviimise eesmärgiks oli kontrollida e-hääletuse läbiviimise vastavust e-hääletamist reguleerivale dokumentatsioonile ja infoturbe heale tavale.

Hindamise tulemusena leidsime, et e-hääletamise protseduurid viidi olulises osas läbi vastavalt olemasolevatele juhenditele ning käsiraamatule ning ei tuvastatud asjaolusid, mis oleksid ohustanud e-hääletuse terviklikkust ja konfidentsiaalsust.

Järgnevas raportis on kirjeldatud e-hääletuse hindamise ulatust ja sisu ning toodud välja e-hääletuse protseduuride ajal audiitorite poolt tehtud tähelepanekud.

2 Töö sisu

2.1 Eesmärk

Vastavalt Vabariigi Valimiskomisjoni (edaspidi VVK) ja KPMG Baltics OÜ (edaspidi KPMG) vahel 03. veebruaril 2011 a. sõlmitud lepingule hindasime ajavahemikus 15.02-11.04.2011 Riigikogu valimistel e-hääletuse läbiviimist. Töö eesmärgiks oli kontrollida e-hääletuse protseduuride käigus tehtavate toimingute vastavust e-hääletuse juhenditele ja käsiraamatule (vt. loetelu peatükis 2.4). Juhenditega katmata olukordade tekkimisel hinnati toimingute vastavust infoturbe heale tavale.

2.2 Ulatus

E-hääletuse protsessi vastavuse kontrolli e-hääletust reguleerivale dokumentatsioonile viisime läbi alljärgnevate etappide ulatuses:

Hääletuseelse perioodi protseduurid:

- E-hääletamise arvutitele baassüsteemide paigaldamine
- Valimiste veebisaidi SSL serveri sertifikaadi hankimine
- Valijarakenduse koodi signeerimise sertifikaadi hankimine
- Valimisjaoskondade ja valikute/kandidaatide failide tekitamine
- Valijate esialgse nimekirja tekitamine
- Riistvaralise turvamooduli (HSM serveri) initsialiseerimine
- Võtmepaari genereerimine ja varundamine
- Valijarakenduse pakendamine
- Häälteedastamisserveri tarkvara paigaldus
- Häälteedastamisserveri häälestus
- Häältetalletamisserveri tarkvara paigaldus
- Häältetalletamisserveri häälestus
- Häältelugemisrakenduse tarkvara paigaldus
- Häältelugemisrakenduse häälestus
- Süsteemi prooviläbimine
- Proovihäälte kokkulugemine
- Süsteemi uus alghäälestus
- Serverite ülespanek majutuskohta

Hääletusperioodi protseduurid:

- E-hääletamise alustamine
- Valijate nimekirja täiendamine
- E-hääletamise lõpetamine

Hääletusjärgse perioodi protseduurid:

- Serverite tagasitoomine majutuskohast Vabariigi Valimiskomisjonile
- E-häälte tühistuste kogumine ja häälte tühistamine
- Häälte kokkulugemine
- E-hääletamise tulemuse failide ülekanne valimiste infosüsteemi
- Võtmepaari hävitamine
- Krüpteeritud häälte hävitamine
- SSL serveri ja koodisigneerimise salajaste võtmete hävitamine.

Protseduuride käigus kasutati andmete tervikluse ja konfidentsiaalsuse tagamiseks turvaümbrikke ja turvakleebiseid, millega tagati seadmete ja andmekandjate füüsiline turvalisus. Info kasutatud turvaümbrikute ja kleebiste kohta on toodud lisas 1.

2.3 Meeskond

Töö viisid läbi alljärgnevad KPMG Baltics töötajad:

- Janno Kase, Manager, CISA, CIA
- Alar Kurvits, Advisor, CISA

2.4 Vastavuse auditeerimiseks kasutatud dokumentatsioon

Töö käigus kontrolliti e-hääletuse protseduuride vastavust järgnevatele dokumentidele:

- EHA-02-01-1.0 E-hääletamise organisatsioon ja infrastruktuur
- EHA-02-03-1.0 E-hääletamise süsteemi infoturbe poliitika
- EHA-03-02-1.6 E-hääletamise käsiraamat
- EHA-03-03-1.14 E-hääletamise süsteem. Süsteemiülema juhend hääleedastusserveri, hääletalletusserveri ja häältelugemisrakenduse operaatorile
- EHA-03-04-2.3 E-hääletamise süsteem. Valija rakenduse pakendamine
- EHA-03-05-2.0 Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Üldosa
- EHA-03-06-2.1 Raudvaralise turvamooduli SafeNet Luna SA haldusjuhend. Tegevusjuhis
- EHA-03-10-3.0 E-hääletamise süsteem. Operatsioonisüsteemi paigaldus
- Kehtetu hääle analüüsi tegevuskava v 1.0

3 Hinnang e-hääletuse läbiviimisele

Leiame, et meie poolt läbi viidud toimingud annavad aluse hinnangu andmiseks e-hääletuse läbiviimisele.

E-hääletamise protseduurid viidi olulises osas läbi vastavalt olemasolevatele juhenditele ning käsiraamatule.

E-hääletuse protseduuride vaatluse käigus leidsime neli juhtumit, millega ei olnud arvestatud e-hääletuse protseduurides ning mille kordumine võib ohustada edaspidiste e-hääletuse sujuvat läbiviimist. Järgnevas on välja toodud nende juhtumite olemus, mõju e-hääletusele ning soovitused olukorra parandamiseks.

3.1 Apache veebiserveri konfiguratsiooni muutmine

24. veebruaril muudeti protseduuriväliselt häälte edastamise serveri (HES) Apache veebiserveri konfiguratsiooni. HES Apache veebiserveri konfiguratsioon oli selline, mis ei lubanud saada HES-ga ühendust Windows operatsioonisüsteemi kasutavaid klientsüsteeme juhul, kui neil oli paigaldamata tarkvara uuendus (http://www.microsoft.com/technet/security/bulletin/MS10-049.mspx). Apache konfiguratsioonis eemaldati trellid rea „SSLInsecureRenegotiation on" eest mis tähendas vastava seadistuse juurest kommentaaride märkide eemaldamist ja seadistuse aktiveerimist. Seadistuse muutmise tagajärjel said HES ühendust ka klientarvutid, kus Windows operatsioonisüsteemil puudus vajalik turvauuendus.

Turvauuenduse puudumine oli kujunenud probleemiks paljudele hääletajatele, millele viitas suur hulk päringuid ID-kaardi infotelefonile. Konfiguratsiooni muudatuse otsuse tegi Tarvi Martens mitteformaalse riskihinnangu alusel.

Leiame, et antud protseduuriväline konfiguratsiooni muudatus ei mõjutanud e-hääletuse turvalisust. Eelmainitud turvaaugu ärakasutamine oleks nõudnud teadlikku ja koordineeritud tegevust. Turvaaugu ärakasutamine oleks viinud olukorrani, kus realiseerub teesklusrünnak (spoofing attack), mille tulemusena valijale jääb mulje, et tema hääl on läinud arvesse, kuid tegelikult ei ole. Oleme arvamusel, et sellise turvaaugu korduv ärakasutamine ei oleks jäänud e-hääletuse läbiviijatele märkamata.

3.2 Vaheauditi käigus esinenud viga olekupuus

Protseduuriliselt on ette nähtud HTS vaheauditi teostamine, mille käigus kontrollitakse serveri andmestruktuuride kooskõlalisust ja talletatud häälte terviklust. Vaheauditi genereerimisel 01.03.2011 ilmus teade - Vigu olekupuus 1. Viga olekupuus esines, kuna üht häält sisalduv failinimi sisaldas sümbolit „?", mis ei ole olekupuu failinimedes aktsepteeritud.

Häälte talletusserver (HTS) talletab häälefaile Linuxi failisüsteemis. Häälefaili nimi koosneb hääle oleku kirjeldusest (kehtiv, tühistatud), kellaajast ja hääletaja andmetest BASE64 kujul. Kodeeritud hääletaja andmed on: nimi, jaoskonna number, ringkonna number ja isiku järjekorranumber algses failis.

Valdavalt on neist andmetest koostatud baidijada lühem kui 57 baiti, ehk BASE64 kodeering mahub 76 tähemärgi sisse. Pikkade isikunimede korral on kodeeritav baidijada pikem kui 57 baiti. BASE64 kodeerimisel tekib mitmerealine kodeering, mis sisaldab erisümbolit '\n'.

Hääli talletav, tühistav, verifitseeriv ja lugemisele saatev kood saab '\n' sümbolit sisaldavate failinimedega hakkama, kuid olekupuu konsistentsuse kontrollimisel kasutatavad regulaaravaldised ei oska '\n' sümboliga arvestada. Selleks, et vastav oskus tekiks, tuli regulaaravaldisi protseduuriväliselt täiendada Pythoni mooduli re.py spetsiifilise muutujaga re.DOTALL. Täiendavat informatsiooni antud muutuja toime kohta saab Pythoni dokumentatsioonist: http://docs.python.org/release/2.5.2/lib/module-re.html

Antud erisus ei takistanud valijatel (korduvalt) e-hääletamast ning hääl läks kokkulugemisel arvesse.

3.3 Häälte verifitseerimise ebaõnnestumine

HTS auditi funktsiooni käigus, mis käivitati 03.03.2011 ning mis verifitseerib e-hääled, ei õnnestunud kahe hääle verifitseerimine.

Nende kahe isiku sertifikaat oli hääle andmise ja auditi funktsiooni käivitamise vahelisel ajal aegunud. Sertifikaadi aegumise tähtaeg on kaasas digitaalallkirjal, millega hääl allkirjastati. Auditi käigus kontrollitakse sertifikaadi aegumise kuupäeva ja juhul, kui see on auditi ajaks aegunud jäetakse hääl verifitseerimata. Verifitseerimata jäänud hääled ei mõjutanud hääletamise tulemust, kuna häälte andmise hetkel olid isikute sertifikaadid kehtivad ning auditi tulemus ei mõjuta häälte kokkulugemist.

Soovitame tulevikus HTS auditi funktsioonidest jätta välja kontroll, mis kontrollib sertifikaadi kehtivust auditi hetkel või muuta kontrolli selliseks, et kontrollitaks sertifikaadi kehtivust hääletamise hetkel.

3.4 Rikutud e-hääl kokkulugemisel

Tulenevalt Riigikogu valimise seadusest ei võimalda e-hääle andmiseks kasutatav Valijarakendus sedeli rikkumist. 06.03.2011 toimunud e-häälte lugemisel tunnistati siiski üks e-hääl kehtetuks, mis tõttu see konkreetne hääl ei kajastunud valimistulemustes. Kuna e-hääl jõudis lugemisele ehk läbis edukalt kõik eelnevad verifitseerimised, dekrüpteerus ilma vigadeta ning kandidaatide nimekirjad HES'is ja HLR'is olid omavahel kooskõlas, jääb järele neli võimalust kehtetu hääle tekkimiseks:

1. viga Valijarakenduses, mis on ümbrikusse pannud vigase andmestruktuuri;
2. viga HES'is, mis on saatnud valijale vigase kandidaatide nimekirja;
3. viga HLR'is, mis on dekrüpteeritud andmeid valesti interpreteerinud;
4. sihilik rikutud e-hääle postitamine konkreetse isiku poolt.

Kuna eeltoodud neljanda võimaluse realiseerumist hinnatakse pigem ebatõenäoliseks, tuleks hääletussüsteemi tulenevalt rikutud e-häälest põhjalikumalt analüüsida. Muuhulgas soovitame, et tulevaste valimiste eel viiakse hääletussüsteemis läbi põhjalikum sõltumatu ülevaatus (sh valijarakenduse koodi läbivaatus), et maandada süsteemi arendajast tulenevaid riske.

Lisa 1. Turvakleebiste kasutamine

Ümbriku (Ü) või kleebise (A) nr	Sisu	Kleepimise aeg	Eemaldamise aeg	Rikkumata?
Ü 2163890	Installimeedia: 7 plaati ja mälupulk	15.02.2011 13:03	15.02.2011 14.03	OK
Ü 867580	HES HDD (2tk)	15.02.2011 13:05	18.02.2011 10.02	OK
Ü 867573	HTS HDD (2tk)	15.02.2011 14:42	18.02.2011 10.04	OK
Ü 867574	Varuserveri HDD (2tk)	15.02.2011 15:20	11.04.2011 13.00	OK
Ü 2163891	Installimeedia: 7 plaati ja mälupulk	15.02.2011 15:25	18.02.2011 10.07	OK
Ü 867578	4 kaameralinti	15.02.2011 15:26	11.04.2011 12.59	OK
Ü 2163862	2 kaameralinti	16.02.2011 12:19	11.04.2011 13.00	OK
A40005840	HLR toide	15.02.2011 15:28	16.02.2011 10.00	OK
A40005839	HLR korpus	15.02.2011 15:28	ei eemaldatud	OK
465688, 465689, 465690	HSM tehase turvakleepsud	HSM tootmisel	ei eemaldatud	OK
A40005837	HSM varutoken	16.02.2011 11:37	11.04.2011 12.46	OK
Ü 867575	HSM varuvõtmed 3tk	16.02.2011 11:38	11.04.2011 13.34	OK
Ü 867577	www, RK2011, koodi sign võtmed	16.02.2011 12:11	18.02.2011 10.06	OK
A40005838	HLR korpus	16.02.2011 12:14	18.02.2011 11.20	OK
A40005835	HLR toide	16.02.2011 12:14	18.02.2011 11.20	OK
A40005836	HSM toide	16.02.2011 12:16	18.02.2011 13.34	OK
Ü 2163864	HTS HDD (2tk)	18.02.2011 13.30	22.02.2011 15.43	OK
Ü 2163863	HES HDD (2tk)	18.02.2011 13.33	22.02.2011 15.43	OK
Ü 2163889	Installimeedia: 7 plaati ja mälupulk x2 ja võti 1 plaat	18.02.2011 14.10	11.04.2011 12.51	OK
Ü 2163888	4 kaameralinti	18.02.2011 14.11	11.04.2011 13.00	OK
A40005824	HSM toide	18.02.2011 14.12	06.03.2011 19.15	OK
A40005845	HLR toitelüliti	18.02.2011 14.13	06.03.2011 19.15	OK
A40005823	HLR toide	18.02.2011 14.13	06.03.2011 19.15	OK
A40005846	Racki põrand	22.02.2011 15.25	02.03.2011 20.35	OK
A40005834	Racki põrand	22.02.2011 15.26	02.03.2011 20.30	OK
A40005822	Racki tagumine külg 1	22.02.2011 16.23	02.03.2011 20.30	OK
A40005821	Racki tagumine külg 2	22.02.2011 16.23	02.03.2011 20.30	OK
A40005820	Racki tagumine külg 3	22.02.2011 16.23	02.03.2011 20.30	OK
A40005819	Racki esimene külg 1	22.02.2011 16.26	24.02.2011 08.45	OK
A40005817	Racki esimene külg 2	22.02.2011 16.26	24.02.2011 08.45	OK
A40005818	Racki esimene külg 3	22.02.2011 16.27	24.02.2011 08.45	OK
A40005811	Racki esimene külg 1	24.02.2011 9.05	24.02.2011 16.04	OK
A40005813	Racki esimene külg 2	24.02.2011 9.05	24.02.2011 16.04	OK
A40005814	Racki esimene külg 3	24.02.2011 9.05	24.02.2011 16.04	OK
Ü 2163882	Varukoopia HTS olekupuu	24.02.2011 16.15	11.04.2011 12.57	OK

A40005812	Racki esimene külg 1	24.02.2011 16.20	25.02.2011 16.05	OK
A40005815	Racki esimene külg 2	24.02.2011 16.20	25.02.2011 16.05	OK
A40005816	Racki esimene külg 3	24.02.2011 16.20	25.02.2011 16.05	OK
Ü 2163887	Varukoopia HTS olekupuu	25.02.2011 16.14	11.04.2011 12.58	OK
A40005825	Rack esimene külg 1	25.02.2011 16.15	26.02.2011 16.02	OK
A40005826	Rack esimene külg 2	25.02.2011 16.15	26.02.2011 16.02	OK
A40005827	Rack esimene külg 3	25.02.2011 16.15	26.02.2011 16.02	OK
Ü 2163883	Varukoopia HTS olekupuu	26.02.2011 1620	11.04.2011 12.58	OK
A40005867	Racki esimene külg 1	26.02.2011 16.20	27.02.2011 15.59	OK
A40005866	Racki esimene külg 2	26.02.2011 16.20	27.02.2011 15.59	OK
A40005828	Racki esimene külg 3	26.02.2011 16.20	27.02.2011 15.59	OK
Ü 2163884	Varukoopia HTS olekupuu	27.02.2011 16.09	11.04.2011 12.56	OK
A40005832	Racki esimene külg 1	27.02.2011 16.10	28.02.2011 16.01	OK
A40005831	Racki esimene külg 2	27.02.2011 16.10	28.02.2011 16.01	OK
A40005830	Racki esimene külg 3	27.02.2011 16.10	28.02.2011 16.01	OK
Ü 2163886	Varukoopia HTS olekupuu	28.02.2011 16.15	11.04.2011 12.56	OK
A40005877	Racki esimene külg 1	28.02.2011 16.16	01.03.2011 15.57	OK
A40005876	Racki esimene külg 2	28.02.2011 16.16	01.03.2011 15.57	OK
A40005829	Racki esimene külg 3	28.02.2011 16.16	01.03.2011 15.57	OK
Ü 2163885	Varukoopia HTS olekupuu	01.03.2011 16.29	11.04.2011 12.55	OK
A40005874	Racki esimene külg 1	01.03.2011 16.31	02.03.2011 16.02	OK
A40005873	Racki esimene külg 2	01.03.2011 16.31	02.03.2011 16.02	OK
A40005875	Racki esimene külg 3	01.03.2011 16.31	02.03.2011 16.02	OK
A40005871	Racki esimene külg 1	02.03.2011 16.17	02.03.2011 19.51	OK
A40005870	Racki esimene külg 2	02.03.2011 16.17	02.03.2011 19.51	OK
A40005872	Racki esimene külg 3	02.03.2011 16.17	02.03.2011 19.51	OK
Ü 2163879	HES HDD (2tk)	02.03.2011 20.31	11.04.2011 11.45	OK
Ü 2163868	HTS tühistusperioodi DVD	02.03.2011 20.32	11.04.2011 13.11	OK
Ü 2163881	HES olekupuu+Apache DVD	02.03.2011 20.32	11.04.2011 12.53	OK
Ü 2163880	HTS HDD (2tk)	02.03.2011 20.32	03.03.2011 11.11	OK
Ü 2163866	HTS HDD (2tk)	03.03.2011 15.37	06.03.2011 17.53	OK
Ü 2163869	Plaadid (3tk) - tühistusnimekiri, tulemus	06.03.2011 20.25	11.04.2011 12.51	OK
A40005833	HLR toitepesa	06.03.2011 20.26	11.04.2011 11.56	OK
A40005841	HLR toitelüliti	06.03.2011 20.27	11.04.2011 11.56	OK
A40005842	HSM toitepesa	06.03.2011 20.28	11.04.2011 12.05	OK
Ü 2163870	HTS HDD (2tk)	06.03.2011 20.30	11.04.2011 12.50	OK

Kontaktisik

Janno Kase
Manager
Tel: +372 6 268 814
Mob: +372 511 29 45
E-mail: jkase@kpmg.com

KPMG Baltics OÜ
Narva mnt 5
Tallinn 10117
ÜId: +372 6 268 700
Fax: +372 6 268 777

www.kpmg.ee