KPMG
cutting through complexity

Riigikogu valimiste e-hääletamise protsessi auditi lõpparuanne

6. mai 2015

Sisukord

1 Kokkuvõte

Vastavalt KPMG Baltics OÜ ja Vabariigi Valimiskomisjoni vahel 18. jaanuaril 2015 sõlmitud lepingule teostas KPMG Baltics OÜ Riigikogu valimiste elektroonilise hääletuse komisjoni toimingute auditeerimist. Auditi eesmärgiks oli kontrollida elektroonilise hääletamise süsteemi testimise, süsteemi tervikluse ja komisjoni toimingute vastavust seadustele, Vabariigi Valimiskomisjoni õigusaktidele ning elektroonilise hääletamise dokumentatsioonile.

Käesolev lõpparuanne on koostatud pärast riigikogu valimiste elektroonilise hääletuse komisjoni hääletusjärgse perioodi toimingute teostamist, viimased toimingud viidi läbi 27. aprillil 2015.

Hindamise tulemusena leidsime, et elektroonilise hääletamise süsteemide ettevalmistamise, hääletamise perioodi ja hääletamisjärgse perioodi protseduurid peatükis 2 kirjeldatud mahus viidi olulises osas läbi vastavalt Elektroonilise Hääletamise Komisjoni poolt kinnitatud juhenditele ning E-hääletamise käsiraamatule. Audiitorid ei tuvastanud olulisi puuduseid, mis võiksid ohustada e-hääletuse protsessi ning tulemuste terviklust ja konfidentsiaalsust.

Käesolevale lõpparuandele on lisatud hindamise käigus ning e-hääletuse protseduuride ajal audiitorite poolt teostatud eritegevuste protokollid.

2 Töö sisu

2.1 Hääletuseelse perioodi protseduurid

E-hääletuse protsessi auditi käigus kontrolliti protseduuride vastavust e-hääletust reguleerivale dokumentatsioonile alljärgnevate etappide ulatuses:

- 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;
- Häälte edastamisserveri (HES) tarkvara paigaldus;
- Häälte edastamisserveri häälestus;
- Häälte talletamisserveri (HTS) tarkvara paigaldus;
- Häältetalletamisserveri häälestus;
- Häältelugemisrakenduse (HLR) tarkvara paigaldus;
- Häältelugemisrakenduse häälestus;
- Süsteemi testimine (prooviläbimine, proovihäälte kokkulugemine);
- Süsteemi uus alghäälestus;
- Serverite ülespanek majutuskohta.

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 aruande lisas 1.

Süsteemide seadistamise lõpptulemuse hindamiseks viidi läbi proovihääletus. Proovihääletuste tulemuste kajastamiseks koostati audiitori poolt protokoll, mis on esitatud antud aruande lisas 2.

2.2 Hääletamise perioodi protseduurid

E-hääletuse hääletamise perioodil kontrolliti protseduuride vastavust e-hääletust reguleerivale dokumentatsioonile alljärgnevate etappide ulatuses:

- elektroonilise hääletamise alustamine;
- igapäevane valijate nimekirja täiendamine ja varukoopiate tegemine;
- elektroonilise hääletamise lõpetamine.

Hääletamise perioodil osales audiitor kõigil majutuskohas igapäevaselt läbiviidavatel valijate nimekirja uuendamise ja andmete varundamise protseduuridel.

Protseduuride käigus kasutati andmete tervikluse ja konfidentsiaalsuse tagamiseks turvakotte ja turvakleebiseid, mis on nummerdatud ja mida ei saa kasutada mitu korda. Audiitor registreeris ja kontrollis jooksvalt pitseerimisel kasutatud turvakottide ja turvakleebiste seerianumbrite õigsust. Info kasutatud turvakottide ja kleebiste kohta on toodud aruande lisas 1.

2.3 Hääletamisjärgse perioodi protseduurid

E-hääletuse hääletamisjärgse perioodi ajal kontrolliti protseduuride vastavust e-hääletust reguleerivale dokumentatsioonile alljärgnevate etappide ulatuses:

- serverite tagasitoomine majutuskohast elektroonilise hääletamise komisjoni;
- elektrooniliste häälte tühistuste kogumine ja häälte tühistamine;
- häälte kokkulugemine;
- elektroonilise hääletamise tulemuste failide ülekanne valimiste infosüsteemi;
- logifailide kontrollimine;
- võtmepaari hävitamine;
- krüpteeritud häälte hävitamine.

Audiitorid osalesid e-hääletamise lõpetamise ja valimispäeval läbiviidavatel hääletamisjärgse perioodi protseduuridel 1. märtsil 2015.

Audiitor osales valimispäevale järgneval päeval logifailide tervikluse kontrollimise protseduuril. Kontrollitud e-hääletamise tulemused signeeriti Elektroonilise Hääletamise Komisjoni esimehe poolt 2. märtsil kell 10:44.

Audiitor osales HSM privaatvõtme ning krüpteeritud häälte hävitamise protseduuril 27. aprillil 2015. Sensitiivseid andmeid sisaldavate serverite kõvakettad hävitati füüsiliselt. Füüsiliselt hävitati ka kõik eelnevate protseduuride käigus DVD-dele tehtud ja turvakleebistega kaitstud varukoopiad. Protseduuri käigus koguti kokku valimiskomisjoni liikmete kätte usaldatud HSM võtmed ja privaatvõtme varukaart.

2.4 Meeskond

Töö viisid läbi alljärgnevad audiitorid:

- Teet Raidma, CISA
- Janno Kase, CISA, CIA, CRISC

2.5 Vastavuse auditeerimiseks kasutatud dokumentatsioon

Elektroonilise hääletamise süsteemi ettevalmistamise käigus kontrolliti e-hääletuse protseduuride vastavust järgnevatele dokumentidele:

- „E-hääletamise organisatsioon ja infrastruktuur“ (versioon 2.0, 09.2013);
- „ E-hääletamise süsteemi infoturbe poliitika“ (versioon 2.1, 02.2015);
- „ E-hääletamise käsiraamat“ (09.2013) (versioon 1.9, 01.2015);
- „E-hääletamise süsteemiülema juhend“ (versioon 1.22.1, 02.2015);
- „Operatsioonisüsteemi paigaldusjuhend“ (versioon 4.3, 01.2015);

- „Valijarakenduse pakendamine“ (versioon 2.5, 04.2014);
- „Raudvaralise turvamooduli üldjuhend“ (versioon 1.3, 09.2009);
- „Raudvaralise turvamooduli tehniline juhend“ (versioon 2.3, 04.2014).
- „RK2015 väljavõetav teave“ (täiendav protseduurijuhend, koostatud 25.02.2015)

3 Elektroonilise hääletuse protseduuride auditi tähelepanekud

E-hääletuse hääletamise perioodi protseduurid viidi olulises osas läbi vastavalt olemasolevatele tehnilistele juhenditele ning E-hääletamise käsiraamatule. Audiitorid ei tuvastanud protseduuride läbiviimise hindamisel sisulisi puuduseid, mis oleksid võinud mõjutada elektroonilise hääletuse protseduuride läbiviimise ja tulemuste usaldusväärsust.

Töö käigus leidsime mõningaid väheolulisi puuduseid protseduuride läbiviimisel ja protseduuride aluseks olevates juhendites, mis vajavad protseduurijuhendite täpsustamist. Samuti tegime tähelepanekuid, kuidas muuta protsessi edaspidi läbipaistvamaks ja paremini jälgitavaks. Sellekohane informatsioon edastati elektroonilise hääletamise komisjonile auditi käigus, väljaspool käesolevat aruannet.

3.1 Auditi tähelepanekud

Järgnevalt toome välja auditi käigus tuvastatud olulisemad tähelepanekud, mille juures tuleb edaspidi kaaluda kirjalike ja kinnitatud protseduuride ja tegelikult läbiviidavate tegevuste vastavusse viimist:

3.1.1 Protseduurimuudatus hääletusperioodi lõpetamisel

Protseduuri käigus tekkis vajadus muuta kinnitatud protseduuri osas, mis puudutab logide plaatidele kirjutamist pärast hääletamisperioodi lõpetamist. Olemasolevat protseduuri täiendati uue juhendiga „RK2015 väljavõetav teave".

Soovitame kinnitada kõik protseduurijuhendid enne protseduuride algust ja tungiva vajaduseta neid mitte protseduuride käigus muuta. Kõik muudatused peaksid saama enne rakendamist elektroonilise hääletamise komisjoni kirjaliku kinnituse.

3.1.2 Irdmeedia kasutamine on reguleerimata

Protseduuri erinevates faasides kasutati andmete ülekandmiseks USB mälupulka. Protseduurijuhendid ei sisalda meetmeid, kuidas tagatakse mälupulga kasutamise turvalisus. Praktikas kasutati üht konkreetset mälupulka, mida ei kasutatud protseduuride vahel muuks otstarbeks.

Soovitame irdmeedia kasutamine e-hääletust puudutavates juhendites täpsemalt reguleerida.

3.1.3 Andmete hävitamise protseduur ei ole läbipaistev

Valimissüsteemi arendusserver (DEV server) võeti valimistulemuste väljakuulutamisele järgneval perioodil ning enne elektrooniliste häälte hävitamise protseduuri taaskasutusse, audiitor ei osalenud turvakleebiste eemaldamise ja kõvaketaste kustutamise protseduuril. DEV server ei sisaldanud tundlikku teavet, seega tundlike andmete lekkimise risk puudus.

E-hääletamise käsiraamatu punkt „6.8 Krüpteeritud e-häälte hävitamine“ kohaselt oleks tulnud kõvaketastel olevad andmed esmalt kustutada, kirjutades nende iga sektor viis korda üle juhuslike andmetega ja siis sobilike seadmetega hävitada. Protseduuri käigus eelnevat kustutamist ei toimunud, kõvakettad hävitati füüsiliselt. Audiitorite hinnangul on see piisav meede takistamaks andmete hilisemat taastamist.

Soovitame parema läbipaistvuse huvides kehtestada kõikide protseduurides kasutavatele serverite ja andmekandjate andmete kustutamise või hävitamise reeglid, mis sätestavad üheselt mõistetavalt, millal, mis meetodil ja kelle poolt andmed kustutatakse või hävitatakse.

Lisad

Lisa 1. Turvaümbrike ja turvakleebiste kasutamine

Ümbriku (Ü) või kleepeka (K) nr	Sisu (seisuga 02.03.2015)	Kleepimise aeg	Kontrollimise / Eemaldamise aeg	Tulemus (rikkumata)
Ü 2138979	tarkvara plaadid	10.02.2015 14:03	10.02.2015 14:50	OK
Ü 2138978	DEV serveri kettad	10.02.2015 14:06	31.03.2015 0:00	vt.ptk 3.1.3
K 4349	testkleepimine	10.02.2015 16:58	10.02.2015 16:59	OK
Ü 2138977	tarkvara plaadid	10.02.2015 17:01	13.02.2015 11:58	OK
Ü 2138976	HES ja HTS serveri kettad	10.02.2015 17:03	13.02.2015 10:34	OK
Ü 2138975	HLR serveri kettad	10.02.2015 17:03	11.02.2015 10:31	OK
Ü 2138974	LOG serveri kettad	10.02.2015 17:04	13.02.2015 10:31	OK
K 4350	HES serveri toide	10.02.2015 17:06	13.02.2015 10:33	OK
K 4351	HTS serveri toide	10.02.2015 17:06	13.02.2015 10:32	OK
K 4352	HLR serveri toide	10.02.2015 17:06	11.02.2015 10:31	OK
K 4353	LOG serveri toide	10.02.2015 17:08	13.02.2015 10:32	OK
K 4354	DEV serveri toide	10.02.2015 17:08	31.03.2015 0:00	vt.ptk 3.1.3
K 4355	HSM varukaart	11.02.2015 11:33	27.04.2015 14:18	OK
Ü 2138972	HLR serveri kettad	11.02.2015 11:41	13.02.2015 10:33	OK
Ü 2138973	salasõnad ja varuvõtmed	11.02.2015 11:44	27.04.2015 14:20	OK
K 4356	HLR serveri toide	11.02.2015 11:47	13.02.2015 10:32	OK
K 4357	HSM toide	11.02.2015 11:49	13.02.2015 14:00	OK
Ü 2138970	HLR serveri kettad	13.02.2015 14:58	1.03.2015 17:58	OK
Ü 2138971	HES ja HTS serveri kettad	13.02.2015 15:00	17.02.2015 15:20	OK
Ü 2138969	tarkvara plaadid	13.02.2015 15:03	2.03.2015 10:20	OK
K 4358	HES serveri toide	13.02.2015 15:04	17.02.2015 15:14	OK
K 4419	HTS serveri toide	13.02.2015 15:04	17.02.2015 15:12	OK
K 4420	HSM toide	13.02.2015 15:05	1.03.2015 17:52	OK

K 4359	HLR serveri toide	13.02.2015 15:06	1.03.2015 17:51	OK
Ü 2138968	HSM admin. parool (ümbrik Tarvi käes)	13.02.2015 15:11	Ei kasutatud	
K 4360	LOG serveri toide	13.02.2015 15:13	17.02.2015 15:10	OK
Ü 2138967	LOG serveri kettad	13.02.2015 15:20	17.02.2015 15:16	OK
K 4361	rack põrand keskel	17.02.2015 16:41	25.02.2015 19:55	OK
K 4362	rack põrand taga	17.02.2015 16:42	25.02.2015 19:55	OK
K 4363	rack põrand ees	17.02.2015 16:43	25.02.2015 19:56	OK
K 4364	rack külg üleval	17.02.2015 16:46	25.02.2015 19:56	OK
K 4365	rack külg all	17.02.2015 16:47	25.02.2015 19:56	OK
K 4366	rack taga üleval	17.02.2015 16:49	25.02.2015 19:56	OK
K 4367	rack taga all	17.02.2015 16:50	25.02.2015 19:56	OK
K 4368	rack taga lukk	17.02.2015 16:51	25.02.2015 19:48	OK
K 4369	rack ees üleval	17.02.2015 16:55	25.02.2015 19:57	OK
K 4370	rack ees all	17.02.2015 16:55	25.02.2015 19:57	OK
K 4371	rack ees lukk	17.02.2015 16:56	19.02.2015 8:40	OK
K 4372	rack ees lukk	19.02.2015 9:09	19.02.2015 15:16	OK
K 4373, 4374	19.02 backup plaat	19.02.2015 15:37	27.04.2015 14:43	OK
K 4375	rack ees lukk	19.02.2015 15:41	20.02.2015 15:07	OK
K 4376, 4377	20.02 backup plaat	20.02.2015 15:31	27.04.2015 14:43	OK
K 4378	rack ees lukk	20.02.2015 15:33	21.02.2015 15:09	OK
K 4379, 4380	21.02 backup plaat	20.02.2015 15:34	27.04.2015 14:43	OK
K 4381	rack ees lukk	21.02.2015 15:36	22.02.2015 15:07	OK
K 4382, 4383	22.02 backup plaat	22.02.2015 16:00	27.04.2015 14:43	OK
K 4384	rack ees lukk	22.02.2015 16:03	23.02.2015 15:06	OK
K 4385, 4386	23.02 backup plaat	23.02.2015 15:48	27.04.2015 14:42	OK
K 4387	rack ees lukk	23.02.2015 15:49	24.02.2015 15:06	OK
K 4388, 4389	24.02 backup plaat	24.02.2015 15:48	27.04.2015 14:42	OK
K 4390	rack ees lukk	24.02.2015 15:49	25.02.2015 15:06	OK

K 4391, 4392	25.02 backup plaat	25.02.2015 15:51	27.04.2015 14:42	OK
K 4393	rack ees lukk	25.02.2015 15:52	25.02.2015 17:55	OK
Ü 2138966	HTS hääletusperioodi eksport	25.02.2015 18:49	27.04.2015 14:41	OK
Ü 2138965	HES serveri kettad	25.02.2015 19:07	27.04.2015 14:55	OK
Ü 2138964	LOG serveri kettad	25.02.2015 19:10	27.04.2015 14:55	OK
Ü 2138963	HTS serveri ketas 1	25.02.2015 19:46	1.03.2015 17:55	OK
Ü 2138962	HTS serveri ketas 2	25.02.2015 19:47	1.03.2015 17:55	OK
K 4398	HES serveri toide	25.02.2015 19:51	27.04.2015 14:59	OK
K 4397	HTS serveri toide	25.02.2015 19:52	1.03.2015 17:53	OK
K 4396	LOG serveri toide	25.02.2015 19:54	27.04.2015 14:58	OK
Ü 2138961	HTS serveri ketas 1	1.03.2015 20:06	2.03.2015 10:20	OK
Ü 2138960	HTS serveri ketas 2	1.03.2015 20:06	2.03.2015 10:21	OK
Ü 2138959	HLR serveri kettad	1.03.2015 20:08	27.04.2015 14:10	OK
K 4394	HTS serveri toide	1.03.2015 20:09	2.03.2015 10:22	OK
K 4395	HSM toide	1.03.2015 20:09	27.04.2015 14:05	OK
K 4399	HLR serveri toide	1.03.2015 20:10	27.04.2015 14:06	OK
Ü 21388958	Hääletamistulemuste plaadid (2 tk	1.03.2015 20:13	2.03.2015 10:31	OK
K 4400	HTS serveri toide	2.03.2015 10:47	27.04.2015 15:00	OK
Ü 2138957	tarkvara plaadid (9 tk)	2.03.2015 10:48	27.04.2015 14:54	OK
Ü 2138956	HTS serveri kettad	2.03.2015 10:47	27.04.2015 14:27	OK
Ü 2138955	HTS logide ja hääletustulemuste plaadid	2.03.2015 10:51	27.04.2015 14:50	OK

Lisa 2. E-hääletuse prooviläbimine ja häälte kokku lugemine

E-hääletuse prooviläbimine viidi läbi e-hääletuseks ettevalmistatud tehnilises keskkonnas 13.02.2015, Vabariigi Valimiskomisjoni ruumes ning valimiskomisjoni liikmete ning vaatlejate juuresolekul ning osalusel. Testitulemused ei kajasta hääletuses osalejate isiklikke hääletuseelistusi kandidaatide valikul. Antud hääled (ajalises järjestuses):

Hääletaja	Valik	Op. süsteem	Meetod	Kehtetu / Kehtiv
Tarvi	733	Windows 7	M-ID	Kehtetu
Tarvi	420	Windows 7	ID-kaart	Kehtetu
Tanel	115	Windows 7	ID-kaart	Kehtetu
Epp	521	Mac OS X	ID-kaart	Kehtiv
Heli	974	Windows 7	ID-kaart	Kehtiv
Uve	970	Linux x64 (Ubuntu 14)	ID-kaart	Kehtiv
Tanel	620	Mac OS X	ID-kaart	Kehtiv
Virgo	119	Windows 7	ID-kaart	Kehtetu
Virgo	536	Windows 7	ID-kaart	Kehtiv
Ulrika	971	Windows 7	ID-kaart	Kehtiv
Dilaila	425	Windows 7	ID-kaart	Kehtiv
Priit	970	Mac OS X	M-ID	Kehtiv
Aare	737	Windows 7	M-ID	Kehtiv
Tarvi	108	Windows 7	M-ID	Kehtiv

Tulemused

- Hääletamisel osales 10 inimest, hääletusperioodi jooksul hääletati koos kordushääletustega kokku 14 korda, arvesse läks 10 häält.
- Käsitsi loetud hääled ühtisid HLR-s loetud häältega.
- Käsitsi loetud kandidaat 970-le antud 2 häält ühtis süsteemist saadud tulemusega.
- Hääletada sai edukalt Windows, Linux ja Mac OS keskkonnast.
- Hääletamise tulemus on kontrollitav erinevate operatsioonisüsteemidega telefonidest.

Kontakt

Teet Raidma
Manager
Tel: +372 6 268 814
E-mail: traidma@kpmg.com

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

www.kpmg.com