ABCD

Vabariigi Valimiskomisjon

E-valimiste läbiviimise hindamine

17. aprill 2007
This report contains 13 pages
Appendices comprise 5 pages
KPMG_VVK_lõppraport

Heiki Sibul
Vabariigi Valimiskomisjon
Lossi plats 1
Tallinn

17. aprill 2007

E-valimiste läbiviimise hindamise lõpparuanne

Vastavalt KPMG Baltics AS ja Vabariigi Valimiskomisjoni vahel 22.12.2006 sõlmitud lepingule viis KPMG Baltics AS ajavahemikus 12.02.2007–9.04.2007 läbi Vabariigi Valimiskomisjoni poolt Riigikogu valimiste raames korraldatud e-valimiste hindamise.

Hindamise läbiviimise eesmärgiks oli kontrollida e-valimiste 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 9.04.2007. Aruandes ei kajastata sündmusi ja muudatusi, mis on toimunud pärast antud kuupäeva.

Lõpparuande levitamine ja avalikustamine kolmandatele osapooltele on piiratud vastavalt Vabariigi Valimiskomisjoni ja KPMG Baltics AS-i vahel sõlmitud lepingu üldtingimustele.

Kontaktisik antud töö puhul on Kitty Mamers (tel. +372 6268743).

Lugupidamisega,

Taivo Epner
Partner

Kitty Mamers
Senior Advisor

Sisukord

1 Kokkuvõte

Ajavahemikus 12.02.2007–9.04.2007 viis KPMG Baltics AS läbi Vabariigi Valimiskomisjoni poolt Riigikogu valimiste raames korraldatud e-valimiste hindamise. Hindamise läbiviimise eesmärgiks oli kontrollida e-valimiste 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-valimiste terviklikkust ja konfidentsiaalsust

Järgnevas raportis on kirjeldatud e-valimiste hindamise ulatust ja sisu ning toodud välja tuvastatud suuremad kõrvalekaldumised e-hääletamise juhenditest.

2 Töö sisu

2.1 Eesmärk

Vastavalt Vabariigi Valimiskomisjoni (edaspidi VVK) ja KPMG Baltics AS (edaspidi KPMG) vahel 22. detsembril 2006 a. sõlmitud lepingule hindasime ajavahemikus 12.02-09.04.2007 Riigikogu valimistel e-valimiste läbiviimist. Töö eesmärgiks oli kontrollida e-valimiste protseduuride käigus tehtavate toimingute vastavust e-hääletuse juhenditele ja käsiraamatule. Juhenditega katmata olukordade tekkimisel hinnati toimingute vastavust infoturbe heale tavale.

2.2 Ulatus

E-valimiste 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 import
Valijate esialgse nimekirja import
Riistvaralise turvamooduli (HSM serveri) initsialiseerimine
Võtmepaari genereerimine ja varundamine
Valijarakenduse pakendamine
Hääleedastamisserveri häälestus
Hääletalletamisserveri häälestus
Häältelugemisrakenduse häälestus
Süsteemi prooviläbimine
Proovihäälte kokkulugemine
Süsteemi uus alghäälestus
Serverite ülespanek majutuskohta

Hääletusperioodi protseduurid:
E-hääletamise alustamine
Valijate nimekirja igapäevane täiendamine
E-hääletamise lõpetamine

Hääletusjärgse perioodi protseduurid:
Serverite tagasitoomine
E-häälte tühistuste kogumine ja häälte tühistamine
Häälte kokkulugemine
E-hääletamise tulemuse failide eksportimine ülekandmiseks valimiste infosüsteemi
Võtmepaari hävitamine
Krüpteeritud häälte hävitamine
SSL serveri ja koodisigneerimise salajaste võtmete hävitamine

Kõigi ülalnimetatud protseduuride jooksul kasutati kriitilise valimisinfo tervikluse kaitseks objektide ja artefaktide ajutist pitseerimist turvakleebistega. Kokkuvõte turvakleebiste kasutamisest on toodud käesoleva aruande Lisas 1.

2.3 Meeskond

Töö viisid läbi alljärgnevad töötajad:

- Kitty Mamers, KPMG Baltics Senior Advisor, CISA
- Janno Kase, KPMG Baltics Senior Advisor, CISA, CIA

2.4 Vastavuse auditeerimiseks kasutatud dokumentatsioon

Töö käigus kontrolliti e-valimiste protseduuride vastavust järgnevatele dokumentidele:

- EHA-03-02-1.3 E-hääletamise käsiraamat
- EHA-03-06-1.1 Raudvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhis
- EHA-03-10-1.5 E-hääletamise süsteem. Operatsioonisüsteemi paigaldus
- EHA-03-04-1.8 E-hääletamise süsteem. Valija rakenduse pakendamine
- EHA-03-03-1.9 E-hääletamise süsteem. Süsteemiülema juhend hääleedastusserveri, hääletalletusserveri ja häältelugemisrakenduse operaatorile
- Apache'i kompileerimine. Uve Lokk, 20.02.2007
- EHA-02-03-1.0 E-hääletamise süsteemi infoturbe poliitika
- EHA-02-01-1.0 E-hääletamise organisatsioon ja infrastruktuur
- EHA-02-02-1.1 E-hääletamise dokumentatsioon
- EHA 02-05-1.0 Nõudmised e-hääletamise majutusteenusele

3 Hinnang e-valimiste läbiviimisele

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

E-hääletamise protseduurid viidi olulises osas läbi vastavalt olemasolevatele juhenditele ning käsiraamatule. Üksikutel juhtudel esines minimaalseid kõrvalekaldeid juhenditest ja käsiraamatust, mis olid põhjustatud juhendite puudulikkusest ning mille mõju ei ohustanud e-valimiste terviklikkust ning konfidentsiaalsust.

E-valimiste protseduuride vaatluse käigus leidsime kaks suuremat kõrvalekallet juhenditest ja käsiraamatutest, mille kordumine võib ohustada edaspidiste e-valimiste sujuvat läbiviimist. Järgnevas on välja toodud nende kõrvalekallete olemus, nende läbi tekkivad riskid ning soovitused olukorra parandamiseks.

3.1 Hääletalletusserveri varundamine

Pärast e-hääletamise lõpetamist 28.02.2007 õhtul ei õnnestunud protseduurides ettenähtud hääletalletusserveri varundamine, kuna varundamiseks kuluv aeg ületas 1 tunni. Hääletalletusserver toodi majutuskohast tagasi ning varundamist alustati uuesti. 01.03.2007 hommikuks oli süsteem moodustanud olekupuu varundusfaili suurusega 997 MB. Süsteem ei võimaldanud sellise suurusega faili andmekandjatele kirjutada, vaid väljastas veateate. Seetõttu varundati hääletalletusserverist vajalikud andmed (sh krüpteeritud hääled) eraldi andmekandjatele käsitsi.

Hääletalletusserveri varundusfaili suurus ning varundamisele kulunud aja pikkus oli tingitud häälte talletamiseks kasutatavast keerukast kataloogistruktuurist.

Eksisteerib risk, et e-häälte hulga suurenemisel ei ole võimalik teostada ka igapäevaseid hääletalletusserveri varundamisi, kuna need võtavad liiga palju aega. See omakorda toob kaasa riski, et hääletalletusserveri hävimisel pole võimalik valijate poolt juba antud hääli taastada ning e-valimised tuleb katkestada ja/või uuesti alustada.

Soovitame muuta häälte talletamise andmestruktuure nii, et varundatavate andmete kogumaht ja seega ka varundamiseks kuluv aeg oleks väiksem. Soovitame süsteemile lisada funktsionaalsuse, mis võimaldaks hääletalletusserveri andmeid vajadusel varundada ka mitmele andmekandjale.

3.2 Andmete talletamine häältelugemisrakenduses

Proovihäälte lugemise käigus ilmnes, et häältelugemisrakenduse häälestamisel tekitatakse valikute ja jaoskondade jaoks andmestruktuurid ajutisse kataloogi (/var/tmp/evote). Häältelugemisrakenduse tööjaama väljalülitamisel selle kataloogi sisu kustutatakse ning häälte lugemisel annab süsteem veateate.

Nõuet, et sisendfailide laadimise ja häälte lugemise vahel ei tohi tööjaama välja lülitada, pole e-hääletuse dokumentatsioonis dokumenteeritud. Rakendusse on sisse ehitatud võimalus kontrollida, kas kõik sisendandmed on laetud, kuid see kontroll ei tuvastanud probleemi.

E-valimiste häälte kokkulugemisel antud probleemi ei tekkinud, kuna valikute ja jaoskondade fail laeti häältelugemisrakendusse vahetult enne häälte lugemist, ilma tööjaama vahepeal välja lülitamata. Kuna vastav nõue on dokumenteerimata, eksisteerib aga risk, et viga tekib uuesti, kui vahetuvad süsteemi operaatorid ning uued töötajad ei ole nõudest teadlikud. Sellisel juhul tekib e-häälte kokkulugemises viivitus kuni vea tuvastamise ja sisendfaili uuesti laadimiseni.

Soovitame muuta süsteemi disaini ja mitte tekitada seadistusperioodil ajutisi struktuure. Kui disaini muutmine pole mingil põhjusel võimalik, tuleb sellest tulenevad piirangud kindlasti dokumenteerida kõigis asjassepuutuvates e-hääletuse juhendites. Soovitame ka üle vaadata rakendusse sisseehitatud kontrollid ning täiendada sisendandmete olemasolu kontrollimise funktsionaalsust nii, et vajaliku failistruktuuri puudumine tuvastataks.

Lisa 1. Turvakleebiste kasutamine

Objekt	**Kleebisega suletud**	**Kleebise nr**	**Kleebis avatud**	**Artefakt hävitatud**
Veebiserveri salajane võti ja sertifikaadipäring CD1	12.02.07	6J1007248, 6J1007249	14.02.07	05.04.07
	14.02.07	6J1007269, 6J1007270	05.04.07	
Veebiserveri salajane võti ja sertifikaadipäring CD2	12.02.07	6J1007250	21.02.07	05.04.07
		6J1007251	05.04.07	
	21.02.07	6J1007285	05.04.07	
Backup token	12.02.07	6J1007252	05.04.07	Uue partitsiooniga üle kirjutatud 09.04.07
HSM korpus	12.02.07	6J1007253, 6J1007254		Uue partitsiooniga üle kirjutatud 09.04.07
HSM kast	12.02.07	6J1007255, 6J1007256	13.02.07	
		6J1007257, 6J1007258		
	13.02.07	6J1007259	20.02.07	
	20.02.07	6J1007276	21.02.07	
	21.02.07	6J1007292	04.03.07	

	04.03.07	6J1007343	09.04.07	
Valijarakenduse koodi signeerimise sertifikaat (kiipkaardil)	13.02.07	6J1007260, 6J1007261	14.02.07	
	14.02.07	6J1007267, 6J1007268	21.02.07	
	21.02.07	6J1007283, 6J1007284		
HLR korpus	13.02.07	6J1007264		
HLR toitepistik	13.02.07	00003252	14.02.07	
	14.02.07	6J1007271	20.02.07	
	20.02.07	6J1007277	21.02.07	
	21.02.07	6J1007293	04.03.07	
	04.03.07	6J1007339	09.04.07	
Karp lintide jm säilitatava materjaliga	14.02.07	6J1007272, 6J1007273	05.04.07	
Artefaktide karp	14.02.07	6J1007274	23.02.07	
	14.02.07	6J1007275	20.02.07	
	20.02.07	6J1007282	21.02.07	
	21.02.07	6J1007294	23.02.07	
	23.02.07	6J1007295	05.04.07	
	23.02.07	6J1007296	04.03.07	
	04.03.07	6J1007344	05.04.07	

HTS toitepistikud	20.02.07	6J1007278, 6J1007279	21.02.07	HTS kõvaketas hävitatud 05.04.07
	21.02.07	6J1007290, 6J1007291	23.02.07	
	01.03.07	6J1007332, 6J1007333	04.03.07	
	04.03.07	6J1007341, 6J1007342	05.04.07	
HTS esipaneel	28.03.07	6J1007320, 6J1007321	01.03.07	
	01.03.07	6J1007331	04.03.07	
	04.03.07	6J1007340	05.04.07	
HES toitepistikud	20.02.07	6J1007280, 6J1007281	21.02.07	HES kõvakettad formaaditud 05.04.07
	21.02.07	6J1007288, 6J1007289	23.02.07	
	28.02.07	6J1007322	05.04.07	
Serverikapi põrand	23.02.07	6J1007297, 6J1007298	28.02.07	
Serverikapi tagakülg	23.02.07	6J1007301, 6J1007302	28.02.07	
Serverikapi uks	23.02.07	6J1007299, 6J1007300	26.02.07	

	26.02.07	6J1007303, 6J1007304	26.02.07	
	26.02.07	6J1007307, 6J1007308	27.02.07	
	27.02.07	6J1007311, 6J1007313	28.02.07	
	28.02.07	6J1007316, 6J1007317	28.02.07	
CD „RK07 serverite andmed”	21.02.07	6J1007286, 6J1007287	04.03.07	05.04.07
26.02 varundus	26.02.07	6J1007305, 6J1007306	05.04.07	05.04.07
27.02 varundus	27.02.07	6J1007309, 6J1007310	05.04.07	05.04.07
28.02 esimene varundus	28.02.07	6J1007314, 6J1007315	05.04.07	05.04.07
28.02 teine varundus	28.02.07	6J1007318, 6J1007319	05.04.07	05.04.07
01.03 HTS varundus	01.03.07	6J1007326, 6J1007327	05.04.07	05.04.07
CD „HTS expordi kõik 04.03.07 1/2”	04.03.07	6J1007334	05.04.07	05.04.07
	04.03.07	6J1007335	04.03.07	
	04.03.07	6J1007338	05.04.07	
CD „HTS expordi kõik 04.03.07 2/2”	04.03.07	6J1007336, 6J1007337	05.04.07	05.04.07

Riigikogu serveriruumi uks (sisemine)	20.02.07	6J1007324	01.03.07	
Riigikogu serveriruumi uks (välimine)	20.02.07	6J1007325	01.03.07	