Eesti Vabariigi Valimiskomisjon

Euroopa Parlamendi E-hääletamise protseduuride täitmise jälgimine*

LÕPPARUANNE

19. august 2009

*connectedthinking

PRICEWATERHOUSECOOPERS

PRICEWATERHOUSECOOPERS

AS PricewaterhouseCoopers Advisors
Pärnu mnt. 15
10141 Tallinn

Telefon 614 1800
Faks 614 1900
www.pwc.ee

Heiki Sibul
Vabariigi Valimiskomisjon
Lossi plats 1A
Tallinn

19. august 2009

E-hääletamise protseduuride täitmise auditi aruanne

Lugupeetud Heiki Sibul

Oleme läbi viinud Euroopa Parlamendi E-hääletamise protseduuride täitmise jälgimise. Töö on teostatud vastavalt 29. aprillil 2009 aastal sõlmitud kliendilepingule.

Aruande eesmärgiks on anda hinnang Euroopa parlamendi valimiste e-hääletamise protseduuride järgimisele.

Juhime Teie tähelepanu asjaolule, et meie ülesannete hulka ei kuulunud meile esitatud informatsiooni õigsuse kontrollimine, mistõttu AS PricewaterhouseCoopers Advisors ei vastuta esitatud andmete õigsuse eest ega ka tulemuste eest juhul kui need põhinevad puudulikel või ebaõigetel algandmetel. Meie töö oli piiratud lepingus sätestatud tegevustega ning meile edastatud informatsiooniga. Juhul kui me oleks viinud läbi teisi tegevusi või meile oleks edastatud teistsugust informatsiooni, siis meie poolt tuvastatud leiud ning välja pakutud soovitused oleksid võinud olla ka teised.

Aruandes sisalduv informatsioon on mõeldud Vabariigi Valimiskomisjonile andmaks kindlust, et Euroopa Parlamendi valimiste E-hääletamine viidi läbi vastavalt välja töötatud protseduuridele.

Lisaks juhime Teie tähelepanu, et PricewaterhouseCoopers Advisors ei võta vastutust kolmandate osapoolte ees, kellele käesolev dokument on avaldatud või mõnel muul moel kättesaadavaks saanud.

Käesolevaga täname VVK töötajaid meeldiva koostöö eest.

Lugupidamisega

Teet Tender
AS PricewaterhouseCoopers Advisors

/allkirjastatud digitaalselt/

Sisukord

1. Sissejuhatus

Auditi eesmärgiks oli hinnata Vabariigi Valimiskomisjonil (edaspidi VVK) poolt läbi viidud Euroopa Parlamendi valimiste e-hääletamise protseduuride vastavust välja töötatud juhenditele. Auditi käigus vaatlesime süsteemide paigaldamist ja seadistamist, e-hääletamist ja häälte kokkulugemist ning hääletusjärgseid protseduure.

E-hääletamise kontseptsiooni turbe analüüs on läbi viidud 2003 aastal. Turbe analüüsi tulemusel kaardistati e-hääletamise ohud ning pakuti välja lahendused ohtude maandamiseks. Turbe analüüsi tulemusi arvestades on koostatud E-hääletamise käsiraamat ning täpsemad juhendid. Sellest tulenevalt tuginesime E-hääletamise Auditi programmi koostamisel eelkõige e-hääletamise käsiraamatule ja juhenditele. Auditi käigus vaatlesime järgnevaid E-hääletamise käsiraamatus loetletud e-hääletamise etappe:

- ✓ **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
  Süsteemi võtmepaari loomine ja varundamine
  *HES häälestus**
  *HTS häälestus **
  *HLR häälestus **
  Valijarakenduse pakendamine
  Serverite ülespanek majutuskohta
  Süsteemi prooviläbimine
  Proovihäälte kokkulugemine
  Süsteemi uus alghäälestus
  Serverite ülespanek majutuskohta

- ✓ **Hääletusperioodi protseduurid:**

  E-hääletamise alustamine
  Valijate nimekirja täiendamine, varukoopiate tegemine
  E-hääletamise lõpetamine

* HES – häälteedastamisserver; HTS – häältetalletamisserver; HLR - häältelugemisrakendus

- ✓ **Hääletusjärgse perioodi protseduurid:**

  Serverite tagasitoomine
  E-hääletanute nimekirja printimine
  E-häälte tühistuste kogumine ja häälte tühistamine
  Häälte kokkulugemine
  E-hääletamise tulemuse failide ülekanne valimiste infosüsteemi
  Võtmepaari hävitamine
  Krüpteeritud häälte hävitamine
  SSL serveri võtme hävitamine.

Antud töö viisid läbi PricewaterhouseCoopersi töötaja Mart Mäe ning PricewaterhouseCoopers Advisors poolt sõlmitud alltöövõtu lepingu alusel Martin Luts (CISA) ja Vilmar Vahe (CISA).

Meie töö kokkuvõte ja soovitused on esitatud peatükis 2.

2. Kokkuvõte

Lähtuvalt meie töö eesmärgist ja auditi programmist jälgisime Euroopa Parlamendi valimiste e-hääletuse protseduuride läbi viimist ja vastavust juhendites ning E-hääletamise käsiraamatus kirjeldatule. Enne auditi algust võtsid projektis osalevad audiitorid osa Vabariigi Valimiskomisjoni poolt läbi viidud E-hääletamise vaatlejate koolitusest, mille tulemusel omandasime parema ülevaate e-hääletamise süsteemist ja tehnilisest lahendusest.

Töö viisime läbi ajavahemikul 4.05.2009 – 3.08.2009 järgnevates etappides:

- *18.05. – 22.05 Installeerimise ja seadistamise vaatlus*
- *25.05 – 27.05 Seadmete transpordi vaatlus*
- *28.05 – 03.06 E- hääletamise vaatlus*
- *7.06 E-hääletamise tulemuste kokkulugemise vaatlus*
- *3.08 andmete hävitamise vaatlus*
- *4.05 – 3.08 - ettevalmistus, täiendavad tegevused ja aruandlus*

Kogu auditi läbi viimise perioodi suleti olulised andmekandjad turvakottidesse ja serverid pitseeriti turvakleebistega vältimaks ning tuvastamaks mitte autoriseeritud kasutust. Kõik auditi jooksul kasutatud turvakleebised ning turvakotid olid markeeritud unikaalsete numbrite ja tähtede kombinatsioonidega. Hävitamise päeva seisuga jäid avamata turvakleebised, numbritega 6J1007365, 6J1007366 ja 6J1007367, millega on suletud CD karpi kiipkaart e-hääletuse koodi signeerimise sertifikaadiga. Lisaks on avamata turvakleebis numbriga 6J1007363, kuna antud kleebis ei seganud läbi viimast hääletusjärgseid tegevusi HLRiga.

Kokkuvõttes ei tuvastanud me Euroopa Parlamendi E-hääletamise protseduuride täitmise auditi käigus olulisi kõrvalekaldeid E-hääletamise käsiraamatust ja välja töötatud juhenditest.

Järgnevalt tutvustame kokkuvõtlikult auditi käigus tuvastatud olulisemaid tähelepanekuid, mis on abiks VVKle protsesside parendamisel.

Tähelepanek nr 1

Dokumendi “Raudvaralise turvamooduli Safenet Luna SA haldusjuhend. Tegevusjuhis” punkt 1.1.88 järgi tuleb HLR –i kell seadistada 1 päeva võrra tagasi, mille järgi vajadus on VVK sõnul tingitud HLR –i eripärast. Peale seadistamist ilmnes vajadus seadistada kellaaega veel tunni aja võrra tagasi tulenevalt suveajast.

E-hääletuse protseduuride jälgitavuse huvides soovitame täiendada juhendmaterjale kirjeldamaks ära ka erisus protseduurist suveaja korral.

Meie hinnangul puudub tähelepanekul oluline mõju E-hääletuse tulemustele, kuid ohtude maandamiseks ning protseduuri paremaks jälgitavuseks tuleks kindlasti protseduuri vastavalt täiendada.

Tähelepanek nr 2

E-hääletamise tarkvara oli e-hääletuse alguseks üle antud arendaja poolt VVK ‘le, kes testis ka tarkvara funktsionaalsuse vastavust tellitule. 28.05.2009 paigaldati planeerimata veaparandus e-hääletamise tarkvarale hääletusperioodi ajal.

Vähendamaks vajadust planeerimata veaparanduste järele soovitame tarkvara testimist alustada varem tagamaks, et funktsionaalsus saab piisavalt testitud ning et vead jõutakse kõrvaldada enne hääletusperioodi algust.

Meie hinnangul puudub tähelepanekul oluline mõju E-hääletuse tulemustele, kuid vähendamaks hääletusperioodil tarkvara paikamisel tekkivad võimalikke ohtude realiseerumist tulevikus tuleks hääletuseelsel perioodil tõhustada tarkvara testimist.

Tähelepanek nr 3

Jälgides protsesside vastavust juhendmaterjalidele tuvastasime mitmeid tegevusi, mis ei olnud piisavalt detailselt või õiges järjekorras juhendmaterjalides kirjeldatud.

Soovitame hääletamisvälisel ajal simuleerida kogu protsessi, et optimeerida ning kaasajastada tegevuste kirjeldus. Näiteks dokumendis „EHA-03-10-2.1 E-hääletamise süsteem. Operatsioonisüsteemi paigaldus“ punktis 3 ei ole kirjeldatud, millise tarkvaraga kontrollida e-hääletuse tarkvara plaadi terviklikkust. Simulatsiooni läbi viimine aitab protseduure muuta täpsemaks, paremini jälgitavaks ja auditeeritavaks.

Meie hinnangul puudub tähelepanekul oluline mõju E-hääletuse tulemustele, kuid soovitame E-hääletamise protseduuride parema jälgitavuse huvides soovitus rakendada.

Tähelepanek nr 4

Vastavalt dokumendi “E-hääletamise käsiraamat” punktile 5.3 tuleb e-hääletamise lõpetamisel läbi viia mitmeid tegevusi, kuid loetletud ei ole varukoopiate tegemist ja nende säilitamist ning transportimist. Varukoopiaid hoiustati samas ruumis koos serverite kõvaketastega ning ka transporditi ühes liiklusvahendis.

Soovitame kõvakettad ja varukoopiad säilitada erinevates asukohtades tagamaks andmete säilimine ka ühe säilituskoha osalisel või täielikul hävinemisel. Sama põhimõtet tuleks jälgida ka varukoopiate ja serverite transpordil majutuskohast VVKsse tagamaks andmete säilimine ka ühe liiklusvahendi osalise või täieliku hävinemise korral.

Meie hinnangul puudub tähelepanekul oluline mõju E-hääletuse tulemustele, kuid vähendamaks varukoopiatega seotud ohtude realiseerumise tõenäosust tulevikus soovitame läbi viia analüüs ning vajadusel soovitus rakendada.

Tähelepanek nr 5

Vastavalt E-hääletamise käsiraamatu punktile 6.6 peaks audiitor kontrollima välisele andmekandjale eksporditud valimistulemuste importi valimiste infosüsteemi (edaspidi VIS). Valimispäeval (7.05.2009) ei olnud võimalik audiitoril importi VISi jälgida, kuna tegevus leidis aset väljaspool suletud ruumi. Veendumaks valimistulemuste korrektses impordis VISi võrdlesime HLRi andmeid VISi andmetega ning võrdluse käigus me erinevusi ei tuvastanud.

Soovitame järgmistel valimistel tagada audiitorile võimalus jälgida valmistulemuste importi VISi.

Meie hinnangul puudub tähelepanekul oluline mõju E-hääletuse tulemustele, kuid soovitame E-hääletamise protseduuride parema jälgitavuse huvides soovitus rakendada.

Lisa 1. Protseduuride vastavuse hindamisel kasutatud juhendid

- EHA-03-02-1.4 E-hääletamise käsiraamat
- EHA-03-06-1.3 Raudvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhis
- EHA-03-10-2.1 E-hääletamise süsteem. Operatsioonisüsteemi paigaldus
- EHA-03-04-1.9 E-hääletamise süsteem. Valija rakenduse pakendamine
- EHA-03-03-1.10 E-hääletamise süsteem. Süsteemiülema juhend hääleedastusserveri, hääletalletusserveri ja häältelugemisrakenduse operaatorile
- EHA-02-03-1.1 E-hääletamise süsteemi infoturbe poliitika
- EHA-02-01-1.0 E-hääletamise organisatsioon ja infrastruktuur
- EHA-03-05-1.2 Riistvaralise turvamooduli SafeNet Luna SA haldusjuhend. Üldosa

Lisa 2. Turvakleebiste ning turvakottide kasutamise kontrolltabelid

2.1 Turvakleebiste kontrolltabel

Kood kleebiselt	Kleebise paigaldamise kuupäev	Paigaldamise koht	Kleebise eemaldamise kuupäev	Eemaldamise koht	Kirjeldus
6J1007349	19.05.2009	VVK	20.05.2009	VVK	HLR peale installeerimist
6J1007350	19.05.2009	VVK	20.05.2009	VVK	HLR peale installeerimist
6J1007351	19.05.2009	VVK	3.08.2009	VVK	"www.valimised.ee" sertifikaat - CD karbis
6J1007352	19.05.2009	VVK	3.08.2009	VVK	"www.valimised.ee" sertifikaat - CD karbis
6J1007353	19.05.2009	VVK	22.05.2009	VVK	Kohver
6J1007354	19.05.2009	VVK	22.05.2009	VVK	Kohver
6J1007355	20.05.2009	VVK	3.08.2009	VVK	Varukoopia HLR
6J1007356	20.05.2009	VVK	22.05.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007357	20.05.2009	VVK	22.05.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007358	20.05.2009	VVK	22.05.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007359	20.05.2009	VVK	20.05.2009	VVK	Kleebis purunes paigaldamisel
6J1007360	20.05.2009	VVK	22.05.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007361	20.05.2009	VVK	7.06.2009	VVK	HSM
6J1007362	20.05.2009	VVK	22.05.2009	VVK	HLR
6J1007363	20.05.2009	VVK		VVK	HLR - kleebis eemaldamata kuna ei sega seadme kasutamist
6J1007364	22.05.2009	VVK	7.06.2009	VVK	HLR
6J1007365	22.05.2009	VVK		VVK	Kiipkaart koodi signeerimiseks - CD karbis.
6J1007366	22.05.2009	VVK		VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007367	22.05.2009	VVK		VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007368	22.05.2009	VVK	3.08.2009	VVK	Kohver
6J1007369	22.05.2009	VVK	27.05.2009	VVK	Kohver
6J1007370	27.05.2009	VVK	3.06.2009	RIA	Kohver
6J1007371	27.05.2009	RIA	3.06.2009	RIA	Serveriruumi põrand
6J1007372	27.05.2009	RIA	3.06.2009	RIA	Serveriruumi põrand
6J1007373	27.05.2009	RIA	3.06.2009	RIA	Serveri kapp - tagumine osa
6J1007374	27.05.2009	RIA	3.06.2009	RIA	Serveri kapp - tagumine osa
6J1007375	27.05.2009	RIA	3.06.2009	RIA	Serveri kapp - tagumine osa
6J1007376	27.05.2009	RIA	3.06.2009	RIA	Serveri kapi külg
6J1007377	27.05.2009	RIA	3.06.2009	RIA	Serveri kapi külg
6J1007378	27.05.2009	RIA	27.05.2009	RIA	Kleebis purunes paigaldamisel
6J1007379	27.05.2009	RIA	3.06.2009	RIA	Serveri kapi uks
6J1007380	27.05.2009	RIA	27.05.2009	RIA	Serveri kapi uks
6J1007381	27.05.2009	RIA	27.05.2009	RIA	Serveri kapi uks
6J1007382	27.05.2009	RIA	28.05.2009	RIA	Serveri kapi uks
6J1007383	27.05.2009	RIA	28.05.2009	RIA	Serveri kapi uks
6J1007384	28.05.2009	RIA	29.05.2009	RIA	Serveri kapi uks
6J1007385	28.05.2009	RIA	29.05.2009	RIA	Serveri kapi uks
6J1007386	29.05.2009	RIA	30.05.2009	RIA	Serveri kapi uks
6J1007387	29.05.2009	RIA	30.05.2009	RIA	Serveri kapi uks
6J1007388	30.05.2009	RIA	31.05.2009	RIA	Serveri kapi uks
6J1007389	30.05.2009	RIA	31.05.2009	RIA	Serveri kapi uks

6J1007390	31.05.2009	RIA	1.06.2009	RIA	Serveri kapi uks
6J1007391	31.05.2009	RIA	1.06.2009	RIA	Serveri kapi uks
6J1007392	1.06.2009	RIA	2.06.2009	RIA	Serveri kapi uks
6J1007393	1.06.2009	RIA	2.06.2009	RIA	Serveri kapi uks
6J1007394	2.06.2009	RIA	3.06.2009	RIA	Serveri kapi uks
6J1007395	2.06.2009	RIA	3.06.2009	RIA	Serveri kapi uks
6J1007396	3.06.2009	RIA	3.06.2009	RIA	Serveri kapi uks
6J1007397	3.06.2009	RIA	3.06.2009	RIA	Serveri kapi uks
6J1007398	3.06.2009	RIA	4.06.2009	RIA	Kohver
6J1007399	4.06.2009	VVK	4.06.2009	VVK	Kohver - videolindi lisamine kohvrisse
6J1007400	4.06.2009	VVK	7.06.2009	VVK	Kohver
6J1007401	7.06.2009	VVK	7.06.2009	VVK	Viga kleebise paigaldamisel.
6J1007402	7.06.2009	VVK	3.08.2009	VVK	HSM
6J1007403	7.06.2009	VVK	3.08.2009	VVK	Kohver
6J1007404	7.06.2009	VVK	22.06.2009	VVK	HLR
6J1007405	22.06.2009	VVK	3.08.2009	VVK	HLR
6J1007406	8.07.2009	VVK	3.08.2009	VVK	Kohver

2.2 Turvakottide kontrolltabel

Kood kleebiselt	Kleebise paigaldamise kuupäev	Paigaldamise koht	Kleebise eemaldamise kuupäev	Eemaldamise koht	Kirjeldus
867562	19.05.2009	VVK	19.05.2009	VVK	Installeerimise plaadid
867563	19.05.2009	VVK	22.05.2009	VVK	HES kõvakettad
867564	19.05.2009	VVK	22.05.2009	VVK	HTS kõvakettad
867565	19.05.2009	VVK	3.08.2009	VVK	CDd (e-hääletus tarkvara lisa (Cybernetica); hääletusskript; Luna SSA klient)
867566	19.05.2009	VVK	3.08.2009	VVK	CDd (operatsiooni süsteem, e-hääletus tarkvara (VVK)
867567	22.05.2009	VVK	27.05.2009	VVK	HES kõvakettad
867568	22.05.2009	VVK	27.05.2009	VVK	HTS kõvakettad
867569	20.05.2009	VVK	3.08.2009	VVK	Videosalvestused
867570	20.05.2009	VVK	7.06.2009	VVK	HSM võtmed
867571	27.05.2009	RIA	3.08.2009	VVK	HES ja HTS varukoopia ning videolint
867572	3.06.2009	RIA	3.08.2009	VVK	HTS varukoopia
867601	4.06.2009	VVK	7.06.2009	VVK	HTS kettad
867602	3.06.2009	RIA	4.06.2009	RIA	HTS kettad
867603	7.06.2009	VVK	3.08.2009	VVK	HTS ja HLR varukoopiad ja CDle talletud e-hääletamise tulemused
867604	7.06.2009	VVK	3.08.2009	VVK	HTS kettad
867605	3.06.2009	RIA	3.08.2009	VVK	HTS varukoopia
867606	31.05.2009	RIA	3.08.2009	VVK	HTS varukoopia ja videolint
867607	1.06.2009	RIA	3.08.2009	VVK	HTS varukoopia
867608	2.06.2009	RIA	3.08.2009	VVK	HTS varukoopia
867609	30.05.2009	RIA	3.08.2009	VVK	HTS varukoopia
867610	29.05.2009	RIA	3.08.2009	VVK	HTS varukoopia ja videolint
867611	28.05.2009	RIA	3.08.2009	VVK	HTS varukoopia

pwc.com

© 2009 PricewaterhouseCoopers. All rights reserved. “PricewaterhouseCoopers” refers to the network
of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. *connectedthinking is a trademark of
PricewaterhouseCoopers LLP (US)