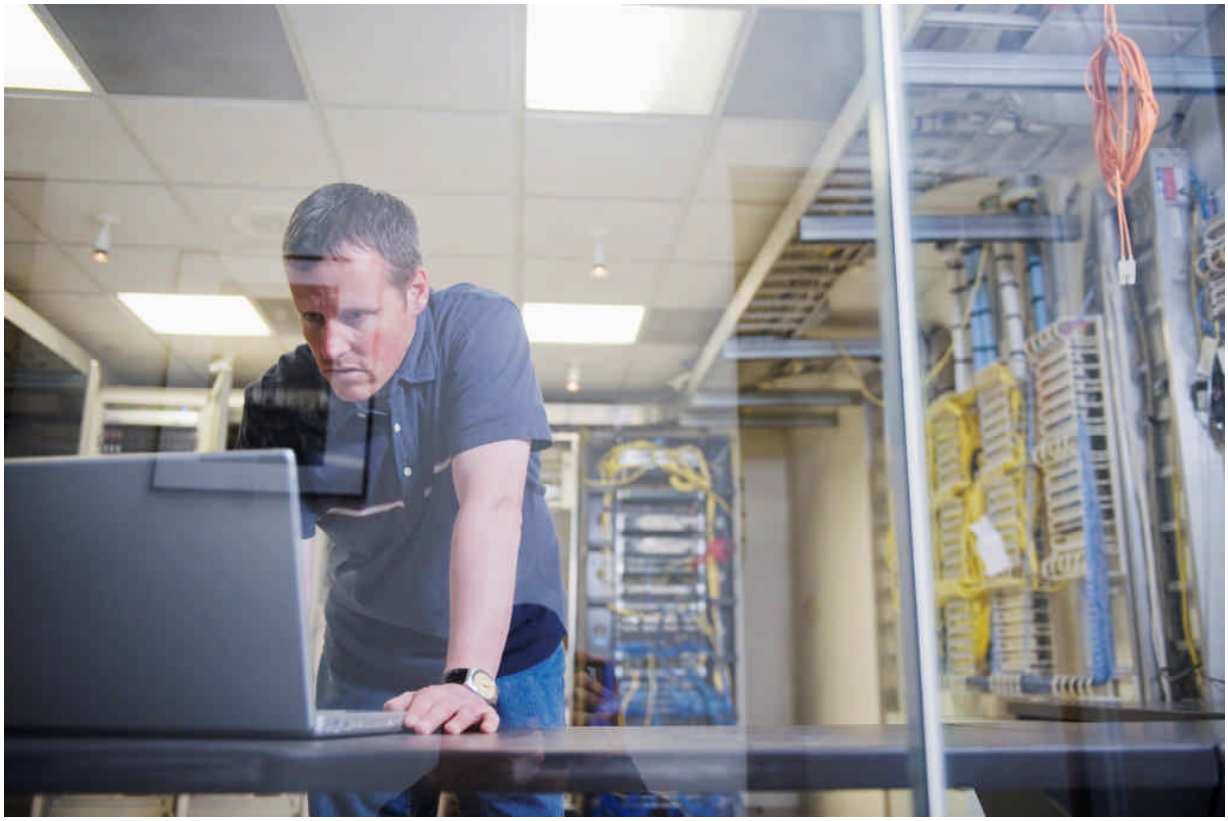
Eesti Vabariigi Valimiskomisjon

Kohaliku omavalituse volikogu E-hääletamise protseduuride täitmise jälgimine*

LÕPPARUANNE

22. detsember 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

22. detsember 2009

E-hääletamise protseduuride täitmise auditi aruanne

Lugupeetud Heiki Sibul

Oleme läbi viinud kohaliku omavalitsuse volikogu E-hääletamise protseduuride täitmise jälgimise. Töö on teostatud vastavalt 14. septembril 2009 aastal sõlmitud kliendilepingule.

Aruande eesmärgiks on anda hinnang kohaliku omavalitsuse volikogu 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 kohaliku omavalitsuse volikogu 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 4
2. Kokkuvõte 6
Lisa 1. Protseduuride vastavuse hindamisel kasutatud juhendid 8
Lisa 2. Turvakleebiste ning turvakottide kasutamise kontrolltabelid 9

1. Sissejuhatus

Auditi eesmärgiks oli hinnata Vabariigi Valimiskomisjonil (edaspidi VVK) poolt läbi viidud kohaliku omavalitsuse volikogu 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
  Süsteemi võtmepaari loomine ja varundamine
  *HES häälestus**
  *HTS häälestus **
  *HLR häälestus **
  Valijarakenduse pakendamine
  Serverite ülespanek majutuskohta

- ✓ **Hääletusperioodi protseduurid:**

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

- ✓ **Hääletusjärgse perioodi protseduurid:**

  Serverite tagasitoomine
  E-hääletanute nimekirja printimine
  E-häälte tühistuste kogumine ja häälte tühistamine
  Häälte kokkulugemine

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

E-hääletamise tulemuse failide ülekanne valimiste infosüsteemi
Võtmepaari hävitamine
Krüpteeritud häälte hävitamine
SSL serveri võtme hävitamine.

Antud töö viis läbi PricewaterhouseCoopersi töötaja Mart Mäe (CISA).

Meie töö kokkuvõte ja soovitused on esitatud peatükis 2.

2. Kokkuvõte

Lähtuvalt meie töö eesmärgist ja auditi programmist jälgisime kohaliku omavalitsuse volikogu valimiste e-hääletuse protseduuride läbi viimist ja vastavust juhendites ning E-hääletamise käsiraamatus kirjeldatule.

Töö viisime läbi ajavahemikul 28.09.2009 – 22.12.2009 järgnevates etappides:

- 28.09-02.10 süsteemi seadistamine
- 8.10, 14.10.2009 e-hääletuse algus, e-hääletuse lõpp
- 18.10.2009 e-häälte kokkulugemine
- 28.09 – 14.10.2009 Täiendavad tegevused ja aruandlus
- Peale valimistoimingute lõppu - e-hääletuse järgsed protseduurid

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 numbrite ja tähtede kombinatsioonidega. Hävitamise päeva seisuga avamata jäänud turvakleebised on numbritega 6J1007407, 6J1007409, 6J1007433, 6J1007253, 6J1007254 ja turvakott numbriga 867576.

Kokkuvõttes ei tuvastanud me kohaliku omavalitsuse volikogu 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 1.4.57 järgi tuleb HLRi sisestada peale musta võtit ka sinine. Siiski protseduuri käigus selgus, et sinise võtme sisestamise vajadust protsessi lõpetamiseks ei olnud.

E-hääletuse protseduuride jälgitavuse huvides soovitame täiendada juhendmaterjale kirjeldamaks ära ka erisus protseduurist ehk millal ei ole vajadust sinise võtme sisestamiseks.

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

Tähelepanek nr 2

Jälgides protsesside vastavust juhendmaterjalidele tuvastasime, et dokumendis „EHA-03-02-1.5 E-hääletamise käsiraamat“ punktis 6.9 on kirjeldatud sertifikaatide hävitamise vajadus ning põhimõtted, kuid ei ole piisavalt detailselt kirjeldatud tulemuse saavutamiseks läbiviidavaid tegevusi. Vähene kirjeldamine loob ohu, et läbiviidavad tegevused ei ole piisavad vajaliku tulemuse saavutamiseks.

Soovitame hääletamisvälisel ajal analüüsida ning dokumenteerida täpsem kirjeldus punktis 6.9 läbitavatest tegevustest, mis ühtlasi tagaks ka protseduuri parema jälgitavuse ja auditeeritavuse.

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-03-02-1.5 E-hääletamise käsiraamat
- EHA-03-06-1.4 Raudvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhis
- EHA-03-10-2.3 E-hääletamise süsteem. Operatsioonisüsteemi paigaldus
- EHA-03-04-1.11 E-hääletamise süsteem. Valija rakenduse pakendamine
- EHA-03-03-1.12 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-03-05-1.3 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
6J1007407	29.09.2009	VVK			HLR külg
6J1007408	29.09.2009	VVK	30.09.2009	VVK	HLR toiteplokk
6J1007409	29.09.2009	VVK			HLR - esimene pool
6J1007410	29.09.2009	VVK	30.09.2009	VVK	Kohver - esimene pool
6J1007411	29.09.2009	VVK	18.12.2009	VVK	Kohver - tagumine pool
6J1007412	29.09.2009	VVK	18.12.2009	VVK	Kohver - tagumine pool
6J1007413	29.09.2009	VVK	30.09.2009	VVK	Kohver - esimene pool
6J1007414	30.09.2009	VVK	18.12.2009	VVK	HSM 'varundustoken'
6J1007415	30.09.2009	VVK	18.10.2009	VVK	HSM - esimene pool
6J1007416	30.09.2009	VVK	18.10.2009	VVK	HSM - esimene pool
6J1007417	30.09.2009	VVK	2.10.2009	VVK	Veebiserveri sertifikaadi päring
6J1007418	30.09.2009	VVK	2.10.2009	VVK	Veebiserveri sertifikaadi päring
6J1007419	30.09.2009	VVK	2.10.2009	VVK	Veebiserveri sertifikaadi päring
6J1007420	30.09.2009	VVK	2.10.2009	VVK	Veebiserveri sertifikaadi päring
6J1007421	30.09.2009	VVK	2.10.2009	VVK	HLR toiteplokk
6J1007422	30.09.2009	VVK	2.10.2009	VVK	Kohver - esimene pool
6J1007423	30.09.2009	VVK	2.10.2009	VVK	Kohver - esimene pool
6J1007424	2.10.2009	VVK	18.10.2009	VVK	HLR toiteplokk
6J1007425	2.10.2009	VVK	7.10.2009	RIA	Kohver - esimene pool
6J1007426	2.10.2009	VVK	7.10.2009	RIA	Kohver - esimene pool
6J1007427	7.10.2009	RIA	14.10.2009	RIA	Serveri kapp – tagumine uks

6J1007428	7.10.2009	RIA	14.10.2009	RIA	Serveri kapp – tagumine uks
6J1007429	7.10.2009	RIA	14.10.2009	RIA	Serveri kapp – tagumine uks
6J1007430	7.10.2009	RIA	14.10.2009	RIA	Kohver - esimene pool
6J1007431	7.10.2009	RIA	14.10.2009	RIA	Kohver - esimene pool
6J1007432	7.10.2009	RIA	8.10.2009	RIA	Serveri kapp – esimene uks
6J1007433	7.10.2009	RIA			Serveri kapp – ülemine äär
6J1007434	7.10.2009	RIA	8.10.2009	RIA	Serveri kapp – esimene uks
6J1007435	8.10.2009	RIA	8.10.2009	RIA	Serveri kapp – esimene uks
6J1007436	8.10.2009	RIA	8.10.2009	RIA	Serveri kapp – esimene uks
6J1007437	8.10.2009	RIA	9.10.2009	RIA	Serveri kapp – esimene uks
6J1007438	8.10.2009	RIA	9.10.2009	RIA	Serveri kapp – esimene uks
6J1007439	9.10.2009	RIA	10.10.2009	RIA	Serveri kapp – esimene uks
6J1007440	9.10.2009	RIA	10.10.2009	RIA	Serveri kapp – esimene uks
6J1007441	10.10.2009	RIA	11.10.2009	RIA	Serveri kapp – esimene uks
6J1007442	10.10.2009	RIA	11.10.2009	RIA	Serveri kapp – esimene uks
6J1007443	11.10.2009	RIA	12.10.2009	RIA	Serveri kapp – esimene uks
6J1007444	11.10.2009	RIA	12.10.2009	RIA	Serveri kapp – esimene uks
6J1007445					Viga kleebise paigaldamisel.
6J1007446					Viga kleebise paigaldamisel.
6J1007447	12.10.2009	RIA	13.10.2009	RIA	Serveri kapp – esimene uks
6J1007448	12.10.2009	RIA	13.10.2009	RIA	Serveri kapp – esimene uks
6J1007449	13.10.2009	RIA	14.10.2009	RIA	Serveri kapp – esimene uks
6J1007450	13.10.2009	RIA	14.10.2009	RIA	Serveri kapp – esimene uks
6J1007451	14.10.2009	RIA	14.10.2009	RIA	Serveri kapp – esimene uks
6J1007452	14.10.2009	RIA	14.10.2009	RIA	Serveri kapp – esimene uks
6J1007453	14.10.2009	RIA	15.10.2009	RIA	Kohver - esimene pool
6J1007454	14.10.2009	RIA	15.10.2009	RIA	Kohver - esimene pool

6J1007455	15.10.2009	VVK	18.10.2009	VVK	Kohver - esimene pool
6J1007456	15.10.2009	VVK	18.10.2009	VVK	Kohver - esimene pool
6J1007457	18.10.2009	VVK	18.12.2009	VVK	HSM - esimene pool
6J1007458	18.10.2009	VVK	18.12.2009	VVK	HSM - esimene pool
6J1007459	18.10.2009	VVK	18.12.2009	VVK	HLR toiteplokk
6J1007460	18.10.2009	VVK	18.12.2009	VVK	Kohver - esimene pool
6J1007461	18.10.2009	VVK	18.12.2009	VVK	Kohver - esimene pool

2.2 Turvakottide kontrolltabel

Kood kleebisel t	Sulgemise kuupäev	Paigaldami se koht	Avamise kuupäev	Eemaldami se koht	Kirjeldus
867576	21.12.2009	VVK			Kiipkaart koodi signeerimiseks - CD karbis
867579	18.12.2009	VVK	21.12.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
867581	14.10.2009	RIA	18.12.2009	VVK	HESi kõvakettad
867582	14.10.2009	RIA	15.10.2009	VVK	HTSi kõvakettad
867583	15.10.2009	VVK	18.10.2009	VVK	HTSi kõvakettad
867584	18.10.2009	VVK	18.12.2009	VVK	HTSi kõvakettad
867585	8.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867586	9.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867587	11.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867588	10.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867589	12.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867590	13.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867591	13.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867592	14.10.2009	RIA	18.12.2009	VVK	HTS varukoopia
867593	2.10.2009	VVK	7.10.2009	RIA	HESi kõvakettad
867594	2.10.2009	VVK	7.10.2009	RIA	HTSi kõvakettad
867595	29.09.2009	VVK	18.12.2009	VVK	CDd (operatsiooni süsteem, lisa, e-hääletus tarkvara)
867596	30.09.2009	VVK	18.12.2009	VVK	HSM varuvõtmed
867597	30.09.2009	VVK	2.10.2009	VVK	Avalik võti
867598	2.10.2009	VVK	18.12.2009	VVK	Avalik võti, süsteemivõti, kiipkaart koodi signeerimiseks
867599	29.09.2009	VVK	2.10.2009	VVK	HTSi kõvakettad
867600	29.09.2009	VVK	2.10.2009	VVK	HESi kõvakettad

2.3 Turvakleebised eelmistest valimistest

Kood kleebise lt	Kleebise paigaldamise kuupäev	Paigaldamise koht	Kleebise eemaldamise kuupäev	Eemaldamise koht	Kirjeldus
6J1007253					HSM külg
6J1007254					HSM külg
6J1007365	22.05.2009	VVK	2.10.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis.
6J1007366	22.05.2009	VVK	2.10.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis
6J1007367	22.05.2009	VVK	21.12.2009	VVK	Kiipkaart koodi signeerimiseks - CD karbis