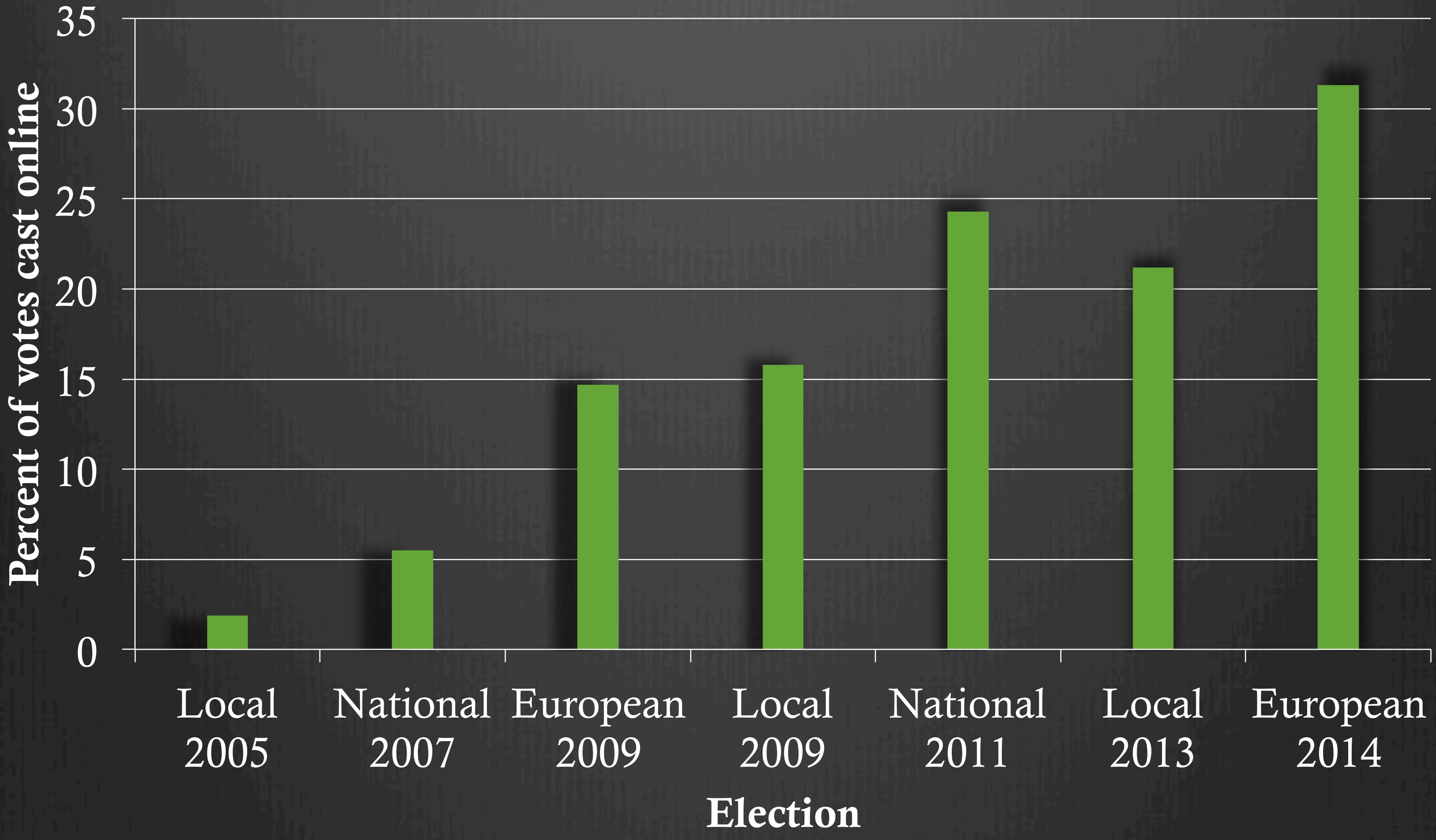
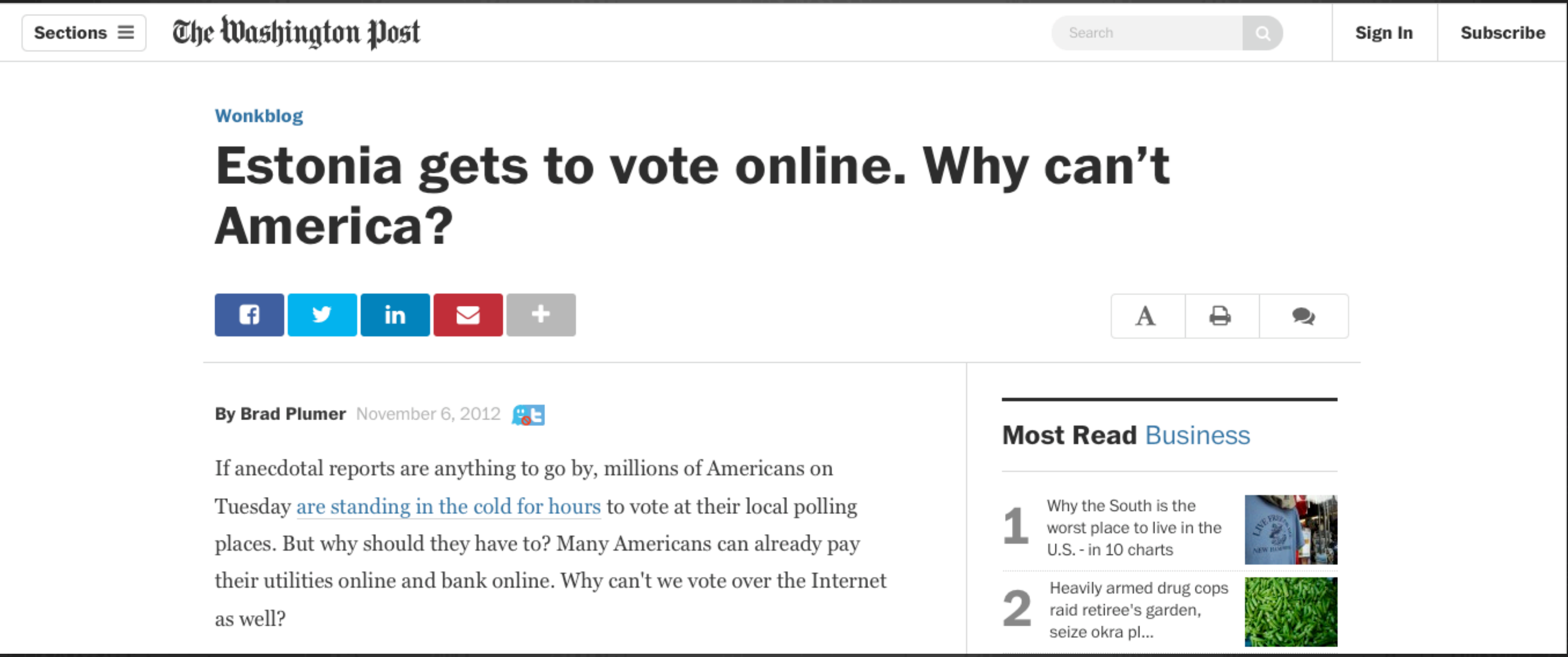
Security Analysis of the Estonian Internet Voting System

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat,
Harri Hursti, Margaret MacAlpine, and J. Alex Halderman

Internet Voting?

Internet Voting in Estonia





Wonkblog

Estonia gets to vote online. Why can’t America?

By Brad Plumer November 6, 2012

If anecdotal reports are anything to go by, millions of Americans on Tuesday are standing in the cold for hours to vote at their local polling places. But why should they have to? Many Americans can already pay their utilities online and bank online. Why can't we vote over the Internet as well?

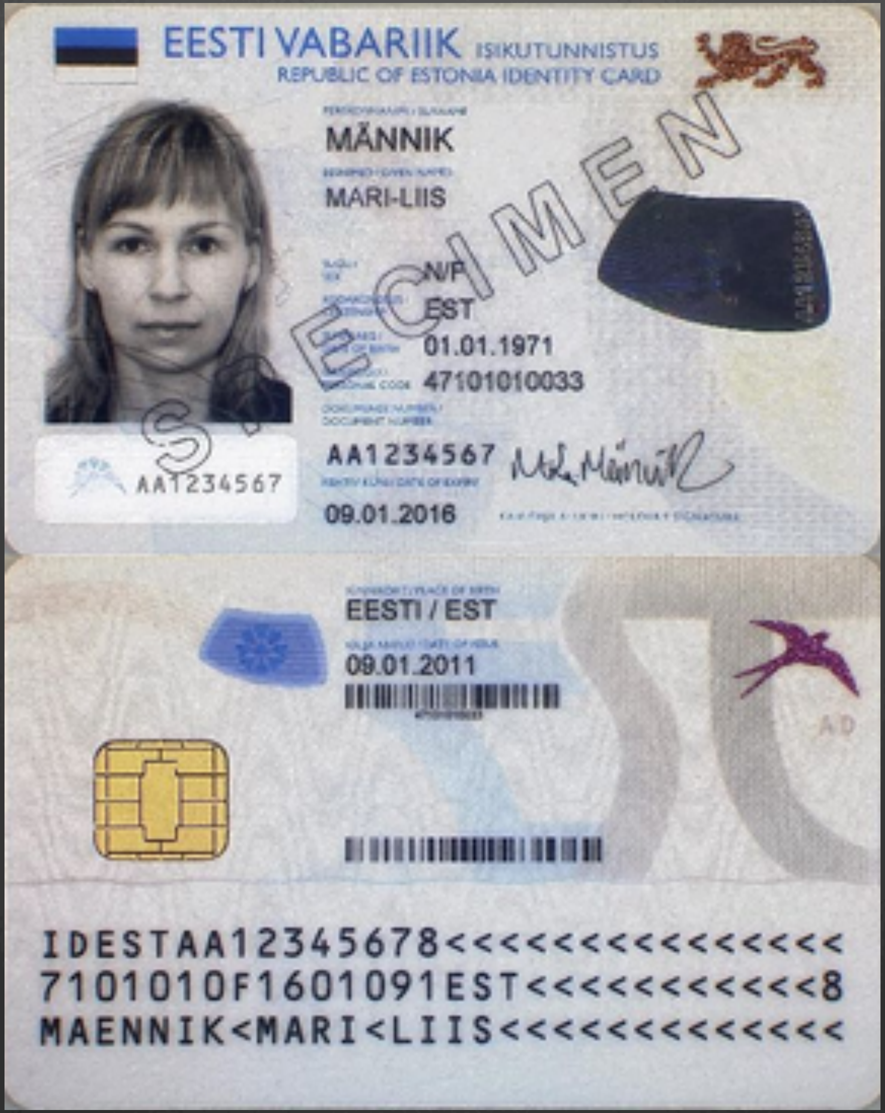
Most Read Business

1 Why the South is the worst place to live in the U.S. - in 10 charts

2 Heavily armed drug cops raid retiree's garden, seize okra pl...

- Is Estonia’s Internet voting system secure against attackers the country may face?
- What is a realistic threat model for a national Internet voting system?
- What can other countries considering Internet voting learn from Estonia?

- Motivation
- **How Estonia’s system works**
- Proper Threat Model
- Analysis
- Estonian Response
- Conclusions



EESTI VABARIIK ISIKUTUNNISTUS
REPUBLIC OF ESTONIA IDENTITY CARD

PEREKONNANIMI / SURNAME
MÄNNIK

EESNIMED / GIVEN NAMES
MARI-LIIS

SUGU / SEX
N/F

KODAKONDSUS / CITIZENSHIP
EST

SÜNNIAEG / DATE OF BIRTH
01.01.1971

ISIKUKOOD / PERSONAL CODE
47101010033

DOKUMENDI NUMBER / DOCUMENT NUMBER
AA1234567

KEHTIV KUNI / DATE OF EXPIRY
09.01.2016

AA1234567

SPECIMEN

SÜNNIKOHT / PLACE OF BIRTH
EESTI / EST

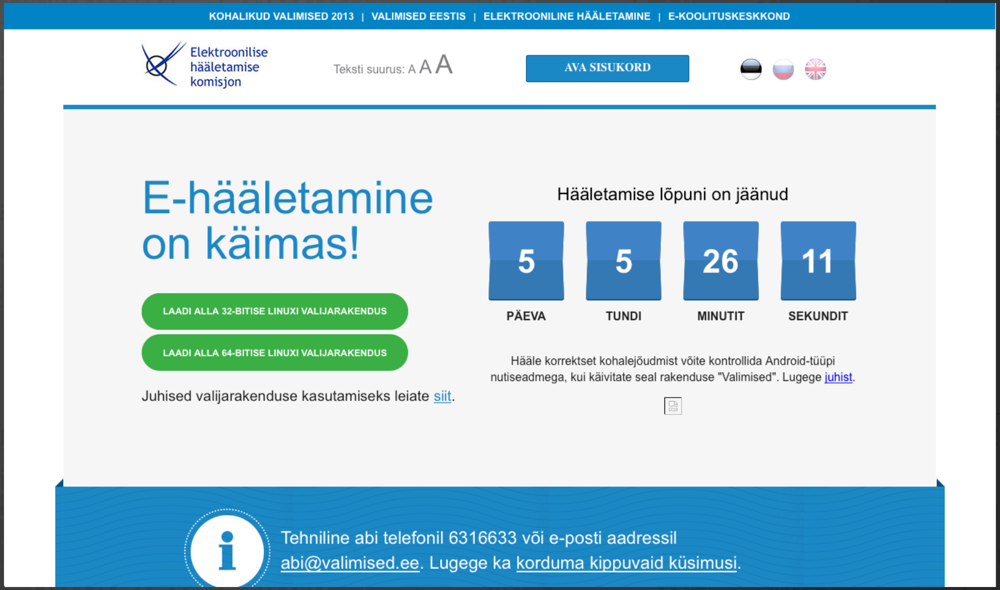
VÄLJA ANTUD / DATE OF ISSUE
09.01.2011

AD

```
IDESTAA12345678<<<<<<<<<<<<<<<
7101010F1601091EST<<<<<<<<<<<8
MAENNIK<MARI<LIIS<<<<<<<<<<<<<
```

Voting Process

Election Servers



KOHALIKUD VALIMISED 2013 | VALIMISED EESTIS | ELEKTROONILINE HÄÄLETAMINE | E-KOOLITUSKESKKOND

Elektroonilise hääletamise komisjon

Teksti suurus: A A A

AVA SISUKORD

E-hääletamine on käimas!

LAADI ALLA 32-BITISE LINUXI VALIJARAKENDUS

LAADI ALLA 64-BITISE LINUXI VALIJARAKENDUS

Juhised valijarakenduse kasutamiseks leiate siit.

Hääletamise lõpuni on jäänud

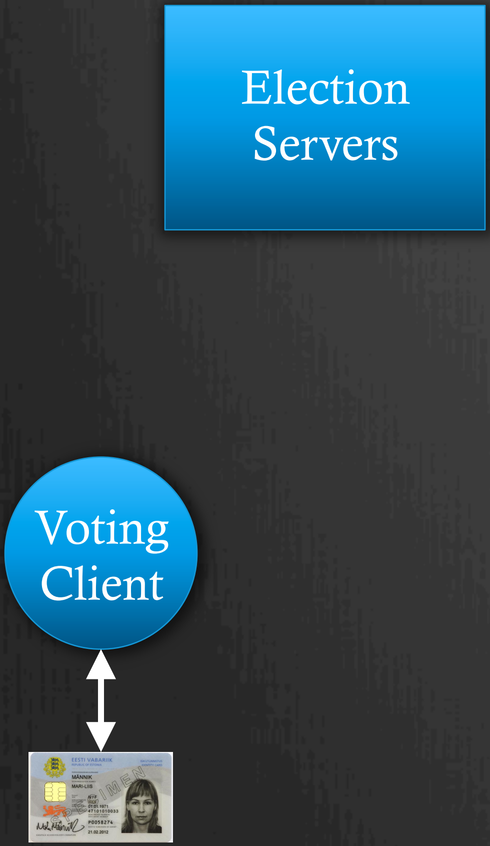
5	5	26	11
PÄEVA	TUNDI	MINUTIT	SEKUNDIT

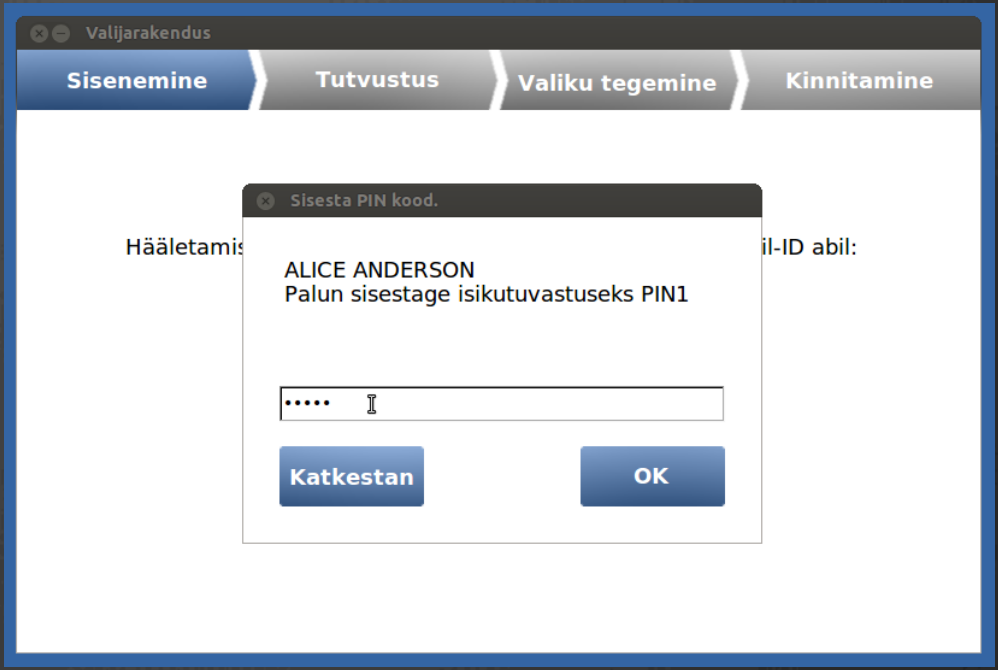
Hääle korrektset kohalejõudmist võite kontrollida Android-tüüpi nutiseadmega, kui käivitate seal rakenduse "Valimised". Lugege juhist.

Tehniline abi telefonil 6316633 või e-posti aadressil abi@valimised.ee. Lugege ka korduma kippuvaid küsimusi.

Voting Client

Voting Process





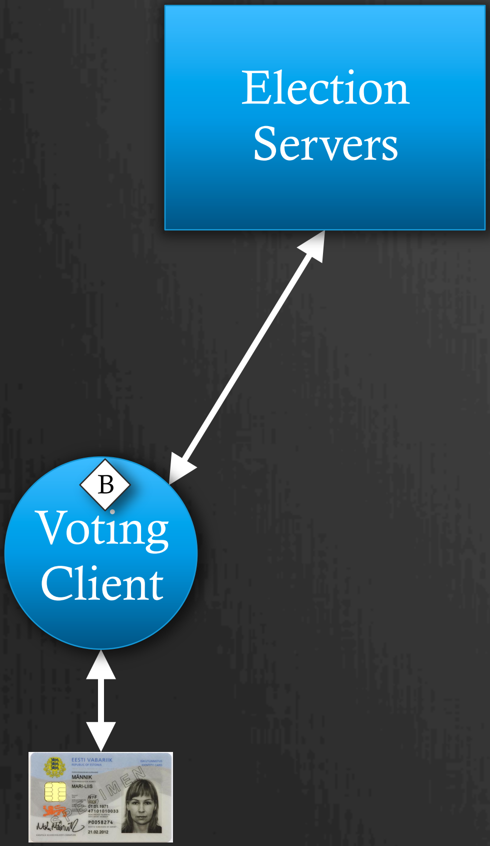
Hääletamis

il-ID abil:

ALICE ANDERSON
Palun sisestage isikutuvastuseks PIN1

•••••

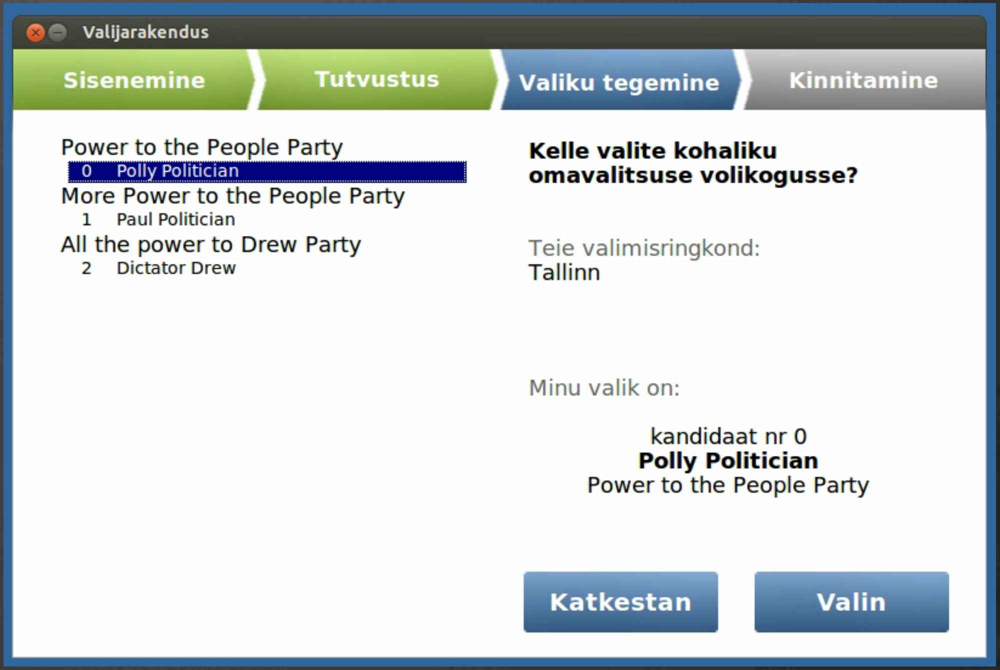
Voting Process



Election Servers

B

Voting Client



Power to the People Party
0 Polly Politician
More Power to the People Party
1 Paul Politician
All the power to Drew Party
2 Dictator Drew

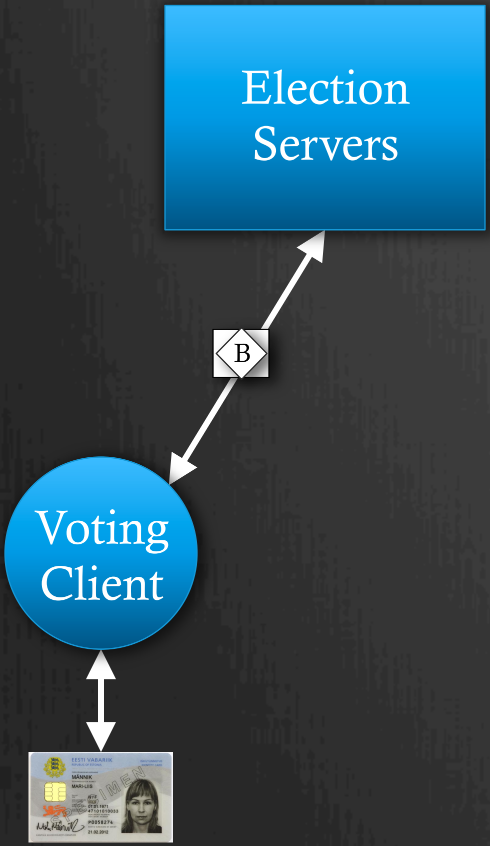
Kelle valite kohaliku omavalitsuse volikogusse?

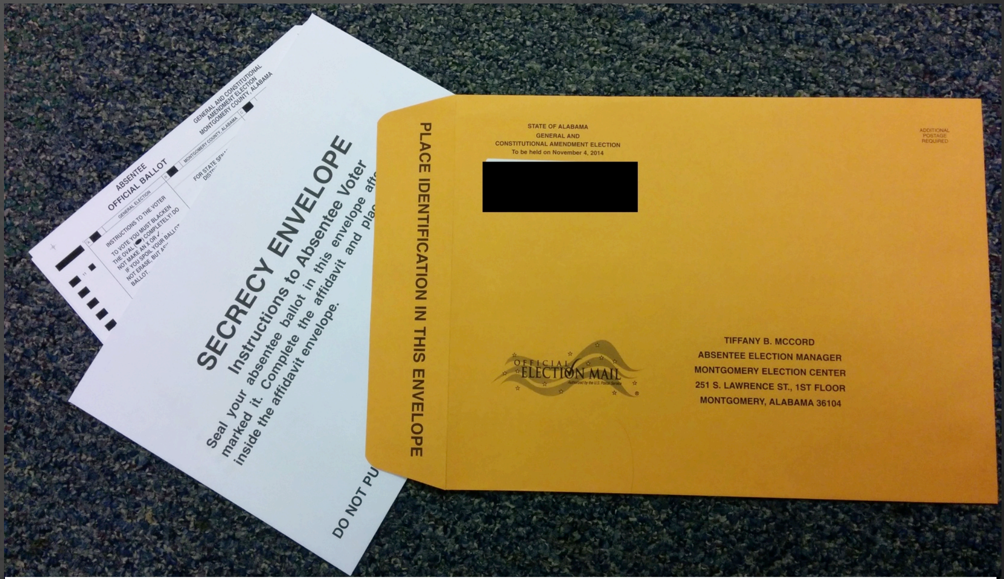
Teie valimisringkond:
Tallinn

Minu valik on:

kandidaat nr 0
Polly Politician
Power to the People Party

Voting Process




ABSENTEE OFFICIAL BALLOT
GENERAL AND CONSTITUTIONAL AMENDMENT ELECTION
MONTGOMERY COUNTY, ALABAMA
SECRECY ENVELOPE
Instructions to Absentee Voter
Seal your absentee ballot in this envelope
marked it. Complete the affidavit and plac
inside the affidavit envelope.
DO NOT PU
PLACE IDENTIFICATION IN THIS ENVELOPE
STATE OF ALABAMA
GENERAL AND
CONSTITUTIONAL AMENDMENT ELECTION
To be held on November 4, 2014
[redacted]
ADDITIONAL POSTAGE REQUIRED
OFFICIAL ELECTION MAIL
TIFFANY B. MCCORD
ABSENTEE ELECTION MANAGER
MONTGOMERY ELECTION CENTER
251 S. LAWRENCE ST., 1ST FLOOR
MONTGOMERY, ALABAMA 36104

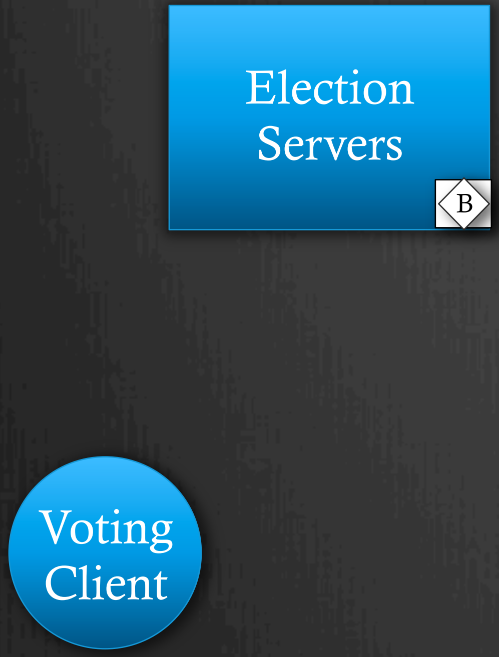
Inner Envelope :

$$\text{Encrypt}(PK_{elect}, \text{Pad}_r(\text{Ballot}))$$

Outer Envelope :

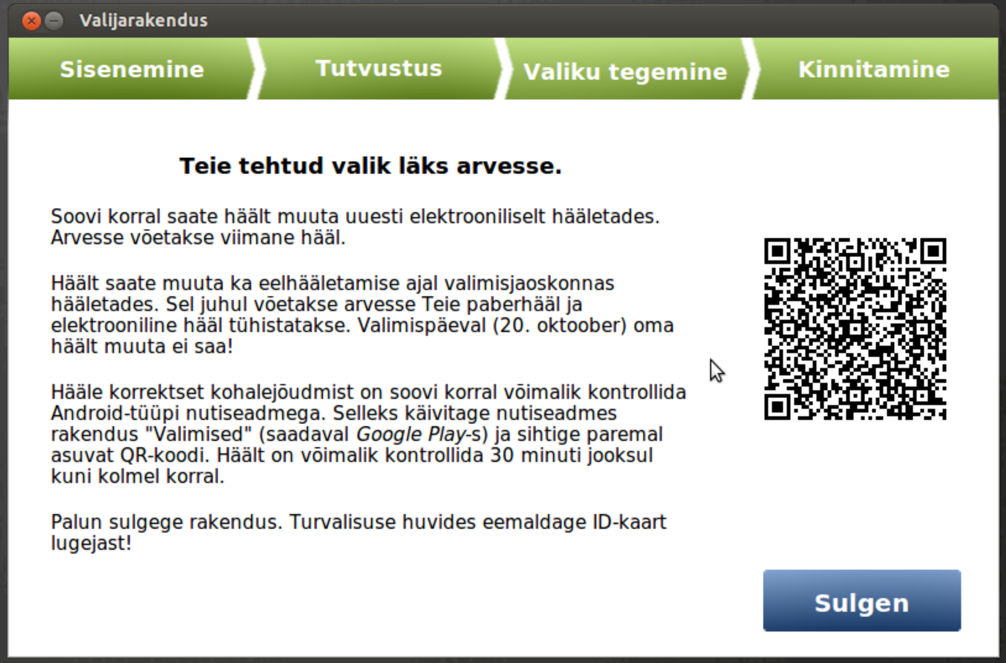
$$\text{Sign}(SK_{voter}, \text{Inner Envelope})$$

Voting Process



Election Servers

Voting Client



Teie tehtud valik läks arvesse.

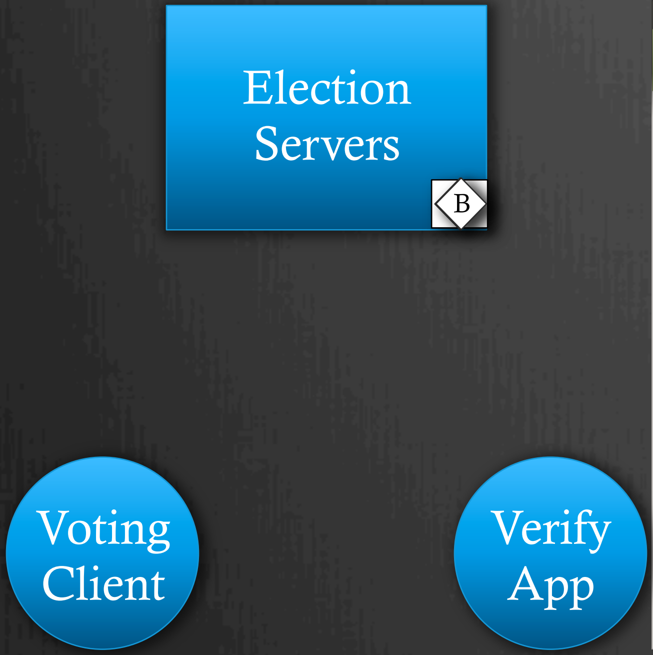
Soovi korral saate häält muuta uuesti elektrooniliselt hääletades. Arvesse võetakse viimane hääl.

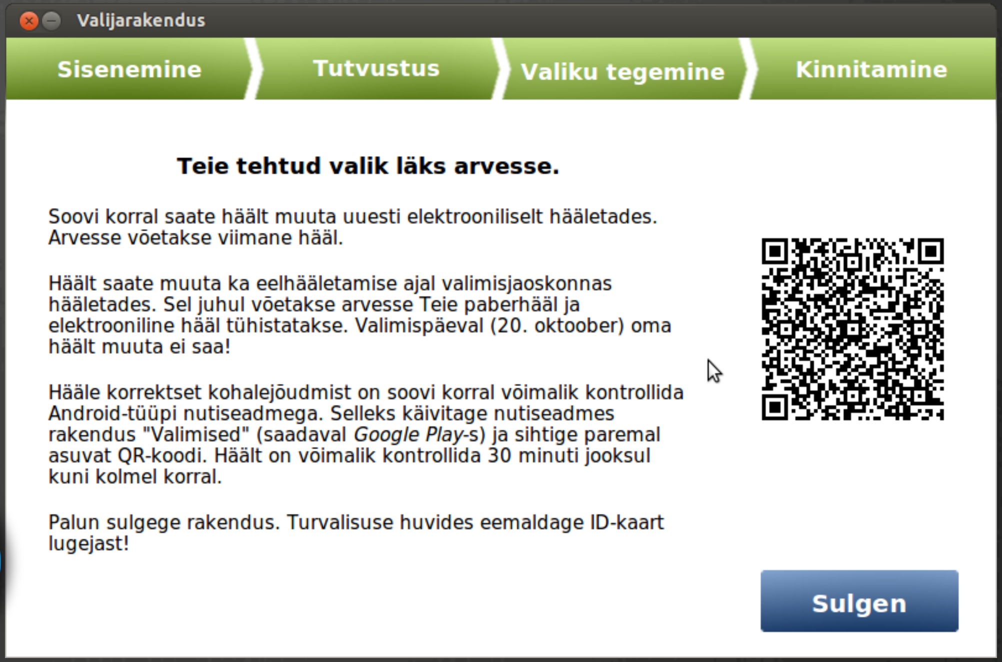
Häält saate muuta ka eelhääletamise ajal valimisjaoskonnas hääletades. Sel juhul võetakse arvesse Teie paberhääl ja elektrooniline hääl tühistatakse. Valimispäeval (20. oktoober) oma häält muuta ei saa!

Hääle korrektset kohalejõudmist on soovi korral võimalik kontrollida Android-tüüpi nutiseadmega. Selleks käivitage nutiseadmes rakendus "Valimised" (saadaval *Google Play*-s) ja sihtige paremal asuvat QR-koodi. Häält on võimalik kontrollida 30 minuti jooksul kuni kolmel korral.

Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart lugejast!

Verification Process





Teie tehtud valik läks arvesse.

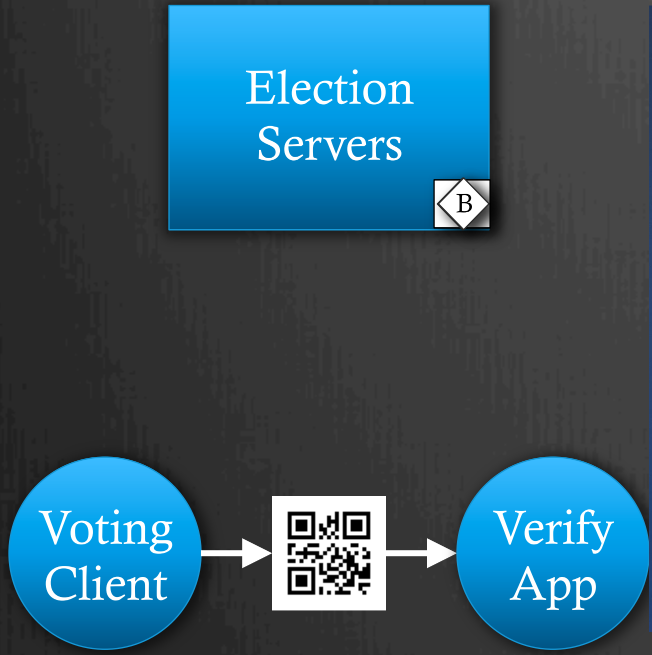
Soovi korral saate häält muuta uuesti elektrooniliselt hääletades. Arvesse võetakse viimane hääl.

Häält saate muuta ka eelhääletamise ajal valimisjaoskonnas hääletades. Sel juhul võetakse arvesse Teie paberhääl ja elektrooniline hääl tühistatakse. Valimispäeval (20. oktoober) oma häält muuta ei saa!

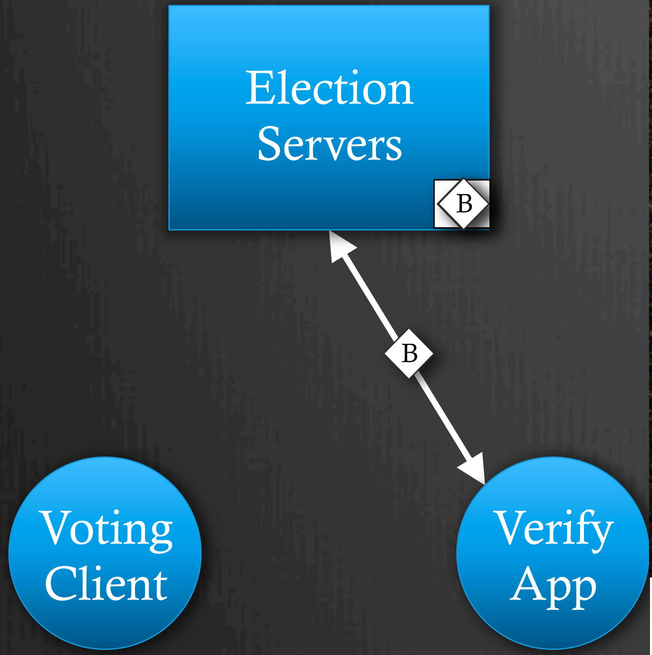
Hääle korrektset kohalejõudmist on soovi korral võimalik kontrollida Android-tüüpi nutiseadmega. Selleks käivitage nutiseadmes rakendus "Valimised" (saadaval *Google Play*-s) ja sihtige paremal asuvat QR-koodi. Häält on võimalik kontrollida 30 minuti jooksul kuni kolmel korral.

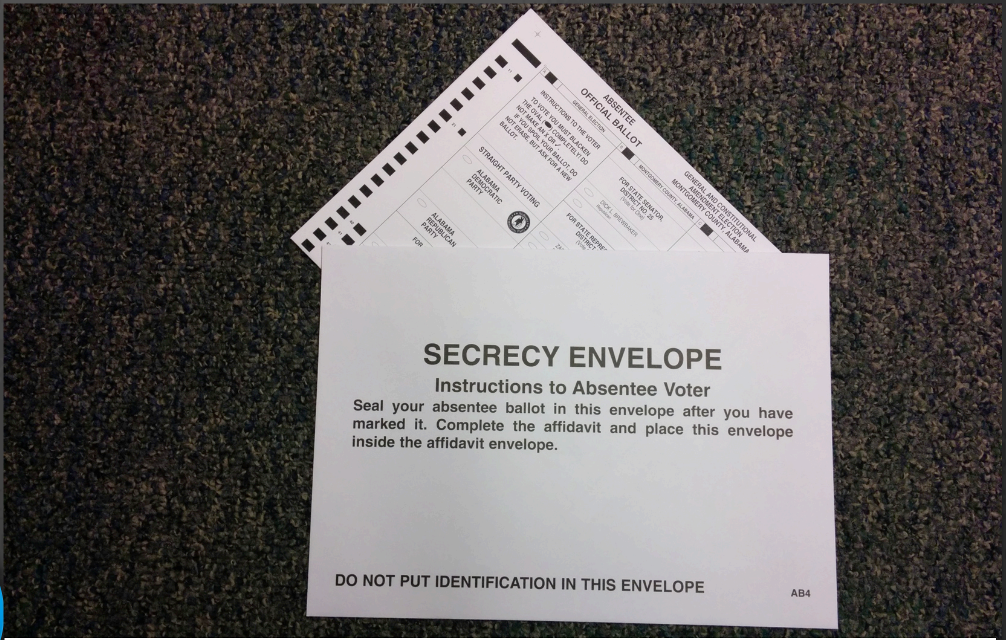
Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart lugejast!

Verification Process



Verification Process




ABSENTEE
OFFICIAL BALLOT

SECRECY ENVELOPE

Instructions to Absentee Voter

Seal your absentee ballot in this envelope after you have marked it. Complete the affidavit and place this envelope inside the affidavit envelope.

DO NOT PUT IDENTIFICATION IN THIS ENVELOPE

AB4

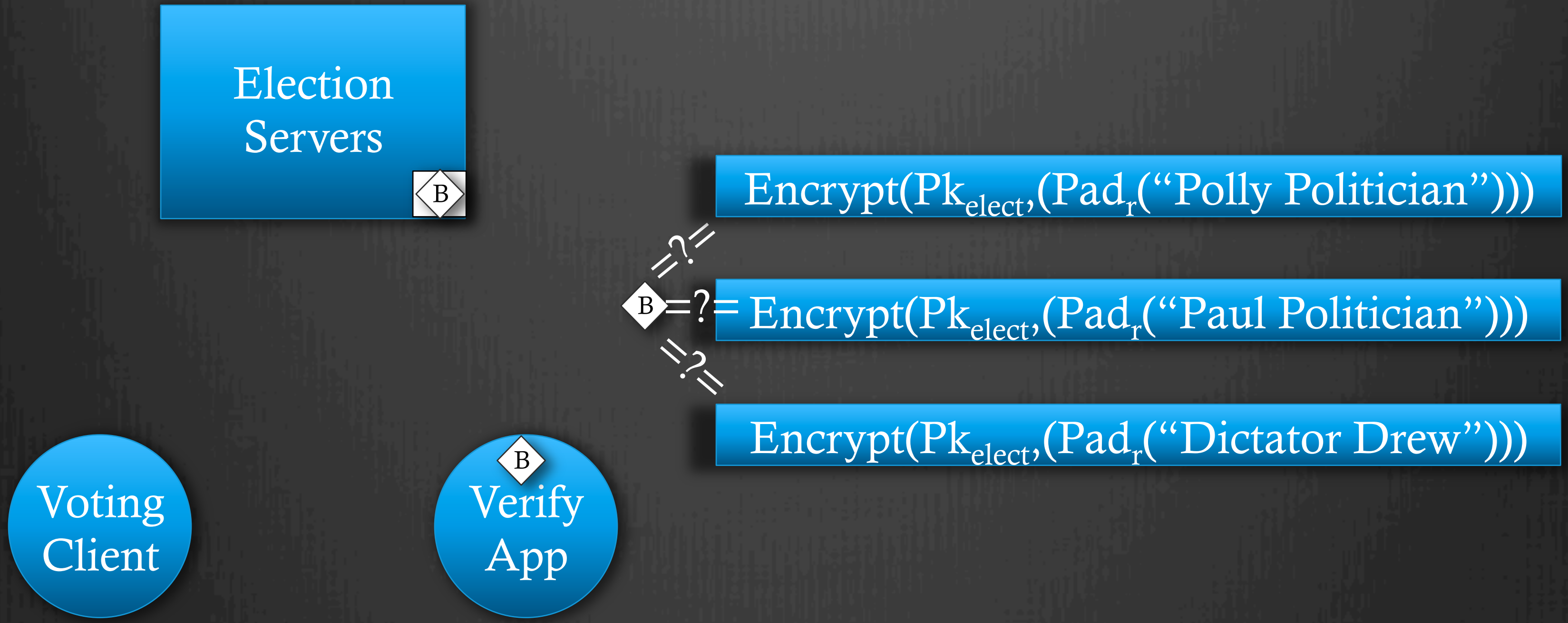
Inner Envelope :

$$\text{Encrypt}(PK_{elect}, \text{Pad}_r(\text{Ballot}))$$

~~Outer Envelope :~~

~~Sign(SK_{voter}, Inner Envelope)~~

Verification Process



Election Servers

B

Voting Client

B

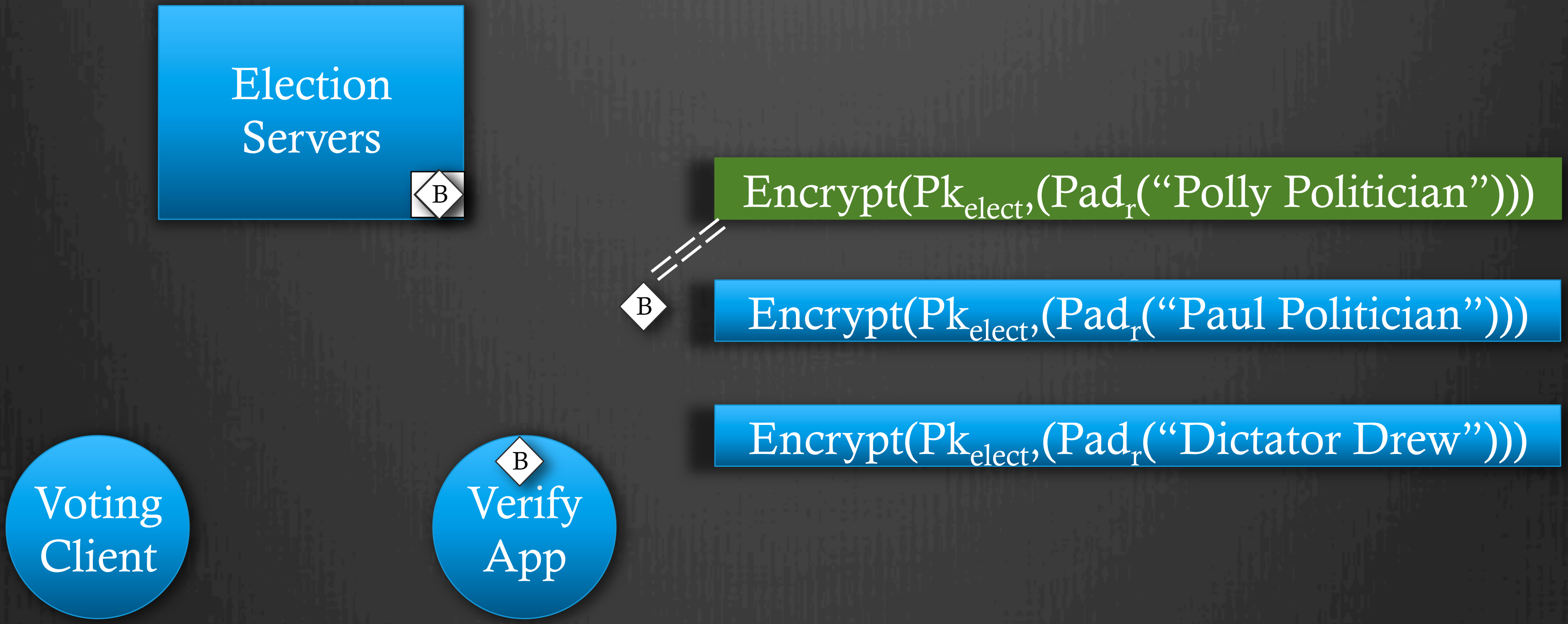
Verify App

B =?= Encrypt(Pk_{elect},(Pad$_r$("Paul Politician")))

=?= Encrypt(Pk_{elect},(Pad$_r$("Polly Politician")))

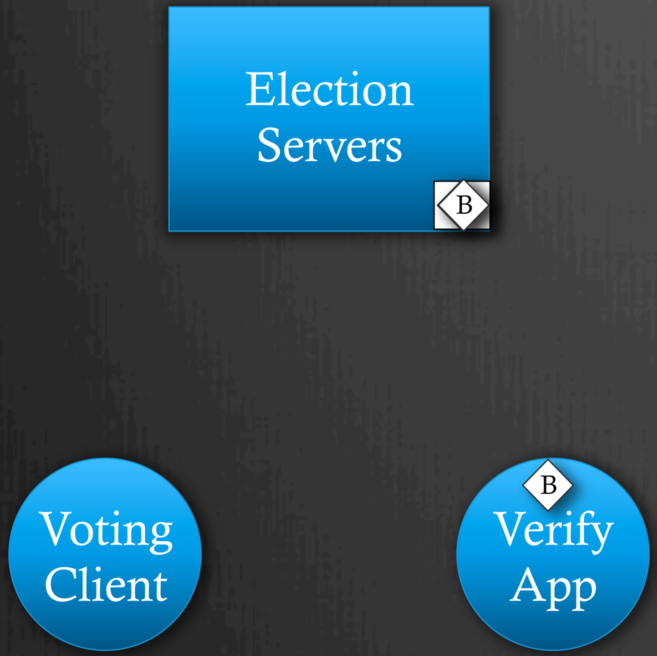
=?= Encrypt(Pk_{elect},(Pad$_r$("Dictator Drew")))

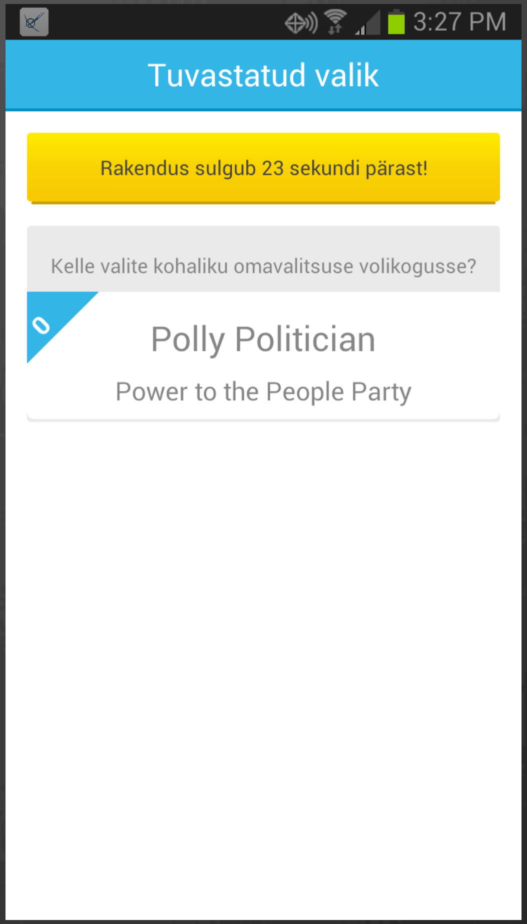
Verification Process



Election Servers
B
Encrypt(Pk_{elect},(Pad$_r$(“Polly Politician”)))
B
Encrypt(Pk_{elect},(Pad$_r$(“Paul Politician”)))
Encrypt(Pk_{elect},(Pad$_r$(“Dictator Drew”)))
Voting Client
B
Verify App

Verification Process





Tuvastatud valik

Rakendus sulgub 23 sekundi pärast!

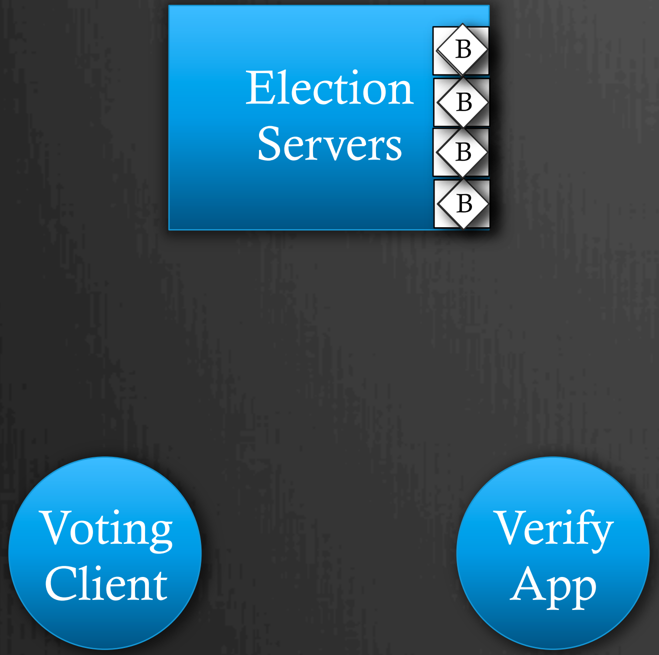
Kelle valite kohaliku omavalitsuse volikogusse?

0

Polly Politician

Power to the People Party

Tally Process



Election Servers

B

B

B

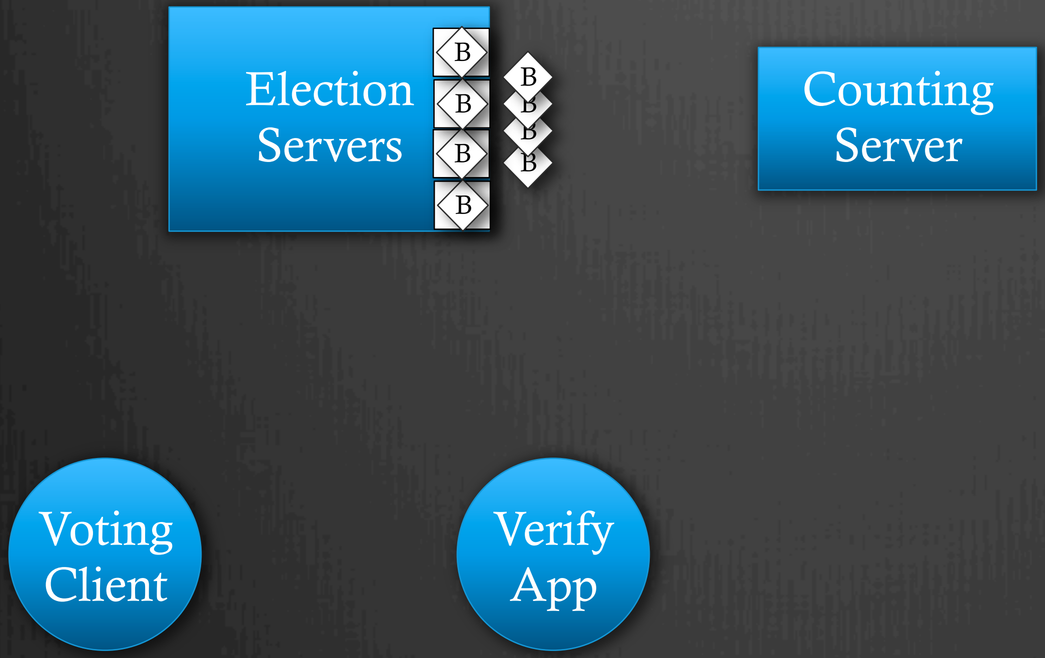
B

Counting Server

Voting Client

Verify App

Tally Process



Election Servers

B

B

B

B

B

B

B

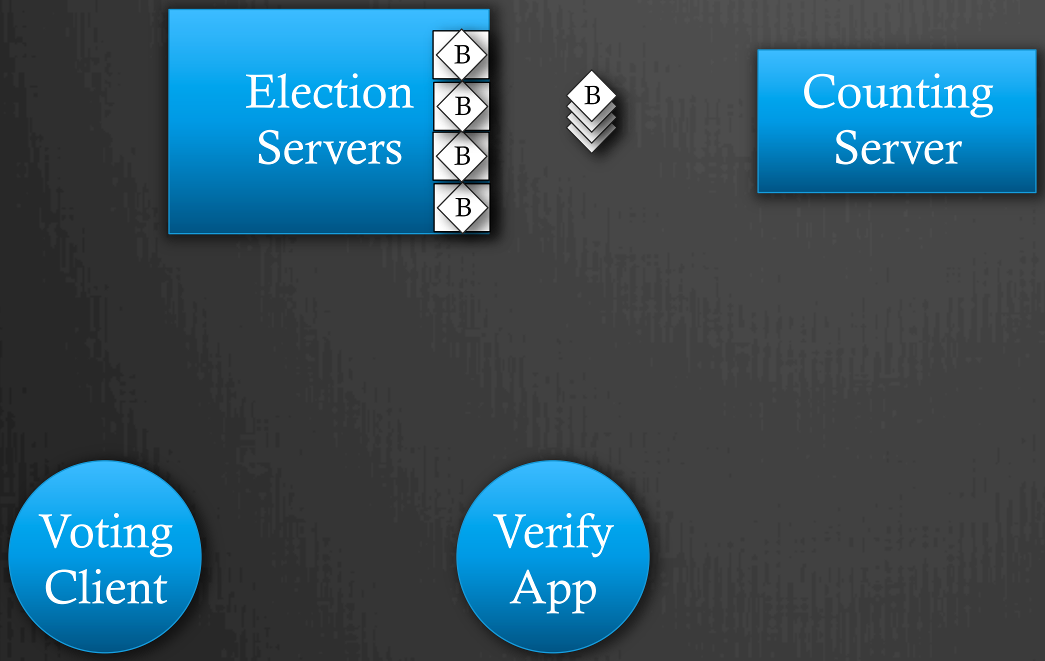
B

Counting Server

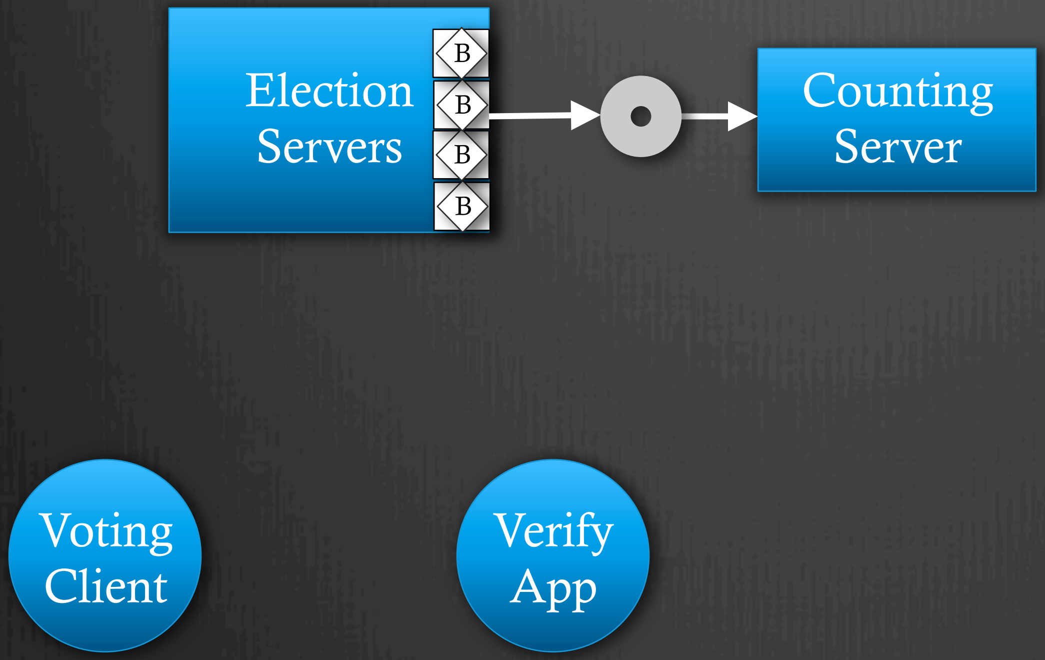
Voting Client

Verify App

Tally Process



Tally Process



Election Servers

B

B

B

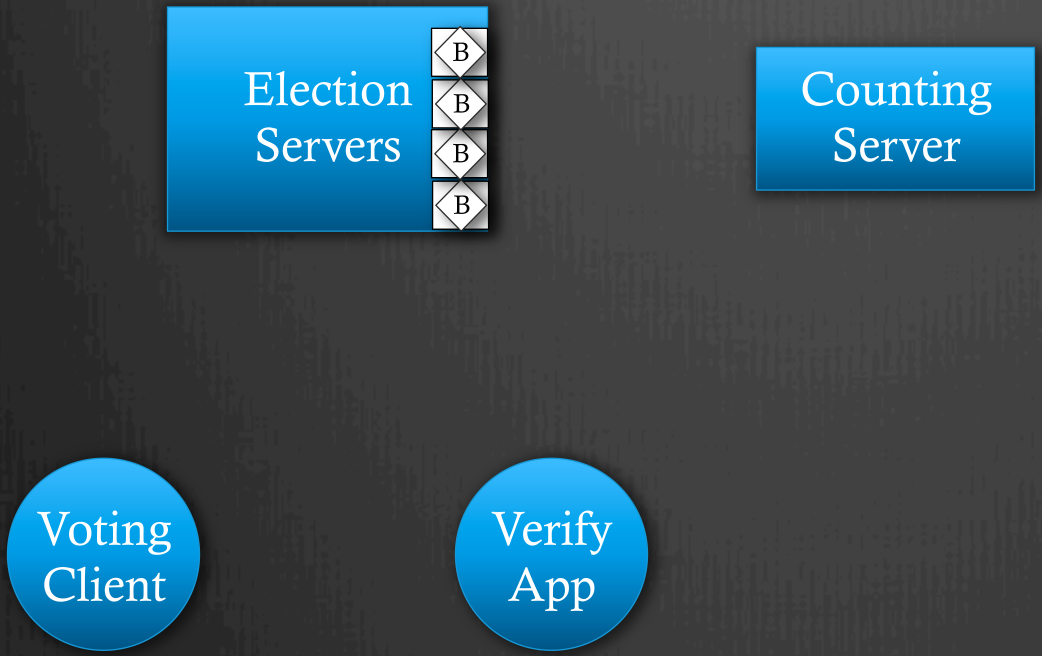
B

Counting Server

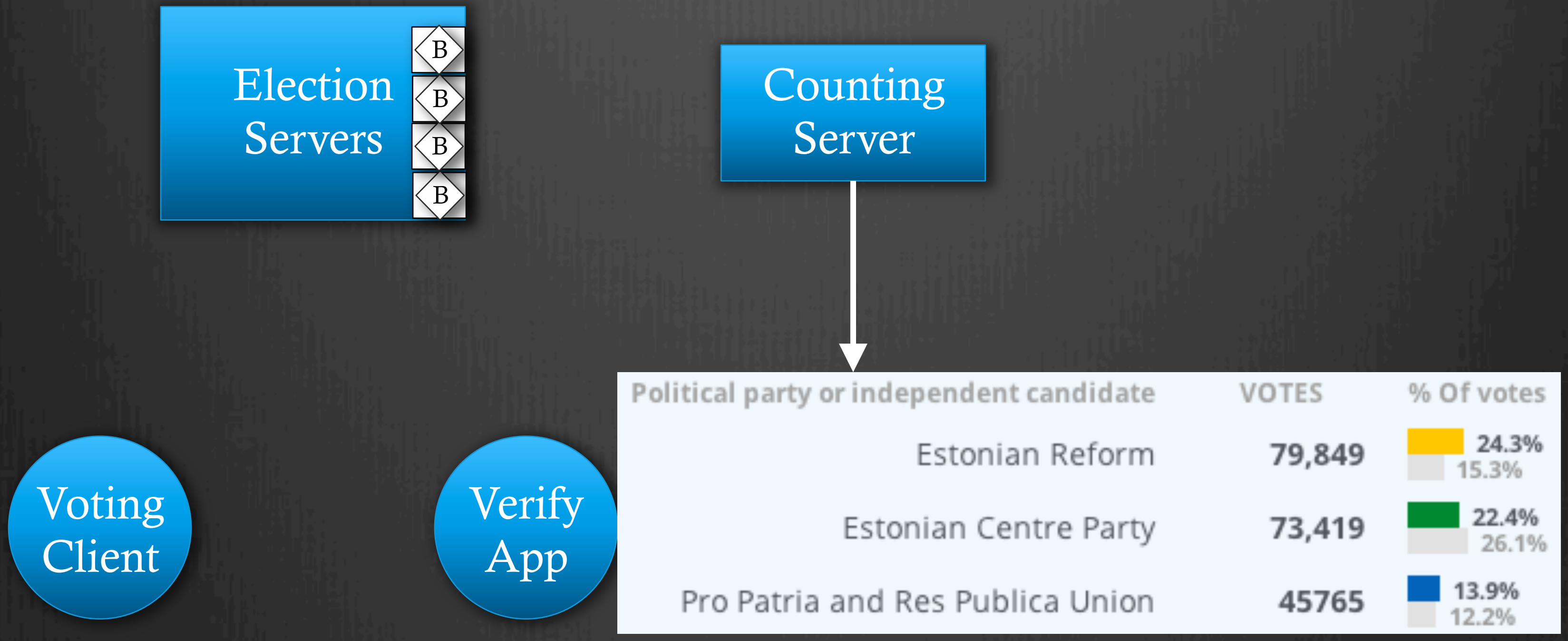
Voting Client

Verify App

Tally Process

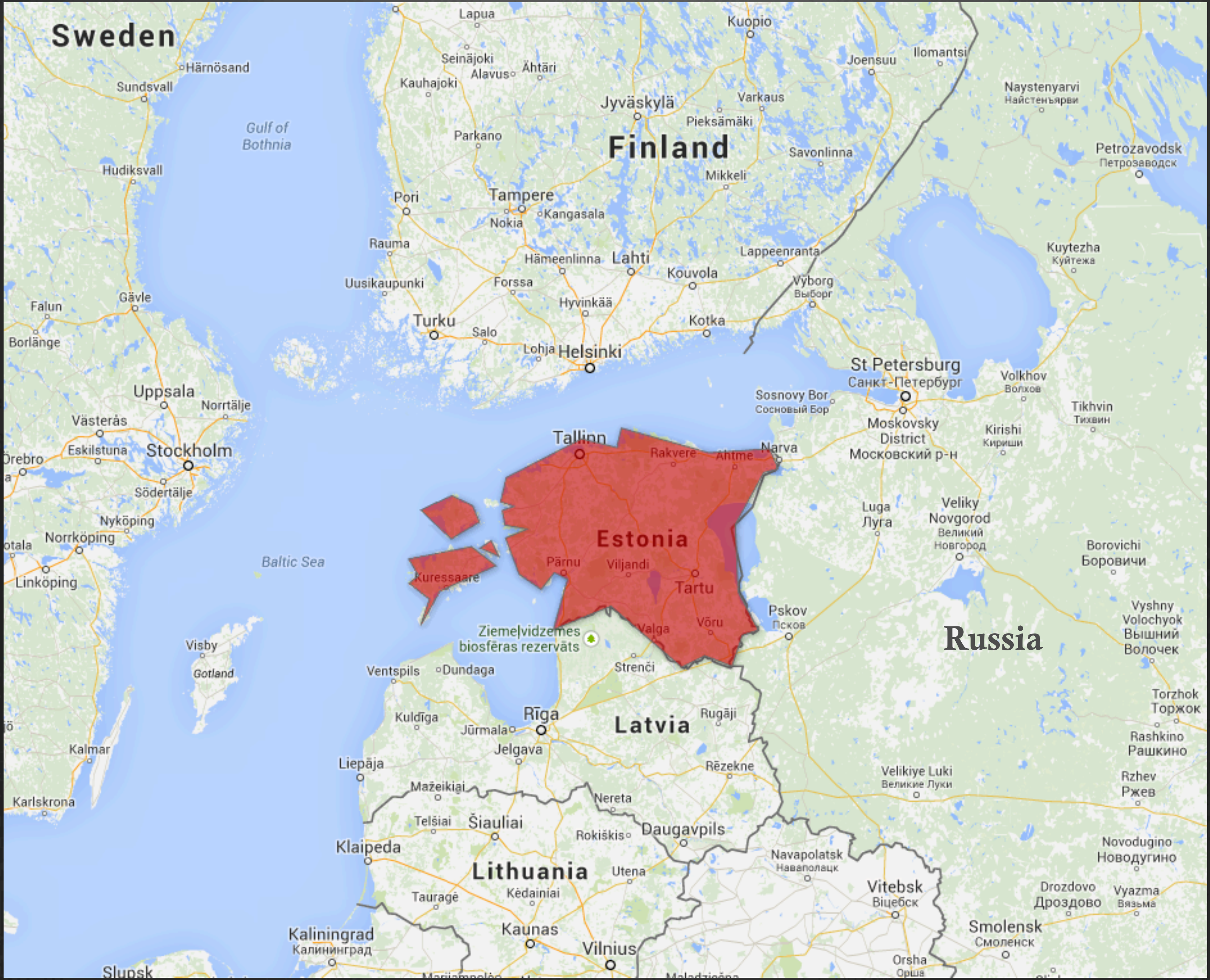


Tally Process



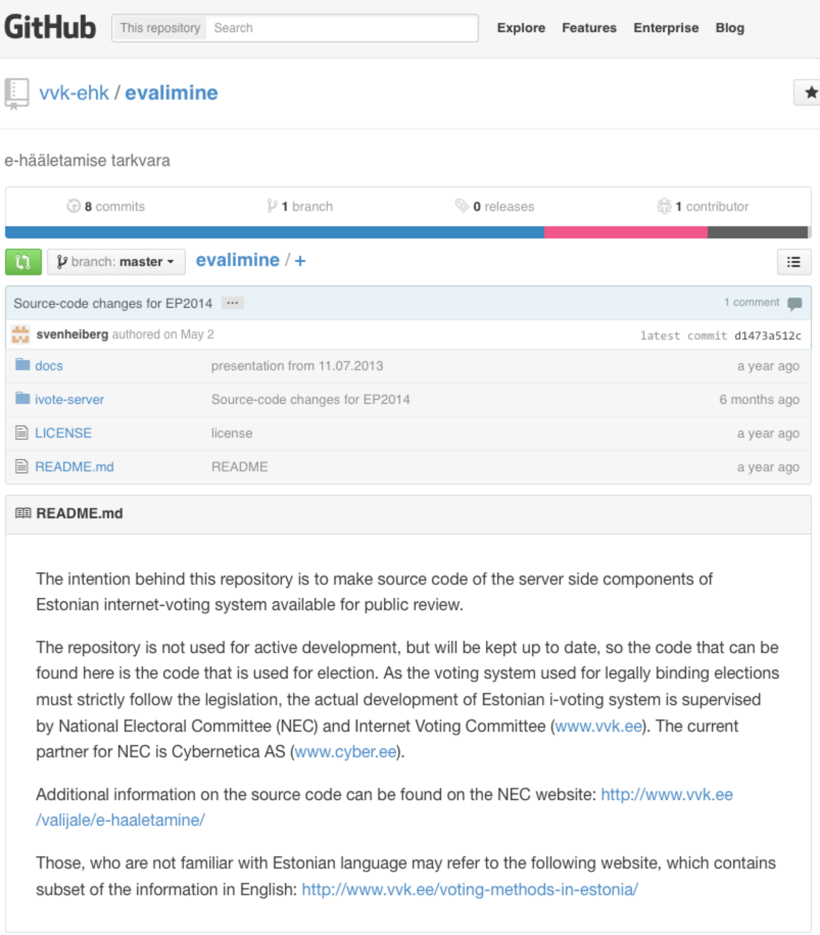
Political party or independent candidate	VOTES	% Of votes
Estonian Reform	79,849	🟨 24.3% 15.3%
Estonian Centre Party	73,419	🟩 22.4% 26.1%
Pro Patria and Res Publica Union	45765	🟦 13.9% 12.2%

- ◆ Motivation
- ◆ How Estonia’s system works
- ◆ **Proper Threat Model**
- ◆ Analysis
- ◆ Estonian Response
- ◆ Conclusions


Sweden
Finland
Estonia
Latvia
Lithuania
Russia
Gulf of Bothnia
Baltic Sea
Gotland
Härnösand
Sundsvall
Hudiksvall
Gävle
Falun
Borlänge
Uppsala
Norrtälje
Västerås
Eskilstuna
Stockholm
Örebro
Södertälje
Nyköping
Norrköping
Linköping
Visby
Kalmar
Karlskrona
Slupsk
Lapua
Seinäjoki
Alavus
Ähtäri
Kauhajoki
Parkano
Kuopio
Joensuu
Ilomantsi
Varkaus
Jyväskylä
Pieksämäki
Savonlinna
Mikkeli
Pori
Tampere
Kangasala
Nokia
Rauma
Hämeenlinna
Lahti
Lappeenranta
Kouvola
Uusikaupunki
Forssa
Hyvinkää
Vyborg
Выборг
Turku
Salo
Kotka
Lohja
Helsinki
Naystenyarvi
Найстенъярви
Petrozavodsk
Петрозаводск
Kuytezha
Куйтежа
St Petersburg
Санкт-Петербург
Sosnovy Bor
Сосновый Бор
Volkhov
Волхов
Tikhvin
Тихвин
Moskovsky District
Московский р-н
Kirishi
Кириши
Tallinn
Rakvere
Ahtme
Narva
Luga
Луга
Veliky Novgorod
Великий Новгород
Borovichi
Боровичи
Pärnu
Viljandi
Tartu
Kuressaare
Valga
Võru
Pskov
Псков
Ziemeļvidzemes biosfēras rezervāts
Vyshny Volochyok
Вышний Волочек
Ventspils
Dundaga
Strenči
Kuldīga
Rīga
Jūrmala
Jelgava
Rugāji
Torzhok
Торжок
Rashkino
Рашкино
Liepāja
Rēzekne
Velikiye Luki
Великие Луки
Rzhev
Ржев
Mažeikiai
Nereta
Telšiai
Šiauliai
Rokiškis
Daugavpils
Klaipeda
Navapolatsk
Наваполацк
Novodugino
Новодугино
Utena
Vitebsk
Віцебск
Tauragė
Kėdainiai
Drozdovo
Дроздово
Vyazma
Вязьма
Kaliningrad
Калининград
Kaunas
Vilnius
Smolensk
Смоленск
Orsha
Орша

- Motivation
- How Estonia’s system works
- Proper Threat Model
- **Analysis**
- Estonian Response
- Conclusions

Analysis Approaches



e-hääletamise tarkvara

Source-code changes for EP2014 ··· 1 comment

svenheiberg authored on May 2 latest commit d1473a512c

docs	presentation from 11.07.2013	a year ago
ivote-server	Source-code changes for EP2014	6 months ago
LICENSE	license	a year ago
README.md	README	a year ago

README.md

The intention behind this repository is to make source code of the server side components of Estonian internet-voting system available for public review.

The repository is not used for active development, but will be kept up to date, so the code that can be found here is the code that is used for election. As the voting system used for legally binding elections must strictly follow the legislation, the actual development of Estonian i-voting system is supervised by National Electoral Committee (NEC) and Internet Voting Committee (www.vvk.ee). The current partner for NEC is Cybernetica AS (www.cyber.ee).

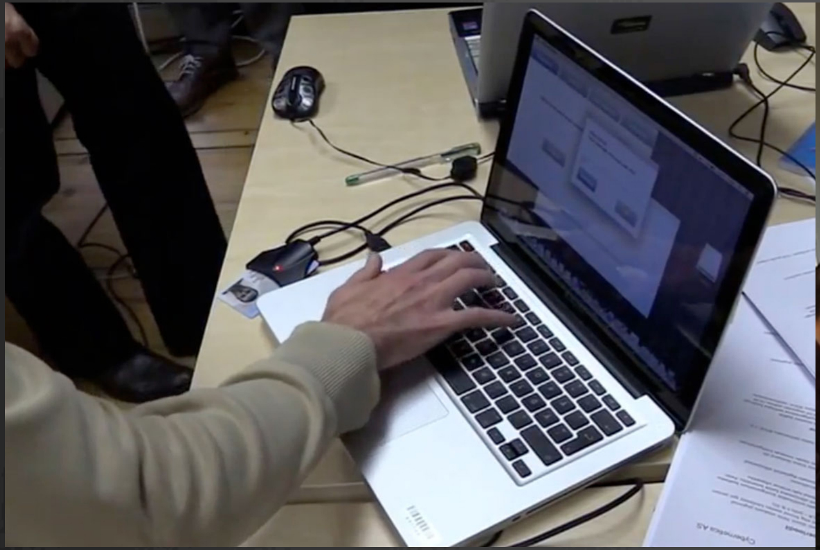
Additional information on the source code can be found on the NEC website: http://www.vvk.ee/valijale/e-haaletamine/

Those, who are not familiar with Estonian language may refer to the following website, which contains subset of the information in English: http://www.vvk.ee/voting-methods-in-estonia/

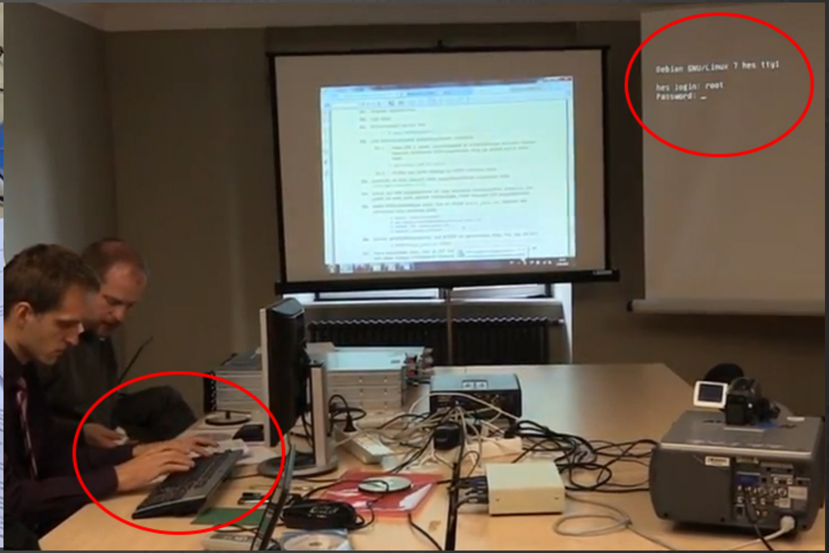
Observational Approach

- Observed 2013 Local Elections
- Interviewed election officials, developers, and researchers
- Reviewed 20+ hours of official election videos
- Studied written procedures

OPSEC Failures



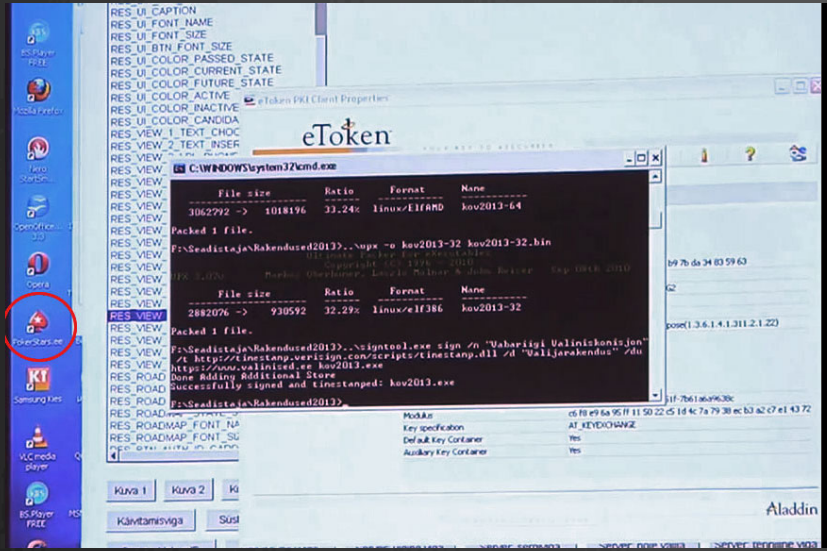
ID card PINs on camera



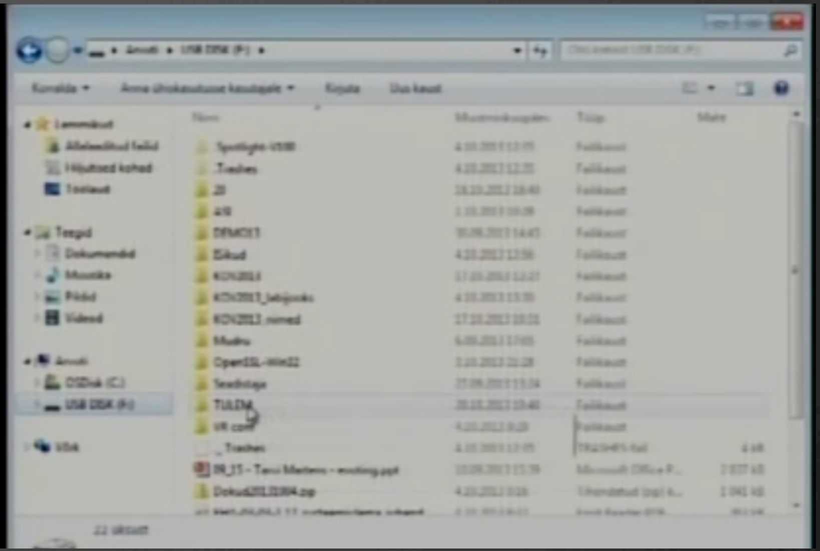
```
Debian GNU/Linux 7 hes tty1

hes login: root
Password: _
```

Root password on camera

OPSEC Failures



```
C:\WINDOWS\system32\cmd.exe
        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   3062792 ->   1018196   33.24%   linux/ElfAMD   kov2013-64

Packed 1 file.

F:\Seadistaja\Rakendused2013>..\upx -o kov2013-32 kov2013-32.bin
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2010
UPX 3.07w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   2882076 ->    930592   32.29%   linux/elf386   kov2013-32

Packed 1 file.

F:\Seadistaja\Rakendused2013>..\signtool.exe sign /n "Vabariigi Valimiskomisjon"
 /t http://timestamp.verisign.com/scripts/timestamp.dll /d "Valijarakendus" /du
https://www.valimised.ee kov2013.exe
Done Adding Additional Store
Successfully signed and timestamped: kov2013.exe

F:\Seadistaja\Rakendused2013>
```

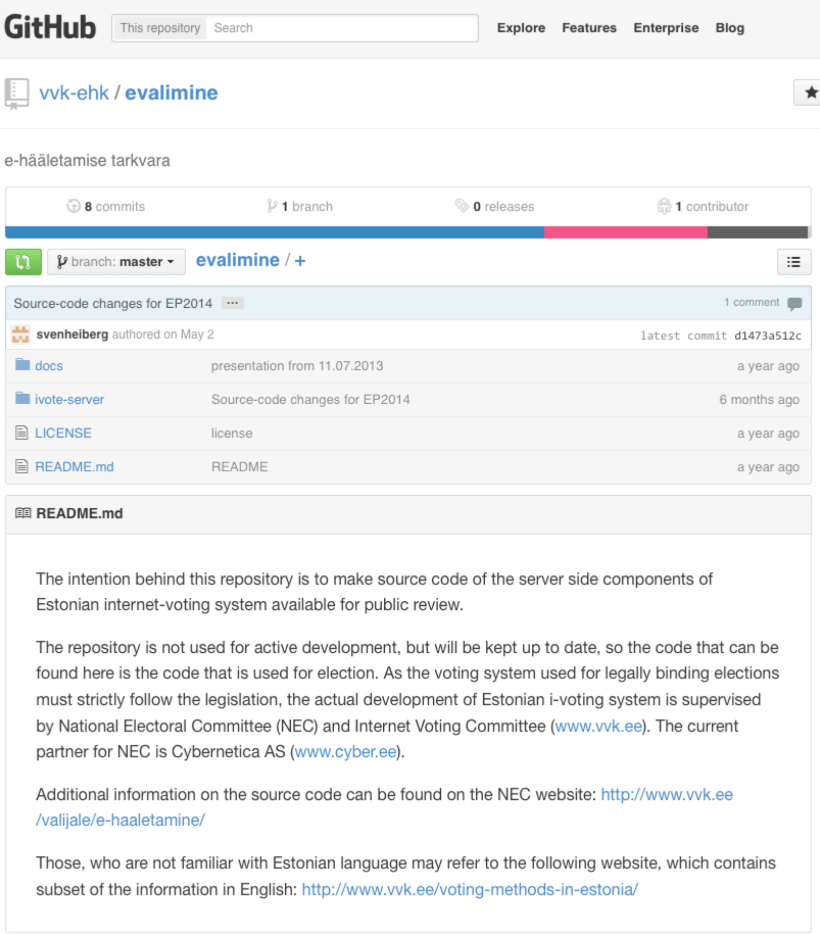


Voting Client built on personal computer

Personal USB stick used for transferring results

Technical Approach

- Reproduced system in lab
- Core of server source code available on GitHub
- Patched voting client
- Built proof-of-concept attacks



vvk-ehk / evalimine

e-hääletamise tarkvara

8 commits | 1 branch | 0 releases | 1 contributor

evalimine / +

Source-code changes for EP2014 ··· 1 comment

svenheiberg authored on May 2 — latest commit d1473a512c

docs	presentation from 11.07.2013	a year ago
ivote-server	Source-code changes for EP2014	6 months ago
LICENSE	license	a year ago
README.md	README	a year ago

README.md

The intention behind this repository is to make source code of the server side components of Estonian internet-voting system available for public review.

The repository is not used for active development, but will be kept up to date, so the code that can be found here is the code that is used for election. As the voting system used for legally binding elections must strictly follow the legislation, the actual development of Estonian i-voting system is supervised by National Electoral Committee (NEC) and Internet Voting Committee (www.vvk.ee). The current partner for NEC is Cybernetica AS (www.cyber.ee).

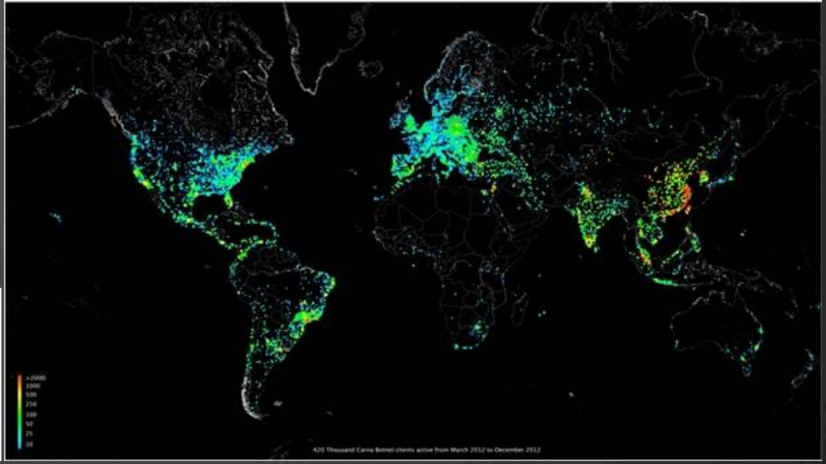
Additional information on the source code can be found on the NEC website: http://www.vvk.ee/valijale/e-haaletamine/

Those, who are not familiar with Estonian language may refer to the following website, which contains subset of the information in English: http://www.vvk.ee/voting-methods-in-estonia/

Client Infection Method

metasploit®

CORE IMPACT™
PROFESSIONAL

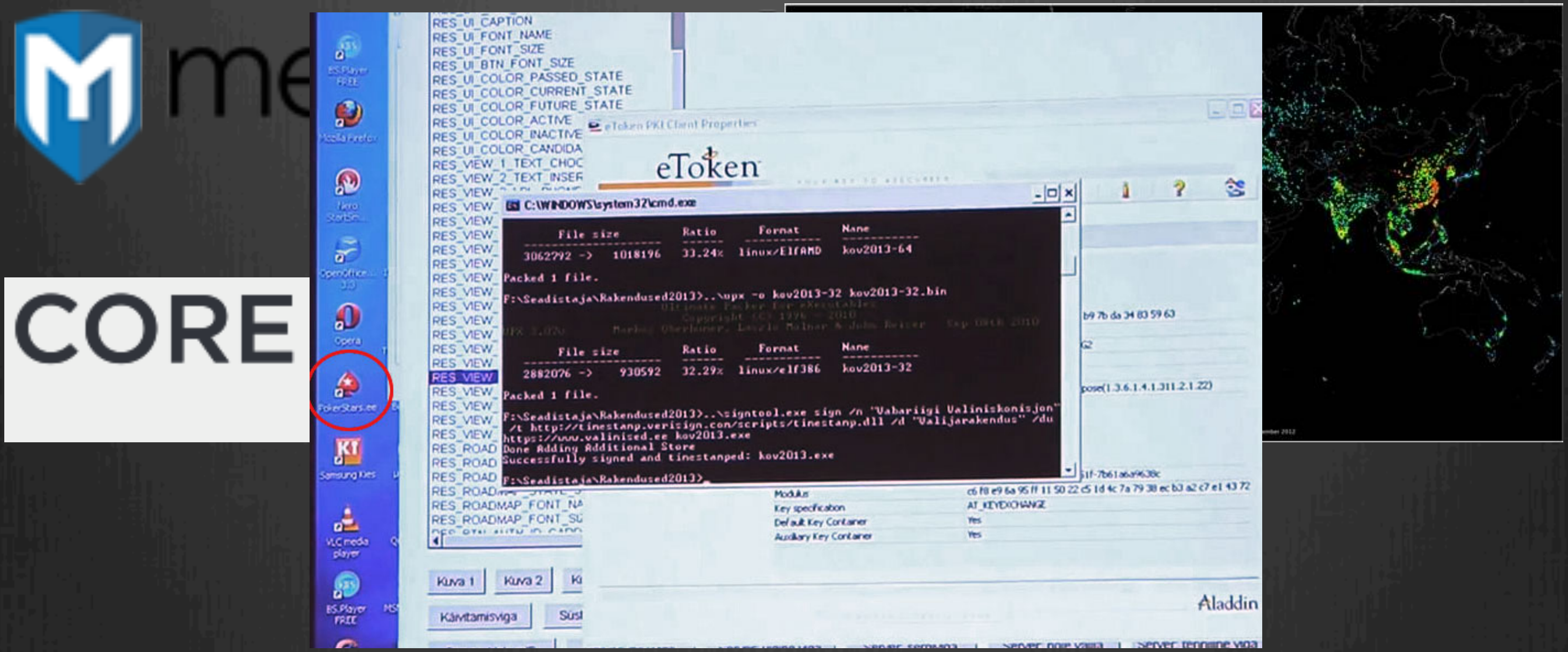


420 Thousand Carna Botnet clients active from March 2012 to December 2012

0-day

Botnet

Client Infection Method

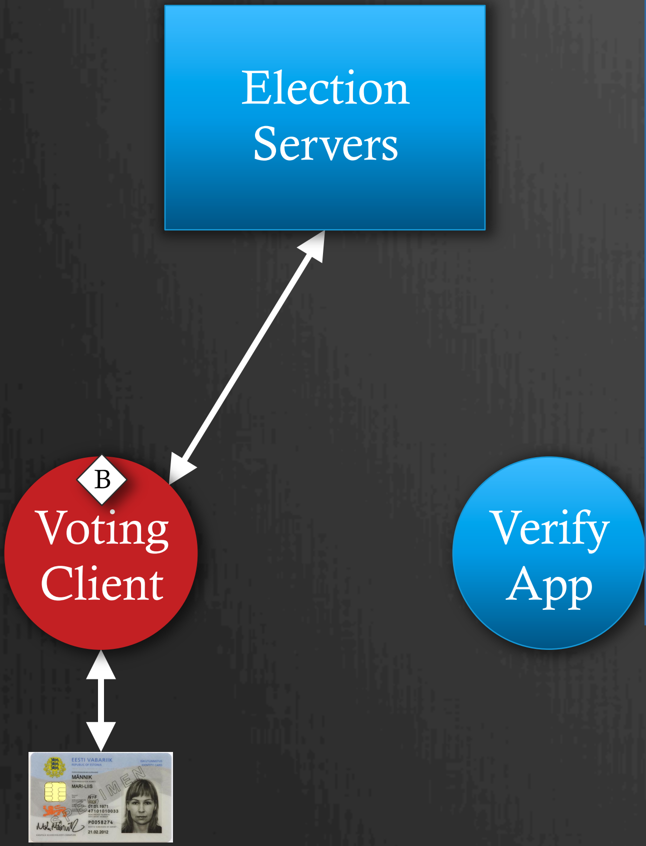


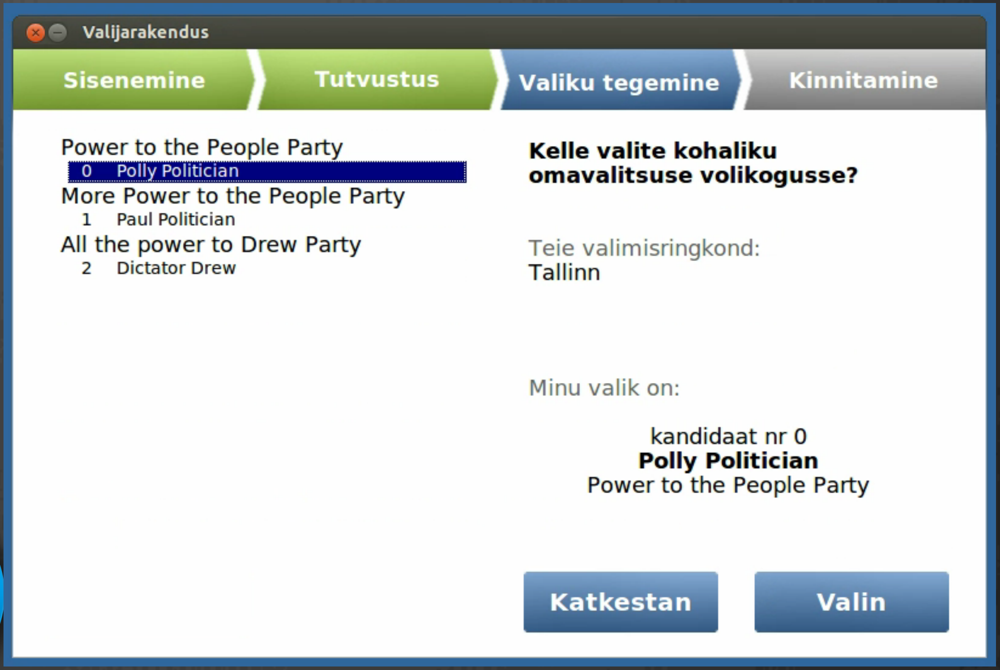
```
C:\WINDOWS\system32\cmd.exe

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   3062792 ->   1018196   33.24%   linux/ElfAMD   kov2013-64

Packed 1 file.

F:\Seadistaja\Rakendused2013>..\upx -o kov2013-32 kov2013-32.bin
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2010
UPX 3.07w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   2882076 ->    930592   32.29%   linux/elf386   kov2013-32

Packed 1 file.

F:\Seadistaja\Rakendused2013>..\signtool.exe sign /n "Vabariigi Valimiskomisjon"
 /t http://timestamp.verisign.com/scripts/timestamp.dll /d "Valijarakendus" /du
https://www.valimised.ee kov2013.exe
Done Adding Additional Store
Successfully signed and timestamped: kov2013.exe

F:\Seadistaja\Rakendused2013>
```

Modulus: c6 f8 e9 6a 95 ff 11 50 22 c5 1d 4c 7a 79 38 ec b3 a2 c7 e1 43 72
Key specification: AT_KEYEXCHANGE
Default Key Container: Yes
Auxiliary Key Container: Yes

Infect voting client

Client-side Attack





Power to the People Party
0 Polly Politician
More Power to the People Party
1 Paul Politician
All the power to Drew Party
2 Dictator Drew

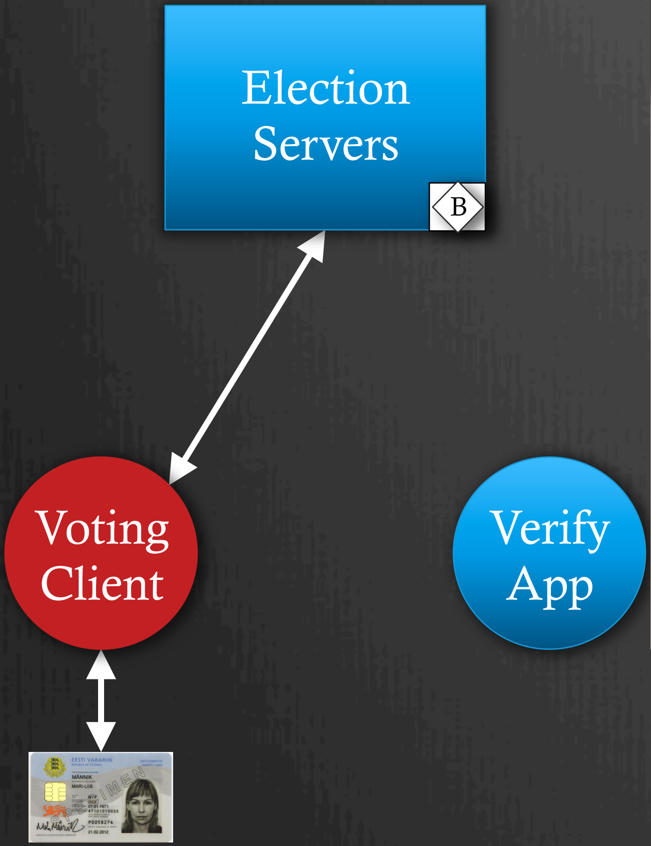
Kelle valite kohaliku omavalitsuse volikogusse?

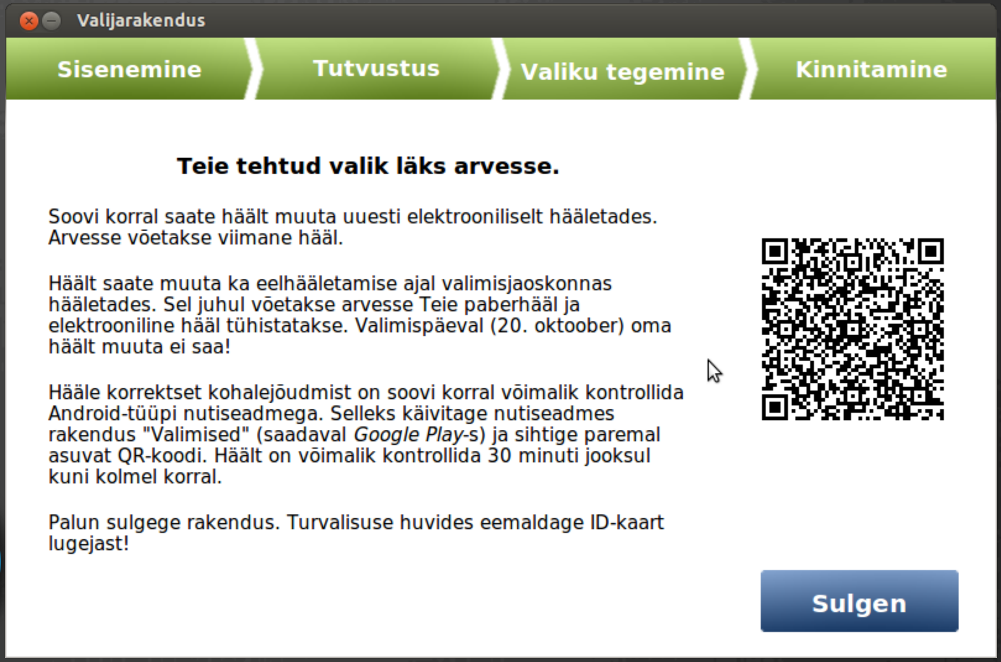
Teie valimisringkond:
Tallinn

Minu valik on:

kandidaat nr 0
Polly Politician
Power to the People Party

Client-side Attack





Teie tehtud valik läks arvesse.

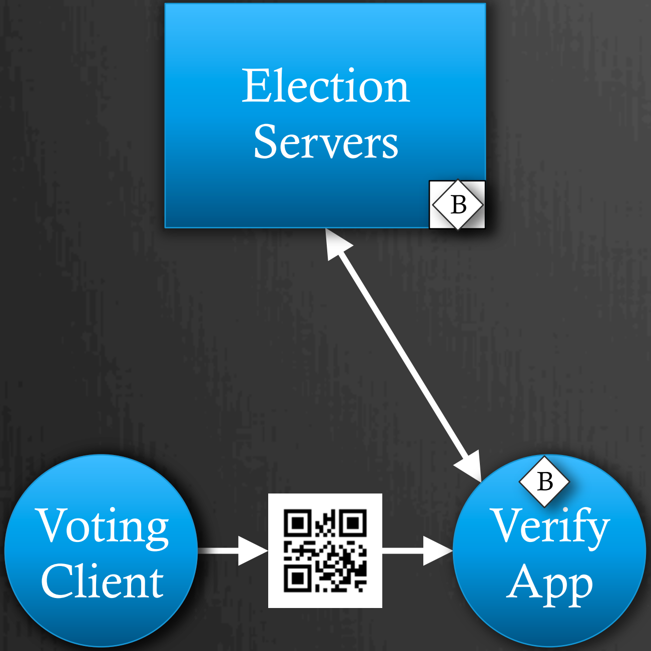
Soovi korral saate häält muuta uuesti elektrooniliselt hääletades. Arvesse võetakse viimane hääl.

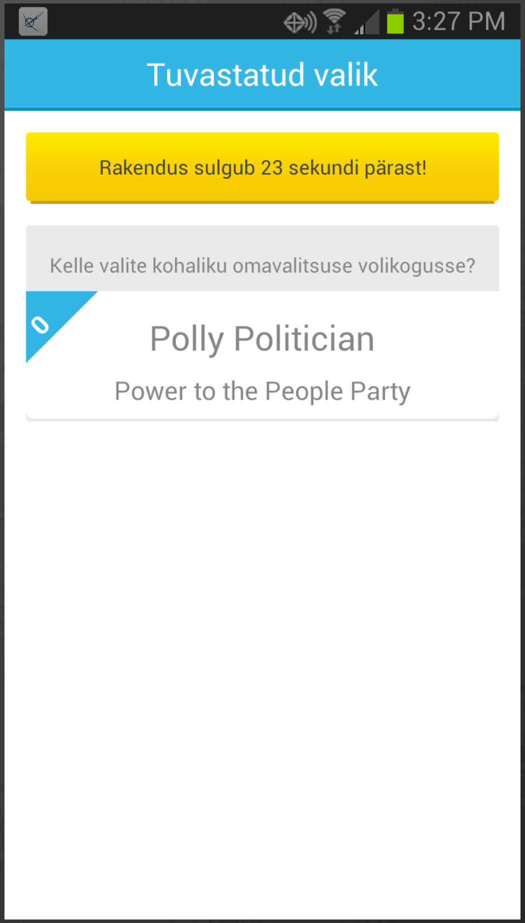
Häält saate muuta ka eelhääletamise ajal valimisjaoskonnas hääletades. Sel juhul võetakse arvesse Teie paberhääl ja elektrooniline hääl tühistatakse. Valimispäeval (20. oktoober) oma häält muuta ei saa!

Hääle korrektset kohalejõudmist on soovi korral võimalik kontrollida Android-tüüpi nutiseadmega. Selleks käivitage nutiseadmes rakendus "Valimised" (saadaval *Google Play*-s) ja sihtige paremal asuvat QR-koodi. Häält on võimalik kontrollida 30 minuti jooksul kuni kolmel korral.

Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart lugejast!

Client-side Attack




3:27 PM

Tuvastatud valik

Rakendus sulgub 23 sekundi pärast!

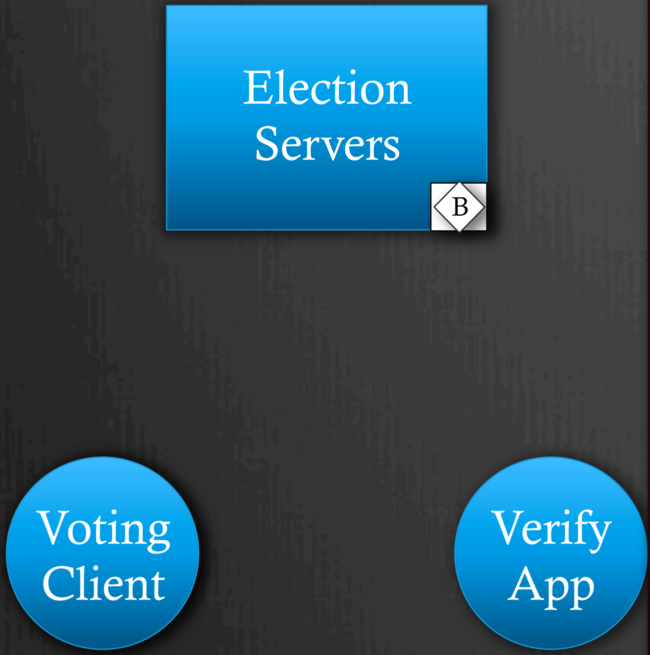
Kelle valite kohaliku omavalitsuse volikogusse?

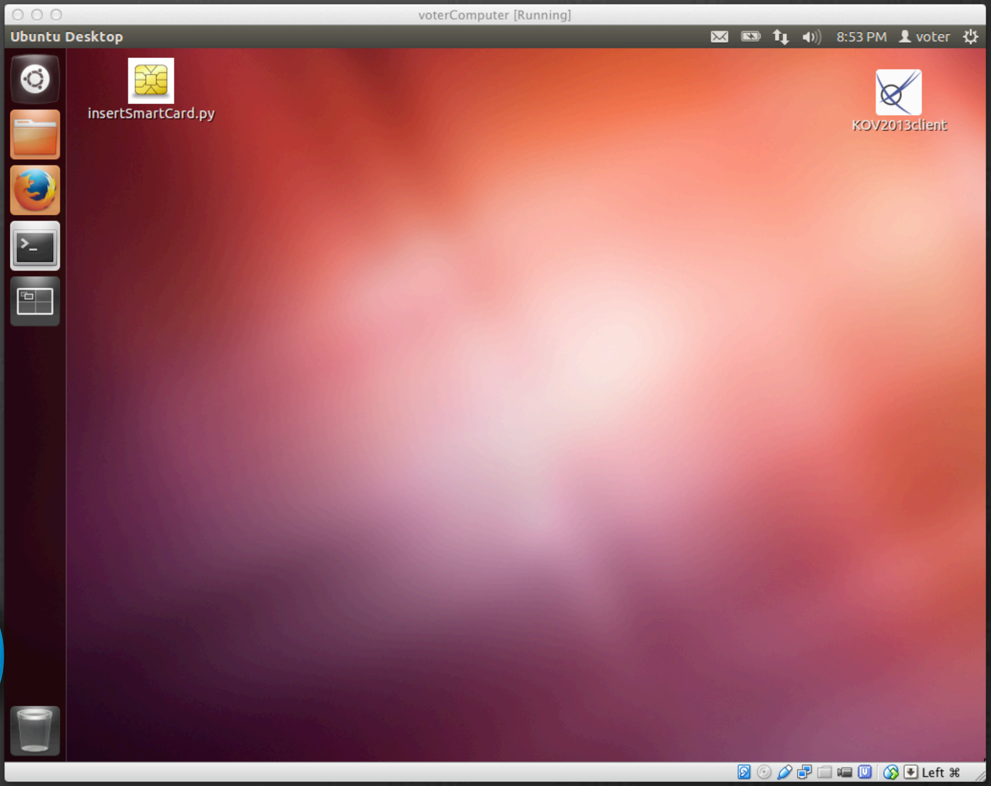
0

Polly Politician

Power to the People Party

Client-side Attack





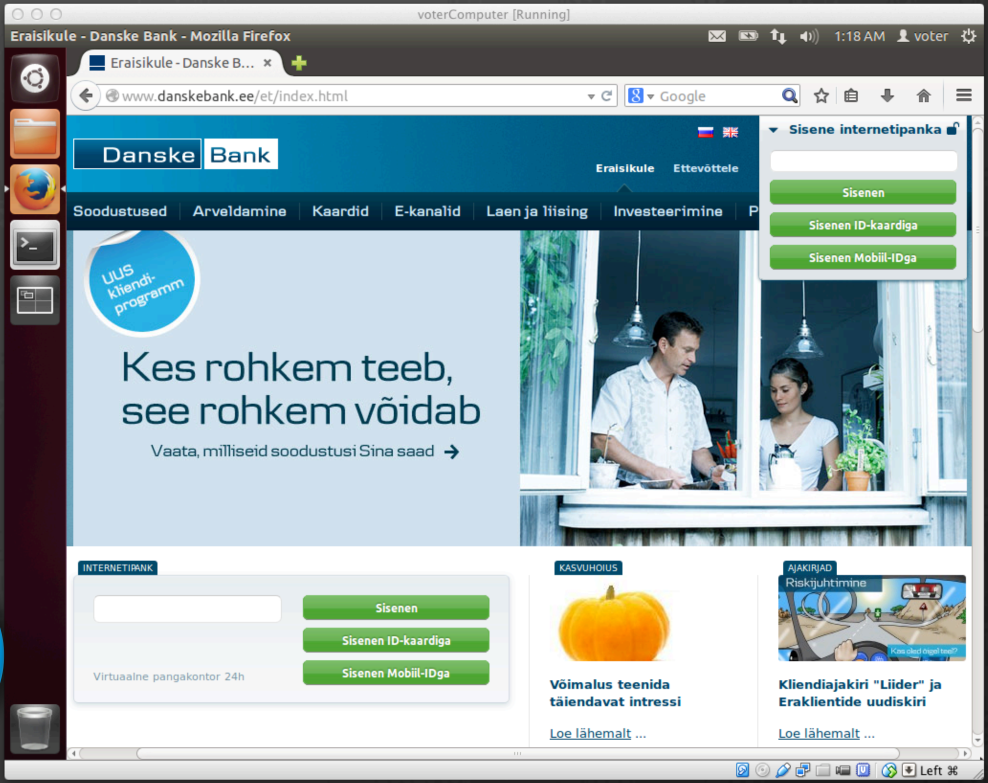
Client-side Attack

Election Servers

B

Voting Client

Verify App



Kes rohkem teeb, see rohkem võidab

Vaata, milliseid soodustusi Sina saad →

Virtuaalne pangakontor 24h

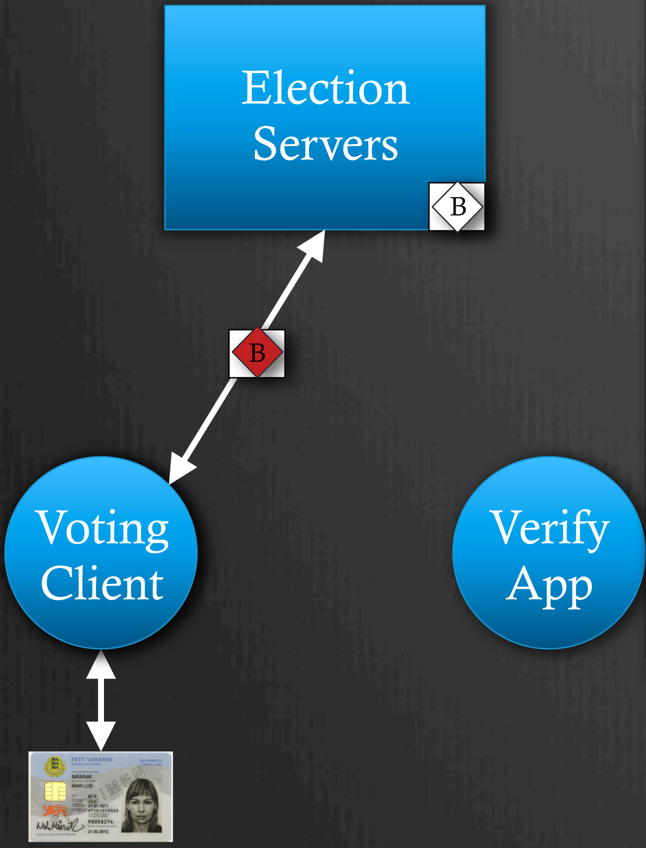
Võimalus teenida täiendavat intressi

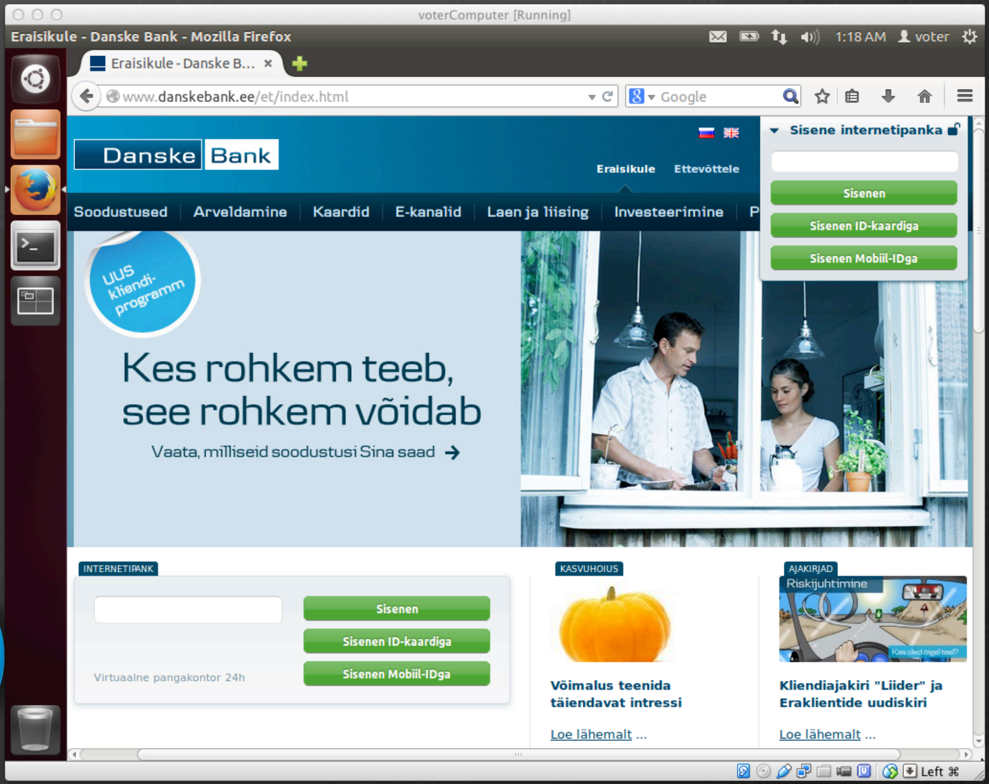
Loe lähemalt ...

Kliendiajakiri "Liider" ja Eraklientide uudiskiri

Loe lähemalt ...

Client-side Attack





Kes rohkem teeb, see rohkem võidab

Vaata, milliseid soodustusi Sina saad →

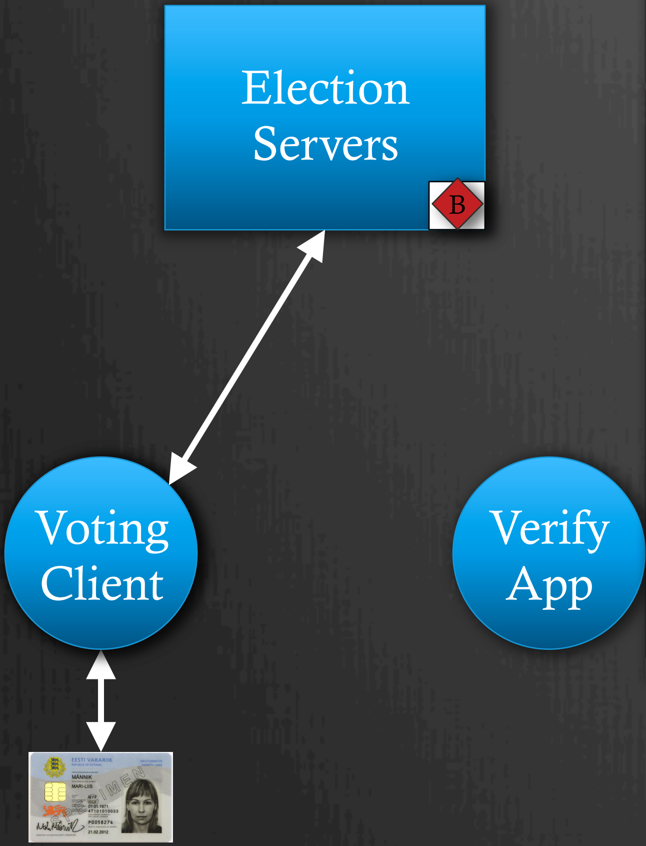
Võimalus teenida täiendavat intressi

Loe lähemalt ...

Kliendiajakiri "Liider" ja Eraklientide uudiskiri

Loe lähemalt ...

Client-side Attack

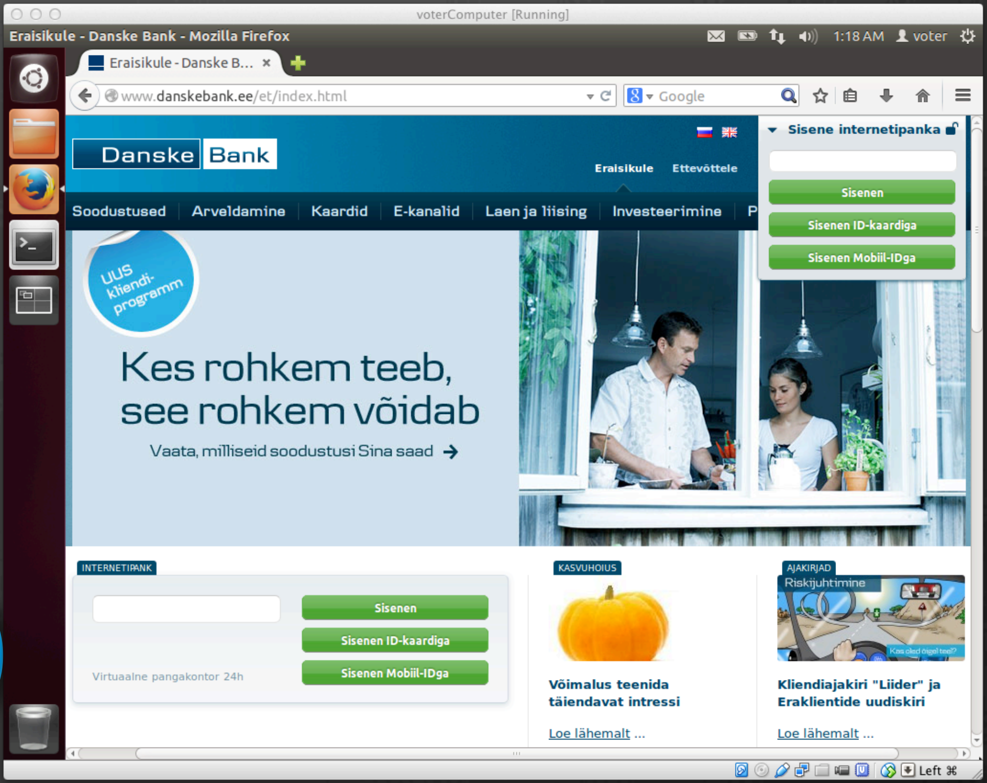


Election Servers

B

Voting Client

Verify App



Kes rohkem teeb, see rohkem võidab

Vaata, milliseid soodustusi Sina saad →

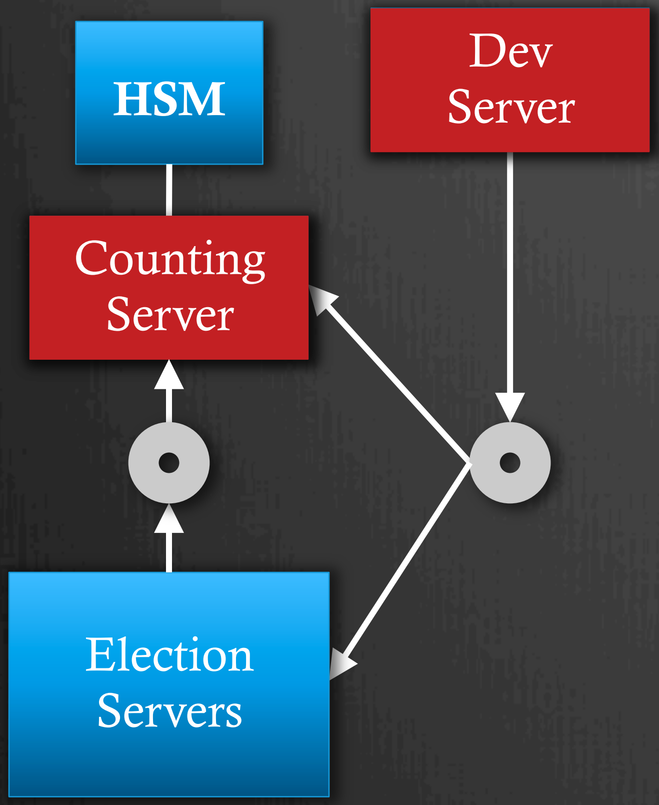
Võimalus teenida täiendavat intressi

Loe lähemalt ...

Kliendiajakiri "Liider" ja Eraklientide uudiskiri

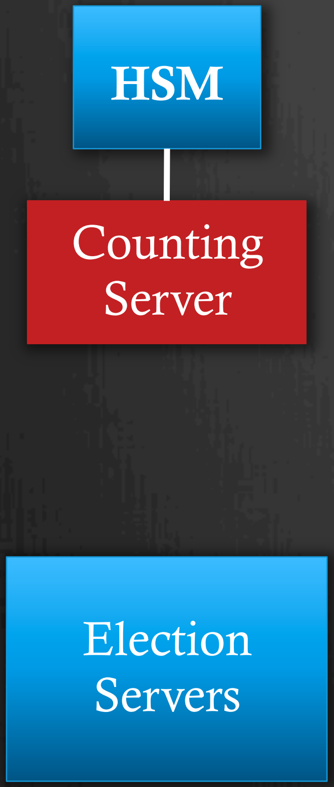
Loe lähemalt ...

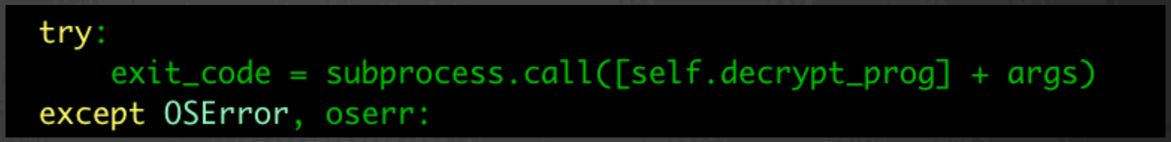
Server Infection Method



- Votes stripped and exported to the Counting Server
- HSM decrypts votes and returns to be counted
- OS ISO stored on Dev Server
- Attack Dev Server
  - Inject malware into OS ISO
  - Election officials spread malware during Configuration Ceremony

Server-side Attack





```
try:
    exit_code = subprocess.call([self.decrypt_prog] + args)
except OSError, oserr:
```

- Motivation
- How Estonia’s system works
- Proper Threat Model
- Analysis
- **Estonian Response**
- Conclusions

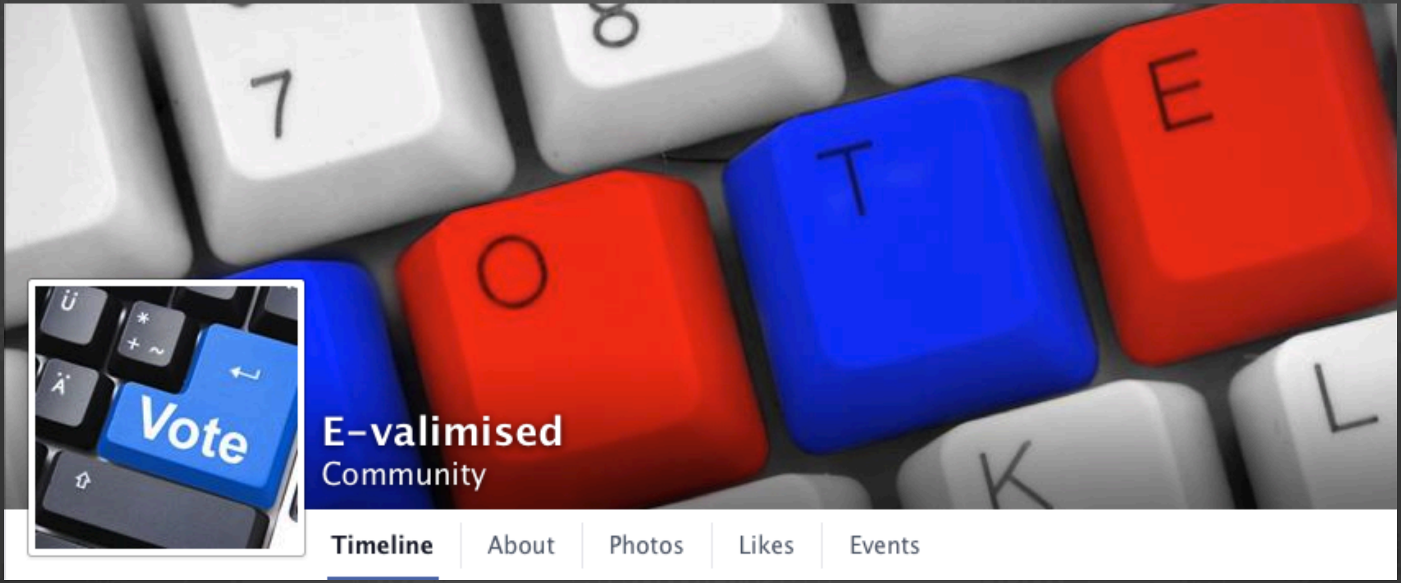
Politician Response

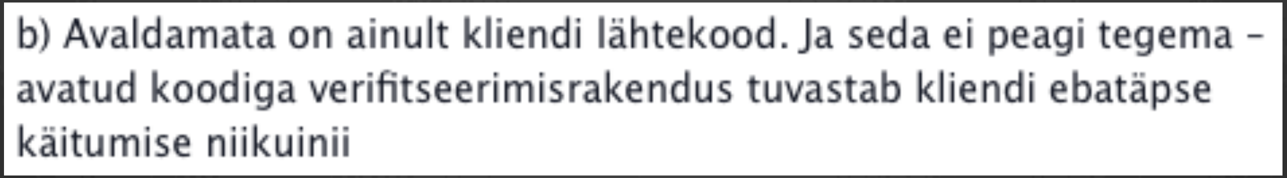
Prime Minister Taavi Rõivas

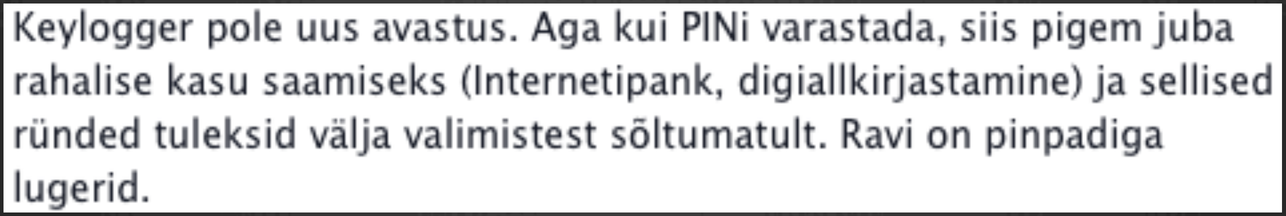
Facebook says they're agents of the [other] party

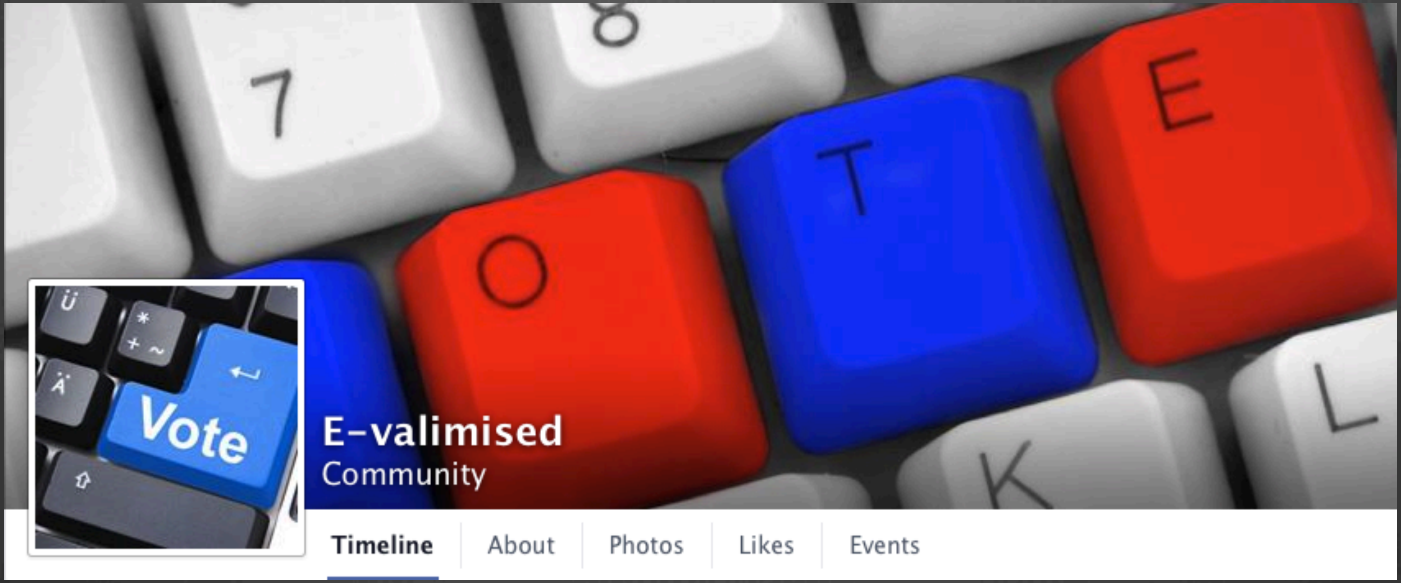
President Toomas Hendrik Ilves

Our security is better than Google's




b) Avaldamata on ainult kliendi lähtekood. Ja seda ei peagi tegema – avatud koodiga verifitseerimisrakendus tuvastab kliendi ebatäpse käitumise niikuinii

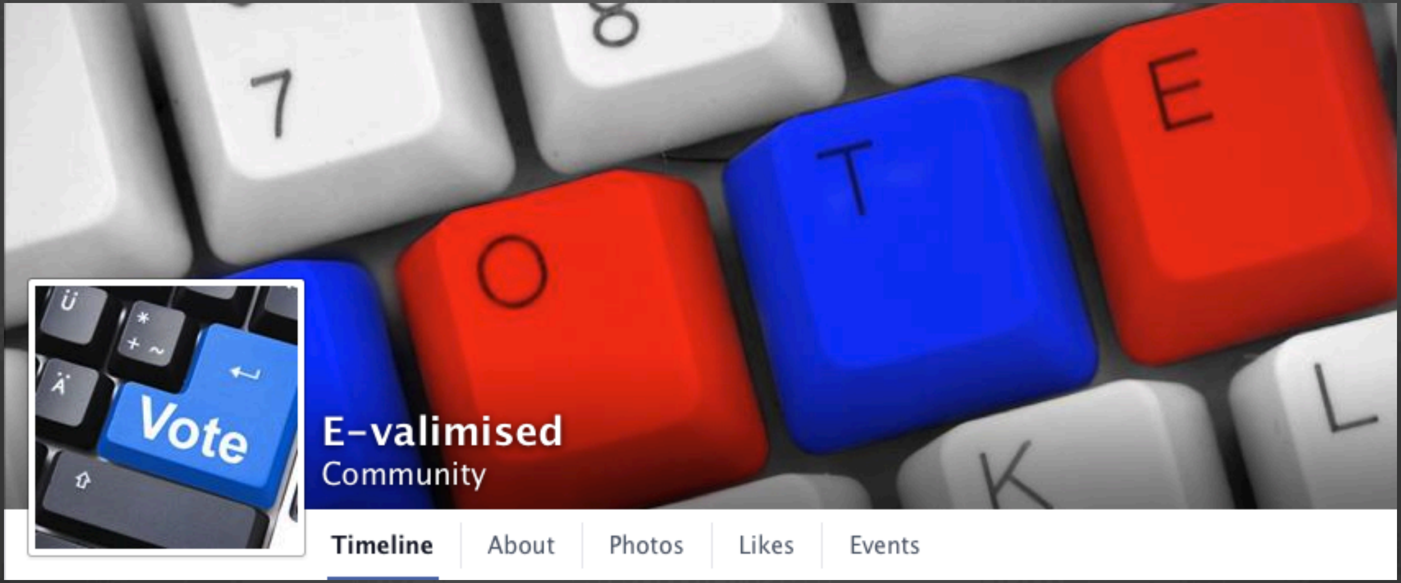

Keylogger pole uus avastus. Aga kui PINi varastada, siis pigem juba rahalise kasu saamiseks (Internetipank, digiallkirjastamine) ja sellised ründed tuleksid välja valimistest sõltumatult. Ravi on pinpadiga lugerid.



b) Avaldamata on ainult kliendi lähtekood. Ja seda ei peagi tegema – avat[illegible]se käitumise niikuinii

Verification app detects all bad behavior.

Keylogger pole uus avastus. Aga kui PINi varastada, siis pigem juba rahalise kasu saamiseks (Internetipank, digiallkirjastamine) ja sellised ründed tuleksid välja valimistest sõltumatult. Ravi on pinpadiga lugerid.

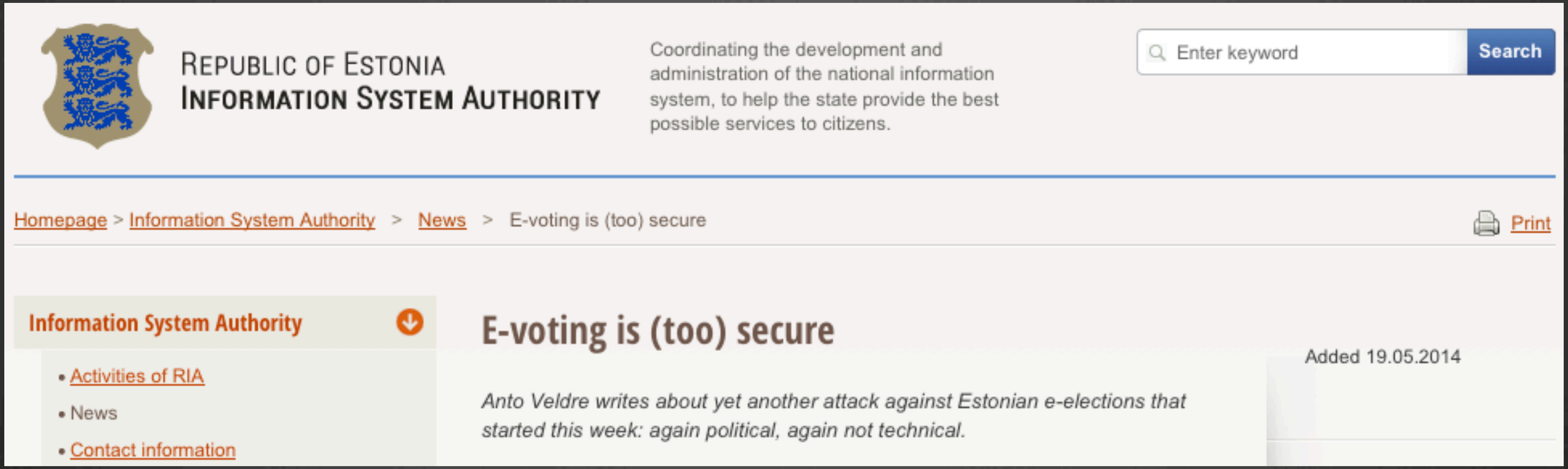


Verification app detects all bad behavior.

b) Avaldamata on ainult kliendi lähtekood. Ja seda ei peagi tegema – avat[illegible] käitumise niikuinii

Why steal votes when you can steal money?

Keylogger pole uus avastus. Aga kui PINi varastada, siis pigem juba rahalise kasu saamiseks (Internetipank, digiallkirjastamine) ja sellised ründed [illegible] valja valimistest sõltumatult. Kavi on pinpadiga lugerid.


REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Coordinating the development and administration of the national information system, to help the state provide the best possible services to citizens.

Homepage > Information System Authority > News > E-voting is (too) secure

Information System Authority

- Activities of RIA
- News
- Contact information

E-voting is (too) secure

Added 19.05.2014

Anto Veldre writes about yet another attack against Estonian e-elections that started this week: again political, again not technical.

- “nice people who care about computer hygiene have no viruses”
- “In practice, computer risks have been eliminated”
- “they’re here not because of their technical savvy, but their politically suitable (although technically incompetent) message”

- Motivation
- How Estonia’s system works
- Proper Threat Model
- Analysis
- Estonian Response
- **Conclusions**

Conclusions

- Threat model should include state-level attackers.
- Attackers could exploit Estonian system to alter results.
  - Major weaknesses are architectural and not easily fixed.
- Lax operational security observed in many areas.
  - Possibly a practical reality of implementation.
- *Recommendation*: Estonia should discontinue Internet voting until there are fundamental technical advances.

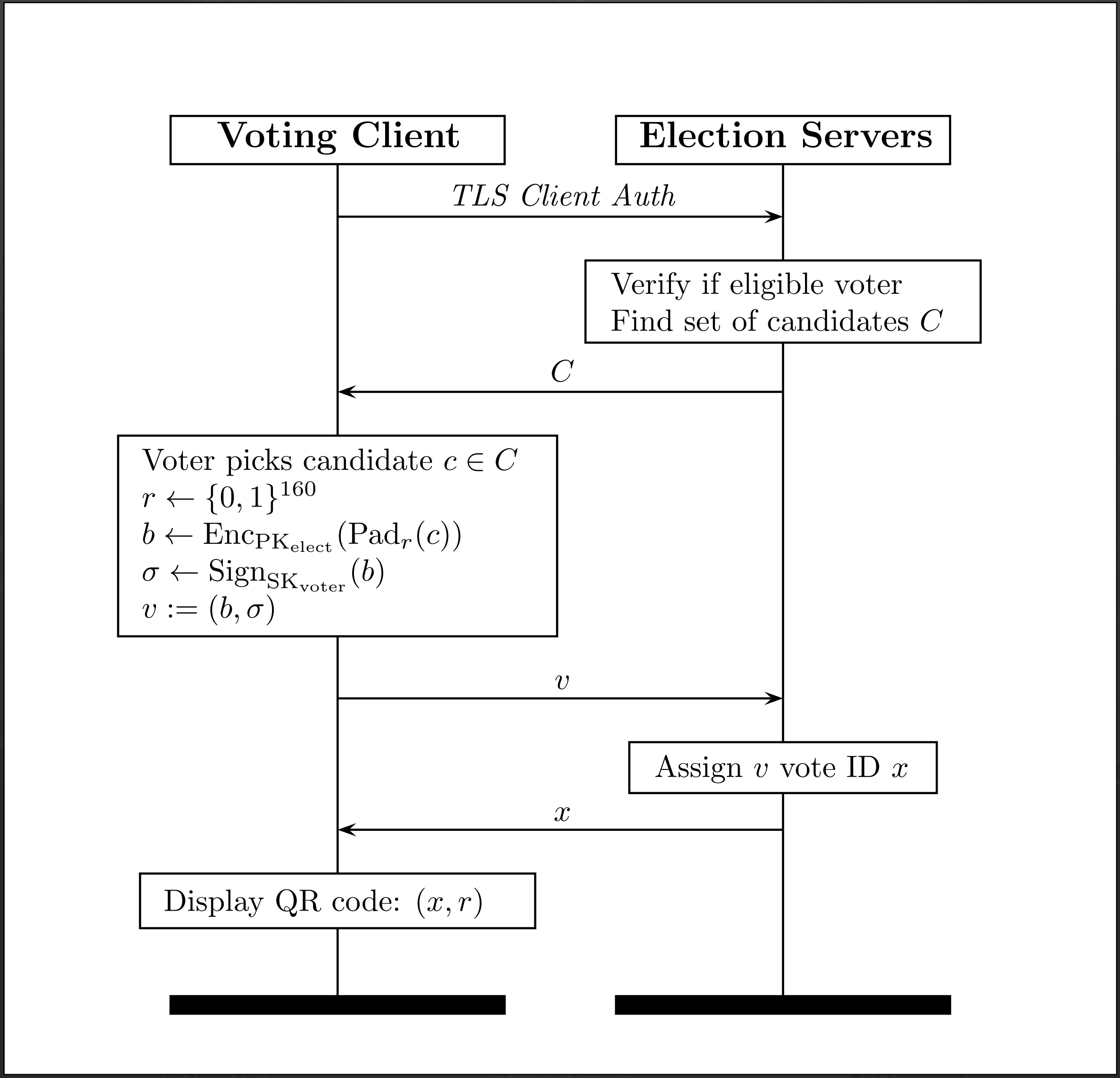
Security Analysis of the Estonian Internet Voting System

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat,
Harri Hursti, Margaret MacAlpine, and J. Alex Halderman

Backup slides

STOP

Voting Protocol



Voting Client

Election Servers

TLS Client Auth

Verify if eligible voter
Find set of candidates C

C

Voter picks candidate $c \in C$
$r \leftarrow \{0,1\}^{160}$
$b \leftarrow \mathrm{Enc}_{\mathrm{PK}_{\mathrm{elect}}}(\mathrm{Pad}_r(c))$
$\sigma \leftarrow \mathrm{Sign}_{\mathrm{SK}_{\mathrm{voter}}}(b)$
$v := (b, \sigma)$

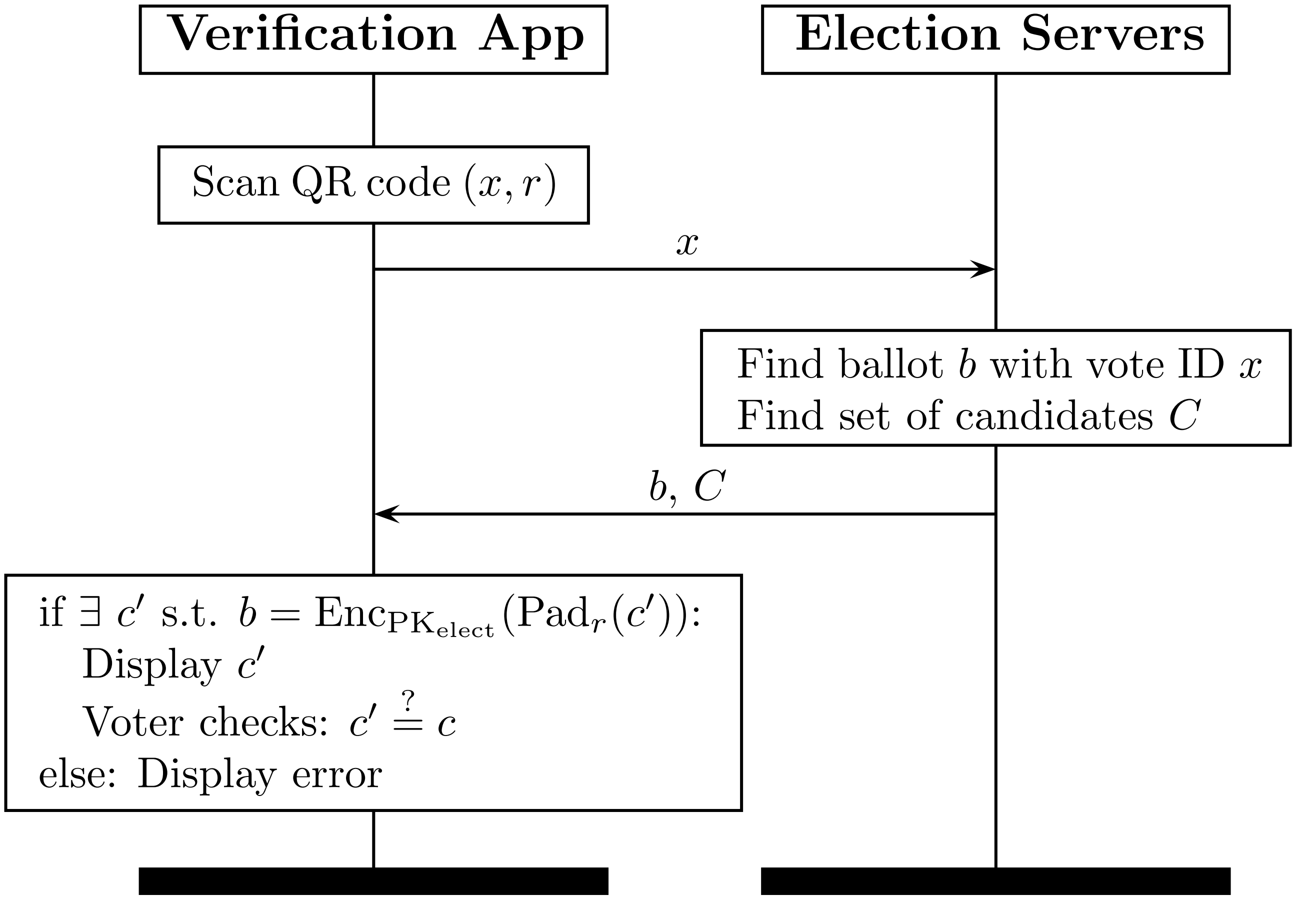
v

Assign v vote ID x

x

Display QR code: (x, r)

Verify Protocol



Verification App

Election Servers

Scan QR code (x, r)

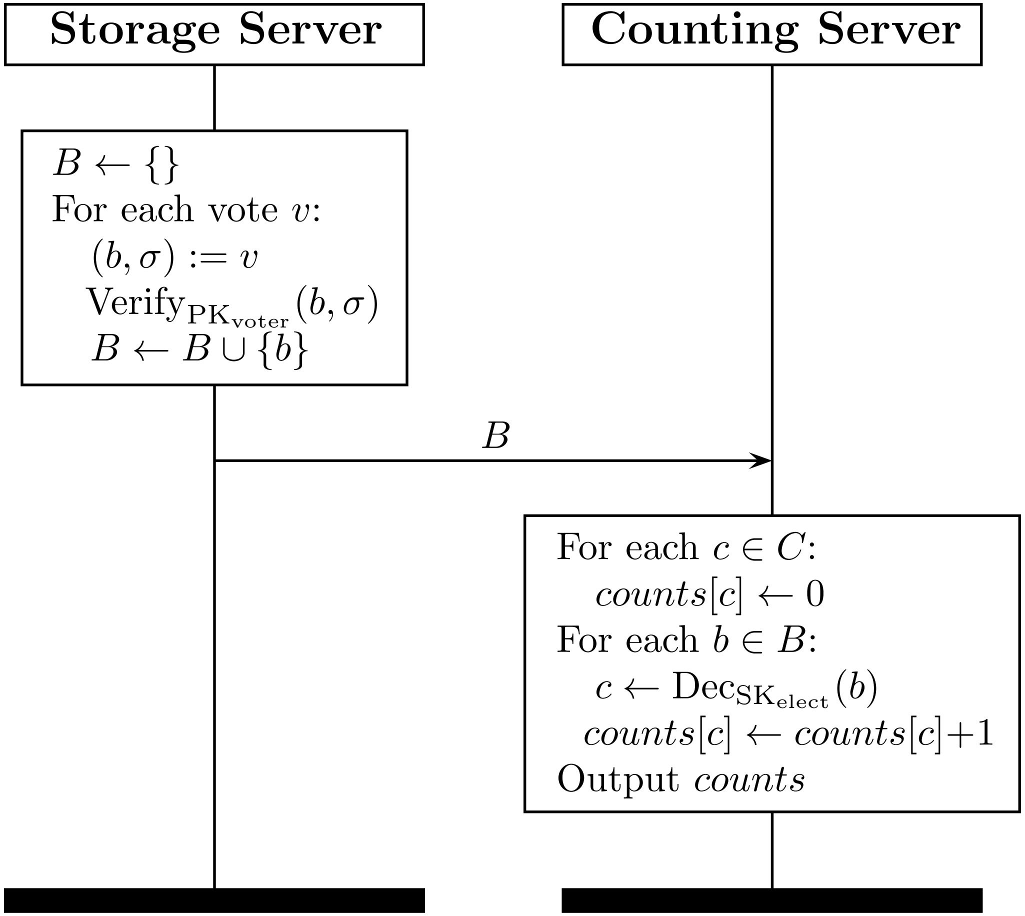
x

Find ballot b with vote ID x
Find set of candidates C

b, C

```
if $\exists\ c'$ s.t. $b = \mathrm{Enc}_{\mathrm{PK}_{\mathrm{elect}}}(\mathrm{Pad}_r(c'))$:
   Display $c'$
   Voter checks: $c' \overset{?}{=} c$
else: Display error
```

Counting Protocol



```
$B \leftarrow \{\}$
For each vote $v$:
    $(b, \sigma) := v$
    $\mathrm{Verify}_{\mathrm{PK}_{\mathrm{voter}}}(b, \sigma)$
    $B \leftarrow B \cup \{b\}$
```

```
For each $c \in C$:
    $counts[c] \leftarrow 0$
For each $b \in B$:
    $c \leftarrow \mathrm{Dec}_{\mathrm{SK}_{\mathrm{elect}}}(b)$
    $counts[c] \leftarrow counts[c]{+}1$
Output $counts$
```