SECURITY ANALYSIS OF THE ESTONIAN INTERNET VOTING SYSTEM

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


Sweden
Gulf of Bothnia
Norway
Finland
Turku
Helsinki
Saint Petersburg
Санкт-Петербург
Oslo
Stockholm
Tallinn
Estonia
Baltic Sea
Gothenburg
Riga
Latvia
Moscow
Москва
Denmark
Copenhagen
Lithuania
Kaunas
Vilnius
Gdańsk
Minsk
Мінск
Hamburg
Szczecin
Bialystok
Belarus
Berlin
Poland
Poznan
Warsaw
Lodz
Wroclaw
Dresden
Germany
Kyiv

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

BY **BRAD PLUMER** November 6, 2012 at 3:26 pm

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?

That's the question raised by Thad Hall, a political scientist and author of *Electronic Elections*. In theory, he says, allowing Americans to vote online could have all sorts of benefits. We wouldn't

What makes Estonia's election system unique?

Security strengths / weaknesses?

How can new technology help?

Lessons for other countries about I-Voting?

Estonian approach

- An online voter can vote multiple times, and only the last vote will count
- The voter is authenticated by the Estonian Government-issued smart card containing multiple private keys for different purposes
  - As a new approach they also have ‘Mobile-ID’ which works with smart phones

VAATLEJATUNNISTUS

Kohaliku omavalitsuse volikogu valimised

JASON KITCAT

vaatleja ees- ja perekonnanimi

9.10.2013

väljaandmise kuupäev

LINNA VALIMISKOMISJON
NCMXCVIII
TALLINN

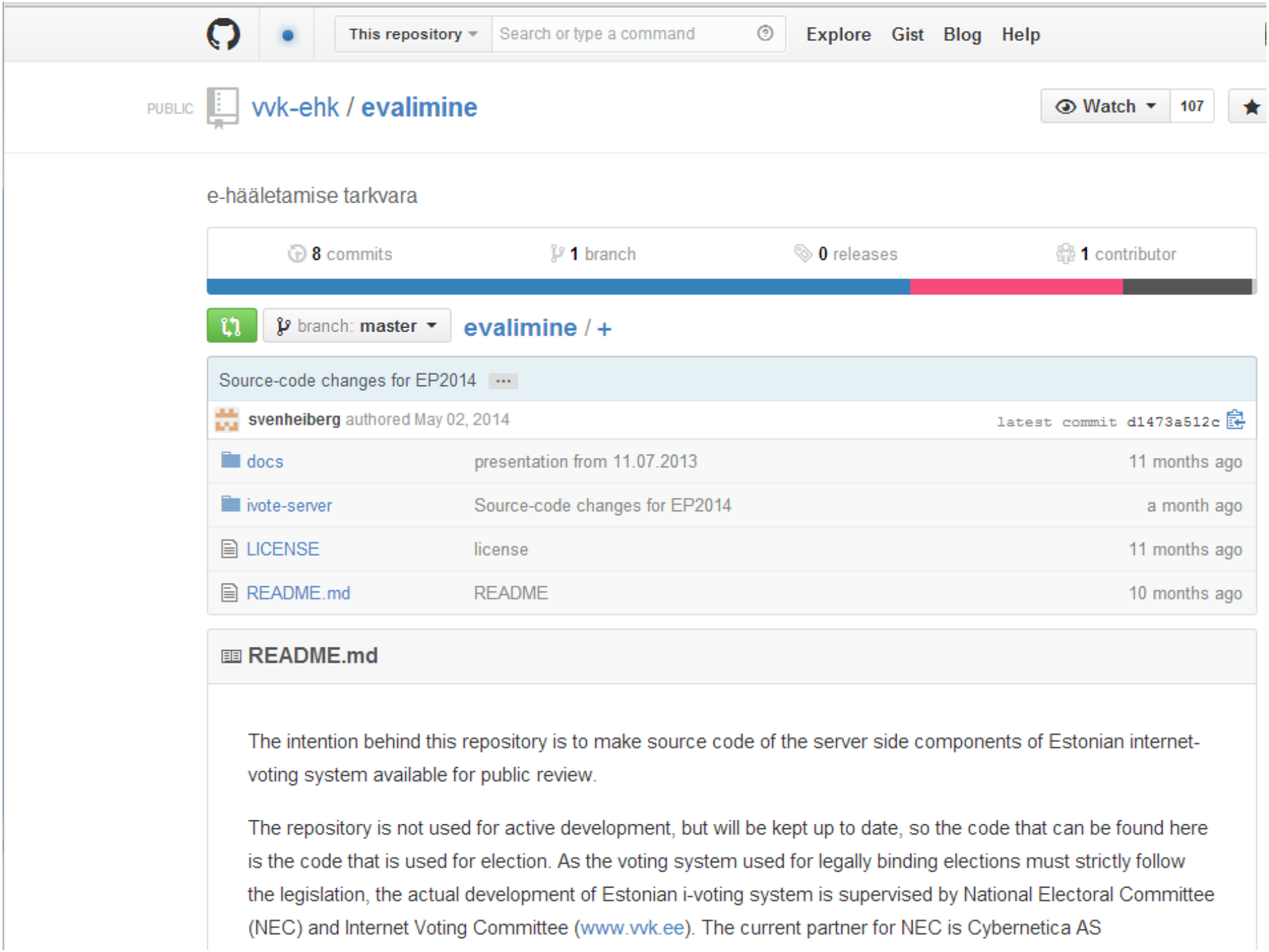

Riigi
Infosüsteemi
Amet

Open source?

- With a large announcement the “entire” system was published as Open Source in July 2013
  - Soon after the researchers realized that only partial source code was made available, mainly the server-side code
- The code release was mandated by the government, not the technologists responsible
- The backend calls other government systems

Client software

- Estonians said they will not to publish the client code because :
  - “Attackers would be able to learn the protocol”
  - It would make it too easy to make a fake client
- Binaries of the client were available
  - The executable was obfuscated using the UPX packing tool


This repository
Search or type a command
Explore
Gist
Blog
Help
PUBLIC
vvk-ehk / evalimine
Watch
107
e-hääletamise tarkvara
8 commits
1 branch
0 releases
1 contributor
branch: master
evalimine / +
Source-code changes for EP2014
svenheiberg authored May 02, 2014
latest commit d1473a512c
docs
presentation from 11.07.2013
11 months ago
ivote-server
Source-code changes for EP2014
a month ago
LICENSE
license
11 months ago
README.md
README
10 months 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

What does the source look like?

- Code base : about 17K lines
  - Python 61%
  - C++ 37%
  - Reminder shell scripts
- Nearly typical code drop: no docs, no harness, no tests, no protocol description
- Evidence of very poor software engineering practices (looks like a one man hack job)

Documentation?

- Documentation coverage is embarrassing
  - 2.3% coverage for Python code
  - 1.2% coverage for C++
- the majority of comments are in reused library code, not in Estonia's code (proper)

Documentation?

- A large amount of the included code is lifted from libraries and is used for handling server-side crypto (particularly cert management)
  - "borrowed" code has no attribution of source, authorship, or license
  - Includes undocumented code from GNU
- No non-source documentation (architecture, requirements, test plan, etc.)

TODO?

- file : ivote-server/hes/vote_analyzer.py as it was originally published :

```
def analyze(ik, vote, votebox):
    # TODO: implement security checks
    # such as verifying the correct size
    # of the encrypted vote
    return []
```

TODO handled!

- That was embarrassing! They cleaned it up, the newest version of the file of the same file :

```
def analyze(ik, vote, votebox):
    return []
```

- It says it all, too much documentation already

Overview

- Horrible engineering practices
  - not even an attempt at rigor or quality
  - vote auditing does not exist
  - vote validity is a stub and only logged
  - malformed votes will be logged and stored and detected during decryption

YouTube

Upload

Ehk Videod

Subscribe 6

Home | Videos | Playlists | Channels | Discussion | About

Uploads

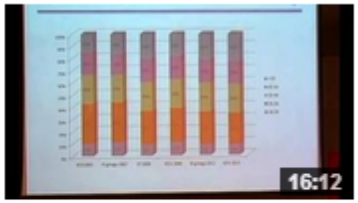
Date added (newest - oldest)

E-häälte hävitamine 1/2
118 views 4 months ago

E-häälte hävitamine 1/1
58 views 4 months ago

20.10.2013 seadmete kokkupanek
41 views 7 months ago

20.10.2013 e-häälte tühistamine ja lugemisek...
54 views 7 months ago



20.10.2013 häälte üleslaadimine infosüsteemi
29 views 7 months ago

20.10.2013 häälte kokkulugemine...
76 views 7 months ago

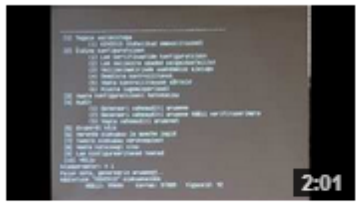
20.10.2013 ettevalmistus häälte lugemiseks
36 views 7 months ago

16 10 2013 e hääletamise lõpetamine 3/3
39 views 7 months ago

17.10.2013 E-hääletanute nimekirjade valmendus 4/4
54 views 7 months ago

17.10.2013 E-hääletanute nimekirjade valmendus 2/4
23 views 7 months ago

17.10.2013 E-hääletanute nimekirjade valmendus 1/4
26 views 7 months ago



17.10.2013 E-hääletanute nimekirjade valmendus 3/4
13 views 7 months ago

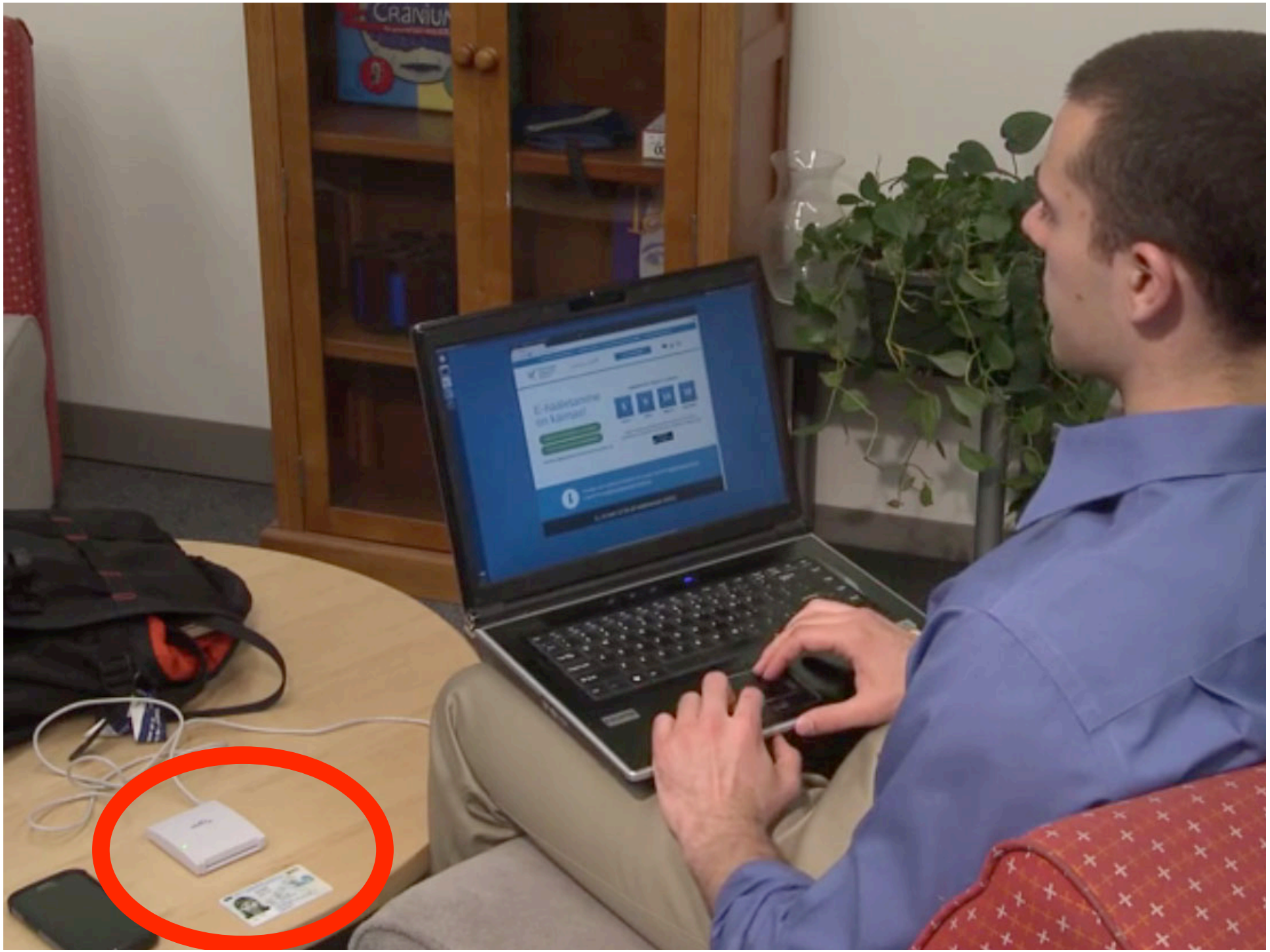
16.10.2013 e-hääletamise lõpetamine 2/3
45 views 7 months ago

16.10.2013 nimekirjade uuendamine
8 views 7 months ago

16.10.2013 e-hääletamise lõpetamine 1/3
19 views 7 months ago

Build your own system

- The research team was able reconstruct the whole e-voting server-side system and connect into that with client binaries
- Hundreds of hours of video published by the Estonian election officials that show them preparing and operating the system
- This allowed us to recreate the whole system as it was set up for the real election

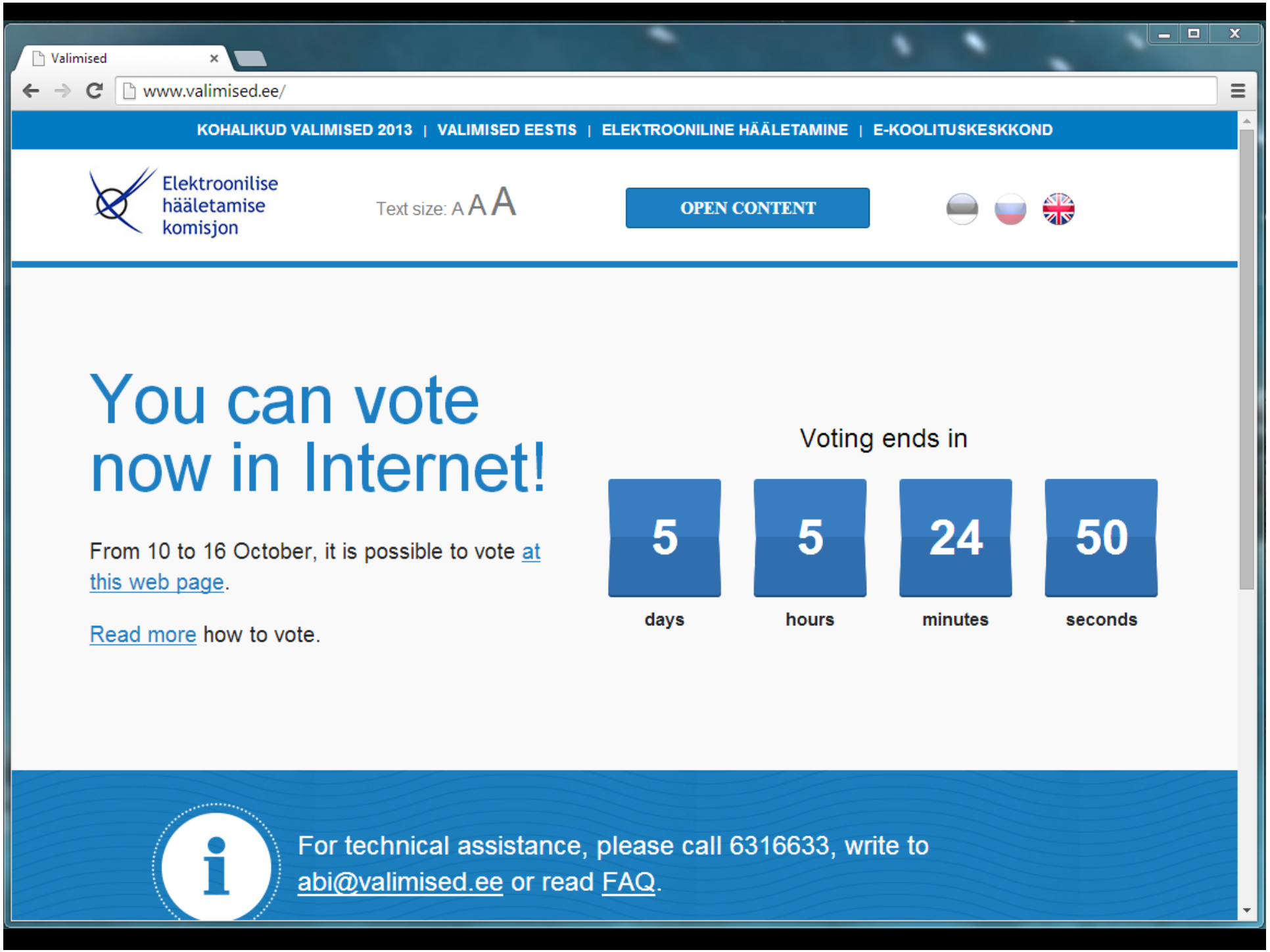



EESTI VABARIIK ISIKUTUNNISTUS
REPUBLIC OF ESTONIA IDENTITY CARD
PERSONNANIMI / SURNAME
MÄNNIK
EESNIMED / GIVEN NAMES
MARI-LIIS
SUGU / SEX
N/F
KODAKONDSUS / CITIZENSHIP
EST
SÜNNIAEG / DATE OF BIRTH
01.01.1971
ISIKUKOOD / PERSONAL CODE
47101010033
DOKUMENDI NUMBER / DOCUMENT NUMBER
AA1234567
KEHTIV KUNI / DATE OF EXPIRY
19.05.2015
KASUTAJA ALLKIRI / HOLDER'S SIGNATURE
SPECIMEN
AA1234567
EST
AA1234567


SÜNNIKOHT / PLACE OF BIRTH
EESTI / EST
VÄLJA ANTUD / DATE OF ISSUE
19.05.2010
47101010033
IDESTAA12345678<<<<<<<<<<<<<<<
7101010F1505199EST<<<<<<<<<<<0
MAENNIK<<MARI<LIIS<<<<<<<<<<<

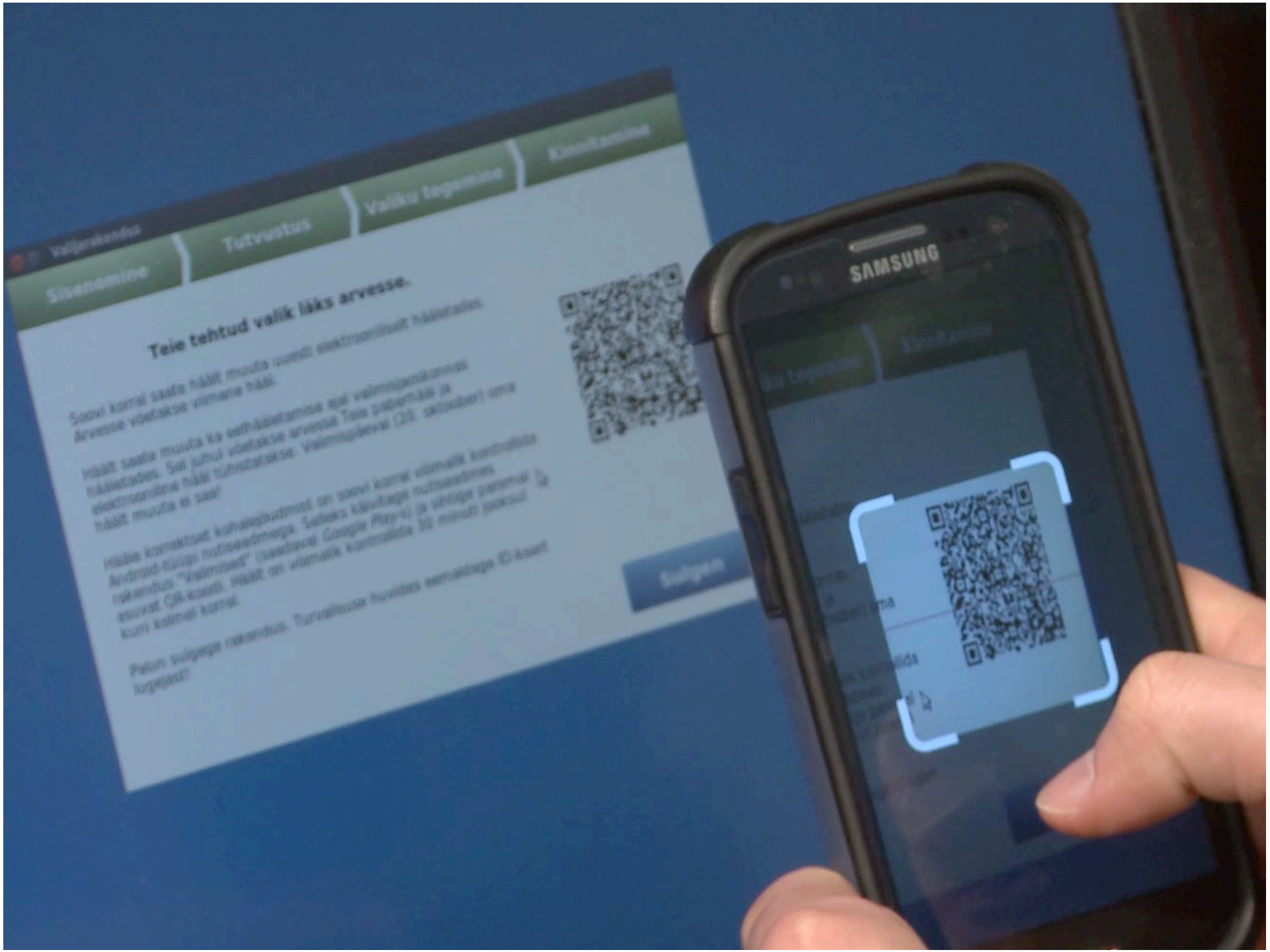
You can become Estonian too!

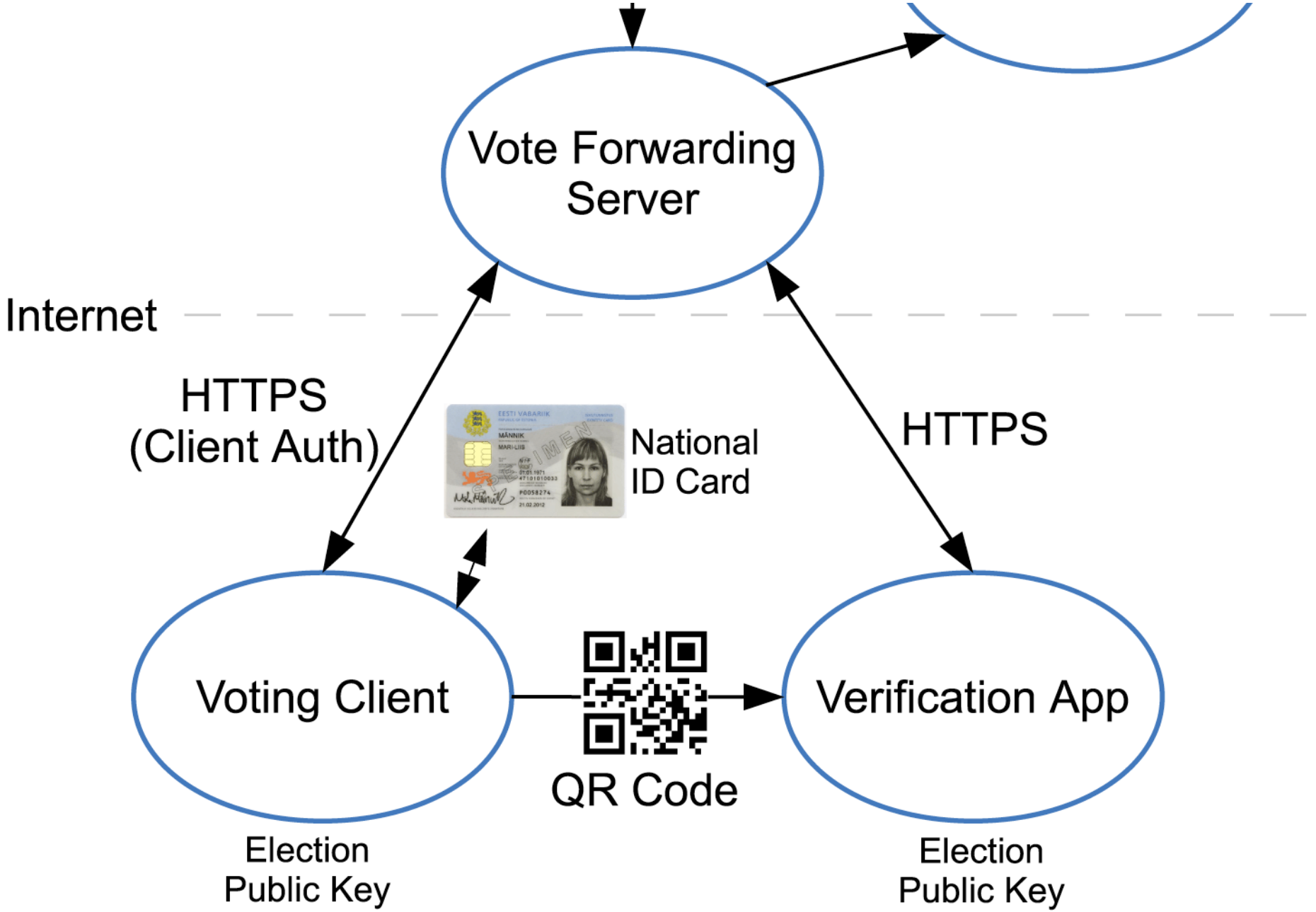
- They plan to let anyone become European – digitally
- http://e-estonia.com/e-residents/become-e-resident/
- Estonian E-residents will receive ID card allowing them to sign legally binding agreements digitally throughout the European Union


Valimised
www.valimised.ee/
KOHALIKUD VALIMISED 2013 | VALIMISED EESTIS | ELEKTROONILINE HÄÄLETAMINE | E-KOOLITUSKESKKOND
Elektroonilise hääletamise komisjon
Text size: A A A
OPEN CONTENT
You can vote now in Internet!
From 10 to 16 October, it is possible to vote at this web page.
Read more how to vote.
Voting ends in
5
days
5
hours
24
minutes
50
seconds
For technical assistance, please call 6316633, write to abi@valimised.ee or read FAQ.

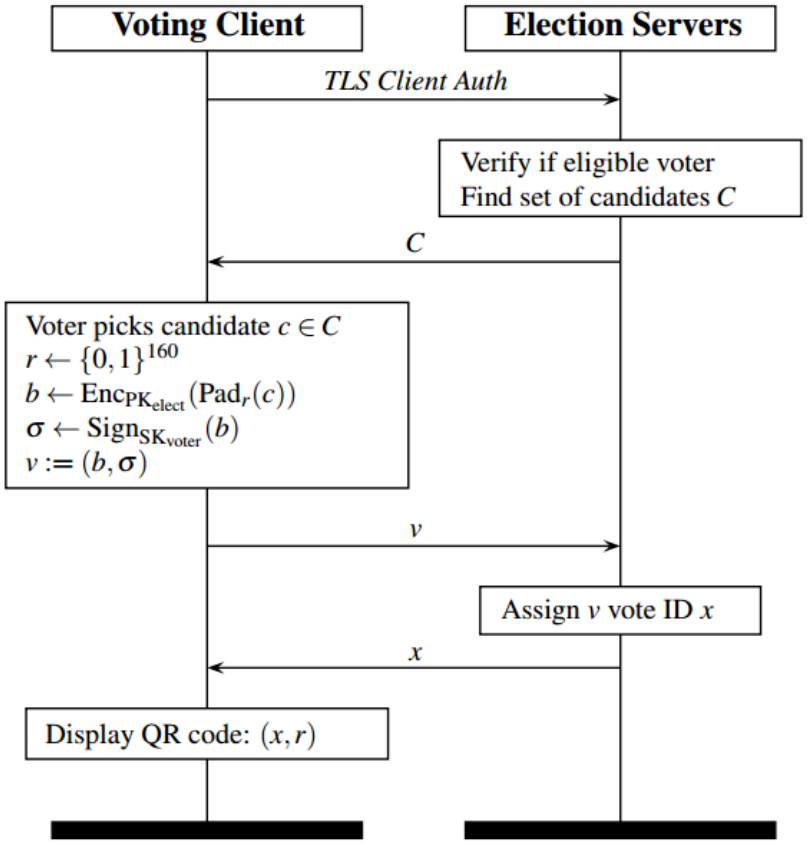

Valijarakendus
Sisenemine
Tutvustus
Valiku tegemine
Kinnitamine
Hääletamis
il-ID abil:
Sisesta PIN kood.
ALICE ANDERSON
Palun sisestage isikutuvastuseks PIN1
Katkestan
OK


Valijarakendus
Sisenemine
Tutvustus
Valiku tegemine
Kinnitamine
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
Katkestan
Valin

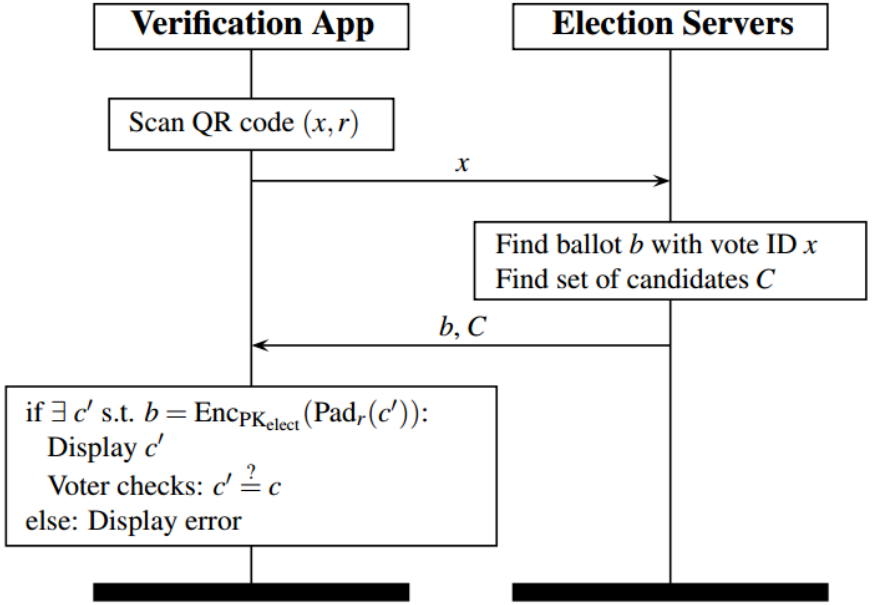

Valijarakendus
Sisenemine
Tutvustus
Valiku tegemine
Kinnitamine
Teie tehtud valik läks arvesse.
Soovi korral saate hääli muuta vastti elektroonilisel hääletades.
Arvesse võetakse viimane hääl.
Hääli saate muuta ka isehäälestamise või valimisjaoskonnas
hääletades. Sel juhul võetakse arvesse Teie paberhääl ja
elektrooniline hääl tühistatakse. Valimispäeval (20. oktoober) ema
hääli muuta ei saa!
Hääle korrektset kohaletoimetust on soovi korral võimalik kontrollida
Android-tüüpi nutiseadmega. Selleks käivitage nutiseadmes
rakendus "Valimised" (saadaval Google Playst) ja ühtige paremal
asuvat QR-koodi. Hääli on võimalik kontrollida 30 minuti jooksul
kuni kolmel korral.
Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart
lugejast!
Sulgeda
SAMSUNG

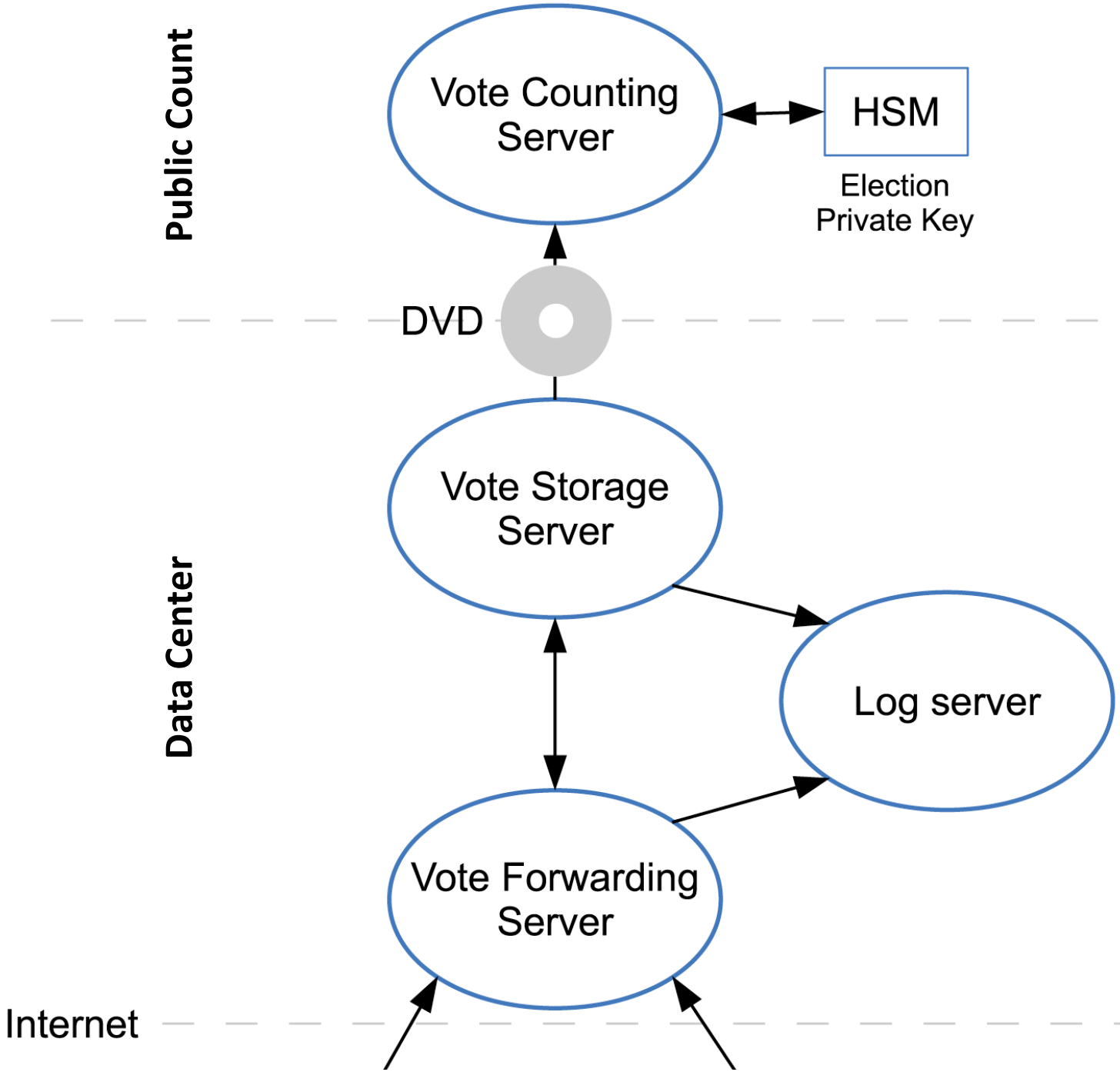

Vote Forwarding Server
Internet
HTTPS (Client Auth)
HTTPS
National ID Card
Voting Client
QR Code
Verification App
Election Public Key
Election Public Key

Voting Protocol



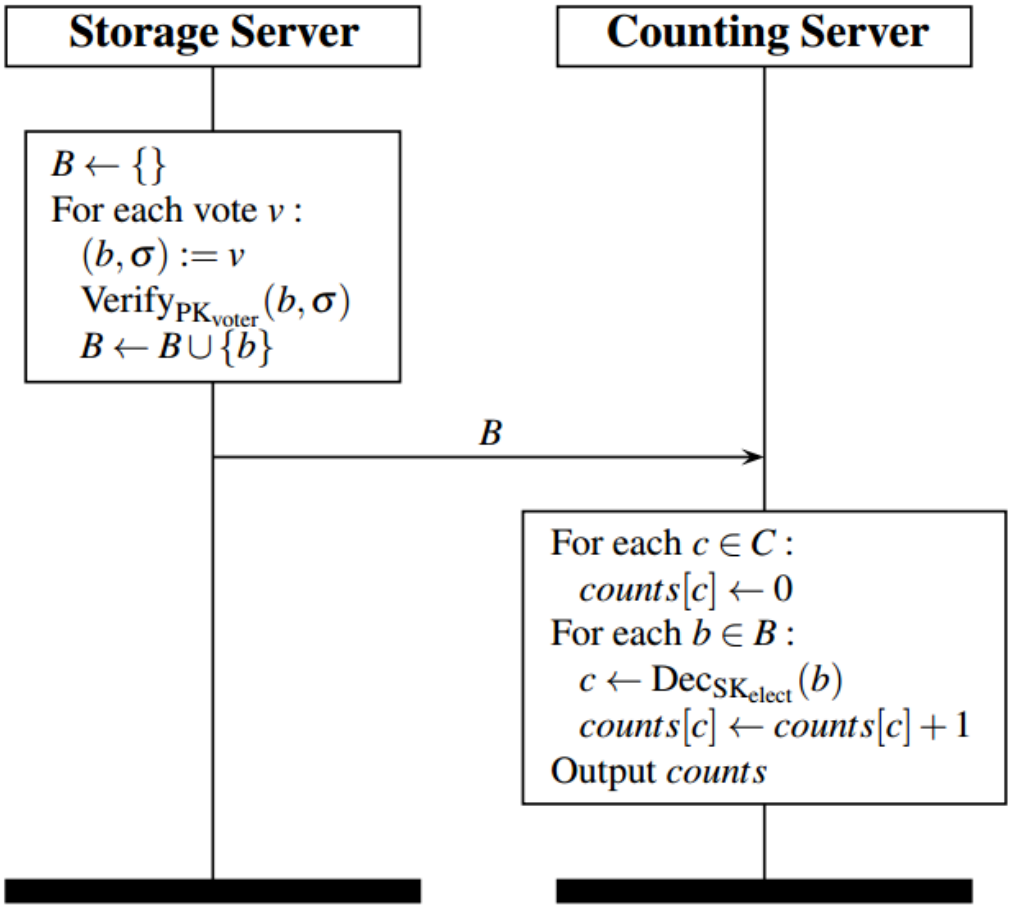
Verification Protocol



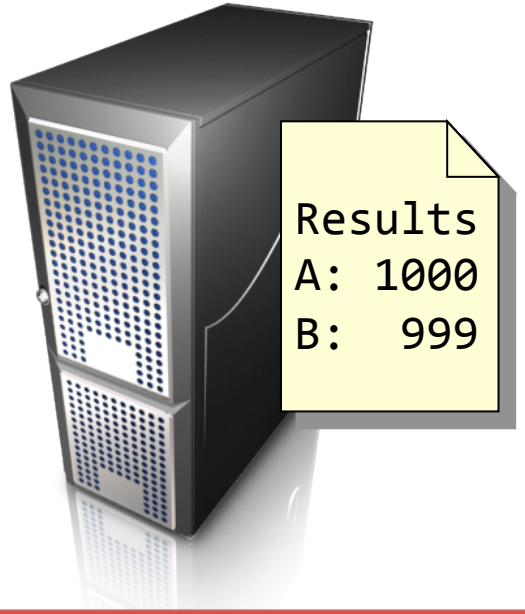

Public Count
Vote Counting Server
HSM
Election Private Key
DVD
Data Center
Vote Storage Server
Log server
Vote Forwarding Server
Internet

Counting Protocol

Cryptographic “double envelope”



Threats



- Coercion
- Credential Theft
- Imposter Sites
- Malware
- Botnets
- Denial of Service
- Remote Compromise
- Insider Attacks
- APTs
- Hardware-based Attacks

BBC NEWS

Watch One-Minute World News

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Programmes
Have Your Say

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Estonia says many state websites have been affected

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

"In the 21st century it's not just about tanks and artillery."

RT QUESTION MORE. LIVE

News | USA | Russian politics | Business | Op-Edge | In vision | In motion

UKRAINE TIMELINE

BREAKING NEWS OSCE CONFIRMS UKRAINE BOMBED LUGANSK ADMIN HQ FRO

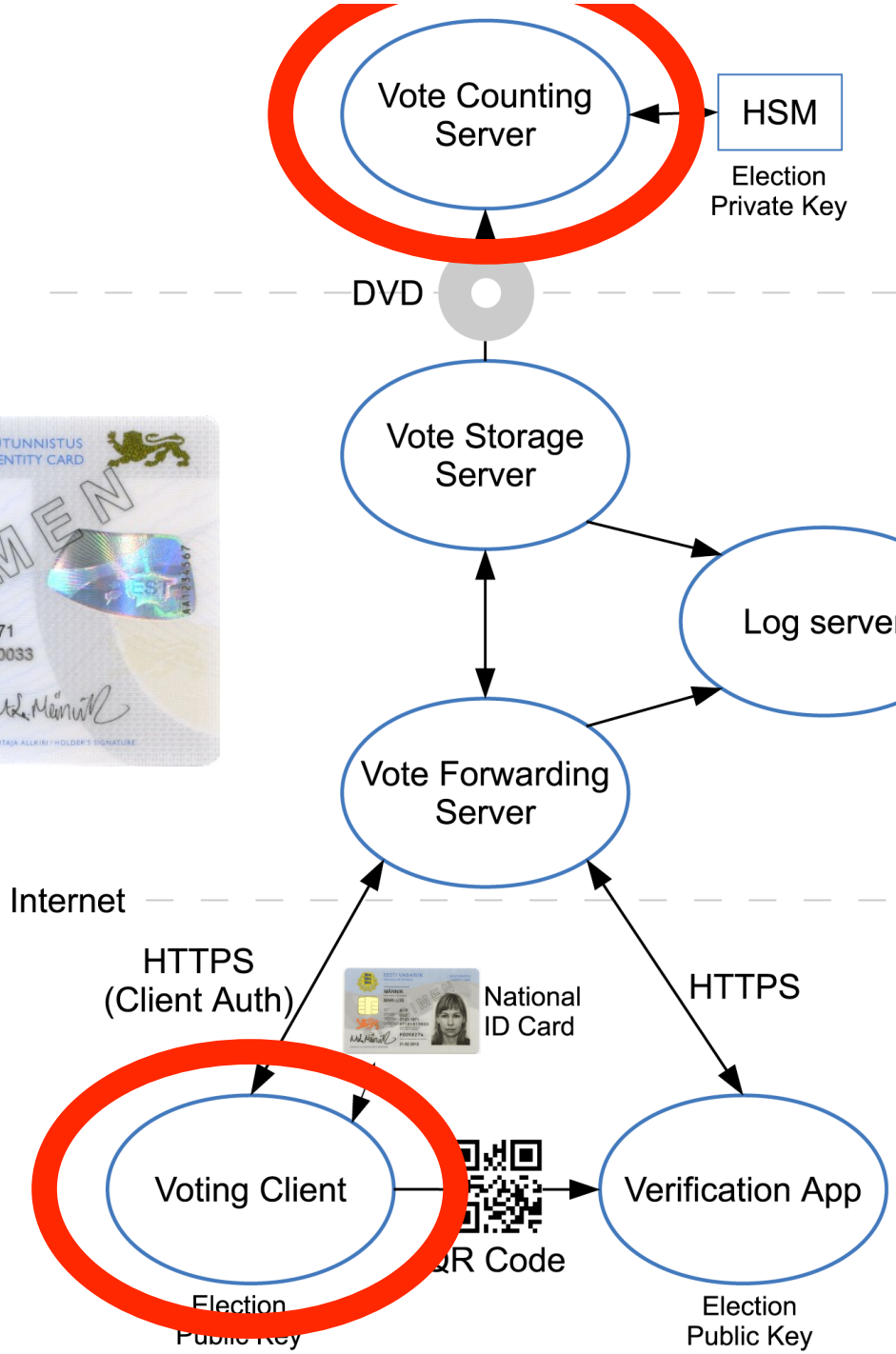
Home / News /

'Cyber-attack' cripples Ukraine's electronic election system ahead of presidential vote

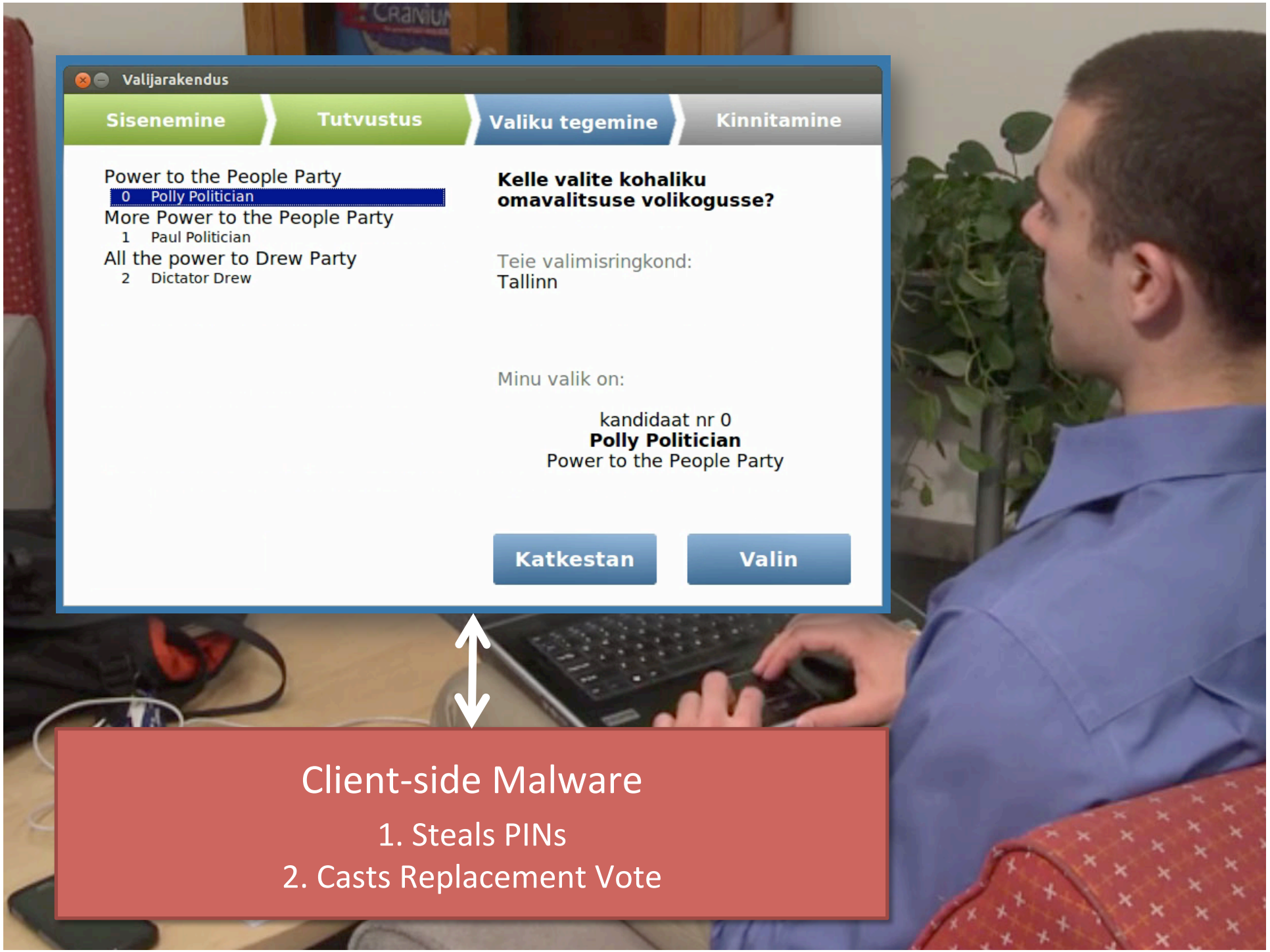
Published time: May 24, 2014 23:02
Edited time: May 26, 2014 01:16

Get short URL


EESTI VABARIIK ISIKUTUNNISTUS
REPUBLIC OF ESTONIA IDENTITY CARD
MÄNNIK
MARI-LIIS
N/F
EST
01.01.1971
47101010033
AA1234567
19.05.2015
SPECIMEN


Vote Counting Server
HSM
Election Private Key
DVD
Vote Storage Server
Log server
Vote Forwarding Server
Internet
HTTPS (Client Auth)
National ID Card
HTTPS
Voting Client
QR Code
Verification App
Election Public Key
Election Public Key

1. Client-side Attacks


Valijarakendus
Sisenemine
Tutvustus
Valiku tegemine
Kinnitamine
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
Katkestan
Valin
Client-side Malware
1. Steals PINs
2. Casts Replacement Vote

Two attacks

- Ghost Click
  - cast a delayed vote to replace the real vote
- Bad verify
  - Tandem PC and smartphone malware
  - Malware on the PC detects which candidate the voter selects and modifies the QR code encoding that into it
  - A malicious verification app displays whatever candidate is embedded in the QR code, rather than the candidate for whom the vote was actually cast
  - This allows the PC malware to arbitrarily change the submitted vote without being detected by verification or causing a suspicious number of replacement votes

Client side attacks

- Advanced version of malware could be used to harvest PIN codes and report in C&C present ID cards for malicious activities
  - Individual level targeted attacks with larger implications than Internet voting
  - The smart card infrastructure is used both private and public sector. For example all banks in Estonia use it to authenticate their clients
    - ID cards are used frequently in daily life

1. Client-side Attacks
2. Server-side Attacks

Our security is better than Google’s.

— Toomas Hendrik Ilves
President of Estonia

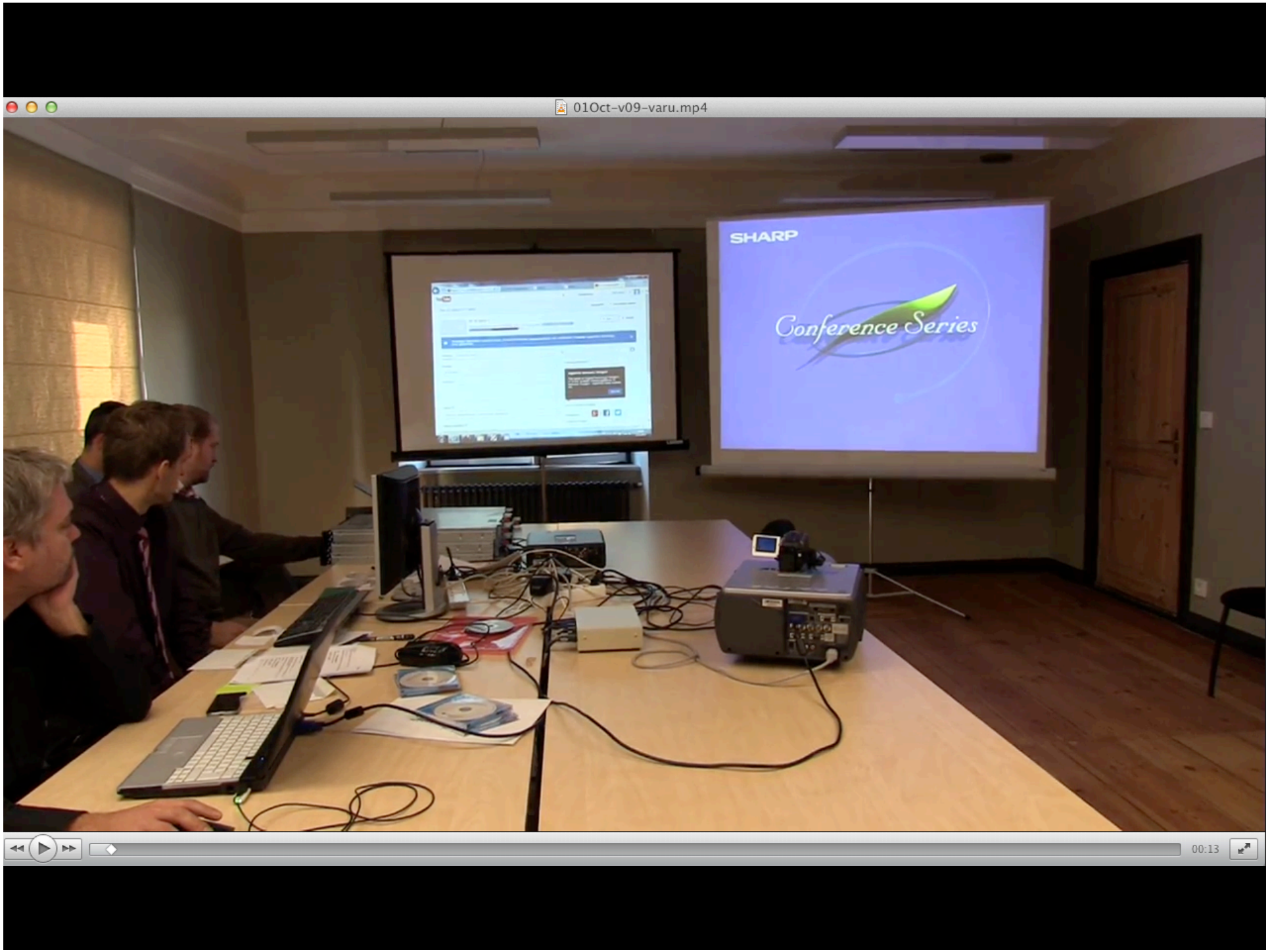
Server side attack

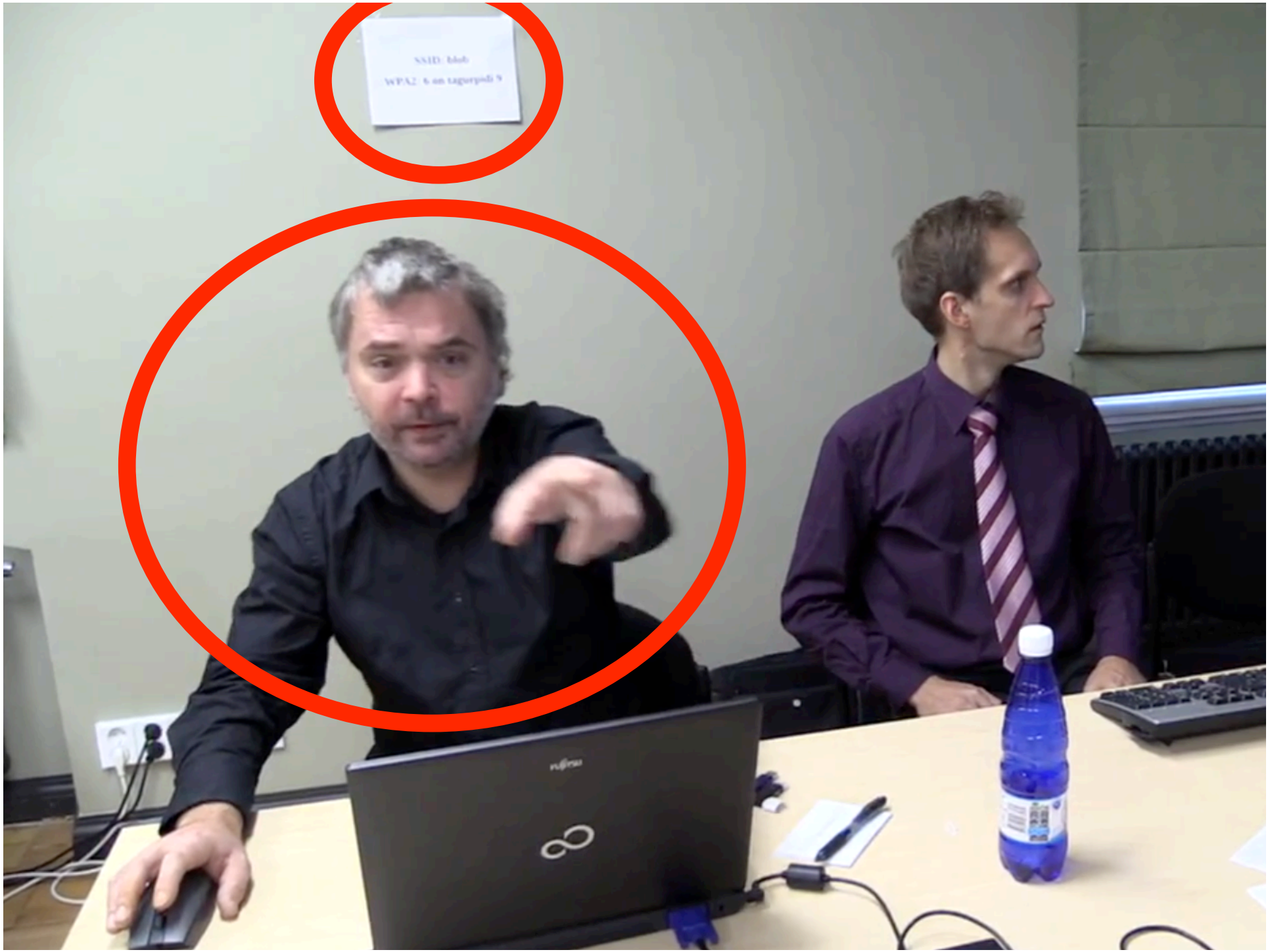
- The integrity of the count depends on the correct operation of the counting server and its HSM, which are the only components with the ability to decrypt vote
- Malware acts as a wrapper around the process responsible for using the HSM to decrypt votes
- Allows the malware to alter the decrypted votes prior to returning them to the counting application

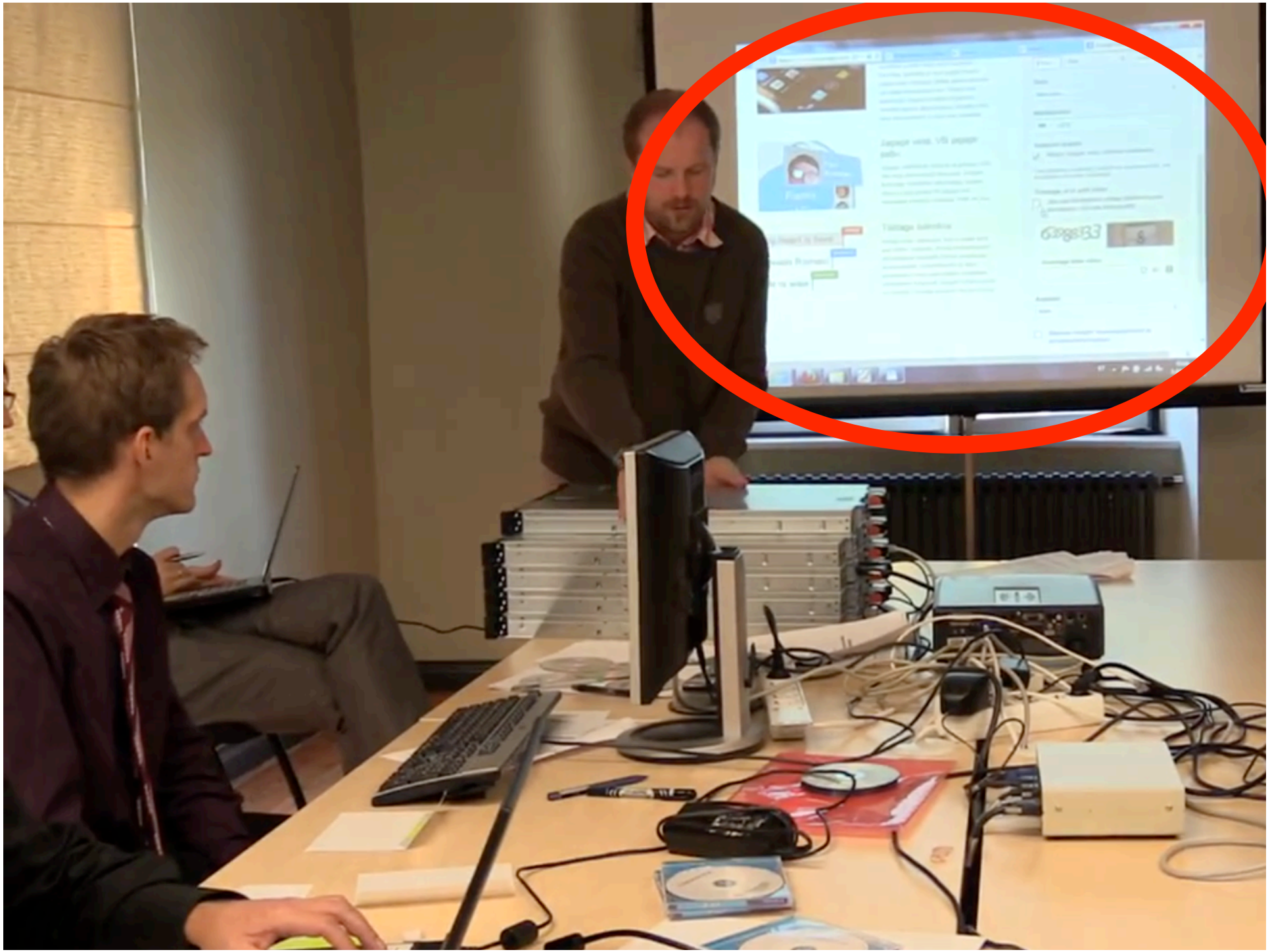
Server side attacks

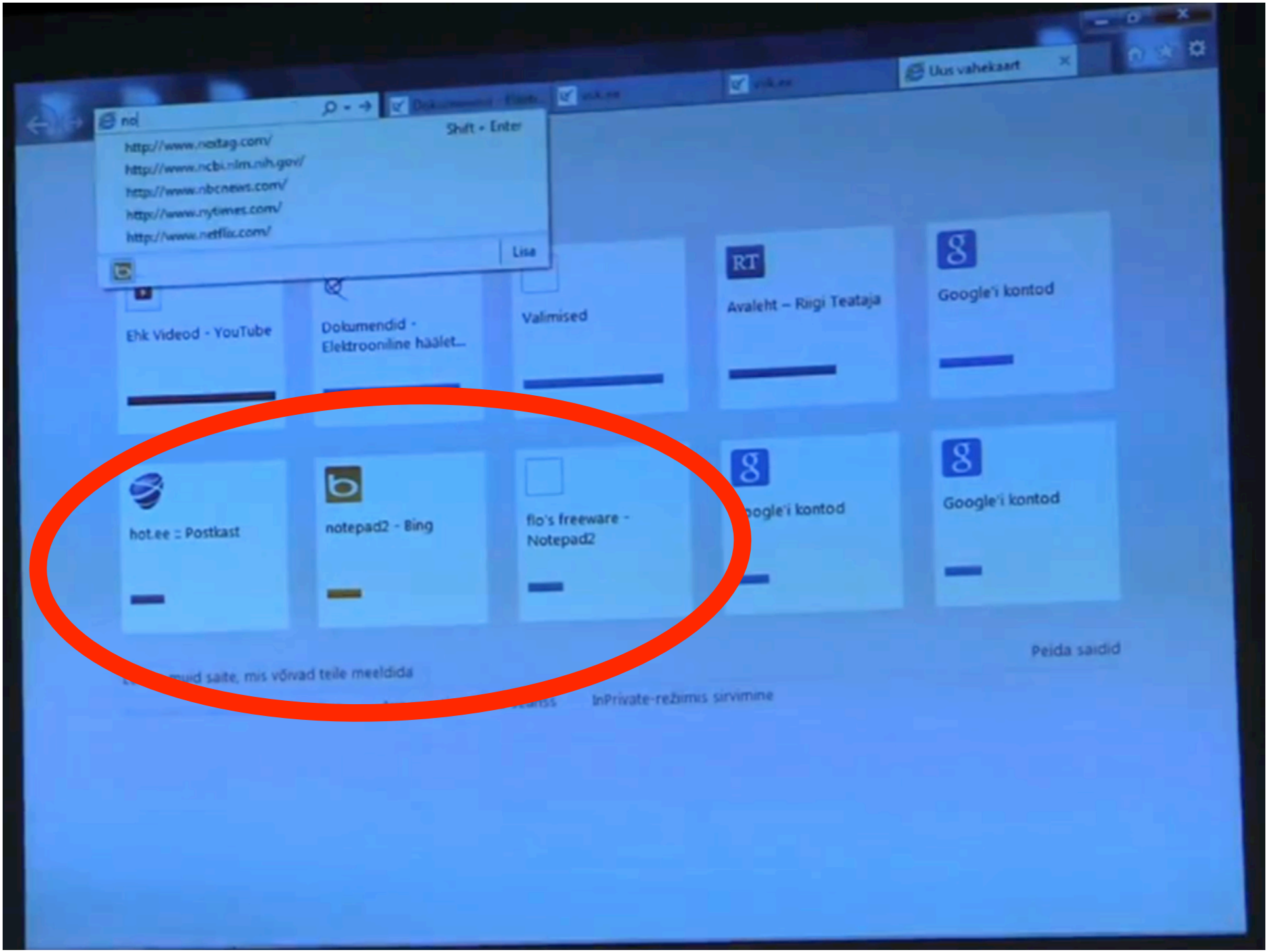
- The altered votes are then counted and released as the official results
- Such an attack would be unlikely to be detected, as there is no audit mechanism to check the accuracy of the decryption

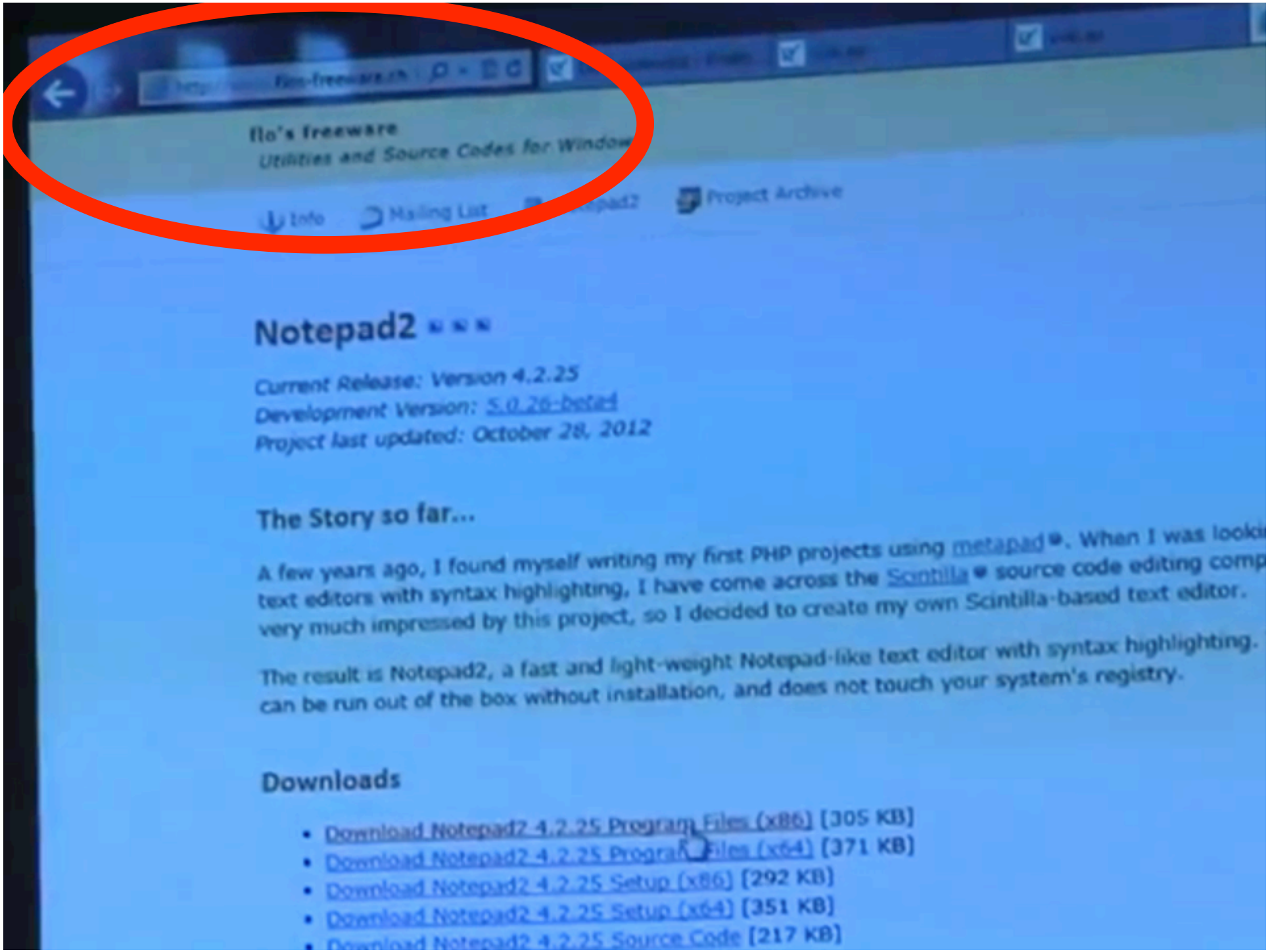
Operational Security?

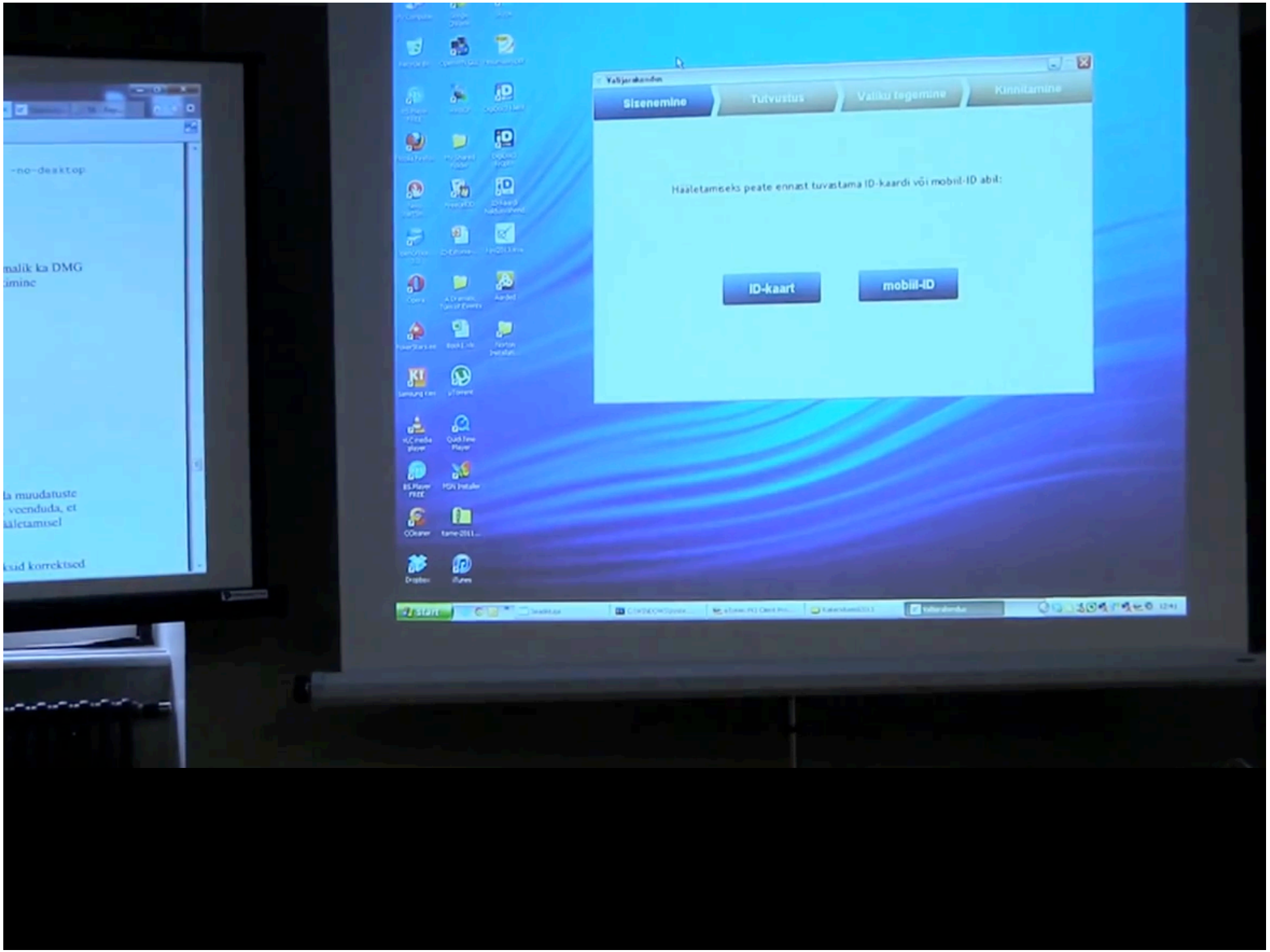

01Oct-v09-varu.mp4
SHARP
Conference Series
00:13

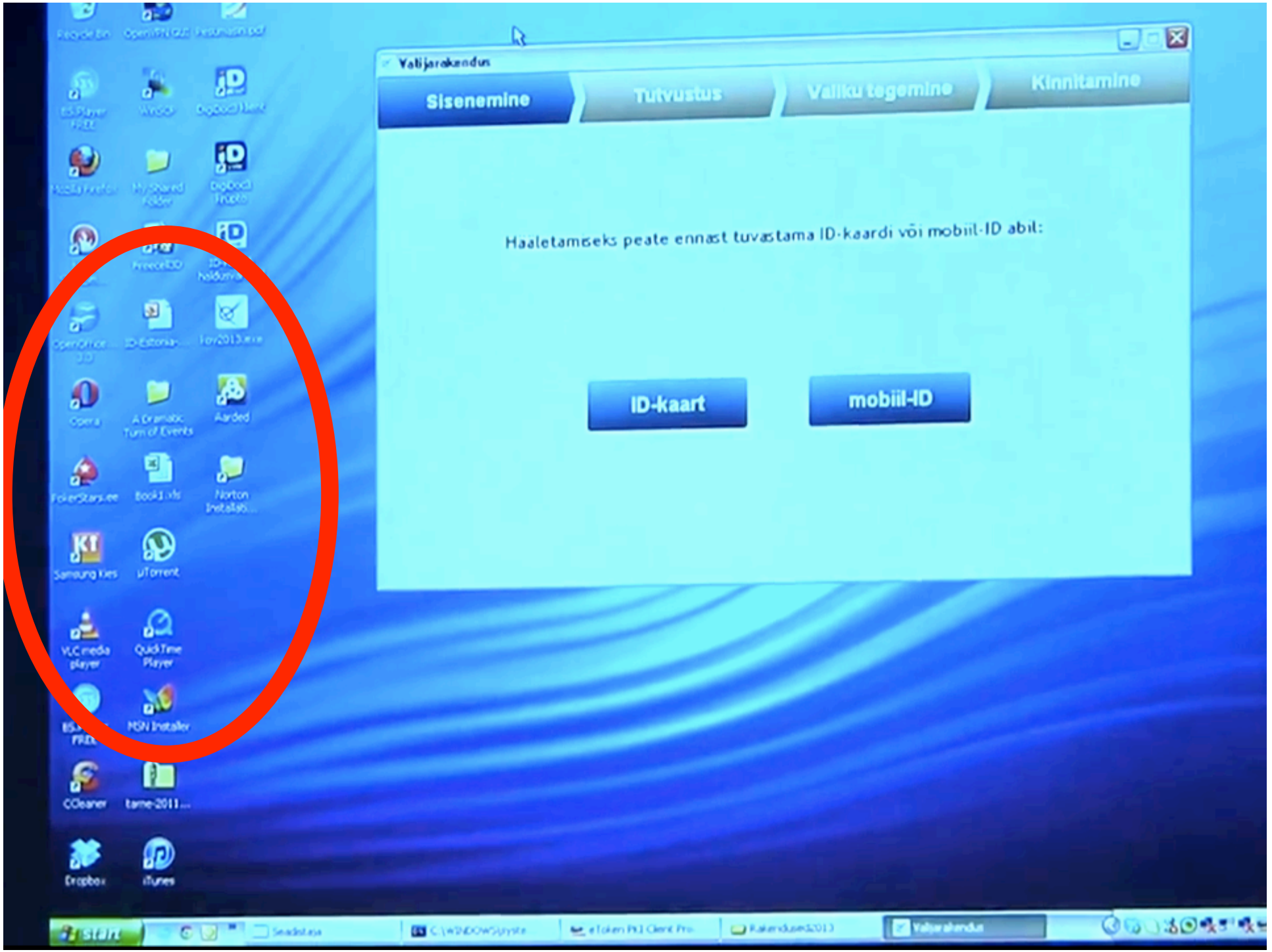

SSID: blob
WPA2: 6 on tagurpidi 9

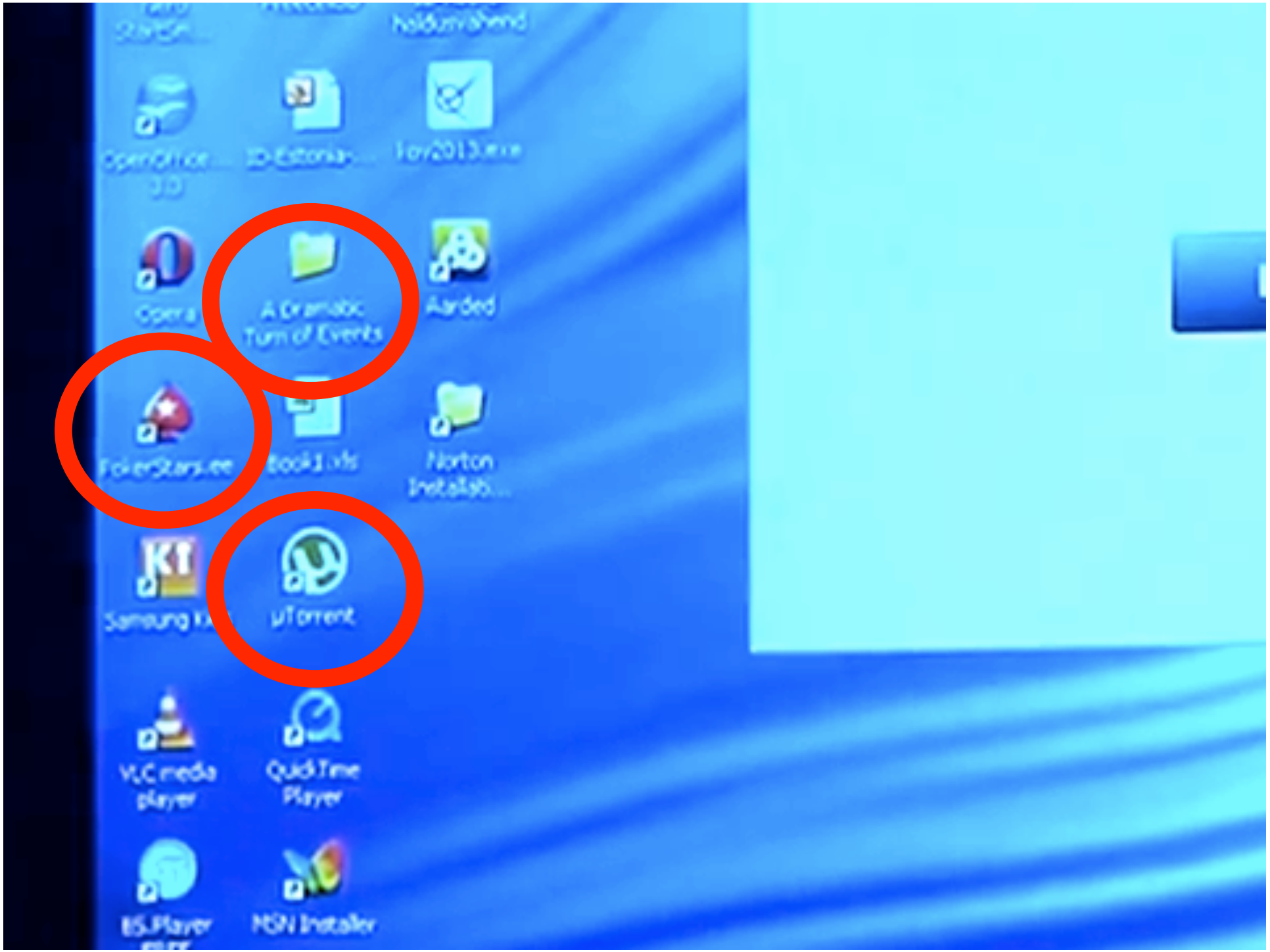


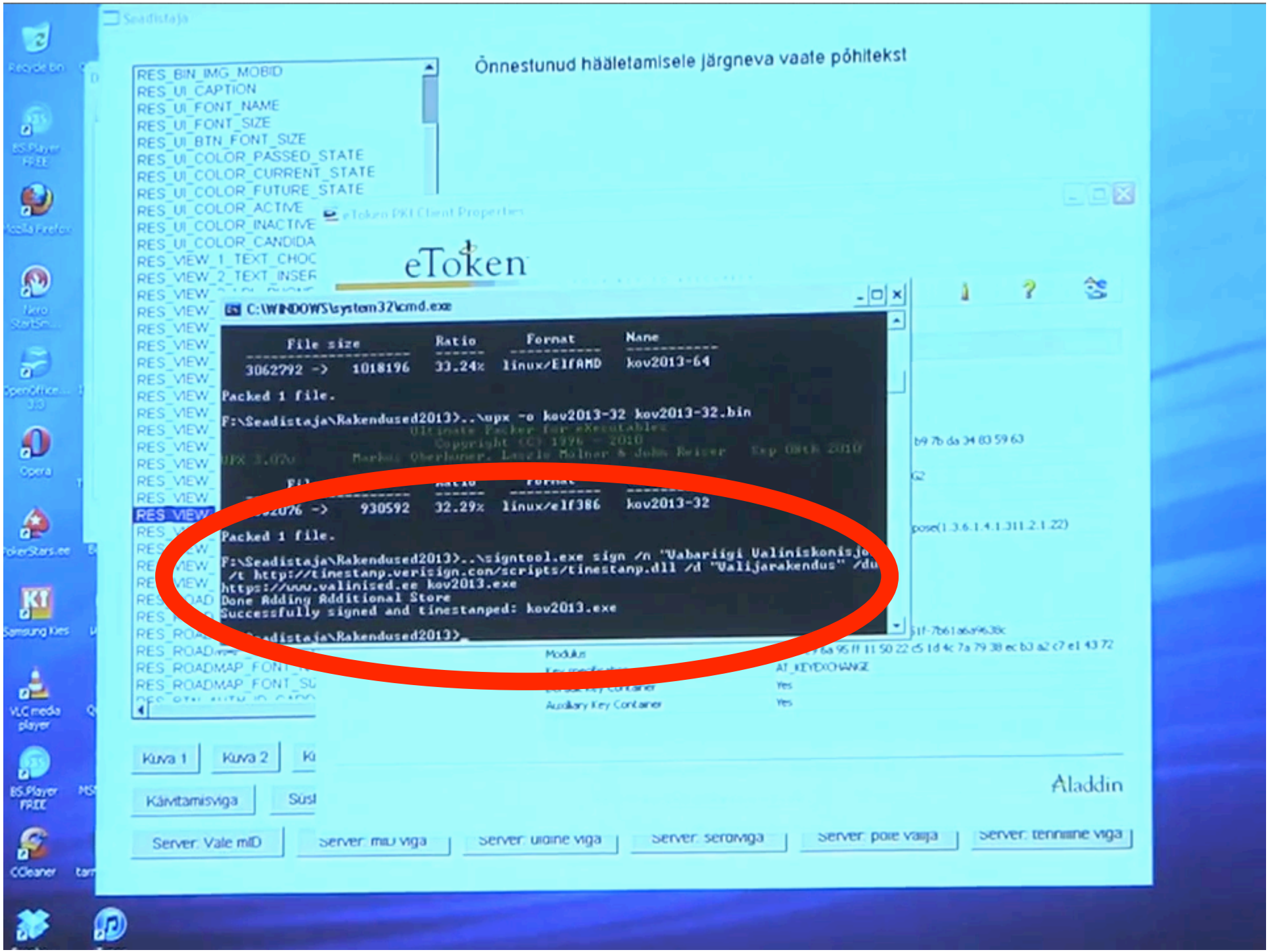

Uus vahekaart
nol
Shift + Enter
http://www.nextag.com/
http://www.ncbi.nlm.nih.gov/
http://www.nbcnews.com/
http://www.nytimes.com/
http://www.netflix.com/
Lisa
Ehk Videod - YouTube
Dokumendid - Elektrooniline häälet...
Valimised
Avaleht – Riigi Teataja
Google'i kontod
hot.ee :: Postkast
notepad2 - Bing
flo's freeware - Notepad2
Google'i kontod
Google'i kontod
Peida saidid
InPrivate-režiimis sirvimine

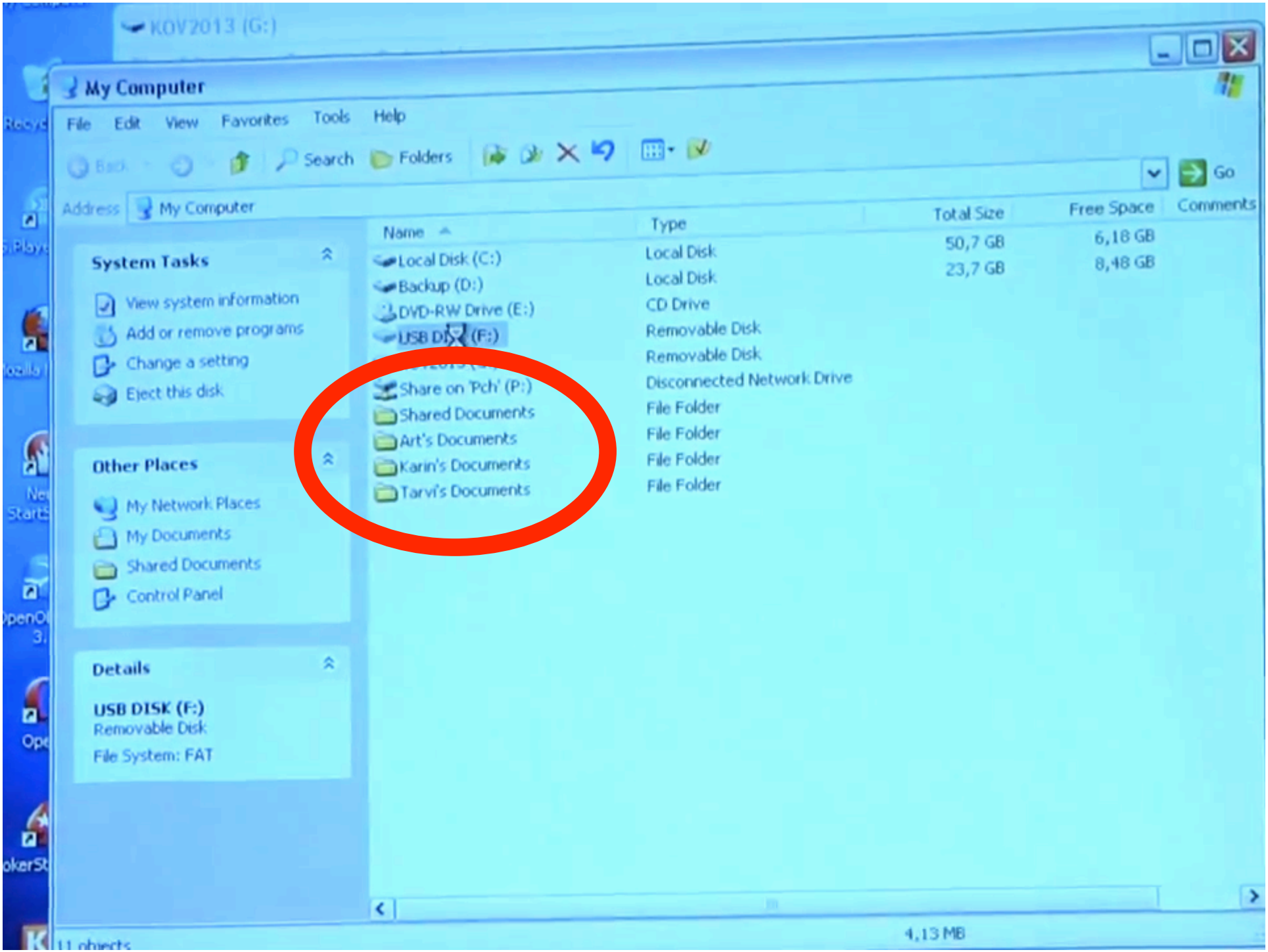

flo's freeware
Utilities and Source Codes for Windows
Info
Mailing List
Project Archive
Notepad2
Current Release: Version 4.2.25
Development Version: 5.0.26-beta4
Project last updated: October 28, 2012
The Story so far...
A few years ago, I found myself writing my first PHP projects using metapad. When I was looki
text editors with syntax highlighting, I have come across the Scintilla source code editing comp
very much impressed by this project, so I decided to create my own Scintilla-based text editor.
The result is Notepad2, a fast and light-weight Notepad-like text editor with syntax highlighting.
can be run out of the box without installation, and does not touch your system's registry.
Downloads
Download Notepad2 4.2.25 Program Files (x86) [305 KB]
Download Notepad2 4.2.25 Program Files (x64) [371 KB]
Download Notepad2 4.2.25 Setup (x86) [292 KB]
Download Notepad2 4.2.25 Setup (x64) [351 KB]
Download Notepad2 4.2.25 Source Code [217 KB]

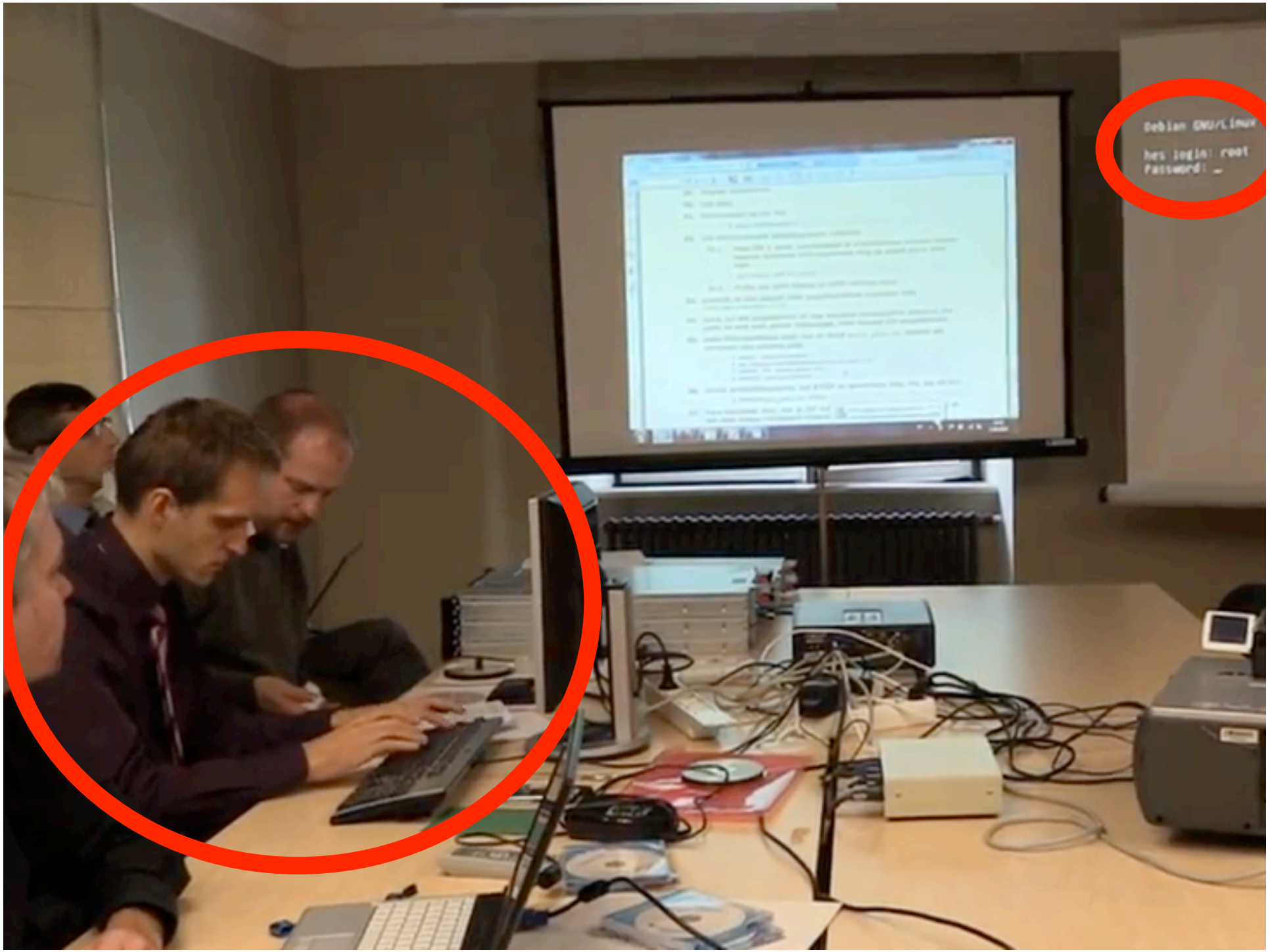

Sisenemine
Tuvastus
Valiku tegemine
Kinnitamine
Haaletamiseks peate ennast tuvastama ID-kaardi või mobiil-ID abil:
ID-kaart
mobiil-ID

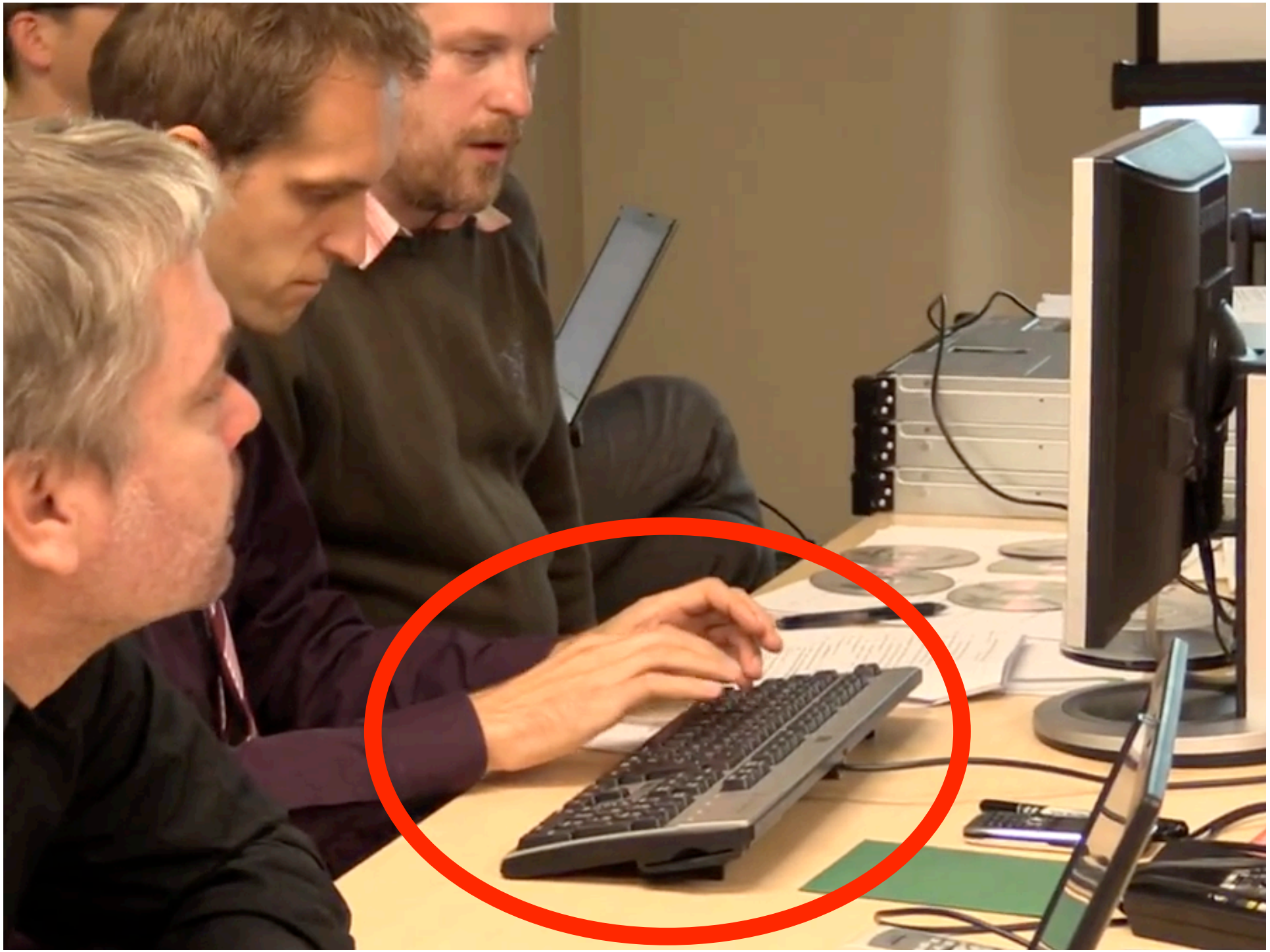

Valijarakendus
Sisenemine
Tutvustus
Valiku tegemine
Kinnitamine
Haaletamseks peate ennast tuvastama ID-kaardi või mobiil-ID abil:
ID-kaart
mobiil-ID

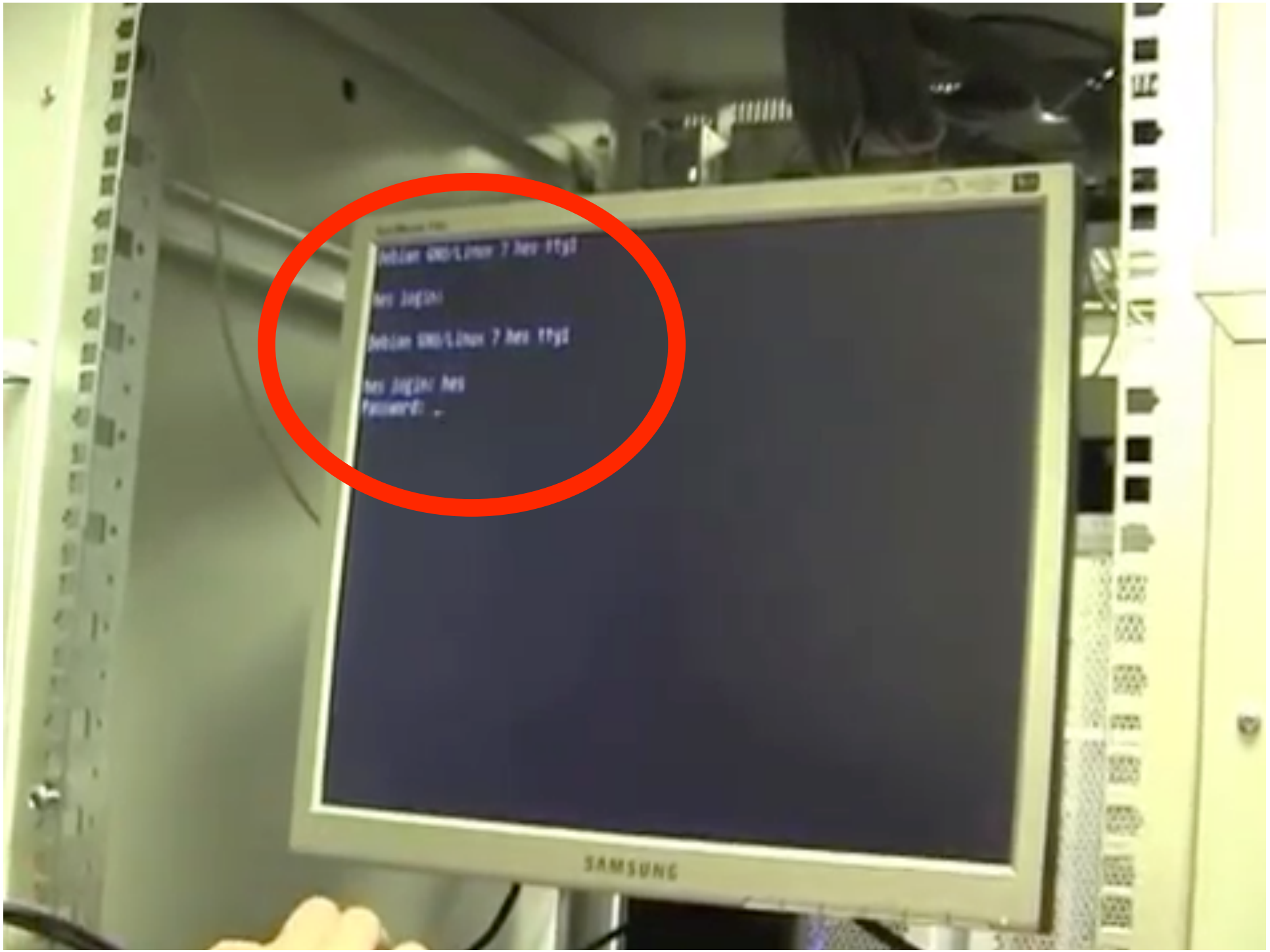

A Dramatic Turn of Events
Aarded
Opera
Norton
VLC media player
QuickTime Player
uTorrent
MSN Installer


Õnnestunud hääletamisele järgneva vaate põhitekst
RES_BIN_IMG_MOBID
RES_UI_CAPTION
RES_UI_FONT_NAME
RES_UI_FONT_SIZE
RES_UI_BTN_FONT_SIZE
RES_UI_COLOR_PASSED_STATE
RES_UI_COLOR_CURRENT_STATE
RES_UI_COLOR_FUTURE_STATE
RES_UI_COLOR_ACTIVE
RES_UI_COLOR_INACTIVE
RES_UI_COLOR_CANDIDA
RES_VIEW_1_TEXT_CHOC
RES_VIEW_2_TEXT_INSER
eToken
C:\WINDOWS\system32\cmd.exe
File size Ratio Format Name
3062292 -> 1018196 33.24% linux/ElfAMD kov2013-64
Packed 1 file.
F:\Seadistaja\Rakendused2013>..\upx -o kov2013-32 kov2013-32.bin
930592 32.29% linux/elf386 kov2013-32
Packed 1 file.
F:\Seadistaja\Rakendused2013>..\signtool.exe sign /n "Vabariigi Valimiskomisjo
/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
Seadistaja\Rakendused2013>
Kuva 1
Kuva 2
Kõvtamisviga
Server: Vale mID
Aladdin

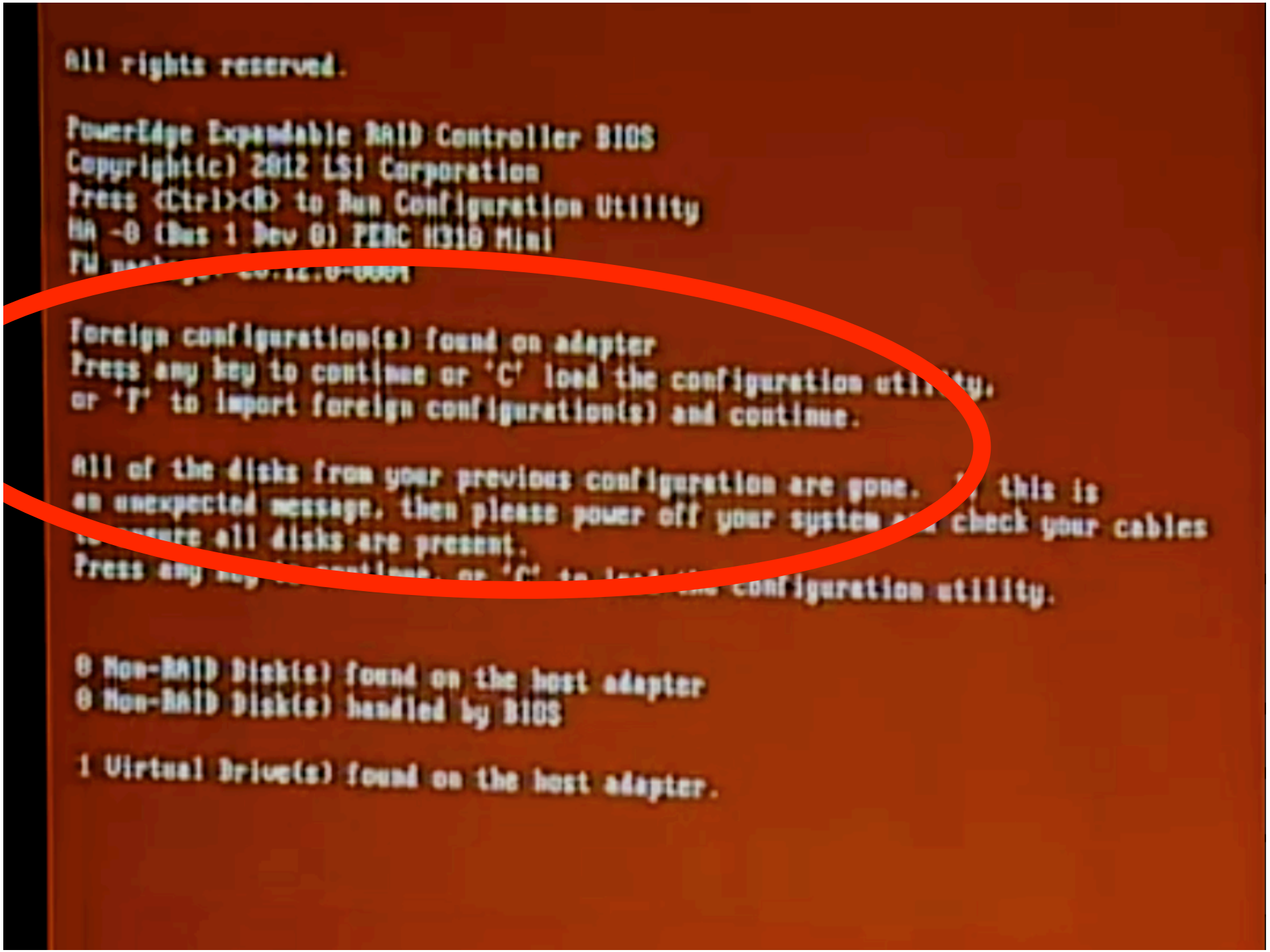

KOV2013 (G:)
My Computer
File Edit View Favorites Tools Help
Search Folders
Go
Address My Computer
System Tasks
View system information
Add or remove programs
Change a setting
Eject this disk
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
USB DISK (F:)
Removable Disk
File System: FAT
Name
Type
Total Size
Free Space
Comments
Local Disk (C:) Local Disk 50,7 GB 6,18 GB
Backup (D:) Local Disk 23,7 GB 8,48 GB
DVD-RW Drive (E:) CD Drive
USB DISK (F:) Removable Disk
Removable Disk
Share on 'Pch' (P:) Disconnected Network Drive
Shared Documents File Folder
Art's Documents File Folder
Karin's Documents File Folder
Tarvi's Documents File Folder
4,13 MB

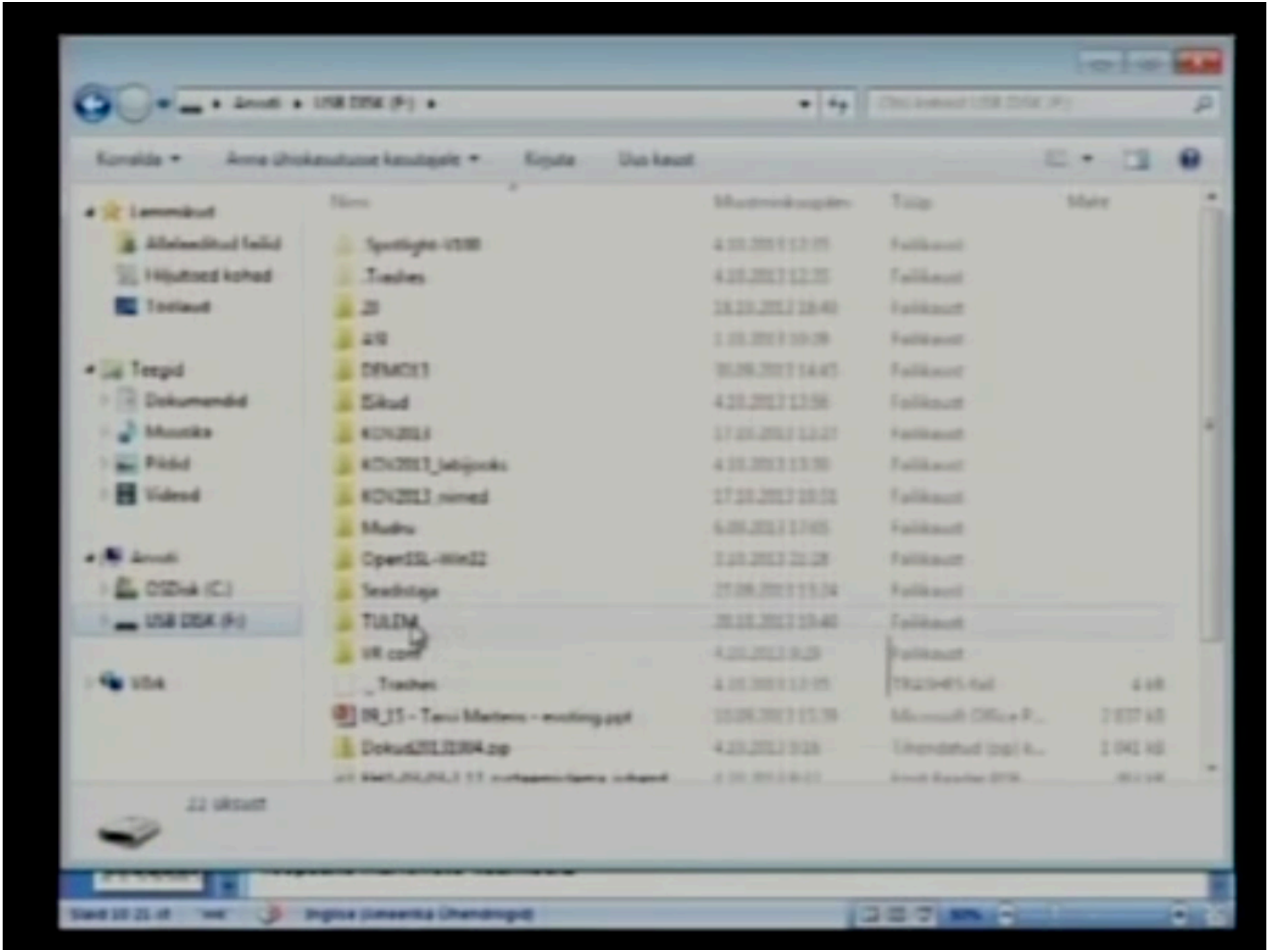

Debian GNU/Linux
hes login: root
Password:




SAMSUNG


A40005754
LABELLOCK
SEAL
SECUR


All rights reserved.
PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2012 LSI Corporation
Press <Ctrl><R> to Run Configuration Utility
HA -0 (Bus 1 Dev 0) PERC H310 Mini
Foreign configuration(s) found on adapter
Press any key to continue or 'C' load the configuration utility,
or 'F' to import foreign configuration(s) and continue.
All of the disks from your previous configuration are gone. If this is
an unexpected message, then please power off your system and check your cables
to ensure all disks are present.
0 Non-RAID Disk(s) found on the host adapter
0 Non-RAID Disk(s) handled by BIOS
1 Virtual Drive(s) found on the host adapter.



Fallout

- Arnis Cimdars, chairman of Latvia's Central Electoral Commission (CVK) claimed that electronic voting was not secure enough to allow it to be used in Latvian elections. “According to our experts, it is not possible for us with current technology. We have some mental reservations about this method of voting, too... at the moment it is not possible to ensure the anonymity and security of this method of voting, so I don't think it will happen very soon,” he added.

SECURITY ANALYSIS OF THE ESTONIAN INTERNET VOTING SYSTEM

https://EstoniaEVoting.org

Full research paper downloadable

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