
Should e-voting experience
of Estonia be copied?

E-voting at 2023 parliamentary elections

- Population 1.4 million
- Eligible to vote 966 129
- E-voting from 27.02 9:00 to 4.03 20:00
- Election day 5.03 (no e-voting)
- Votes cast 613 801
- Turnout 63.5%, rise 5.2%
- E-votes 312 181 => **51%**

Observing e-voting at 2023 elections

- Only one party sent their observer
- Outdated handbooks, docs & specs
- Deviations mended by *ad hoc* decisions
- Videos and terminal logs not provided
- Dismissed complaints, random explanations, legal recourse not possible up to Supreme Court and Prosecutor’s Office

An electronic vote / ballot


```
MIIDGjALBgkrBgEEAZdVAgEwggMJAoIBgQD+YZMTKXs+nR0emtxwE9rE0BoZNkx9aNhzNFJ
XEwJgTtvV74RvnfIDTyC+voSRknXkybE+kQbwa4cXwDebgW4AX/GtS6lrnI3qQPyv5K++S3
12D311Rj1j3jMwE1CzvcWXQ+fqFlJ7ydWCeyEFFHIhg6RgO4dgv3mwjaYlfD3u+UUmwJ58S
qtJxfouu4pFaRnFd/ioLycP7ssR1eeRcm/TwCxcqq5AG7v24qF41PkyowzOFPvda+gqduuQ
vXrTk6vW+/3iA0oAwVQt/C/jF1aPpZCcRDFyHwIl1PisdSh/daZQFR0ooYa4Tuqz3ZEw+zL
8gDmGoaESnUl9+o3DtfTOMK723tZet94rtQQqQR4r+/v669lCXPHH29MK9NQQMBB9gscGJS
UpOMhnYSU4TlbUmLSrpbEIFg6zFMZcD1YrAM1FYV7KO0rG/7+i6Q5yTj6tV9YztgkTXg/FZ
XqCj++rKnQ5t0nAGeqeSEUAHgbV8Orpmbl4cd9DdUYujajVEvECggGANKhbA0HRexiJXrA1
cOb9xdIZNIv/uYag9zI8+tfUOpBVKzXncqapVfrKLodHcnPlrOV++BMbQEtemF5Dy/hKdcc
Xu+IXF4gB6fod/C3+0Hd3PexnH2VimIIfASoOrfQDRP+ksMFHLWil2Gq/fuatHuieWAhiOs
/N/GYmAbukVJTiJe7VErgLqr6ItnNxfhGZdOQRa5yi+9scslgqUKGP/8aYxbTArWSB3luPo
JFTdEzuxCiPvL3t54j0EenZf1I9DLMwjugSx46pFP+zHW4DTpnH7Z/QM2yCpD15JHUIbTJw
ujvu5O+El3rIsaKZ1cQy2kGRY/vkVXyRw/VgQIRLj/B6mIARZ4/Tb7wHiSJriNSdFicfuqF
G+L40t2mVzrfKtoiOWVS9bm666R1BJ/ueiAxRIAtV30ga4zeYTwi+TYia1VYYSKHTHrcqZy
hQMVdxjDlUzg9G8+yPkpiSWqU643ODgwdAfK4ibaWj6mQIGJmDXeo99lf1AXMPhmwlQm/0
```

A decrypted electronic vote

```
0  0  0  0  .  6  5  9
30 30 30 30 2E 36 35 39 1F

E  r  a  k  o  n  d     E  e  s  t  i     2  0  0
45 72 61 6B 6F 6E 64 20 45 65 73 74 69 20 32 30 30 1F

J  O  H  A  N  N  A  -  M  A  R  I  A     L  E  H  T  M  E
4A 4F 48 41 4E 4E 41 2D 4D 41 52 49 41 20 4C 45 48 54 4D 45
```

The format of decrypted vote

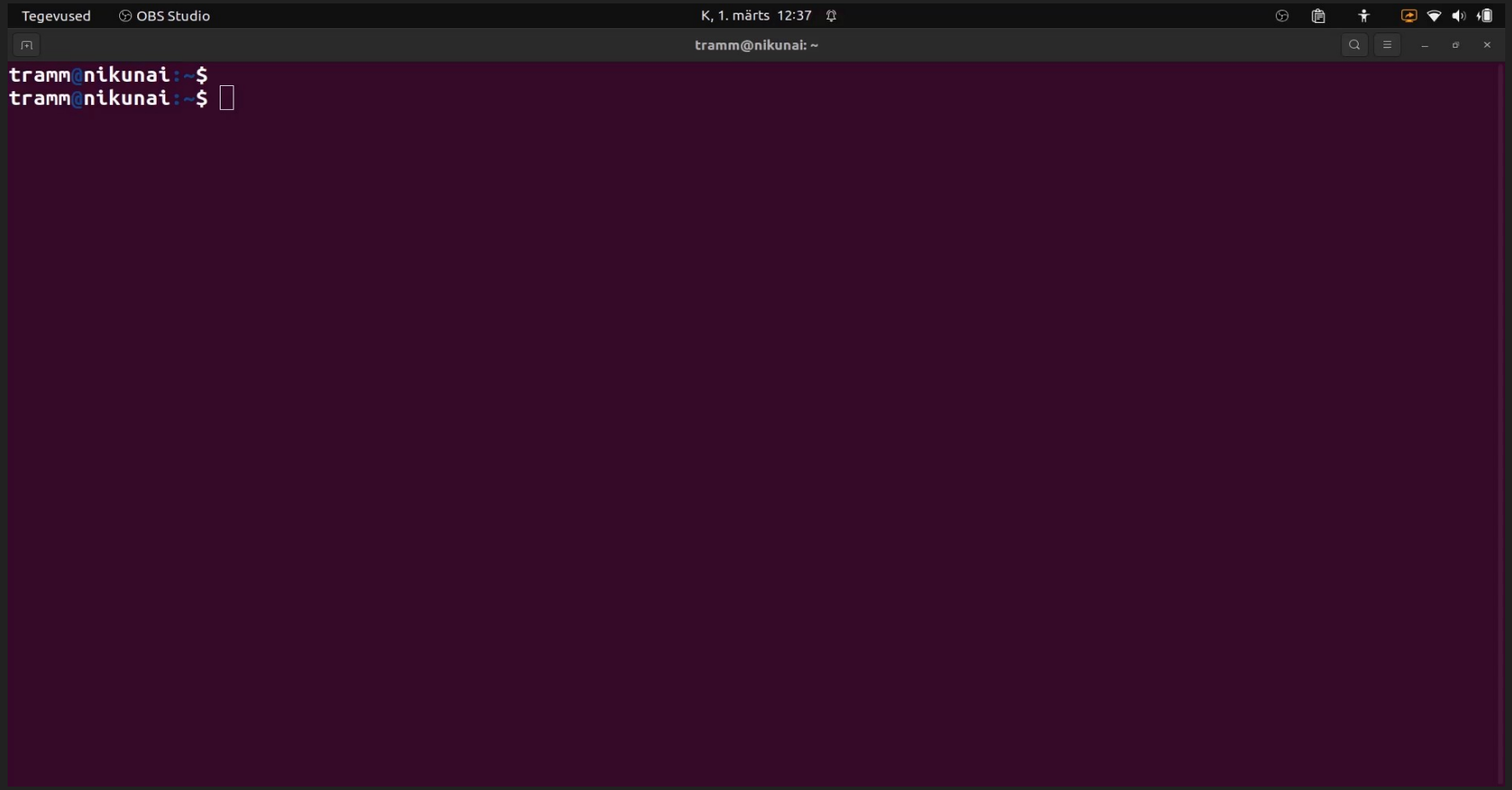
```
0  0  0  0  .  6  5  9
30 30 30 30 2E 36 35 39 1F
Adm. unit      Cand. no

E  r  a  k  o  n  d     E  e  s  t  i     2  0  0
45 72 61 6B 6F 6E 64 20 45 65 73 74 69 20 32 30 30 1F
Name of political party / “independent candidates”

J  O  H  A  N  N  A  -  M  A  R  I  A     L  E  H  T  M  E
4A 4F 48 41 4E 4E 41 2D 4D 41 52 49 41 20 4C 45 48 54 4D 45
Name of the selected candidate
```

Inside a digitally signed ZIP container

```
Archive:  FZCGDnrf3T6z61ya1WBqOg==.bdoc
  Length      Date    Time    Name
---------  ---------- -----   ----
       31  1980-00-00 00:00   mimetype
        0  1980-00-00 00:00   META-INF/
      381  1980-00-00 00:00   META-INF/manifest.xml
      798  1980-00-00 00:00   RK_2023.question-1.ballot
     4973  1980-00-00 00:00   META-INF/signatures0.xml
---------                     -------
     6183                     5 files
```


Tegevused
OBS Studio
K, 1. märts 12:37
tramm@nikunai: ~
tramm@nikunai:~$
tramm@nikunai:~$

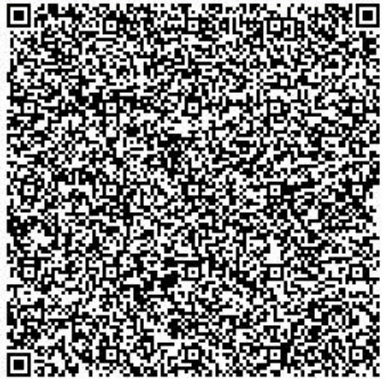
Valijarakendus (RK_2023)

Sisenemine — Tutvustus — Valiku tegemine — E-hääletamine

Teie tehtud valik läks arvesse

Soovi korral saate e-häält muuta uuesti elektrooniliselt hääletades (kuni 4. märts kella 20:00ni).

Kui olete hääletanud mitu korda elektrooniliselt, võetakse arvesse viimane hääl.
Kui soovite kontrollida, kas Teie e-hääl jõudis muutmata kujul valimiste serverisse, kasutage Android või iPhone nutitelefoniga mobiilirakendust "EH kontrollrakendus", et skaneerida ekraanil asuvat QR-koodi. Saate seda teha 30 minuti jooksul kuni kolm korda.
Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart lugejast!



Sulgen

Vote verification mechanism

- QR code contains 1) session identificator, 2) ElGamal ephemeral key and 3) vote identificator.
- Using vote identificator voter can download the vote container up to three times in 30 minutes.
- Usually done by iPhone/Android application, which decrypts the ballot and shows voter choice on screen.
- DIY version: https://github.com/infoaed/kryptogramm

Communicating with the election servers

```
{"id": 0.0, "method": "RPC.VoterChoices",
"params": [{"OS": "Ubuntu 22.04.2 LTS",
"AuthMethod": "tls"}]}

{"id": 0.0, "method": "RPC.Vote", "params":
[{"OS": "Ubuntu 22.04.2 LTS", "AuthMethod":
"tls", "Choices": "0000.10", "Type": "bdoc",
"SessionID": "...", "Vote": "..."}]}
```

Submitting electronic votes with openssl

```
tramm@ludus:~$ cat template.txt | openssl
s_client -tls1_2 -ign_eof -connect
koguja1.valimised.ee:443 -servername
choices.ivxv.valimised.ee --engine pkcs11 --
keyform eng --key "pkcs11:type=private;token=P
%C3%95DER%2CM%C3%84RT
%2C37909110298%20%28PIN1%29;pin-value=9999" --
cert filename.pem
```

Responses from voting server

```
tramm@ludus:~$ cat vote.txt | openssl s_client
CONNECTED(00000008)
{"id":0.0,"result":
{"SessionID":"...","VoteID":"8qvmACRcJuLm3ztLsSo1
jw==","Qualification":
{"ocsp":"MIIFAoB..." ,"tspreg":"MIIJ2g..."}},
"error":null}
closed
tramm@ludus:~$
```

Submitting after end of voting period

```
tramm@ludus:~$ cat auth.txt | openssl s_client
Engine "pkcs11" set.
CONNECTED(00000008)
---
{"id":0.0,"result":null,"error":"VOTING_END"}
closed
tramm@ludus:~$
```

Contents of the 20:13 container

```
Archive:  8qvmACRcJuLm3ztLsSo1jw==.bdoc
  Length      Date    Time    Name
---------  ---------- -----   ----
       31  2023-03-04 19:56   mimetype
      386  2023-03-04 19:56   META-INF/manifest.xml
      384  2023-03-04 19:54   RK_2023.question-1.ballot
    11962  2023-03-04 19:56   META-INF/signatures0.xml
---------                     -------
    12763                     4 files
```

Finding out which container was counted

- Submitted altogether 26 different vote containers
- Counting legally had to start March 5th 20:00
- Invalid vote reportedly removed in preprocessing
- Procedures not repeated during “second counting”
- Electoral Office suggested personal data request
- Socially engineered into meeting with SEO
- Private session to inspect submitted containers

VOTING_END container to be removed

“We were dealing with a voter who sent his vote to the e-ballot box not with an official, but with a self-made voter application. 20:13 is the moment his vote reached the e-ballot box. No personal identification took place and it *would be correct to display a dash in that place in the log*.”

-- Electoral Office Head Arne Koitmäe in 15.03 response to “Õhtuleht” contradicting 17.03 decision of NEC

Is it possible to observe counting?

"*Counting of votes cast by electronic means is public*. Persons who are present at the counting of votes must follow the oral orders of the persons designated by the Head of the State Electoral Office."

-- Riigikogu Election Act § 60[1] section 7

The last submitted “vote”

“In case of several votes cast using electronic means, *the last vote* cast by the voter is taken into account.”

-- Riigikogu Election Act § 48[7] section 1

“*A valid mark on an official ballot* indicating the voter’s preference for a particular candidate or ballot question.”

-- Glossary of Election Terminology (2021)

Electronic voting has no invalid ballots

“In case of electronic voting voter makes a choice between candidates in voter application. In comparison to paper ballot elections this rules out possibility of invalid ballots, because voter application is guaranteed to render voter choice into a valid e-vote.”

-- Constitution of Estonia § 60 comment 60

“Incorrect counting of votes”

Criminal offence according to Penal Code §163:
“incorrect counting of votes *is punishable by a pecuniary punishment or up to three years’ imprisonment*”

- Election complaint dismissed because of missing three day deadline, Supreme Court did not accept reinstating the deadline because of delayed observation.

All 312 181 containers illegally counted?

- Vote containers produced by official voting application 1) failed to have valid digital signatures and 2) instead of administrative unit code displayed “0000”
- Both required by Riigikogu Election Act § 48^4 section 4 and National Electoral Committee 10.10.2022 decision nr 47 on form of an electronic vote in 2023 elections
- Electoral Office failed to comment as a reply to mail on 28.03, another election complaint made on 30.03

g49QIXHUyLAAqVEmMV+l0w==.bdoc

DIGIDOC

No card readers found

Help Settings

SIGNATURE

CRYPTO

My eID

1 signature is not valid! More information

Container: /home/tramm/Kood/kryptogramm/data/g49QIXHUyLAAqVEmMV+l0w==.bdoc

Container files

1

RK_2023.question-1.ballot

Container signatures

MÄRT PÕDER - Signature is not valid
37909110298 - Signed on 01. March 2023 at 19:17

Ver. 4.4.0.4447

← START ENCRYPT SAVE AS SEND WITH E-MAIL PRINT SUMMARY SIGN WITH SMART-ID

```
  Document (application/octet-stream): RK_2023.question-1.ballot (798 bytes)

Signatures (1):
  Signature 0 (BES):
2023-12-30T10:28:20Z D [SignatureXAdES_B.cpp:397] - SignatureXAdES_B::validate(POLv2)
DEBUG [SignatureXAdES_B.cpp:689] - Digest to sign { 6C 0A B8 68 64 96 13 DD 1E 46 BF 7C D4 EF A2 E2
84 65 21 FC 9B BC AF D9 0E C1 DE 49 CF 91 ED 68 }:32
    Validation: FAILED (Invalid)
    Exception:
QualifyingProperties block 'UnsignedProperties' is missing.

    EPES policy:
    SPUri:
    Signature method: http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
    Signing time: 2023-03-01T18:17:26Z
    Signing cert: PÕDER,MÄRT,37909110298
    Signed by: PÕDER,MÄRT,37909110298
    Produced At:
    OCSP Responder:
    Message imprint (0):
    TS:
    TS time:
    TSA:
    TSA time:
tramm@nikunai:~/Kood/kryptogramm/data$
```

Administrative unit code “0000”

```
0  0  0  0  .  6  5  9
30 30 30 30 2E 36 35 39 1F

E  r  a  k  o  n  d     E  e  s  t  i     2  0  0
45 72 61 6B 6F 6E 64 20 45 65 73 74 69 20 32 30 30 1F

J  O  H  A  N  N  A  -  M  A  R  I  A     L  E  H  T  M  E
4A 4F 48 41 4E 4E 41 2D 4D 41 52 49 41 20 4C 45 48 54 4D 45
```

Complaint about 312 181 illegal votes

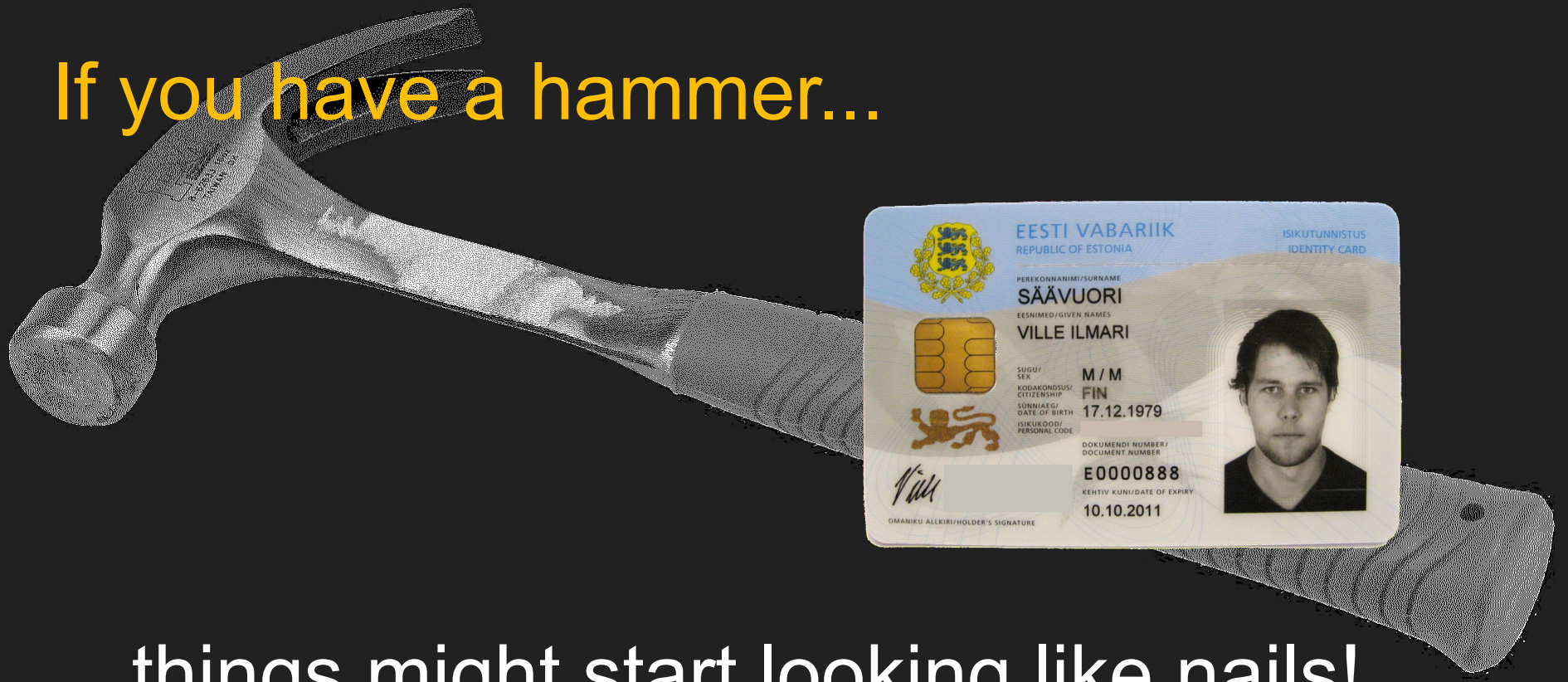
- Electoral Office on 4.04 confirmed that ballots failed to have proper administrative unit codes
- Electoral Office claimed and has kept claiming invalid digital signatures not possible
- Complaint was informally dismissed on 30.03 misguidedly referring to Supreme Court precedent in case 5-21-31 that allowed declaring the election results if the complaint *does not affect the election results*.

Rushed announcement of the results

“The National Electoral Committee registers, by a resolution, the elected members of the Riigikogu after the election day if the term for filing complaints or appeals with the National Electoral Committee and the Supreme Court has expired *or if final resolutions or judgments have been adopted in respect of the complaints filed*.”

-- Riigikogu Election Act § 74 section 1

If you have a hammer...



…things might start looking like nails!

Petition of e-voting observers 2011-2023

1. Right to file complaints in the public interest
2. Auditability of devices and data in all processes
3. IT operations to be legally contestable acts
4. Deadlines take account of specific nature of e-voting
5. Timely access to information, code and other materials

-- E-voting has to be made observable! (12.05.2023)

Is it even possible to conduct legally?

“It can not be said that electronic voting in 2023 parliamentary elections in Estonia was conducted in accordance with the law and in an accountable manner, or *if in its current form this would be even possible*.”

-- Votes without ballots: Observer report on e-voting at 2023 elections in Estonia (draft 4.12.2023)

Who has the burden of proof?

“An election must not just convince the winners that they won, but *prove to the losing candidates that they lost*. Internet voting’s expansion would result in unprovable election results and create grave public distrust in our elections."

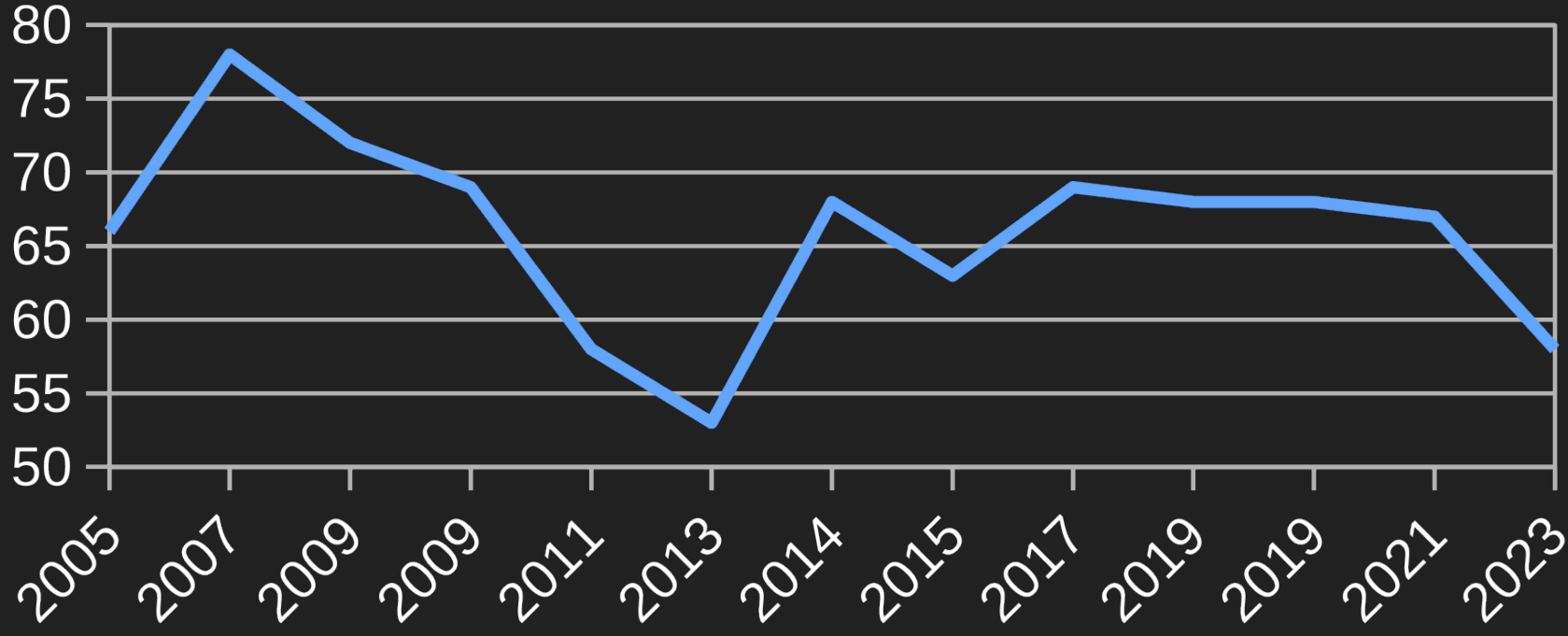
-- Casting Votes Safely: Examining Internet Voting’s Dangers and Highlighting Safer Alternatives (Verified Voting 2023)

Rube Goldberg’s voting system?

"My worry is not so much that none of these problems can be corrected as that correcting all of them perfectly is going to result in a *system that's too complicated to conduct and to administer* -- it's just going to result in a Rube Goldberg system."

-- J. Alex Halderman: Security Analysis of Estonia's Internet Voting System (Chaos Communication Congress 2014)

Fluctuation of trust in e-voting 2005-2023



(data from Estonian Internet voter study 2005-2023 by Johan Skytte Institute, pg 15)

Slides for 37C3 talk 30.12.2023

Should e-voting experience of Estonia be copied?

by Märt Põder

Full report:

Votes without ballots: https://infoaed.ee/evote2023/
Summary of the findings: https://infoaed.ee/findings2023/

Petition of the observers: https://vaatlejad.github.io/

Contact:

tramm@infoaed.ee
@tramm:matrix.org
tramm@mstdn.social

Images used:

Strangels counting ephemeral e-votes: Märt Põder CC BY 2023
Estonian identity card: Wkentaur PD/CC BY-SA 2007
Claw-hammer: Evan-Amos PD 2010