31th Chaos Communication Congress, December 30th 2014

The rise and fall of Internet Voting in Norway

(and the spiders from Mars)

Tor E. Bjørstad (@tbj)
torebj@gmail.com

Evaluating a complex cryptographic implementation

Summary

1. The Norwegian Internet voting trial genuinely tried to do Internet voting "right"
2. Norway's experiment was shaped both by politics and by technology
3. Large unsolved problems remain (both in principle and in practice)

Image: http://commons.wikimedia.org/wiki/File:Ballot_box.JPG (CC-BY-SA 3.0)

Who is this “Tor” guy, anyway?

- Crypto ph.d. (Uni. Bergen)
- IT security consultant at www.mnemonic.no
- 6th time at CCC

Image: http://commons.wikimedia.org/wiki/File:Europe-Norway.svg (CC-BY-SA 3.0)

Norway

- Population 5.08M
- Stable and rich democracy
- High levels of public trust

Image: http://commons.wikimedia.org/wiki/File:Norway_municipalities_2012_blank.svg (CC-BY-SA 2.0)

Concept for Internet Voting in Norway

- Voter may cast advance ballot(s) over the Internet, as well as a physical ballot
- Fancy cryptographic protocol provides end-to-end verifiable security
- Voters get an out-of-band return code that can be used to verify the ballot-as-cast

Image: http://commons.wikimedia.org/wiki/File:Stortinget_i_Oslo.JPG (excerpt) (CC-BY-SA 3.0)

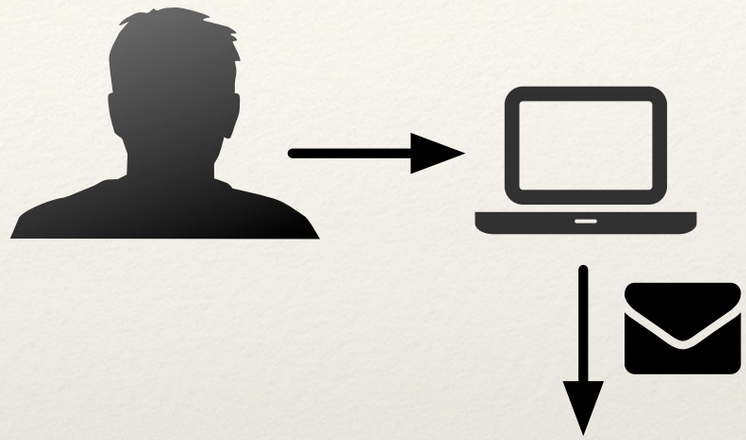
Key security requirements

- Strong authentication
- Anonymous ballots
- Verifiable election result
- Possible to *detect* attacks

Image: http://commons.wikimedia.org/wiki/File:Viking_Age_lock.png (Public domain)

Common counterarguments

- Transparency / verifiability
- Voting in an "uncontrolled environment"
- Cyber-security, state-sponsored threat actors



Cryptographic protocol

- Reasonably “standard” voting protocol
- ElGamal encryption, Schnorr signatures, mix networks
- Shamir Secret Sharing to split keys between operators
- Well described and analysed, see papers by Gjøsteen:

  http://eprint.iacr.org/2010/380

  http://eprint.iacr.org/2013/473

2013: Internet voting trial

- 12 (of 428) municipalities
- 250 000 eligible voters
- 70 000 Internet ballots cast

Image: http://commons.wikimedia.org/wiki/File:Norway_municipalities_2012_blank.svg (CC-BY-SA 2.0)

2013: Internet voting trial

- 12 (of 428) municipalities
- 250 000 eligible voters
- 70 000 Internet ballots cast

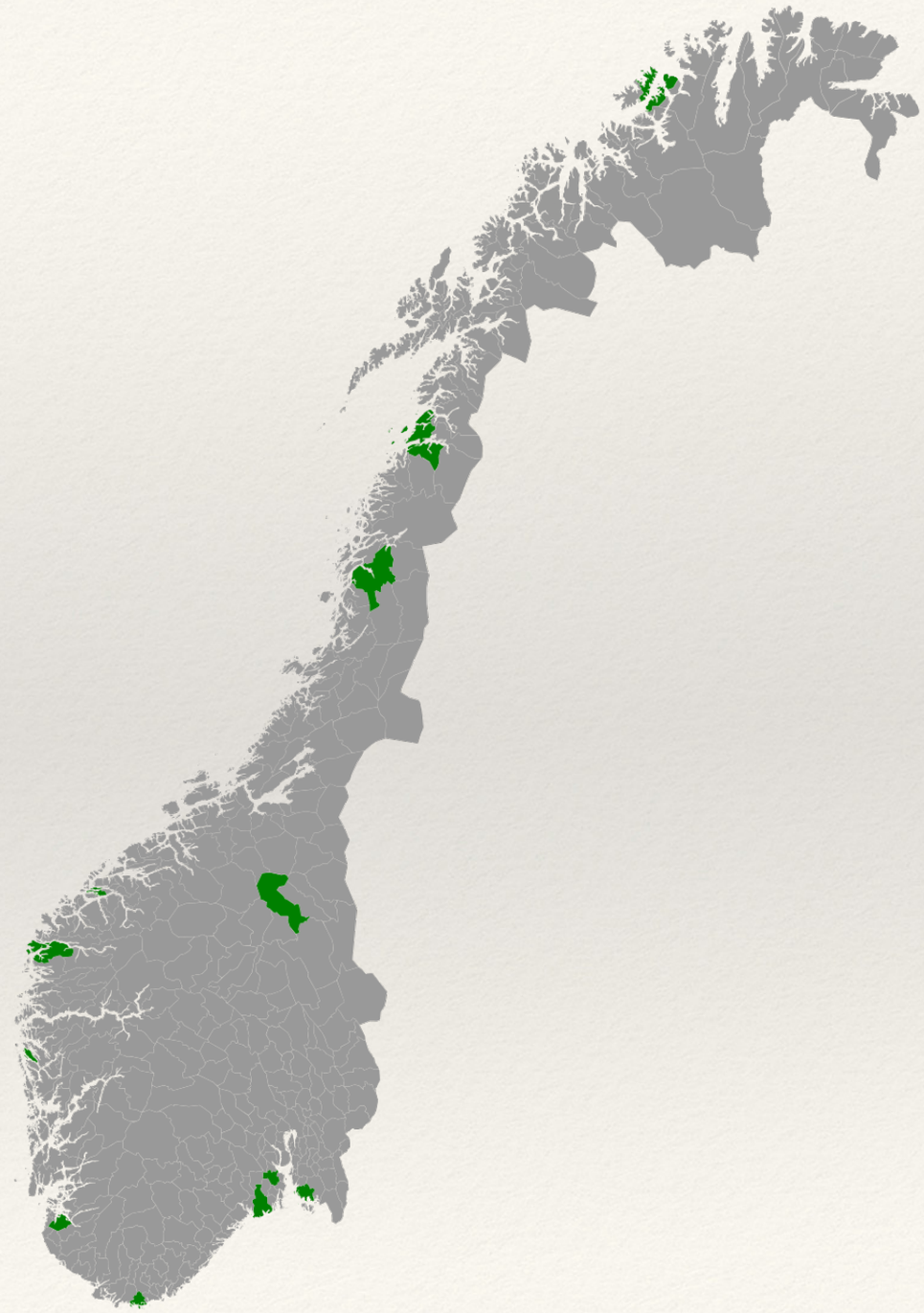


Image: http://commons.wikimedia.org/wiki/File:Parliamentary_election_2013,_Norway,_internet_voting.svg (CC-BY-SA 3.0)

VALG | Internettstemmegivning

A A A

Stortingsvalget 2013

Bokmål

Om internettstemming

Alle stemmeberettigede i Bodø, Bremanger, Fredrikstad, Hammerfest, Larvik, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn og Ålesund kommune kan stemme via Internett ved stortingsvaget 2013.

Du kan stemme fram til 6. september kl. 23.59.

For din sikkerhet vil du automatisk bli logget ut etter 30 minutter.

Hvordan stemme via Internett

Du logger deg inn via ID-porten (f.eks MinID eller BankID). For å stemme må du registrere mobiltelefonnummeret ditt i ID-porten.

Første gang du logger inn kan du bli bedt om å dele ditt telefonnummer. **Du må huke av for "Del med eValg" for å kunne avgi en stemme**.

Se opplæringsvideo.

Valget skal være hemmelig

Pass derfor på at ingen andre ser hva du stemmer.

Husk at du når som helst i forhåndsstemmeperioden kan stemme på nytt via Internett. Du kan også stemme med papirstemmeseddel i et valglokale. En papirstemme annullerer en internettstemme.

Source: https://evalg.stat.no/ (site is now offline)

Additional safeguards

- Feedback mechanisms: Return codes and ballot hashes
- Election monitors to “shadow” system operators
- Source code is public (but under a proprietary licence)
- Independent 3rd party contractors to audit solution
- Operational procedures (physical security, air-gaps, monitoring)

For info on individual verifiability, see e.g.
https://www.regjeringen.no/nb/dep/kmd/prosjekter/e-valg-2011-prosjektet/omprosjektet/bli-digital-valgobservator/id731817/

5 days before election: a bug

SKJERPES: Sikkerheten rundt e-valget er skjerpet etter feil i krypteringen. Foto: Espen Zachariassen

E-VALG 2013

Feil i krypteringen av e-stemmer

Kryptolog ville forkaste alle stemmene. Departementet skjerper sikkerheten.

Source: Teknisk Ukeblad, 2013-09-05. http://www.tu.no/it/2013/09/05/feil-i-krypteringen-av-e-stemmer

2014: Project ends

Source: https://www.regjeringen.no/en/aktuelt/Ikke-flere-forsok-med-stemmegivning-over-Internett-/id764300/

2014: BBC's interpretation

E-voting experiments end in Norway amid security fears

E-voting in Norway did not boost voter turnout, suggests a report into online trials

Source: BBC News, 2014-06-27. http://www.bbc.com/news/technology-28055678

2014: Government response

BBC misreports on ending of Norwegian internet voting pilots

News about e-vote trial

Friday, 27.06.2014, The BBC misreports on ending of Norwegian Internet voting pilots. The Ministry of Local Government and Modernisation has prepared a response to correct the misreported facts and statements:

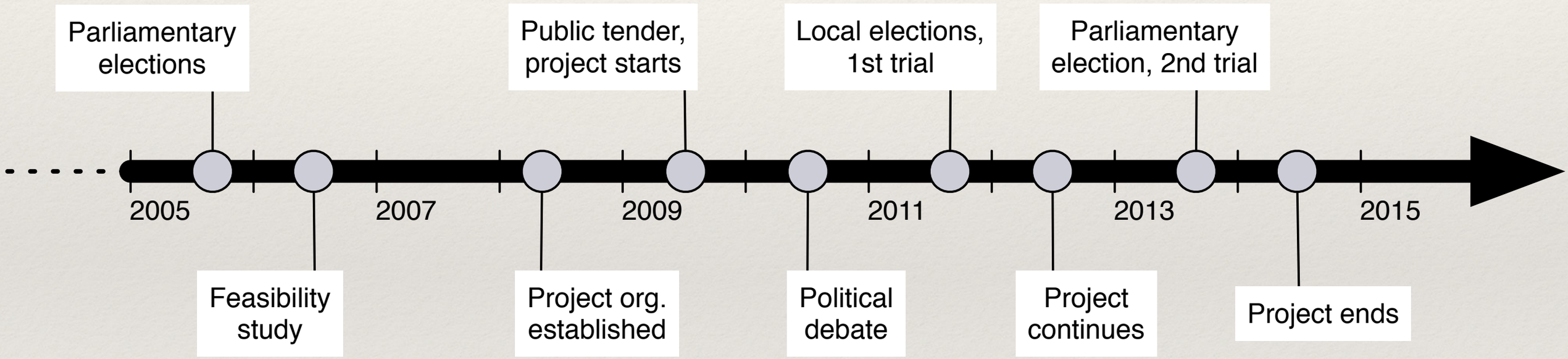
Source: Ministry of Local Government and Modernisation, 2014-06-27. https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/news-about-the-e-vote-2011-project/year/2013/BBC-misreports-on-ending-of-Norwegian-internet-voting-pilots/id764809/

"Norway has a strong traditon of seeking consensus in all matters regarding electoral policy. Due to the lack of broad political will to introduce Internet voting, the Minister of Local Government and Modernization, mr. Jan Tore Sanner, decided not to continue expending public resources on continuing the pilots."

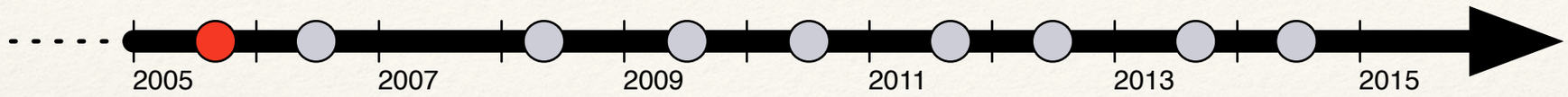
Press statement, 2014-06-27

Source: Ministry of Local Government and Modernisation, 2014-06-27. https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/news-about-the-e-vote-2011-project/year/2013/BBC-misreports-on-ending-of-Norwegian-internet-voting-pilots/id764809/

How did we get here?



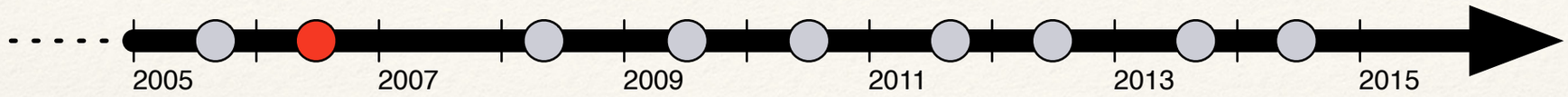
2005: Parliamentary election



- Centre-left coalition wins election
- Minor coalition partners support Internet voting
- (At least) one party named Internet voting in their manifesto

Image: http://commons.wikimedia.org/wiki/File:Champagne_uncorking_photographed_with_a_high_speed_air-gap_flash.jpg
(CC-BY-SA 3.0)

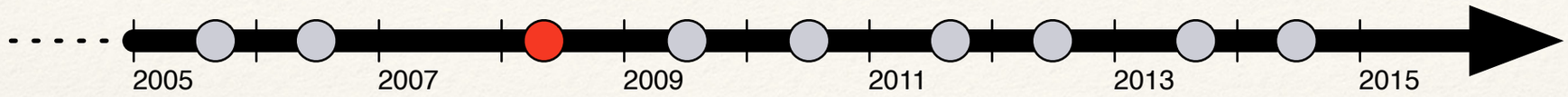
2004-2006: Feasibility study



- "Electronic voting — challenges and possibilities"
- Feasibility study commissioned by previous government
- Concluded that Internet voting could be feasible

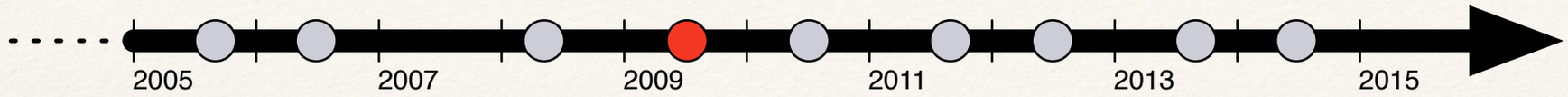
https://www.regjeringen.no/nb/dokumenter/elektronisk-stemmegivning---utfordringer/id278479/

2008: Pre-project planning



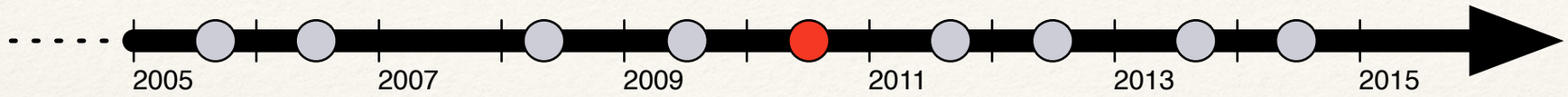
- Departmental funding was obtained
- Project organisation for “e-Valg 2011” established
- Requirements specifications and use-cases
- Voting process documentation

2009: Vendor selection



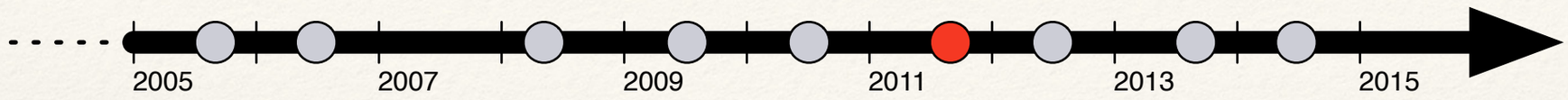
- A public tender process was initiated
- By late 2009, two main vendors had been selected
- Goal: trials leading to full general availability by 2017
- Initial version finished (after some delays) in July 2011

2010: Political debate



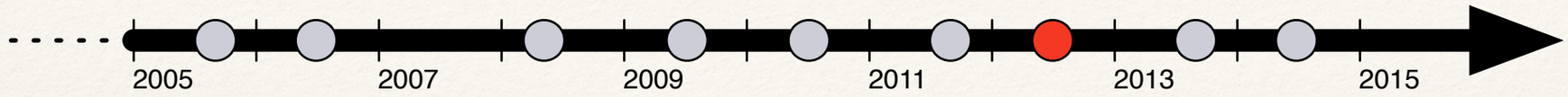
- The imminent voting trial triggers public debate
- Sceptical voices: academia, journalists, political opposition
- 3 MPs submit a motion to cancel the trial, but lose the vote
- Two municipalities withdraw from the trial

2011: Local elections



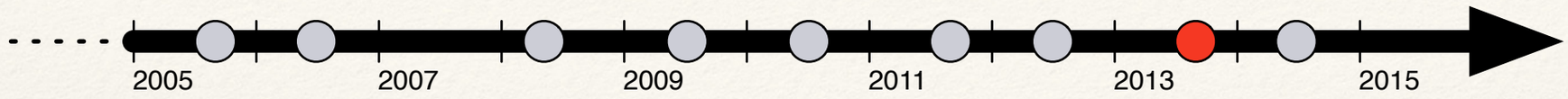
- Internet voting pilot in 10 municipalities
- Various operational hi jinx, but overall success
- 168 000 eligible voters
- 27 500 voters used the Internet
- 9 invalid votes (!)

2012: Project continues



- Project continues with a single software vendor
- Improvements in mixing (anonymization) phase
- Replace client Java applet with JavaScript crypto

2013: Parliamentary election



- Back to where the talk started
- Internet voting in 12 municipalities
- 70 000 Internet ballots cast
- Post election, a change of government (after 8 years)

Image: http://commons.wikimedia.org/wiki/File:Champagne_uncorking_photographed_with_a_high_speed_air-gap_flash.jpg
(CC-BY-SA 3.0)

Summary: what went right

- The system *worked well* technically:
  - Not significant availability / performance issues
    - Few spoiled or invalid ballots
    - Audit log verification did not show irregularities
- System proved popular among the users
- Several issues encountered, but no “black swans”

Summary: difficult areas

- Tradeoff: Security vs verifiability / testability
- Physical artifacts (voting cards / return codes)
- Key management, separation of duties
- Voter understanding of security mechanisms
  - Ability to verify
  - Phishing demonstration
- Secure software development

For info on the phishing demonstration by Olsen and Nordhaug, see e.g. http://www.tu.no/it/2011/09/30/alle-ble-lurt-i-falskt-e-valg (Norwegian only)

Technical review

- Source code was publicly available
- Low degree of (public) scrutiny, no in-depth analysis
- Project generally didn't succeed in engaging tech community
- Some exceptions:
  - Phishing experiment by Olsen and Nordhaug in 2011
  - Report on code quality by Østvold and Karlsen in 2012

"[Perform a] third party review of those parts of the [server-side electronic voting system] that implement cryptographic primitives and generate keys"

– *Assignment given me by KRD*

OK, what does this look like?

SUBVERSION REPOSITORIES INTERNETTSTEMMEGIVNING

Internettstemmegivning | English - English

(root)/src/ - Rev 8

Rev HEAD Go

Rev 7 | Last modification | Compare with Previous | View Log | Download | RSS feed

LAST MODIFICATION

Rev 8 2013-09-05 22:55:18

Author: evalgsvn

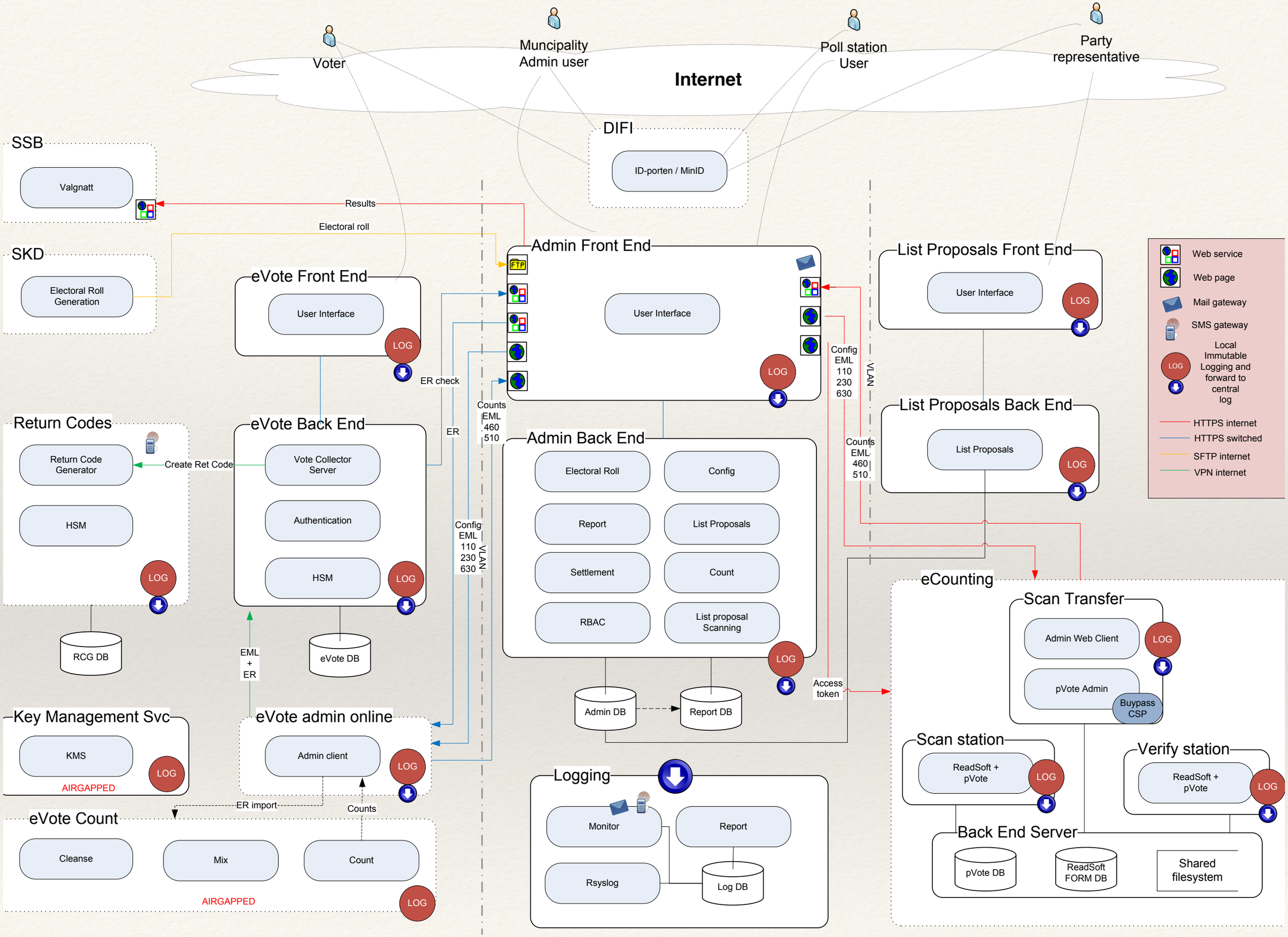
Log message:

ver 3.2.7.1

Path		Last modification		Log	Download	RSS
src/	8	472d 21h	evalgsvn	Log	Download	RSS
auditing/	8	472d 21h	evalgsvn	Log	Download	RSS
authentication/	6	501d 06h	evalgsvn	Log	Download	RSS
counting/	8	472d 21h	evalgsvn	Log	Download	RSS
cryptography/	6	501d 06h	evalgsvn	Log	Download	RSS
evoting/	8	472d 21h	evalgsvn	Log	Download	RSS
jbasis-parent/	4	538d 10h	evalgsvn	Log	Download	RSS
parent-config/	2	538d 11h	evalgsvn	Log	Download	RSS
protocol/	8	472d 21h	evalgsvn	Log	Download	RSS
secure-logger/	4	538d 10h	evalgsvn	Log	Download	RSS
vsframework/	8	472d 21h	evalgsvn	Log	Download	RSS

Compare Paths

Source: Internet voting source code repository at: https://sourcecode.valg.no/websvn/



Source: System documentation at: https://brukerveiledning.valg.no/Dokumentasjon/Dokumentasjon/Forms/AllItems.aspx

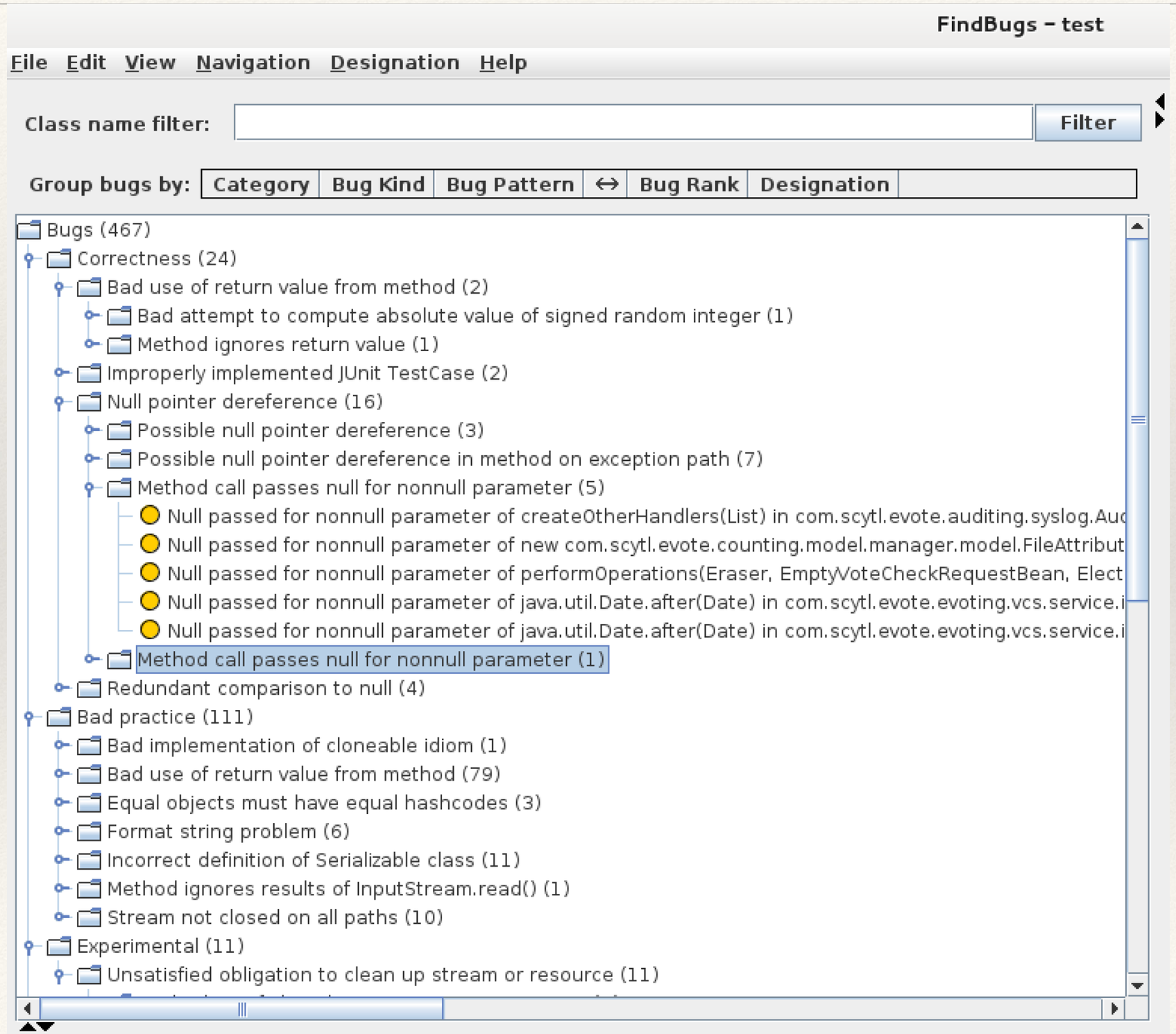
200 000 lines?!

Project	Version	Purpose	Size (SLoC)
auditing	3.2.4	Auditing	5 750
authentication	3.2.4	Client authentication	11 250
counting	3.2.4	Ballot counting	38 000
evoting	3.2.4	e-voting application	25 250
jbasis-parent	2.8.9	Library covering basic java functionality	24 000
parent-config	2.3.1	Build configuration, no code	-
protocol	3.2.5	e-voting cryptographic protocols	34 500
secure-logger	2.0.6	Library for secure logging	4 500
vsframework	3.2.4	Voting system framework	68 250
TOTAL			**211 500**

Approximate Java source length, not counting comments, white space, unit tests, and unused modules.

Source: Own work

FindBugs



Source: Own work


Review of crypto
looks purrfect
ICANHASCHEEZBURGER.COM

Code safari findings (I)

Poor separation between “security logic” and “business logic”

- Unclear links between high-level design and implementation
- Dependency injection (Spring) also obfuscates readability
- Difficult to understand what’s happening, and where
- Security depends on runtime environment and config

Code safari findings (II)

Large amounts of low-level crypto code

- Common anti-pattern with Java crypto (JCE)
- “Copy-and-paste” development
- Mostly sensible choices, but often inconsistencies
- Duplication of crypto functionality and interfaces

Code safari findings (III)

Enterprise software syndrome:

- Code looks suspiciously like “average” enterprise software
- Difficulty to establish and enforce technical quality metrics
- Appropriate quality and assurance levels for critical code?

Crypto bugs (I)

```
String salt = "Static salt for use in key
     genereation while exporting security token";
PBEKeySpec keySpec = new
     PBEKeySpec(password.toCharArray(), salt.getBytes(), 2, 256);
SecretKeyFactory keyFactory =
     SecretKeyFactory.getInstance(“PBKDF2WithHmacSHA1");
SecretKey key = keyFactory.generateSecret(keySpec);
cipher = Cipher.getInstance(“AES/CFB/PKCS7PADDING",
     new BouncyCastleProvider());
byte[] iv =
   new byte[] {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06,
   0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };
AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
cipher.init(mode, key, paramSpec);
byte[] outData = cipher.doFinal(inData);
```

Source code excerpt from utility class UtilsRBAC.java, method cipherSymmetrically()

Crypto bugs (I)

```
String salt = "Static salt for use in key
     genereation while exporting security token";
PBEKeySpec keySpec = new
     PBEKeySpec(password.toCharArray(), salt.getBytes(), 2, 256);
SecretKeyFactory keyFactory =
     SecretKeyFactory.getInstance(“PBKDF2WithHmacSHA1");
SecretKey key = keyFactory.generateSecret(keySpec);
cipher = Cipher.getInstance(“AES/CFB/PKCS7PADDING",
     new BouncyCastleProvider());
byte[] iv =
   new byte[] {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06,
   0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };
AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
cipher.init(mode, key, paramSpec);
byte[] outData = cipher.doFinal(inData);
```

Source code excerpt from utility class UtilsRBAC.java, method cipherSymmetrically()

Crypto bugs (II)

- Shamir Secret Sharing (SSS) is used to split encryption keys
- SSS is *unconditionally* secure iff correctly implemented
- Bug in the coefficient generation broke the security proof
- Probably still *statistically* secure, though

Crypto weirdnesses

Hard to judge impact, depends on usage and threats:

- Use of MD5 to verify temporary file integrity
- Strange custom implementation of data enveloping
- Secure audit logger is not by itself secure against truncation
- Sensitive plaintext written to disk during key generation
- SecureRandom not explicitly initialised, uses platform defaults
- …

That critical encryption bug

A single misplaced statement …

```
this._key = '';
```

… in the JavaScript client's PRNG.generate function …

… which was outside my crypto audit scope.

Thoughts (I)

- What I did was a pure source code analysis exercise
- System is too complex to be “verified” bottom up
- Someone else tested the voting front-end web app
- No tests of back-end runtime (e.g. malware infection scenario)

Thoughts (II)

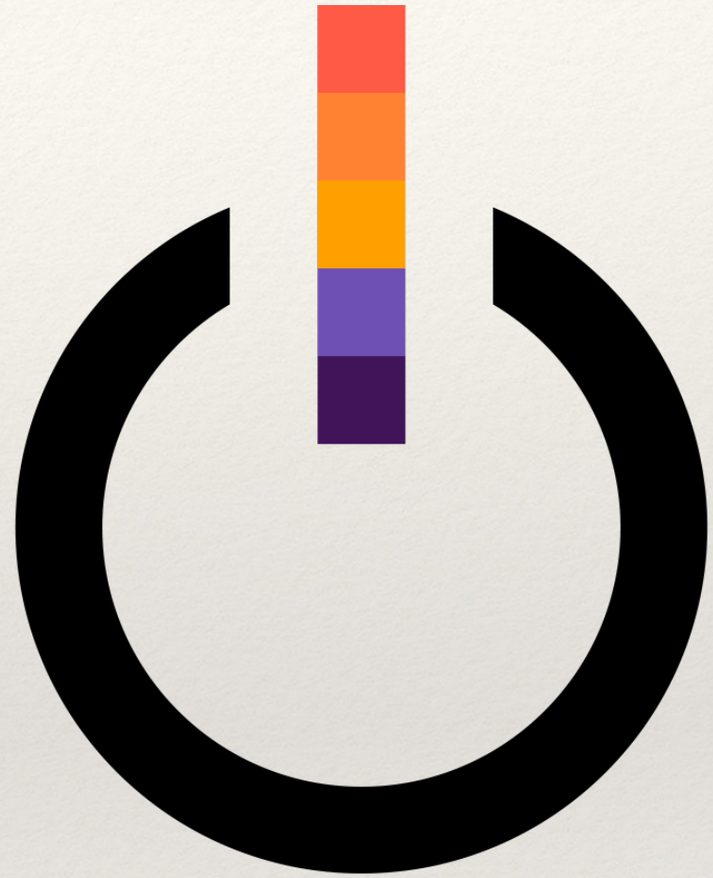
- How to involve the tech community?
  - Common instinctive reaction: “No!” (won’t participate)
    - High barrier to entry even for techies
    - Could the incentives be improved?
- Culture / language barrier inhibiting foreign interest
- Norway is after all a small and rather obscure country

The end …?

- Of Internet voting in Norway, at least for now
- Technology marches on in other areas;
  - Electronic voter rolls
  - Scanning and counting
- Internet / computerised voting on the agenda elsewhere

Thank you

- Thanks for getting up early!
- Questions and comments?
- Get in touch:
  - Email: torebj@gmail.com
  - Twitter: @tbj
- Enjoy the rest of 31C3!



a new dawn