Verifiability experiences in government online voting
E-Vote-ID 2017

Jordi Puiggalí
CSO and SVP of Research & Security
Scytl Secure Electronic Voting

October, 2017
Online voting security and verifiability

Government adoption
<table>
<thead>
<tr>
<th>Year</th>
<th>E2E encryption</th>
<th>Standard security</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security and verifiability
Privacy & Integrity

Anonymous tally
E2E encryption
Neuchâtel
Geneva
Standard security

Countries: Switzerland, Canada, France, India, UK, France, England.
<table>
<thead>
<tr>
<th>Security and verifiability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verifiability</strong></td>
</tr>
</tbody>
</table>

### Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal verifiability</td>
<td>2002-2019</td>
</tr>
<tr>
<td>Individual verifiability</td>
<td>2002-2019</td>
</tr>
<tr>
<td>Anonymous tally</td>
<td>2002-2019</td>
</tr>
<tr>
<td>E2E encryption</td>
<td>2002-2019</td>
</tr>
<tr>
<td>Standard security</td>
<td>2002-2019</td>
</tr>
</tbody>
</table>

**Countries Represented:**
- Neuchâtel
- Geneva
- Estonia
- Canada
- United Kingdom
- France
- Netherlands

**Flag Colors:**
- Red
- Blue
- White
- Black
- Other colors as necessary
Verifiability
Verifiability

Types of verifiability

Based on what is verified
- Cast-as-intended
- Recorded-as-cast

Based on who verifies
- Individual verifiability
- Universal verifiability

Eligibility verification
- Counted-as-recorded
- Eligibility verification

Vote counting

Electoral board

Vote preparation

Vote casting

Vote reception

Vote

Scytl
Innovating Democracy
• Cast-as-intended
  • Return Codes: Norway and Switzerland
  • Cast and decrypt: Estonia and Australia (NSW)
  • Cast or cancel: used by Helios but not adopted by governments
• Recorded-as-cast
  • Voting receipts: Norway and Switzerland
  • Embedded in cast-as-intended proof: Estonia and Australia
• Counted-as-recorded
  • Verifiable mixnet: Norway and Switzerland
  • Homomorphic tally: none of the governments implemented it
How is possible to verify if verifiability properties are properly designed?

Provable security uses security (cryptographic) and/or formal (symbolic) proofs to define the security properties of the system.

- Security proofs are based on modeling the security of the protocol in front an adversary.
- Formal proofs use an specific mathematical formal algebra to represent the protocol and test it using an automated formal framework.
Source code publication provides transparency

```java
/**
 * The HelloWorldApp class implements an application that
 * simply prints "Hello World!" to standard output.
 */
class HelloWorldApp {
    public static void main(String[] args) {
        System.out.println("Hello World!"); // Display the string.
    }
}
```

But not verifiability

- Publishing source code **does not ensure** that there are **no security errors** in the code that can be exploited (e.g., Washington DC project)
- Publishing the source code **does not ensure that this code is the same one used** by the voter to cast a vote
- Election accuracy should be independent from software audits: **software independence**
• Types of votes correctness:
  • Before casting the vote: warns voters against incorrect selections.
  • Before storing the vote in the Ballot Box: checks contents of received votes (without compromising voter privacy)
  • Before counting the votes: prevents counting invalid votes
The analysis of implemented voting system will evaluate the following parameters:

- Cast-as-intended implementation
- Recorded-as-cast implementation
- Counted-as-recorded implementation
- Voter verification usage
- Publication of source code
- Provable security
- Other properties (e.g., vote correctness)
Verifiability in government implementations

Government adoption
Government implementations
Norway

Voter
Voting card

Verifies return codes

Encrypted vote

Operates encrypted vote

Online voting server

Operates encrypted vote

Operated vote

Sends return codes

<table>
<thead>
<tr>
<th>Brukernavn</th>
<th>Passord</th>
<th>Sikkerhetskoder</th>
</tr>
</thead>
<tbody>
<tr>
<td>02045698156</td>
<td>sdppa3</td>
<td>Sert- d8by-cs9- u7lo-jf7d</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parti</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disney Party</td>
<td>186473</td>
</tr>
<tr>
<td>Marvel Party</td>
<td>657794</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kandidat</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donald Duck, f. 1934, Disneyland</td>
<td>453782</td>
</tr>
<tr>
<td>Peter Pan, f. 1904, Disneyland</td>
<td>083128</td>
</tr>
</tbody>
</table>
Government implementations
Estonia

1. Cast

2. Verify

1. Voter
2. Stores encrypted vote
3. Verification bar code
4. Vote identifier
5. Online voting system server
6. Vote decryption
Government implementations
Switzerland – SwissPost/Scytl

1. Cast & verify
   - Encrypted vote + verification proof
   - Return codes
   - Online voting system server
   - Return Codes from encrypted vote
   - Encrypted vote
   - Online voting system server
   - Operates validation code

2. Confirm
   - Voting card
   - Verifies Return Codes
   - Verifies Finalization Code

3. Voter
   - 657294
   - 1
   - 2

4. Cast & verify
   - Voting card
   - Verifies Return Codes
   - Verifies Finalization Code

5. Voter
   - Validation code
   - 0921

6. Finalization code
   - 15149002
   - Online voting system server
Government implementations
Switzerland – Geneva

1. Cast & verify
   - Voter
   - Verifies Return Codes

2. Confirm
   - Verifies Return Codes
   - Voting card

3. Return Codes from clear text vote
   - Online voting system server
   - Clear-text vote
   - 657294
   - return codes

4. Operates validation code
   - Validation code
   - 0921

5. Verification
   - Voter
   - Validation code
   - 0921

6. Online voting system server

7. Finalization code
   - 15149002

8. Online voting system server
   - Finalization code
Government implementations
Australia – New South Wales

1. Cast
   - Voter
   - Encrypted + verification vote
   - Online voting system
     - Stores encrypted vote
     - Stores verification vote

2. Verify
   - Credential + Receipt Number
   - Vote contents
   - Verification system
     - Decrypts verification vote
<table>
<thead>
<tr>
<th></th>
<th>Norway</th>
<th>Estonia</th>
<th>Switzerland (Swiss Post)</th>
<th>Switzerland (Geneva)</th>
<th>Australia (NSW)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cast-as-intended</strong></td>
<td>Return codes</td>
<td>Decryption in device</td>
<td>Return codes</td>
<td>Return codes</td>
<td>Decryption in server</td>
</tr>
<tr>
<td><strong>Recorded-as-cast</strong></td>
<td>At any time with receipts</td>
<td>Up to 1 hour</td>
<td>After counting with receipts</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Counted-as-recorded</strong></td>
<td>Verifiable mixnet</td>
<td>None</td>
<td>Verifiable mixnet</td>
<td>None</td>
<td>Vote re-encryption</td>
</tr>
<tr>
<td><strong>Voter verification</strong></td>
<td>70% (small sample)</td>
<td>4% (large sample)</td>
<td>Unknown</td>
<td>Unknown</td>
<td>1% (large sample)</td>
</tr>
<tr>
<td><strong>Public source code</strong></td>
<td>All the system</td>
<td>Only server side + verifier</td>
<td>None</td>
<td>Only counting side</td>
<td>None</td>
</tr>
<tr>
<td><strong>Vote correctness</strong></td>
<td>Yes</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td><strong>Provable security</strong></td>
<td>Yes (Individual and Universal)</td>
<td>None</td>
<td>Yes (Individual and Universal)</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>E2E encryption</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Conclusions
• Not enough case studies to point a specific model as example of best practice, but Norway and Switzerland still the ones that have made so far more efforts
• Cast-as-intended implementation is more adopted than counted-as-recoded
• Governments still keep trust on server side and do not broad adopt universal verifiability
• Only two system provides full verifiability: Norway and Switzerland (SwissPost)
• Publication of source code is usually partial and full disclosure is linked to achieve full verifiability to avoid risks
• Provable security is gaining on acceptance to evaluate the correct implementation of the security properties (mainly verifiability)
Any Questions?
Innovating Democracy