E-Democracy and e-voting
How to make them secure and transparent

August 2013

Jordi Puiggali
CSO and SVP R&D
Jordi.puiggali@scytl.com
- Introduction e-Democracy
- Security and Transparency in e-Voting
- Example of Verifiable Voting Solution
- Conclusions
Introduction

About e-democracy
Consultations and Referendums allow the public to express their opinion and exert some influence on decision-making processes.

e-Democracy uses the support of the Information and Communication Technologies (ICT) to allow the public to participate in the decision-making process (e.g., e-Participation, e-Consultations, e-Voting…).

The use of ICT provides the following benefits to the participation process:

- The public can express their opinion more easily and at their own convenience
- Information provided by the public can be processed faster
- Decision-makers can reach a wider public on a more regular basis
- Decision-makers can be assisted in order to extract conclusions from the public’s opinions

e-Government does not replace conventional participation processes. On the contrary, it should be used to compliment and enhance them.
Mexico - IEDF

- Citizen consultation: More than 7,200,000 people from 1,815 neighborhoods of Mexico City can participate every year during the city-wide citizen consultation. In November 2012 Internet Voting was available as the unique channel during the advanced voting period.

Spain – Madrid

- Citizen consultation: The City of Madrid started in 2004 to carry out the e-consultations. It has performed more than 20 binding e-participation processes involving approximately 3 million people.

Switzerland - Neuchatel

- Canton Referendum: Every 3 months, Swiss Cantons execute referendum processes for their citizens. Since 2004 Neuchâtel Canton is using an Internet voting platform to carry out from 3 to 6 citizen consultations, binding electoral processes and referenda each year. Internet channel has received up to 60% of the total votes tallied.
E-democracy

Advantages

• **Convenience:** Citizens can access to the democratic processes from anywhere at anytime.
• **Immediate:** Dissemination of information or citizen consultations can be done very fast and more often.
• **Costs:** Less logistics and material costs and therefore, cheaper to update information and setup consultation processes.
• **Accessibility:** People with accessibility problems can participate in the process without requiring logistics or assistance.

Risks

• **Digital divide:** Citizens that do not have access to new technologies could be excluded to the process. Alternative ways to participate can be provided in these cases.
• **Transparency:** Information becomes electronic instead of tangible, making the process less transparent to observers and auditors. Special considerations need to be make this systems as transparent as traditional ones (e.g., E2E verifiability).
• **Security:** Remote systems are more vulnerable to security issues than standalone ones. Strong security measures need to be considered to implement these systems.

Is it possible to make a secure and transparent e-voting process?
E-voting Security

Risks and requirements
Electronic voting creates a new indirect voting relationship that brings **new security risks** that reduce the trustworthiness of the electoral process.
Four main sources of security risks emerge due to the technical infrastructure interposed between the voter and the electoral board:

- **The digital (virtual) nature of the ballots**
  - Ballots may be added, deleted or otherwise manipulated
  - Voters’ privacy may be compromised on a large scale

- **The complexity of the systems used**
  - Electronic equipment may malfunction
  - Software may contain programming errors

- **The lack of transparency of the systems used**
  - The technical infrastructure is not easily audited

- **The introduction of people with privileges on the systems used**
  - New players enter the scene

These risks can be mitigated using adequate cryptographic voting protocols.
Evolution of e-voting Research

Past, present and future
Evolution of e-voting Research

Overview

Privacy and Integrity

Verifiability
Privacy and integrity

Overview
Standard security measures: Channel encryption (SSL)

Concerns: Data vulnerable to external/internal attacks against voters’ privacy and election integrity

End-to-end protection

• Protection of votes in the voting terminal
  • Encryption: Votes encrypted using election public key
  • Digital signatures: Preservation of vote eligibility and integrity
Vote encryption is enough to preserve privacy?

No: voters still can be correlated with votes when decrypted

Practices
- Anonymization of vote decryption process: Prevents correlation between decrypted votes and voting order
- Multiparty computation: Prevents correlation between decrypted votes and voting order
Privacy and Integrity

Anonymization schemes

- Pollsterless
- Homomorphic Tally
- Two Agencies
- Mixing
• **Homomorphic tally features**
  
  • Votes are encrypted by voters using a cryptographic algorithm with homomorphic properties (e.g., El Gammal)
  
  • Votes are digitally signed by voters before being cast
  
  • Encrypted votes are operated to obtain a encrypted result
  
  • To obtain the election result, only the encrypted result of the vote operation is decrypted instead the individual votes
Encrypted votes

Operation

Result:
C1: 1 vote
C2: 2 votes
C3: 0 votes
C4: 0 votes
C5: 1 vote
• **Mixing features**

  • Encrypted votes are digitally signed by voter’s digital certificate

  • Voting server accepts votes digitally signed by an eligible voter

  • Mixing server shuffles and decrypts the votes in an isolated environment
Mixing process sample
Scytl’s protocol uses the following cryptographic techniques:

- **Secret sharing schemes**
  - Protect the election private key
- **Digital certificates**
  - Implement strong authentication of voters and digital signature of information
- **Digital envelopes**
  - Preserve the vote secrecy
- **Voting receipts**
  - Allow voters to check if their votes are present in the final tally
- **Mixing**
  - Breaks the correlation between encrypted votes and decrypted ones
- **Immutable logs**
  - Preserve log integrity and authenticity
Verifiability

Concepts
Standard cryptography = Data Protection

- Encrypts the votes and signs it
- Does the encrypted vote really contain the selected voting options?
- Does the decryption process properly retrieve the contents of the encrypted vote?

No Verifiability
Verifiability Concerns

Voter Vote Encryption E-vote Malicious software

Privacy and Integrity protection

Vote Decryption Counting

Electoral Board Results

Voting options

24
Open Source = Programming transparency

/**
 * 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.
    }
}

No 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 **do 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**
Advanced cryptography = Verification Proofs

- Irrefutable mathematical proofs without compromising privacy
  - Proofs of valid encrypted contents
  - Proofs of correct decryption
  - Proofs of correct anonymization
• Votes and processes (e.g., counting) are based on tangible elements.
• Audit can be done by voters, observers and independent auditors by human means when the processes are carried out.
• Vote casting process is **difficult to audit**:
  • Voters **cannot verify if their votes are stored** in the ballot box
  • Observers have **limited or no access to the vote delivery and storage process**
Verifiability in electronic voting elections

- Votes and processes are happening in a **logical dimension**:  
  - Audit cannot be done by human means
Verifiability

Types of election verifiability

- Individual verifiability
  - Cast as intended
  - Recorded as cast

- Universal verifiability
  - Eligibility verification
  - Counted as recorded

Based on what is verified
Based on who verifies

Voter → Electoral board

Vote preparation → Vote casting → Vote reception

Election observers / auditors

Results

Vote Counting

Scytl
Innovating Democracy
Verifiable voting

Norway case
Verifiable Voting System

Verifiability mechanisms implemented at Norwegian voting platform
Norway implements a Scytl cryptographic e-voting scheme that uses advanced cryptographic algorithms for providing verifiable mechanisms based on mathematical proofs.

**Cast as intended verifiability (individual)**
- Based on Return Codes generated by the voting servers over the encrypted vote (preserves voter privacy)

**Recorded as cast verifiability (individual)**
- Based on using the Return Codes and providing voting receipts to voters

**Counted as recorded verifiability (universal)**
- Based on generating mathematical zero knowledge proofs of correct mixing and decryption.

**Eligibility verifiability (universal)**
- Based on using individual digital certificates per voter
Scytl Cast as Intended Verification

Verifiability mechanisms implemented at Scytl solutions
### Scytl Cast as Intended Verification

**Voting Card with Return codes**

<table>
<thead>
<tr>
<th>Parti</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disney Party</td>
<td>186479</td>
</tr>
<tr>
<td>Marvel Party</td>
<td>657294</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>
<tr>
<td>Mickey Mouse, f. 1928, Disneyland</td>
<td>537287</td>
</tr>
<tr>
<td>Minnie Mouse, f. 1928, Disneyland</td>
<td>975659</td>
</tr>
<tr>
<td>Aurora Princess, f. 1959, Disneyland</td>
<td>736181</td>
</tr>
</tbody>
</table>

**Voting options**

**Return codes**

```plaintext
Brukernavn: 02045698156
Passord: sdppa3
Sikkerhetskoder: 5ert - df8y - csd9 - u7lo - jfdb
```
Scytl Recorded as Cast Verification

Recorded as cast verification – Return Codes

Scytl
Innovating Democracy

Voter

Voting Card

Verifies Return Codes

Encrypted vote

Voting Receipt

Internet

E-Vote System Server

Operates Encrypted Vote

Operated Vote

Validation System

Sends Return Codes

Return Codes

Brukernavn: 02045698156
Passord: sdppa3

<table>
<thead>
<tr>
<th>Sikkerhetskoder</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>5ert – df8y – csd9 – u7lo - jf8b</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parti</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disney Party</td>
<td>186479</td>
</tr>
<tr>
<td>Marvel Party</td>
<td>657294</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>
Verification can be done by human means

- It is as easy as search a number in a voting card (it does not require the voter to make mathematical calculations or use a tool for making them like in Helios system).

Verification is accessible

- Return codes can be represented in Braille or audible form to facilitate the verification process to visual impaired voters

Verification of valid vote contents

- Voting server can check if the encrypted vote contains valid contents if the Return Codes are valid.
Scytl Recorded as Cast Verification

Verifiability mechanisms implemented at Scytl solutions
Receipt ID: w6kh-cdqw-2bc6-adf4
Scytl Counted as Cast Verification

Verifiability mechanisms implemented at Scytl solutions
**Proof of content equivalence:** Proves that the votes have not been manipulated by the Mixing process

**Proofs of correct decryption:** Proofs that the decryption process did not manipulate any vote
Conclusion

About Scytl e-voting solution
Security and transparency are key for e-democracy

End-to-end encryption

Votes should be protected by encrypting and digitally signing voting options in the voting terminal instead of servers.

Anonymous preserving decryption

To preserve in practice voter’s privacy, the decryption process should implement cryptographic mechanisms that prevent correlation of decrypted information and encrypted one.

End-to-end verifiability

Voters should be able to verify that the encrypted vote is cast as intended and observers and independent auditors should be able to check that votes are counted as cast without compromising voters’ privacy.

Software independence

Audit processes should be independent of the software, so the verification does not depend on software audits but on irrefutable mathematical proofs.