Safety first!

Verifiability in the e-vote 2011-system

Christian Bull

The Norwegian E-voting Conference, Sept. 11, 2011
Let’s look back a couple of years

http://www.youtube.com/watch?v=1aBaX9GPSaQ
BIST DU SICHER, DASS DEINE STIMME RICHTIG GEZÄHLT WIRD?
Lessons learned from others

• Openness in every way is essential.
• Secure e-voting in polling stations is also really hard to implement.
• You really want software independent verifiability wherever possible.
• Doing it right takes a lot of time.
A basic premise for e-voting

• One basic and all important premise for all electronic voting is that the public trusts the government not to conspire against it.

• That having been said, the system should not require that no conspiracy against it exists within the government!
What are Norway's advantages?

• ...and prerequisites for e-voting in general?
• Very high public trust in Government
• Absolute trust in central election administration
• Relatively low levels of political conflict
What we believe we’ve achieved

A New approach to transparency

• A fully open source system  
  (you must be very clear in procurement process)
• Voter verifiability in remote e-voting by use of return codes
• Much improved robustness against client side (in)security.
• Excellent auditability and verifiability  
  • Can be improved further by an N-version architecture in some components
• Observation in the “back office” combined with voter observation of return code replaces the function of the observer in the polling station
A quick overview of the solution

- Log on
- Submit vote

E-voting system

Receipt code

Polling card
How does the system know who I am?
Authentiwhat?

• When you turn up at the polling station, you are required to *identify* yourself.
• In Norway, voters have been required to produce an *ID-card* to vote (since 2007)
• This is analogous to the process of *authentication* to a computer system, for instance using an eID.
Important properties of a good eID

• It must be obvious to the user that this is an identity document.
• A voter should not be tempted to sell his voting credentials.
  • It must have other uses than just e-voting.
  • These other uses must be familiar and of value to the voter
Select an electronic ID to identify yourself:

- **MinID**
  - SELECT
  - Use your personal password and code from SMS or PIN code letter.

- **Bypass**
  - SELECT
  - Use smart card and card reader from Bypass.

- **Commfides**
  - SELECT
  - Use your Commfides USB stick.

Help to log in: [Contact form](#) | Tel.: 800 30 300 | [Frequently asked questions](#) | [About the use of electronic ID](#)

Hosted by the Agency for Public Management and eGovernment (Difi)
The Particular Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- Home computer security
- Anonymity of the vote
- Attacks scale
The Particular Challenges of Remote e-voting

- **Auditability / transparency to the lay person**
  - The buying and selling of votes
  - Coercion / family voting
  - Home computer security
  - Anonymity of the vote
Transparent e-voting?

• Complete openness and transparency in all aspects of the project
• Available source code
  – Unfortunately cryptography is really, really hard.
• Cryptographic proofs of correctness
  – Even the voter gets one
  – The good thing about crypto is that it’s all just maths
• Immutable logging of all significant system events
Transparent e-voting?

• Obviously open source won’t make the system understandable to “everyone”
• ...and extensive use of esoteric cryptography makes things worse...
• ..but at least the lay person can choose which expert to trust.
The Particular Challenges of Remote e-voting

• Auditability / transparency to the lay person

• The buying and selling of votes

• Coercion / family voting

• Home computer security

• Anonymity of the vote
Buying and selling of votes

- In practice this doesn’t scale
- The seller can re-vote
  - Return code for all ballots cast, not only the final
- Votes submitted from a polling station will supersede any vote cast remotely
- Buyer would have to control seller’s eID
  - Would require the voter to give up a lot more than his vote
The Particular Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- Home computer security
- Anonymity of the vote
The Particular Challenges of Remote e-voting

• The coerced can re-vote
  • Return code for all ballots cast, not only the final (receipt freeness)
• Votes submitted from a polling station will supersede any vote cast remotely
• The system will never divulge that a previous vote has already been recorded
• If you accept that bastards are evenly distributed across the political spectrum, this doesn’t really scale either.
The Particular Challenges of Remote e-voting

• Auditability / transparency to the lay person
• The buying and selling of votes
• Coercion / family voting
• Home computer security
• Anonymity of the vote
Encryption and storage of the vote
Conceptual model

Vote verification

Distribution of secrets

Voter → Voting client → Internet → Vote Collection Server → Return Code Generator → Mix and count

Air gap

M of N key shares from parties with competing interests

Voter Administrative system
"Cleansing service"

Counting e-votes

<table>
<thead>
<tr>
<th></th>
<th>Parti A</th>
<th>Parti B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vote</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Counting e-votes

“Cleansing service”

<table>
<thead>
<tr>
<th>Parti A</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parti B</td>
<td>1</td>
</tr>
</tbody>
</table>

Mixing service

Decryption service
Lessons learned.

- Wow, this *really* takes a lot of time to implement.
- High security means it’s time consuming to test, and there are a lot of special cases to test.
- Work closely with the vendor.
- Verifiability and a good monitoring solution gives a lot of confidence.