Trust in E-Voting

Oliver Spycher at Swiss Cyber Storm
Bern, 30th October 2018
E-Voting introduced by Cantons

- CHvote system: developed by GE; AG, BE, BS*, LU, SG and VD have joined.
- Swiss Post solution: FR, NE, TG. GL and GR are planning reintroduction in 2019 respectively 2020.
- These cantons carried out electronic voting trials up to the end of 2015.
- These cantons have not yet carried out any electronic voting trials.

*BS will change over to the Swiss Post system (probably in 2019).
Moving ahead step by step

- Trials since 15 years
- Open to 3.8% of the overall electorate (September 2018)
- Security first

www.bk.admin.ch
People need to trust that…

• Result reflects the voters’ intentions

• Secrecy of the vote is respected

→ …even if they’re not an observer
Trust in Will and Ability
Trust One Trustee

...out of many
Trust in Will and Ability
E-Voting cannot be trusted…

• Transparency…
  • …inherently impossible
  • …only towards experts
  • …eats secrecy

• No meaningful recounts

• And anyhow, administrations will fail
Sure about that?
Trust through verification
Trust through re-verification
Trust through verification

e-mail
Trust through re-verification
Summing up votes is verifiable...

...by checking equations

Ja : 2
Oui: 1
Nein: 1
Full Verifiability

Voters or observers verify that votes have been

- cast as intended
- recorded as cast
- tallied as recorded
Cast as intended

<table>
<thead>
<tr>
<th>N°</th>
<th>Démoc Votation populaire fédérale / Demo Eidgenössische Volksabstimmung</th>
<th>Codes de vérification / Prüfcodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Oui / Ja</td>
<td>Non / Nein</td>
</tr>
<tr>
<td>1a</td>
<td>Initiative populaire: Acceptez-vous «l'initiative populaire A»?</td>
<td>Volksinitiative: Wollen Sie die «Volksinitiative A» annehmen?</td>
</tr>
<tr>
<td></td>
<td>Oui / Ja</td>
<td>Non / Nein</td>
</tr>
<tr>
<td>1b</td>
<td>Contre-projet: Acceptez-vous le contreprojet de l'Assemblée fédérale «Contre-projet B»?</td>
<td>Gegenentwurf: Wollen Sie den Gegenentwurf der Bundesversammlung «Gegenentwurf B» annehmen?</td>
</tr>
<tr>
<td>1c</td>
<td>Question subsidiaire: Si le peuple et les cantons acceptaient à la fois «l'initiative A» et «le contre-projet B»: Est-ce l'initiative populaire A ou le contre-projet B qui doit entrer en vigueur?</td>
<td>Stichfrage: Falls sowohl die «Volksinitiative A» als auch der «Gegenentwurf B» von Volk und Ständen angenommen werden: Soll die Volksinitiative A oder der Gegenentwurf B in Kraft treten?</td>
</tr>
</tbody>
</table>

Taken from the online demo-system by Swiss Post at e-voting.ch
Cast as intended

Voter  Ballot-Box
Recorded as cast

Ballot-Box
Tallying

Bundeskanzlei BK
Sektion Politische Rechte

Ballot-Box
Tallying

Ballot-Box

anonymous?
Secrecy

Ballot-Box
Secrecy

Ballot-Box
Secrecy

Ballot-Box
Secrecy

Ballot-Box
Secrecy
Tallied as recorded
Tallied as recorded
Tallied as recorded

Can be verified and re-verified
By checking equations
Tallied as recorded

Full chain can be verified and re-verified
By checking equations
Tallied as recorded

Full chain can be verified and re-verified
By checking equations

Ja := 2
Nein := 1
Tallied as recorded

Full chain can be verified and re-verified
By checking equations
Voters or obervers need to be able to detect fraud, assuming that

- 1 out 4 trustees is behaving correctly
- Printing office does not leak codes
Ordinance of the FCh on E-Voting

- Crypto-Protocol
  - Proof of compliance
  - Audit of proof
- Certification
  - Accredited by Swiss Accreditation Service
  - Software EAL2 / EAL4
  - ISO27001
- Source Code Publication
Public Intrusion Test

- Decision by Confederation and Cantons
- 1.Q 2019 enabled by Swiss Post
- Pre-Register: https://pit.post.ch/

Tell your friends!
Conclusion

- Verifiability as a foundation of trust
- Required by the FCh ordinance
- Assessed through certification
- Documented towards the public
Contact:

Oliver Spycher
Dep. Project Leader Vote électronique
oliver.spycher@bk.admin.ch

www.bk.admin.ch