The Adventurous Tale of Online Voting in Switzerland

Christian Folini / @ChrFolini

USENIX Enigma 2021
#Swederland – don't get this wrong

Graphic: Swedish Embassy in Teheran
<table>
<thead>
<tr>
<th>Kanton</th>
<th>Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bezirk Muri</td>
<td></td>
</tr>
<tr>
<td>Wahlzettel-Nr.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Kandidatin/Kandidat</th>
<th>Klasse/Position</th>
<th>Wohnort</th>
<th>Berufliche Erfahrungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td>glp – Grünliberale Partei</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.01</td>
<td>Budmiger Hans-Peter (Hampi), 1976, Unternehmer, Gemeindepräsident, Muri</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.02</td>
<td>Langenbacher Knüsel Silvia, 1966, Unternehmerin, Abtwi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.03</td>
<td>Peyer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.04</td>
<td>Meesch Loredana, 1996, Blaw, Masterstudentin Rechtswissenschaften, Wartenswil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.05</td>
<td>Stöckli Corneli, 1975, Dr. med., Rheumat. &amp; Innere Med., Integrationskom., Muri</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.06</td>
<td>Chande Sabrina, 1980, Projektleiterin Elektroplanung, Mitglied GL, Buttwi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.07</td>
<td>Weber Thomas, 1974, Content Manager, Journalist, Buttwi</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vom Wahlbüro auszufüllen: Kandidatenstimmen: Zusatzstimmen: Total:
## Typical Swiss Election Ballot

<table>
<thead>
<tr>
<th>Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bezirk Muri</td>
</tr>
<tr>
<td>Wahlzettel-Nr.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Kanton</th>
<th>Kandidat</th>
<th>Partei/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td>Aargau</td>
<td>glp – Grünliberale Partei</td>
<td></td>
</tr>
<tr>
<td>06.01</td>
<td>Muri</td>
<td>Budmiger Hans-Peter (Hamp), 1976, Unternehmer, Gemeindepräsident, Muri</td>
<td></td>
</tr>
<tr>
<td>06.02</td>
<td>Muri</td>
<td>Langenbacher Knüsel Silvia, 1966, Unternehmerin, Abtwi</td>
<td></td>
</tr>
<tr>
<td>06.03</td>
<td>Muri</td>
<td>Peyer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri</td>
<td></td>
</tr>
<tr>
<td>06.04</td>
<td>Muri</td>
<td>Menoch Loredana, 1996, Blaw, Masterstudentin Rechtswissenschaften, Waalenswil</td>
<td></td>
</tr>
<tr>
<td>06.05</td>
<td>Muri</td>
<td>Stöckli Cornel, 1975, Dr. med., Rheumat. &amp; Innere Med., Integrationskom., Muri</td>
<td></td>
</tr>
<tr>
<td>06.06</td>
<td>Muri</td>
<td>Chande Sabrina, 1980, Projektleiterin Elektroplanung, Mitglied GL, Buttwil</td>
<td></td>
</tr>
<tr>
<td>06.07</td>
<td>Muri</td>
<td>Weber Thomas, 1974, Content Manager, Journalist, Buttwil</td>
<td></td>
</tr>
</tbody>
</table>

Bonus points for spotting the content manager from Butt-ville.
"We simply can’t build an Internet voting system that is secure against hacking because of the requirement for a secret ballot."

Bruce Schneier, Online Voting Won’t Save Democracy, The Atlantic, May 2017
Arguments in Favor of Internet Voting

The Swiss Perspective
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad

- Visually impaired and quadriplegic voters
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
- Visually impaired and quadriplegic voters
- Formally invalid ballots
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
- Visually impaired and quadriplegic voters
- Formally invalid ballots
- Security issues of physical voting
The Cantons of Switzerland
1st Swiss internet voting project is launched with three pilot cantons.

1st project

2000

1st Geneva trial

Canton Geneva runs the first Swiss internet voting trial.

Entering Scytl

2008

Swiss expats are allowed to vote via Scytl internet voting system in canton Neuchâtel.

Steering Board

2009

Federal administration and cantons establish a joint steering committee.

Consortium

2011

Eight Swiss cantons form a consortium and commission Unisys with the creation of an internet voting system.
Timeline

2011
Federal administration and cantons establish a joint steering committee.

2015
Steering Board

2016
Spanish Scytl and Swiss Post form joint venture and go into production.

2017
Scytl/Swiss Post join

Consortium dies
The eight consortium cantons throw towel after federal administration bars system from use in national elections.

Mainstreaming attempt
The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.
Geneva Quits

2018: Development stopped
2019: System terminated

Source: Twitter: @GE_chancellerie (1141332323025195009)
Spanish Scytl and Swiss Post form joint venture and go into production.

**2016**

**2017**

**2018**

**2019**

**Scytl/Swiss Post join**

**Mainstreaming attempt**

The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.

**Geneva quits**

Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.

**Source Code Publication**

Scytl / Swiss Post publish the source code of their system.
Swiss Post is Being Quit (for the moment)

---

The trapdoor-commitment issue in the Swiss e-voting system was also independently discovered by Thomas Haines of NTNU and by Rolf Huonn of Bern University of Applied Sciences.

---

Researchers Find Critical Backdoor in Swiss Online Voting System

Hey, at least it was dis – which is the whole p... by Thomas Cebul in San Francisco

---

Swiss Post puts e-voting on hold after researchers uncover critical security errors

---

I agree with @damanion on the safety of paper ballots in Aus elections, but the electronic Senate count opens the possibility for undetected error or fraud unless there's a rigorous public audit of the paper records against the digitized preferences. arxiv.org/abs/1610.00127

---

to be continued ...
Spanish Scytl and Swiss Post form joint venture and go into production.

**2016**

**Scytl/Swiss Post join**

**2017**

**Mainstreaming attempt**

The federal chancellor calls on 2/3 of the cantons to offer internet voting for national elections in 2019.

**2018**

**Geneva quits**

Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.

**2019**

**Source Code Publication**

Scytl / Swiss Post publish the source code of their system. Researchers identify three critical vulnerabilities within weeks. The system is put on hold.

**2020**

**Rebooting**

The steering board establishes a dialog with 25 scientists to assess viability of internet voting and support with writing new regulation.
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
  David Basin, ETH Zurich
  Srdjan Capkun, ETH Zurich
  Eric Dubuis, BFH Bern
  Bryan Ford, EPF Lausanne
  Reto Koenig, BFH Bern
  Philipp Locher, BFH Bern
  Olivier Pereira, University of Leuven, Belgium
  Vanessa Teague, Australia
  Bogdan Warinschi, Bristol, UK
  Rolf Haenni, BFH Bern

COMPUTER SCIENTISTS
  David-Olivier Jaquet-Chiffelle, University of Lausanne
  Oscar Nierstrasz, University of Bern
  Adrian Perrig, ETH Zurich
  Carsten Schürmann, Denmark
  Matthias Stürmer, University of Bern
  Ulrich Ultes-Nitsche, University of Fribourg

SECURITY INDUSTRY
  Stéphane Adamiste, SCRT
  Sergio Alves Domingues, SCRT
  Tobias Ellenberger, One Consult

POLITICAL SCIENTISTS
  Florian Egloff, ETH Zurich
  Fabrizio Gilardi, University of Zurich
  Uwe Serdült, Center for Democracy, Aarau

MODERATOR
  Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
  David Basin, ETH Zurich
  Srdjan Capkun, ETH Zurich
  Eric Dubuis, BFH Bern
  Bryan Ford, EPF Lausanne
  Reto Koenig, BFH Bern
  Philipp Locher, BFH Bern
  Olivier Pereira, University of Leuven, Belgium
  Vanessa Teague, Australia
  Bogdan Warinschi, Bristol, UK
  Rolf Haenni, BFH Bern

SECURITY INDUSTRY
  Stéphane Adamiste, SCRT
  Sergio Alves Domingues, SCRT
  Tobias Ellenberger, One Consult

COMPUTER SCIENTISTS
  David-Olivier Jaquet-Chiffelle, University of Lausanne
  Oscar Nierstrasz, University of Bern
  Adrian Perrig, ETH Zurich
  Carsten Schürmann, Denmark
  Matthias Stürmer, University of Bern
  Ulrich Ultes-Nitsche, University of Fribourg

POLITICAL SCIENTISTS
  Florian Egloff, ETH Zurich
  Fabrizio Gilardi, University of Zurich
  Uwe Serdült, Center for Democracy, Aarau

MODERATOR
  Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
David Basin, ETH Zurich
Srdjan Capkun, ETH Zurich
Eric Dubuis, BFH Bern
Bryan Ford, EPF Lausanne
Reto Koenig, BFH Bern
Philipp Locher, BFH Bern
Olivier Pereira, University of Leuven, Belgium
Vanessa Teague, Australia

SECURITY INDUSTRY
Stéphane Adamiste, SCRT
Sergio Alves Domingues, SCRT
Tobias Ellenberger, One Consult

COMPUTER SCIENTISTS
David-Olivier Jaquet-Chiffelle, University of Lausanne
Oscar Nierstrasz, University of Bern
Adrian Perrig, ETH Zurich
Carsten Schürmann, Denmark
Matthias Stürmer, University of Bern
Ulrich Ultes-Nitsche, University of Fribourg

POLITICAL SCIENTISTS
Florian Egloff, ETH Zurich
Fabrizio Gilardi, University of Zurich
Uwe Serdült, Center for Democracy, Aarau

MODERATOR
Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
The dialogue starts with a survey over 62 questions sent to 25 scientists.

Survey

2020.2

Covid-19 hits

When the on-site workshops were slowly taking shape, Switzerland entered a lockdown and the on-site gatherings had to be called off.

Online dialogue

2020.3

The workshops are replaced with a 12 weeks online dialogue on a dedicated gitlab platform.

2020.4

Additional research

Several separate research articles are commissioned with individual scientists to bring up more information on individual questions.

2020.7

Scientific report

The steering board publishes the 70 pages report with the recommendations of the scientists.

2020.11
Scientific report

Summary of the expert dialog
Redesign of Internet Voting Trials in Switzerland 2020

19th November 2020

Contents
1. Purpose .................................................................................................................. 4
2. Background ............................................................................................................ 4
3. Introductory Remarks ............................................................................................ 4
4. Block 1 - Effectiveness of Cryptography ................................................................. 4
   4.1 Overview ........................................................................................................... 4
   4.2 Summarize of the answers to the related questions of the questionnaire ....... 5
   4.3 Introduction to Block 1 on the platform ......................................................... 6
   4.4 Questions and summaries of the discussions on the platform ....................... 6
5. Block 2 - Diversity to support security and trust building ..................................... 9
   5.1 Overview ........................................................................................................... 9
   5.2 Summarize of the answers to the related questions of the questionnaire ...... 9
   5.3 Introduction to Block 2 on the platform ......................................................... 11
   5.4 Questions and summaries of the discussions on the platform ....................... 11
6. Block 3 - Printing Offices (Finally to support security and trust building - Part 2) .... 20
   6.1 Overview ........................................................................................................... 20
   6.2 Summarize of the answers to the related questions of the questionnaire ...... 20
   6.3 Introduction to Block 3 on the platform ......................................................... 21
   6.4 Questions and summaries of the discussions on the platform ....................... 21
7. Block 4 - Public Bulletin Board ............................................................................... 25
   7.1 Overview ........................................................................................................... 25
   7.2 Summarize of the answers to the related questions of the questionnaire ...... 25
   7.3 Introduction to Block 4 on the platform ......................................................... 25
   7.4 Questions and summaries of the discussions on the platform ....................... 25
8. Block 5 - Sealed ballots Mandated by Government .............................................. 31
   8.1 Overview ........................................................................................................... 31
   8.2 Summarize of the answers to the related questions of the questionnaire ...... 31
   8.3 Introduction to Block 5 on the platform ......................................................... 33
   8.4 Questions and summaries of the discussions on the platform ....................... 33
9. Block 6 - Development and Publication ............................................................... 37
   9.1 Overview ........................................................................................................... 37
   9.2 Summarize of the answers to the related questions of the questionnaire ...... 37
   9.3 Introduction to Block 6 on the platform ......................................................... 40
   9.4 Questions and summaries of the discussions on the platform ....................... 40
10. Block 7 - Public Incentive Test and Bug Bounty ................................................. 43

Key Recommendations of Dialogue
Key Recommendations of Dialogue

- Strict hierarchy of specifications
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
- Maximum level of transparency, namely in development
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
- Maximum level of transparency, namely in development
- Voting security beyond internet voting
Summary

- Switzerland is a useful test bed for online voting
- Iterative process with strict supervision on federal level
- Expert dialogue with recommendations in 2020

Contact

Christian Folini

christian.folini@netnea.com

@ChrFolini

Download English version of report from