Scytl
Innovating Democracy

Defining a national framework for online voting and meeting its requirements: the Swiss experience

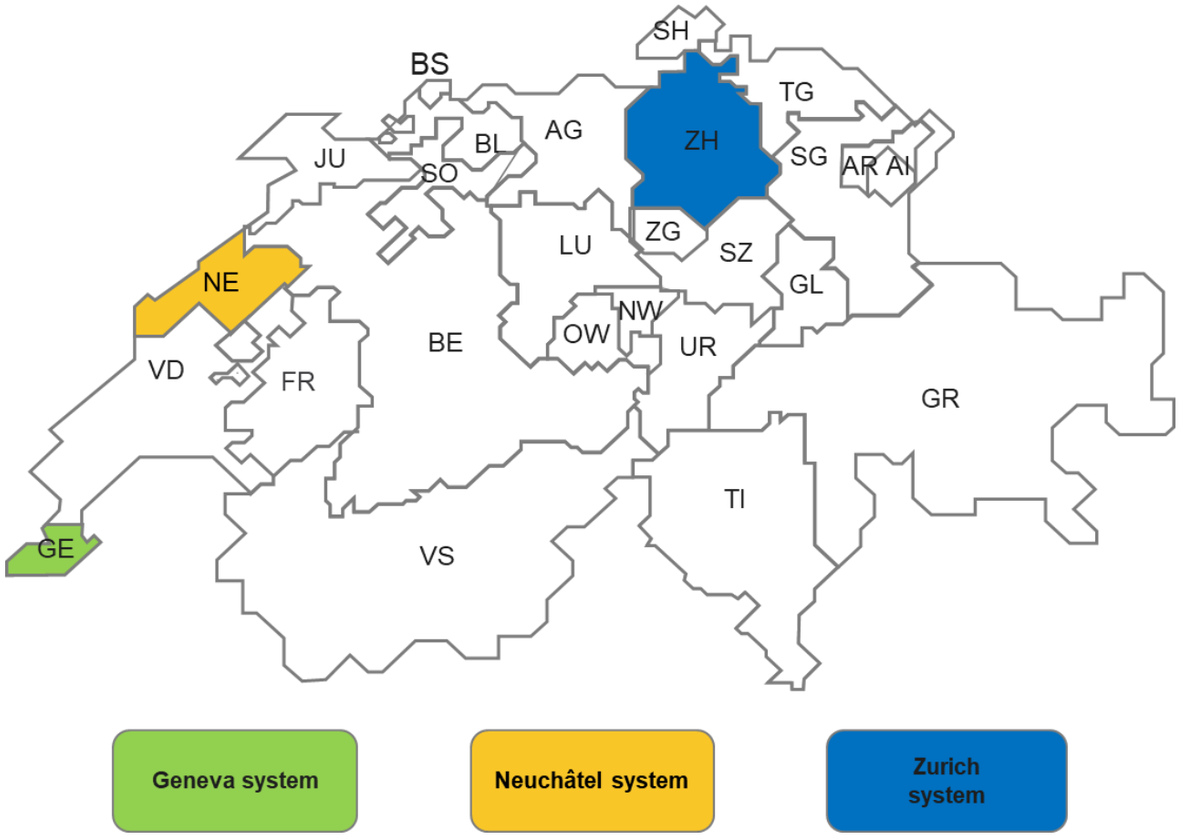
E-VOTE-ID 2018: Third International Joint Conference on Electronic Voting

Wednesday, 3 October 2018 (Bregenz, Austria)

Jordi Puiggalí and Adrià Rodríguez-Pérez
Research and Security, Scytl Secure Electronic Voting, S.A.
jordi.puiggali@Scytl.com

Background
First trials

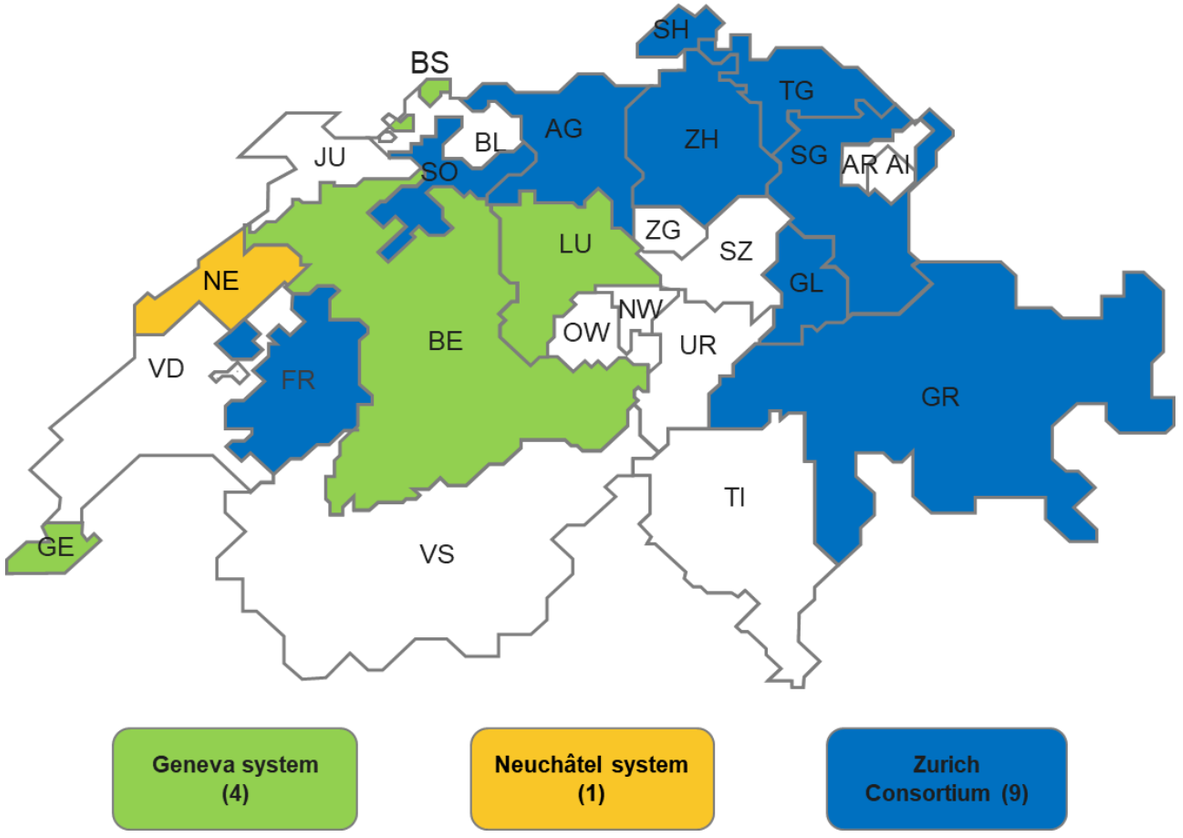
- A tradition of direct democracy (Landsgemeinde)
- Country's federalism: elections is a subnational matter (Driza Maurer, 2016)
- One of the first countries introducing internet voting (Pratchett and Wingfeld; 2004; Solop, 2004)
  - 1970's: postal voting (1990's generalised)
  - 1998: Federal Council proposes to study internet voting
  - 2000: Swiss Parliament asks Federal Council for starting i-voting program
  - 2002: starts pilots in Geneva (2003); Neuchâtel and Zurich (2005)



Scytl
Innovating Democracy

Background
Extending to all Cantons

- In 2006, the Federal Government opened the door for all cantons to use internet voting; with limitations:
  - 20% of the cantonal electorate (later extended to 30%);
  - 10% of the Swiss electoral roll
- Geneva and Zurich (Consortium) started offering their system to other cantons
- Some drawbacks were also experienced:
  - Geneva (2005 – 2007) regulation problems
  - Zurich (2011 – now) technical problems



Scytl
Innovating Democracy

The new regulation of 2014

Ordinance of Electronic voting - VEleS

- In 2011, the Federal Council set up a task force to study the security issues of internet voting

- New regulation for internet voting at the Federal level is set up in 2013:
  - Amendment to the Ordinance of Political Rights of 24 May 1978 (OPR)
  - Ordinance on Electronic voting (VEleS) by the Federal Chancellery

- Two main novelties as of 2014:
  - Limits for the use of internet voting by the Cantons
  - Authorisation and certification processes

Scytl
Innovating Democracy

The new regulation of 2014
Three authorization levels

Level	Limit(1)	Requirements	Certification
1	30% cantonal 10% Swiss	Functional and security • BSI Common Criteria PP for Internet Voting Products • Council of Europe standards	• None, only ChF experts revisions of documentation (risk assessment, security architecture…) and security tests of system (functional and infrastucture)
2	50% cantonal 30% Swiss	Individual verifiability • Cast-as-intended verifiability • Recorded-as-cast verifiability	• Security: Common Criteria EAL 2 • Cryptography: Security and formal proofs (printing, server and tally are trusted) • Infrastructure and printing offices
3	No limit	Complete verifiability • Individual verifiability • Counted-as-recorded verifiability • Control components (2 or 4)	• Security: Common Criteria EAL 2 + EAL 4 (control components) • Cryptography: Security and formal proofs (printing and one control component are trusted) • Infrastructure and printing offices

(1) According to Art. 27f.2 OPR, expatriate Swiss citizens who are eligible to vote are not included in these limits

Scytl
Innovating Democracy

The new regulation of 2014
Authorization requirements

- Authorisation process:
  1. Trials require an initial license from the Federal Council (art. 17a.1 OPR)
  2. Five successive problem-free individual trials in Federal ballots → federal popular votes for 2 years (Art. 27a.3 OPR)
  3. Federal Chancellery authorisation request prior to every voting process (Art. 27e.1 OPR)

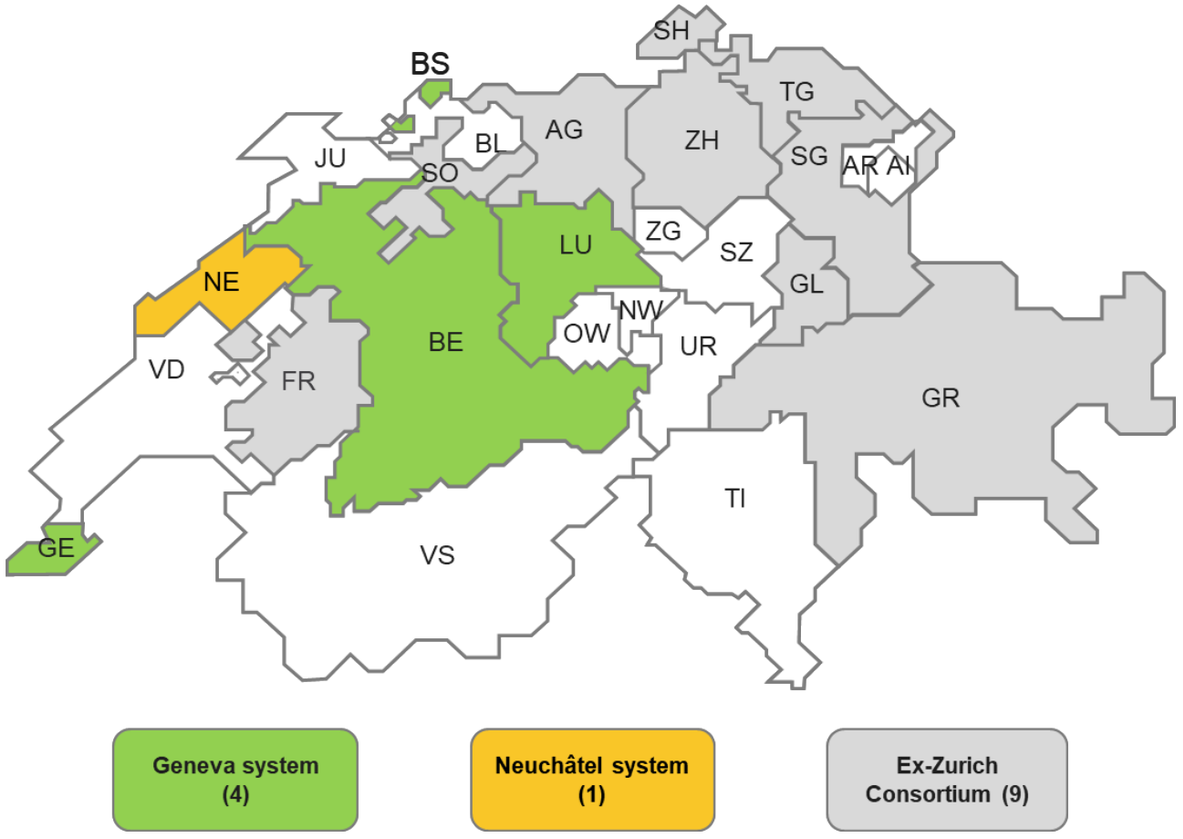
- Participants (Art. 27l.1 OPR):
  - For level 1: *groups d'accompagnement* (four different cantons using a different system) (Art. 511 of the Catalogue)
  - For levels 2 and 3(1): specialised institutions or certification agencies (Annex 5 to the VEleS)
  - At any level: Academic support (Art. 27o2 OPR)

(1) And as of July 2018, for all Cantons using a system providing complete verifiability

Swiss internet voting authorisation in practice

Impact of new ordinance

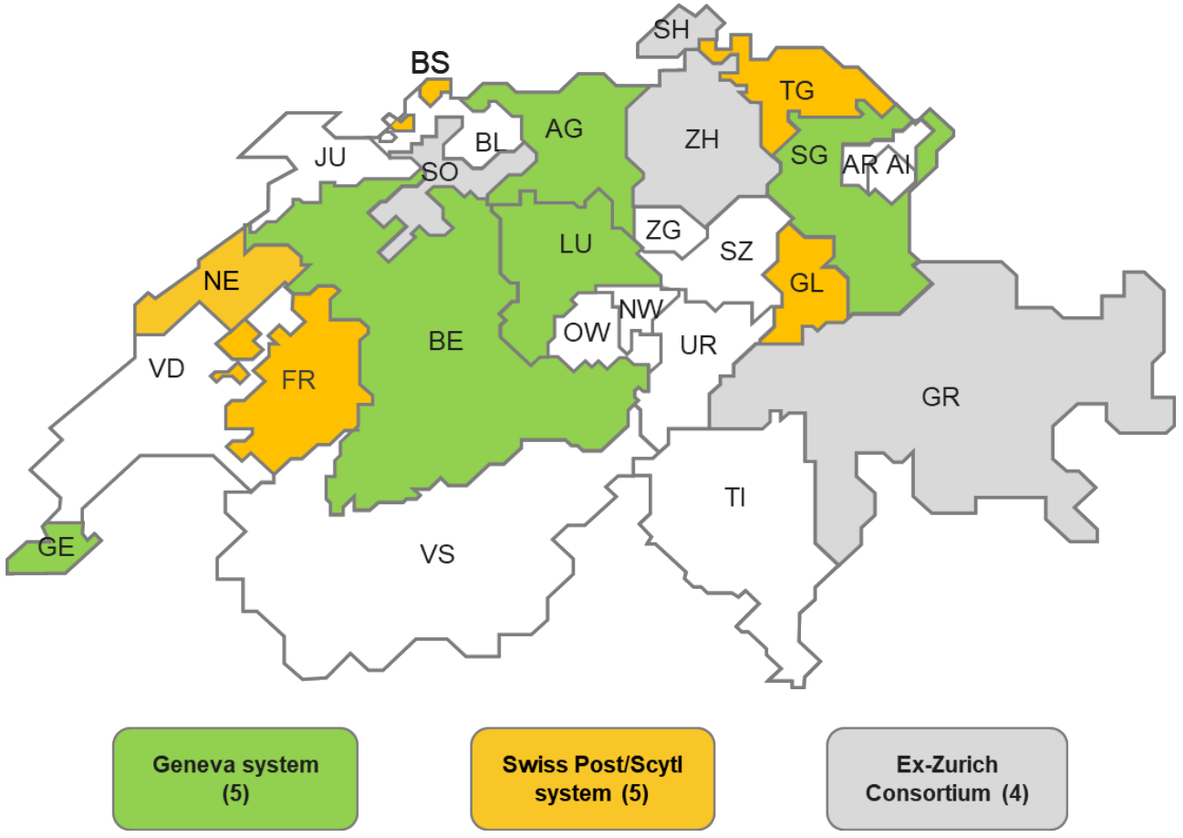
- After the new regulation: level 1 authorisation seek by all existing solutions
  - Neuchâtel was authorised at level 1
  - Geneva upgraded their system and was also authorised at level 1
  - The Consortium upgraded their system but were not authorised (9 cantons were left without voting system)



Swiss internet voting authorisation in practice

New player: Swiss Post

- In 2015, Swiss Post makes a partnership with Scytl and starts offering their solution to cantons
  - Geneva: Aargau (2017), St. Gallen (2017)
  - Swiss Post: Fribourg (2016) + Neuchâtel (2017), Thurgau (2018), Basel Stadt (2019), Glarus (2019)



Swiss internet voting authorisation in practice

Level 2 authorisation: the first certified voting system

- In 2016, KPMG becomes VEleS certification authority

- In 2016, Swiss Posts starts authorisation process for level 2 – achieved in 2017
  - Individual verifiability based on Neuchâtel's return codes: security and symbolic proofs (including with the participation of ETH Zurich)
  - Common Criteria framework for certifying the solution at EAL2 with the BSI Protection Profile
  - System architecture and security controls in compliance with ISO 27001

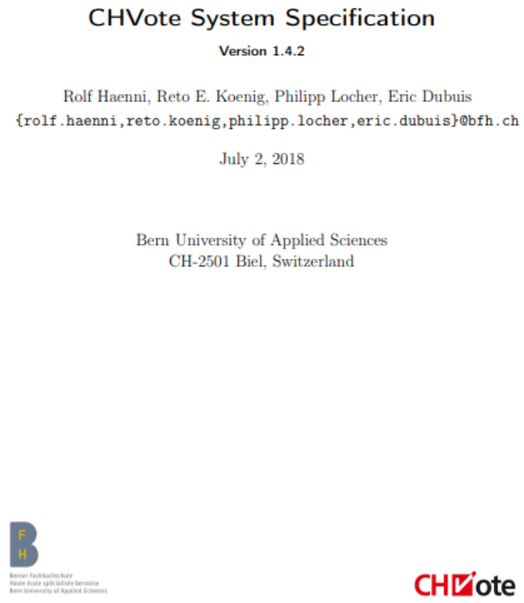
- Swiss Post's is the only solution certified at level 2 → currently working on the authorisation at this level for Thurgau Canton

Swiss internet voting authorisation in practice

Level 3 authorisation: objective 2019 elections

- Since 2016, Geneva is working on certification at level 3
  - Collaboration agreement with Bern University of Applied Sciences (BfH) for the design of a new voting system
  - Proof of concept implemented in 2017
  - Authorisation is expected for the next federal elections (2019)

- Swiss Post is also working on achieving certification at level 3 for the next federal elections (2019)



CHVote System Specification

Version 1.4.2

Rolf Haenni, Reto E. Koenig, Philipp Locher, Eric Dubuis

{rolf.haenni,reto.koenig,philipp.locher,eric.dubuis}@bfh.ch

July 2, 2018

Bern University of Applied Sciences
CH-2501 Biel, Switzerland

Scytl
Innovating Democracy

Future Plans

- In August 2017, Federal Council stablished a group of experts on internet

- Recommendations by the expert group (April 2018):
  - Authorisation process: simplification with a unique mechanism (with authorisation by the Federal Council) and clarifying the distinction between authorisation and certification + *groups d'acompagnement* should not be compulsory
  - Publication of the source code for those solutions providing complete verifiability and public intrusion test, as amended in July 2018 (Art. 7a and 7b VEleS)
  - Dematerialisation: move towards paper-saving electronic voting (only voting cards are printed) and conduct pilots for full dematerialisation of voting

Scytl
Innovating Democracy

Conclusions

- Gradual steps in the introduction of internet voting allow for identifying and mitigating the impact of risks;
- Evaluation processes and requirement definitions should rely on security experts and election management bodies;
- Clear frameworks to evaluate and certify the security of online voting solutions work better than designing specific closed voting solutions;
- Legal and technical requirements should be reviewed often – to cope with evolving technology, security and auditability

Innovating Democracy