The Adventurous Tale of Online Voting in Switzerland

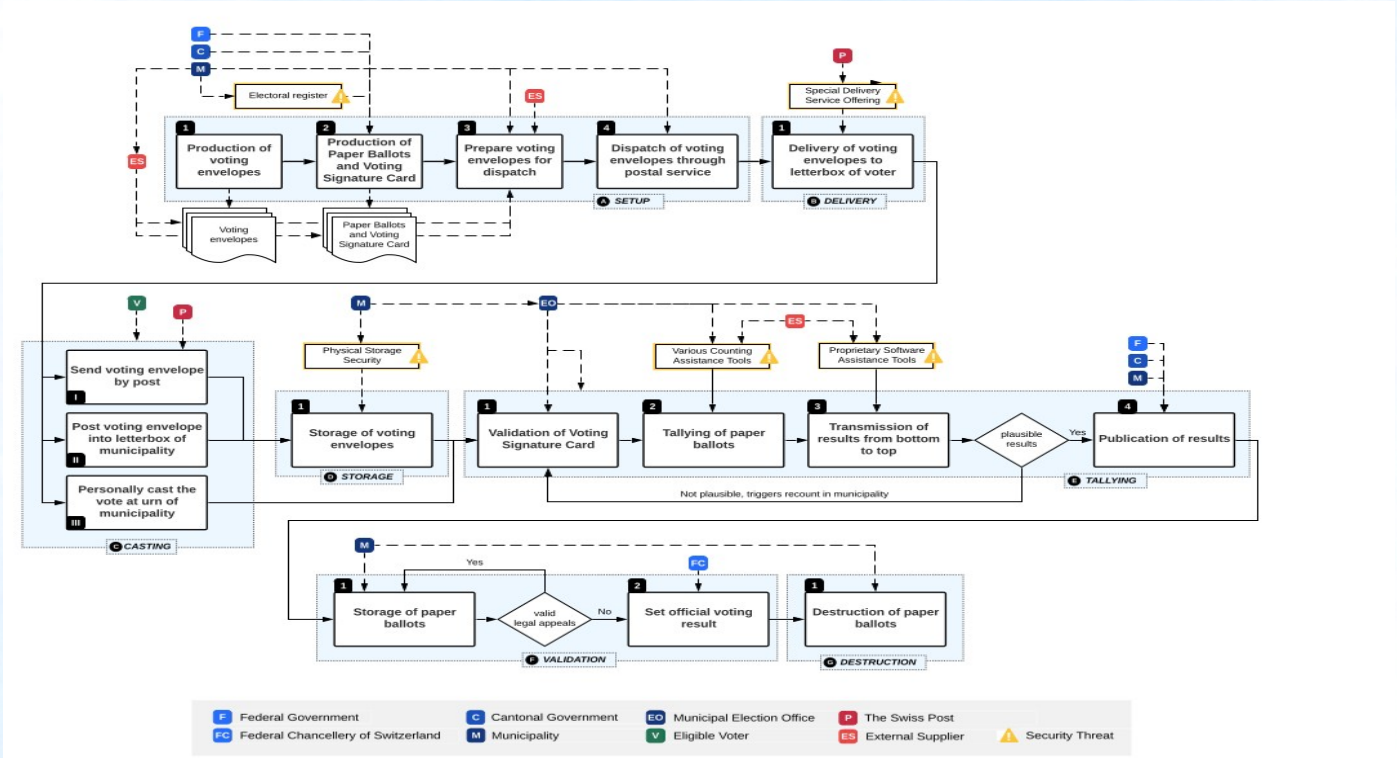
Christian Folini / @ChrFolini

OWASP BE - 2021-03-18

Voting in Switzerland

Photo: Gian Ehrensberger

Process Around Swiss Mail-in Ballots



Killer / Stiller : The Swiss Postal Voting Process and its System and Security Analysis

Typical Swiss Election Ballot

KANTON AARGAU

Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020

Bezirk Muri

Wahlzettel-Nr.

06	glp – Grünliberale Partei	
06.01	**Budmiger Hans-Peter (Hampi),** 1976, Unternehmer, Gemeindepräsident, Muri	1
~~06.02~~ 06.01	~~**Langenbacher Knüsel Silvia,** 1966, Unternehmerin, Abtwil~~ Budmiger Hans-Peter	2
06.03	**Peyer Samuel,** 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3
~~06.04~~ 06.05	~~**Masoch Loredana,** 1996, BLaw, Masterstudentin Rechtswissenschaften, Waltenschwil~~ Stöckli Cornel	4
06.05	**Stöckli Cornel,** 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri	5
~~06.06~~ 06.01	~~**Chande Sabrina,** 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil~~ Bucher Ralf, CVP	6
06.07	**Weber Thomas,** 1974, Content Manager, Journalist, Buttwil	7

Vom Wahlbüro auszufüllen →	Kandidatenstimmen:	Zusatzstimmen:	Total:

Typical Swiss Election Ballot

KANTON AARGAU

Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020

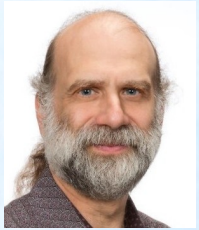
Bezirk Muri

Wahlzettel-Nr.

06	glp – Grünliberale Partei	
06.01	**Budmiger Hans-Peter (Hampi),** 1976, Unternehmer, Gemeindepräsident, Muri	1
~~06.02~~ 06.01	~~**Langenbacher Knüsel Silvia,** 1966, Unternehmerin, Abtwil~~ Budmiger Hans-Peter	2
06.03	**Peyer Samuel,** 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3
~~06.04~~ 06.05	~~**Masoch Loredana,** 1996, BLaw, Masterstudentin Rechtswissenschaften, Waltenschwil~~ Stöckli Cornel	4
06.05	**Stöckli Cornel,** 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri	5
~~06.06~~ 06.01	~~**Chande Sabrina,** 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil~~ Bucher Ralf, CVP	6
06.07	**Weber Thomas,** 1974, Content Manager, Journalist, Buttwil	7

Vom Wahlbüro auszufüllen →	Kandidatenstimmen:	Zusatzstimmen:	Total:

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

Graphic: Wikipedia

Timeline

2000 — 1st project

1st Swiss internet voting pro-ject is launched with three pilot cantons.

2004 — 1st Geneva trial

Canton Geneva runs the first Swiss internet voting trial.

2008 — Entering Scytl

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

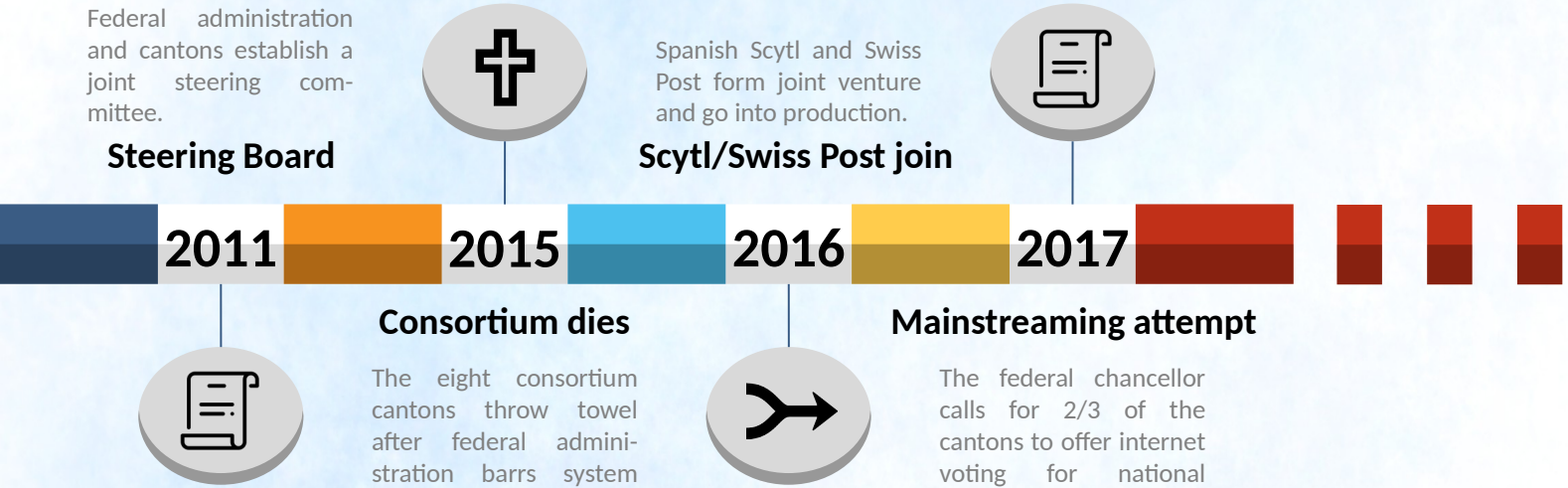
2009 — Consortium

Eight Swiss cantons form a consortium and com-mission Unisys with the creation of an internet voting system.

2011 — Steering Board

Federal administration and cantons establish a joint steering com-mittee.

Timeline

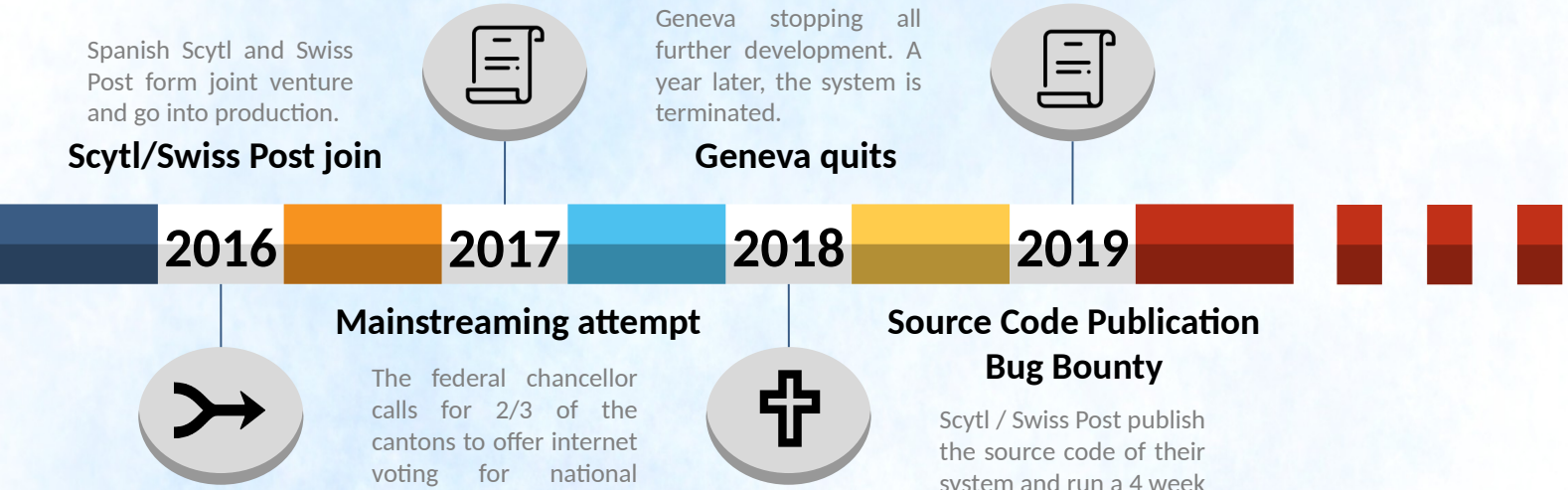

2011
2015
2016
2017
Steering Board
Federal administration and cantons establish a joint steering committee.
Consortium dies
The eight consortium cantons throw towel after federal administration barrs system from use in national elections.
Scytl/Swiss Post join
Spanish Scytl and Swiss Post form joint venture and go into production.
Mainstreaming attempt
The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.

Geneva Quits

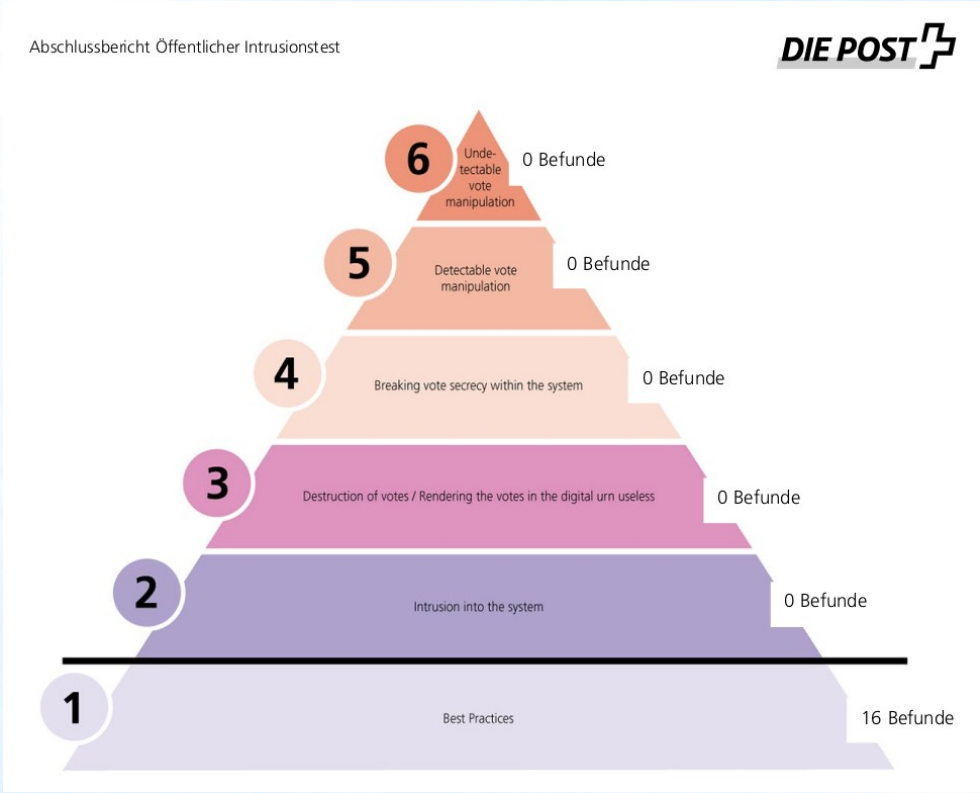
2018: Development stopped
2019: System terminated

Source: Twitter: @GE_chancellerie (1141332323025195009)

Timeline


Spanish Scytl and Swiss Post form joint venture and go into production.
Scytl/Swiss Post join
Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.
Geneva quits
2016
2017
2018
2019
Mainstreaming attempt
The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.
Source Code Publication
Bug Bounty
Scytl / Swiss Post publish the source code of their system and run a 4 week bug bounty

Swiss Post Bug Bounty: We got this!



[BEST PRACTICES] Incorrect 'HTTP-Strict-Transport-Security' header on 'pit-admin.evoting-test.ch'

REDMINE ID: #188
SUBMISSION: Feb. 25th 2019, 23:19 (GMT+1)
RESEARCHER(S): Jacob.Rees-Earcher
COMPENSATION: CHF 200.-

When connecting to 'pit-admin.evoting-test.ch' on port 443, the server sends an HTTP-Strict-Transport-Security header even for plaintext HTTP connections, which is a violation of RFC 6797. The additional header also does not contain the 'includeSubdomain' directive, which would be a security best-practice.

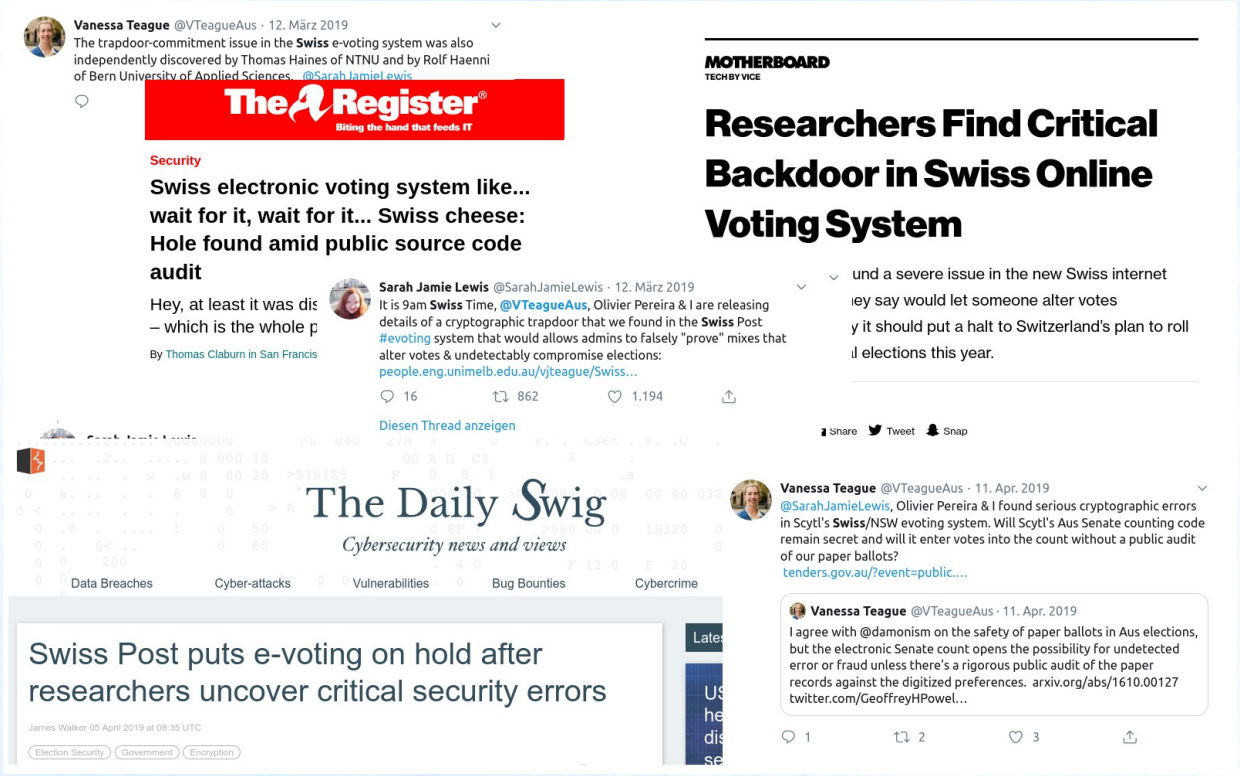
[BEST PRACTICES] Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy

[BEST PRACTICES] Multiple occurrences of 'X-XSS-Protection' HTTP header

REDMINE ID: #234
SUBMISSION: Feb. 28th 2019, 14:57 (GMT+1)
RESEARCHER(S): pitbull
COMPENSATION: CHF 100.-

Some error messages sent as responses by the web server (specifically, the '403 Forbidden' status code) include two identical occurrences of the 'X-XSS-Protection' security header. This behavior is non-standard, and could lead to undefined behavior in some browsers.

Swiss Post / Scytl Source Code: Not so good



Vanessa Teague @VTeagueAus · 12. März 2019
The trapdoor-commitment issue in the **Swiss** e-voting system was also independently discovered by Thomas Haines of NTNU and by Rolf Haenni of Bern University of Applied Sciences. @Sarah JamieLewis

The Register®
Biting the hand that feeds IT

Security

Swiss electronic voting system like... wait for it, wait for it... Swiss cheese: Hole found amid public source code audit

Hey, at least it was dis
– which is the whole p

By Thomas Claburn in San Francis

Sarah Jamie Lewis @SarahJamieLewis · 12. März 2019
It is 9am **Swiss** Time, **@VTeagueAus**, Olivier Pereira & I are releasing details of a cryptographic trapdoor that we found in the **Swiss** Post #evoting system that would allows admins to falsely "prove" mixes that alter votes & undetectably compromise elections:
people.eng.unimelb.edu.au/vjteague/Swiss...

16 862 1.194

Diesen Thread anzeigen

MOTHERBOARD
TECH BY VICE

Researchers Find Critical Backdoor in Swiss Online Voting System

und a severe issue in the new Swiss internet
ıey say would let someone alter votes
y it should put a halt to Switzerland's plan to roll
ıl elections this year.

Share Tweet Snap

The Daily Swig
Cybersecurity news and views

Data Breaches Cyber-attacks Vulnerabilities Bug Bounties Cybercrime

Vanessa Teague @VTeagueAus · 11. Apr. 2019
@SarahJamieLewis, Olivier Pereira & I found serious cryptographic errors in Scytl's **Swiss**/NSW evoting system. Will Scytl's Aus Senate counting code remain secret and will it enter votes into the count without a public audit of our paper ballots?
tenders.gov.au/?event=public....

Vanessa Teague @VTeagueAus · 11. Apr. 2019
I agree with @damonism 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
twitter.com/GeoffreyHPowel...

1 2 3

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

James Walker 05 April 2019 at 08:35 UTC

Election Security Government Encryption

to be continued ...

Timeline

Scytl/Swiss Post join

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

Mainstreaming attempt

The federal chancellor calls on 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. Researchers identify three critical vulnerabilities within weeks. The system is put on hold.

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

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
- 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
- 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

Timeline

2020.2 — Survey

The dialogue starts with a survey over 62 questions sent to 25 scientists

2020.3 — 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.

2020.4 — Online dialogue

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

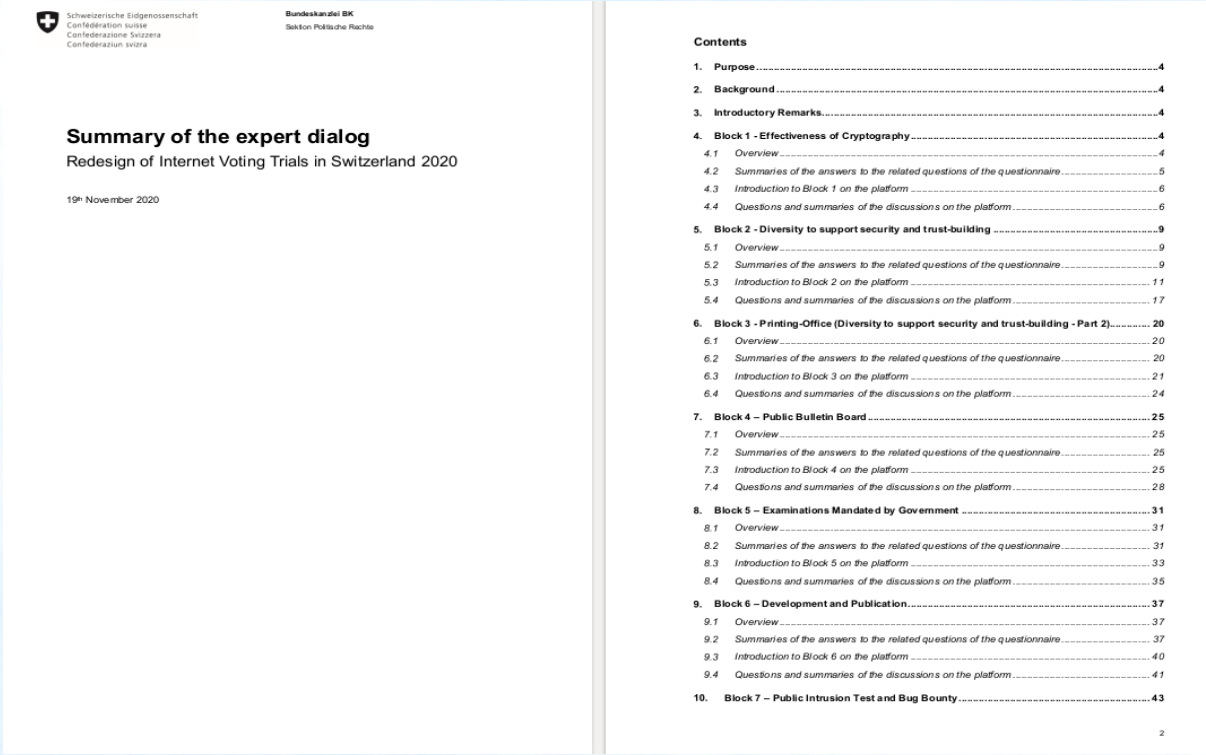
2020.7 — Additional research

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

2020.11 — Scientific report

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

Scientific report



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Summary of the expert dialog

Redesign of Internet Voting Trials in Switzerland 2020

19th November 2020

Contents

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

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

Download English version of report from
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

Contact

Christian Folini

christian.folini@netnea.com

@ChrFolini

Download English version of report from
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html