



# The Adventurous Tale of Online Voting in Switzerland

---

**Christian Folini / @ChrFolini**

**USENIX Enigma 2021**

# Voting in Switzerland

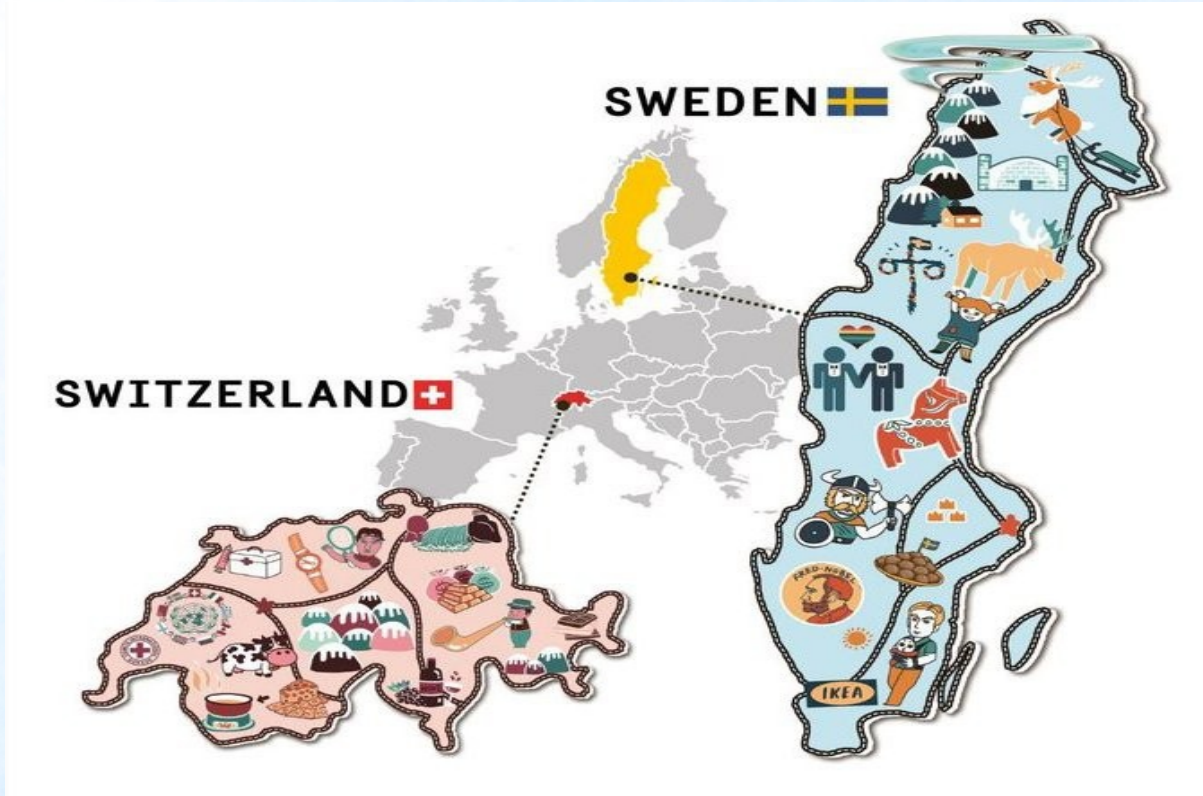


*Photo: Gian Ehrensberger*

# #Swederland – don't get this wrong



ENIGMA

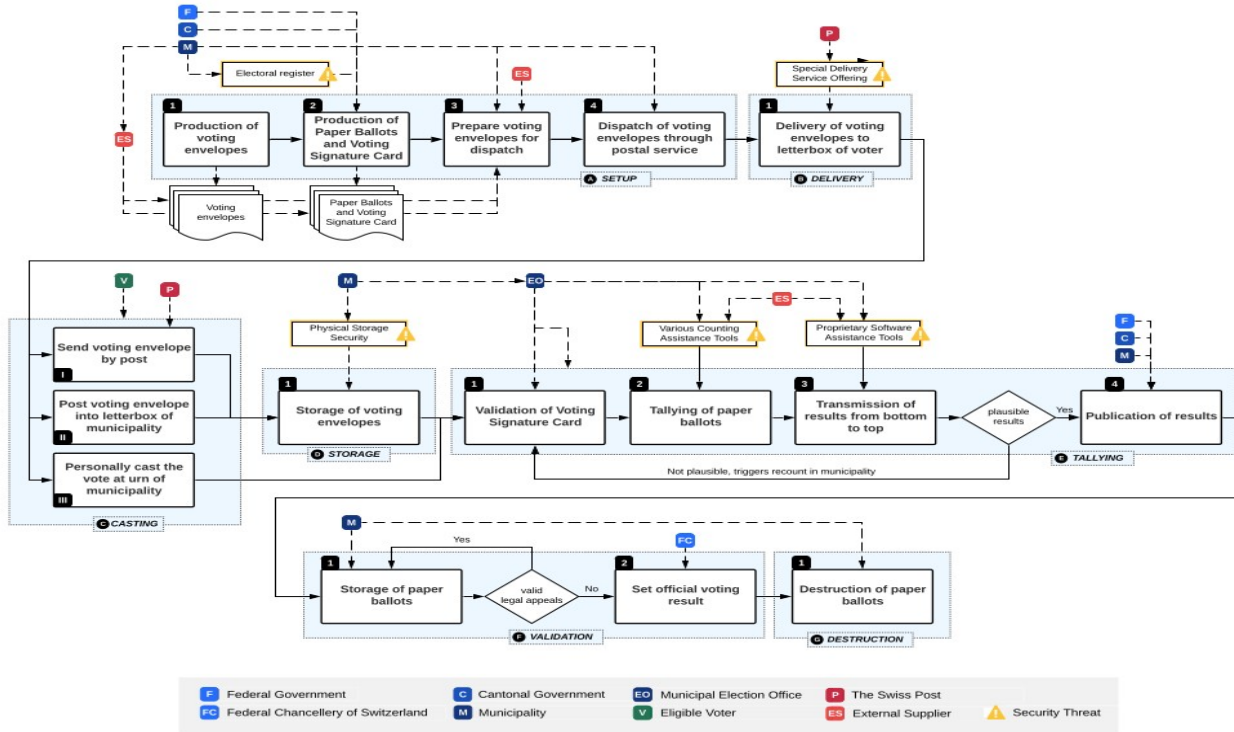


Graphic: Swedish Embassy in Teheran

# Process Around Swiss Mail-in Ballots





ENIGMA



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

# Typical Swiss Election Ballot



 **KANTON AARGAU**  **Bezirk Muri**

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



Wahizettel-Nr. \_\_\_\_\_

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

Vom Wahlbüro auszufüllen →	Kandidatenstimmen:	Zusatzstimmen:	Total:

# Typical Swiss Election Ballot



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

Wahzettel-Nr. \_\_\_\_\_

06	glp – Grünliberale Partei	
06.01	Budmiger Hans-Peter (Hampi), 1976, Unternehmer, Gemeindepräsident, Muri	1
<del>06.02</del>	<del>Langenbacher Knüsel Silvia, 1966, Unternehmerin, Abtwil</del>	<del>2</del>
06.01	Budmiger Hans-Peter	2
06.03	Peyer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3
<del>06.04</del>	<del>Masoch Loredana, 1996, BLaw, Masterstudentin Rechtswissenschaften, Waltenschwil</del>	<del>4</del>
06.05	Stöckli Cornel, 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri	5
<del>06.06</del>	<del>Chande Sabrina, 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil</del>	<del>6</del>
06.01	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

---



ENIGMA



*Graphic: Wikipedia*

# The Cantons of Switzerland



ENIGMA



Delaware

Graphic: Wikipedia

# Timeline



1st Swiss internet voting project is launched with three pilot cantons.

## 1st project

2000



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

## Entering ScytI

2008



Federal administration and cantons establish a joint steering committee.

## Steering Board

2011



## 1st Geneva trial

Canton Geneva runs the first Swiss internet voting trial.



## Consortium

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



# Timeline



Federal administration and cantons establish a joint steering committee.

## Steering Board



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

## ScytI/Swiss Post join



2011

2015

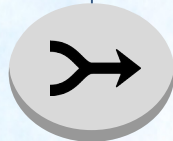
2016

2017



## 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.



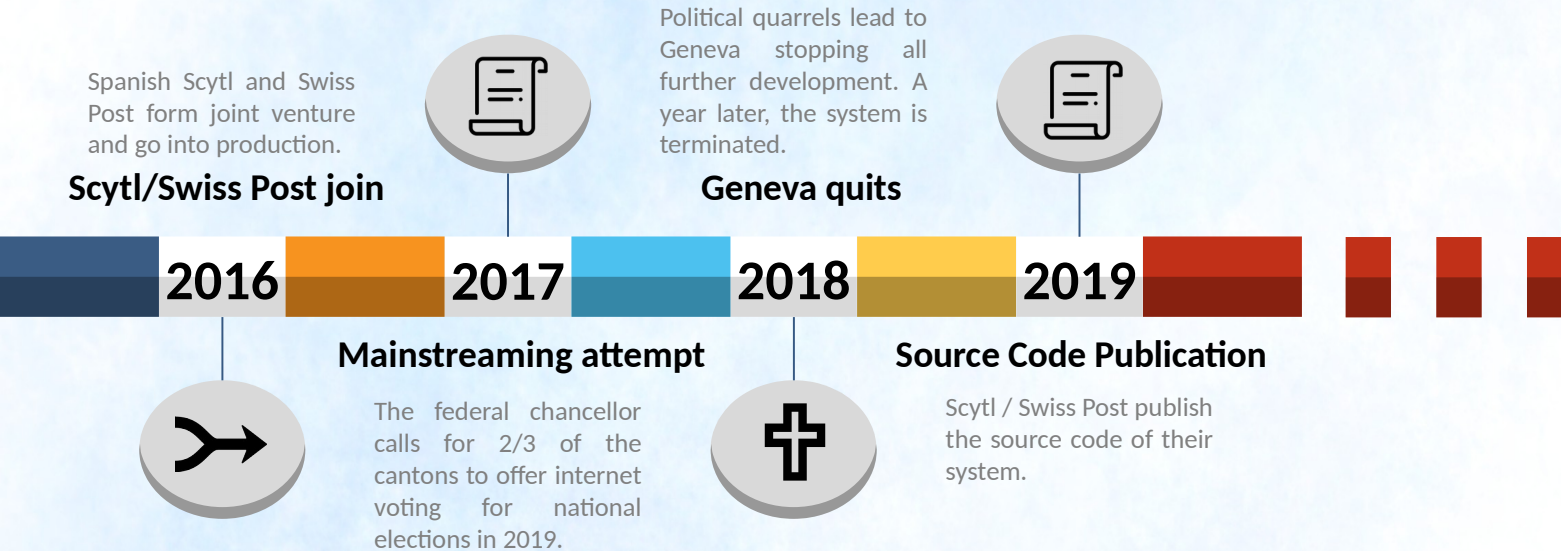
# Geneva Quits



*2018: Development stopped  
2019: System terminated*

Source: Twitter: @GE\_chancellerie (1141332323025195009)

# Timeline



# Swiss Post is Being Quit (for the moment)



ENIGMA

**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. [@SarahJamieLewis](#)



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 discovered – which is the whole point  
By Thomas Claburn in San Francisco

**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 allow admins to falsely "prove" mixes that alter votes & undetectably compromise elections: [people.eng.unimelb.edu.au/vjteague/Swiss...](http://people.eng.unimelb.edu.au/vjteague/Swiss...)

16 replies 862 retweets 1,194 likes

Diesen Thread anzeigen

MOTHERBOARD  
TECH BY VICE

## Researchers Find Critical Backdoor in Swiss Online Voting System

... and a severe issue in the new Swiss internet key they say would let someone alter votes ... it should put a halt to Switzerland's plan to roll out elections this year.

Share Tweet Snap

**Vanessa Teague** @VTeagueAus · 11. Apr. 2019  
[@SarahJamieLewis](#), Olivier Pereira & I found serious cryptographic errors in Scyt's Swiss/NSW e-voting system. Will Scyt'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...](https://tenders.gov.au/?event=public...)

**Vanessa Teague** @VTeagueAus · 11. Apr. 2019  
I agree with @demonism 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](https://arxiv.org/abs/1610.00127) [twitter.com/GeoffreyHPowel...](https://twitter.com/GeoffreyHPowel...)

1 reply 2 retweets 3 likes

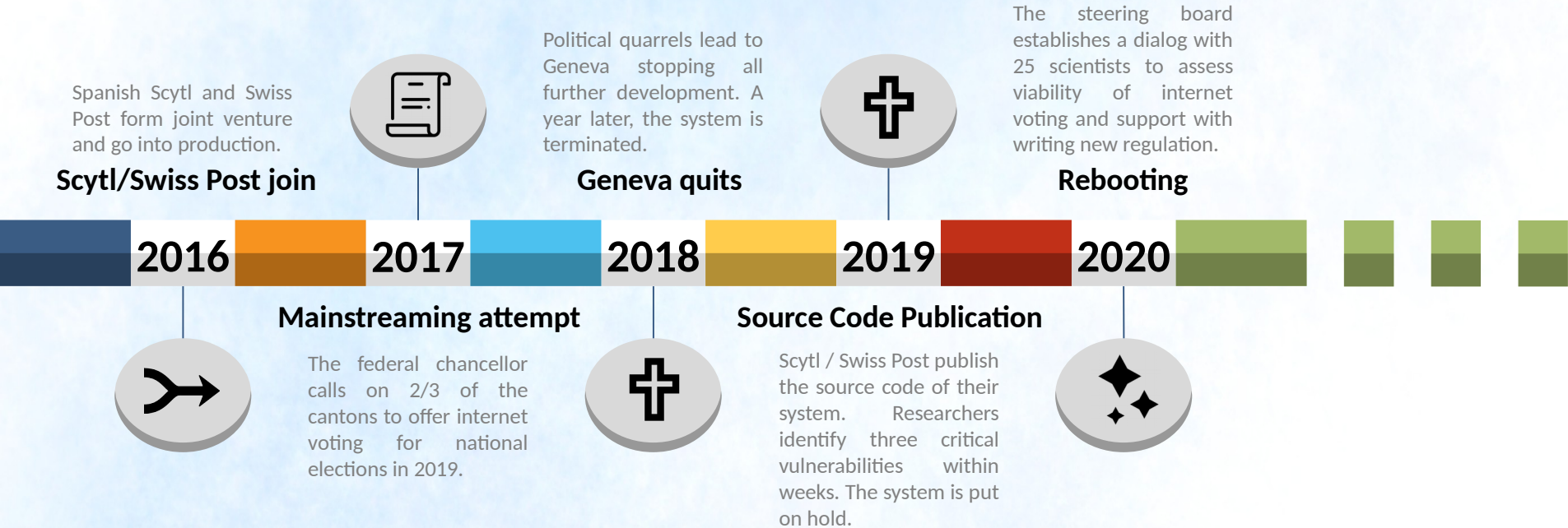
## Swiss Post puts e-voting on hold after researchers uncover critical security errors

James Walker 05 April 2019 at 08:35 UTC

Election Security Government Encryption

to be continued ...

# Timeline



# Expert Dialogue – Participating Scientists



ENIGMA

## 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

# Expert Dialogue – Participating Scientists



ENIGMA

## 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

# Expert Dialogue – Participating Scientists



ENIGMA

## 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

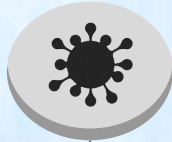
# Timeline



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

## Survey

2020.2



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.

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

## Online dialogue

2020.4



2020.7

## Additional research

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

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

## Scientific report

2020.11





# 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

19<sup>th</sup> 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 Summaries 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 Summaries 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.....	17
6. Block 3 - Printing-Office (Diversity to support security and trust-building - Part 2).....	20
6.1 Overview.....	20
6.2 Summaries 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.....	24
7. Block 4 - Public Bulletin Board.....	25
7.1 Overview.....	25
7.2 Summaries 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.....	28
8. Block 5 - Examinations Mandated by Government.....	31
8.1 Overview.....	31
8.2 Summaries 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.....	35
9. Block 6 - Development and Publication.....	37
9.1 Overview.....	37
9.2 Summaries 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.....	41
10. Block 7 - Public Intrusion 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

*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>*