Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

August 2019

Vote électronique – Public Intrusion Test 2019

Final report of the steering committee

System tested: Fully verifiable system developed by Swiss Post (Version of February 2019)

Table of contents

1 Purpose

This report presents a summary of the organisational structure, procedure and conclusions drawn from the 2019 public intrusion test (PIT) on the electronic voting system developed by Swiss Post.

2 Background

The cantons have been conducting e-voting trials since 2004 as part of the Vote électronique project conducted by the federal government and the cantons based on Art. 8*a* of the Federal Act on Political Rights (BPR, SR 161.1). The conditions for conducting these trials are set out under federal law in the Political Rights Ordinance 161.11) and the Federal Chancellery Ordinance on Electronic Voting (OEV, SR 161.116).

In total, 15 cantons have allowed a share of their electorate to vote via internet in federal ballots on multiple occasions. Since 2015, the systems in use have offered the feature of individual verifiability. However, in order for electronic voting to be used on a wider scale the systems in use must be able to offer full verifiability. Before such a system can be used for the first time, the Electronic Voting Ordinance requires that the systems first be certified and that the source code be disclosed.

In April 2017, the Confederation and the cantons decided to subject the fully verifiable e-voting systems to a pilot public intrusion test. An intrusion test involves assessing the security of a system by subjecting it to attacks. The OEV demands that an intrusion test be conducted by an accredited body as part of the certification process. In the case of a public intrusion test, interested parties from around the world can also take part in testing the system.

Conducting a public intrusion test serves a number of purposes. The feedback from participants can lead directly to improvements in security. It also enables independent experts to build on their knowledge and expertise in the field of electronic voting. In the long term, this can reduce dependency on individual persons and organisations and can also contribute to the public debate. In addition, public intrusion tests can serve as an instrument of transparency and help to establish public confidence. In order for a public intrusion test to be successful, there needs to be active involvement on the part of the largest possible number of competent people. Furthermore, public debate (in the media and in political circles) surrounding public intrusion testing reveals how mistakes are perceived and assessed in the context of e-voting.

3 System tested

In recent years, two different electronic voting systems have been in use in Switzerland, both offering individual verifiability: a system offered by Swiss Post (last used in the cantons of Fribourg, Neuchâtel, Thurgau and Basel-Stadt) and a system developed by the Canton of Geneva (last used by the cantons of Bern, Lucerne, St. Gallen[1], Aargau, Vaud and Geneva).

On 28 November 2018, the Genevan authorities announced that would only continue to operate their system until February 2020 at the latest. Work towards developing the system to be fully verifiable was consequently discontinued. There was therefore no need to conduct a public intrusion test on that system.

The PIT was only conducted on the fully verifiable system developed by Swiss Post. The version tested was the future system, and not the one currently in use. That system can only be used for federal votes once it has satisfied all of the requirements under federal law and subsequently been authorised by the authorities.

The system configuration of the PIT test system corresponded 1:1 with the planned productive system configuration. Only one aspect of the security configuration was deactivated, so as not to unnecessarily hinder those participating in the PIT (the exclusion of conspicuous IP addresses using Fail2Ban).

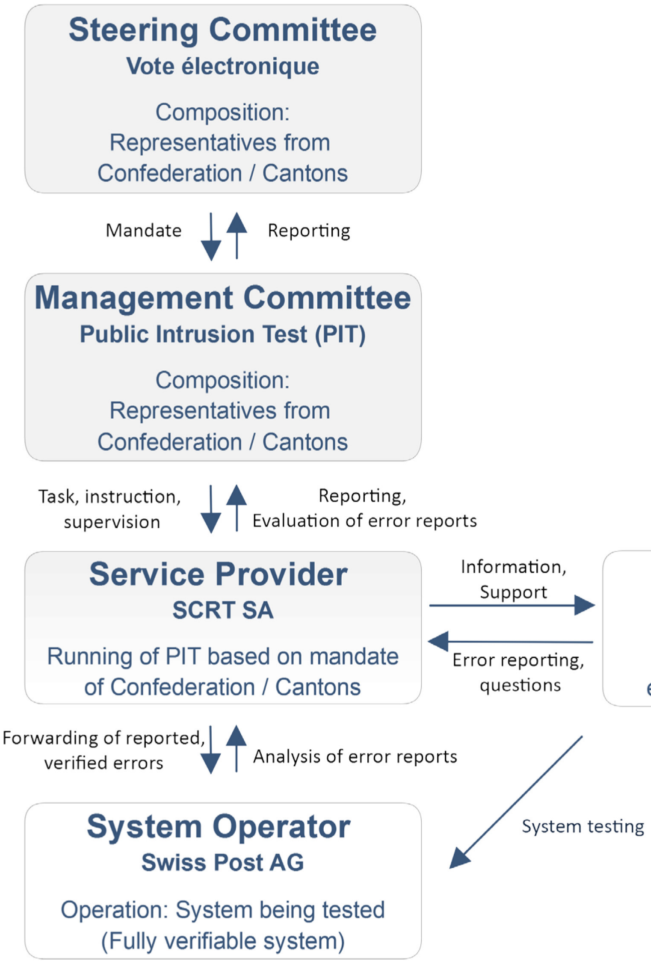
4 Test setup and organisation

The Confederation and the cantons took the decision to work together on the public intrusion test. They drew up common requirements for the system operator[2]. They also contributed the sum of CHF 250,000 towards the public intrusion test via the eGovernment Switzerland priority plan of the Confederation, cantons and communes. Of that amount, CHF 150,000 went to Swiss Post and CHF 100,000 to SCRT SA as a service provider to the Confederation and the cantons.

[1] The Canton of St. Gallen plans to use Swiss Post's system in future.

[2] https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf.download.pdf/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf

Organisation PIT



Swiss Post made the system available for the public intrusion test between 25 February and 24 March, and ensured its proper operation. In return for useful feedback, participants were eligible for a compensatory payment (CHF 100 up to a maximum of CHF 50,000 per feedback report; maximum total of CHF 150,000). The criteria for a compensatory payment were defined in advance and made available to test participants on a dedicated PIT website (PIT platform[3]).

The management committee (MC), composed of representatives from the Confederation and the cantons, supervised the public intrusion test on behalf of the Vote électronique steering committee (SC). It served the Confederation and the cantons as a point of contact for questions regarding the public intrusion test. During the test, the MC had the task of providing periodic updates on the state of test findings. It coordinated communication activities among the participating actors and drafted elements of official communications for the benefit of the public.

The Confederation and the cantons commissioned SCRT SA, a specialised company, to run the public intrusion test; it acted on the instruction of the MC. SCRT was responsible for communicating with test participants, it acquired, registered and supported them, and gathered and evaluated their feedback. It set up a PIT platform for that purpose.

[3] https://www.onlinevote-pit.ch/

People from all around the world were invited to take part in the PIT. On registering on the PIT platform, they were required to acknowledge and agree to abide by Swiss Post's code of conduct (agreement with Swiss Post). The code of conduct covered the scope of the test and the procedure to follow on discovering shortcomings.

The way in which the test was set up generated a certain amount of criticism.

- In accordance with the requirements set by the Confederation and cantons, Swiss Post limited the test to attacks on Swiss Post's e-voting infrastructure and drew up the code of conduct accordingly. Infrastructures belonging to the cantons, surrounding systems e.g. printing companies involved in preparation of voting material, and other Swiss Post services were off limits. Attacks intended to prevent voters from accessing the system (Distributed Denial-of-Service, DDoS attacks) were also out of scope. Also excluded from the test were attacks on voting platforms. That also applied to any attacks aimed at influencing actors via fake messages. For example, one strategy could be to encourage voters to deviate from the instructions on e-voting given by the authorities (social engineering). The Confederation and the cantons responded to the criticism (see section 5).

- The requirements defined by the Confederation and the cantons for the PIT require Swiss Post to disclose the system's source code prior to the test in accordance with the provisions of Art. 7*a* f. OES. The step was intended to give participants the opportunity to prepare for the test. In order for participants to be able to access the source code, they had to agree to a special set of terms and conditions. The criticism was directed at those terms and conditions, as well as the way in which the source code was presented. Critics highlighted inadmissible restrictions in the terms and conditions on examining, modifying, compiling and executing the source code, as well as on producing and publishing studies. These rights are granted under Art. 7b para. 4 OES. There were also allegations of a breach of Art. 7b para. 1 OES due to the poor legibility of the source code and inadequate accompanying documentation. The Federal Chancellery urged Swiss Post to review and adapt the conditions for releasing the source code.[4]

5 Procedure

On 7 February 2019, the Federal Chancellery and the cantons of Fribourg, Graubünden, Neuchâtel, St. Gallen and Thurgau issued a press release announcing the public intrusion test[5]. Interested parties were then able to register anonymously on the PIT platform. SCRT publicised the test in IT community circles via Twitter and other channels. Swiss Post duly granted access to the source code the same day.

To mark the start of the PIT, and in view of the considerable media interest, the Federal Chancellery invited journalists to a press briefing on 25 February 2019. Representatives from the Confederation, the cantons and Swiss Post handed out fact sheets and fielded questions[6]. The fact sheets explained the aims and scope of the PIT, thereby responding to the widespread

[4] https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-74307.html
[5] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73898.html
[6] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html

criticism surrounding the test conditions. Further explanations were provided in the form of FAQs on the Federal Chancellery website.[7]

During the test, participants were able to obtain voter authentication cards from the PIT platform, and submit questions and feedback. SCRT classified the feedback and notified participants of its assessment after contacting them to clarify any queries where necessary. If the feedback was confirmed to be a potential vulnerability, SCRT notified both the MC and Swiss Post. At regular intervals SCRT and Swiss Post submitted their feedback assessments to the MC. On no occasion did SCRT, Swiss Post and the MC disagree on the assessment of feedback reports.

6 Results

By the end of the test on 24 March 2019, 3,186 people from 137 countries had registered to take part[8]. 1,090 people or teams had actually logged into the PIT platform. 822 people requested voter authentication cards for the test. 80 people submitted a total 173 feedback reports via the PIT platform. In 16 of those cases, SCRT identified a breach of best practices on security technology[9]. Swiss Post paid those participants a total compensatory amount of CHF 2,000. No infrastructure penetration, vote manipulation or breach of voter secrecy was identified in the course of the PIT.

Nevertheless, researchers identified three significant flaws in the system outside the scope of the PIT based on disclosure of the source code[10]. One of the shortcomings also concerned the production version of the individually verifiable system. This ultimately led to the decision taken by Swiss Post not to use the system during the ballot on 19 May 2019. Furthermore, the Federal Chancellery announced a review with the aim of pre-empting such mistakes in good time in future. There were no reports of any attacks on the system that had taken advantage of these particular flaws. As the flaws did not come to light in the course of an attack on the system being tested, the feedback reports did not fall within the scope of the PIT.

7 Conclusions

The fact that a large number of skilled people from around the world took part in the test can be considered a success. Their work allowed the shortcomings in terms of best practices to be remedied and thereby helped to further improve the security of the system as a whole. They are likely to be able to make use of their experience with electronic voting in Switzerland in future, by perhaps addressing security issues in other systems or simply by contributing to public debate on the matter.

It can be assumed that the participants were not only composed of experts, but also of interested citizens. The PIT has given them the opportunity to familiarise themselves with an e-voting system that may in future be used in their canton.

[7] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html
[8] According to declarations by participants
[9] Point 4.3 Annex and https://www.onlinevote-pit.ch/stats/
[10] https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-74508.html

Swiss Post satisfied the requirements set by the Confederation and the cantons in most areas. It invested sizeable resources and qualified staff into running a PIT which delivered plenty of valuable insights. The areas in which improvements need to be made are in the preparation and disclosure of the source code. These points must be addressed.

The frequently voiced criticism regarding the scope of the PIT must be taken into account. And with regard to security issues that cannot be dealt with within the scope of a public intrusion test, measures to promote and structure constructive dialogue with independent experts should be examined as part of the Federal Chancellery's forthcoming review. In terms of system development and quality assurance-related measures, independent experts should also be involved to a greater extent in future.

The most valuable reports concerned the significant flaws identified in the source code. There were no reports of successful attempts to penetrate the system. For future tests, it would be worth considering incentives to encourage people to disclose valuable observations regarding the source code and documentation. The experiences gained during the PIT can serve as guidelines in establishing a quality and error management culture in the context of e-voting.

It is safe to assume that media coverage of the PIT helped to stimulate the strong interest in analysing the source code.

This was the first PIT to be carried out on an electronic voting system in Switzerland. The lessons learned will be incorporated into any future tests of such systems.

8 Further documentation, reports, reference material

Information on the public intrusion test provided by the Confederation, the cantons and the service provider charged with conducting the test (SCRT):

Document / Report / Link	Link
Confederation website with information on the 2019 public intrusion test	https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html
Requirements set out by the Confederation and the cantons on public intrusion tests	https://www.bk.admin.ch/dam/bk/en/dokumente/Federal%20and%20cantonal%20requirements_public%20intrusion%20tests.pdf.download.pdf/Federal%20and%20cantonal%20requirements_public%20intrusion%20tests.pdf
PIT fact sheet published by the Federal Chancellery	https://www.bk.admin.ch/dam/bk/en/dokumente/pore/PIT_Factsheet%20BK_EN.p

	df.download.pdf/PIT_Factsheet%20BK_EN.pdf
PIT fact sheet published by the Management Committee	https://www.bk.admin.ch/dam/bk/en/dokumente/pore/PIT_Factsheet%20Leitungsausschuss_EN.pdf.download.pdf/PIT_Factsheet%20Leitungsausschuss_EN.pdf
PIT registration platform for interested parties and participants	https://www.onlinevote-pit.ch/
FAQs on the PIT (FAQ) for interested parties and participants	https://www.onlinevote-pit.ch/faq/
Accepted and published PIT findings	https://www.onlinevote-pit.ch/stats/

Information provided by the system operator, Swiss Post, on the Public Intrusion Test:

Document / Report / Link	**Link**
Detailed technical final report from the system operator (Swiss Post AG)	https://www.post.ch/-/media/post/evoting/dokumente/abschlussbericht-oeffentlicher-intrusionstest-post.pdf?la=en&vs=1
Terms, Conditions and Code of Conduct Public Intrusion Test (PIT)	https://www.onlinevote-pit.ch/conduct/
Swiss Post website with information on the 2019 Public Intrusion Test	https://www.post.ch/de/geschaeftsloesungen/e-voting/publikationen-und-quellcode#oeffentlicher-intrusionstest-2019
Swiss Post's blog article on source code disclosure	https://www.evoting-blog.ch/de/pages/2019/die-post-veroeffentlicht-den-quellcode-ihres-e-voting-systems
Swiss Post portal for voters on e-voting incl. Swiss Post demo-system	https://www.evoting.ch/en
Access to source code via Swiss Post website	https://www.post.ch/de/geschaeftsloesungen/e-voting/publikationen-und-quellcode#offenlegung-quellcode

9 Annex

Public Intrusion Test, Final Report, SCRT SA, 2019