The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation

Ardita Driza Maurer(✉)

Centre for Democracy Studies Aarau, University of Zurich, Zürich, Switzerland
ardita.drizamaurer@uzh.ch

Abstract. In Switzerland, internet voting has been in the experimental phase for over fifteen years. With a view to putting an end to trials and normalizing its use alongside the paper-based channels (polling station and postal voting), a thoroughly updated federal regulation entered into force in January 2014. Only systems that are formally certified and offer complete verifiability can be authorized to propose internet voting in an unrestricted manner, i.e. to all the electorate. Furthermore, since July 2018, the publication of the source code of fully verifiable systems is mandatory. A major transparency exercise took place in February – March 2019. The first system to introduce complete verifiability – the Swiss Post/Scytl system – was submitted to a public intrusion test (PIT), open to anyone interested. In a parallel development, the source code of the same system was published on the internet. Researchers found critical errors in the source code of both individual and universal verifiability. The PIT revealed other, less critical issues. This experience has fuelled the already heated debate over the future development of internet voting in Switzerland. It questions the procedures for controlling verifiability solutions and, ultimately, the consensus to develop such solutions. Lessons learned will most probably be reflected in the future update of the regulation.

Keywords: Switzerland · Internet voting · Regulation · Security · Transparency · Public intrusion test (PIT) · Source code publication

1 Introduction

Debate on internet voting in Switzerland focuses on security and transparency. After initial experiences with "black-box"[1] internet voting systems in political elections in several countries, including Switzerland, at the beginning of 2000, consensus emerged within the research community that end-to-end verifiable voting systems are a necessary condition for internet voting [1].[2] Systems started to be developed that may allow the voter and anyone else to verify important aspects of the election, namely his/her

[1] We use this term to characterise first generation internet voting systems introduced in the beginning of 2000 which did not provide for independent, transparent verifications.

[2] See also the 2007 Dagstuhl Accord, http://drops.dagstuhl.de/portals/index.php?semnr=07311. **All links were last checked on 28 June 2019**.

R. Krimmer et al. (Eds.): E-Vote-ID 2019, LNCS 11759, pp. 83–99, 2019.
https://doi.org/10.1007/978-3-030-30625-0_6

own vote and the final tally, while protecting the secrecy of the vote, without introducing any additional danger of improper influence of the voter as compared to postal voting and without relying on trust in persons, processes, devices or software. According to this consensus, the challenge for government and civil society should be to find ways to foster development and testing of new election paradigms in general and to allow them to be assessed and expeditiously rise to meet their potential to improve elections, the goal being to develop systems that increase transparency regarding the correctness of the election results and yet maintain secrecy of individual votes. Improved voter confidence may follow.[3] Proper implementation of such systems as well as voter education are considered important to avoid misuse. Recent developments in Switzerland show that control of end-to-end verifiability solutions and requirements thereof are crucial.

Complete verifiability is required by federal regulation if a system is to be authorized to cover more than 50% of the cantonal electorate [2].[4] It is the sum of extended individual verifiability and universal verifiability. Extended individual verifiability allows the voter to ascertain whether their vote has been manipulated or intercepted on the user platform or during transmission. Voters must receive proof that the server system has registered the vote as it was entered by the voter on the user platform as being in conformity with the system. The proof must also confirm to the voters that the data relevant to universal verification has reached the trustworthy part of the system. Voters (rather "electors" in this case, i.e. persons with voting rights but who did not vote) must be able to request proof after the electronic voting system is closed that the trustworthy part of the system has not already registered a vote cast using their client-sided authentication. For universal verification, the auditors receive proof that the result has been ascertained correctly. The proof must confirm that the result ascertained: a. takes account of all votes cast in conformity with the system that were registered by the trustworthy part of the system; b. takes account only of votes cast in conformity with the system; c. takes account of all partial votes in accordance with the proof generated in the course of the individual verification.[5] Verifiability relies on several trust assumptions.[6]

The development of end-to-end verifiable systems provides valuable real-world experience. One of the two Swiss internet voting systems, the Swiss Post/Scytl system, became the first to allegedly introduce complete verifiability[7] after it had been certified to offer individual verifiability.[8]

---

[3] *Ibid.*

[4] The definition of complete verifiability is to be found in article 5 read in combination with article 4 of the federal Chancellery Ordinance on Electronic Voting (VEleS), RS 161.116.

[5] *Ibid.*

[6] See e.g., art. 4 para. 4 and 5 as well as art. 5 para. 3 let. c and para. 5 and 6 VEleS.

[7] https://www.post.ch/-/media/post/evoting/dokumente/complete-verifiability-security-proof-report.pdf?la=fr&vs=1.

[8] Individual verifiability is required for authorization for more than 30% of the cantonal electorate, whereas complete verifiability is required for more than 50% (art. 27*f* PRO and articles 4 and 5 VEleS). The Swiss Post system was the first and eventually only system (as Geneva decided to stop developing its system) to be certified for more than 30% of the cantonal electorate. See fn. 14.

The Swiss Post set the objective to present a system offering complete verifiability by the end of 2018.[9] In this context, it underwent the most complete transparency exercise organized so far on a Swiss internet voting system and, to our knowledge, the most complete on an internet voting system for political elections. The system was submitted to a public intrusion test (PIT) decided by the federal Chancellery and the cantons[10] which took place from 25 February to 24 March 2019.[11] In a parallel development, the Swiss Post and its partner, the Spanish firm Scytl, published the source code of their software on 7 February 2019,[12] in accordance with the federal requirement to do so which came into force in July 2018.[13] The publication of the source code should take place when the system has the property of complete verifiability in terms of article 5 VEleS and after successfully passing the examinations foreseen in article 7 VEleS.[14]

A group of researchers discovered significant flaws in the source code [3].[15] As for the PIT, a total of 16 responses were classified as breaches of best practice. According to the federal Chancellery, they do not constitute major risks.[16]

---

[9] https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting?shortcut=evoting.

[10] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-73898.html. See also https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system.

[11] See https://onlinevote-pit.ch and https://pit.post.ch/en.

[12] https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting/e-voting-source-code?shortcut=evoting-sourcecode.

[13] Article 7*a* and 7*b* of the federal Chancellery Ordinance on Electronic Voting (VEleS).

[14] Two types of examinations are foreseen: for less than 30% of the electorate (paragraph 3) and for more than 30% (paragraph 2). The Swiss Post system had successfully passed a number of examinations required by paragraph 2 of art. 7 VEleS for more than 30% of the electorate, in May and June 2017. The certificates issued end June 2017 are valid till end June 2020. The information is published on https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting. The examinations/certificates published are the following:

- Verification of the cryptographic protocol https://www.post.ch/-/media/post/evoting/dokumente/zertifikat-pruefung-des-kryptographischen-protokolls.pdf?la=en&vs=1
- Verification of functionality https://www.post.ch/-/media/post/evoting/dokumente/zertifikat-pruefung-der-funktionalitaet.pdf?la=en&vs=1
- Verification of infrastructure and operation https://www.post.ch/-/media/post/evoting/dokumente/zertifikat-pruefung-infrastruktur-und-betrieb.pdf?la=en&vs=1
- Verification of protection against attempts to infiltrate the infrastructure https://www.post.ch/-/media/post/evoting/dokumente/zertifikat-pruefung-des-schutzes-gegen-versuche-in-die-infrastruktur-einzudringen.pdf?la=en&vs=1

We could not find information on the internet about the examination required by art. 7 paragraph 2 let. e (printing offices) and f (control components) VEleS on the internet. We take for granted that "the disclosed source code relates to the implementation of the cryptographic protocol for complete verifiability at application level" (see https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting/e-voting-source-code) and that all preconditions for doing so (art. 7*a* VEleS) were respected.

[15] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html.

[16] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html.

The federal Chancellery declared itself satisfied that these measures (PIT and publication of source code) led to the discovery of weaknesses and allowed important findings to be made. It also declared that it would conduct a review namely of the licensing and certification procedures for e-voting systems. The Swiss Post decided to suspend internet voting until the source code and other identified errors are addressed and not to offer e-voting at 19 May 2019 federal vote. The federal Chancellery considered the decision on the part of Swiss Post not to make its system available for the vote on 19 May to be logical under the circumstances.[17]

The next federal vote is the federal (National Council) election of 20 October 2019. Requirements for authorizing use of e-voting at federal elections are stringent [4]. The correction of the source code most probably classifies as "substantive change" which should be followed by tests and a new certification [5].[18] The certification requirements are currently under review by the federal Chancellery.[19] Given this, it is questionable whether the Swiss Post system can be ready in time for the 2019 federal election. The federal Government will decide on authorizing the Swiss Post system to use electronic voting in the federal election of 20 October foreseeably on 14 August 2019, provided cantons working with the Post will apply for such an authorization.[20]

The second system belongs to the canton of Geneva and is operated by its administration. It offers individual verifiability but not the universal one. Geneva system was used for the 19 May 2019 vote. It has not been formally certified so far and is authorized for less than 30% of the cantonal electorate. End November 2018, the Geneva Government announced it would cease operating its e-voting system in 2020 for lack of financial support to upgrade it to a fully compliant system, namely, to set up a new system that offers complete verifiability and have it certified.[21] On 19 June 2019 the Geneva Government decided to stop e-voting with immediate effect because of uncertainties around the possible authorization by the federal Government to use e-voting at the October 2019 federal election. The canton of Geneva and the other cantons working with it on internet voting estimated that the expected moment for the federal Government decision (14 August 2019) did not leave enough time to adapt the procedures in case the decision would be negative.[22]

Another potentially disruptive development started in March 2019: the collection of signatures in support of a popular initiative – the so-called e-voting moratorium initiative – to stop any form of e-voting for at least five years.[23] The initiative aims at changing the federal Constitution to prohibit e-voting. It foresees a possible ban lift by the federal Parliament, through a law, which can be introduced at the earliest five years

[17] *Ibid.*

[18] See article 27 *l* 2 PRO and article 7 paragraph 1 VEleS.

[19] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html.

[20] This was still pending on 28.06.2019 when this paper was last reviewed. See https://www.swissinfo.ch/ger/schweiz-demokratie-volksabstimmungen-evoting/45061040.

[21] https://www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018.

[22] https://www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

[23] Initiative populaire fédérale « Pour une démocratie sûre et fiable (moratoire sur le vote électronique) », FF 2019 2081 ("*FF" is an abbreviation of the Swiss Federal Gazette*).

after the introduction of the ban. Several cumulative conditions should be fulfilled to lift the ban, namely: e-voting should offer at least the same level of security against manipulations than paper voting; it should allow voters without specialized knowledge to verify the main steps of the e-voting procedure and enable count-as-cast of cast-as-intended votes while also respecting vote secrecy; the system should exclude external influences and should make sure that results are unequivocal and unfalsified; results can be verified in a sure manner and without special knowledge through new counting; it should be possible to exclude results that do not respect the beforementioned requirements. One of the conditions, namely the possibility for the layman to understand and control every important step without specialized knowledge, seems, at first reading, impossible to achieve.[24] The 18 months signature collection period ends on 12 September 2020. If the initiative committee gathers the required one-hundred-thousand valid signatures, the fate of internet voting will be decided in a popular vote by the majority of the people and cantons.

These developments unfold in the context of the implementation of a federal Government's decision of April 2017 to introduce internet voting into regular operation alongside the postal and polling-station voting.[25] The federal Council submitted in December 2018[26] a proposal to modify the federal Act on political rights (PRA) [6] in this sense. The proposed modification upheld the current requirements for internet voting and proposed to improve the structure of the regulation by bringing core principles of complete verifiability, transparency, certification, risk assessment framework and accessibility to the level of the law instead of having them at the ordinances' level, as is currently the case. The normalized use of e-voting would have put an end to the experimental phase that lasts since 2004. The proposed revision of the PRA was submitted to a consultation procedure from 19 December 2018 to 30 April 2019. Cantons and interested organizations were invited to comment on the proposal. The results of the consultation were published end June 2019.[27] They show that developments around the Swiss Post transparency exercise influenced the debate. The consultation revealed that most respondents, including a clear majority of the cantons and political parties, support the introduction of e-voting in principle. However, most respondents, including political parties which support e-voting in principle, also considered its introduction into regular operation to be premature. On 26 June 2019, the federal Council took the decision "to provisionally forgo introducing electronic voting into regular operation" and "not to proceed with the partial revision of the Political Rights Act at the present time".[28] Internet voting's introduction as a regular voting channel is thus technically delayed. The federal Council also commissioned the federal Chancellery "to amend the general conditions for future trials" namely "to redesign the

[24] A few months earlier the federal Parliament had refused such a "layman control" on e-voting https://www.swissinfo.ch/eng/boost-for-expat-swiss-group_opponents-of-e-voting-suffer-setback-in-parliament/44395904.

[25] https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-66273.html.

[26] https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-73491.html.

[27] https://www.newsd.admin.ch/newsd/message/attachments/57568.pdf.

[28] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-75615.html.

way in which the trials are operated, and to present the results in a report by the end of 2020. The aim is to establish stable trial operations using the latest generation of systems. Other measures include extending independent audits, increasing transparency and trust, and greater involvement of scientific specialists".[29]

The following sections focus on lessons learned from the PIT and the publication of source code, from a regulatory point of view. After an overview of the federal legal requirements on security and transparency (Sect. 2), we present the PIT and the publication of the source code and related events (Sect. 3). The results call into question the current regulation, particularly the control requirements for end-to-end verifiable systems and, ultimately, the consensus on the role and adequacy of such solutions. The experience has already had an impact on regulation as it prevented the amendment of PRA and the introduction of e-voting into regular operation. It will continue to have an impact as the federal Chancellery is expected to amend the conditions for future trials and decide later on its transformation into a regular voting channel (Sect. 4).

2 Internet Voting Development in Switzerland

2.1 Federal Regulation of Internet Voting

Switzerland has adopted a cautious approach to internet voting which is reflected in the long experimental phase. E-voting has been tested with binding effect in political votes and elections for more than 15 years. The motto is "security before speed". At the same time, Switzerland has a unique situation: its direct democracy system imposes frequent votes at all levels of government. Electors, i.e. the persons with voting rights, are invited to vote on issues or elect representatives at local, cantonal (state) and federal levels an average four times a year. It is thus important to find ways and means to offer effective voting channels to a maximum of electors, including those living abroad and those with special needs.

At the beginning of the years 2000 Swiss authorities concluded that any use of internet voting in the political field required a legal basis [7]. Federal regulation of internet voting, including a dedicated article (art. 8*a*) and other modifications in the political rights Act (PRA) [6] and a dedicated chapter (art. 27*a* ff.) in the political rights ordinance (PRO) [5] was introduced in 2002 and has been in force since 1st January 2003. Swiss cantons started internet voting trials in 2003 (cantonal votes) and 2004 (federal votes). The federal Council (federal Government) evaluated the trials in 2006 [8] and 2013 [9].[30] In 2006 it decided to continue to experiment internet voting and extend the trials to include the Swiss abroad and new cantons. New forms of cooperation developed between cantons with an internet voting system (Geneva, Zurich and Neuchâtel) and those without system. Fifteen out of the 26 cantons have tried internet voting so far; the majority outsources the internet voting service to another canton with a system (Geneva until June 2019) or to a privately held system (currently, the Swiss

[29] *Ibid.*

[30] All evaluations can be found at https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/rapports-et-etudes-concernant-le-vote-electronique.html.

Post). In its third evaluation report of 2013, the federal Council decided to continue to use internet voting but to gradually replace the "black box" first generation systems with "end-to-end verifiable" systems. As a result, the federal regulation was thoroughly modified in December 2013: the federal Ordinance on Political Rights (PRO) was updated and a new instrument, the Ordinance of the federal Chancellery on e-voting (VEleS) was introduced,[31] both in force since 15 January 2014. An additional requirement became mandatory as of 1st July 2018: the publication of the source code of the software of complete verifiability as well as the procedure for its publication (see articles 7*a* and 7*b* VEleS).[32]

Regulation is based on the idea that e-voting must respect all principles applicable to democratic votes and elections and the ensuing legal requirements.[33] The federal regulatory framework for e-voting has a cascade structure that includes the Constitution and the higher-level formal law (PRA), the federal Council ordinance (PRO) that implements the PRA and, further down, the federal Chancellery ordinance on electronic voting (VEleS) and its Appendix which contain detailed provisions that implement the higher level requirements to e-voting. This structure allows for a relatively quick adaptation of the detailed provisions (VEleS) to reflect technical developments and good practices which are considered important in the security area.[34] Generally speaking, the federal regulation requires that e-voting systems and their security are state of the art, as stated in art. 27 *l* para. 1 let. b PRO.

According to federal regulation, use of internet voting at federal votes is furthermore subject to authorization by the federal Council and agreement by the federal Chancellery.[35] Different levels of compliance and respective limitations are foreseen.[36] The Swiss Post system became the first to be formally certified compliant with regulation for systems providing individual verifiability, potentially allowed to cover up to 50% of the electorate. End 2018 it was expected to become fully compliant with the federal regulation for systems providing complete (individual and universal) verifiability which opens the door to authorization to cover up to 100% of the electorate.[37] At this point, it was required to pass two important tests: a public intrusion test (PIT)[38] and

[31] RO 2013 5365 and RO 2013 5371.

[32] RO 2018 2279.

[33] At the federal level e-voting must comply namely with the principle of free elections of art. 34.2 of the federal Constitution (Cst., RS 100), the principles mentioned in article 8*a* PRA, which is the legal basis for introducing e-voting, and the detailed provisions of articles 27*a* ff PRO, of VEleS and its appendix.

[34] The VEleS Appendix contains several references to good/best practice.

[35] Art. 8*a* para. 1 and 1bis PRA, art. 27*a* and 27*e* PRO.

[36] Art. 27*f* PRO. *See* also the discussion in Puiggali/Rodriguez-Pérez (2018).

[37] On its web page, the Swiss Post says that the advantage of its e-voting solution is that it "offers state-of-the-art technology and, in its most advanced phase of development, meets all statutory provisions". To the attention of cantons and municipalities it says that its solution is "Certified for all eligible voters resident in Switzerland and abroad", https://www.post.ch/en/business-solutions/e-voting/the-e-voting-solution-for-cantons.

[38] See fn. 10.

the publication of the source code of the software for complete verifiability in compliance with the VEleS requirements for doing so.[39]

We do not refer to cantonal legislation as it is less detailed and mainly a repetition of federal provisions. In principle, cantons have important autonomy in the electoral field [10]. However, with respect to internet voting, the main requirements, namely those related to security, are defined at the federal level and are the same across the country and the systems.

2.2 Federal Requirements on Security and Transparency

The federal regulation of internet voting introduced in 2002 was quite a detailed piece of legislation which also inspired the development of the Council of Europe 2004 Recommendation on e-voting [11, 12]. Electoral authorities controlled the implementation of security related requirements. External audits were conducted but the findings were not published.[40] Privileged players, i.e. federal authorities in the context of the authorization procedure and the electoral commission in cantons where it existed, had access to the documentation. Political parties represented at the electoral commissions, namely in Geneva and Neuchâtel, could access the documents, which is a good practice.[41] A form of peer-control was provided by federal groups accompanying each cantonal e-voting project whose members are e-voting specialists from other cantons. However, security and transparency of first generation systems, and indirectly the regulation on which they were based, was criticized by research which referred to them as "security by obscurity" approach [13].[42] To sum up, first generation systems introduced in the beginning of 2000 did not provide for independent, transparent verifications. They were not submitted to federal requirements to divulgate the source code or security relevant documents.[43]

---

[39] Art. 7*b* VEleS.

[40] In its second report on e-voting the federal Government said that "the technical documentation including evaluations of an e-voting system and its security are cantonal confidential documents that are annexed to the request for authorization addressed by a canton to the federal Council. These documents are not public. Cantons that apply the transparency principle can attach conditions to the consultation by the public of these documents and source codes or even refuse access to the extent that they contain sensitive security information or trade secrets. This practice has been upheld by the federal Court" (our translation), FF 2006 5205, 5215. In its third report, the federal Council reminds that only one canton (Geneva) had introduced legislation on limited access to the source code, FF 2013 4519, 4596 f. The federal Council notes that the mid and long-term objective is to achieve maximum transparency without violating legal or contractual obligations.

[41] Third report of the federal Government on e-voting, point 5.4.4, FF 2013 4519, 4600.

[42] For an overview of major weaknesses that technical research identified in first generation systems and proposals to correct them in second generation systems, see in particular Dubuis, Haenni, Koenig (2012), pp. 10 ff, in particular points 1, 2, 5 and 11.

[43] Security was mainly based on measures taken by the voter to protect her own computer, on the discouraging effect of penal law provisions and on the security provided by the system itself at the structural, functional and technical levels. The fact for e-voting to be only a complementary voting method, not an exclusive one, was considered relevant to its security: See the first report of the federal Government on e-voting, FF 2002 612, 632 ss, 640.

The thoroughly revised regulation introduced in December 2013 resulted from close cooperation with research.[44] It has the following general approach to security and transparency issues. The higher-level principles that e-voting should satisfy[45] are as many objectives that an e-voting system and program should fulfil to receive federal authorization. The objectives take into account the weaknesses inherent to the underlying technology, as well as main threats, both internal and external ones. Threats include malware on the client or server side, DNS spoofing, MITM attacks, administrator attacks both on the content of votes and on the secrecy of the information, criminal organisations' attacks, DOS etc. Switzerland having already a generalised system of distant postal voting, threats related to "family voting" are not considered as they are not specific to e-voting [9].[46] Risks must be constantly evaluated and kept at an acceptable level by the cantons. A risk arises if a weakness in the system can be exploited by a threat and therefore the fulfilment of a security objective is potentially jeopardised. Threats and vulnerabilities inherent to e-voting should be monitored permanently and appropriate countermeasures are introduced whenever necessary by federal and cantonal authorities.[47]

The regulation admits that absolute security is impossible to achieve in e-voting, or in any other voting channel for that matter.[48] Optimum security is the objective.[49] It rests on three pillars: strong requirements (federal regulation of e-voting refers to state of the art solutions), controls by independent and competent bodies of the conformity of the system with requirements (incl. formal certification)[50] and the possibility to detect possible problems that may still arise during the voting or counting process (plausibility and verifiability checks).[51] If more than 30% of the cantonal electorate are to be authorised to participate in e-voting, the system and its operation must be

[44] The main novelties of the new regulation introduced in 2013, namely verifiability and formal certification, as well as the source code publication introduced in 2018, reflect proposals by technical research. The federal Chancellery accompanied the publication of the Berner Fachhochschule study on the concept and implications of verifiable e-voting systems of 21 February 2012 with a note saying that, although the full implementation of the proposals of BFH is to be considered in the long term, nothing prevents (the authorities) from integrating them already in the daily work of improving the systems (our translation), https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/rapports-et-etudes-concernant-le-vote-electronique.html.

[45] Mainly found in art. 27*b* PRO. Some of them, such as the publication of source code are currently to be found in the lower level VEleS. The proposed modification of PRA aimed at bringing the main principles from PRO and VEleS up to the PRA level. As discussed above, the Government decided on 26 June 2019 to postpone the PRA amendment.

[46] This being so, critique on end-to-end verifiable systems related to secrecy does not affect the Swiss verifiability solution. With respect to such critique, see e.g. Jones D.W.: Some problems with end-to-end voting (2009).

[47] VEleS Appendix, point 3 "Security requirements".

[48] Already the first report of the federal Government on e-voting in 2002 noted that «permanent and absolute security is illusory», FF 2002 612, 639.

[49] VEleS Appendix, point 3 "Security requirements".

[50] Art. 27*l* PRO.

[51] art. 27*i* PRO.

examined in particular detail with regard to several criteria:[52] control of the cryptographic protocol which can be done by a highly specialised institution upon approval by the federal Chancellery; control of other aspects (functionalities, security of infrastructure and operation, protection against attempts to infiltrate the infrastructure, requirements for printing offices and control components) which is to be carried out by an institution accredited by the Swiss Accreditation Service (SAS).[53]

A third provision, important for security, came into force in July 2018: the publication of the source code of systems that offer complete verifiability. The source code should be published only after the system has been certified. In the words of the federal Chancellery, a trustworthy control prior to publication guarantees that the advantages of the publication of the source code outweigh the potential risks associated with it [14].[54] Further, the publication should be done in line with good practice to make sure that interested persons have effective access to the source code and the time needed to analyse it and to submit remarks. In particular, the source code should be prepared and documented in line with good practice.[55] Access should be simple and free.[56] The documentation on the system and its operation must explain the relevance of the individual components of the source code for the security of electronic voting. The documentation must be published along with the source code.[57] Finally, anyone is entitled to examine, modify, compile and execute the source code for ideational purposes, and to write and publish studies thereon.[58] This provision integrates and goes beyond good cantonal and international practice.[59] The legal requirement to publish the source code marks a new approach in e-voting security, in line with good practice and suggestions from research: security is no longer linked to secrecy but to openness and independent verification [15].

To summarize, the regulation requires state-of-the-art security measures. Control of compliance with the regulation and detection of problems rely mainly on certification, verifiability and publication of the source code. These controls are expected to prove a system's conformity with requirements and the absence/presence of potential problems during implementation and should themselves be conducted in a state-of-the-art fashion. The Swiss regulation on security and transparency of internet voting is quite detailed and integrates research recommendations and good practice. It is the first standardisation and certification framework for online voting systems [16]. However, the PIT and source code publication revealed lacunae and raise questions.

[52] Art. 7 para. 2 VEleS.

[53] Appendix VEleS, chapter 5.

[54] See in particular comments on art. 7*a*, al. 2, VEleS in reference [14].

[55] Art. 7*b* para. 1 VEleS.

[56] Art. 7*b* para. 2 VEleS.

[57] Art. 7*b* para. 3 VEleS.

[58] Art. 7*b* para. 4 VEleS.

[59] Canton Geneva introduced legislation on source code publication already in 2016. An important previous milestone was the publication of the source code of the Norwegian system.

3 Public Intrusion Test and Publication of the Source Code of the Swiss Post/Scytl System

Intrusion tests are required by federal regulation to check a system's security. They should be organized at least every three years and be conducted by an accredited organism as part of the certification process.[60] The federal Chancellery and cantons decided to organize a public intrusion test (PIT), open to anyone, to check the security of the Swiss Post system offering complete verifiability.[61] The PIT took the form of a "bug bounty" with the Swiss Post committing financial compensation to participants who would be the first to reveal a relevant vulnerability. The Confederation contributed a substantive amount (250'000 Swiss francs) to the "bug bounty" fund. The PIT lasted one month, from 25 February to 24 March 2019. Around 3,200 people from 137 countries participated.[62] The PIT was accompanied and monitored by a management committee composed of members of the Confederation and the Cantons. The management committee should prepare a final report to the attention of the Steering Committee of the federal internet voting project.[63] The PIT participants discovered least severe vulnerabilities which include findings that show uncritical optimization opportunities.[64]

The most critical vulnerabilities were discovered by examining the source code of the Swiss Post system, whose publication was done in line with the newest requirements of VEleS. According to researchers of the Berner Fachhochschule, these vulnerabilities were already apparent in the system specification documentation; the PIT and publication of source code only played a secondary role in their detection.[65]

The code was published[66] on the platform GitLab and made available upon registration and acceptance of the terms of use, among which the requirement to publish the findings only 45 days afterwards.[67] The published code "leaked" in the sense that researchers who did not accept the terms of use, received it from others and were able to examine it. A group of them detected major vulnerabilities affecting the universal

[60] Point 5.5 of Appendix to VEleS.

[61] Fn. 10.

[62] Swiss Post press release of 29 March 2019 "Facts and figures on the public intrusion test on the e-voting system", https://www.post.ch/en/about-us/company/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system.

[63] Federal Chancellery's information on the PIT https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html.

[64] The 16 accepted vulnerabilities published on the PIT page https://www.onlinevote-pit.ch/stats/ are classified as breaches of best practice which do not constitute major risks. See "Qualifying vulnerabilities" on https://www.onlinevote-pit.ch/conduct/.

[65] Dubuis, E.: Schwachstellen im E-Voting-System der Post entdeckt, https://www.societybyte.swiss/2019/03/25/schwachstellen-im-e-voting-system-der-post-entdeckt/.

[66] https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting/e-voting-source-code?shortcut=evoting-sourcecode.

[67] La Poste Suisse, Accord d'accès au code source de la solution de vote électronique, Janvier 2019.

and individual verifiability [3].[68] They communicated their findings ongoing on Twitter, after a short advance notice to the Post, thus in breach of the 45 days deadline. Although the distribution of the source code to third parties who have not accepted the terms of use is prohibited according to the terms of use, the Swiss Post and the federal Chancellery didn't mention this detail in their communications and took notice and reacted after each published finding.[69]

The first critical error discovered related to universal verifiability.[70] A trapdoor was found that would allow the system operator or any person with access to the system to modify any number of votes in a way that cannot be detected by the verifiability mechanisms. According to the Post, this vulnerability had already been pointed out two years earlier by Swiss researchers of BFH but still persisted. They said regretting that the technology partner, Scytl, which is responsible for the source code, had not made the correction in full earlier.[71] The trapdoor was found in the new version of the system (for +50% of the electorate) which has never been used so the vulnerability couldn't have been already exploited to falsify a vote. This time, according to the Swiss Post, Scytl rectified the error, in full and immediately.[72]

A second vulnerability was found that affects individual verifiability. Someone could theoretically invalidate votes without being detected. Individual verifiability is part of the system that has already been used. However, the Swiss Post relativized saying that exploiting this vulnerability would have produced invalid votes which cannot be accepted by the system and would have been noticed.[73] The question remains: why was it not detected by certification and other tests?

The group of researchers noted that their control was limited as they could only examine a very small percentage of the source code documents, enough though to find two critical vulnerabilities. They would not be surprised to find others. They question other controls which proved successful such as cryptographic and symbolic proofs of verifiability properties,[74] the role of trust assumptions,[75] and suggest solutions to rectify the trapdoor [17].[76]

Lewis, Pereira and Teague also highlighted the extremely complex structure of the source code (6000 documents). Other researchers also mentioned that in addition to the security issues, namely the fact that the code allowed manipulations that could have gone unnoticed, a quick examination of the source code revealed other problems,

---

[68] https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-74508.html.

[69] See the two Press releases of the federal Council of 12 March and 29 March 2019, resp. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74307.html and https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html.

[70] *Ibid.* Press release of 12 March 2019.

[71] https://www.post.ch/en/about-us/media/press-releases/2019/error-in-the-source-code-discovered-and-rectified.

[72] *Ibid.*

[73] https://www.evoting-blog.ch/en/pages/2019/new-finding-in-the-source-code.

[74] https://decryptage.be/2019/03/svote/.

[75] *Ibid.* See also the Berner Fachhochschule experts' conclusions in https://www.societybyte.swiss/2019/03/25/schwachstellen-im-e-voting-system-der-post-entdeckt/.

[76] See also fn. 74.

namely: the code is not clear; the documentation does not comply with the standards; all building blocks (code) must be individually configured (by the Post or cantons) which makes it prone to errors; the documentation must not be cited which makes it impossible for researchers to inform and discuss about errors. This last condition clearly does not comply with the VEleS requirements on publication of the source code.[77]

Eventually, the Swiss Post decided to temporarily suspend e-voting and not provide the service to the cantons for the vote of 19 May. It informed it will correct the source code and have it reviewed again by independent experts.[78] The federal Chancellery invited the Swiss Post to review its security related procedures. It decided to re-examine the certification and agreement procedures.[79] On 26 June 2019 the federal Council mandated the federal Chancellery to amend the general conditions for future trials.[80]

4 Lessons Learned and Questions

The publication the of source code and the PIT were meant to confirm an already certified system and help discover potential errors that certification and other tests could not detect. Instead, examination of the code has shown that certification and other controls had failed to notice some critical vulnerabilities in both individual and universal verifiability. No complete evaluation of the experience has been published so far. There will certainly be important lessons and conclusions that will be drawn on the technical side. E-voting supporters hope that this will make the system/s more secure. The experience also raises more fundamental legal and policy questions.

4.1 Controls

The Swiss regulation on internet voting is an advanced example of designing internet voting requirements to achieve end-to-end verifiable systems in conformity with good practice on security and transparency. The practical implementation shows that, despite good will and the important means dedicated to this, we have not yet obtained an end-to-end verifiable system free of errors. Of course, experts note that these errors would not be there had state-of-the-art solutions been used [e.g. 3, 13, 17].[81] Yet, experts are

[77] Kolly, M.-J. based on a discussion with Stiller, B. and Killer, Ch. of the Zurich University: Der Quellcode des E-Voting-Systems ist problematisch, und das hat nicht nur mit Sicherheit zu tun. NZZ, 12 March 2019, https://www.nzz.ch/schweiz/e-voting-der-quellcode-ist-undurchsichtig-sagen-experten-ld.1461406.

[78] Swiss Post press release of 29 March 2019: https://www.post.ch/en/about-us/company/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system. See also Scytl press release of 1st April: https://www.scytl.com/en/statement-related-to-the-recent-decision-to-place-evoting-temporarily-on-hold-in-switzerland/.

[79] Fn. 69.

[80] Fn. 28.

[81] See also fn. 77.

puzzled by the fact that other cryptographic proofs and controls (other than certification) failed to notice the vulnerabilities.[82] And they also question one of the basic building blocks of verifiability as practiced here – the trust assumptions.[83] This raises a first question of principle. The lay person considers end-to-end verifiability as the way to verify the result of the election given the impossibility to certify that a system, as implemented during e-voting, can be considered 100% secure. If the control of the end-to-end verifiability solution and its implementation presents difficulties similar to those related to controlling the system itself, is end-to-end verifiability a good solution?

Second, the regulation requires state-of-the-art solutions on all aspects related to security, including its control. A constructive dialogue has taken place between cantons, the Confederation and technical research, who have been actively involved in designing and evaluating the two systems. Yet, introducing state-of-the-art solutions in a timely manner is very challenging, as shown by this experience. Certification procedures for end-to-end verifiable solutions were designed end 2013 and allegedly respected good practice at that time. According to researchers, at least by the end of 2018, it became clear that procedures should be redesigned. However, this has not yet been done and the certification of the Swiss Post system was conducted according to the 2013 regulation. According to researchers of the Berner Fachhochschule, this, among others, explains why the system got the certification, despite the flaws.[84] This shows that, although the Swiss federal internet voting regulation is built in a cascade structure which allows the federal Chancellery to rapidly adapt VEleS to take into account technical developments, it still takes some time to adapt the regulation and the processes. This is unavoidable. Regulation cannot follow technique without delay and there will always be a time lag. In our case this was very detrimental as it allowed certification of a flawed system. State-of-the-art that requires adaptations of regulation cannot be implemented without a time lag. Legality seems to weaken the state-of-the-art requirement. Quid?

A third issue is the definition of good practice and state-of-the-art. Researchers for instance pointed out the complexity and quality of the source code of the solution [3]. Certification bodies are expected, according to regulation, to control that the system and security measures are state-of-the-art and respect good practice.[85] Is this possible at all? Is certification the right instrument for doing this? If yes, is such a certification possible within reasonable time and financial costs? If not, who should define what is state-of-the-art at a given moment and who should check this? Additional questions relate to partial implementation of state-of-the-art and consequences for doing so.

A fourth, crucial issue, relates to the cost of state-of-the-art security. In Switzerland they are covered by the cantons mainly, who organize and conduct elections, including federal ones. As security requirements are determined at the federal level and can vary

[82] Fn. 74.

[83] Dubuis, E.: Schwachstellen im E-Voting-System der Post entdeckt, https://www.societybyte.swiss/2019/03/25/schwachstellen-im-e-voting-system-der-post-entdeckt/.

[84] *Ibid.*

[85] Art. 27*l* para. 1 let. b PRO and references to good practice in VEleS.

according to risk evaluation, there is increasingly a friction which may result, as in the case of Geneva, in a decision to abandon internet voting.[86] The relation between security requirements, which should be uniform and determined at the federal level, and financial means, which come from cantons (states), needs further clarification.

4.2 Transparency

The publication of the source code was the starting point for discovering the most critical vulnerabilities. This highlights the importance of this transparency exercise. The "leaked code" experience shows that restrictions to publication of source code, such as the 45 days silence period, may be unenforceable.

Despite its importance, the publication of the source code and its examination is not a full and systematic control of a system's security. Researchers indicated that they could only examine a very small fraction of the code. Time and resources fail to do more. Unlike the PIT, the source code examination was not designed as a "bug bounty", so incentives to detect and report vulnerabilities may be lower. As publication of the source code of systems offering complete verifiability is permanent, conditions may be reconsidered to integrate lessons learned from this first exercise.

4.3 Future Directions?

Putting an end to the experimental phase and transforming e-voting into an ordinary voting channel similar to the postal and polling station voting proves to be very challenging. On 26 June 2019, the federal Government decided to delay its introduction as a regular voting channel and reframe the trial phase. Depending on the outcome of the recent popular initiative to introduce a moratorium on e-voting and the interpretation of its requirements, e-voting may even become impossible until its control by the layman is ensured.[87]

Cooperation with research has been crucial in developing second generation systems that offer verifiability and transparency. However, cooperation is important not only in order to develop and evaluate solutions that respect the federal regulation. More should be done already when defining an e-voting policy and regulation. The last decision of the federal Government announced "greater involvement of scientific specialists". This seems to point into the right direction and should be welcomed.

[86] Following the cantonal government's decision of fall 2018 to stop using their own system and outsource the internet voting service to an external provider from the beginning of 2020, on 14 May 2019 the cantonal parliament voted a draft law, which, requires that the design, management and exploitation of an internet voting system remains in public administration's hands. The Government of Geneva expressed this position – of an internet voting system in public hands – at the consultation on the proposed amendment of PRA (see fn. 27). On 19 June 2019 the cantonal Government decided to advance the deadline and stop using the Geneva system with immediate effect.

[87] For the time being however the task of verifying the security of internet voting can be conducted by specialists.

The contribution of end-to-end verifiability to the security of the internet voting needs a new reflection. Does researchers' consensus on developing end-to-end verifiable systems need an update? Are elections appropriate playground to try and test end-to-end verifiability? Are there undisputed techniques to achieve "optimum" security?

References

1. Benaloh, J., Rivest, R., Ryan, P., et al.: End-to-end verifiability (2014). http://arxiv.org/abs/1504.03778
2. Federal Chancellery Ordinance on Electronic Voting (VEleS), RS 161.116. https://www.admin.ch/opc/en/classified-compilation/20132343/index.html
3. James Lewis, S., Pereira, O., Teague, V.: Trapdoor commitments in the SwissPost e-voting shuffle proof. https://people.eng.unimelb.edu.au/vjteague/SwissVote
4. Federal Chancellery, Catalogue des exigences à remplir pour recourir au vote électronique lors de l'élection du Conseil national en 2019, Version 5 April 2018. https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/Anforderungskatalog%20NRW%202019.pdf.download.pdf/Catalogue_des_exigences_ECN_2019_FR.pdf
5. Federal Ordinance on Political Rights (PRO), RS 161.11. https://www.admin.ch/opc/fr/classified-compilation/19780105/index.html
6. Federal Act on Political Rights (PRA), RS 161.1. https://www.admin.ch/opc/en/classified-compilation/19760323/index.html
7. Federal Council: «Rapport sur le vote électronique. Chances, risques et faisabilité», FF 2002 612, 9 January 2002 (2002). We refer to it as "first report"
8. Federal Council: «Rapport sur les projets pilotes en matière de vote électronique», FF 2006 5205, 31 May 2006 (2006). We refer to it as "second report"
9. Federal Council: «Rapport du Conseil fédéral sur le vote électronique. Evaluation de la mise en place du vote électronique (2006–2012) et bases de développement», FF 2013 4519, 14 June 2013 (2013). We refer to it as "third report"
10. Driza Maurer, A.: Internet voting and federalism: the Swiss case. In: Barrat i Esteve, J. (Coord.) El voto electronic y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado, Iustel, Madrid, pp. 261–288 (2016)
11. Braun, N.: E-voting: Switzerland's projects and their legal framework in a European context. In: Prosser, A., Krimmer, R. (eds.) Electronic Voting in Europe. Technology, Law, Politics and Society, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), vol. P-47, pp. 43–52 (2004)
12. Driza Maurer, A.: Ten Years Council of Europe Rec (2004)11. Lessons learned and outlook. In: Krimmer, R., Volkamer, M. (eds.) Proceedings of Electronic Voting 2014 (EVOTE 2014), pp. 111–120. TUT Press, Tallinn (2014)
13. Dubuis, E., Haenni, R., Koenig, R.: Konzept und Implikationen eines Verifizierbaren Vote Électronique Systems (im Auftrag der Schweizerischen Bundeskanzlei) (2012). https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/berichte-und-studien.html (see "Von der Bundeskanzlei in Auftrag gegebene Studien", "Konzept Berner Fachhochschule")
14. Federal Chancellery: Vote électronique: publication du code source. Rapport explicatif sur la modification de l'ordonnance de la ChF sur le vote électronique (VEleS), du 30 mai 2018, https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/criteres-pour-les-essais.html (see "Adaptation des dispositions légales 2018", "Rapport explicatif OVotE")

15. Driza Maurer, A.: E-voting source code publication: a good practice becomes a legal requirement. In: Jusletter IT 26. September 2018
16. Puiggali, J., Rodriguez-Peréz, A.: Designing a national framework for online voting and meeting its requirements: the Swiss experience. In: Krimmer, R., et al. (eds.) E-Vote-ID 2018 Proceedings, pp. 82–97. TUT Press, Tallinn (2018)
17. Haenni, R.: Swiss Post Public Intrusion Test Undetectable Attack Against Vote Integrity and Secrecy (2019). https://e-voting.bfh.ch/publications/2019/
18. Haenni, R.: Swiss Post Public Intrusion Test: Generating Random Group Elements (Best Practice) (2019). https://e-voting.bfh.ch/publications/2019/