www.jusletter-it.eu

Ardita Driza Maurer

E-voting source code publication: a good practice becomes a legal requirement

Security is at the centre of discussions on e-voting. The ordinance of the federal Chancellery on e-voting (OVotE) was recently modified introducing a new legal requirement: the publication of the source code of the software of complete verifiability. The public can analyse the code of one of the main security-relevant components and contribute to improve it. «Security by transparency», so far a good practice, is now reflected in the federal legislation on e-voting. It sets a milestone in the legal design of e-voting, more particularly of its security and transparency, in line with best cantonal and international practices.

Category: Articles
Region: Switzerland
Field of law: E-Voting; E-Democracy

Citation: Ardita Driza Maurer, E-voting source code publication: a good practice becomes a legal requirement, in: Jusletter IT 26 September 2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Development of legal requirements on security[1]

[Rz 1] E-voting must respect all principles applicable to democratic votes and elections and the ensuing legal requirements.[2] It is accepted that absolute security is impossible to achieve in e-voting, or in any other voting channel for that matter.[3] Optimum security of e-voting rests on three pillars: strong requirements (namely on security) applicable to all e-voting systems used by cantons during federal votes and elections (federal legislation on e-voting);[4] control of the conformity of the system with the requirements by independent and competent bodies (also referred to as certification)[5] and the possibility for the voter and IT experts to detect possible problems that may nevertheless arise during the voting or the counting processes (verifiability).[6]

[Rz 2] Verifiability is based on cryptographic tools. Its broadest form is called «complete verifiability» [7] and includes both the individual and the universal verifiability. Individual verifiability enables the voter to control that the registered vote reflects her will.[8] It also enables the elector who did not vote to check whether her voting rights were (ab)used by someone else.[9] Universal verifiability enables anyone with the necessary knowledge and equipment to check that votes were counted as registered and that only votes from legitimate voters were registered.[10] Certification and complete verifiability provide proofs of an e-voting system's conformity with requirements and of the absence or presence of potential problems during a specific vote or election. This is a major improvement compared to postal voting – the other form of voting from an uncontrolled environment and preferred voting method in Switzerland.[11]

[Rz 3] First generation Internet voting systems introduced at the beginning of 2000 were not subject to requirements of individual and universal verifiability or certification (also known as « security by obscurity » approach). Legal requirements applicable to e-voting have since be-

1 Abbreviations and references to federal legislation and reports refer to the French version published in the systematic collection (RS), the chronological one (RO) and the official gazette (FF). All documents are available in German and Italian too. Links were last checked on 14 August 2018.

2 At the federal level e-voting must comply with constitutional principles, namely art. 34.2 of the federal Constitution of 18 April 1999 (Cst.; RS 101) on the freedom to vote and the principles found in the federal law on political rights of 17 December 1976 (PRA; RS 161.1), namely article *8a* which is the legal basis for introducing e-voting. Detailed provisions on the implementation of principles are found in articles 27*a* ff. of the federal ordinance on political rights of 24 May 1978 (ODP; RS 161.16) as well as in ordinance of the federal Chancellery on e-voting and its appendix of 13 December 2013 (OVotE; RS 161.116).

3 The first report of the federal Government on e-voting in 2002 noted that « *Permanent and absolute security is illusory* » (FF 2002 612, 639).

4 See fn. 2.

5 Art. 27*l* ODP.

6 Art. 27*i* ODP.

7 Art. 5 para. 2 OVotE.

8 Art. 4 and 5 para. 3 OVotE.

9 Art. 5 para. 2 let. b OVotE.

10 Art. 5 para. 4 OVotE.

11 Uwe Serdült / Eric Dubuis / Andreas Glaser, Elektronischer versus brieflicher Stimmkanal im Vergleich, in: Jusletter IT 21. September 2017.

en strengthened and further elaborated, especially with the update of the federal ordinance on political rights (ODP) and the introduction of a new instrument, the ordinance of the federal Chancellery on e-voting (OVotE) in December 2013 (in force since 15 January 2014).[12] A newer generation of systems compliant with the actual requirements is gradually replacing the previous one. Certification and complete verifiability are preconditions to the use of e-voting at a larger scale.[13]

[Rz 4] Detailed legal requirements included in OVotE are expected to evolve to take into account technical or social developments, for instance by making good practices, especially in the area of security, mandatory.[14] The latest modification of OVotE[15] requires the publication of the source code of the software for complete verifiability. The publication should be done after certain controls, namely after successful certification of the system.[16] It should furthermore be in line with good practice so that interested persons have effective access to the source code and the time needed to analyse it and to submit their feedback.[17]

[Rz 5] The publication of the source code of complete verifiability is a significant development from the security and transparency viewpoints. It is a reaction to several parliamentary interventions asking for more transparency,[18] but not only. Similar developments at the cantonal and international level also led to it. We will briefly go through them.

2. Development of transparency requirements

[Rz 6] A legal study commissioned by the State Chancellery of canton Geneva[19] recommended, already in 2001, to give experts the largest access possible to the source of the system. Not only to experts designated by State authorities or private providers but, first of all, to experts from political parties and to independent researchers.

[Rz 7] However, first generation systems were not required to divulgate the source code or security relevant documents.[20] Electoral authorities mandated external audits. The findings were not published. Access to them was granted to privileged players, namely to the federal authorities in

12 The third report of the federal Government on e-voting of 14 June 2013 (FF 2013 4519), presented the main lines of development of the second generation of internet voting in Switzerland. It was followed by the modification of articles *27a* ff. ODP (RO 2013 5365) and the introduction of OVotE on 13 December 2013 (RO 2013 5371), in force since 15 January 2014.

13 See articles 4 and 5 OVotE.

14 See references to good/best practices in the Appendix to OVotE.

15 The modification of 30 Mai 2018 of OVotE (RO 2018 2279) entered into force on 1 July 2018. All documents on https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/criteres-pour-les-essais.html (switch languages on the top right of the page).

16 Art. 7*a* para. 2 OVotE.

17 Art. 7*b* OVotE.

18 Motion Lukas Reimann 15.4237 « *E-Voting. Ja, aber nur mit Transparenz* », Motion Christophe Darbelley 15.3492 « *Pour un système de vote électronique public et transparent* », Motion Balthasar Glättli 13.3812 « *Kein unsicheres E-Voting. Nur Systeme mit Verifizierbarkeit und offenem Source Code zulassen* », Interpellation Jean Christophe Schwaab 12.3288 « *Vote électronique. Stimuler l'innovation pour garantir la sécurité* », parliamentary initiative Josef Zisyadis 08.486 « *Inscription de la transparence du vote dans la Constitution fédérale* », www.parlement.ch.

19 Andreas Auer/Nicolas von Arx, «La légitimité des procédures de vote: les défis du e-voting», Genève 2001, https://www.ge.ch/document/10276/telecharger.

20 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. E-voting being only a complementary voting method (as opposed to an exclusive one) was considered rele-

the context of the authorization procedure and to the electoral commission, where it existed (in Geneva and Neuchâtel). Access to documents by political parties' representatives (at the electoral commission) is considered to be a good practice.[21] Some sort of peer-control was provided by federal groups accompanying each cantonal e-voting project and whose members were e-voting experts from other cantons.

[Rz 8] Transparency was the topic of the first decision on e-voting of the Supreme Federal Court on 23 March 2006 in case 1P.29/2006.[22] The case opposed a voter to the State Chancellery of Geneva and their (then) private provider of the e-voting solution about voter's access to the source code and to the e-voting documentation. The federal Court held, in a general way, that the right to access information about the system was not absolute but could be restricted for reasons such as State security, trade secrets or the need not to unduly favour competitors. In saying that, the Court took into account the fact that political parties represented at the electoral commission had privileged access to documentation (see point 2.6 of the decision). The federal Court took note of the cantonal Court's decision to authorize access to the source code and to consider the Non Disclosure Agreement as disproportionate except for the provision banning code dissemination. «Access» was however understood, by both courts, as the possibility to consult a printed (paper) copy of the code at the premises of the Chancellery. Online publication of the code was not an issue, at that time.

[Rz 9] Both courts recognized «*the interest of the citizen to test the reliability of the voting system*» and both considered on-site consultation of printed source code as being a satisfactory measure to protect that interest. As for the consultation of audit reports, both courts followed a more restrictive line estimating that «*the nature of the* (e-voting) *system required . . . that certain information remains unknown to the public*». This differentiated approach, authorising (limited) access to the source code but barring from access to the audit reports is difficult to understand, given both documents' relevance for the security and reliability of the e-voting system.

[Rz 10] However, the discussion did not stop there. The repeated demands for access pushed the cantonal legislator to change the law. In 2009 Geneva's cantonal law on the exercise of political rights (LEDP, rs/GE A5 05) introduced the requirement that audit reports should be published (art. 60 C al. 3 LEDP). Furthermore, external audits should be organised every three years at least. The first audit report was published in 2012. A more recent change of the law (2016) requires the cantonal Government to take the necessary steps to publish the source code of the applications that enable e-voting. The Government should clarify the conditions and practical modalities of the publication (art. 60 B LEDP). A report by a parliamentary commission was presented to the cantonal parliament (Grand Conseil) before the law was changed. It summarises the key issues and concerns related to the publication of the source code.[23] It is interesting to note that the

vant to security. See e.g. the first report of the federal Government on e-voting from 2002 (FF 2002 612, 632 ss, esp. the example given on page 640).

21 See point 5.4.4 of the third report of the federal Government on e-voting of 2013 (above, fn. 5).

22 Available at https://www.bger.ch/index.htm.

23 Report «Rapport de la Commission des droits politiques et du règlement du Grand Conseil chargée d'étudier le projet de loi du Conseil d'État modifiant la loi sur l'exercice des droits politiques (LEDP) (A 5 05) (Accès au code source du vote électronique)» of 7 January 2016. PL 11701 – A http://ge.ch/grandconseil/data/texte/PL11701A.pdf.

parliamentary commission unanimously approved the source code publication. CHVote's code was published (partially) for the first time in 2016.[24]

[Rz 11] At the international level, the old Recommendation of the Council of Europe on e-voting,[25] in force between 2004 and 2017, prescribed in general the publication of all information that allows to understand how the system works.[26] The guidelines on transparency that completed the old Recommendation, mentioned that national and international observers should have access to all relevant documents (para. 6) and that the source code should be part of those elements that the authorities should check (para. 12). Clearly, the main priority was (and still is in many countries) to make sure that electoral authorities have access and are able to control e-voting software provided by private firms.

[Rz 12] The office of democratic institutions and human rights (ODIHR) of the Organisation for security and cooperation in Europe (OSCE) – the organisation for international observation in Europe – has issued recommendations on e-voting to Switzerland, Estonia, Norway or France, with Council of Europe e-voting recommendations as main legal background. There have been no specific recommendations on transparency for Switzerland. Generally speaking, OSCE/ODIHR recommends that audit reports are published to improve transparency and process verification.[27]

[Rz 13] The real impetus at the international level has come from peers. The publication of the source code of the Norwegian internet voting application[28] (provided by a Spanish firm, SCYTL) did contribute to increasing e-voting transparency in the region. Estonia followed suit publishing its code in 2013.[29]

[Rz 14] The new Recommendation of the Council of Europe on standards for e-voting (Rec(2017)5) recommends member states to be transparent in all aspects of e-voting (standard 31, Appendix I). Standard 33 says that the components of the e-voting system shall be disclosed. However it is also mentioned in the accompanying Explanatory Memorandum that the actual level of disclosure of the elements of the system, necessary for achieving appropriate assurance, depends on the peculiarities of the system. Disclosure should take place well in advance of the election period.[30]

[Rz 15] Most issues related to transparency of internet voting in Switzerland are of cantonal competence. However it is admitted that federal guidance and common requirements are needed, especially when it comes to security, to make sure that constitutional principles are implemented uniformly by all cantonal systems. The cascade structure of the federal legislation on e-voting (including LDP, ODP, OVotE and its Appendix) allows for a relatively quick development of the lower level detailed provisions (i.e. those in OVotE and its Appendix) to adapt for instance to technical developments, important for security.

---

24 GitHub, https://github.com/republique-et-canton-de-geneve/chvote-1-0.

25 See the Council of Europe e-voting page https://www.coe.int/fr/web/electoral-assistance/e-voting.

26 Standards 20 ss. of the old Recommendation Rec(2004)11 of the Committee of Ministers to Member States on legal, operational and technical norms for e-voting, adopted on 30 September 2004.

27 For an overview of relevant international recommendations, see the third report of the federal Council on e-voting (2013), point 1.8.1.

28 The e-vote trial, https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/id597658/.

29 GitHub, https://github.com/vvk-ehk/ivxv.

30 Guidelines on the implementation of the provisions of Recommendation Rec(2017)5 on standards for e-voting, no. 31.b.

[Rz 16] It can be discussed whether the publication of the source code of e-voting cantonal systems should be regulated at the federal or cantonal level. Further, one can also question whether it's up to the legislator (parliament) or to the regulator (here the federal Chancellery) to address this issue. The point of view which has been adopted in this case is that complete verifiability is closely related to security and aspects which are important from a security perspective need to be regulated in detail at the federal level. So, within its competence to uniformly regulate the details of security, the federal Chancellery has introduced the source code publication requirement in its ordinance on e-voting, aligning federal regulation with cantonal legislation and cantonal and international good practices.

[Rz 17] Cantons can do more and better, also on transparency and source code publication. Article 7*b* paragraph 4 last sentence OVotE says for instance that cantonal authorities may authorize other uses of the source code. In addition to disclosing the source code and allowing it to be examined and tested for research purposes, cantons can make it open source.[31] Theoretically they may publish the source code of other elements of an e-voting system, in addition to complete verifiability. However the relevance of such publication for security and hence the question of making it subject to federal detailed requirements is not clear.

3. Digitalization imposes a virtuous spiral

[Rz 18] Before introducing e-voting, cantons initiate or pursue efforts to systemize and digitalise documents and procedures related to votes and elections. For instance, to be able to offer internet voting to expatriates, they harmonise or centralize at the cantonal level registers of Swiss abroad. This process has contributed to improving the quality of data of these registers. Another contribution is the elaboration of eCH XML standards in the field of political rights. In addition to preparing for e-voting introduction, such groundwork is also beneficial to the organisation of votes and elections in general.

[Rz 19] Work continues after e-voting has been introduced as federal legislation requires continuous efforts to maintain the system in line with good practice and state of the art technical knowledge. Also, federal legal requirements continue to evolve to reflect and integrate such developments, as shown by the recently introduced condition of source code publication.

[Rz 20] These two aspects illustrate the fact that digitalisation in general and e-voting in particular are demanding for the electoral authorities. However this allows them to be aware and involved with technical and social developments, which is positive from the perspective of democracy development. E-voting is a continuously evolving process. The publication of the source code for instance constitutes a new approach to its security: from centralized and secret it becomes open and public, in line with good practice.

Ardita Driza Maurer, Jurist, Doctoral candidate, University of Zurich, Centre for Democracy Studies Aarau.

31 See also the report accompanying the modification of OVotE of 30 May 2018 published on https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/criteres-pour-les-essais.html.