Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials)

Explanatory report for consultation

---

28 April 2021

Table of contents

1. Background

Electronic voting in Switzerland (e-voting) has been in a trial phase since 2004 and is part of the e-government strategy adopted by the Swiss Confederation and cantons. The legal basis for the trials is Article 8*a* of the Federal Act of 17 December 1976 on Political Rights (PRA; SR 161.1), Articles 27*a*-27*q* of the Ordinance of 24 May 1978 on Political Rights (PoRO; SR 161.11) and the Federal Chancellery Ordinance of 13 December 2013 on Electronic Voting (OEV; SR 161.116). The principle for the project has remained, from the very beginning, 'security before speed'. In Switzerland, only e-voting systems which meet the high security requirements set in federal law are permitted.

Since 2004, 15 cantons have enacted related legal provisions at cantonal level and in over 300 trials have allowed some voters to vote online. In all cantons, Swiss citizens living abroad have been permitted to take part in the trials, and some cantons have allowed some of their resident voters to cast their vote electronically. Two online voting systems were available to the cantons in recent years: that of the Canton of Geneva and that of Swiss Post. As both of these providers withdrew their systems in mid-2019, e-voting is currently not available in Switzerland.

In 2019, Swiss Post disclosed the source code of its future system with complete verifiability and conducted a public intrusion test.[1] After discovering various flaws in its previously used system as well as its future system, Swiss Post communicated in July 2019 that it would no longer be using its current system with individual verifiability but would instead focus on further developing system that offers complete verifiability. In January 2021, it published the cryptographic protocol of this system, the design of which is intended to meet federal requirements for complete verifiability.

The Canton of Geneva developed and ran its own e-voting system, which was also used by several other cantons. In November 2018, the Canton of Geneva announced that it would not be developing its system any further as it was not the canton's task to single-handedly develop, operate and finance an IT system of such complexity and size. In June 2019, the canton further announced that it would cease operation of its current system with immediate effect.[2] In 2019, the Canton of Geneva published the source code of its incompletely developed system with complete verifiability under open source licence. Bern University of Applied Sciences completed the security-critical elements of the Geneva system and made it available under open source licence in the autumn of 2020. The design of this system is also geared towards meeting federal requirements for complete verifiability.

On 19 December 2018, the Federal Council launched the consultation procedure on the introduction of e-voting as a standard voting method. The partially revised PRA submitted for consultation would have seen the end of the trial phase and the establishment of e-voting as a third voting channel. The consultation showed that a clear majority of the cantons and political parties are in essence in favour of introducing e-voting. The Conference of Cantonal Governments and 19 cantons were in favour of e-voting becoming a standard voting method. However, the parties generally in favour of e-voting did not feel that the time was right for this next step.

[1] FCh press release of 29 March 2019; available at www.bk.admin.ch > Political rights > E-Voting > Media releases.

[2] Canton of Geneva press releases of 28 November 2018 and 19 June 2019; available at www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018#extrait-12897 and www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

2. Redesign of e-voting trials

2.1 Federal Council mandates

Based on the results of the consultation on bringing e-voting into regular operation, the Federal Council decided on 26 June 2019 not to undertake a partial revision of the PRA for the time being. This decision also took account of the developments in the two systems available at the time. The Federal Council also commissioned the FCh to work with the cantons to redesign e-voting trials,[3] setting the following objectives:

1. Further development of the systems
2 Effective control and oversight
3. Increasing transparency and trust
4. Closer cooperation with the academic community

The 'Steering Committee Vote électronique' (SC VE) set up a task force to work on the redesign and relaunch of trials[4] and commissioned it to draw up appropriate measures and a schedule for the staggered relaunch of trials.

At its meeting of 18 December 2020, the Federal Council took note of the final report of the SC VE of 30 November 2020 on the redesign and relaunch of trials. It instructed the FCh to work with the cantons to gradually implement the measures required for the redesign and to submit by mid-2021 a bill for consultation containing the necessary amendments to the Ordinance on Political Rights (PoRO) and the FCh Ordinance on Electronic Voting (OEV).

The Federal Council's intention is to allow the cantons to once again conduct limited e-voting trials. More precise security requirements, increased transparency, closer cooperation with independent experts and effective auditing on behalf of the Confederation aim at ensuring the security of e-voting.[5]

2.2 Dialog with the academic community

In preparing the redesign, the Confederation and the cantons conducted a broad-based dialog on e-voting in Switzerland with 23 experts from Switzerland and abroad in the fields of computer science, cryptography and political science. The full evaluations of their discussions have been published.[6]

The experts see a need for action with respect to security, transparency and independent scrutiny, while recognising that valuable experience has been gathered in the last 15 years. They recommend that other means of voting should also be analysed with respect to security, and that about building trust should be examined in depth.

The experts are of the opinion that verifiability and diversity of components that are important for verifiability (i.e. so-called control components and verifiers) are basic conditions for a system's trustworthiness. The cryptographic security standards already required today are important and should be continually adapted according to the latest insights and scientific progress. Furthermore, the experts advise the public authorities to work towards a standardisation of the cryptographic building blocks.

Care must also be taken to ensure that the system documentation and source code are available in a form that allows conformity with the legal requirements to be reviewed effectively. The experts underline the importance of involving specialists - especially from academic circles - in the design, development and testing of e-voting systems on an ongoing basis. An academic committee could play a role in this regard. The experts are of the opinion that the public authorities should still have the task of assessing risks and of introducing measures where necessary.

---

[3] Federal Council press release of 27 June 2019; available at. www.bk.admin.ch > Political rights > E-Voting > Media releases.

[4] The task force on the redesign and relaunch of trials comprised representatives from the cantons of BE, FR, BS, SG, GR, AG, TG and NE under the lead of the FCh. Swiss Post, as the only remaining system provider, attended all of the task force's meetings.

[5] Federal Council press release of 21 December 2020; available at www.bk.admin.ch > Political rights > E-Voting > Media releases.

[6] FCh press releases of 23 June 2020 and 19 November 2020; available at www.bk.admin.ch > Political rights > E-Voting > Media releases.

Instead of relying on system certification as in the past, the authorities should facilitate an ongoing improvement process. Independent examinations should be commissioned by the Confederation or by an independent committee. Effective and continuous (public) scrutiny can be achieved by involving independent experts and creating suitable framework conditions. Public scrutiny is considered to be of utmost importance and transparency is a prerequisite for its effectiveness. Instead of a public intrusion test (PIT), as was conducted in 2019, the experts recommend holding hackathons or an ongoing bug bounty program with financial compensation for anyone who detects a bug.

The involvement of experts from a range of specialist areas led to a broad discussion of where action needs to be taken and of possible solutions. The experts are in favour of the authorities and the academic community pursuing their communication on an ongoing basis. In future, greater emphasis should be placed on social and societal aspects. The experts also recommend addressing trust issues more closely, and also that security issues should be considered not only with regard to e-voting but also to the other voting channels. A holistic view of possible attacks would improve the security of the voting process in general.

2.3 Main features of the redesigned trials

Following the dialog with the academic community, the Confederation and the cantons drew up a final report containing a comprehensive catalogue of measures. The results of the dialog were taken into account in developing the measures. The SC VE adopted its final report on the redesign and relaunch of trials on 30 November 2020.[7]

The need for action identified in the four objectives set by the Federal Council will be met by implementing a range of measures. These measures will be implemented gradually, beginning with those for the relaunch of trials. This should enable the resumption of small-scale trials while work continues on implementing the medium to long-term objectives.

Continuing the trials in individual cantons will prevent the loss of existing resources and know-how as well as investments already made by the cantons and system providers. It also allows all actors to gain essential experience in the use of completely verifiable systems. The trial nature of the operations is underlined by various measures, which include retaining the limit on the numbers permitted to use e-voting. The principle 'security before speed' will continue to apply. Further measures are planned for subsequent years. According to initial estimates, the medium- to longer-term measures will be implemented within five years of the relaunch of trials.

[7] The final report and the complete documents on the dialog with the academic community are published on the FCh website: www.bk.admin.ch > Political rights > E-Voting.

The main features of the redesigned trials and the implementation timetable can be summarised as follows:

Features	Implementation timetable	Expression in bill for consultation 2021
1. Further development of the systems		
Ensure the quality of the system by defining quality criteria more precisely and establish clear development and deployment processes	Relaunch of trials; continuous improvement process	Specification of requirements
Ensure the forensic readiness of the systems used by means of effective recognition and investigation of incidents	Relaunch of trials; continuous improvement process	Specification of requirements
Create a joint (Confederation and the cantons) public planning instrument for the ongoing implementation of security-related measures	Relaunch of trials; ongoing audits	--
Improve verifiability by introducing greater diversity and independent individual components	Medium-term; greater detail up to 2 years after relaunch of trials	--
2. Effective control and oversight		
Ensure efficacy of independent system examinations	Relaunch of trials	Adjustment of responsibilities and specification of requirements
Set up a regulated process to deal with identified and suspected non-conformities	Relaunch of trials	--
Introduce improvements in risk assessment and crisis management	Relaunch of trials; continuous improvement process	Specification of requirements (risk assessment)
Further develop plausibility checks	Ongoing, first stage by 2022	--
Adapt and revise processes in licensing procedure, as well as roles and tasks	Relaunch of trials and long-term auditing	Adaptation to the new responsibilities
3. Increasing transparency and trust		
Limit number of voters in trials	Relaunch of trials	Adaptation
Create greater transparency and easier access to system information, audit reports and findings	Ongoing	Specification of requirements
Promote creation and involvement of a community of specialists and of the public (politicians, specialists, interest groups and general public) for ongoing public scrutiny	Ongoing	Specification of requirements
4. Closer cooperation with the academic community		
Ongoing support by academia and involvement of independent experts	Cross-sectional topic, ongoing implementation	Adaptation
Set up an academic committee to support and advise the Confederation and cantons	Medium term	--

3. Overview of the present bill under consultation

The present bill for consultation involves a partial revision of the PoRO and a total revision of the OEV and its annex. These amendments are the first stage in the implementation of the measures for the redesign of e-voting trials.

The key points of the bill are:

- **Continuation of trials:**
  E-voting should continue to be used in a trial phase. Previously, under federal regulations the electorate permitted to use e-voting was limited at three different levels, depending on the degree of development of the systems. In the next phase of the trials, the limit for the use of completely verifiable systems will also be set uniformly at 30 per cent of a cantonal electorate and 10 per cent of the national electorate. These limits will be reviewed regularly, taking into account developments in the field of e-voting. As before, Swiss voters abroad will not be considered when the limits are calculated (Art. 27*f* para. 3 PoRO). A new aspect is that voters with a disability who are unable to cast their vote autonomously while maintaining voting secrecy will also not be subject to limits.

- **Improved security:**
  In future, the Confederation will only authorise completely verifiable systems. This is an important measure to ensure the security of e-voting: complete verifiability makes it possible to detect manipulations of the votes cast electronically. The security of e-voting systems will be further tightened by introducing more precise security and quality specifications for the systems and their development.

- **Division of responsibilities between the Confederation and the cantons:**
  As before, the cantons can choose whether or not to conduct e-voting trials. System procurement also remains the responsibility of the cantons; they can either operate their own system, use that of another canton or call in a private company as before (Art. 27*k*^{bis} para. 1 let. b PoRO). The Confederation continues to set the regulatory framework and to give authorisation for the systems.

- **Independent examinations:**
  Instead of the previously required certification of systems and their operation, an independent examination commissioned by the Confederation will now ensure that the system security is effectively tested and that conformity with the licensing requirements is assured. It will also highlight potential for future improvements. The bill for consultation therefore provides that in future the greater part of the examinations will no longer be carried out on behalf of the cantons or the system operator, but on behalf of the FCh.

- **Transparency, cooperation with the public and with the academic community:**
  Tighter transparency requirements and greater involvement of independent experts in the design, development and scrutiny of e-voting systems should help to establish a process of continuous improvement. The public should have access to all system, operational and examination report information and participation should be encouraged. This lays the foundation for ongoing public scrutiny, in which the academic community also has an important role to play. The existing requirements for the disclosure of the source code of e-voting systems are to be specified and there will be a mandatory bug bounty programme. The latter will involve financial compensation for valuable input from the public.

4. Cost implications for the Confederation, cantons and other actors

Security is essential for online voting. This creates costs for the authorities and system providers. These costs are to be financed in accordance with the division of responsibilities between the Confederation and the cantons in the area of political rights. This means that the greater part of the costs will continue to be borne by the cantons.

According to their estimates, implementing the first stage of measures in the period 2021-2022 will incur additional costs of around CHF 1.2-1.5 million for the cantons. Annual operating costs are expected to increase by around CHF 50,000-70,000. Additional costs of CHF 3.4-4.1 million are estimated for the implementation of the medium to longer-term measures. These measures entail an increase in annual operating costs of around CHF 0.9-1.1 million. The estimates given are the total costs for all cantons.

The Confederation estimates that it will have one-off additional costs of around CHF 1.25 million in the first stage of the trials. These costs will be incurred over the period 2021-2022. One of the main expenses will be the independent examinations of e-voting systems to be carried out on behalf of the FCh. Recurring costs are to be expected in the medium to longer term. The redesign of trials will not create a need for additional personnel resources in the Confederation.

The costs are likely to be borne by a small number of cantons over a long period of time. If e-voting is to be introduced successfully, the Confederation must contribute more to the costs of the cantons during trials. Two instruments are currently available for co-financing cantonal e-voting projects. Cantonal project costs can be co-financed via the eGovernment Switzerland or Digital Administration Switzerland implementation plan and in part on the basis of the Swiss Abroad Act (Art. 21 SAA; SR 195.1) and the Swiss Abroad Ordinance (Art. 15 SAO; SR 195.11).

The measures for the redesign will also have consequences for Swiss Post, which is currently the only system provider. The Confederation is not aware of any costs that Swiss Post might incur that exceed the above-mentioned cost estimates for the Confederation and the cantons.

5. Explanation of the individual provisions

5.1 Political Rights Ordinance (PoRO)

Art. 27b let. b

In order to make clear the relationship between the basic licensing procedure and the authorisation procedure, letter b is replaced by a reference to the fulfilment of the conditions for authorisation. This amendment is in line with previous practice and has no practical impact.

Art. 27c para. 2

With the amendment to Article 27*b* letter b of the draft PoRO, this provision can be repealed.

Art. 27d let. c

In the basic licence, the Federal Council specifies not only the geographical area, but also the part of the electorate for which e-voting is authorised. The Federal Council requires information on the number of voters who are to be admitted to electronic voting in order to ensure compliance with the limit set out in Article 27*f* paragraph 1 of the draft PoRO.

Art. 27e paras 1-2

Paras 1 and 1bis: The paragraphs comprise the existing paragraph 1 with the addition that the FCh must specify the requirements for the system and its operation. This provision regarding delegation of responsibilities was previously in Article 27*f* PoRO and is now regulated here.

Para. 2: Editorial revision.

Art. 27f Limits

Para. 1: The graduation of limits previously provided for was linked to the implementation of security requirements. For completely verifiable systems, the Federal Council could have authorised unlimited use. In the trials to date, no canton met the requirements for allowing more than 30 per cent of the cantonal electorate to vote electronically. The limit of 10 per cent of the national electorate was also never attained.[8] The limit is now to be set uniformly at 30 per cent of the cantonal electorate and 10 per cent of the national electorate, even when completely verifiable systems are used. Limiting the proportion of the electorate to the previous lowest category underscores that this is the trial phase of electronic voting.

As before, compliance with the cantonal limits is the responsibility of the cantons. The cantons are free to decide how to ensure compliance with the limit for voters living in Switzerland. Up to now this has been achieved in a variety of ways, e.g. a registration procedure or the use of e-voting in pilot communes. The Confederation is responsible for ensuring that the national limit is observed.

Para. 2: The limitation in paragraph 1 applies to the next phase of the trials. The cantons will be allowed to gain experience in the use of completely verifiable systems, while trials remain limited. A regular review of the limit levels can take account of developments in e-voting. The review should take into account the current and planned use of e-voting in the cantons, the political environment, the stability of the trial operation and the voters' confidence in e-voting. If, taking these aspects into account, the FCh considers it appropriate to adjust the limits, it will request the Federal Council to amend paragraph 1 correspondingly.

Para. 3: Originally paragraph 2 with the following amendment: In addition to Swiss voters abroad, voters with a disability who are unable to cast their vote autonomously while maintaining voting secrecy are also a special target group in e-voting. With the addition of paragraph 3, both target groups can be excluded from the calculation of the limits. This gives the cantons the opportunity to offer e-voting to these groups without the electorate limits constituting an obstacle.

[8] To date, the highest proportion of Swiss voters in Switzerland authorised to use e-voting, just under 2.5 per cent, was at the vote held on 10 February 2019.

Art. 27i paras 1 and 2

The previous wording of Article 27*i* paragraphs 1 and 2 referred to the possibility of allowing either part or all of the electorate to vote electronically. As Article 27*f* paragraph 1 of the draft PoRO excludes the possibility of admitting the entire electorate in the next trial phase, the wording must be adapted.

Para. 1: Plausibility checks of the results of ballots cast via e-voting should provide indications of inadvertent errors in determining the results and of any manipulation of the results. As previously, the cantons can use a variety of plausibility checks. For example, votes cast can be logged and checked by observers, the results can be compared with votes cast by post and in person at the ballot box, or the counted electronic votes can be compared with the log files on the voting server. Where available and as far as the data corpus allows, statistical methods are to be used in the trials.

Para. 2: The verifiability of electronic voting is the main measure for ensuring this voting method is secure as it allows any manipulation of the votes cast electronically to be detected. With verifiability, it must be possible to check whether the vote:

- was cast as intended,
- was recorded as cast,
- was counted as recorded.

In addition to the plausibility check under paragraph 1, e-voting systems will in future only be permitted in Switzerland if they are completely verifiable, even if only part of the electorate is permitted to vote electronically. The wording of the existing provision has also been slightly revised.

Art. 27k^{bis} para. 2

This provision can be repealed since, in contrast to previous practice, the FCh is no longer involved in contractual relations. The contractual relationship between the cantons and any private companies is governed by paragraph 1.

Art. 27l Examination of the system and the operational modalities

Para. 1: Adopts the previous provision in paragraph 2 and regulates when an evaluation is required.

Para. 2: The object of the evaluation is the same as previously. The examining body must be independent of the evaluated body.

Paras 3 and 4: The FCh Ordinance specifies the details of the evaluation, the requirements that the examining bodies must meet, and the responsibilities involved. Following the revision of the statutory basis in 2013, e-voting systems had to be evaluated in most cases by accredited external bodies. The cantons were responsible for commissioning the required certification either themselves or through the system operator and for providing the evidence of this in the licensing procedure. In the course of the work on redesigning the trials, it became apparent that it would be desirable for the Confederation to commission the system evaluations. In future, the division of tasks between the Confederation and the cantons will be such that the Confederation assumes more responsibility and a more direct role in evaluating the systems.

Art. 27m Involvement of and information for the public

Para. 1: In order to involve the public and specialist groups, the FCh and the cantons may use measures such as organising conferences, idea competitions and hackathons, running information platforms and organising citizen science projects. In particular, incentives to encourage specialists among the general public to participate may be created, such as bug bounty programmes run by the cantons.

Para. 2: Publishing information on the e-voting system and its operation aims at ensuring that the processes involved are well understood. Both specialists and persons without specialist knowledge should be addressed. Central to allowing this understanding is publication of the source code and of the associated documentation. The existing Articles 7*a* and 7*b* OEV already require the cantons to disclose and sufficiently document the software source code of a completely verifiable system for e-voting. From the

source code it can be seen how the votes are to be registered and processed by the system. The principle of transparency is important and will now be established in the PoRO. The published information is intended to encourage input from expert circles. This should have a beneficial effect on the security and quality of the systems as well as on trust. The publication of information on the system, in particular the source code and its operation, encourages objective and fact-based debate and reduces the dependence on individual persons and organisations. The FCh will continue to make clarifications in its ordinance.

Para. 3: Corresponds to the previous paragraph 1; the wording has been slightly altered. As before, the cantons should provide information to the voters. This would typically be information in the voting and election papers, explaining the specific procedure for e-voting and what to do in the event of irregularities or problems. In addition, it is felt that the basic concept of verifiability should be explained to voters because the verifiability process only makes it possible to detect irregularities when it is actually applied by the voters. Complete verifiability can only promote voter confidence in e-voting if its essential benefits are understood.

Para. 4: Corresponds in principle to the previous paragraph 2. The provision now makes it clear that observation may be carried out during procedures relating to the conduct of the ballot (e.g. the process of counting, encrypting and decrypting of the ballot). As before, the purpose of this provision is to establish transparency for the voters. And also as before, it does not require the cantons to create a permanent representation for voters, for example an electoral commission; in principle it suffices when procedures and processes can be clearly observed e.g. by an electoral office comprising voters appointed by the competent authority. Furthermore, not *all* steps have to be made accessible and not *all* documents have to be published. If there are important reasons against access or publication, this can still be denied. In this case, the exemption provisions of the applicable legislation on freedom of information can be applied. The reference to the Freedom of Information Act of 17 December 2004 is no longer considered necessary and can be deleted. The primary concern is that the voting process should be completed punctually and not held up at any time because of this provision.

Para. 5: The cantons are now obliged to publish the results of e-voting, for the primary purpose of establishing transparency.

The following results are to be published:

- in popular votes: the number of votes cast electronically in favour, against and blank.
- in elections: the number of votes cast electronically per candidate (candidate votes) and per list (list votes).

In principle, the information should be published in as much detail as possible. The aim should be to publish details per commune in popular votes and details per constituency in elections. The publication of these details must not compromise voting secrecy. This may happen if, for example, only Swiss voters living abroad are permitted to vote electronically and there is only one person living abroad who is entitled to vote in a commune. If voting secrecy is compromised by the publication of voting data, as a rule the principle of publication should not be deviated from, but alternative options should be examined. For example, the feasibility of publishing in less detail, such as an aggregation of the results of several communes, should be considered.

The results do not have to be published in an official gazette; publication on the canton's website is sufficient. The information must be easily accessible and usable.

Art. 27o Involvement of independent experts and the academic community

Para. 1: The authorities are to be increasingly supported in their work by independent experts where this offers added value, for example in relation to the acquisition of knowledge on issues relating to the security of the electronic voting channel. The experts should be independent of the system operator and, if possible, of the authority. Experts may be called in to provide specific services or advice, such as conducting system examinations, providing support and advice in drawing up risk assessments, or assisting with system operation – for example, in evaluating verification results and in conducting possible follow-up investigations.

Para. 2: In addition, the FCh will arrange for the academic community to be involved in the e-voting trials. This provision covers research carried out by the academic community which – in contrast to paragraph 1 – does not have to directly serve the work of the authorities directly relating to conducting ballots. The intention is to promote the development of a basis for evaluating the trials and which might point to possible improvements.

Para. 3: Corresponds in essence to the previous paragraph 2.

5.2 Federal Chancellery Ordinance on Electronic Voting (OEV)

5.2.1 Main part

Art. 1 Subject matter

The definitions are now regulated in the main part of the OEV (see Art. 2 draft OEV).

Art. 2 Definitions

Para.1: Essentially adopts the definitions from the previous annex to the OEV, where relevant for the main part.

Explanation of individual definitions:

Let. a: The system also includes components with special functions that are important for the verifiability of e-voting. These are control components, set-up components, printing components and the technical aids used by the auditors.

Let. b: The online system does not include system components that are used for setting up and counting (such as the printing office and set-up components).

Let. c: The purpose of the trustworthy part of the system is to ensure that malfunctions or attacks can be detected even if only one control component is functioning correctly. Furthermore, the control components allow the distribution of information necessary to decrypt the votes. This means an attacker would need to gain control over all the control components in order to read the votes. The details are set out in the provisions of Annex 2.

Let. d: The requirements for independent design and independent operation can be found in Number 3 of the Annex.

Let. h: The use of auditors promotes transparency. Voters should be able to assume that auditors will draw attention to possible irregularities. The use of auditors in the sense of voter-representation meets Article 27*m* paragraph 4 of the draft PoRO (see also the associated explanations). The specific organisation and design of the deployment of auditors is governed by cantonal law.

Let. i: The user device is not part of the infrastructure.

Let. j: Concerns in particular the implementation of the following elements:

- Generation of the cryptographic secret elements
- Verification of the right to vote (by means of the server-side authentication credential to ensure the sender has the right to vote; this can be done anonymously)
- Validity check
- Registration of incoming votes
- Cryptographic mixing of the registered votes
- Vote decryption
- Establishing the proofs resulting from individual and universal verifiability using the control components

Let. n: In this context, the trustworthy part of the system refers to a group of control components belonging to the online system.

Let. p No 1: In elections run using the first-past-the-post system, blank text fields ('write-in votes') are always considered to have been completed in conformity with the system.

Let. q: Based on the client-side authentication credentials, the technical tool used creates an authentication message (e.g. the signature of the vote) that is sent to the infrastructure; using the authentication message and the server-side authentication credentials (e.g. a public key to verify the signature), the infrastructure authenticates the sender of a vote as a person with a right to vote. Client-side authentication credentials should be difficult to guess.

Let. s: In practice it should not be possible to generate a valid authentication message without knowledge of a client-side authentication credential.

Art. 3 Basic requirements for the authorisation of electronic voting per ballot

Introductory sentence, letters a and c: The wording of the provisions has been revised. In addition, the concept of verifiability has been added to letter a, as this is now required for the use of all e-voting systems according to Article 27*i* paragraph 2 of the draft PoRO.

Let. a: Concerns in particular compliance with the requirements in Articles 4–9 draft OEV.

Let. c: Concerns in particular compliance with the requirements in Articles 10–12 draft OEV.

Let. d: Addition to the existing provision with a new requirement for public access to information and public participation (in particular in accordance with Art. 27*m* draft PoRO and Art. 13 draft OEV). This addition underscores the importance of transparency and public involvement in e-voting. The information is prepared so as to address the target groups – the general public or specialist circles – appropriately.

Art. 4 Risk assessment

Para. 1: In order to obtain authorisation, the cantons must, as hitherto, prepare assessments of risks in their area of responsibility. A risk assessment must be drawn up for all risks pertinent to the fulfilment of the security objectives. Furthermore, risks affecting the administrative and public environment of e-voting also need to be assessed.

Risk assessments should also take into account public trust and acceptance of e-voting. This is an overarching objective and must be incorporated across all security objectives and risks. Practical examples:

- Example 1: In order to prevent any doubt about the correctness of the results, the process that defines how to proceed if the results are shown to be incorrect is described and communicated in detail.
- Example 2: In order to counteract the risk of a materially unfounded loss of confidence possibly resulting from the discovery of an insignificant flaw in the system, independent experts are consulted with regard to risk assessment and communication.

The assessment must be carried out according to a methodology that ensures all risks are identified, analysed and assessed. The details of the methodology used and the risk acceptance criteria specified by the canton must be documented. The risk assessments must be reviewed at least annually and whenever significant changes are made to the system. In addition, before each ballot, it will be ascertained whether new risks have arisen and whether existing risks have increased.

As part of its assessment of the situation, the FCh may draw up its own assessment of the risks in its area of responsibility. A risk assessment by the FCh is not a prerequisite for the cantons to obtain approval for the use of an e-voting system; however, it may be taken into account when deciding whether to grant approval. It is sent to the cantons for their information, so that they can take account of the FCh's assessment. The FCh considers the cantons' risk assessments when drawing up its own risk assessment.

The FCh provides the cantons with guidelines on how risk assessments must be carried out. The risk assessments must reflect the current situation in each case and incorporate the latest developments and findings.

Para. 2: In particular when an external system is used, the system operator or system manufacturer is now required to draw up its own risk assessment. For other service providers offering security-relevant services, such as a printing office, providers of technical aids for auditors (verifiers), or control components, the canton must ascertain whether the risk assessment can be conducted by the canton alone or whether an additional risk assessment by the service provider is necessary. The service providers draw up the risk assessments for submission to the canton. The latter takes them into account in its own risk assessment and submits them to the Confederation as part of the authorisation procedure.

Para. 3: Linguistic revision of the introductory sentence and of the security objectives in letters a–e. The security objective in letter f has been made more precise. The issue of vote-buying, for example, falls under this security objective.

Para. 4: Essentially the same as the previous paragraph 2. The need for explanation of why the risks are considered to be sufficiently low is now included in paragraph 1.

The original provision in paragraph 3 can be deleted, as Article 11 draft OEV requires the documents to be published in full; the provision is thus no longer required.

Art. 5 Requirements for complete verifiability

With complete verifiability, systematic malfunctions can be detected in the election or voting process that occur as a result of software errors, human error or deliberate attempts at manipulation while maintaining the secrecy of the vote. It is imperative that voters receive proof that their vote has reached the system unchanged and has not been manipulated – for example, by a malware program on the computer used. Irrespective of the system used, auditors can establish that all correctly cast votes (as verified beforehand by the voters) are also counted correctly – i.e. in accordance with the proof that the voters receive. Verifiability must be applied based on recognised cryptographic methods.

In future, only completely verifiable systems are to be approved. The requirements in former Articles 4 and 5 are incorporated, with some revisions, in Articles 5–8 of the draft OEV.

Para. 2: With individual verifiability, voters can detect any misuse of their voting rights. This should be possible even if the user device or the transmission path are not trustworthy. It must be assumed a priori that the user device or transmission path contains undetectable viruses or has been otherwise tampered with.

Para. 3: With universal verifiability, manipulations in the infrastructure can be detected. Unlike individual verifiability, it does not necessarily have to be offered to voters. Instead, auditors can be employed to apply universal verifiability. It must be possible to observe the auditing process. This means that the auditors should be able to understand the significance and the results of the individual steps in the voting process as far as possible. To this end, they must be able to witness that the steps in the process are correctly conducted as well as the test results, for example by going to the place of performance.

Art. 6 Soundness of the proof

No proof can confirm with absolute certainty that all votes have been correctly processed in accordance with the requirements in Article 5 paragraphs 2 and 3. Proof must therefore be interpreted in the light of its soundness. Article 6 sets out minimum soundness requirements on which persons interpreting proof must be able to rely. A high degree of soundness equates to a low degree of falsifiability. Clarifications as well as additional soundness requirements can be found in the Annex (Nos 2.9.1, 2.9.2 and 2.11).

Voters who benefit from individual verifiability should, on the basis of a verification reference sent by post, be able to rely on their vote having reached its destination with a high degree of probability, provided that the data for the verification reference were correctly generated and printed and that one of four control components is functioning correctly (see explanations in Annex No 2). If a voter does not believe that these conditions have been met, then the result of the proof validity check logically has no or only limited meaning for them, i.e. the proof would be 'not sufficiently sound' for this person.

For the soundness of the proof referred to in Article 5 paragraph 2 letters a and b, it must not be assumed that the voter's user device and the transmission channel function correctly. This means that the proof

must be shown to be sound even if a manipulated user device or a man-in-the-middle[9] manipulates the vote unnoticed. Thanks to the proof required by Article 5 paragraph 2, the voters can still notice if their vote has been manipulated.

Analogous for the soundness of proof in paragraph 3: The proof is sound if it enables the auditors to detect manipulations under the given trust assumptions. This prevents the attacker from misleading the auditors by using the non-trustworthy system components to fabricate evidence in order to justify a manipulated result. As long as the auditors are confident that one of four control components and the technical tool they use to check the proof (typically a laptop computer) are working correctly, then the proof is sound.

Art. 7 Preservation of voting secrecy and exclusion of premature results

To ensure voting secrecy and to exclude premature results, the system must be designed in such a way that at least three of the four control components would have to be brought under control for a successful attack after the vote has been cast. There are stricter requirements for the online system if it is operated by a private system operator. Further details can be found in the Annex (No 2.9.3).

Art. 8 Requirements for the trustworthy part of the system

The purpose of these requirements is to ensure that successful unauthorised access does not, as far as possible, confer an advantage when an attempt is made to access another control component undetected.

Art. 9 Additional measures to minimise risk

Corresponds, with some linguistic changes, to former Article 6 OEV.

Art. 10 Requirements for examination

In order to increase the effectiveness of the examinations and the independence between the examining body and the examined entity, the division of responsibilities between the Confederation and the cantons is adapted so that the Confederation assumes greater responsibility and a more direct role in examining the systems. The majority of the examinations are to be commissioned by the FCh in future (para. 1). In these areas, no further certification by bodies accredited by the Swiss Accreditation Service (SAS) will be required in future. The canton still ensures that an audit of the system operation is conducted at the system provider's computer centre (para. 2). Further requirements, such as the scope, responsibilities and timing of the examinations, are still set out in the Annex (No 26).

Para. 1 let. b: term changed to 'system software'. This examination includes the former examination under Numbers 5.2 (Functionality) and 5.4 (Control components) of the Annex. With the new formulation, the examination includes of both the software of the entire system and the control components.

Para. 1 let. c: The requirements for printing offices are now examined under the provision 'security of infrastructure and operation'.

Para. 2: The operation of the system in the system provider's data centre must be certified in accordance with ISO 27001. A canton that does not operate a system itself may have its cantonal processes certified in accordance with ISO 27001, but is not required to do so.

Para. 3: The canton and its service providers must give the FCh and the bodies appointed to conduct the examinations under paragraph 1 access to the necessary documents. This includes all documents required for the checks under paragraph 1 and all available reports (including certification reports), supporting documents and certificates (ISO 27001 certificate under paragraph 2 and any cantonal certifications).

[9] The attacker in a man-in-the-middle attack. This is a form of attack that is used in computer networks. The attacker stands either physically or – as is mainly the case nowadays – logically between the two or more network participants and, using their own system, has complete control over the data traffic between them and can view and even manipulate the data at will.

Para. 4: All examination results pertaining to licensing must be published. The body commissioning the examination is responsible for publishing the results. It must publish evidential documents and certificates drawn up in the course of the examinations referred to in paragraphs 1 and 2. Examination reports are also understood to be evidential documents. The published results must be clear and comprehensible. Any other documents referred to must, as a rule, be made available. If additional documents cannot be made public, a summary of the relevant aspects of the unpublished documents should be provided in order to ensure that the examination reports can be understood. If the examined entity responds to a report, this should also be published. Publication may be dispensed with in justified cases. Exceptions can be made if justified in the sense of laws on freedom of information and data protection. In each case, a balance must be struck between the public interest in publication and the interest in confidentiality. Confidentiality interests may include internal guidelines, the protection of internal matters or the protection of third party data.

Art. 11 Disclosure of the source code and of the documentation on the system and its operation

The existing requirements for disclosure of the source code and documentation relating to the system and its operation have been made more detailed. Paragraph 1 now contains a list of the documents that must be published. Explanation of some terminology:

Para. 1 let. a: The relevant parameters include all the information and data necessary to run the system on its own premises.

Para. 1 let. b: The software documentation includes the cryptographic protocol, the specification and design, instructions, test concepts, reports on flaws and corrections as well as the results of the review process.

Para. 1 let. c: Includes documents that explain how the system is operated for examination purposes (e.g. instructions, FAQs, etc.).

Para. 1 let. d: Includes the documents showing how the requirements of the OEV are met. This includes those documenting significant risk-mitigating measures referred to in the risk assessment. In principle, the more the documentation relates to the operation, maintenance or security of a trustworthy component or the handling of a data carrier containing critical data, the more important publication is. The exemptions relating to freedom of information also apply here.

Para. 1 let. e: The system operator is required to disclose any flaws in the published source code or documentation of which it is aware. It must describe the flaw and any measures planned to remedy it. This serves the purpose of comprehensibility, transparency and cooperation with the public.

Para. 2 let. c: Exceptions can be made if justified in the sense of laws on freedom of information and data protection. In addition, documents with little or no relevance to the security of the system and its operation do not need to be published in justified cases. These might include descriptions of operational processes without direct reference to the system or simply additional details that have little or no relevance to security or which it may be assumed have been implemented correctly. In such cases, a balance must be struck between the public interest in publication and confidentiality interests. Confidentiality interests may include internal guidelines, the protection of internal matters or the protection of third party data.

Art. 12 Publication modalities

Para. 1: The documents will be published via established platforms. The files should be organised in line with common practice, taking into account their size and complexity.

Para. 2: The published documents must be obtainable anonymously and interested persons must not be required by the source-code proprietor to register in order to obtain the documents. If a person is entitled to financial compensation under Article 13 of the draft OEV, the proprietor may ask for any information necessary to transfer it. Publication at least six months in advance of the planned deployment of the system is considered appropriate to allow for effective public review.

Para. 3: It must be possible to discuss with other persons and cite from published information, in particular for specialists involved in finding flaws.

Para. 4: In the sense of 'responsible disclosure', the proprietor may require participants to comply with the following rules:

- Errors must be reported to the proprietor immediately.
- A flaw should not be made public immediately; a certain embargo may not be exceeded.
- Information on suspected errors must be handled responsibly. Participants may not unnecessarily publicise any security vulnerabilities that are in the process of becoming apparent. Information about vulnerabilities may only be shared and discussed with people who are presumed to be able and willing to deal with the issue and who will do so responsibly.

Para. 5: The proprietor may only take action against violations of the terms of use in exceptional cases. It must point out the limitation of liability or the exclusion of liability to the participating persons in the terms of use. It may not require the user to give a declaration of intent.

Art. 13 Public involvement

The article regulates the principles of a bug bounty programme, a measure which implements Article 27*m* paragraph 1 of the draft PoRO. Where possible, the cantons should take further measures to create financial and non-financial incentives.

Para. 1: In principle, the cantons shall ensure that interested members of the public can submit suggestions for improving the system (bug bounty programme). The programme should be launched in advance of submitting a definitive application for the basic licence from the Federal Council. Around six months before the planned productive use of the system is considered reasonable. A bug bounty programme is designed to permanently search for flaws in the system (let. a) and involves a recurring internet test (let. b).

Para. 1 let. a: Search for errors in the published documentation or source code and by analysing the executable system in private infrastructure. This programme to identify errors runs continuously.

Para. 1 let. b: The sole objective of this so-called internet test is to penetrate the infrastructure. Denial-of-Service (DoS) and social engineering attacks may be excluded from the bug bounty programme. The internet test can be implemented either as a permanent programme or as a recurring test of limited duration.

Participation in the bug bounty programme is governed by the modalities set out in Article 12 of the draft OEV.

Para. 2: The system operator or an external company may be designated to run the bug bounty programme. This body implements the programme, receives suggestions, and handles communication with the person who submitted the suggestion. The person must be informed of any decisions regarding how suggestions will be dealt with and of any measures taken.

In addition, any information on suggestions received must be published. The following information is to be published: information on the content of the suggestion, indication of the source of the suggestion (if the person or institution providing it agrees), assessment of the body responsible for the bug bounty programme and information on any measures taken on the basis of the suggestion.

Para. 3: Information relating to security either directly or indirectly is to be rewarded, provided that it contributes to the improvement of the system. Suggestions that are indirectly related to security include, for example, those that improve the quality of the source code. This is because the quality of the source code affects readability and thus also influences the probability that errors can be found. The amount of financial compensation must be determined on the basis of the seriousness of the flaw. The amount should be chosen in such a way as to effectively create incentives for specialists among the public to participate.

The FCh legislation merely establishes the basic conditions for the bug bounty programme. The detailed design of the programme, e.g. defining categories for assessing the severity of the vulnerabilities and setting the amount of financial compensation, is the responsibility of the cantons or the system operator. As part of the licensing procedure, the Confederation examines the extent to which the objectives of the

bug bounty programme have been achieved by the procedure selected by the cantons and the competent authority under paragraph 2.

Art. 14 Principles governing the allocation of tasks and responsibilities

The tasks and responsibilities were previously regulated in the Annex. The division of tasks and responsibilities is now regulated in the main part of the OEV.

Para. 1: The important tasks to be carried out by the canton are set out in the provisions in the Annex. These include the design of the voting papers and communication with voters on issues related to voting in specific cases.

Para. 2: The canton may delegate the above tasks to external organisations. In doing so, however, it continues to bear overall responsibility under paragraph 1. For example, it bears the full risks associated with the performance of a task, even when this has been delegated. As an exception to paragraph 1, communication on matters relating to the functioning of the system may be delegated, provided that these matters are of a highly technical nature and require in-depth expert knowledge.

Para. 3: The operating bodies act on the instructions of the canton and assume responsibility for their tasks towards the canton.

Para. 4: Cantonal legislation determines how the auditors are organised and deployed.

Art. 15 Tasks of the body responsible at cantonal level

The tasks of the body responsible at cantonal level were previously regulated in the Annex. The tasks are now regulated in the main part of the OEV.

Let. a: The overarching information security policy defines the objectives, framework and responsibilities for information security. It also draws up a lower-level information security policy and establishes how this is to applied. It is communicated to all employees and must be reviewed and amended at scheduled intervals.

Let. b: The information classification and processing policy defines a binding security framework for the entire operation of the system. It is communicated to all employees and must be reviewed and amended at scheduled intervals.

Let. c: The risk management policy defines in particular the scope and boundaries for the management of information security risks, risk management organisation, the risk acceptance criteria and the method for carrying out the risk assessment. It must be reviewed and amended at scheduled intervals.

Let. d: Examples of measures: Conduct risk assessment, review compliance with information security policies, revise information security policies, provide appropriate tools.

Let. f: 'Critical acts and operations' include in particular preparation of the ballot (Annex No 5), the opening and closing of the electronic voting channel (Annex No 9), the counting of the votes cast electronically (Annex No 11) and the destruction of data after the results of the vote or election have been stored (Annex No 12.9).

Let. g: Cantonal legislation determines how the auditors are organised and deployed. The auditors undergo training including performing practical exercises.

Let. h: With further indicators, the number and type of anomalies reported by voters to the canton are be submitted to the auditors, in accordance with Annex No 11.10.

Art. 16 Evidential documents for the applications

Para. 1: Article 27*b* letter b of the draft PoRO having been amended, only the evidential documents for the application for authorisation are regulated here. The exact deadlines and further details are published by the FCh in a separate document in each case. The list of evidential documents has been adapted to

reflect the new provisions of the OEV. In addition, the list in the previous Number 6 of the Annex to the OEV has been included here so that only one list of evidential documents is kept.

Para. 1 let. a: Amended to reflect the new responsibilities in the examination under Article 10.

Para. 1 let. b:): Amendment of the previous provision on risk assessments under Article 4 of the draft OEV. The canton undertakes to draw attention immediately to any changes in risk assessments.

Para. 1 let. c: The canton submits evidential documents to confirm that the documents have been disclosed in accordance with Article 11 of the draft OEV. In doing so, it informs the FCh of the dates on which the documents were disclosed. It also submits information on the suggestions from the public. This includes a list of the suggestions received, the respective assessment by the canton or the competent body, the amount of financial compensation paid and a description of the measures taken on the basis of these suggestions.

Para. 1 let. d: Adoption of former Number 6.3 of the Annex to the OEV. The canton submits further test protocols if a test is carried out shortly before the ballot. If there are flaws in the system of which the canton or the system operator are aware, the FCh must be informed of these, their impact and any measures planned to rectify them.

Para. 2: The canton may refer to the validity of examination results or evidential documents from previous ballots. If it does so, the canton must explain why a repeat of the given examination is not necessary for the current ballot. In addition, it must provide details of all modifications to the system and to operating and maintenance processes carried out or planned up to the time of the ballot. In doing so, it must show that these are minor alterations that have no negative influence on the risk assessment. The term 'valid' is to be understood both in the narrow sense of validity (for example, the validity of a certificate) as well as in the broader sense (documents that have not been modified and do not need to be because, for example, there have been no changes to the system design, the state of scientific knowledge or the legal basis). When a canton refers to previous documents, it must give reasons for doing so and confirm that the documents provided are still valid.

Art. 17 Further provisions

Para. 2: In exceptional cases, a canton may be exempted from meeting individual requirements. This option is subject to the three conditions set out in letters a-c. In particular, there must be a clear justification for making an exception. An exception might be: in an election run using the first-past-the-post system, the requirement of individual verifiability can be waived if the vote is cast by entering a name in blank text field (‘write-in votes’).

5.2.2 Annex setting out the technical and administrative requirements for electronic voting

General remarks

The reference to the protection profile of the Federal Office for Information Security (BSI Germany, previous No 3.15) has been deleted as it is no longer maintained by the BSI and has been archived. The relevant requirements arising from the protection profile have been incorporated in existing requirements or in new requirements.

Explanations on selected provisions

No 1 Definitions

No 1.5: The voter compares the codes displayed on the screen with the codes in the verification reference.

No 1.6: Data by means of which it can be established whether voters have cast a vote are not covered by this provision.

No 2 Cryptographic protocol requirements for complete verifiability (Art. 5)

Electronic votes travel from the time they are cast to the time they are counted from the user device through the internet and via numerous servers of the system provider to the canton. The individual infrastructure elements used on this journey are numerous and difficult to control. Cryptographic protocols make it possible to reduce to a minimum the number of elements that an attacker would have to control in order to manipulate votes without being detected or violate voter secrecy. Measures to prevent an attacker from taking control of an element can therefore focus on a limited number of elements. These elements are particularly worthy of protection and, ideally, can also be protected particularly effectively.

Such elements – found under Numbers 2.1 and 2.2 'System participants' and 'Communication channels' – are referred to as 'trustworthy'. This may seem surprising at first glance: why is an element that is particularly worthy of protection called 'trustworthy'? The reason lies in the fact that cryptographic protocols are not aimed at protecting those elements. The designation 'trustworthy' signals to authors and readers of the document in which the cryptographic protocol is specified that they do not need to worry about possible attacks in which an attacker takes control of these elements. By being trustworthy, system participants “refuse” to cooperate with an attacker. The protocol must be defined in such a way that, as long as the trustworthy system participants adhere to the protocol, the attacker will not succeed even if they bring the remaining non-trustworthy system participants under control. The use of the term is based on the literature.

The cryptographic protocol consists of abstract instructions in mathematical form to all system participants about which calculations they must perform when receiving which messages, which data they must store, and which messages they must send over which channels. The protocol is compliant with the OEV if the attacker under Number 2.3, despite his control over the non-trustworthy system participants and communication channels in Numbers 2.1, 2.2 and 2.9, is unable to achieve the objectives in Numbers 2.5–2.8 under the conditions in Numbers 2.11 and 2.12. Under Number 2.13, secure cryptographic building blocks (e.g. encryption algorithms) must be used and the instructions to the system participants must be clear and not underspecified. Under Number 2.14 mathematical proofs of the protocol conformity are required, as is usual in scientific practice.

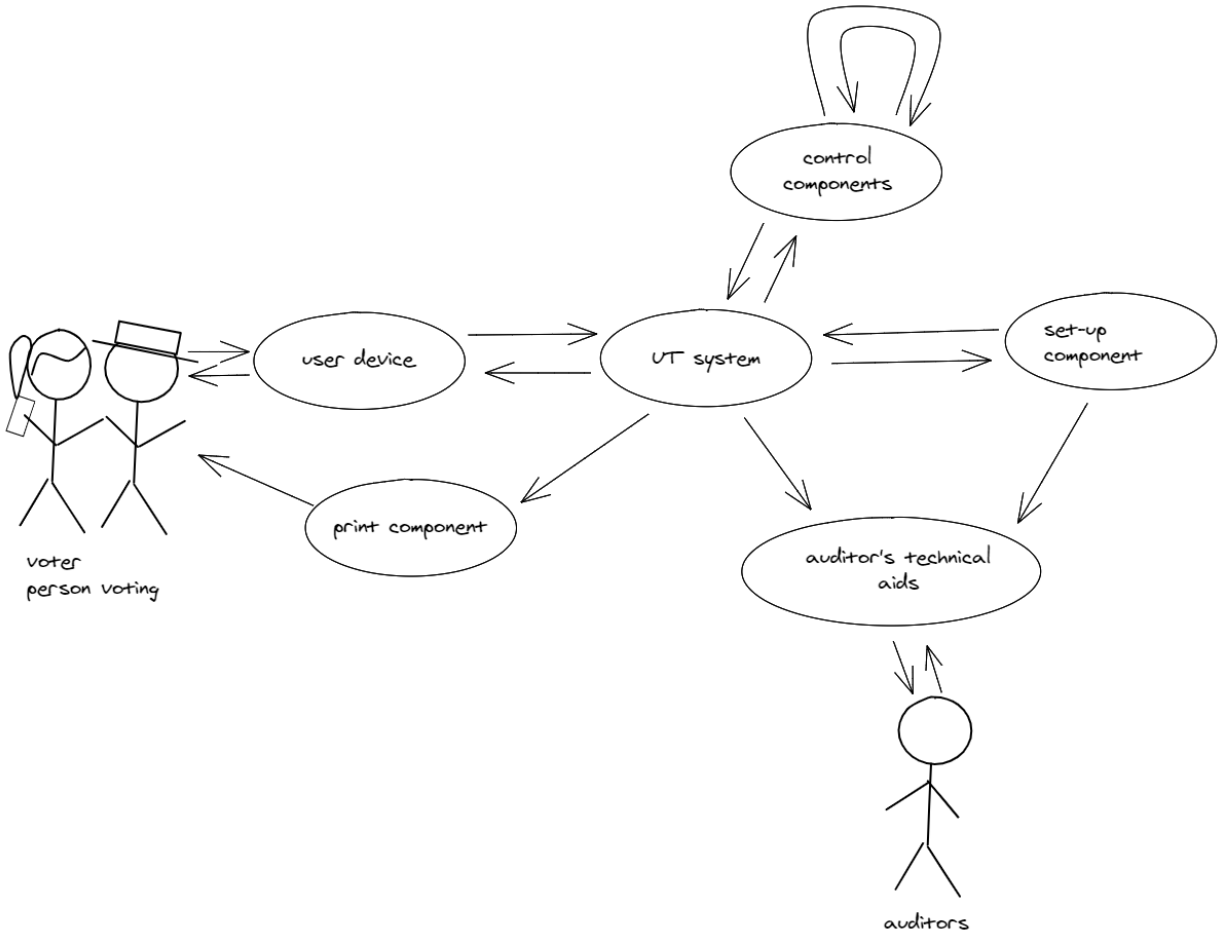
The cryptographic protocol is the basis for system development. It can only be effective if the instructions of the trustworthy elements are correctly implemented as software and the components on which the software runs are sufficiently protected. The OEV contains requirements on this. See also the explanations to Numbers 2.3 and 2.4.

No 2.1:

- Voter/person voting: Voters receive their confidential client-side authentication credentials and the verification reference by letter from the canton or from the printing office in advance of the ballot. To cast their vote, they enter their client-side authentication credentials and their vote via the user device. In order to make use of the individual verifiability under Article 5 with reference to Number 2.5., they check the evidence displayed to them on the user device against the verification reference.
- User device: The user device creates the authentication messages and sends them to the UT system along with the encrypted vote and other messages necessary to ensure verifiability. To do this, it uses the software, including public parameters, which it has received in advance from the UT system. It displays messages from the UT system to the voting person, e.g. the proof referred to in Number 2.5.
- Untrustworthy system (UT system): The UT system serves as a communication node between the other system participants. It must be considered not to be trustworthy with regard to all cryptographic protocol requirements (see No 2.9).
- Set-up component: The set-up component is operated in the canton's infrastructure (see No 3.1). The canton prepares data for the ballot using the set-up component. This includes data whose randomness and confidentiality are crucial to achieving the requirements for the cryptographic protocol set out in Numbers 2.5, 2.7 and 2.8, such as the voters' verification reference. This abstract term may also cover technical aids such as laptops and data carriers.

- One or more groups of control components: The control components interact with the other control components in their group in such a way that the cryptographic protocol requirements of Numbers 2.5, 2.6 and 2.7 are met even if only one of them is trustworthy and therefore functions correctly.
- Print component: It prints the verification reference for the voters. This abstract term includes packaging and mailing to voters. It also includes all the technical aids used in printing. The term can thus also include - in addition to the printer itself - a laptop for decrypting the print data and a USB stick for storing the encrypted data.
- Auditors: After tallying, the auditors receive a proof from the UT system in accordance with Number 2.6 which confirms that the results have been tallied correctly. They conduct the check at least once with a technical aid. During the setup phase, they can also use their technical aid to perform checks on behalf of the setup component.
- Auditors' technical aids: The auditors require a technical aid to assess the proof in accordance with Number 2.6.

No 2.2:



No 2.3: For the requirements on the cryptographic protocol, no distinction is made between attackers with different resources or expertise: Whether an attacker takes control of system participants via threats, hacking or social engineering is irrelevant for the definition of the cryptographic protocol. Instead, it is a prerequisite that the attacker has taken control of the untrustworthy system participants and communication channels. The cryptographic protocol must be defined so that the attacker cannot cause any damage despite successful attacks on such system participants and communication channels. An implicit prerequisite for this is the assumption that the attacker is not capable of breaking the cryptographic building blocks and their implementation in the source code. The requirements in Numbers 2.13 and 2.14 and requirements for quality in software development in Numbers 24 and 25 aim to achieve this objective.

No 2.4: If the attacker could control all system participants, there would be no one left who would be interested in whether manipulations had taken place. It is in the nature of elections and popular votes that a large proportion of those eligible to vote are interested in whether their vote has been properly received. These voters cannot be controlled by the attacker. They are therefore regarded as trustworthy. Similarly, individual auditors may be considered trustworthy. The attacker cannot bring them under his control either. Since voters and auditors work with technical aids, some of these technical aids must also be allowed to be considered trustworthy - otherwise the attacker could easily mislead trustworthy persons by taking control of all the aids, particularly those that the auditors use for their work. By only allowing technical aids as trustworthy system participants that can be particularly effectively protected in practice, it is especially difficult for an attacker to carry out manipulations unnoticed or to breach the voting secrecy. Technical aids that do not have to be connected to a network can be protected particularly effectively. Furthermore, it is possible to avoid having to trust individual technical aids by having their function performed by several technical aids. In order to gain value from this, the cryptographic protocol must be defined so that the attacker cannot do any damage unless he can take control of one of these devices. This follows the logic that not all auditors need to be trustworthy; it is sufficient for one auditor to point out a discovered flaw. The corresponding allocation of responsibilities can be seen in the groups of control components: An attacker would have to take control of all control components to be able to cause damage. However, this is particularly difficult when the control components differ in terms of software and operating modalities.

The permissible assumptions about the trustworthiness of the individual system participants and communication channels are listed in Number 2.9.

The requirements for the operation of trustworthy components are set out in Number 3.

At this point, a message is regarded as authentic if the message recipient can trust that the sender corresponds to the system participant specified in the definition of the channel.

No 2.5: The proofs can only be effective if the voters actually examine the proofs and if they contact the competent authority in the event of any doubt. The extent to which they do this and what measures could help to ensure that voters examine the proofs in accordance with the instructions could be the subject of research and scientific monitoring. Some requirements of the OEV could help to make the proofs an effective tool: for example, the division of the proofs into partial proofs in accordance with numbers 2.12.5-2.12.10 is intended to allow voters to stop the voting process before it is completed and cast their vote by mail or in person if they have difficulty confirming that their vote has been recorded correctly. In contrast to the previous partial proofs, the examination of the partial proof confirming the definitive vote must be particularly easy to carry out. The requirement in Number 8.10 is intended to discourage social engineering attacks aimed at preventing voters from examining the proofs properly. In addition, Number 8 imposes further requirements on providing information and assistance to voters. Social engineering attacks must be evaluated in the risk assessment under Number 13.

A correct proof confirms to the persons voting that at least the control component that may be considered trustworthy in accordance with Number 2.9.1 has registered the vote as being cast in conformity with the system. The auditors must establish, by examining the evidence referred to in Number 2.6, that the vote was counted correctly and therefore in accordance with the proof referred to in Number 2.5 that was shown to the voters. As a condition for the successful examination of the proof referred to in Number 2.6, all control components must have recorded the same votes as having been cast in conformity with the system. Cases where the control components show inconsistencies in this respect must be anticipated in accordance with Number 11.11 and the procedure determined in advance.

The provision does not prescribe how to interpret cases where a proof is displayed incorrectly or not at all. In particular, it is theoretically possible for the group of control components to register a vote as in conformity with the system even though it was not cast in conformity with the system. However, it follows from Number 2.6 that such votes must be sorted out at a later stage so that the auditors can establish whether the attacker has inserted votes that were not cast in accordance with the system. In addition, the UT system (not necessarily the group of control components) must, in accordance with Number 10, still detect such votes when they are cast and must not treat them as votes cast in accordance with the system.

Regarding '...the attacker did not improperly cast a vote on behalf of the voter which was subsequently recorded and counted as a vote cast in conformity with the system': such a proof would be of limited use

during the ballot, as the attacker would still have time to cast a vote. Therefore, it is sufficient if voters can request this proof after the ballot. For reasons of efficiency, it is sufficient for the competent cantonal office to confirm to the voter that no vote has been cast on their behalf. The assumptions of trustworthiness set out in Number 2.9.1 apply to the examination by the competent body, and the auditors' technical aids may also be considered trustworthy. Furthermore, the requirement breaks the trust model, in that the attacker must not be able to access the client-side authentication credentials at all. With regard to the present requirement, the assumption must be made that the attacker has access to the client-side authentication credentials of individual voters.

No 2.6: a vote is deemed to be cast in conformity with the system only if the client-sided authentication credential used corresponds to a server-sided authentication credential that was adopted and "assigned" to a voter in the preparatory phase of the ballot. The proof must therefore include confirmation that no unallocated authentication credentials for casting votes have been issued. In addition, during preparations for the ballot, the control components or the auditors must have been given corresponding data as the basis for making a comparison. The auditors must ascertain that the number of authentication credentials corresponds to the (official) number of authorised voters. In this event, the authentication credentials may be deemed to have been "assigned" to a voter. However, this does not guarantee that the client-sided authentication credentials for a trustworthy voter have not been misused to cast a vote in conformity with the system. However, according to Number 2.5, voters must be able to establish this.

No 2.7.3: It may be assumed that the manipulation of the server-side software has no effect on the trustworthiness of the user device during the verification.

The ability to protect user devices from misuse is much weaker than for components in a protected environment. However, it is a conscious decision not to use the cryptographic protocol to guarantee the secrecy of the vote and the absence of premature results. This takes user-friendliness into account. However, the protocol should provide protection where votes are centrally stored. The designation of the user device as "trustworthy" signals that no attacks on the user device need be considered in the development and analysis of the cryptographic protocol (see introductory explanations to Number 2).

No. 2.9.3: One implication is that the key needed to decrypt the votes must be split among four different control components. At least one of these control components must be operated by the canton (expressly stated in No. 3.1).

A significant proportion of voters must count as untrustworthy in order for the UT system to find out the content of a vote cast in collaboration with an untrustworthy voter. In particular, it must be ensured that the voter cannot externally modify and cast as his or her own an encrypted vote that has already been cast, with the aim of finding out what the vote is using the proof that he or she receives during the examination in accordance with Number 2.5.

An attacker could attempt to use the untrustworthy system participants to mark votes before they are counted and then use the decrypted votes to breach voting secrecy. The auditors may find after tallying that the votes were not processed as they were registered, but in marked form. By this time, however, voting secrecy would already have been breached. This must be prevented by having trustworthy components ensure that no marked votes are processed before tallying. In view of this objective, a technical aid used by the auditors may also be considered trustworthy.

For the designation of the user platform as 'trustworthy', see the explanation on Number 2.7 (second paragraph).

No 2.11.1: An implication of this provision is that a proof must be able to assume at least 1000 different values (for example, in the case of a numeric code, all values between 000 and 999). Thus, the probability of an attacker correctly guessing a proof would be exactly 0.1 per cent. By gathering information about the untrustworthy system participants and communication channels, he could gain an advantage so that he would not have to guess the code blindly, thus increasing the probability. With regard to such cases, a code must be able to assume sufficient values a priori so that the probability does not exceed 0.1 per cent.

No 2.11.3: As an example, assume that the probability for the attacker is 1 per cent. In this case, it must be possible to repeat the tallying steps such that the probability after repetition is lower than 1 per cent. Further repetitions should make it possible to reduce the probability as far as necessary.

No 2.12.4: With this declaration, the vote is not yet definitively cast. First of all, the person voting must be able to verify the correct transmission using a first partial proof. Thereafter, the person voting must be able to cancel the vote and cast the vote via a conventional channel.

No 2.12.5: It is not permissible to have voters make a check for purely psychological reasons if the result of the check is irrelevant to the assessment of whether the vote has been manipulated.

No 2.12.8: In the case where two partial proofs are used to meet the requirements of Number 2.5, the penultimate partial proof is equivalent to the first partial proof. Furthermore, it can be deduced from Number 2.8 that together with confirming their intention to submit the vote pursuant to paragraph 2.12.8, voters must enter a secret element that has not yet been entered into the user device. The secret element can also be regarded as a client-side authentication credential.

No 2.12.11: Set-up components and printing components are generally intended for use in preparation for the ballot. Use at a later date, for example, is not prohibited at this point. However, it should not be possible to process votes or other data that only arise during the voting process on the assumption that these components are trustworthy. If the components are used to process such data, then they may not be regarded as trustworthy.

No 3 Requirements for trustworthy components in accordance with Number 2 and their operation

Here, requirements are specified for the components that are assumed to be trustworthy according to the cryptographic protocol in order to meet at least one of the requirements in Numbers 2.5–2.8. These may be the following components:

- Set-up components
- Print components
- Control components
- Auditors' technical aids

No 3.1: This includes the set-up (operating system, runtime environment, e-voting software), checking the correctness of the files with the e-voting software, updating, configuring and securing. See also the comments on Number 2.9.3.

No 3.4: The concrete organisation and procedure of auditors is governed by cantonal law (see also the explanations on Art. 27*m* para. 4 E-VPR).

No 3.7: This refers not only to the software for electronic voting but also to the software for the infrastructure, such as operating systems.

No 4 Voting procedure

No 4.10: In particular, the soundness of the proof may in this case be dependent on the trustworthiness of the user device. Thus, for example, the verification reference may be scanned in prior to voting. These facilities may only be offered to a small group of voters who are unable to interpret the proof otherwise. In principle, voters to whom this does not apply should be encouraged to examine the proof according to the intended procedure.

No 4.11: Voters are required to report to the competent cantonal authority if proofs are incorrectly displayed or if they are unsure about this. Voting by post or in person remains an option if an electronic vote has not yet been received. In order to assess this, the cantons have functionality at their disposal in accordance with Number 11.6.

No 4.12: Confirmation of the definitive vote in accordance with Number 2.12.8 must be made using a secret element that has not yet been entered into the user device. An E-ID may in some circumstances be used as a substitute for this secret element. This would have to be based on a risk assessment. However, an E-ID cannot replace the postal delivery of the verification reference. For the time being, postal delivery of the voting papers will remain necessary.

Furthermore, the provision that the permissibility of using an e-ID must be examined on the basis of a risk assessment applies even if the e-ID is issued by the state or is state-approved.

No 7 Requirements for printing offices

In future, the requirements for printing offices will no longer be regulated in a separate list of requirements, but directly in the Annex. These provisions apply in particular in addition to the provisions in Number 3.

No 7.4: For example, the data carrier and the secret element for decryption must be stored separately in a secure location (e.g. a safe). The person who has the secret element to decrypt the data must not be able to open the safe unnoticed. The decryption and processing of the data as well as the printing process are carried out by two persons. It must be impossible for the data to be unencrypted on a component without at least two people monitoring the component.

If the two persons cannot seamlessly supervise the processing of critical data, for example as a result of an extended interruption, the data must be destroyed.

No 7.6: If there are good reasons, data destruction may be postponed at the latest until the legal requirements regarding storage and traceability have been met.

No 8 Information and instructions

No 8.10: Voters must know the correct procedure for voting in order to be protected against social engineering attacks. By sending out the instructions by letter and advising them to follow these instructions in case of doubt and to contact the competent cantonal office if necessary, the authorities make social engineering attacks more difficult. The effectiveness of this approach, as well as alternative approaches for instructing voters, could be the subject of research and scientific monitoring.

No 10 Conformity check and storing finalised votes

Only votes cast in accordance with the system may be filed for tallying. This functionality can also be ensured by using a non-trustworthy component in accordance with Number 2.

No 11 Tallying votes in the electronic ballot box

No 11.1: Decryption in accordance with Number 11.2 must take place on the day of the vote. Earlier decryptions performed at the system provider may already start as soon as the electronic voting system has been closed. The effectiveness of the encryption must remain high despite the upstream decryptions.

No 11.2: If another canton's system is used, decryption and tallying may also take place at the canton providing the system.

No 11.6: It is not possible to decide whether a vote cast by post or in person is a double or even multiple vote by using only the votes cast electronically as a basis for comparison. Nevertheless, the functionality under Number 11.6 falls within the scope of the OEV. However, it is not necessary to specify the functionality by reference to trust assumptions under Number 2.

No 12 Confidential data

No 12.9: For system components whose trustworthiness is decisive for the preservation of voting secrecy under Number 2.9.3 in particular, it must be ensured that the data have been irretrievably deleted.

No 13 Threats

The security objectives (see Art. 4 para. 3) cannot be achieved with one hundred per cent certainty. In every case it is possible to identify security risks. Based on a methodical risk assessment (Art. 4 para. para. 1), it must be demonstrated that any security risks there may be are sufficiently limited.

A risk can be identified by identifying threats to and vulnerabilities in the system. A risk arises if a vulnerability in the system can be exploited by a threat and therefore the fulfilment of a security objective is potentially jeopardised. Security measures are used to minimise risks. Security measures must meet the security standards at the levels of infrastructure, functionality and operations to the extent that the identified risks are adequately minimised.

The list of threats has been adapted in line with new findings from recent years and the use of completely verifiable systems. A new definition and new terms for actors in threats has been introduced to clarify the scenarios.

No 13.12: The protocol requires that voters examine the proofs in accordance with Number 2.5. In accordance with the provision, the risk must be assessed that an external attacker might alter the information provided by the canton in order to induce voters to deviate from the steps to be followed for the examination. The aim is not to address false information that could be spread on social networks.

Nos 13.13, 13.14 and 13.15: An electronic means is understood here as a means that allows access to important information without the attacker having to be physically present. For example, it may be a form of malware.

A physical means is understood here to signify a means that allows the attacker to gain access to important information by personally going to the site.

Social engineering refers to an approach by which an attacker gains access to important information by misleading a person into providing the desired information directly or into granting access by physical or electronic means.

Nos 13.16, 13.17 and 13.18: The cryptographic protocol defines certain parameters, algorithms and processes. The threats mentioned here would exploit a vulnerability in one or more of these elements.

No 14 Identifying and reporting security events and vulnerabilities; managing security events and enhancements.

E-voting systems must allow for the effective detection and investigation of incidents such as suspected vote tampering or system attacks. The content and scope of the logs must be defined to ensure this. Voting secrecy must be guaranteed.

In addition, a continuous improvement process must be defined for detecting and investigating incidents. The following aspects should be taken into account in particular:

- There should be an open dialog between the Confederation, cantons and system providers.
- Regular analyses will be conducted of the suitability of the bases for monitoring and investigation. The scenarios defined in the crisis agreement will be taken into account in these analyses. Improvements can be made more efficiently by involving IT forensic experts in these analyses.
- Findings from the analyses will influence improvements in the instruments and processes.

No 14.2: The audit, identification and authentication processes are particularly sensitive and require special monitoring both in the part of the system operated by the canton and in the part operated by the system provider. Identification is the process of identifying a person, for example with a user name or a smart card. Authentication is the process by which the system can ensure access authorisation. This is done, for example, by verifying a password.

No 14.7: The objective is to establish that votes are correctly processed and tallied. For this purpose, the control votes are processed according to the same procedures as the votes cast in conformity with the system. Control votes must not be reflected as votes cast in accordance with the system in the final result.

No 14.10: This provision does not necessarily apply only to the online system. Components in the pre- or post-ballot process may also be affected.

No 15 Using cryptographic measures and key management

No 15.3: Encryption at the level of the software, the need for which results from Number 2, is not sufficient to meet this requirement.

No 17 Testing the system

No 17.2: Interfaces are those elements that enable the software to exchange information with the environment. These may be graphical interfaces, command lines or technical interfaces (API).

No 17.3: This requirement considers two levels of software structure:

- A module is the lowest level and represents a grouping of classes in the source code that work towards the same, clearly defined goal.
- A subsystem is a collection of modules that covers a system functionality, such as the administration of a popular vote, the issue of a polling card, or the registration of a vote.

No 24 Developing and maintaining information systems

The quality of e-voting systems must be guaranteed throughout the development process. In order to improve quality assurance, the requirements were specified with the following objectives:

- It must be possible to trace and verify any changes to the system.
- It must be possible to ensure traceability between the individual elements of the documentation (protocol, specification, architecture, etc.) and the source code, at all times and in both directions.
- The results of test processes flow back into the development.
- Conformity with legal requirements is ensured and maintained throughout the entire life cycle.

In particular, the requirements of Common Criteria Level EAL 4, which previously applied to control components, are extended to the entire system. In addition, they have been supplemented with requirements from Common Criteria above EAL 4, where this makes a significant contribution to the security objectives and is in the spirit of the above objectives.

No 24.1: The development tools considered here are the tools that are important for the security of software development. These include IDEs, build tools, and configuration management tools. They are also configuration options that may have an impact on the security of the development.

As in Number 17.2, 'interfaces' are understood as those elements which enable the software to exchange information with the environment. These may be graphical interfaces, command lines or technical interfaces (API).

A configuration list is a unified set of configuration items that represents the state of the software and its documentation at a particular point in time. Ideally, it allows a past version of the software to be reconstructed.

No 24.3: Correct preparation of the system from source code to its installation in production (build and deployment) must be ensured. For this purpose, the system provider must use a proven and traceable build and deployment method that is used to achieve the following objectives:

- The build and deployment method ensures that the deployed software conforms to the published, examined and approved version (traceability).
- Moreover, the build and deployment method will help prevent the manipulation of system components as much as possible.
- The introduction of vulnerabilities into the system through the software development tools and libraries that would make the system vulnerable must be avoided.

New requirements have been introduced for this purpose. They are based on the Colorado State Guidelines for the Use of Electronic Voting Systems,[10] the Trusted Build documentation published by GitHub[11] and the Reproducible Builds documentation[12] of the project of the same name.

No 24.4: Users are all persons who come into contact with the software in any way. This may include cantonal employees, voters, testers and ultimately anyone with an interest in the system.

In order for the developer to deal with reports on flaws appropriately and communicate effectively in this area, it is important that users know how to submit reports on flaws to the developer and how to register with the developer to receive related information.

Collecting reports of as many suspected vulnerabilities as possible and addressing them systematically should help improve system security. These requirements are complementary to the disclosure of the source code (Art. 11-12 draft OEV) and the bug bounty programme (Art. 13 draft OEV).

No 25 Quality of the source code and documentation

The quality of the source code and documentation is a key element in the security of e-voting. In the previous legal provisions, appropriate requirements were laid down. However, these included rather general concepts, such as preparation and documentation according to best practices and the implementation of certain points of the Common Criteria. The previous quality criteria have therefore been made more precise. Clear criteria should ensure the high quality of e-voting systems, which in turn will benefit security by facilitating audits by all stakeholders as well as the public. In order to define these quality criteria, a quality model for e-voting systems has been created. This model is based on the ISO 25010 standard and McCall's quality model.[13] The criteria were selected according to their contribution to the defined security and quality objectives.

No 26 Examination criteria for the systems and their operation

The responsibilities have been adapted to guarantee the effectiveness and credibility of examinations. The division of tasks between the Confederation and the cantons will be adapted so that the Confederation assumes more responsibility and a more direct role in examining the systems.

The Confederation is now responsible for examinations to check compliance with the requirements relating to the system and the underlying processes. This should also help to ensure that the findings from the review are incorporated in a targeted manner as the trials continue. External experts are to be appointed to conduct the examinations.

The canton and/or the system provider remains responsible for audits relating to the operation of the system in its data centres (ISO 27001 certification).

No further certification by bodies accredited by the Swiss Accreditation Service (SAS) will be required in future.

[10] Colorado Election Rules [8 CCR 1505-1] Rule 1. definitions, 2020 and Colorado Voting Systems Trusted Build Procedures, 2020

[11] GitHub How to: Trusted builds, 2017

[12] https://reproducible-builds.org/

[13] FACTORS IN SOFTWARE QUALITY - Vol. 1: Concept and Definitions of Software Quality - Jim A. McCall, Paul K. Richards, Gene F. Walters (1977)