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 its entry into force on 1 July 2022

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 on Political Rights (PRA; SR 161.1), Articles 27*a*-27*q* of the Ordinance on Political Rights (PoRO; SR 161.11) and the Federal Chancellery (FCh) Ordinance 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.

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.

The Federal Council subsequently 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. At the same time, it instructed the FCh to work with the cantons to redesign e-voting trials,[1] 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

Following a wide-ranging dialogue with the academic community, the Confederation and the cantons drew up a final report containing a comprehensive catalogue of measures. The Steering Committee Vote électronique (SC VE) adopted this final report on 'Realignment and resumption of trials' on 30 November 2020.[2] The need for action identified in the four objectives set by the Federal Council will be met by implementing the agreed measures. The measures are to be implemented gradually. A first stage involves implementing measures for the resumption of the trials. This should allow limited trials to be conducted again, while work is ongoing to implement the medium to long-term objectives.

At its meeting on 18 December 2020, the Federal Council took note of the final report of the SC VE. It instructed the FCh to work with the cantons to gradually implement the measures required for the redesign and to submit a bill for consultation containing the necessary amendments to the PoRO and the 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.[3]

The consultation procedure for the partial revision of the PoRO and the total revision of the OEV as part of the redesign of the trials began on 28 April 2021 and lasted until 18 August 2021. 25 cantons, 1 commune, 8 political parties, 29 organisations and various private individuals submitted opinions in the consultation procedure. The majority welcomed the main features and objectives of the redesign. The focus

[1] Federal Council media release, 27 June 2019; available at www.bk.admin.ch > Political Rights > E-Voting > Media releases.

[2] The final report and all the documents on the dialogue with the academic community are published on the FCh website: www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

[3] Federal Council media release dated 21 December 2020; available at www.bk.admin.ch > Political Rights > E-Voting > Media releases.

on the further development of the systems, effective control and oversight, the strengthening of transparency and trust as well as closer cooperation with the academic community met with widespread approval, as did the stronger role of the Confederation in the independent examination of the systems and their operation. However, fundamental questions were also raised, in particular about the responsibilities of the Confederation, the cantons and the system providers and about the obligation to disclose e-voting systems under an open source licence. The opinions submitted and the report on the results have been published.[4]

At its meeting on 10 December 2021, the Federal Council took note of the results of the consultation procedure and instructed the FCh to finalise the ordinances, taking account of the detailed feedback on the individual provisions, so that the cantons can relaunch the trials.[5] The fundamental reservations expressed in the consultation procedure are to be taken into account in the medium to longer term in the form of the catalogue of measures to be carried out by the Confederation and the cantons that is set out in the SC VE's final report of 30 November 2020.

2. Overview of the 2022 revision of the legal provisions

The revision of the legal provisions in 2022 comprises a partial revision of the PoRO and a total revision of the OEV and its annex, both of which will come into force on 1 July 2022. These amendments are the first stage in implementing the measures for the redesign of e-voting trials.

The key points of the revision are:

- **Continuation of trials:**
  E-voting will continue in the form of trials. 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. The procurement of the systems also remains the responsibility of the cantons and they can operate their own system as before, use the system of another canton or engage a private company (Art. 27*k*^{bis} let. b PoRO). The Confederation continues to set the regulatory framework and to be responsible for licensing.

- **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, as well as considering potential for future improvements. With the current revision, most of the examinations will no longer be carried out on behalf of the cantons or the system operator, but on behalf of the FCh.

[4] Available in German, French and Italian at www.admin.ch > Bundesrecht > Vernehmlassungen > abgeschlossene Vernehmlassungen > 2021 > BK. The report on the results in English is available at www.bk.admin.ch > Political Rights > E-Voting > Federal legislation.

[5] Federal Council media release dated 10 December 2021; available at www.bk.admin.ch > Political Rights > E-Voting > Media releases.

- **Transparency, public involvement and cooperation 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 will have access to all system, operational and examination report information and participation will 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 will be specified and there will be a mandatory bug bounty programme. The latter will involve financial compensation for valuable input from the public.

3. 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. The Federal Council believes that it makes sense for the Confederation to contribute to the development costs and is therefore in favour of this taking place via Digital Public Services Switzerland (DPSS). An initial request to provide the additional funding has been granted by DPSS under the current implementation plan, which runs until 2023.

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.

4. Explanation of the individual provisions

4.1 Political Rights Ordinance (PoRO)

Art. 27b let. b

A two-stage licensing procedure applies to e-voting trials: the cantons require a basic licence from the Federal Council, which is granted for several ballots or for the National Council elections (Art. 27*a* PoRO); in addition, authorisation by the FCh is required for each ballot (Art. 27*e* PoRO). The Federal Council may only grant a basic licence if the requirements for authorisation set out in the OEV are met. Compliance with these requirements is checked by the FCh as part of the authorisation procedure. Accordingly, the basic licensing procedure always includes an authorisation procedure. In order to clarify the relationship between the basic licensing procedure and the authorisation procedure, reference is made in letter b to the fulfilment of the conditions for authorisation. This amendment simply provides a clearer explanation of the existing procedure, and is therefore 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 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 – i.e. the percentage of voters – 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 limits set out in Article 27*f* paragraph 1 of the PoRO.

Art. 27e paras 1-2

As in the previous trials, authorisation from the FCh is required for each ballot. Since the Federal Council grants the basic licences for several trials (with the exception of the National Council elections), the FCh checks whether the requirements are met for each trial. The authorisation requirements are regulated in the OEV.

Paras 1 and 1bis: The paragraphs comprise the former 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: Previously the setting of limits 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.[6] 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 a 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. If, due to the national limit, not all requesting cantons can be granted a basic licence, the granting of basic licences to cantons

[6] To date, the highest percentage 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.

that regularly conduct trials takes priority over basic licences for cantons conducting trials for the first time. Thus, the continuity of electronic voting in cantons that have already used e-voting and are requesting a basic licence to be renewed is given priority over the use of e-voting for the first time.

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 public trust in e-voting. The FCh may initiate a review of this type on its own initiative or if requested by the cantons. 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: Former 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. The cantons are responsible for implementing the exceptions. With regard to the design and operation of e-voting systems for persons with disabilities, the cantons should involve experts in the fields of disability policy and accessibility wherever possible.

Art. 27i Subject heading and paras 1 and 2 Verifiability and plausibility of electronic voting

Article 27*j* PoRO requires electronic voting to be reliable. Article 27*i* PoRO regulates verifiability of the correct processing of the votes and of the correct result, and the plausibility check. The former 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 PoRO excludes the possibility of admitting the entire electorate in the next trial phase, the wording must be adapted. In addition, the order in the subject heading and in paragraphs 1 and 2 is adjusted so that the verifiability is dealt with before the plausibility check.

Para. 1: 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.

Under the former provision, complete verifiability was required if the whole electorate was included in the trials. Complete verifiability is now required, irrespective of the proportion of the electorate admitted.

Para. 2: 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, the results can be compared with votes cast by post and in person at the ballot box, the counted electronic votes can be compared with the log files on the voting server, or can be checked against control votes cast, for example, by voters' representatives. Where available and as far as the data corpus allows, statistical methods are to be used in the trials. In the final report from the SC VE, the Confederation and the cantons agreed to further develop the plausibility checks of e-voting results.[7]

Paragraphs 3 and 4 remain as they were before.

[7] See Measure B.8 in the final report of the SC VE dated 30 November 2020, available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

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 examination is required. See also the provisions on the timing of examinations in paragraph 26 of the Annex to the OEV.

Para. 2: The objects of the examinations are basically the same as in the previous provision. The previous term 'security requirements' now applies to all FCh requirements. In terms of content, this corresponds to the previous approach. In addition, the examining body must be independent of the examined body.

Paras 3 and 4: The FCh Ordinance specifies the details of the examination, the intervals at which examinations are conducted, the requirements that the examining entities must meet, and the responsibilities involved. Following the revision of the legal provisions in 2013, e-voting systems had to be examined in most cases by accredited external entities. 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. Experiences from 2019 have shown that the previous requirements in relation to system and process reviews have not been effective. Disclosure of the source code and a subsequent independent evaluation revealed significant security flaws that had not been detected by the previous evaluations and certifications. To ensure the effectiveness and credibility of the evaluations, the responsibilities and the design of the system examinations are adjusted.[8] Independence between the evaluating body and the evaluated body plays an important role in the adjustment of responsibilities. The division of tasks between the Confederation and the cantons is therefore adapted so that the Confederation assumes more responsibility and a more direct role in evaluating the systems.

Art. 27l^{bis} Public availability of information on the system and its operation

Para. 1: 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.

Para. 2: The key measure here is the disclosure of the source code and the associated documentation (letters a and b). The former Articles 7*a* and 7*b* OEV already required 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. Based on letter c, the documentation of the development process will also be disclosed. The development process is understood here as all the processes for the development and delivery of the source code, together with its control mechanisms. The requirements for the development process are set out in Numbers 24.1 and 24.3-24.5 of the Annex to the OEV. In particular, they cover the life cycle, development tools, development methods, change management, configuration management and reliable and traceable compilation and deployment. However, they do not include the products resulting from these processes (such as change requests, configuration lists or the commit history). According to letter d, a document is now also published confirming that the published source code is also the one used by the system when it is in operation.

The principles of transparency and comprehensibility are important and related provisions will now be included in the PoRO. The published information is intended to encourage input from experts. 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.

[8] See Measure B.1 in the final report of the SC VE dated 30 November 2020, available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

Para. 3: Publication may be dispensed with in justified cases. If overriding public or private interests are compromised by publication, consideration should be given to whether an alternative form of publication is possible (e.g. redacting certain passages or summarising the contents). Publication may only be dispensed with if there is no alternative form of publication that protects overriding interests. In this context, the overriding interests should be based on the interests that serve as the basis for the exceptions provided for in the freedom of information and data protection legislation. In such cases, a balance must be struck between the public interest in publication and public and private interests in confidentiality. It can be assumed that the public interest in transparency, especially on security-related issues, is high. Confidentiality interests may include internal guidelines, the protection of internal matters or the protection of third party data.

Art. 27l^{ter} Public involvement

Para. 1: In order to involve the public and experts, the FCh and the cantons implement measures such as organising conferences, idea competitions and hackathons, running information platforms and organising citizen science projects. In addition, one of the FCh's tasks is to explain the concept of verifiability. The cantons are responsible under Article 27*m* paragraph 1 for explaining how verifiability works.

Para. 2: The cantons are responsible in particular for providing experts from the public with incentives to help improve the e-voting systems. This includes, for example, running a bug bounty programme (Art. 13 OEV).

Art. 27m Provision of information to voters and publication of the results of electronic voting

Para. 1: The wording of this paragraph 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 how verifiability works 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. 2: 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 is sufficient if procedures and processes can be observed, for example, by an electoral office appointed by the competent authority, as this is usually composed of persons who are entitled to vote in the canton. 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. 3: 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. Publication may be dispensed with if no alternative form of publication is available that guarantees that voting secrecy will be preserved.

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, reviewing and advising on the user-friendliness and accessibility of the system 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. Letters a and b could include, but are not limited to, research on the following:

- Requirements for trust and acceptance
- Use of the electronic voting channel
- Improving verifiability
- Formal methods for formulating requirements and system specifications
- User-friendliness and accessibility

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

Para. 4: Previous paragraph 3.

4.2 Federal Chancellery Ordinance on Electronic Voting (OEV)

4.2.1 Main part

Art. 1 Subject matter

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

Art. 2 Definitions

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

Explanation of individual definitions:

Let. a: 'Conducting electronic ballots' also includes the preparation and follow-up work, insofar as this work relates specifically to electronic voting. Conducting the ballots does not include administrative processes in advance, such as any procedures for registering voters so that they receive voting documents for electronic voting.

The system includes:

- The functionality of being able to import the electoral register data needed to conduct electronic ballots.
- The infrastructure for printing the voting papers specially designed for electronic voting.
- Components with special functions that are important for the verifiability of e-voting. These are control components, set-up components, print components and the technical aids used by the auditors.

The system does not include maintaining of the voting register, as this does not specifically concern electronic voting, and the software for combining the partial results from the different voting channels.

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: A cryptographic protocol must ensure that in the event of malfunctions or even attacks, vote manipulation (altering, adding, deleting) can be detected even if only one control component per group is functioning correctly. Likewise, voting secrecy must be preserved even if only one control component per group is functioning correctly. The details are set out in Articles 5-8, Annex Number 2 and the detailed explanations. Annex Number 3 contains provisions for the technical implementation and operation of the control components, which are designed to ensure that, as far as possible, all control components of a group actually function correctly. The more control components that are used in a group, the more they differ in their technical implementation, the more independently they are operated from each other and the better they are protected against attacks, the greater is the probability that at least one of them will function correctly.

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 2 PoRO (see also the associated explanations). Cantonal legislation determines how the auditors are organised and deployed.

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

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

Let. s: Covers an ISO 27001 certificate, for example.

Art. 3 Basic requirements for the authorisation of electronic voting for the individual ballots

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 1 PoRO.

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

Let. b: When implementing this provision, particular care must be taken to ensure that the system is designed in such a way that the needs of persons with disabilities are taken into account (Art. 27*g* para. 1 PoRO). For this purpose, the e-voting portal must be barrier-free and – with the exception of Chapter 2.4 – comply with the eCH-0059 Accessibility Standard; this needs to be confirmed by a competent body (see Annex No 25.7.3; Conformity test in accordance with Annex No 26.2.1). Suggestions on improving the system in relation to accessibility can be submitted on the basis of Article 13 paragraph 1 OEV. Furthermore, the PoRO provides that facilitations for people with disabilities may be permitted when implementing the requirements, provided that security is not significantly restricted as a result (see Art. 27*g* para. 2 PoRO).

Let. c: Concerns in particular compliance with the requirements in Articles 10-12 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*l*^{bis} und 27*l*^{ter} PoRO and Art. 13 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 experts – 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: A description is provided of the process that defines how to proceed if the results of a vote or an election are shown to be incorrect (e.g. using the auditors' technical aids; see Art. 5 para. 3 let. b OEV). This is to avoid possible doubts about the correctness of the voting and election results.

- Example 2: Even if insignificant flaws are discovered, there is a risk that public trust will be affected. To counteract this, independent experts can be called in to classify any flaws that are discovered (assessment of flaws, communication).

The risk assessments must be carried out according to a methodology that ensures all risks are identified, analysed and evaluated. 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 former 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 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 trustworthy part of 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 OEV.

Para. 2: With individual verifiability, voters can detect any deliberate or inadvertent 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. The vote as entered by the person voting on the user device always corresponds to the intention of the person voting unless the voter has made an error when entering it.

Para. 3: With universal verifiability, deliberate or inadvertent manipulations (changes, additions, deletions) 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 proofs

No proof can confirm with absolute certainty that all votes have been correctly processed in accordance with the requirements of Article 5 paragraphs 2 and 3 OEV. Proof must therefore be interpreted in the light of its soundness. Article 6 OEV 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 of the OEV (Nos 2.9.1, 2.9.2 and 2.11). The criteria listed in Article 6 letters a-c are exhaustive. Accordingly, the three criteria listed in letters a-c are exclusively decisive for the soundness of the proof in accordance with Article 5.

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 letter a OEV, 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 OEV, 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 partial results

To ensure voting secrecy and to exclude premature partial results, the system must be designed in such a way that all the 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 to the OEV (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 risks

Corresponds, with some linguistic changes, to former Article 6 OEV. The article stipulates that additional measures must be taken if the risks are not sufficiently low despite the measures taken in compliance

[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.

with the requirements of this ordinance - in particular based on Articles 3 and 5-8 OEV. The term 'sufficiently low' is based on the criteria for the assessment and acceptance of risks defined by the cantons and the FCh.

Art. 10 Requirements for examination

In order to increase the effectiveness of the examinations and the independence between the examining entity 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, see also explanations on Art. 27*l* paras. 3 and 4 PoRO). In these areas, no further certification by entities 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 operator's computer centre (para. 2). Further requirements, such as the scope, responsibilities and timing of the examinations, are still set out in the Annex to the OEV (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'. The infrastructure and operation can be shared between the system operator and the cantons. This division depends on the system chosen and the method of cooperation. All infrastructure elements and all operational aspects are examined. The examination is carried out by the body responsible for the element concerned.

Para. 2: The operation of the system in the system operator's data centre is certified in accordance with ISO 27001.This examination is left to the cantons, as it is based on a recognised standard and there is a set method for carrying it out. 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 entities appointed to conduct the examinations under paragraph 1 access to the necessary documents. This includes all documents required for the examinations under paragraph 1 and all available reports (including certification reports), evidential documents and certificates (ISO 27001 certificate under paragraph 2 and any cantonal certifications).

Para. 4:

- All examination results pertaining to licensing must be published. The competent office 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. For examinations under paragraph 2, the 'Statement of Applicability' (SoA) must be published as a minimum, otherwise the comprehensive results are to be published.
- 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 audited office prepares a response to an audit report and requests publication, the response must be published by the competent office under paragraphs 1 and 2.
- The office commissioning the examination is responsible for publishing the results. For audits under paragraph 1, this is the FCh and for audits under paragraph 2, the canton or the system operator.
- For the exception to the principle of publication, see the explanations on Article 27*l*^{bis} paragraph 3 PoRO.

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

The former 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 the private premises of interested persons.

Para. 1 let. c: 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 audits carried out as part of the system development (e.g. code reviews, test reports).

Para. 1 let. d: Includes the documents describing the development process (see the explanations on Art. 27*l*[bis] para. 2 let. c PoRO).

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

Para. 1 let. f: 'Main components' means components whose correct functioning is significant for reducing risks. This includes, in particular, the trustworthy components in accordance with Annex Number 2. The technical specifications include the name of the manufacturer and of the product as well as the information about it that is relevant for identifying security vulnerabilities (e.g. version of the operating system or firmware, version of the Java runtime environment).

Para. 1 let. g: 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 in accordance with Annex Number 2 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. h: 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: As stated in the explanations to Article 27*l*[bis] paragraph 3 PoRO, the justified exceptions are generally based on the legislation on freedom of information and data protection legislation. In addition, in relation to publication under Article 11, 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. If exceptions are claimed, a balancing of interests must be carried out (see explanations on Art. 27*l*[bis] para. 3 PoRO).

Art. 12 Disclosure modalities

In principle, strict requirements apply to the transparency and availability of information on the system and its operation. The OEV does not require that the documents be disclosed under an open source licence. In 2020, the Confederation and the cantons declared themselves in favour of future systems and system components being disclosed under an open source licence.[10] The present provision in the OEV for the disclosure of documents is aimed at ensuring that as many independent experts as possible examine the disclosed documents.

Para. 1: The documents should 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 OEV, the proprietor may ask for any information necessary to

[10] See Measure B.2 in the final report of the SC VE dated 30 November 2020; available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

transfer it. Publication around 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 experts involved in finding flaws.

Para. 4 let. b: In the sense of 'responsible disclosure', the proprietor may require compliance with the following rules:

- Flaws are reported immediately to the source code proprietor.
- 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: If the proprietor of the source code imposes conditions for using the source code and the documentation (e.g. exclusion of commercial use by third parties) or conditions based on paragraph 4 letter b (conditions for the submission of suggestions under Art. 13 para. 1 OEV), breaches thereof may only be penalised in the exceptional cases specified in paragraph 5 (commercial use or productive use of the source code or parts thereof). The proprietor of the source code must make reference in the conditions of use to the restrictions relating to the possible penalties. 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*l*^{ter} 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 OEV.

An office in the canton itself, the system operator or an external company may be designated to run the bug bounty programme.

Para. 2: 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 must 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 experts 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 1.

Art. 14 Responsibility for running the ballot with electronic voting correctly

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. 2: This provision applies in particular to the following tasks:

- Tasks of the body responsible at cantonal level under para. 3.
- Deciding on the design of the voting papers and the information contained therein.
- Operating the set-up component and at least one control component of the group containing part of the key for decrypting the votes (Annex No 3.1).
- Decrypting and tallying the votes (Annex No 11.2).
- Communicating with voters on issues related to voting in the specific case.

With the exception of the mentioned important tasks, 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 the important tasks, which the canton must carry out itself, 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 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.

Para. 3 let. a: The general information security policy can be a general cantonal policy or a policy specific to e-voting. It 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.

Para. 3 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.

Para. 3 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.

Para. 3 let. d: Examples of measures: Conduct risk assessment, review compliance with information security policies, revise information security policies, provide appropriate tools.

Para. 3 let. f: 'Critical actions and operations' include in particular preparation for the ballot (Annex No 5), the opening and closing of the electronic voting channel (Annex No 9), the tallying 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 12.8).

Para. 3 let. h: Cantonal legislation determines how the auditors are appointed and how their deployment is organised. The office responsible at cantonal level supervises the deployment of the auditors and instructs them. The auditors undergo training including performing practical exercises.

Para. 3 let. i: With further indicators, the number and type of anomalies reported by voters to the canton are to be submitted to the auditors, in accordance with Annex No 11.10.

Para. 4: The operating bodies act on the instructions of the canton and assume responsibility for their tasks towards the canton.

Para. 5: Cantonal legislation determines how the auditors are organised and deployed.

Art. 15 Application documents

Para. 1: With the amendment of Article 27*b* letter b PoRO, only the documents that must be submitted with the application for authorisation are regulated here. The additional information to be submitted for a basic licence procedure is laid down in Article 27*c* PoRO.

The canton may refer to the validity of examination results or evidential documents from previous ballots (for the definition of 'validity', see also the explanations on para. 2). 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 current information on the planned use of e-voting that must be submitted as part of the authorisation procedure includes, for example, the versions of the system and system components to be used, a description and explanation of any deviations from the tested versions, timetables for the planned ballot and current information on the concrete organisation of the crisis cell.

With regard to evidence of compliance with the legal requirements, evidence must in particular be submitted as part of the authorisation procedure that is not part of the examination commissioned by the FCh. This concerns, for example, information on the planned communication with the voters in accordance with Article 27*m* paragraph 1 PoRO, the planned or previously carried out plausibility check in accordance with Article 27*i* paragraph 2 PoRO and the planned or previously carried out publication of e-voting results in accordance with Article 27*m* paragraph 3 PoRO, as well as the supporting documents mentioned in letters a-e. This list of evidential documents includes – with adaptation to the new provisions of the OEV – the former Article 8 paragraph 1 OEV and the list in the former number 6 of the Annex to the OEV, so that only one list of evidential documents is maintained. The exact deadlines and further details are published by the FCh in a separate document in each case.

Para. 1 let. a: The canton submits the current risk assessments from the canton and, if applicable, from its service providers in accordance with Article 4 OEV. The canton undertakes to draw attention immediately to any changes in risk assessments.

Para. 1 let. b: In accordance with the responsibilities for examining the systems and their operation, the cantons submit certificates and their annexes that they have drawn up as part of their examinations in accordance with Article 10 paragraph 2 OEV, as well as evidence of compliance with the publication obligation under Article 10 paragraph 4 OEV.

Para. 1 let. c: The canton submits evidential documents to confirm that the documents have been disclosed in accordance with Article 11 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 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 academic

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. 16 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 on 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').

4.2.2 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, former 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 1.3: The voter compares the codes displayed on the screen with the codes in the verification reference.

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

From the time they are cast to the time they are counted from the user device, electronic votes are transmitted through the internet and via numerous servers of the system operator 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 could enable an attacker 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. The requirements in Number 3 serve to do this.

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, 2.9 and 2.10 is unable to undermine 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

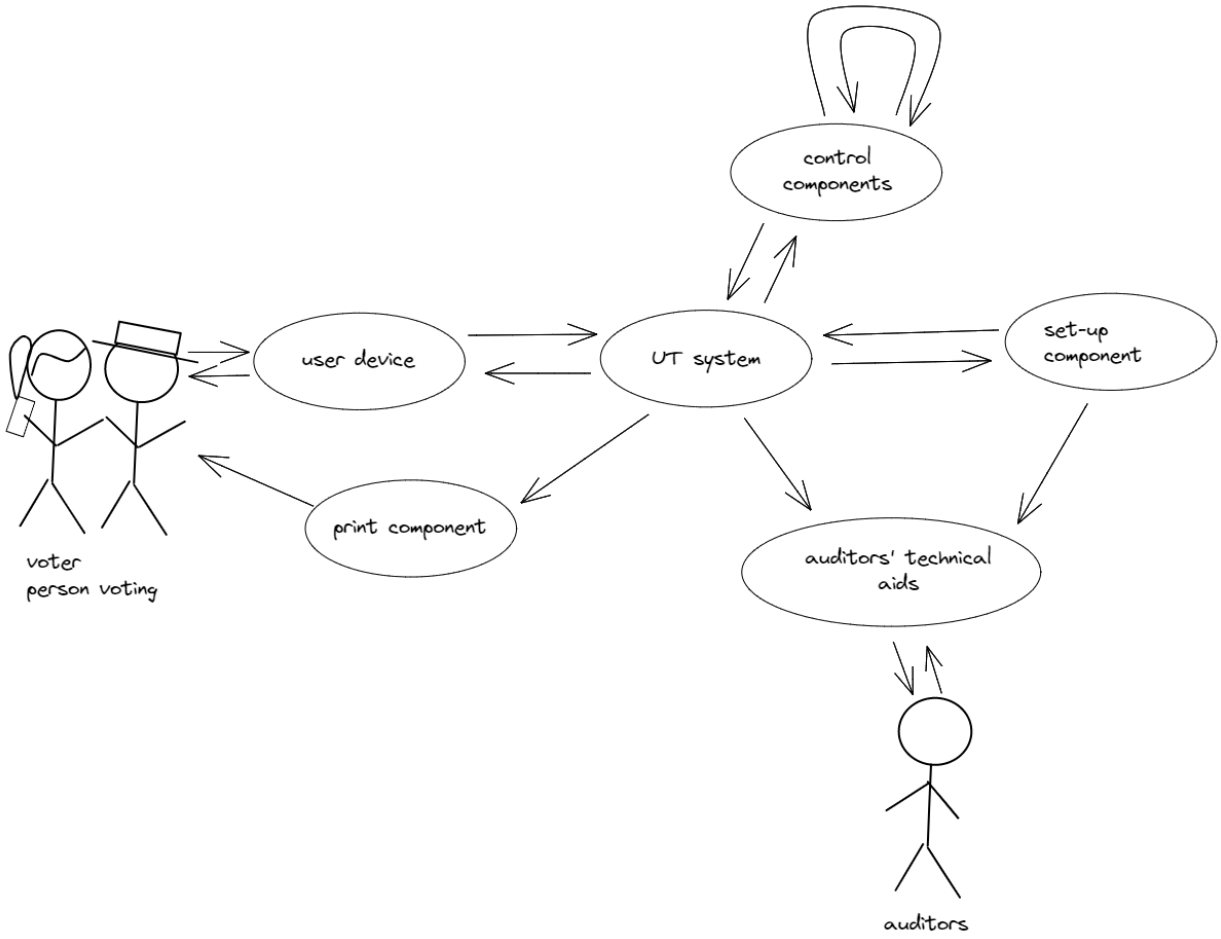
be clear and not underspecified. Under Number 2.14 mathematical proofs of the protocol conformity (conformity proofs) are required, as is usual in academic practice.

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.
- 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.
- 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).
- 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.
- 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.
- 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 after the result has been tallied at least once with a technical aid. They can also check intermediate results before or during the voting process. In particular, 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 2.3.2: The attacker can feed in messages via untrustworthy channels, for example by altering or duplicating messages for his benefit that other actors have exchanged.

Section 2.3.2 defines the assumptions to be made about the capabilities of the attackers ('what can attackers achieve in any case'). Under Number 2.4 it is determined to what extent the capabilities may be considered limited ('what attackers cannot necessarily achieve').

No 2.4: Trustworthy system participants and communication channels are considered to be protected against the attacker. The fewer elements are considered trustworthy, the greater the protection offered by the cryptographic protocol must be (see the explanations at the beginning of No 2). Number 2.9 specifies which system participants and communication channels may be considered trustworthy with regard to the requirements in Numbers 2.5-2.8.

In principle, it is desirable to consider system participants and communication channels as untrustworthy even if this would be unnecessary based on Number 2.9. However, this possibility is limited. For example, it would not be possible to detect manipulations according to Number 2.6 if all auditors were not trustwor-

thy and thus acted according to the instructions of the attacker. Options for further strengthening verifiability by weakening the trust assumptions must be explored in cooperation with the academic community based on the federal and cantonal catalogue of measures[11], and systems must be adapted accordingly.

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

It may be assumed that messages sent through trustworthy channels are not manipulated. 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 academic 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 8.8 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 tallied 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 has not maliciously cast a vote on the voter’s behalf which has subsequently been registered as a vote cast in conformity with the system and counted': 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 under Number 2.8 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

[11] See Measures A.5 and A.6 in the final report of the SC VE of 30 November 2020; available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

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 2.7.2: The fewer votes that are counted in a counting district, the greater the probability that all the votes are the same. If an attacker has access to the result of a counting district with identical votes and also manages to find out the identity of the voters, he could break the secrecy of the vote without any additional effort. He could also learn how the voters did not vote. This is the situation with both conventional and electronic voting. In line with conventional voting, the Ordinance does not regulate the minimum size of the counting districts.

In larger counting districts, such attacks are more difficult. Nevertheless, it is assumed that an attacker would try to break the secrecy of the vote in a similar way. First, by controlling untrustworthy system participants, he would have to ensure that only a small number of votes are counted. For example, he could try to manipulate the NT system so that it does not forward most votes to the control component after they have been cast. If the attack is successful, after the (possibly premature) closure of the electronic voting channel, only votes from voters who are either under the control of the attacker or whose voting secrecy he is trying to break would be registered. Based on the trustworthiness of at least one control component, it is recommended that the cantons, taking into account the number of votes registered by the control components, consider whether it seems possible that an attack has taken place and whether the secrecy of the vote could be threatened by the count. The cantons decide whether the votes are to be counted. Based on the growing experience with electronic voting, the cantons determine the maximum number of votes that could suggest an attack.

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 basis of comparison for the verification may also be published on a secure and trustworthy external platform if there are good reasons for doing so. In particular, such a platform as well as the corresponding communication channel may be considered trustworthy in terms of Numbers 2.9.3.2 and 2.10.2 respectively.

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 exclusion of premature partial 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 be regarded 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 tallied and then use the decrypted votes to breach voting secrecy. The auditors could 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 compromised. This must be prevented by having a group of control components ensure that no marked votes are processed before tallying. For the designation of the user platform as 'trustworthy', see the explanation on Number 2.7.3 (second paragraph).

No 2.9.3.3: Thus, no private system operator has the data that it would need to break the secrecy of the vote or to establish premature partial results.

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: The objective in dividing the proof into partial proofs is user-friendliness. It is not to achieve a higher degree of soundness through the division.

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 Number 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 print 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 2.14.1: In cases where Number 2.9.3.3 applies, as a result of the exclusion in Number 2.7.2, assumptions may be made in providing evidence of compliance with Number 2.7 that differ from Numbers 2.9.3.1 and 2.9.3.2. For example, it would be permissible to assume that a control component correctly registers and subsequently does not delete a sufficient number of votes from trustworthy voters as sent by the trustworthy user platform. Alternatively, it would be permissible to assume that the secrecy of the vote is not endangered if not all votes cast are tallied, but simply an arbitrary subset.

No 3 Requirements for trustworthy components in accordance with Number 2 and for 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: Operation 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 the individual components. See also the explanations on Number 2.9.3.

No 3.2: As a basis for the choice of random values ('seeds'), at least enough entropy must be aggregated so that the basic cryptographic components under Number 15.4 are effective. This can be promoted by aggregating seeds for random values from different independent components. In any case, functions and bases that are generally recognised as reliable are used. If necessary, it must be ensured that the necessary conditions are in place. Conditions may include that an operating system does not compute a seed

until the sources used (which may include, for example, the movement of the mouse) have made sufficient contributions to entropy.

No 3.4: The concrete organisation and procedure of auditors is governed by cantonal law (see also the explanations on Art. 27*m* para. 2 PoRO).

No 3.6: It must be possible to observe the auditing process. This means that people who could be present during the process should be able to understand the meaning and the results of the individual steps as far as possible. For this purpose, they must be able to witness the correct execution of the steps, for example by going to the place where they are carried out. With regard to the installation of the software, Number 24.3 must be considered.

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. It must be ensured that the software comes from an official and trustworthy source.

No 3.14: In contrast to a weaker form of the two-person control principle, it must be ensured that one person cannot access critical data without another person noticing. It is thus not sufficient to limit the two-person control principle to the execution of the process steps. In compliance with a strict two-person control principle, the secure storage of critical data could consist of storing the data encrypted on a data carrier and keeping the data carrier in a safe. One person knows the access code to the safe and the other person has the key to decrypt the data.

No 3.15: It is sufficient to use the same software for all control components. Manufacturer-independent software should be used for individual control components in the future, based on the catalogue of federal and cantonal measures.[12]

No 3.18: Based on the catalogue of federal and cantonal measures[13], manufacturer-independent software for the auditors' technical aid should be used.

No 4 Voting process

No 4.9: This is a provision that authorises the canton to provide the corresponding functionality. The canton is not obliged to do so.

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.

[12] See Measure A.4 in the final report of the SC VE of 30 November 2020; available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

[13] See Measure A.4 in the final report of the SC VE of 30 November 2020; available at www.bk.admin.ch > Political Rights > E-Voting > Reports and studies.

No 7 Requirements for printing offices

The requirements for printing offices are no longer 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 and if need be report any misuse.

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 8.8: This must also be observed in particular if the first item of proof under Number 2.12.5 was displayed incorrectly and the voter has interrupted the voting process as a result of this.

No 8.9: The aim of this provision is to counteract cases in which third parties maliciously cast a vote using voting papers belonging to others. In this context, account must be taken of the fact that the owners of the voting papers cannot necessarily recognise that a vote has been maliciously cast without consulting the system as mentioned in Number 2.5 (second indent). Furthermore, account must be taken of the fact that even after the first item of proof according to Number 2.12.5 has been displayed, it may still be possible to cast a vote.

No 8.11: 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 academic 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.

The term 'electronic ballot box' means a storage area containing the votes that are to be tallied. The electronic ballot box may be implemented by the control components referred to in Number 2. Alternatively, an additional storage area may be provided. In this case, the electronic ballot box must in any case be regarded as untrustworthy in accordance with Number 2.4.

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 operator 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 11.7: Auditors should, as a principle, be present at the venue. In addition, other auditors can be offered the opportunity to follow the procedures, for example, via live link.

No 12 Confidential data

No 12.7: The Confederation does not regulate the minimum size of counting districts – and thus in particular of constituencies (see explanations on Number 2.7.2). If necessary to preserve the secrecy of the vote, the results of small constituencies should be treated confidentially. In cases where constituencies are divided into individual counting districts, the requirement applies by analogy.

No 12.8: 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 OEV) 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. 1 OEV), 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 one or more security objectives 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; dealing with security events and making security improvements

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 system logs must be defined to ensure this. Voting secrecy must be guaranteed. Voting secrecy must be preserved.

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

- An open dialogue between the Confederation, cantons and system operators is maintained.
- 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.

The technical aspect of these requirements is mainly directed at the system operator. The body responsible at cantonal level must understand the content of the system logs and be able to respond to a message transmitted by its system operator.

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 operator. 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 14.9: 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 Use of 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 16 Secure electronic and physical exchange of information

No 16.2: The system must be logically or physically separated from all other activities. However, some elements of the infrastructure (e.g. monitoring, firewall) may be shared with other activities if this does not significantly increase the risks of the system and provides a significant benefit.

No 17 System tests

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 22 Management of communication and operations

No 22.3: Verification that the data backup is functioning correctly is provided as a minimum by conducting a data recovery test. It may be supplemented by other checks aimed at continuous improvement of the data backup processes.

No 24 Development and maintenance of 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 security functions are of crucial importance for the software. They must therefore be treated with special care and be traceable in all phases of the development process. It is important to ensure that all security functions provided for in the design of the software are present at all levels up to the source code. The term source code here also includes any external libraries.

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 operator 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,[14] the Trusted Build documentation published by GitHub[15] and the Reproducible Builds[16] documentation of the project of the same name.

No 24.3.3: With regard to 'evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference', the ‘trusted reference’ could be the Maven Central Repository, for example.

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 OEV) and the bug bounty programme (Art. 13 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

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

[15] GitHub How to: Trusted builds, 2017

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

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.[17] The criteria were selected according to their contribution to the defined security and quality objectives.

No 25.7.3. The e-voting portal must in principle be barrier-free and comply with the eCH-0059 Accessibility Standard. The contents of the standard are mandatory, with the exception of the requirements for alternative forms of communication (see Chapter 2.4 of the standard). With this exception, the requirements for information in plain language and sign language, particularly for the design of information on the proposal such as explanatory notes on voting or voting instructions, are not set higher than the requirements for postal and personal voting at the ballot box. Evidence that the e-voting portal is compliant with the requirements of the eCH-0059 Standard may take the form of a certificate or a test report from a competent body.

No 25.13.2: The aim of this requirement is to avoid unexpected behaviour from any parts of the software or from any possible values. To do this, at least one value must be tested from each set of values that lead to different results. Within a set of values, not all values need to be tested for. Error situations must also be tested for.

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 operator 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.

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