Federal Chancellery Ordinance on Electronic Voting
(OEV)

of 25 May 2022 (Status as of 1 July 2022)

The Swiss Federal Chancellery (FCh),

based on Articles 27*e* paragraph 1[bis], 27*g* paragraph 2, 27*i* paragraph 3 and 27*l* paragraphs 3 and 4 of the Ordinance of 24 May 1978[1] on Political Rights (PoRO),

ordains:

Art. 1 Subject matter

This Ordinance regulates the requirements for authorising electronic voting trials.

Art. 2 Definitions

[1] In this Ordinance:

a. *system* is the generic term for all the software and infrastructures that are used to conduct electronic ballots;

b. *online system* means the part of the system that is used to verify eligibility to vote, to cast the encrypted vote and to store the encrypted vote;

c. the *trustworthy part of the system* is the part of the system that includes one or more groups of control components; the trustworthiness of this part of the system arises from the fact that misuse can be detected even if only one of a group's control components is functioning correctly;

d. *control components* are separate components of the system that are designed in a variety of ways, operated by different persons and secured by special means;

e. *system operator* means the authority or private company that operates and maintains the online system at a ballot as directed by the canton;

f. *operation* means any action, including maintenance, with a technical, administrative or legal aspect and related management activities, carried out by

AS **2022** 336

1 SR **161.11**

a canton, system operator or printing office that are required to conduct electronic ballots;

g. *operating body* means an organisation or organisational unit responsible for operation, such as a cantonal chancellery, a system operator or printing office;

h. *auditor* means a person who checks on behalf of the canton that the ballot is correctly conducted;

i. *infrastructure* means hardware, software of third-party components in accordance with Article 11 paragraph 2 letter a, network elements, premises, services and equipment of any nature at any operating bodies that are required for the secure operation of electronic voting;

j. *software* means the entire implementation originating from the cryptographic protocol for complete verifiability that is carried out by the system developer for electronic voting;

k. *cryptographic protocol* means a protocol with cryptographic security functions to meet the requirements in Number 2 of the Annex; the cryptographic protocol is located in the model level and therefore does not contain direct instructions for implementation, but instead abstract security functions;

l. *user device* means any multifunctional, programmable device that is connected to the internet and is used to vote, such as a conventional computer, a smartphone or a tablet;

m. *registered vote* means a vote the final casting of which has been acknowledged by the trustworthy part of the system;

n. *partial vote:*
   1. in the case of popular votes: vote for a proposal, a counter-proposal or a deciding question,
   2. in the case of elections: the choice of a list or of a candidate;

o. *vote cast in conformity with the system* is a vote:
   1. that complies with a predetermined way of completing a ballot paper in a vote or election,
   2. that a sender has confirmed as final,
   3. in respect of which the client-side authentication credentials used or the resulting authentication messages match the server authentication credentials established in the preparatory phase of the ballot and assigned to an voter, and
   4. that has been cast using authentication credentials that have not already been used to cast a vote that has already been registered by the trustworthy part of the online system;

p. *client-side authentication credential* means a piece of information, such as a PIN, given to an individual voter that he or she requires, in some cases with other client-side authentication credentials, to be able to vote;

q. *server-side authentication credential* means a piece of information that is required, in some cases with other server-side authentication credentials, to authenticate the sender of a vote as a voter based on authentication messages;

r. *authentication message* means any information that a user device sends to the online system on submission of the client-side authentication credential so that the online system authenticates the sender of a vote as the voter;

s. a *certificate* is a document that confirms that an examined item conforms to a certain reference framework or standard;

t. an *electronic certificate* is a data record that confirms certain characteristics of a person or object and whose authenticity and integrity can be verified by cryptographic procedures; the electronic certificate is mainly used to identify and authenticate the holder, but also to encrypt messages;

u. *critical actions and operations* are processes in which critical data are processed;

v. *critical data* are data whose integrity or confidentiality is decisive in meeting the cryptographic protocol requirements.

[2] Further definitions are provided in Number 1 of the Annex.

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

Authorisation is required for each individual ballot; it is granted if the following requirements are met:

a. The system is designed and operated so as to guarantee verifiable, secure and trustworthy electronic voting.

b. The system is easy to use for the voters; account must be taken of the special needs of all voters wherever possible.

c. The system and the operational procedures are designed and documented so that the details of the technical and organisational procedures can be checked and understood.

d. The public have access to information appropriate to the addressees on how the system works and its operational processes, and there are incentives for experts among the public to participate.

Art. 4 Risk assessment

[1] The canton shall conduct a risk assessment in which it demonstrates and justifies that the security risks in its area of responsibility are sufficiently low. The level of public trust in and acceptance of electronic voting must also form part of the assessment.

2 It shall check whether it can itself assess risks within the field of activity of its service providers and to what extent separate risk assessments by these service providers are required. If necessary, it shall request these separate risk assessments.

3 The risk assessments cover the following security objectives:

a. the accuracy of the result;

b. preserving voting secrecy and excluding premature partial results;

c. availability and operability of the voting system;

d. protecting personal information relating to voters;

e. protecting information intended for voters from manipulation;

f. ensuring that evidence of voting behaviour is not maliciously exploited.

4 Each risk must be identified and clearly described on the basis of the documentation on the system and its operation with regard to the following criteria:

a. security objectives;

b. any data records related to the security objectives;

c. threats;

d. weaknesses.

Art. 5 Requirements for complete verifiability

1 It must be possible to detect any manipulation that leads to a falsification of the result while preserving voting secrecy (complete verifiability). This is considered to be the case if requirements for individual and universal verifiability are met.

2 The requirements for individual verifiability are as follows:

a. The person voting is given the opportunity to ascertain whether the vote as entered on the user device has been manipulated or intercepted on the user device or during transmission; to this end, the person voting receives proof that the trustworthy part of the system (Art. 8) has registered the vote as it was entered by the person voting on the user device as being in conformity with the system; proof of correct registration is provided for each partial vote.

b. A voter who has not cast his or her vote electronically can request proof after the electronic voting system is closed and within the statutory appeal deadlines that the trustworthy part of the system has not registered any vote cast using the client-side authentication credential of the voter.

3 The requirements for universal verifiability are as follows:

a. The auditors receive proof that the result has been established correctly; the proof confirms that the result ascertained includes the following votes:

1. all votes cast in conformity with the system that have been registered by the trustworthy part of the system;

2. only votes cast in conformity with the system;

3. all partial votes in accordance with the proof generated in the individual verification process.

b. The auditors evaluate the proof in an observable procedure; to do so, they must use technical aids that are independent of and isolated from the rest of the system.

Art. 6 Soundness of the proofs

The soundness of the proofs under Article 5 is based on the trustworthiness:

a. of the trustworthy part of the system for proofs under Article 5 paragraphs 2 and 3;

b. of the procedure for generating and printing the voting papers for proofs under Article 5 paragraph 2; and

c. of the technical aids used by the auditors for the audit for proofs under Article 5 paragraph 3.

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

The trustworthiness of:

a. the trustworthy part of the system;

b. the procedure for generating and printing the voting papers;

is decisive in preserving voting secrecy and excluding premature partial results within the infrastructure.

Art. 8 Requirements for the trustworthy part of the system

[1] The trustworthy part of the system includes one or more groups of control components.

[2] Even if only one of the control components in each group functions correctly, the proof is still sound (Art. 6) and voting secrecy is still preserved (Art. 7).

[3] The trustworthiness of the trustworthy part of the system is guaranteed by the diverse design of the control components and the independence of their operation and supervision.

Art. 9 Additional measures to minimise risks

If the risks are not sufficiently low despite the measures taken, additional measures must be taken to minimise risks. This applies in particular even if all the requirements of the Annex have already been met.

Art. 10 Requirements for examination

[1] Independent entities commissioned by the Federal Chancellery shall examine:

a. the cryptographic protocol (Annex No 26.1);

b. the system software (Annex No 26.2);

c. the security of infrastructure and operation (Annex No 26.3);

d. the protection against attempts to infiltrate the infrastructure (Annex No 26.4).

2 The canton shall ensure that the system operator has an information security management system (ISMS) and this is examined by independent entities (Annex No 26.5). The ISMS shall as a minimum comprise the system operator's processes and infrastructure that are relevant to achieving the security objectives.

3 The canton shall ensure that the Federal Chancellery and the independent entities that it commissions to conduct the examinations under paragraph 1 are given access to the system and the required documents.

4 The authorities responsible for the examinations under paragraphs 1 and 2 shall publish the evidential documents and certificates. Further documents must also be published if they are relevant for comprehensibility. Documents or parts of documents do not need to be published if there is a justified exemption, in particular under the law on freedom of information or data protection.

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

1 The canton shall ensure that the following documents are published:

a. the source code of the system software including files with relevant parameters;

b. evidence that the machine-readable programmes were generated from the published software source code;

c. the software documentation;

d. the development process documentation;

e. instructions and other documents that experts require to be able to compile, execute and analyse the system on the basis of the source code within their own infrastructure;

f. technical specifications of the main components of the system;

g. the process documentation for operating, maintaining and securing the system;

h. information on and descriptions of known flaws.

2 The following need not be published:

a. the source code for third-party components such as operating systems, databases, web and application servers, rights management systems, firewalls or routers, provided they are widely used and regularly updated;

b. the source code for portals of authorities that are connected to the system;

c. documents or parts of documents for which an exemption from publication is justified, in particular under the law on freedom of information or data protection.

Art. 12 Disclosure modalities

[1] The documents to be published under Article 11 must be drawn up and documented in such a way that they are easy to read and analyse.

[2] In order to facilitate their examination by the public, the documents must be:

a. available online in a simple process that is free of charge and does not require registration; and

b. made available in good time before the planned use of the system.

[3] Any person may examine, modify, compile and execute the source code for ideational purposes and write reports thereon. They may publish reports and findings relating to flaws. They may have discussions with others, in particular in order to identify flaws, and in doing so may quote from the published information.

[4] The proprietor of the source code may:

a. permit the source code to be used for other purposes;

b. set specific conditions for submitting suggestions for improving the system; it may call for flaws to be reported without delay and specify a date before which reports on suspected flaws may not be published.

[5] If the proprietor of the source code issues conditions of use for the source code and the documentation, or conditions under paragraph 4 letter b, it may only take civil or criminal legal action in the event of any breach thereof if a person has made commercial or productive use of the source code or parts thereof. The conditions of use and conditions under paragraph 4 letter b shall make reference to this.

Art. 13 Public involvement

[1] The canton shall designate a body to which interested persons may submit suggestions for improving the system, including:

a. suggestions relating to flaws in the documents published under Article 11;

b. suggestions on the basis of attempts to intrusion in the online system as part of public tests.

[2] The body under paragraph 1 shall evaluate the suggestions and inform the person concerned of its assessment and of any measures taken based on the suggestion. This information shall be published.

[3] The canton shall ensure that suitable financial reward is given for suggestions that relate to security and that help to improve the system.

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

[1] The canton bears overall responsibility for running the ballot with electronic voting correctly.

[2] It must carry out important tasks itself. It may delegate the development of the software used, operational tasks and communication on questions about how the system works to external organisations.

[3] The canton shall appoint a body at cantonal level that bears overall responsibility, and for the following tasks in particular:

a. drawing up general information security policy;

b. drawing up information classification and processing policy for the information resources identified;

c. drawing up risk management policy;

d. defining and implementing measures to ensure compliance with the policies in letters a–c;

e. appointing a system operator and drawing up the requirements for its supervision and monitoring;

f. setting the deadlines for carrying out critical actions and operations;

g. supervising and monitoring the system operator's work;

h. supporting and instructing the auditors;

i. assessing and communicating the accuracy of the result of the ballot based on the proofs under Article 5 and other indicators.

[4] When a ballot is held, the operating bodies bear responsibility towards the canton for the preparation and handling of the technical aspects of electronic voting.

[5] The auditors under cantonal law are responsible for operating their own technical aids.

Art. 15 Application documents

[1] Applications submitted under Article 27*e* PoRO must be accompanied by information on the planned use of the electronic voting channel and documents on how the legal requirements are met. These include the following in particular:

a. up-to-date risk assessments under Article 4, including the information necessary to make them comprehensible;

b. certificates and their attachments produced in examinations under Article 10 paragraph 2 and information on their publication in accordance with Article 10 paragraph 4;

c. information on the disclosure of the documents under Article 11 and suggestions from the public under Article 13;

d. reports on tests that the canton has carried out, and indications of existing flaws in the system;

e. justification and any measures regarding exemptions under Article 16 paragraph 2.

2 Reference may be made to documents under paragraph 1 that the Federal Chancellery has already received and which are still valid.

Art. 16 Further provisions

1 The detailed technical and administrative requirements for electronic voting are regulated in the Annex.

2 The Federal Chancellery may in exceptional cases exempt a canton from meeting individual requirements, provided:

a. the requirements that have not been met are indicated in the application;

b. reasonable justification is brought forward for allowing an exemption; and

c. the canton describes any alternative measures and justifies in reference to the risk assessment why it regards the risks as sufficiently low.

Art. 17 Repeal of another enactment

The FCh Ordinance of 13 December 2013[2] on Electronic Voting is repealed.

Art. 18 Commencement

This Ordinance comes into force on 1 July 2022.

2 [AS **2013** 5371; **2018** 2279]

Annex
(Art. 2 paras 1 let. k and 2, 9, 10 paras 1 and 2 and 16 para. 1)

Technical and administrative requirements for electronic voting

1. Definitions

In addition to Article 2, the following expressions mean:

1.1 *voting secrecy* is a situation in which no person or component has the following data:

1.1.1 votes cast or data indicating the content of votes cast,

1.1.2 data allowing the persons voting to be identified (data on voters), and

1.1.3 data allowing the data on voters to be matched with the votes cast;

1.2 the *exclusion of premature partial results* is a situation in which no person or component has the votes cast or data indicating the votes cast prematurely;

1.3 the *verification reference* is data sent with the voting papers to enable voters to check whether their vote has been cast correctly, in accordance with Article 5 paragraph 2 in conjunction with Number 2.5 of the Annex (e.g. a list showing a code for each voting option);

1.4 an *external attacker* is a person or group of persons who is not familiar with how the system has been developed or how it operates, who has average resources and expertise, from whom an attack originates; their motives may include political activism and financial gain;

1.5 an *internal attacker* is a person or group of persons involved in the development or operation of the system from whom an attack originates; their motives may include political activism, financial gain, or the intention to harm their employer;

1.6 a *hostile organisation* is a group of individuals with substantial resources and above-average expertise that is the source of an attack; it may also be supported by a state; its motives may be to obtain data for profiling purposes, to disrupt a ballot or to influence the results of the ballot;

1.7 an *attacker* is a person, group of persons or organisation as defined in Numbers 1.4-1.6;

1.8 an *electronic ballot box* is storage space in which the votes cast can be stored until they are decrypted and counted;

1.9 a *system log* is a log established from the infrastructure components to monitor the system and investigate incidents.

2. Cryptographic protocol requirements for complete verifiability (Art. 5)

2.1 System participants

The cryptographic protocol regulates the tasks of the following abstract system participants:

- voter / person voting
- user device
- set-up component
- untrustworthy system (any component excluding the other components listed in this Number; UT system)
- print component
- one or more groups of control components
- auditors
- auditors' technical aids

2.2 Communication channels

The cryptographic protocol may provide the following communication channels to enable system participants to exchange messages:

- voter / person voting ↔ user device
- user device ↔ UT system
- set-up component ↔ UT system
- control component ↔ UT system
- UT system → print component
- UT system → auditors' technical aid
- print component → voter / person voting
- set-up component → auditors' technical aid
- auditors ↔ auditors' technical aid
- bi-directional channels for communication between control components

2.3 Attackers

2.3.1 The cryptographic protocol must provide protection against an attacker attempting to tamper with the votes and the result, to breach voting secrecy or to obtain premature partial results (Nos 2.5–2.8).

2.3.2 The assumption must be made that an attacker has the following abilities:

- He can take control of all untrustworthy system participants (cf. No 2.4), so that they share all the secret data with him and act without restriction according to his instructions.
- He can read or prevent delivery of all messages that are exchanged on untrustworthy channels and feed in his own messages as he pleases.

2.4 Trustworthy and untrustworthy system participants and communication channels

2.4.1 System participants and communication channels are considered either to be «trustworthy» or «untrustworthy». The permitted trust assumptions for individual system participants are governed by Number 2.9.

2.4.2 Trustworthy system participants and communication channels are regarded as protected against attackers. For the cryptographic protocol, the following assumptions may be made:

- Trustworthy system participants keep private data secure and only carry out operations defined by the cryptographic protocol.
- Trustworthy communication channels keep transmitted messages private and protect them from manipulation.

2.5 Requirement for the cryptographic protocol: individual verifiability

The voter is given proofs in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that no attacker:

- has altered any partial vote before the vote has been registered as cast in conformity with the system;
- has 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.

2.6 Requirement for the cryptographic protocol: universal verifiability

The auditors receive a proof in accordance with Article 5 paragraph 3 letter a in conjunction with Article 6 letters a and c to confirm that no attacker:

- after the votes were registered as cast in conformity with the system, has altered or misappropriated any partial votes before the result was determined;
- has inserted any votes or partial votes not cast in conformity with the system which were taken into account in determining the result.

2.7 Requirements for the cryptographic protocol: preserving voting secrecy and excluding premature partial results

2.7.1 It must be ensured that no attacker is able to breach voting secrecy or establish premature partial results unless he can control the voters or their user devices.

2.7.2 There is no obligation to prevent attacks that limit the number of tallied votes to the degree that all partial votes for a question, list or candidate are the same.

2.7.3 It must be ensured that no attacker can take control of user devices unnoticed by manipulating the user device software on the server. The person voting must be able to verify that the server has provided his or her user device with the correct software with the correct parameters, in particular the public key for encrypting the vote.

2.8 Requirement for the cryptographic protocol: effective authentication

It must be ensured that no attacker can cast a vote in conformity with the system without having control over the voters concerned.

2.9 List of trustworthy and untrustworthy system participants

2.9.1 For soundness of the proofs referred to in Number 2.5

2.9.1.1 The following system participants are considered untrustworthy:

- user device
- UT system
- three out of four control components per group, leaving open which three they are
- a significant proportion of voters
- auditors
- auditors' technical aids

2.9.1.2 The following system participants may be considered trustworthy:

- set-up component
- print component
- one of four control components per group, leaving open which one it is

2.9.2 For soundness of the proofs referred to in Number 2.6

2.9.2.1 The following system participants are regarded as untrustworthy:

- user device
- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters
- set-up component
- print component

2.9.2.2 The following system participants may be considered trustworthy:

- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is
- one technical aid from a trustworthy auditor, leaving open which aid it is

2.9.3 For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7

2.9.3.1 The following system participants are regarded as untrustworthy:

- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters
- auditors
- auditors' technical aids

2.9.3.2 The following system participants may be considered trustworthy:
- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is

2.9.3.3 If an entire group of control components is used by a private system operator, none of these control components is considered trustworthy.

2.9.4 For the effectiveness of the authentication referred to in Number 2.8

2.9.4.1 The following system participants are regarded as untrustworthy:
- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters
- auditors
- auditors' technical aids
- user device

2.9.4.2 The following system participants may be considered trustworthy:
- set-up component
- print component
- one of four control components per group, leaving open which one it is

2.10 List of trustworthy and untrustworthy communication channels

2.10.1 The following communication channels are considered untrustworthy:
- user device ↔ UT system
- set-up component ↔ UT system
- control component ↔ UT system
- UT system → print component
- UT system → auditors' technical aids
- bi-directional channels for communication between control components

2.10.2 The following communication channels may be considered trustworthy:
- voter / person voting ↔ user device
- auditors' technical aid ↔ auditors
- set-up component → auditors' technical aids
- print component → voter / person voting

2.11 Additional requirements for the soundness of the proofs

2.11.1 The probability of an attacker being able to falsify a proof under Number 2.5 if he changes a partial vote, suppresses a partial vote or casts a vote in someone else's name must not exceed 0.1%.

2.11.2 The probability of an attacker being able to falsify a proof under Number 2.6 if he causes the calculated result to deviate by 0.1% from the correct result by altering and suppressing votes cast in conformity with the system or by entering votes not cast in conformity with the system may not exceed 1% per proposal, list or candidate selection.

2.11.3 If the probability of an attacker being able to falsify a proof under Number 2.6 is not negligible in the cryptographic sense[3], it must be possible to reduce the probability of success as desired by repeated tallying, by providing the auditors with an additional, independent proof under Number 2.6 for each count.

2.12 Functional requirements for the voting process with implications for the cryptographic protocol

2.12.1 Only one vote can be cast with the authentication credentials assigned to a voter.

2.12.2 The person voting enters their vote on the user device.

2.12.3 The person voting can change the vote up to the point of confirming the decision to cast it and can check the vote against a summary.

2.12.4 After the person voting has had the opportunity to check the vote against the summary, he or she confirms on the user device that he or she wants to cast the vote as entered.

2.12.5 The proofs of correct voting under Number 2.5 must be divided into at least two sequential items of proof. Any indication presented as an item of proof must make a genuine contribution to the soundness of the proof referred to in Number 2.5.

2.12.6 The user device displays the first item of proof to the person voting after he or she has confirmed on the user device that he or she wants to cast the vote.

2.12.7 The user device will not display the next item of proof to the voting person until the voting person has entered into the user device that the previous item of proof is correct.

2.12.8 By confirming that the penultimate item of proof is correct, the voting person confirms his or her decision to cast the vote definitively.

2.12.9 The group of control components registers the vote as having been cast in conformity with the system when it has received confirmation of the definitive decision to cast the vote.

2.12.10 When the person voting has checked the last item of proof as being correct, the voting process is complete. The last item of proof should be made particularly easy to check, by limiting the check as far as possible to the correct display of a single code or other simple indication.

[3] This corresponds for example to the probability of being able, without knowing the key, to decrypt an encrypted value that has been encrypted with a secure algorithm and corresponding parameterisation.

2.12.11 If voting data are imported, a setup component or a print component must no longer be considered trustworthy from that point on.

2.13 Requirements for the definition and description of the cryptographic protocol

2.13.1 Wherever possible, building-blocks are used that are in widespread use worldwide and have been thoroughly scrutinised by experts. Standards, reference projects and academic publications can be used as a benchmark. Derogations and cases of doubt must be dealt with separately in the context of the risk assessment referred to in Article 4.

2.13.2 Instructions must not be underspecified. Individual instructions must restrict the options for implementation to such a degree that any form of implementation that the instructions allow is also compliant with meeting the cryptographic protocol requirements.

2.13.3 It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.

2.14 Proofs of compliance with the cryptographic protocol requirements

2.14.1 A symbolic and a cryptographic proof of compliance must demonstrate that the cryptographic protocol meets the requirements in Numbers 2.1–2.12.

2.14.2 The proofs of compliance must directly refer to the protocol description that forms the basis for system development.

2.14.3 The proofs of compliance relating to basic cryptographic components may be provided according to generally accepted security assumptions and constructions (e.g. «random oracle model», «decisional Diffie-Hellman assumption», «Fiat-Shamir heuristic»).

3. Requirements for trustworthy components in accordance with Number 2 and for their operation

3.1 The operation of the set-up component and at least one control component in the group which contains part of the key for decrypting the votes is the direct responsibility of the canton and must take place within its infrastructure. Outsourcing to a private system operator is not permitted.

3.2 Sufficient entropy must be ensured when selecting random values, in particular for set-up components and control components.

3.3 Auditors must verify the proofs referred to in Number 2.6 at least once and must use a technical aid referred to in Number 2 for this purpose.

3.4 The operational requirements for set-up components in accordance with Number 3 also apply to technical aids used by the auditors. Within the scope of their responsibility under cantonal law, the auditors may provide for derogations.

3.5 With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.

3.6 Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.

3.7 Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.

3.8 When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.

3.9 The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.

3.10 Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.

3.11 Trustworthy components may not be connected to the internet when installing or updating software.

3.12 In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.

3.13 Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded.

Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.

3.14 Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two person principle).

3.15 Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect:

- If a person has physical or logical access to a control component, that person may not have access to any other control component.
- The hardware, the operating systems and the monitoring systems for the control components should be as distinct as possible from each other.
- The control components should be connected to different local networks.
- A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.

3.16 Control components must be designed to recognise unpermitted instances of access and to alert the persons responsible. The persons responsible should arrange external monitoring measures, such as the monitoring and the manipulation-resistant logging of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be considered to be particularly trustworthy and reliable.

3.17 Trustworthy components may perform only the intended operations.

3.18 The software for the auditors' technical aids must be obtained from a different system developer from the one who developed the main part of the software for the other system components. The publication of the software for the technical aid under a licence that meets the criteria for open source software[4] may justify an exception. If auditors use several technical aids, this provision applies to at least one of the technical aids.

3.19 All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.

3.20 Any access to and use of a trusted component or data carrier containing critical data must be logged.

4. Voting process

4.1 The person voting must declare that he or she is aware of the rules on electronic voting and of his or her own responsibilities.

4.2 Before casting a vote, the person voting is notified that he or she is taking part in a ballot in the same way as voting by post or voting in person at the ballot box. The person voting may only cast his or her vote after confirming that he or she has taken note of this.

4 See the definition in the Practice Guide to Open Source Software in the Federal Administration, version 1.0 of 19.12.2019, ch. 1; available from: Swiss Federal Chancellery, CH-3003 Bern; www.bk.admin.ch > Digitale Transformation und IKT Lenkung > Bundesarchitektur > Open Source Software (OSS) (available in German only).

4.3 When voting, the person voting is requested to check the proofs in accordance with Number 2.5 against the verification reference and to report any doubts as to its correctness to the canton.

4.4 At any time before casting an electronic vote definitively, the voter may still choose to cast his or her vote via a conventional voting channel.

4.5 The client-side system as it appears to the person voting does not influence the person voting in his or her decision on how to vote.

4.6 The user guidance must not lead persons voting to cast hasty or ill-considered votes.

4.7 The system does not offer the person voting any functionality allowing them to print out or store their vote.

4.8 The person voting is not shown any information after the voting process is completed about the content of the vote that has been encrypted and cast.

4.9 A voter who is unable to cast a vote because third parties have cast a vote using his or her voting papers unlawfully may still be allowed by the canton to vote provided the canton declares the unlawfully cast vote null and void. Voting secrecy in accordance with Number 2.7 must be preserved.

4.10 Voters with disabilities may be provided with a simplified procedure for checking the proofs. Only in such a case are derogations from the requirements set out in Number 2.9.1 permitted.

4.11 As long as the system has not registered confirmation of a definitive electronic vote, the voter may still choose to cast his or her vote via a conventional voting channel.

4.12 The use of a means of authentication independent of electronic voting is permitted. Effects on the integrity of the verification of the right to vote and the preservation of voting secrecy must be examined in detail as part of the risk assessment.

5. Preparations for the ballot

5.1 If the electoral register data is imported from a third-party system that is outside the canton's control, the data must be encrypted and signed. The signature must be verified on receipt of the data. For delivery to the printing office, the provisions of Number 7 take precedence.

5.2 The data required to examine the proofs in accordance with Number 2.6 must be handed over to the auditors.

6. Requirements for polling cards

6.1 If possible, the polling cards shall be designed so as to allow voters with a disability barrier-free access to electronic voting.

6.2 Security elements on the polling card (e.g scratch codes) may only be used if there is a confirmation that the concealed information is well protected against unauthorised reading.

6.3 If it is decided not to use security elements to protect confidential information on the voting card, organisational procedures must be in place to ensure security.

7. Requirements for printing offices

7.1 The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the printing office by two persons, who must both stay with the data carrier until it is delivered.

7.2 The encryption must meet the requirements of eCH standard 0014[5], Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the printing office via a secure secondary channel.

7.3 The person responsible at the printing office who receives the data carrier must sign an acknowledgement of receipt.

7.4 For the data carrier containing the print data, the component on which the critical data is decrypted and all components that process the critical data, the provisions for the print component as set out in Number 3 apply.

7.5 The persons responsible at the printing office carry out a material quantity check.

7.6 After printing the polling cards, the printing office must destroy the data received.

7.7 If the printing office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.

7.8 The channel between the printing office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.

8. Information and instructions

8.1 The body responsible at cantonal level must issue guidelines on providing information to citizens about electronic voting.

5 eCH-0014: Standards and Architectures for eGovernment Applications Switzerland (SAGA.ch), version 9.0 of 09.12.2019; the standard can be obtained from and viewed free of charge from the eCH Association, Mainaustrasse 30, P.O. Box, 8034 Zurich, www.ech.ch

8.2 The guidelines ensure that the information is authorised by the responsible bodies.

8.3 Tips and instructions on vote casting are given on the internet along with information on voters' responsibilities. This should counter over-hasty or ill-considered vote casting behaviour.

8.4 Verifiability, further security measures and the procedure in the event of anomalies are explained to voters in an accessible manner.

8.5 Voters are told what they have to pay attention to in order to cast their vote securely.

8.6 Voters are given instructions on how to delete their vote from all the memories on the device used for entering the vote.

8.7 Voters may request support if they have questions about electronic voting.

8.8 Voters are requested to report incorrectly displayed proofs in accordance with Number 2.5 such as verification codes or other verification steps with negative results to the body responsible at cantonal level. This request is also made in the instructions sent out with the voting papers.

8.9 Voters are requested to keep the voting papers with the security elements in fulfilment of Number 2.5 securely until they cast their final vote or until the voting process is concluded.

8.10 Voters are given the information required to check the authenticity of the website and the server used for voting. The informative value of a successful check must be supported by the use of cryptographic resources according to the best practices.

8.11 The information essential for secure voting is sent with the voting papers. Voters are told that if in doubt, they should comply with the information in the voting papers rather than the information displayed on the user device.

8.12 The measures taken to preserve voting secrecy are explained to voters.

8.13 Known flaws and the need for action associated with them are communicated transparently.

8.14 The auditors should be suitably informed about and trained in the processes that determine the accuracy of the result, the preservation of voting secrecy and the exclusion of premature partial results (for example key generation, printing the voting papers, decryption and tallying). They must be able to understand the essential aspects of the processes and their significance.

9. Opening and closing the electronic voting channel

The electronic voting channel is only available during the permitted period.

10. Conformity check and storing finalised votes

Votes not cast in conformity with the system are not stored in the electronic ballot box.

11. Tallying votes in the electronic ballot box

11.1 The decryption of the votes and the tallying may not begin before Polling Sunday.

11.2 The canton carries out the decryption and tallying within its own infrastructure.

11.3 The canton must ensure that the decryption of votes and their tallying is documented. The minutes are released by the body responsible at cantonal level.

11.4 From the decryption of votes to the transmission of the result of the ballot, any access to the system or to any of its components must be made jointly by at least two persons; it must be recorded in writing and it must be possible for the auditors to check it.

11.5 If the result data is transmitted to a third-party system that is outside the canton's control, the data must be encrypted and signed.

11.6 The system allows the polling card to be used to determine whether someone has cast an electronic vote.

11.7 Auditors must be present during decryption and tallying. The cantons may permit additional remote auditing work.

11.8 If components used to tally votes are not trustworthy in accordance with Number 2.4, the same requirements apply to these components as to set-up components under Number 3.

11.9 The auditors exercise their responsibility in accordance with cantonal law when examining the proofs in accordance with Number 2.6.

11.10 The body responsible at cantonal level submits all relevant indicators of the correctness of the result to the auditors. This includes, in addition to the proofs in accordance with Number 2.6, in particular the number and nature of anomalies reported to the canton by voters.

11.11 The canton anticipates any anomalies and, in consultation with the bodies concerned, draws up an emergency plan specifying the appropriate course of action. It creates transparency towards the public.

11.12 Statistical methods must be used to check the plausibility of the result, provided they are available and there is sufficient data.

12. Confidential data

12.1 It is guaranteed that neither employees nor externals hold data that allow a connection to be made between the identity of persons voting and the votes they have cast.

12.2 It is guaranteed that neither employees nor externals hold data before the decryption of the votes that allow the premature determination of partial results.

12.3 The canton may not pass on to private companies its part of the key for decrypting the votes which it has on the control component that it operates in accordance with Number 3.1.

12.4 The canton must treat the results of the ballot as confidential between the time the votes are decrypted and the time of publication.

12.5 The canton must ensure that data that indicate whether a voter has voted electronically are treated as confidential.

12.6 The canton must treat the individual votes as confidential after they have been tallied.

12.7 The canton must ensure that vote and election results in small constituencies are treated as confidential.

12.8 Following validation and in accordance with a predetermined and documented process, all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential must be destroyed.

13. Threats

13.1 The threats listed in Numbers 13.3-13.40 are of a general nature and form a basis; this must be added to. They relate to the security objectives and must be taken into account when identifying risks. Depending on the system vulnerabilities identified, when the various bodies carry out their risk assessments, the list should be updated with full details based on the actual circumstances and depending on the specific threat.

13.2 The following are considered to be potential threats:

- inadvertent or intended electronic or physical threats from internal or external actors;
- threats resulting from a malfunction of the system or system-supporting elements.

	Description	Security objective concerned (in accordance with Art. 4 para. 3)
13.3	Malware changes the vote on the user device.	Accuracy of the result
13.4	An external attacker redirects the vote using domain name server spoofing (DNS spoofing)[6].	Accuracy of the result
13.5	An external attacker changes vote using the man-in-the-middle (MITM) technique[7].	Accuracy of the result
13.6	Using MITM, an external attacker sends maliciously altered data that are necessary to cast a vote and that originate in the online system (e.g. Javascript files).	Accuracy of the result
13.7	An internal attacker manipulates the software, causing it not to store the votes.	Accuracy of the result
13.8	An internal attacker changes, deletes or duplicates the votes.	Accuracy of the result
13.9	An internal attacker inserts votes.	Accuracy of the result
13.10	A hostile organisation infiltrates the system with the aim of falsifying the result.	Accuracy of the result
13.11	An internal attacker copies voting papers and uses them.	Accuracy of the result
13.12	An external attacker uses social engineering techniques to distract the person voting from following the security measures (individual verifiability).	Accuracy of the result
13.13	An external attacker infiltrates the canton's infrastructure electronically, physically or by means of social engineering and manipulates the set-up components or steals security-relevant data.	Accuracy of the result
13.14	An external attacker infiltrates the printing office's infrastructure electronically, physically or by means of social engineering and extracts the codes of the polling cards.	Accuracy of the result
13.15	An external attacker infiltrates the postal service's infrastructure electronically, physically or by means of social engineering and steals polling cards.	Accuracy of the result
13.16	An error occurs in the individual verifiability.	Accuracy of the result

6 Also known as DNS poisoning. This is an attack which successfully falsifies the correlation between a host name and the related IP address.

7 The attacker in a man-in-the-middle attack. This is a type of attack used in computer networks. The attacker is positioned either physically or logically between the two communication partners and via its system has full control of the data traffic between two or more network participants and can view or even manipulate any information it wants.

	Description	Security objective concerned (in accordance with Art. 4 para. 3)
13.17	An error occurs in the universal verifiability.	Accuracy of the result
13.18	An error occurs in an auditor's technical aid.	Accuracy of the result
13.19	A backdoor[8] is introduced into the system via a software dependency and is exploited by an external attacker to access the system.	Accuracy of the result, preservation of voting secrecy and exclusion of premature partial results, availability and operability of the voting system, protection of information intended for voters from manipulation, prevention of malicious exploitation of evidence of voting behaviour
13.20	Malware on the user device sends the vote to a hostile organisation.	Preservation of voting secrecy and exclusion of premature partial results
13.21	The vote is redirected using DNS spoofing.	Preservation of voting secrecy and exclusion of premature partial results
13.22	An external attacker reads a vote using MITM.	Preservation of voting secrecy and exclusion of premature partial results
13.23	An internal attacker uses the key and decrypts non-anonymous votes.	Preservation of voting secrecy and exclusion of premature partial results
13.24	While checking the accuracy of the processing and tallying, voting secrecy is breached.	Preservation of voting secrecy and exclusion of premature partial results
13.25	An internal attacker reads the votes at an early stage without having to decrypt the votes.	Preservation of voting secrecy and exclusion of premature partial results
13.26	A hostile organisation infiltrates the system with the aim of breaching voting secrecy or obtaining premature partial results.	Preservation of voting secrecy and exclusion of premature partial results
13.27	An error in the encryption process renders it inoperable or reduces its effectiveness.	Preservation of voting secrecy and exclusion of premature partial results
13.28	An internal attacker manipulates the software to reveal the votes.	Preservation of voting secrecy and exclusion of premature partial results
13.29	Malware on the user device makes voting impossible.	Availability and operability of the voting system
13.30	A hostile organisation carries out a denial-of-service (DOS)[9] attack.	Availability and operability of the voting system
13.31	An internal attacker carries out an incorrect configuration; it does not get to the tallying.	Availability and operability of the voting system
13.32	An internal attacker falsifies the cryptographic proofs of universal verifiability.	Availability and operability of the voting system

8 A backdoor is a portion of software that allows access to the computer or an otherwise protected function of a computer program by bypassing normal access protections.

9 In digital data processing, this is the non-availability of a service that should be available.

	Description	Security objective concerned (in accordance with Art. 4 para. 3)
13.33	A technical error in the system causes the system to be unavailable at the time of the tallying.	Availability and operability of the voting system
13.34	One of the auditors' technical aids does not work at the time of tallying.	Availability and operability of the voting system
13.35	A hostile organisation infiltrates the system with the aim of disrupting operations, manipulating voter information or stealing proofs of the voting behaviour of the persons voting.	Availability and operability of the voting system, protection of information intended for voters from manipulation, prevention of malicious exploitation of evidence of voting behaviour
13.36	An internal attacker steals voters' address data.	Protection of personal information relating to voters
13.37	Malware influences voters' opinions.	Protection of information intended for voters from manipulation
13.38	An internal attacker manipulates the information website or voting portal and thereby deceives voters.	Protection of information intended for voters from manipulation
13.39	An internal attacker tells voters whether and how they have to vote. After decryption, he finds evidence in the infrastructure that the voters have followed the instructions.	Prevention of malicious exploitation of evidence of voting behaviour
13.40	An external attacker tells voters whether and how they have to vote and demands evidence that they have followed the instructions.	Prevention of malicious exploitation of evidence of voting behaviour

14. Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

14.1 An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required.

Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.

14.2 Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with

the system, of preservation of voting secrecy and of the exclusion of premature partial results.

The content of the records covers at least the following events:

– start and end of the audit, identification and authentication processes
– start, restart and end of the voting or election phase
– start of the tallying with the determination of the results
– conduct and results of any self-tests
– malfunctions identified in elements of the IT infrastructure that affect the ability to operate

The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented.

The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.

14.3 The monitoring and recording of system logs are subject to a continuous improvement process. The improvement process involves an open dialogue between those involved and a regular and objective assessment of the effectiveness of the instruments and processes used. The results of these evaluations will be taken into account.

14.4 The monitoring and recording of system logs in no way detracts from the effectiveness of the measures taken to preserve voting secrecy.

14.5 It must be guaranteed that in the event of a malfunction, the votes and the data that prove the smooth operation of the vote tallying are stored safely in the infrastructure.

14.6 After a breakdown in the system or a failure of communication or storage media, the system enters a recovery mode in which it is possible to return to a safe state. Voting processes that have been started are interrupted. The person voting cannot resume voting until the system is returned to a safe state.

14.7 It is possible to cast control votes using authentication credentials that are not assigned to any voter. The content of these control votes is recorded. The tallying of the control votes is compared with the records.

It must be ensured that the control votes are dealt with in as similar a way possible as votes cast in conformity with the system, while at the same time ensuring that they are not counted.

14.8 Infrastructure availability must be checked and recorded at selected intervals.

14.9 All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.

14.10 The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.

15. Use of cryptographic measures and key management

15.1 Electronic certificates must be managed according to the best practices.

15.2 In order to guarantee the integrity of data records that substantiate the accuracy of the result and ensure that critical data, including the authorities' identification and authentication data, are kept secret, effective cryptographic measures that correspond to the state of the art must be used.

15.3 To ensure that critical data are kept secret, effective cryptographic measures are used in the infrastructure that correspond to the state of the art. Such data is always stored encrypted on data carriers.

15.4 Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. NIST, ECRYPT, ESigA). The electronic signature meets the requirements of an advanced electronic signature in accordance with the Federal Act of 18 March 2016[10] on Electronic Signatures (ESigA). The signature must be verified by means of an electronic certificate that has been issued by a recognised supplier of certificate services under the ESigA.

16. Secure electronic and physical exchange of information

16.1 All infrastructure components must be operated in a separate network zone. This network zone must be protected in relation to other networks by an appropriate routing control.

16.2 As a principle, electronic voting should be clearly separated from all other applications.

17. System tests

17.1 The functions relevant to the security of the system (security functions) are tested. The tests are documented with test plans, and expected and actual test results.

The test plan:

- specifies the tests to be performed;
- describes the scenarios for each test, including any dependencies on the results of other tests.

The expected results must show the results that are expected if the test is successfully executed.

The actual results must be consistent with expected results.

10 SR **943.03**

17.2 An analysis must be made of the test coverage. This includes evidence that:
- the tests defined in the test documentation match the functional specifications of the interfaces;
- all interfaces have been fully tested.

17.3 An analysis must be made of the depth of testing. This includes evidence that:
- the tests defined in the test documentation match the subsystems related to security functions and modules that play a role in ensuring security;
- all subsystems related to the security functions mentioned in the specifications have been tested;
- all modules that play a role in ensuring security have been tested.

18. Organisation of information security

18.1 All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.

18.2 The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.

18.3 The risks in connection with third parties (contractors such as suppliers and service providers) must be identified and if necessary reduced by means of suitable contractual agreements. Compliance with the agreements must be appropriately monitored and reviewed throughout their term.

19. Management of intangible and tangible resources

19.1 All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements[11], relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.

19.2 The acceptable use of intangible and tangible resources must be defined.

19.3 Classification guidelines for information must be issued and communicated.

19.4 Procedures must be devised for the labelling and handling of information.

[11] The standard can be viewed or obtained against payment from the Central Secretariat of the International Organization for Standardization (ISO), Chemin de Blandonnet 8, P.O. Box 401, 1214 Vernier, www.iso.org

20. Trustworthiness of human resources

20.1 Suitable policies and procedures must be devised and promulgated in order to guarantee the trustworthiness of human resources before, during and after termination of employment or in the case of a change of activity.

20.2 Heads of human resources must accept full responsibility for guaranteeing the trustworthiness of human resources.

20.3 All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.

21. Physical and environment security

21.1 The security perimeters of the various premises of the infrastructure are clearly defined.

21.2 For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.

21.3 To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.

21.4 All data must be processed and in particular stored exclusively in Switzerland.

22. Management of communication and operations

22.1 Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.

22.2 Appropriate measures must be taken to protect against malware.

22.3 A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.

22.4 Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.

22.5 The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.

23. Allocation, administration and withdrawal of access and admission authorisations

23.1 It must be ensured that, during the ballot, any subsequent change in physical and logical access rights takes place only with the consent of the body responsible at cantonal level.

23.2 Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons.

Manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.

23.3 It must be guaranteed that information on the voting portal and related information pages cannot be changed without authorisation.

23.4 During the ballot, access of any nature to the infrastructure that is of no relevance to the ballot must be prevented.

23.5 It must be ensured that none of the elements of the client-sided authentication credentials can be systematically intercepted, changed or redirected during transmission. For authentication, measures and technologies must be used that sufficiently minimise the risk of systematic abuse by third parties.

24. Development and maintenance of information systems

24.1 Development

24.1.1 A life cycle model is defined. The life cycle model:
- is used for the development and maintenance of the software;
- provides for the necessary controls during the development and maintenance of the software;
- is documented.

24.1.2 A list must be made of the development tools used and configuration options chosen for the use of each development tool.

24.1.3 The documentation for the development tools includes:
- a definition of the development tool;
- a description of all conventions and directives used in the implementation of the development tool;
- a clear description of the significance of all configuration options for using the development tool.

24.1.4 The implementation standards to be applied must be specified.

24.1.5 The software must be specified and implemented in such a way that the security functions cannot be bypassed.

24.1.6 The security functions must be specified and implemented in such a way that they are protected against manipulation.

24.1.7 The security architecture of the software must be documented. The documentation:
- has a level of detail that corresponds to the description of the security functions;
- describes the security domains to which the security functions apply;
- describes how the initialisation processes are secured;
- demonstrates compliance with Numbers 24.1.5 and 24.1.6.

24.1.8 The functional specifications are documented. The documentation:
- maps the entire software;
- describes the purpose and application of all interfaces;
- identifies and describes all parameters associated with the interfaces;
- describes all actions associated with interfaces;
- describes all direct error messages that can result from calling the individual interfaces.

24.1.9 Traceability between functional specifications and security requirements is guaranteed to interface level.

24.1.10 All security functions are implemented in the source code.

24.1.11 Traceability between the entire source code and the specifications of the security functions is ensured and their correspondence is evident.

24.1.12 The security functions are designed and implemented in such a way that they are well structured. The internal structure is described and includes a rationale that:
- specifies the criteria used to assess «well-structured» and «complex»;
- shows that all security functions are well structured and not too complex.

24.1.13 The specifications include the following aspects:
- a description of the structure of the software in terms of subsystems;
- a description of the security functions as modules and, for each module, the objective and a description of how the module relates to the other modules; the description of the security enforcing modules must also include the available interfaces, the return values of those interfaces and the interfaces of the other modules that they use to interact with them;
- a description of all subsystems related to the security functions, including the possible interactions between them;
- a clear presentation of the subsystems associated with security functions to demonstrate that all interfaces conform to the behaviour described in the specification; the presentation must have a level of detail at least as far as the modules.

24.1.14 The software is provided with a unique identification.

24.1.15 The configuration management documentation includes:

- a description of how configuration items are identified;
- a configuration management plan describing how the configuration management system will be used in the development of the software and the procedures that will be followed for the adoption of changes or new elements;
- evidence that the procedures for adoption provide for adequate review of changes for all configuration items.

24.1.16 The configuration management system:

- uniquely identifies all configuration items;
- provides automated measures to ensure that only authorised changes are made to configuration items;
- supports the development of the software through automated procedures;
- ensures that the person responsible for accepting the configuration item is not the same person who developed it;
- identifies the configuration items that make up the security functions;
- supports verification of all changes to the software using automated procedures, including logging of the author and the date and time of the change;
- provides an automated method for identifying any configuration items that are affected by a change to a particular configuration item;
- can identify the version of the source code on the basis of which the software is generated.

24.1.17 All configuration items are inventoried in the configuration management system.

24.1.18 The configuration management system is used in accordance with the configuration management plan.

24.1.19 A configuration list is created that contains the following items:

- the software;
- evidence of the checks required to ensure security compliance;
- the parts that make up the software;
- the source code;
- the commit history[12];
- reports on security flaws and on the status of their correction.

For each element relevant to security functions, the developer is named. Each element is uniquely identified.

12 The commit history consists of an ordered list of all changes to a repository and the reason for each change.

24.1.20 Software development security documentation includes:
- a description of the physical, procedural, personnel, and other security measures necessary to protect and ensure the integrity of the design and implementation of the software in its development environment;
- evidence that the security measures provide the necessary level of protection to preserve the integrity of the software.

24.2 Operation

24.2.1 An operating manual is created that includes the following for each user role:
- a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings;
- a description of how the available interfaces can be used in a secure manner;
- a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security;
- a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions;
- a description of the security measures to be implemented in order to achieve the operational security objectives.

24.2.2 The operating manual must identify all possible modes of operation of the software, including the resumption of operation after the detection of errors and the description of the consequences and effects of errors on the maintenance of secure operation.

24.2.3 The operating manual must be precise and fit for purpose.

24.3 Reliable and verifiable compilation and deployment

24.3.1 The preparation process describes all the steps necessary for:
- the secure acceptance of the system components in accordance with the delivery procedure;
- the secure preparation of the operating environment in accordance with the operational security objectives;
- the secure installation of the software in the operating environment.

24.3.2 The delivery of the software or parts of the system must be documented and include all processes required to maintain security in the delivery of the software.

24.3.3 A reliable and verifiable compilation with appropriate security measures must be carried out to ensure that the executable code is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations. The compilation allows a chain of

proofs to be created for the verification of the software and includes in particular:

- evidence that the compilation environment is designed as described on the public platform (all tools with the respective version, operating system and any configurations); any derogations must be documented and justified;
- evidence that the software has been compiled in accordance with the instructions available on the public platform; if an error in the instructions is found during compilation, this must be recorded and the documentation must subsequently be corrected;
- evidence that the source code submitted for public scrutiny and examined is in fact the source code used for compilation;
- evidence that no elements other than those provided for in the instructions have been introduced;
- evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference;
- evidence that a dependency vulnerability analysis has been performed and that, if vulnerabilities relevant to the software exist, they do not render the software vulnerable to attack;
- evidence that the parameters introduced, if any, do not render the system vulnerable.

24.3.4 A reliable and verifiable deployment with appropriate security measures must be carried out to ensure that:

1. the code used in production is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations; and
2. the production environment conforms to that which has been subjected to public scrutiny and independent examinations.

The deployment allows a chain of proofs to be created for the verification of the software and includes in particular:

- evidence that the production environment is the same as that which has been subjected to public scrutiny and independent examinations; any discrepancies (firmware version, configuration files, etc.) must be documented and justified;
- evidence that the software deployed in the production environment is in fact that which was created using a reliable and verifiable compilation process;
- evidence that the parameters introduced, if any, do not render the system vulnerable.

24.3.5 The quality of the evidence of reliable and verifiable compilation and reliable and verifiable deployment must be confirmed by the presence of at least two witnesses from different institutions or by technical procedures to establish the truth of the evidence in the light of current academic knowledge and experience.

24.3.6 The chain of evidence of reliable and verifiable compilation and deployment is made publicly available.

24.4 Systematic correction of flaws

24.4.1 Processes are defined for the correction of flaws. The processes include:

- documentation of specific aspects, in particular with regard to the traceability of flaws for all versions of the software, and of the methods used to ensure that system users have information on flaws, corrections and possible corrective actions;
- the obligation to describe the nature and impact of all security flaws, information on the status of work to find a solution and the corrective measures adopted;
- a description of how system users can make reports and enquiries about suspected flaws in the software known to the software developers;
- a procedure requiring a timely response and automatic dispatch of security flaw reports and appropriate corrective actions to registered system users who may be affected by the flaw.

24.4.2 A process is defined for handling reported flaws:

- This process ensures that all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users.
- It provides for arrangements to ensure that the correction of security flaws does not give rise to new security flaws.

24.4.3 Policies must be defined for the reporting and correction of flaws. These include:

- instructions on how system users can report suspected security flaws to the developer;
- instructions on how system users can register with the developer to receive reports of security flaws and the corrections;
- details of specific contact points for all reports and inquiries on security issues concerning the software.

24.5 Quality Assurance

Regular and objective checks are carried out to ensure that the processes carried out and the associated work products comply with the description of the processes, standards and procedures to be implemented. Deviations are followed up until they are corrected.

25. Quality of the source code and documentation

The source code and documentation must as a minimum meet the following quality criteria:

25.1 Traceability

25.1.1 Traceability is understood as those attributes of the software that provide a thread from the requirements to the implementation.

25.1.2 All cryptographic protocol requirements across all work products associated with the software development process must be traceable.

25.1.3 A description must be provided of the link between the legal requirements and the cryptographic protocol, the specifications and the documentation of the architecture.

25.2 Completeness

25.2.1 Completeness is understood as those attributes of the software that provide full implementation of the required functions.

25.2.2 The software must not contain ambiguous references (input, function, output). If the same element is referenced, the same term is always used.

25.2.3 All data referenced and all functions used are defined in the specifications.

25.2.4 All functions defined in the specifications are used.

25.2.5 For each decision point (e.g. conditional execution), the possible alternatives are defined in the specifications.

25.2.6 All parameters are defined and validated in the specifications (no implicit parameter passing).

25.2.7 All serious reported flaws must be fixed before proceeding to the next step in the development cycle.

25.2.8 The cryptographic protocol, specification, design and source code are aligned.

25.3 Consistency

25.3.1 Consistency is understood as those attributes of the software that provide uniform techniques and notations in design and implementation.

25.3.2 The descriptions in the documentation correspond to a convention created by the software developer.

25.3.3 The functions and the variables correspond to a naming convention created by the software developer.

25.3.4 Input and output of functions are handled according to a convention created by the software developer.

25.3.5 Errors are handled according to a convention created by the software developer.

25.3.6 The variable types used are consistent.

25.4 Commonality of communication

25.4.1 Commonality of communication is understood as those attributes of the software that facilitate the use of standardised protocols and interface routines.

25.4.2 The rules for communication with other systems are defined.

25.4.3 Communication is based on standardised communication methods.

25.5 Commonality of data

25.5.1 Commonality of data is understood as those attributes of the software that facilitate the use of standardised presentation of the data representation.

25.5.2 The standard method of representing data for communication with other systems must be formally defined.

25.5.3 Standards must be defined for converting from one representation to another.

25.5.4 The conversion functions should be centralised in one module.

25.6 Learnability

25.6.1 Learnability is understood as those attributes of the software that enable users to learn how to use the software.

25.6.2 Persons who operate and use the system must be trained and provided with the necessary documentation.

25.6.3 Training includes the opportunity to train on a system designed for training purposes.

25.6.4 Help on using the system must be readily available.

25.7 Usability

25.7.1 Usability is understood as those attributes of the software that enable users to interact with the system.

25.7.2 The software must be user-friendly. The user guidance is based on generally familiar schemes.

25.7.3 The client-side system as it appears to the person voting complies with Accessibility Standard eCH-0059[13], with the exception of the requirements for alternative communication forms in Chapter 2.4 of the standard. The cantons shall ensure that compliance is confirmed by a specialist entity.

25.8 Error tolerance

25.8.1 Error tolerance is understood as the attributes of the software that provide continuity of operation under exceptional conditions.

25.8.2 Errors are detected and dealt with to enable the program to continue to run without interruption.

25.8.3 Error handling, including logging, is performed at the level most relevant to continued operation. An error that cannot be processed at one level is transferred to the next higher level.

13 eCH-0059: Accessibility Standard Version 3.0 of 25.06.2020; the standard can be obtained and viewed free of charge from the eCH Association, Mainaustrasse 30, P.O. Box, 8034 Zurich, www.ech.ch

25.8.4 Validity conditions are defined for the input parameters.

25.8.5 All input parameters are checked before execution starts.

25.9 Modularity

25.9.1 Modularity is understood as those attributes of the software that provide a structure of highly independent modules.

25.9.2 The task of each module is clearly defined.

25.9.3 The task of each module should be limited and focused. The tasks of two modules should not overlap.

25.9.4 The modules do not share data via a common volatile memory (e.g. global variable).

25.10 Simplicity

25.10.1 Simplicity is understood as those attributes of the software that implement functions in the most understandable way, which generally means avoiding practices that increase complexity.

25.10.2 A top-down approach (hierarchical structure) is chosen in the design.

25.10.3 The design does allow the duplication of functions between modules.

25.10.4 The design does not provide for global data, that is, data that can be used by everyone without being cleared as a parameter.

25.10.5 Complicated Boolean combinations in the source code must be avoided as far as possible.

25.10.6 No variables may be reused in the source code for purposes other than those originally intended.

25.10.7 In the source code, the number of nestings is limited as much as possible.

25.10.8 In the source code, cyclomatic and cognitive complexity is limited as much as possible.

25.11 Conciseness

25.11.1 Conciseness is understood as those attributes of the software that provide for implementation of a function with a minimum of instructions in the source code.

25.11.2 The software does not contain any superfluous passages in the source code (so-called «dead code»).

25.11.3 The source code does not contain any superfluous variables.

25.11.4 The source code should not contain any repetitions.

25.12 Self-descriptiveness

25.12.1 Self-descriptiveness is understood as those attributes of the software that create a situation in which addressees can identify the objectives, assumptions, constraints, inputs and outputs, components and status of the software.

25.12.2 Classes, functions and complex processing steps are commented on in the source code according to a convention defined by the software developer.

25.12.3 Variables and functions are given meaningful names.

25.12.4 A statement should only comprise one single line, unless readability is improved by the use of two or more lines. Multiple statements per line should be avoided.

25.13 Instrumentation

25.13.1 Instrumentation is understood as the attributes of the software that allow its use to be measured or errors to be identified.

25.13.2 The unit tests[14] cover all possible paths and limits of the permitted and unpermitted values of the input parameters.

25.13.3 The integration tests cover all modules.

25.13.4 The software tests cover all modules.

25.13.5 Errors and necessary information are recorded in logs.

26. Examination criteria for the systems and their operation

26.1 Examination of the cryptographic protocol (Art. 10 para. 1 let. a)

26.1.1 Subject: the following are examined:

- whether the requirements set out in Article 5 in conjunction with Articles 6–8 and Number 2 of the Annex are met; this assessment is made in particular on the basis of the cryptographic and symbolic proofs of conformity;
- whether and to what extent the cryptographic protocol is based on existing and proven protocols and building blocks;
- which improvements could contribute to a strengthening of security.

26.1.2 Responsibilities: the examination is carried out by experts in cryptography. The Federal Chancellery commissions the examination and monitors its conduct in accordance with the mandate.

26.1.3 Time of examination:

- A complete examination must be carried out before the system is used for the first time.
- The examination is repeated after two to three years.
- The cryptographic protocol must be examined again whenever it is modified and in the event of relevant new research findings concerning the security of cryptographic elements used and the threat situation.

14 In a unit test, the developer tests a module independently from the rest of the program to ensure that the module meets the functional specifications and works correctly under all circumstances. This test is considered essential for critical applications

26.2 Examination of the system software (Art. 10 para. 1 let. b)

26.2.1 Subject: the following are examined:

- whether the cryptographic protocol tested in accordance with Number 26.1 has been implemented; the correct implementation of functions of trusted components must be checked in particular detail;
- whether the system software meets the requirements of this Ordinance and adequately supports the specified objectives;
- whether the client-side system as it appears to the person voting conforms to the eCH-0059 standard in accordance with Number 25.7.3; the examination may be based on a valid certificate or a valid examination report issued by an institution recognised by the Federal Chancellery confirming conformity with the standard.

26.2.2 Responsibilities: the examination is carried out by experts in cryptography and in software development. The examination is commissioned by the Federal Chancellery.

26.2.3 Time of examination:

- A complete examination must be carried out before the system is used for the first time.
- The examination is repeated after two to three years.
- The examination is repeated for each significant modification, in particular:
  - following each modification to the cryptographic protocol;
  - in the event of any modification to the source code of functions whose trustworthiness is essential to the soundness of the proofs provided for in relation to verifiability;
  - in the event of relevant new research findings concerning the security of cryptographic elements used and the threat situation;
  - if it is decided to dispense with mechanisms that aid the secure use of trustworthy components in accordance with Number 2 or if such mechanisms are fundamentally modified.

26.3 Examination of the security of infrastructure and operation (Art. 10 para. 1 let. c)

26.3.1 Subject: the following are examined:

- whether the system and its operation at the canton, the system operator and the printing office meet the requirements of this Ordinance and adequately support the specified objectives;
- whether the basic components, such as the software that aids the secure and independent use of control components, the operating systems used or the server used meet the best standards.

26.3.2 Responsibilities: the examination is carried out by experts on cryptography and in operating highly secure systems. The examination is commissioned by the Federal Chancellery.

26.3.3 Time of examination:

- A complete examination is carried out before the system is used for the first time.
- The examination is repeated after two to three years.
- The examination is repeated for each fundamental modification, in particular:
  - following a modification to the cryptographic protocol;
  - if it is decided to dispense with mechanisms that aid the secure use of trustworthy components in accordance with Number 2 or if such mechanisms are fundamentally modified;
  - in the event of a fundamental modification to processes or infrastructure.
- If new versions of basic components (new servers, patches for operating systems or software that aid the secure and independent use of trustworthy components accordance with Number 2) are used, no new checks are required provided the basic components are still proven to comply with the best standards.

26.4 Examination of protection against attempts to infiltrate the infrastructure (Art. 10 para. 1 let. d)

26.4.1 Subject: it is examined whether experts commissioned by the Federal Chancellery succeed in infiltrating the infrastructure of the online system and gaining access to important data or taking control of important functions during a test.

The tests must be carried out on the basis of potential vulnerabilities identified following a methodological analysis of publicly available documentation, in particular that specified in Article 11.

26.4.2 Responsibilities: the examination is carried out by security experts. The examination is commissioned by the Federal Chancellery.

26.4.3 Time of examination:

- A complete examination is carried out before the system is used for the first time.
- The examination is repeated after two to three years.
- The examination is repeated for each fundamental modification to the infrastructure.
- The examination must take place in the event of relevant new findings concerning the security of the equipment used and the threat situation.

26.5 Audit of the information security management system (Article 10 para. 2)

26.5.1 Objective: to assess whether the system operator's ISMS is compliant with ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. The scope of the ISMS includes all the system operator's organisational units that are legally, administratively and operationally responsible for the system.

26.5.2 Responsibilities: the certification body is accredited by the Swiss Accreditation Service to perform audits according to the standard ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. The audit is commissioned by the canton or the system operator; the canton ensures that the audit is carried out.

26.5.3 Term of validity of a document: Re-audits must be carried out at the intervals specified by ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. A valid certificate and the corresponding «Statement of Applicability» is available each time the system is used. If a new version of Standard ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, is published, valid certification of the ISMS under the new version must be proven at the latest on expiry of the transition period. The scope of the ISMS may not be reduced thereby.