Federal Chancellery Ordinance on Electronic Voting
(VEleS)

of 13 December 2013 (Status as of 1 July 2018)

The Swiss Federal Chancellery (FCh),

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

ordains:

Art. 1 Subject matter and definitions

[1] This Ordinance specifies the requirements for authorising electronic voting.

[2] The definitions in Annex number 1.3 apply.

Art. 2 General requirements for the authorisation of electronic voting per ballot

The authorisation for electronic voting in any individual ballot shall be granted provided the following requirements are met:

a. The system for electronic voting (the system) is implemented and operated so as to guarantee secure and trustworthy vote casting (Annex No 2 and 3).

b. The system must be 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 shall be documented so as to enable the details of all security-relevant technical and organisational procedures to be understood.

Art. 3 Risk assessment

[1] By the means of a risk assessment, the canton must document in detailed and understandable terms that any security risks are within adequate limits. The assessment covers the following security objectives:

AS **2013** 5371
1 SR **161.11**

a. the accuracy of the result;

b. the protection of voting secrecy and non-disclosure of early provisional results;

c. the availability of functionalities;

d. the protection of personal information about voters;

e. the protection of voter information against manipulation;

f. the non-disclosure of evidence of vote casting behaviour.

2 Each risk must be identified and clearly described in the context of the security objectives, any related data records, threats, weaknesses and the documentation on the system and its operation. The canton must on this basis justify why it considers the risks to be sufficiently low.

3 Minimising risks must not be dependent on keeping security-relevant information on the system and its operation secret.

Art. 4 Requirements for authorisation for more than 30 per cent of the cantonal electorate

1 If a system is to be authorised to cover more than 30 per cent of the cantonal electorate, the voters must be able to ascertain whether their vote has been manipulated or intercepted on the user platform or during transmission (individual verifiability, Annex No 4.1 and 4.2).

2 For the purpose of individual verification, voters must receive proof that the server system has registered the vote as it was entered by the voter on the user platform as being in conformity with the system. Proof of correct registration must be provided for each partial vote.

3 If the client-sided authentication measure is sent electronically, voters who have not cast their vote electronically must be able to request proof after the electronic voting system is closed and within the statutory appeal deadlines that the system has not registered any vote cast using their client-sided authentication measure.

4 The substantiveness of the proof must not depend on the trustworthiness of the user platform or transmission channel.

5 It may be based on the following elements:

a. the trustworthiness of the server system;

b. the trustworthiness of the special technical aids for voters; these must meet particularly high security standards;

c. the confidentiality of data provided in paper form; the confidentiality of these data outside the infrastructure must be guaranteed through special measures.

Art. 5 Requirements for authorisation for more than 50 per cent of the cantonal electorate

[1] If a system is to be authorised to cover more than 50 per cent of the cantonal electorate, it must be ensured that voters or the auditors are able, subject to compliance with voting secrecy, to identify any manipulation that leads to falsification of the result (complete verifiability, Annex No 4.3 and 4.4).

[2] Complete verifiability is achieved if additional requirements for individual verifiability (para. 3) and requirements for universal verifiability (para. 4–6) are met.

[3] For individual verification the following requirements must be met in addition to those in Article 4:

a. The proof must also confirm to the voters that the data relevant to universal verification has reached the trustworthy part of the system (para. 6).

b. Voters must be able to request proof after the electronic voting system is closed that the trustworthy part of the system has not already registered a vote cast using their client-sided authentication measure.

c. The substantiveness of the proof must not depend on the trustworthiness of the entire server system. It may however be based on the trustworthiness of the trustworthy part of the system.

[4] For universal verification, the auditors receive proof that the result has been ascertained correctly. They must evaluate the proof in an observable procedure. To do this, they must use technical aids that are independent of and isolated from the rest of the system. The proof must confirm that the result ascertained:

a. takes account of all votes cast in conformity with the system that were registered by the trustworthy part of the system;

b. takes account only of votes cast in conformity with the system;

c. takes account of all partial votes in accordance with the proof generated in the course of the individual verification.

[5] The substantiveness of the proof must depend solely on the trustworthiness of the trustworthy part of the system and the technical aids used for verification. Equally, the guarantee of voting secrecy and the non-disclosure of early provisional results within the infrastructure must depend solely on the trustworthiness of the trustworthy part of the system.

[6] The trustworthy part of the system includes either one or a small number of groups of independent components secured by special measures (control components). Their use must also make any abuse recognisable if per group only one of the control components works correctly and in particular is not manipulated unnoticed. For the trustworthiness of the trustworthy part of the system, the diverse organisation of the control components and the independence of their operation and supervision are decisive.

Art. 6 Additional measures for minimising risks

If the risks are not sufficiently small despite the measures taken, additional measures must be taken to minimise risks. This applies in particular even if all requirements under Annex Nos 2 to 4 have already been implemented.

Art. 7 Requirements for examinations

[1] The cantons shall ensure that meeting the requirements is examined by independent agencies. The examination is made in particular if the system or its operation has been changed in such a way that meeting the requirements for authorisation could be called into question.

[2] If more than 30 per cent of the cantonal electorate are to be authorised to participate in a trial (Art. 4 and 5), the system and its operation must be examined in particular detail with regard to the following criteria:

a. cryptographic records (Annex No 5.1);

b. functionality (Annex No 5.2);

c. security of infrastructure and operation (Annex No 5.3);

d. protection against attempts to infiltrate the infrastructure (Annex No 5.5);

e. requirements for printing offices (Annex No 5.6);

f.[2] when using a system has the property of complete verifiability in terms of Article 5: control components (Annex No 5.4).

[3] If no more than 30 per cent of the cantonal electorate are to be authorised to participate in a trial and the system has the property of complete verifiability in terms of Article 5, the system and its operation must be examined in particular detail with regard to the following criteria:

a. cryptographic protocol (Annex No 5.1);

b. functionality (Annex No 5.2), whereby the examination may exclude the software in portals of authorities that are linked to a system;

c. security of infrastructure and operation (Annex No 5.3), whereby the examination may be limited to the infrastructure that registers the vote and creates the proof for the voter in accordance with Article 4 paragraph 2;

d. protection against attempts to infiltrate the infrastructure (Annex No 5.5);

e. control components (Annex No 5.4).[3]

2 Amended by No I of the FCh O of 30 May 2018, in force since 1 July 2018 (AS **2018** 2279).
3 Inserted by No I of the FCh O of 30 May 2018, in force since 1 July 2018 (AS **2018** 2279).