Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Annex to the FCh Ordinance of 13 December 2013 on Electronic Voting (OEV, SR 161.116)

Technical and administrative requirements for electronic vote casting

Version: **2.0**
Commencement: **1.7.2018**

Table of Contents

1. General Remarks

1.1. References

1.1.1 Federal Act of 17 December 1976 on Political Rights (PoRA; SR 161.1)

1.1.2 Ordinance of 24 May 1978 on Political Rights (PoRO; SR 161.11)

1.1.3 List of requirements printing offices for electronic vote casting (document of the Federal Chancellery)

1.1.4 Common Criteria Protection Profile for Basic set of security standards for online voting products, Version 1.0 (BSI-CC-PP-0037-2008)

1.1.5 ISO/IEC 27001:2005 Standard

1.1.6 Federal Act of 19 December 2003 on Certification Services in relation to Electronic Signatures (ESigA; SR 943.03)

1.1.7 eCH-0059: Accessibility Standard Version 2.0, 13.04.2011

The above documents can be obtained from the following organisations:

Legislative texts with an SR reference

Bundesamt für Bauten und Logistik (BBL)
Vertriebsstelle für Bundespublikationen
CH-3003 Bern
http://www.bundespublikationen.ch

ISO standards

Zentralsekretariat der Internationalen Organisation für Normung (ISO)
Rue de Varembé 1
1211 Genève
http://www.iso.org

List of requirements for printing offices

Schweizerische Bundeskanzlei
CH-3003 Bern
www.bk.admin.ch > Themen > Politische Rechte > Vote électronique > Versuchsbedingungen

Common Criteria Protection Profile

Bundesamt für Sicherheit in der Informationstechnik Postfach 200362 D-53133 Bonn,
Deutschland
https://www.bsi.bund.de

e-CH Standards

Verein eCH
Mainaustrasse 30, Postfach, 8034 Zürich
http://www.ech.ch

1.2. Abbreviations

Federal Chancellery	Federal Chancellery
PoRA	Federal Act on Political Rights
BSI	Federal Office for Information Security (Germany)
CC	Common Criteria
DOS	Denial Of Service
DNS	Domain Name Server
EAL	Evaluation of Assurance Level
ISO	International Organization for Standardization
MITM	Man In The Middle
PIN	Personal Identification Number
PP	Protection Profile
SAS	Swiss Accreditation Service
SFR	Security Functional Requirements
PoRO	Ordinance on Political Rights

1.3. Definitions

1.3.1 Authentication

1.3.1.1 Client-sided authentication measure:

All the information given to individual voters that they need to be able to vote (can for example be a PIN which when entered ultimately results in the vote signature). As a result of the client-sided authentication measure, the technical aid used issues an authentication message (for example the vote signature) that is sent to the infrastructure. Using the authentication message and the server-sided authentication measure (for example a public key to verify the signature), the infrastructure authenticates the sender of a vote as a voter. Client-sided authentication measures should be difficult to guess.

1.3.1.2 Server-sided authentication measure

All information used with the assistance of an authentication message to authenticate the sender of a vote as the voter.

1.3.1.3 Authentication message

All information that a user platform sends to the infrastructure on submission of the client-sided authentication measure so that the infrastructure authenticates the sender of a vote as a voter. It should be practically impossible to generate an authentication message without knowledge of a client-sided authentication measure.

1.3.2 System parts

1.3.2.1 System

Generic term for functionality and infrastructure. The part of the system that comprises the user platform and the client functional software is known as the client-sided system. The part of the system that comprises the server platform and the server functional software is known as the server-sided system.

1.3.2.2 Infrastructure (I)

Hardware, software, network elements, premises, services and equipment of any nature that are required for the technical operation of server functionality while guaranteeing compliance with all security requirements.

1.3.2.3 Functionality (F)

Server software and client software on the user platform that have been developed specifically for electronic vote casting to guarantee compliance with all security requirements.

1.3.2.4 User platform

Multifunctional, programmable device linked to the Internet which is used for vote casting. Generally speaking it is a conventional computer, a smartphone or a tablet.

1.3.3 Vote

1.3.3.1 Vote as entered by the voter on the user platform: A vote corresponding to that entered by the voter on the user platform, and which not been manipulated since. It always reflects the will of the voter unless he or she makes an error in entering it.

1.3.3.2 Registered vote

A vote is registered if the infrastructure has accepted the confirmed vote.

1.3.3.3 Partial vote

In popular ballots a bill, a counter-proposal or a secondary question, and in elections the choice of a list or the choice of a candidate seat on a list.

1.3.3.4 Vote cast in conformity with the system

A vote is “cast in conformity with the system” if

1. its sender has confirmed it; and
2. the client-sided authentication measure used and the resulting authentication message both match a server authentication certificate established in the preparatory phase of the ballot adopted and assigned to a voter; and
3. the electronic ballot box does not contain any vote entered using the same client-sided authentication measure.

1.3.4 Risk assessment

Generic term for the sequence of activities comprising *identifying risks, analysing risks* and *evaluating risks*

1.3.5 System operator

Organisation (authority or private company) responsible for dealing with all the technical aspects of vote casting in a ballot. It provides an appropriate level of human resources, organisation and infrastructure. All the system operator's technical, administrative, legal and management activities are known as operation. The system operator works as directed by the Cantonal Voting Officer.

1.3.6 Classified data and information

1.3.6.1 Confidential data and information

Data and information are confidential if they may only be disclosed to specific individuals.

1.3.6.2 Secret data and information

Data and information are secret if they are confidential and may not be disclosed to anyone. They include as a minimum the data and information that in their entirety would permit voting secrecy to be breached or early provisional results to be obtained. This definition may not correspond to other standards.

2. Requirements for the structure of fundamental procedures

The following sections detail the requirements for the structure of fundamental procedures. The right-hand column indicates the type of examination primarily needed for each requirement (I: Examination of infrastructure and operations; F: Examination on functionality).

2.1. Vote-casting process

2.1.1	The system must be user-friendly. The user guidance is based on generally familiar schemes.	F
2.1.2	The accessibility of the client-sided system must be checked in accordance with Standard eCH-0059 Version 2.0 by an agency that the Federal Chancellery recognises as being professionally competent.	F
2.1.3	Voters must confirm that they are aware of the rules governing electronic vote casting and of their own responsibilities.	F
2.1.4	Before casting their vote, authorised voters must be given express notice that they are validly contributing to a decision of the People by casting their vote electronically. Before casting their votes, voters must confirm that they have been able to read this message.	F
2.1.5	In order to cast a vote electronically, voters must prove to the responsible authority that they are eligible to vote by using the client-sided authentication measure.	F
2.1.6	Voters enter their vote into the user platform and cast it using the client-sided authentication measure.	F
2.1.7	The client-sided system as it appears to the voters does not influence their vote casting decision.	F,I
2.1.8	Until they confirm that they wish to cast their vote, voters can correct their vote. In addition, it is still open to them to vote in the conventional way.	F
2.1.9	The user guidance must not lead to rushed or injudicious vote casting.	F

2.1.10	The system allows a vote to be cast only if the voter reviews the vote properly and confirms it. To this end, the voter will be shown the vote again before it is finally sent.	F
2.1.11	The system offers voters the opportunity to stop the polling process at any time before the vote is cast, without losing their right to vote by doing so.	F,I
2.1.12	The system does not offer voters any functionality allowing them to print out their votes	F
2.1.13	It must be made clear to the voter via the user platform that the vote has been successfully transmitted. The voter receives confirmation that the vote he or she has cast has reached its destination.	F,I
2.1.14	Voters should not receive any information on how they have voted after the vote has been cast.	F
2.1.15	It must be impossible for a further vote to be cast using the same client-sided authentication measure.	F,I

2.2. Preparing authentication certificates, cryptographic keys and additional system parameters

2.2.1	The electoral register is imported into the infrastructure.	F,I
2.2.2	The questions asked in the ballot (e.g. the proposals being voted on or lists of candidates) is imported and stored in the infrastructure for all federal levels and electoral constituencies concerned.	F,I
2.2.3	The server-sided authentication measure for each voter is provided and stored in the infrastructure.	F
2.2.4	If necessary, the client-sided authentication measure for each voter is provided and stored temporarily in the infrastructure. (This is only necessary, if no external means of authentication is available.)	F
2.2.5	The cryptographic keys being used are provided and stored in the infrastructure.	F
2.2.6	The system operator sets the technical parameters relevant to the conduct of a ballot.	I

2.3. Information and help

2.3.1	The Cantonal Voting Officer prepares a concept on providing information to citizens on electronic vote casting.	I
2.3.2	The concept guarantees that the information has been authorised by the responsible bodies.	I
2.3.3	Tips and rules on vote casting are given on the internet along with information on voters' responsibilities. This should prevent over-hasty or injudicious vote casting behaviour.	F,I
2.3.4	The voters will be explained by which means the trustworthiness of electronic vote casting is ensured. The explanations need to be easily understandable and they need to relate to the employed security measures.	F
2.3.5	The voters will be told what they have to do to ensure that they cast their vote securely.	F
2.3.6	The voters will be told how to delete their vote from all the memories on the platform used for entering the vote.	F
2.3.7	The voters can request technical support.	I
2.3.8	The auditors, for example the commission appointed to verify the vote-casting process, should be suitably informed about and trained in the processes that determine the accuracy of the result, the preservation of voting secrecy and the avoidance of early provisional results (for example key generation, printing the voting papers, decryption and tallying). They must be able to understand the processes and their significance.	I

2.4. Preparing to print the voting papers

2.4.1	The voting papers must be so conceived so as to make it impossible to vote twice using a conventional vote casting method.	F,I
2.4.2	The file is provided for printing the voting papers. If applicable, it includes the client-sided authentication measure.	F
2.4.3	The print file is sent to the print office.	F,I

2.5. Opening and closing the electronic vote casting system

2.5.1	The system operator initialises the system. (The initialisation includes all settings that according to the process definition must be made shortly before opening the electronic vote casting system and may for example include activating system monitors or the resetting of counters and the electronic ballot box[1].)	I
2.5.2	The electronic vote casting system is opened to the voters.	F,I
2.5.3	It must be made impossible to open or close the electronic vote casting system too early.	I
2.5.4	The electronic vote casting system is closed to the voters.	F,I

[1] An electronic ballot box is any memory area in which the vote cast can be saved until it is decrypted and counted.

2.6. Conformity check and storing finalised votes

2.6.1	Using the received authentication message and the server-sided authentication measure, the system authenticates the sender of the vote as a voter.	F
2.6.2	The system checks whether a vote has already been stored in the electronic ballot box for the same voter.	F
2.6.3	If the vote has been cast in conformity with the system, the system stores the vote in the electronic ballot box and informs the voter that the vote has been cast successfully. Votes not cast in conformity with the system are not stored in the electronic ballot box. Criteria may be set over and above system conformity to determine whether a vote has been properly cast[2].	F

2.7. Tallying votes in the electronic ballot box

2.7.1	After the electronic vote casting system is closed, the Cantonal Voting Officer activates the decryption of the votes held in the electronic ballot box, at the earliest on Polling Sunday.	F,I
2.7.2	*Repealed*[3]	F,I
2.7.3	The Cantonal Voting Officer records the decryption process and tallying in writing.	I
2.7.4	From the decryption of the votes to the transmission of the result of the vote, any access to the system or to any of its components must be carried out by at least two persons; it must be recorded in writing, and it must be possible for it to be checked by a representative of the responsible authority.	F,I
2.7.5	The result of the vote is transmitted to a third party system for further processing, in particular in order to add the votes to the votes cast via the conventional channels.	F,I
2.7.6	The system provides the information required to determine, using a voter identification card, whether a voter who wishes to vote in person or by post has already cast an electronic vote. In the case of trials involving a very limited electorate (for example the Swiss abroad only), in order to preserve voting secrecy, no list that identifies voters who have cast an electronic vote may be given to any agency outside the infrastructure. Instead on request it must be confirmed whether a vote has been received from an individual voter. Alternatively, the system may provide a list giving anonymous codes that correlate with the voter identification cards used.	F,I
2.7.7	The decryption and the tallying of the votes are carried out in the presence of independent bodies or parties. As a result, they can confirm that the procedure has been duly carried out.	I

[2] A vote is properly cast if a ballot paper has been completed in a pre-determined way. How and whether votes that have not been properly cast should ultimately be taken into account may be defined in advance. For example, it may be decided that where there is a question on the ballot paper, only the responses “yes”, “no” or no response at all can influence the result of the vote. A response such as "I don’t want to vote" would not constitute a properly cast vote in this case. Whether it is even possible to place votes not properly cast in the electronic ballot box, whether they are ignored at the count or whether then may even be shown in the end result must be decided in advance.

[3] Amended by No II of the Amendment of 30 May 2018 of the FCh Ordinance on Electronic Voting (AS *2018* 2279).

2.8. Confidential and secret data

2.8.1	It is guaranteed that neither employees nor externals obtain data that allow a connection to be made between the identity of voters and the votes they have cast.	F,I
2.8.2	It is guaranteed that neither employees nor externals obtain data before the decryption of the votes that allow early provisional results to be determined.	F,I
2.8.3	It is guaranteed that the results of the vote are treated as confidential between the decryption of the votes and the time of publication of the results.	F,I
2.8.4	It is guaranteed that data that indicate whether a voter has voted electronically are treated as confidential.	F,I
2.8.5	It is guaranteed that personal data from the electoral register will be treated as confidential.	F,I
2.8.6	It is guaranteed that individual votes will be treated as confidential even after tallying.	I
2.8.7	It is guaranteed that the results of the vote will be treated as confidential if only a small number of voters in a constituency can vote electronically.	F,I
2.8.8	Upon validation and in accordance with a documented process, the system operator destroys all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential or secret.	I

2.9 Obligations of the Cantonal Voting Officer

	The Cantonal Voting Officer is a natural person who has overall responsibility for a ballot that involves electronic vote casting. In particular, he or she must: a. define, approve and introduce measures for information security (information security guidelines, basic criteria for managing information security risks, scope and limits for managing information security risks, risk management organisation); b. draft the agreement on running the ballot and specify the requirements for its monitoring and verification; c. instruct a system operator to run the ballot; d. specify deadlines for carrying out critical acts and operations; and e. monitor and verify the system operator’s running of the ballot. He may participate in the conduct of a ballot with electronic vote casting.	I

3. Security requirements

The security objectives (see Art. 3 para. 1) cannot be achieved with one hundred per cent certainty. In every case, it will be possible to identify security risks. Based on a methodical risk assessment (Art. 3 para. 2 and Sec. 6.4), proof must be provided that any security risks there may be are sufficiently limited.

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

Section 3.1 lists some general threats and relates these to the security objectives. They must be taken into account when identifying risks. Depending on the identified weaknesses of the system, they must be specified and updated as and when necessary.

The security requirements are summarised in Sections 3.2 – 3.15.

- Firstly, they relate to threats. Security measures that meet the security standards according to the best practices must be provided to guarantee the security objectives in respect of all those weaknesses in the system that are exposed to threats.
- Secondly, they relate to the requirements for organising fundamental procedures (see Section 2). This serves as an aid to understanding what weaknesses must be taken into account when implementing a security requirement. Further weaknesses must be identified on the specific system and the security standards applied thereto in an analogous manner.

Section 3.15 includes security standards from the protection profile (PP) of the German Federal Office for Information Security (BSI) [4]. Here certain derogations are permitted. The derogations and the links to the threats and the requirements for the organisation of fundamental procedures are set out in Section 3.15.

3.1. Threats

	Description	Security objective concerned
3.1.1	Malware changes vote on the user platform	Accuracy of the result
3.1.2	An attacker redirects the vote using DNS spoofing[4]	Accuracy of the result
3.1.3	An attacker changes vote using man-in-the-middle[5] (MITM) technology	Accuracy of the result
3.1.4	An attacker sends a maliciously altered ballot paper using MITM	Accuracy of the result
3.1.5	Administrator manipulates software, which does not store the votes	Accuracy of the result
3.1.6	Administrator changes votes	Accuracy of the result
3.1.7	Administrator adds votes	Accuracy of the result
3.1.8	Criminal organisation infiltrates system with the aim of falsifying the result	Accuracy of the result (here in terms of No 3.1.5/6/7/9)
3.1.9	Administrator copies and uses voting material	Accuracy of the result
3.1.10	Malware on the user platform sends vote to organisation	Protection of voting secrecy and non-disclosure of early provisional results
3.1.11	Vote redirected using DNS spoofing	Protection of voting secrecy and non-disclosure of early provisional results
3.1.12	An attacker reads a vote using MITM	Protection of voting secrecy and non-disclosure of early provisional results
3.1.13	Administrator uses the key and decrypts	Voting secrecy and non-disclosure of

[4] Also DNS poisoning. This is an attack which successfully falsifies the correlation between a host name and the related IP address.

[5] The attacker in a man-in-the-middle attack. This is a type of attack used in computer networks. The attacker is posititioned either physically or – in most cases now – 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.

	non-anonymous votes	early provisional results
3.1.14	While checking the accuracy of the processing / tallying, voting secrecy is breached	Protection of voting secrecy and non-disclosure of early provisional results
3.1.15	Administrator examines plaintext votes too soon	Protection of voting secrecy and non-disclosure of early provisional results
3.1.16	Criminal organisation infiltrates the system with the aim of breaching voting secrecy or obtaining early provisional results	Protection of voting secrecy and non-disclosure of early provisional results (here in terms of threats, No 3.1.13/14/15).
3.1.17	Malware on the voter's computer makes vote casting impossible	Availability of functionalities
3.1.18	Malware influences voter's opinion	Protection of voter information
3.1.19	Criminal organisation carries out a denial-of-service[6] (DOS) attack	Availability of functionalities
3.1.20	Administrator makes a configuration error; count becomes impossible	Availability of functionalities
3.1.21	Administrator manipulates information website or vote casting portal, confusing voters	Protection of voter information
3.1.22	Administrator looks for pre-determined vote casting behaviour following decryption (only possible in elections)	Non-disclosure of evidence of vote casting behaviour in infrastructure
3.1.23	Criminal organisation infiltrates the system with the aim of disrupting operations, manipulating voter information or obtaining evidence of vote casting behaviour the voters	Availability of functionalities, Protection of voter information, non-disclosure of evidence on vote casting behaviour in infrastructure (see in relation to threats, No 3.1.20/21/22)
3.1.24	Administrator steals voter address data	Protection of personal information on voters

[6] In digital data processing, this is non-availability of a service that should be available.

3.2. Identifying / discovering and reporting security events and - weaknesses; dealing with security events and security improvements

3.2.1	An infrastructure monitoring system must discover incidents and alert the human resources responsible. The human resources deal with incidents in accordance with pre-defined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that the vote casting-related activities can continue) and are applied as required.	F,I - 2.2.1/2/3/4/5/6 - 2.3.3/4/5/ - 2.5.2/3/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.2	Protocols of the votes received must be created in the infrastructure and made available as required. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system. In the case of irregularity, they must aid the search for the cause.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.3	Manipulation-resistant protocols of instances of system access must be made in the infrastructure and made available as required. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of compliance with voting secrecy and the avoidance of early provisional results. In the case of irregularity or doubt, they must aid the search for the cause.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.4	The electronically cast and tallied votes must be compared with the protocols of the votes received in the infrastructure in order to check the plausibility of the result.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.5	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.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.2.6	It must be possible to cast control votes with the aid of authentication measures that are not assigned to any voters. A record must be made of the content of these control votes. The tallying of the control votes must be compared with the records of the control votes cast. 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.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.1/2/3/4/5/6/7/8/9/13/14/15/16/17/18/21/23
3.2.7	Infrastructure availability must be checked and recorded at selected intervals.	I - 3.1.19/20/23
3.2.8	It should be possible to use statistical methods to check the plausibility of the result insofar as there is sufficient available data.	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.9	The parts of the vote casting system that are accessible from the Internet must be regularly updated in a documented process in order to eliminate weaknesses that have become apparent.	I - 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24

3.3. Use of cryptographic measures and key management

3.3.1	Electronic certificates must be managed according to the best practices.	I 2.2.13 - 2.2.5/6 - 2.4.3 - 2.7.5 - 3.1.2/3/4/8/12/16/20/23
3.3.2	In order to guarantee the integrity of data records that substantiate the accuracy of the result, effective cryptographic measures that correspond to the state of the art must be used.	I,F - 2.1.6 – 2.2.1/3/4/5/6 - 2.4.3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 3.1.5/6/7/8/9/14/16
3.3.3	In order to guarantee the confidentiality of data records that substantiate voting secrecy and the avoidance of early provisional results, effective cryptographic measures that correspond to the state of the art must be used.	I,F - 2.1.6 - 2.2.1/3/4/5/6 - 2.4.2/3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 2.8.1/2/3/4/6/7/8 3.1.12/13/14/15/16
3.3.4	Votes must not be stored or transmitted in unencrypted form at any time from being entered to tallying.	I,F 2.1.6/13 - 2.4.2/3 - 2.6.1/2/3 - 2.7.1 - 2.8.1/2 - 3.1.3/4/5/6/7
3.3.5	When exchanging electoral register and results data, encryption and a signature must be used. The signature and the data integrity must be reviewed on receipt of such data.	I,F 2.2.1/2 - 2.4.3 - 2.7.5 - 2.8.3/7
3.3.6	Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. FIPS 143-3, NIST, ECRYPT, ESigA). The electronic signature must meet the requirements of an advanced electronic signature under the ESigA. The signature must be verified by means of a certificate that has been issued by a recognised supplier of certificate services under the ESigA.	I,F
3.3.7	Voters are given the information required to check the authenticity of the website and the server used for vote casting. The informative validity of a successful verification must be supported by the use cryptographic resources in accordance with the best practices.	I,F 2.1.13 - 2.2.5 - 3.1.2/3/4/11/12

3.4. Secure electronic and physical exchange of information

3.4.1	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.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/20/22/23/24
3.4.2	The systems must be protected against attack (irrespective of the nature of the attack or of its origin).	I
3.4.3	The system for tallying the votes must be operated within the network zone in which the infrastructure is operated and within its own network subzone, which must be securely separated from all other network subzones.	I 7.2.1/2/3/4/5/6/7 - 2.8.1/2/3/4/5/6/7 3.1.6/7/8/9/13/14/15/16/20/22/23
3.4.4	Processing in connection with electronic vote casting must be kept completely separate from all other applications.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/20/22/23/24

3.5. Testing functionality

3.5.1	On the basis of a test concept, it must be ensured that functionality performs according to specification. The concept must include test scripts for every type of test. It regulates who is responsible for conducting the test, keeping records and preparing reports. It specifies the conditions under which a test is conducted. As a minimum, tests must be conducted for every security-relevant functional capability, even in the case of minor modifications.	I,F

3.6. Information security guidelines

3.6.1	The Cantonal Voting Officer must issue and promulgate information security guidelines that lay down a binding security framework for the entire operation of the system. These guidelines must be checked and if necessary revised at regular intervals.	I

3.7. Organisation of information security

3.7.1	All roles and responsibilities for the operation of the system must be precisely defined, allocated and promulgated.	I - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23
3.7.2	An authorisation process must be set up for information processing facilities in the infrastructure.	I - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23
3.7.3	The risks in connection with third parties (contractors irrespective of type, such as suppliers, service providers, etc.) 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.	I

3.8. Management of non-material and material resources

3.8.1	All non-material and material resources in accordance with the definition of the term "asset" in the ISO/IEC Standard 27001:2005 that are relevant in relation to electronic vote casting (organisation as a whole, in particular its organisational processes and the information as such processed in these processes; data carriers, facilities for information processing within the infrastructure; premises housing the infrastructure) must be recorded in an inventory. A list must be kept of human resources. The inventory and the human resources list must be kept up to date. Every non-material and material resource must be assigned to a person who becomes responsible for that resource.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.8.2	The permitted use of non-material and material resources must be defined.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.8.3	Classification guidelines for information must be issued and promulgated.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24

3.8.4	Procedures must be devised for the labelling and handling of information.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24

3.9. Trustworthiness of human resources

3.9.1	Suitable guidelines 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.	I 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23
3.9.2	Human resources managers must accept full responsibility at guaranteeing the trustworthiness of human resources.	I 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23
3.9.3	All human resources must be acutely aware of the need for information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.	I 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23

3.10. Physical and environmental security

3.10.1	The security perimeter of the various infrastructure rooms (rooms for the various human resources groups, server rooms, etc.) must be defined clearly.	I 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24
3.10.2	For physical admission to these various infrastructure rooms, admission authorisations must be defined, arranged and appropriately checked.	I 3.1.5/6/7/8/9/13/14/15/16/23
3.10.3	To guarantee the security of devices within and outside the infrastructure rooms, appropriate guidelines and procedures must defined and compliance therewith monitored and reviewed.	I 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24

3.11. Management of communication and operations

3.11.1	The operating sequences for the most important system activities must be described in detail.	I 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.2	Productive systems may only be modified in accordance with a documented procedure for change management.	I 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.11.3	Obligations and areas of responsibility must 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.	I - 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.4	Appropriate measures must be taken to protect against malware.	I 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.11.5	A detailed plan for storage must be prepared and implemented. The data storage must be regularly reviewed to check that it is functioning correctly.	I 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.11.6	Appropriate measures must be defined and implemented to protect the network and the security of network services.	I 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.11.7	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.	I - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/9 - 3.1.13/14/15/16 - 3.1.22/23/24
3.11.8	The measures for monitoring and keeping records of system usage, the activities of administrators and of error records must be described, implemented, monitored and reviewed in detail.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24

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

3.12.1	It must be guaranteed that during the ballot, no retrospective change may be made without the consent of the Cantonal Voting Officer.	F,I - 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.4 - 3.1.5/6/7/8/20/23

3.12.2	Access to infrastructure and functionality must be regulated and documented in detail on the basis of a risk assessment. In high risk areas, the dual control principle must be applied.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.12.3	It must be guaranteed that information on the website on electronic vote casting and/or related information pages cannot be changed without authorisation.	F,I 2.3.3/3/4/5/6 - 3.1.21/23
3.12.4	During the ballot, unauthorised instances of access to the infrastructure of any nature must be prevented.	F,I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24
3.12.5	It must be ensured that none of the elements of the client-sided authentication measure 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.	F,I – 2.1.5/6/15 - 2.2.3/4 - 2.4.1/2/3 - 2.6.1/2 - 2.7.1/2/4/5/6 - 2.8.1/4/5 - 3.1.5/6/7/8/9/13/14/15/16

3.13. Requirements for printing offices

3.13.1	Printing offices are governed in the fulfilment of their tasks by the provisions set out in the list of requirements for printing offices.	

3.14. Procurement, development and servicing of information systems

3.14.1	Appropriate procedures for software installation on productive systems must be described in detail and implemented.	I 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.14.2	Appropriate procedures must be described in detail and implemented in order to deal with technical weaknesses. Special attention must be given to parts of the infrastructure that can be accessed via the Internet.	I - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24

3.15. Requirements from the BSI protection profile

The requirements from the BSI protection profile [1.1.4] must also be implemented. In their interpretation, the terminology of the protection profiles applies.

In the event of any contradictions between content of the German and the English versions of the protection profiles, the provisions of the English version take precedence. The VEleS always takes precedence in the event of contradictions with the protection profile.

The following derogations from the protection profile are permitted or mandatory:

3.15.1	OE. Election preparation[7] provides inter alia that voters can verify information in the electoral register and where necessary seek rectification. This need not be implemented analogously here for Swiss voters.
3.15.2	There should be no need for voter registration. The information in the electoral register is sufficient to grant the right to vote.

[7] The requirements specified here from the Protection Profile begin either with "O" from the term "security objective" or "OE" from "security objectives for the operational environment".

3.15.3	OE.ServerRoom provides that only the election officer may enter the server room. This requirement may be relaxed to the effect that only persons authorised by Cantonal Voting Officer may enter the server room under supervision.
3.15.4	O.Correction provides that the voters can correct their vote as often as they wish before it is finally cast. This requirement may be relaxed as follows: until the intention is expressed to finally cast the vote, voters may correct their votes. (No 2.1.8 takes precedence)
3.15.5	In well justified cases, alternative IT security measures (according to the CC terminology; Security Functional Requirements) may be applied.

The following list relates the security objectives (according to the CC terminology) to the threats and the requirements for structuring fundamental procedures in this Ordinance.

O.UnauthorisedVoter	F,I 2.1.5 - 2.2.1/2/3/4 - 2.4.2 - 2.6.1 - 3.1.7/8/9
O.Proof	F,I 2.1.12 - 3.1.22
O.IntegrityMessage	F – 2.1.6/13 – 2.2.5 – 2.4.3 – 3.1.2/3/4
O.SecrecyOfVoting	F – 2.1.6 – 2.2.5 – 2.8.1/2 – 3.1.12/13
O.SecretMessage	F - 2.1.6 - 2.2.5 - 2.8.1/4 - 3.1.9
O.AuthenticityServer	F,I - 2.1.6 - 2.2.5 - 2.4.2 - 3.1.2/3/4/12
O.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
O.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
O.Abort	F - 2.1.11
O.EndingElection	F - 2.5.3/4 - 3.1.20
O.EndOfElection	F - 2.5.4 - 3.1.20
O.SecrecyOfVotingElectionOfficers	F - 2.7.2 - 2.8.1/6/7 - 3.1.13/14/16
O.IntegrityElectionOfficers	F - 2.5.1/2/4 - 2.7.4 - 3.1.5/6/7/8
O.IntermediateResult	F - 2.7.1 - 2.8.2/3 - 3.1.15/16
O.OverhasteProtection	F - 2.1.10
O.Correction	F - 2.1.8
O.Acknowledgement	F - 2.1.13 - 3.1.17
O.Failure	F,I - 2.2.6 - 2.5.1 - 3.1.19/20
O.Audit	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9 - 3.1.13/14/15/16/19/20/21/22/23/24
O.OneVoterOneVote	F,I - 2.1.5/8/11/13/15 - 2.2.1/2/3/4 - 2.4.1 - 2.6.1/2/3 - 2.7.6 - 3.1.7/8/17
O.AuthelectionOfficers	F - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.7.1/2/4/5 - 2.8.1/2/3/4/5/6/7
O.StartTallying	F - 2.5.4 - 2.7.1/2 - 3.1.15/16
O.Tallying	F - 2.2.6 - 2.5.1 - 2.7.2 - 3.1.5/7/8 - 3.1.20
OE.ElectionPreparation	F,I - 2.2.1/2/3/4/5/6 - 2.3.1/3 - 2.4.2/3 - 2.5.1 - 2.8.1/2/3/4/5/6/7/8 - 3.1.7/8/20
OE.Observation	F - 2.1.6
OE.ElectionOfficers	I - 2.2.1/2/6 - 2.3.2 - 2.5.1/2/4 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24
OE.AuthData	F,I - 2.2.1/2/3/4 - 2.4.2/3 - 2.8.1/5 - 3.1.8/9
OE.VoteCastingDevice	F,I - 2.1.3 - 2.3.3/4 - 3.1.1 - 3.1.10
OE.ElectionServer	I - 3.1.8 - 3.1.16 - 3.1.23

OE.Availability	I - 3.1.19
OE.ServerRoom	I - 3.1.5/6/7/8/9/13/14/15/16/23
OE.DataStorage	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
OE.SystemTime	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/6/8 - - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
OE.AuditTrailProtection	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
OE.AuthenticityServer	F - 2.3.3/4/5 - 2.4.2 - 3.1.2/3/4/12
OE.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
OE.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
OE.ProtectedCommunication	I - 3.1.5/6/7/8/9/13/14/15/16/22/23/24
OE.Buffer	F - 2.3.6

4. Verifiability

Articles 4 and 5 set out the provisions on verifiability. This section restates the provisions in a more formal way in order to explain the criteria for both forms of verifiability.

For that purpose, Section 4.1 defines a reduced abstract model for the description of a ballot. On the basis of that model, Section 4.2 contains explanations and further provisions relating to Article 4. Section 4.3 presents the complete abstract model. Section 4.4 contains explanations and further provisions relating to Article 5.

4.1. Reduced abstract model for Art. 4

In the abstraction used, a ballot is defined by a cryptographic protocol[8]. It consists of the exchange of messages between the following system components:

Voters	Voters receive their client-sided authentication measure from the system or from the print office prior to the ballot. In order to send a vote, they notify the user platform of their client-sided authentication measure and their vote.
User platform	It creates the authentication message and sends it with the encrypted vote to the server-sided system. For this it uses public parameters received beforehand from the system. It shows the voters messages from the server-sided system as required.
Trusted technical aids for voters	As an alternative, voters may also notify their vote and/or their client-sided authentication measure to a trustworthy technical aid. This may take over any tasks of the user platform.
System (here always server-sided)	Prior to the ballot, it generates and sends the client-sided authentication measure to the voters (if need be via the print office) and public parameters to the user platform, so that it can create the authentication message and the encrypted vote. It assesses whether votes have been cast in conformity with the system, decrypts them while preserving voting secrecy and calculates the result of the ballot.
Print office	It can be used to print the client-sided authentication measure and the confidential data required by the voters in order to benefit from individual verifiability (the verification reference). It receives the relevant data from the system and sends it on to the voters.

The protocol may provide the following communication channels for the exchange of messages:

- Voters ↔ user platform
- Voters ↔ trustworthy technical aids
- Trustworthy technical aids ↔ user platform
- User platform ↔ system
- System ↔ print office
- Print office → voter

System components and communication channels are either trustworthy or non-trustworthy. Trustworthy system components keep secret data undisclosed without exception and carry out only those operations that are permitted by the protocol. Trustworthy channels guarantee that the messages sent remain secret. In addition the recipient of the message can trust that the sender of a message corresponds to the system component stipulated by the definition of the channel.

In addition the abstraction used formalises an attacker. An attacker can maliciously modify any non-trustworthy system components and communication channels and place them under his control. Maliciously modified system components pass all secret data to the attacker and act without restriction

[8] A cryptographic protocol is a protocol with cryptographic security functions that aims to achieve security goals. The cryptographic protocols are described on the model level and thus contain no direct implementations but only abstract security functions.

according to his instructions. An attacker can also read all messages that are exchanged on non-trustworthy channels or intercept and even feed in his own messages as he pleases.

Trust assumptions in the abstract model (individual verifiability of the protocol): For individual verifiability, in this model it is assumed that trustworthy technical aids, the system and the print office are trustworthy. The user platforms and a significant proportion of the voters are assumed to be non-trustworthy. Among the communications channels, only user platform ↔ system and system ↔ print office are assumed to be non-trustworthy.

Security objective in the abstract model (individual verifiability of the protocol): According to the given trust assumptions, attackers cannot achieve the following objectives without a voter being highly likely to recognise that an attack has been carried out:

- changing the vote before registration
- misappropriating the vote before registration
- casting a vote

In order to achieve the security objective, only cryptographic building-blocks that are deemed secure are used in the protocol.

Individual verifiability of the system in practice: The system applies a cryptographic protocol that meets the security objective of individual verifiability in the abstract model. Where necessary, the assumption that the system components and communication channels are trustworthy is justified by related security measures.

Section 4.2 relates the provisions of Art. 4 to the security objective in the abstract model and provides more details where necessary. In addition, it contains security requirements for the system components and communications channels assumed trustworthy in the abstract model.

4.2. Additional provisions on individual verifiability

4.2.1	(On Art. 4 para. 2) The proof need not be given in a single transaction. It may be spread over several messages that the voter receives during the vote casting process. (In this case, the last of these messages confirms registration as a vote cast in conformity with the system.) If the voter decides to abort the process before the definitive vote (and accordingly before receiving the final message), he or she must still be able to vote by conventional methods.
4.2.2	(On Art. 4 para. 2) This requirement must be met so that the risk of vote selling is not significantly greater than with postal voting.
4.2.3	(On Art. 4 para. 3) The objective is to prevent untrustworthy system components from being able to cast a vote undetected. The provision must be interpreted to this effect and the protocol examined accordingly.
4.2.4	(On Art. 4 para. 4) The proof is substantive if it allows the voter to recognise manipulations of his or her vote in the sense of the security objective and under the given trust assumptions. As a result the attacker is not able to mislead the voter by creating a proof with the aid of the untrustworthy system components that leads the voter to believe that his or her vote has been registered as being cast in conformity with the system in the form that the voter entered it on the user platform. The probability that the attacker will be successful in creating such a proof by guessing correctly (analogous to the proof of confirmation that no vote was cast), must be no greater than 0.1%.
4.2.5	(On Art. 4 para. 4) For voters with disabilities, facilities may be provided for verifying the proofs. Derogations from the security objective are permitted for this purpose only. In particular, the validity of the proof may in this case be dependent on the trustworthiness of the user platform. Thus, for example, the verification reference may be scanned in prior to voting. These facilities may only be offered to a small group of voters who are unable to interpret the proof is completely valid without such facilities. Voters to whom this does not apply should, in principle, be encouraged to verify the proof according to the planned procedure.
4.2.6	(On Art. 4 para. 5) If the voters user a special technical aid for verification, this must have been specifically developed for the secure storage of secret elements and for carrying out cryptographic operations, such as devices used for secure home banking. In addition, the voters must be able to convince themselves of the fact that the aids operate correctly by casting test votes.

4.2.7	(On Art. 4 para. 5) In addition to the list of requirements for printing offices, the following provision applies: all machines involved in any form in the processing of unencrypted or unsigned verification reference data must be physically monitored for the entire computing time according to the dual control principle. The only network connections permitted are those whose participants are connected by a physical cable so it is clear that no other machines can access them before the confidential data is destroyed.
4.2.8	(On Art. 4 para. 5) No further provisions apply to the server-sided system. When implementing the requirements for structuring fundamental procedures and security standards (see Art. 2 and No 2 and 3), it must however be borne in mind that the confidentiality of the data connected with the verification reference is essential for the accuracy of the result, voting secrecy and the non-disclosure of early provisional results.
4.2.9	(On Art. 4 para. 4) The channel between the print office and the voters may only be regarded as trustworthy if the information has been sent by Swiss Post or passed on personally by one participant to the next.

4.3. Complete abstract model for Art. 5

The complete abstract model regards the system as untrustworthy. It provides for auditors that assess whether the result is correct on the basis of a trustworthy aid and independent "control components". It thus identifies the following additional system components:

Control component	It interacts with the system and the other control components so that the system can create substantive proof at the end of the ballot that confirms the correct result.
Auditors	After the tallying, they receive proof from the system confirming the correct result.
Auditors' technical aid	The auditors can use a technical aid to assess the proof.

The cryptographic protocol may provide for the following additional communication channels for exchanging messages:

- Control component ↔ system
- System ↔ auditors' technical aids
- Auditors' technical aids ↔ auditors
- Bidirectional channels for communication between control components.

Trust assumptions in the abstract model (complete verifiability of the protocol): Several control components are used that are combined in one or a few groups. A single control component must - like the system - be assumed to be untrustworthy. However it may be assumed that at least one control component per group is trustworthy, but without specifying which it is. The set of groups of control components forms the trustworthy part of the system. Its trustworthiness is defined by the trustworthiness of at least one of the control components in each of its groups. The substantiveness of the proof that an auditor receives under Art. 5 may only depend on the trustworthiness of the trustworthy part of the system and the auditor's technical aid. In addition, it is assumed that at least one trustworthy auditor will review the proof with the assistance of a trustworthy technical aid. Any additional auditors and their technical aids are deemed untrustworthy. Of the additional communications channels, only those between the auditors and their technical aids may be deemed trustworthy. The system must be regarded as untrustworthy.

Security objective in the abstract model (complete verifiability of the protocol):

- The attacker is unable to achieve the following objectives under the trust assumptions for the complete verifiability of the protocol without a voter or a trustworthy auditor being highly likely to recognise that an attack has been carried out:
  - changing a vote before its registration by the trustworthy part of the system
  - misappropriating a vote before its registration by the trustworthy part of the system
  - casting a vote
  - changing a vote cast in conformity with the system, the casting of which has been registered by the trustworthy part of the system
  - misappropriating a vote cast in conformity with the system, the casting of which has been registered by the trustworthy part of the system
  - inserting a vote

- Under the trust assumptions for complete verifiability of the protocol, the attacker is unable to breach voting secrecy or to obtain early provisional results without changing the voters or their user platforms maliciously.

In order to achieve the security objective, only cryptographic building-blocks that are deemed secure are used.

Complete verifiability of the system in practice: the same provisions apply as for individual verifiability.

Section 4.4 relates the provisions of Art. 5 to the security objective in the abstract model and where necessary explains them. In addition, it contains security requirements for the system components and communications channels deemed trustworthy in the abstract model.

4.4. Supplementary provisions on complete verifiability

4.4.1	(On Art. 5 para. 1) The use of auditors serves transparency. Voters should be able to assume that auditors in the event of any doubt would point out irregularities. However the groups which people who act as auditors should be recruited from is deliberately left open.
4.4.2	(On Art. 5 para. 3) Based on the information in the trustworthy part of the system (which may include the encrypted vote itself), auditors can ascertain whether a vote in its unchanged form has been regarded as an input for determining the result. Voters must accordingly be able to trust that the data in the trustworthy part of the system will not be removed or manipulated. In the technical literature, there are proposals that encrypted votes should be published on an electronic *public board*. A public board is created by combining several trustworthy components, so that entries can only be deleted or changed undetected if several of these components are maliciously changed. With the assistance of a trustworthy user platform, voters can at any time see that their vote is among the set of votes cast. At the end the voting process, the public board displays the result and the proof that the result is correct, which has been issued in the context of universal verifiability. The voters could accordingly assume the role of "auditors" in the spirit of maximum possible transparency. Various risk considerations, connected not least with the practice orientated assumption that user platforms need to be regarded as untrustworthy, can be used as arguments that the data for the trustworthy part of the system that is relevant to verifiability should not be published without restriction. It is therefore permitted to make the data available to a restricted group of auditors. In the terminology of the technical literature, the requirement can therefore be understood as follows: *voters receive proof from the components responsible for the public board that confirms that they have received their vote (i.e. data that are sufficient for universal verification). Its substantiveness must not be dependent on the trustworthiness of an* untrustworthy *user platform or of the system. At the latest after the result has been determined (but before publication), the* auditors *receive access to the public board and ascertain that the result takes into account each vote on the public board in accordance with the applicable rules.*
4.4.3	(On Art. 5 para. 3 let. b) The objective is to prevent untrustworthy system components from being able to cast a vote undetected. The provision must be interpreted to this effect and the protocol examined accordingly.
4.4.4	(On Art. 5 para. 3 let. c) The confidentiality of the data relating to a verification reference may therefore only depend on the trustworthy part of the system even within the infrastructure.
4.4.5	(On Art. 5 para. 4) The independence and isolation of the technical aid must guarantee that the evaluation of the proof cannot be influenced by the system. However it is deliberately left open as to whether technical aids and the corresponding programs should be provided by the system or the auditors. The auditors should however be able to verify easily that the aid works correctly. This can be achieved for example by the auditors being able to write the programs themselves or at least being able to analyse them in advance. Before verification, they and the system managers could the set up the aids and compile and install the verification programs. As a principle, verification programs should be easy to write for the sake of transparency.
4.4.6	(On Art. 5 para. 4 let. a and b) A vote is deemed to be cast in conformity with the system only if the client-sided authentication measure used corresponds to a server-sided authentication measure that was adopted and "assigned" to a voter in the preparatory phase of the ballot. The proof must therefore include confirmation that no unallocated

	authentication certificates for casting votes have been issued. In addition, during preparation for the ballot, the control components or the auditors must have been given corresponding data as the basis for making a comparison. The auditors must ascertain that the number of authentication certificates corresponds to the (official) number of authorised voters. In this event, the authentication certificates may be deemed to have been "allocated" to a voter. However, this does not guarantee that the client-sided authentication measures for a trustworthy voter have not been misused to cast a vote in conformity with the system. Based on the corresponding point in the security objective for the abstract model and Art. 5 para. 3, let. b, voters can however recognise this themselves.
4.4.7	(On Art. 5 para. 5) The proof is substantive if it allows the voters or the auditors to recognise manipulations of the votes in the sense of the security objective and under the given trust assumptions. As a result, the attacker cannot mislead the auditors by creating or influencing the creation of proof to justify a manipulated result with the assistance of the untrustworthy system components. In the context of universal verifiability, the following provisions apply: – The auditors must in every case be able to recognise the event where a vote cast in conformity with the system and registered by the trustworthy part of the system has been misappropriated without it being replaced. – The auditors must in every case be able to recognise the event where a vote has been inserted, without another vote being misappropriated. – The probability of successfully manipulating 0.1% of the partial votes (for example by misappropriating and at the same time inserting votes), so that they no longer reproduce the sense of the proof generated during individual verification may amount to a maximum of 1%. If the probability is not negligible in cryptographic terms[9], it must be possible to reduce the uncertainty sufficiently through multiple tallying using new random values.
4.4.8	(On Art. 5 para. 5) If the application used on the user platform to encrypt the vote is provided by the system, then it must also be regarded as part of the server-sided system. It must be ensured that the voting secrecy of trustworthy voters cannot be breached without maliciously changing their user platform through the server-sided manipulation of the application. Voters should therefore be able, using a trustworthy platform, to satisfy themselves that the application is sending their vote in encrypted form with the correct key. This can for example be achieved using browser technology that allows the source code of the user application to be seen. Voters can in this way satisfy themselves that the public key used corresponds to that of the ballot, and that the application is only carrying out the planned operations. Alternatively, the source code could be signed by a group of control components.
4.4.9	(On Art. 5 para. 5) It follows from the security objective, that it must be ensured that the server-sided system cannot find out the content of a vote cast in cooperation with an untrustworthy voter. In particular, it must be ensured that the voter cannot externally modify and cast as his own an encrypted vote that has already been cast, with the aim of finding out what the vote is using the proof that he receives due to the individual verifiability process.
4.4.10	(On Art. 5 para. 5) Due to the requirement relating to the guarantee of voting secrecy and the absence early provisional results, no system component may know the private keys for decrypting votes, at least during the opening hours of the electronic vote casting system. It is however permitted that they may be calculated with the participation of all control components of a group. It is also permitted to implement a group of control components so that they take the form of a group of people. Each member of this group could hold part of the private key on a portable storage medium. To safeguard voting secrecy, the private key may only be made available following decryption if the votes are cast anonymously and no encryption of a vote can be combined with the identity of a voter under the given trust assumptions. In addition, due to the requirement relating to the absence of early provisional results, it is not permitted for votes to exist during the opening hours of the electronic vote casting system outside the user platform at any time in unencrypted form.
4.4.11	(On Art. 5 para. 6) Whether a serious system malfunction can be recognised depends on the trustworthiness of the "trustworthy part of the system". Such malfunctions include incorrect calculations that influence the result, breaches of voting secrecy or obtaining early provisional results. Implementing familiar proposals from the technical literature guarantees a particularly high level of trustworthiness. The proposals go so far that serious malfunctions can only go unnoticed if every control component in a group, without exception, (for example as a result of undetected manipulations) fails to work correctly.

[9] 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.

	However if only one control component works correctly, any serious system malfunction can be recognised. The control components are often called "trustees" in English in the abstraction. In the abstraction, trustees are described as entities that can initiate complex calculations and keep private elements secret. The calculations may include the provably correct mixing and re-encryption of votes (re. their anonymisation; each trustee corresponds to a mixing node of a re-encryption network), the running of a trustworthy electronic public board or the creation of the PKI and, with the aid of their parts of the distributed private key, the provably correct decryption of votes. In the abstraction, the trustees are often presented as people who can calculate like machines. Whether they keep the secret elements undisclosed, or do not use them to send messages that may be misused, is made solely dependent on their desire not to work with the attacker. In practice, however, a distinction must be made between the machine and the person that configures and monitors them. The description of the cryptographic protocol may however present the control components as autonomous trustees.
4.4.12	(On Art. 5 para. 6) The software of control components should be simple to analyse and be limited if possible to elementary cryptographic functions.
4.4.13	(On Art. 5 para. 6) The control components must be set up, updated, configured and secured in a observable procedure.
4.4.14	(On Art. 5 para. 6) The control components must be as distinct as possible from each other and must operate independently of the other control components. This serves the purpose that one successful unauthorised access, will hardly confer any advantage in an attempt to access a further control component undetected (implementation of "trustees"; see No 4.4.12). As a result, the trustworthiness of a group of control components remains guaranteed. To this end, as a minimum the following measures must be planned: – The operation and supervision of the control components should be the responsibility of different persons. – The hardware and the monitoring systems for the control components should be distinct from each other. – The control components should be connected to different networks. – They may only be physically and logically accessible to persons who are responsible for the operation and monitoring of a given control component. Attempted access by persons responsible for other control components must be recognised and reported to the the persons responsible for the relevant control components.
4.4.15	(On Art. 5 para. 6) The control components must carry out only the planned operations. They must be set up 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 recording of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be particularly trustworthy and reliable.
4.4.16	(On Art. 5 para. 6) At least four control components per group with different operating systems should be used. If the control components are devices that have been specifically developed and tested to carry out cryptographic operations securely (hardware security module, HSM), a group may consist of two control components from different manufacturers. Both HSMs may use the same operating system.
4.4.17	(On Art. 5 para. 6) An HSM must have a trustworthy certificate to confirm that the secret elements are inaccessible and that it registers any use of the secret elements so that the responsible person can recognise any improper use. The certificate must correspond to a mimimum analogous inspection depth of EAL4 according to the Common Criteria or FIPS 140-2 level 3. It is permitted to enhance an HSM with software that runs in a protected area. The certificate must in this case also cover the reliability of the protected area. The software and its correct installation must be examined.

5. Examination criteria for the systems and their operation (authorisation for more than 30 per cent of the cantonal electorate)

Each of Sections 5.1 – 5.6 corresponds to an examination test of the system. If the examination is successful, the responsible organisations create a report for the canton that has instructed the examination. The canton encloses the report in its application for authorisation from the Federal Chancellery. The supporting documents that have to be submitted are summarised in Section 6.

5.1. Examining the cryptographic protocol

5.1.1	Examination criteria: The protocol must meet the security objective according to the trust assumptions in the abstract model in accordance with Section 4. In addition, a cryptographic and a symbolic proof must be provided. The proofs relating to cryptographic basic components may be provided according to generally accepted security assumptions (for example, the "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). The protocol should be based if possible on existing and proven protocols.
5.1.2	Responsibilities: The proofs must be provided or examined by highly specialised institutions. The choice of an organisation must be approved in advance by the Federal Chancellery. The specific procedure is as follows: 1. The canton notifies the Federal Chancellery that it wishes to use a new protocol or modify the existing one. The canton may propose which institution or which person should carry out the test. 2. The Federal Chancellery assesses the proposal. 3. The Federal Chancellery informs the canton of its decision. In the case of individually verifiable systems, simple protocols may be used due to the strong trust assumptions. In this case, the Federal Chancellery may dispense with involving an external organisation.
5.1.3	Term of validity of a proof: A complete review must be carried out before the system is used for the first time. The protocol must be examined again whenever the protocol is modified and in the event of substantial new research findings in relation to the security of the cryptographic elements used.

5.2. Examining functionality

5.2.1	Examination criteria: Functionality must meet the requirements set out in Sections 2, 3 and 4, and support the specified objectives adequately. If needed, a protocol must be implemented in accordance with Art. 4 or Art. 5. It should be ensured that the Security Functional Requirements (SFR) specified in the Protection Profile (PP) of the German Federal Office for Information Security (BSI) or equivalent resources are used as security measures. Functionality must be tested according to the formalism of the Common Criteria (CC) on the basis of the EAL2 main criteria.
5.2.2	Responsibilities: The test is carried out by an institution accredited by Swiss Accreditation Service (SAS).
5.2.3	Term of validity of a proof: Functionality must be tested again in the event of any substantial modification, such as the modification of the cryptographic protocol.

5.3. Examining the infrastructure and its operation

5.3.1	Examination criteria: The system and its operation must meet the requirements set out in Sections 2, 3 and 4, and support the specified objectives adequately. The information security of the system and its operation must be guaranteed by setting up, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS) in accordance with ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements). The scope of the ISMS must include all the system operator's organisational units that are legally, administratively and operationally responsible for the system.
5.3.2	Responsibilities: The effectiveness and appropriateness of the ISMS must be proven by submitting the certificate issued by a certification agency that certifies the certification of the ISMS in accordance with ISO/IEC 27001:2005. In addition the certification agency must certify that the requirements described in Sections 2, 3 and 4 have been met, insofar as these have not already been covered by the audit in accordance with ISO/IEC 27001:2005. The certification agency must be accredited by the Swiss accreditation service (SAS) for the conduct of ISO/IEC 27001:2005 audits.
5.3.3	Term of validity of a proof: Repeat audits must be carried out at the intervals required by ISO 27001:2005. A valid certificate must be submitted for each use. Following a decision to dispense with or substantially modify a monitoring measure that serves the secure and independent use of control components, a repeat audit must also be carried out. If a new version of the standard ISO/IEC 27001:2005 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.

5.4. Examining the control components

5.4.1	Examination criteria: The control components must meet the requirements set out in Section 4 and support the specified objectives adequately. Functions whose trustworthiness is essential to the substantiveness of the proofs provided for in relation to verifiability must be examined in detail on the basis of the source codes and the cryptographic protocol. It should be ensured that the Security Functional Requirements (SFR) specified in the Protection Profile (PP) of the German Federal Office for Information Security (BSI) or equivalent resources are used as security measures. Functionality must be tested according to the formalism of the Common Criteria (CC) on the basis of the EAL4 main criteria. Basic components, such as software that aids the secure and independent use of control components, the operating systems used or the server used must be proven to meet the best standards.
5.4.2	Responsibilities: The examination is carried out by an institution accredited by the SAS.
5.4.3	Term of validity of a proof : control components must be retested in the following cases: in the case of any modification to source code of functions whose trustworthiness is essential to the validity of the proofs provided for in relation to verifiability; and if mechanisms that aid the secure and independent use of control components are dispensed with or substantially modified; and in the case of an HSM, the functions whose trustworthiness is essential to the validity of the proofs provided for in relation to verifiability, must in every case be loaded as part of an examination. If new versions of basic components (new servers, patches for operating systems or software that aid the secure and independent use of control components) are used, no new checks are required provided the basic components are still proven to comply with the best standard.

5.5. Examining protection against attempts to infiltrate the infrastructure

5.5.1	Examination criteria: Competent attackers from the Internet must not be able to infiltrate the infrastructure to gain access to important data or take control of important functions. To test this, a specialist institution will attempt in a penetration test to see if it can infiltrate the infrastructure on the basis of the system documentation, by exploiting known weaknesses in the technologies used. As system documentation, the institution must at least be provided with documents on the architecture, data flow and the technologies used. It tests as a minimum weaknesses that are documented in the Open Web Application Security Project (OWASP).
5.5.2	Responsibilities: The test is carried out by an institution accredited by the SAS.
5.5.3	Term of validity of a proof: After three years a new test must be carried out.

5.6. Examining a print office

5.6.1	Examination criteria: In addition to provisions set out in the list of requirements for printing offices, a print office must meet the requirement of Section 4.2.5.
5.6.2	Responsibilities: The test is carried out by an institution accredited by the SAS.
5.6.3	Term of validity of a proof: After two years a new test must be carried out. If it is decided to dispense with or substantially modify a measure, the test must also be repeated.

6. Documentary evidence to be submitted for authorisation

6.1	The applicant canton submits the documentary evidence on the examinations (see Art. 7) that it has received from the responsible institutions. The report on the test in accordance with Section 5.3 must include a valid certificate under ISO/IEC 27001:2005 handeln.
6.2	The canton may claim that a document is valid for two or more ballots. In such a case, the canton must explain why it has not carried out a repeat of the relevant test for the current ballot. In addition, it must provide details of all modifications to the system carried out or planned up to the time of the ballot. In doing so, it must show that these are minor alterations that have no negative influence on the risk assessment.
6.3	The canton submits all test reports that result from implementing the test concepts (Sec. 3.5). It undertakes to submit further test reports if a test is carried out shortly before the ballot.
6.4	The canton submits its current risk assessment (Art. 3) and undertakes to give immediate notice of any changes in the risk assessment. All risks to meeting the security objectives that arise must be determined in a risk assessment. In addition, risks must be assessed that relate to the environment for vote casting as perceived in its administration and by the general public. The assessment must be carried out according to a methodology that requires the following activities: -- identifying risks -- analysing risks -- assessing risks The details of the methodology used and the risk acceptance criteria specified by the canton specified must be documented. For risks that relate to operating the system, the methodical requirements of ISO/IEC 27001:2005 must be met in their entirety when identifying risks in the case of the authorisation of more than 30 per cent of the cantonal electorate.