# 1. Introduction

1.1 Purpose of the document

# 2. E-voting solution

# 3. Voting process

3.1 Preparation of the contest

3.1.1 Description

3.1.2 Technical infrastructure used

3.2 Electronic casting of ballots by voters

3.2.1 Description

3.2.2 Technical infrastructure used

3.3 Counting of the electronic vote

3.3.1 Description

3.3.2 Technical infrastructure used

3.4 Auditing of the results

# 4. IT infrastructure

4.1 Data centers & BCM

4.2 Online voting portal (OVP)

4.3 Control components layers

4.4 Database infrastructure

4.5 Separation and linking of cantons

4.5.1 Separated infrastructure

4.5.2 Access points for cantons

4.6 E-voting access layer

4.6.1 Reverse proxy infrastructure

4.6.2 Security policy

4.7 SDM

# 5. E-voting security
5.1 Security measures
5.1.1 Access layer / reverse proxies
5.1.2 Firewalls, zones and areas
5.1.3 SDM access
5.1.4 Operating system
5.1.5 OS firewalls
5.1.6 DDoS defence strategy
5.1.7 Mutual authentication at SSL/TLS level
5.1.8 Integrity monitoring
5.1.9 JS response check (response monitoring)
5.1.10 E-voting monitoring
5.1.11 E-voting deployment process

5.2 Special security of the control components
5.2.1 Overview
5.2.2 Physical separation
5.2.3 Different operating systems
5.2.4 Special zones
5.2.5 Access alarms
5.2.6 Root password principle

5.3 Security measures for access via the Internet
5.3.1 SDM access to the admin portal
5.3.2 Voter access to the voter portal
5.3.3 Air-gap principle

5.4 Dedicated organizational security measures
5.4.1 Dual-checking principle – Login
5.4.2 Supervised fitting, installation, configuration and maintenance of the control components
5.4.3 Expanded security screening of e-voting operational employees
5.4.4 E-voting threat intelligence

6. E-voting operation
6.1 Operational principle of Swiss Post Informatics ......................................................... 32
6.2 E-voting operation ........................................................................................................ 32
  6.2.1 E-voting platform operation (e-voting IT service) .................................................. 33
  6.2.2 E-Voting Competence Center ............................................................................... 33
  6.2.3 E-voting deployment process ............................................................................... 34
  6.2.4 Release and change management ......................................................................... 34
  6.2.5 E-voting monitoring .............................................................................................. 34
  6.2.6 E-voting escalation and crisis management .......................................................... 34
1. Introduction

1.1 Purpose of the document

Swiss Post believes that transparency is vital in order to gain the confidence of the voters and cantons when it comes to electronic voting. The Federal Chancellery Ordinance on Electronic Voting (OEV) specifies the following in paragraph 3 of Article 7b, “Procedure for publishing the source code”.

*The documentation for the system and its operation must explain the relevance of the individual elements of the source code for the security of electronic voting. The documentation must be published together with the source code.*

This document describes the procedure for the vote, the platform (infrastructure), security and the operation of Swiss Post’s e-voting solution.

2. E-voting solution

The core e-voting software used at Swiss Post was developed by Scytl in Barcelona in cooperation with Swiss Post. The reliable services from Post CH Ltd make it possible to provide a secure digital channel and are a supplement to traditional election and voting systems, under the control of the cantons.

The software itself already fulfils strict security requirements and the data is completely encrypted, from vote casting through to evaluation. More detailed information about the software and other publications are available at [https://www.swisspost.ch/evoting](https://www.swisspost.ch/evoting) in the section “Transparency and publications” and “Source code”.

The infrastructure is designed to be catastrophe-proof and can reliably prevent unauthorized access from both external and internal origins.

The e-voting solution and its operation are fully certified by accredited auditing agencies in terms of individual verifiability (50 percent), as well as in terms of complete verifiability (100 percent).

---

1 OEV Article 7b, paragraph 1: [https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsbedingungen.html](https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsbedingungen.html)
3. Voting process

The technical components which are used in electronic voting are shown in the following diagram.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pre-election (canton infrastructure) | Pre-processing SDM (workstation without network connection) | Prior to the contest, the contest is configured using the pre-processing SDM (secure data manager).
- Generation of the keys by the electoral authority (in Switzerland several names are used, e.g. also electoral commission).
- Collation of the calculations from the control components and decryption of the codes needed for the vote casting process in a secure and trustworthy environment. The codes are subsequently passed on in encrypted form to the printer.
- The creation of the configuration for the e-voting system.
- Signing and encrypting the files created.
- Storage of the files created on an encrypted data carrier for transfer to the online workstation. |
<table>
<thead>
<tr>
<th>Phase</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pre-election (canton infrastructure) | Online SDM (workstation with network connection) | - Transfer using a secure internet connection of the contest configuration to the Swiss Post voting system and sealing.  
- Initiation of calculations for the codes.                                                                                                           |
| Election (contest)            | Voter’s device                                  | The voter’s device which is used to cast the vote  
This includes all common devices with web browsers.                                                                                                      |
|                               | OVP (online voting platform)                    | The election and voting portal is located on this server, which enables the provision of e-voting.  
- Stores the encrypted votes.  
- Ensures user authentication.  
- Makes the website available for the casting of votes.  
- Carries out the cleansing process (auditing for accuracy of the individual votes, e.g. whether the casting of the vote was finalized using a ballot casting key). |
| Post-election                 | Online SDM (workstation with network connection) | After the closure of the ballot box, the following steps are taken:  
- Retrieval of the electronic ballot box with the encrypted votes.  
- Storage of the file with the encrypted votes on a data carrier for transfer to the post-processing SDM offline workstation.  
- Initiation of the mixing and cleansing processes (see also OVP and control components) |
| Post-election                 | Post-processing SDM (workstation without network connection) | - Retrieval of the files with the encrypted votes that are stored on a data carrier.  
- Launch of the final decryption process (votes can be decrypted only when all control components and the electoral authority are involved).  
- Storage of the decrypted votes.  
- Beginning of counting.  
- Generation of a file with the results for the municipalities.  
- Storage of the files with the results and the receipt confirmations on a data carrier for transfer to the workstation with the online SDM |
| Post-election                 | Verifier (workstation without network connection) | At the end of the contest, the logs are transferred to this workstation.  
- The verification of the accuracy of the results is undertaken using logs from the SDM components (online, pre- and post-processing), as well as from the secure logs of the control components. |
<table>
<thead>
<tr>
<th>Phase</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>During various phases</td>
<td>Control component</td>
<td>The control components are involved in three phases of the contest. - The generation of the codes needed for the casting of ballots. - When a citizen casts a vote, the codes are calculated again. These codes must match the codes printed on the voting card. - The <strong>mixing</strong> process is carried out on three control components after the closure of the electronic voting channel. In the mixing process, the votes are mixed up, meaning that no conclusions can be drawn as to who cast which vote. Simultaneously, each control component decrypts the votes, in part using their private keys. This prevents an individual control component from decrypting the vote.</td>
</tr>
</tbody>
</table>

3.1 Preparation of the contest

3.1.1 Description

The files for the configuration of the contest and the voting register are needed for the preparation of the contest. In this process, the E-Government Standards eCH-0045, eCH-0157 and eCH-0159 are used. For further details, see https://www.ech.ch.

The electoral authority subsequently plays a role in the generation of the certificate for the encryption of voters’ votes. The secret key is protected by all members of the electoral authority by the fact that each person has part of the key. E-voting administrators transfer the contest configuration into the e-voting system. The connection to the e-voting system is made using two-factor authentication.

All members of the electoral authority cast their votes in a fictitious municipality and record their answers in a log which should be retained in sealed envelopes until the closure of the electronic ballot box. The result is checked against the log on the contest date (i.e. election Sunday) and is intended to demonstrate that no changes were made.

Amongst the configuration files generated is the file which contains the start voting keys for the vote, verification, confirmation and finalization of the individual voting cards. This signed and encrypted file is used for the generation of the voting cards. During the generation of the voting cards, signed and encrypted files are created. These files are then brought personally and using the dual-checking (two-person) principle to the printer. The password for the decryption of the voting cards is transmitted via another secure channel.
3.1.2 Technical infrastructure used

The infrastructure used for the configuration of the electronic ballot box is a commercially available workstation. The workstation (online SDM) is connected to the Swiss Post management portal using a secure internet connection. The data for the contest is imported into the management portal and is synchronized with the connected workstation.

After the synchronization, the data is transferred using an encrypted data carrier (see also 5.3.3 Air-gap principle) on to the workstation with the pre-processing SDM, which has no network connection (no Internet access). The preparation of the codes needed for casting a vote is carried out on this workstation. The electoral authority also signs the data for the contest on this workstation.

Once the configuration of a contest is completed, this configuration is imported into the e-voting system. For this, the data is transferred using a data medium on to the “online SDM” workstation. The configurations are then synchronized with Swiss Post’s e-voting portal, using a secure connection. The workstations are stored in a locked cabinet at the state chancellery or with the police.
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Security elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online SDM</td>
<td>The workstation connected to the Swiss Post infrastructure which is used for the configuration and transmission of the data. Installed software:</td>
<td>Up-to-date operating system, browser and anti-virus software; has a certificate, so that it can connect to the Swiss Post infrastructure. The systems are also subjected to a hardening in accordance with specifications.</td>
</tr>
<tr>
<td></td>
<td>- SDM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Web browser</td>
<td></td>
</tr>
<tr>
<td>Pre-processing SDM</td>
<td>Workstation used for:</td>
<td>Workstation without network connection. The systems are also subjected to a hardening in accordance with specifications.</td>
</tr>
<tr>
<td></td>
<td>- Collates the calculations from the control components and decrypts the codes needed for the vote casting process in a secure and trustworthy environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The codes are subsequently encrypted and passed on to the printer for the creation of the voting cards.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Encryption and signing of the contest data by the electoral authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed software:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SDM</td>
<td></td>
</tr>
<tr>
<td>E-voting platform</td>
<td>Application server which provides web interfaces for the administration of the electronic casting of ballots and web services for the provision of e-voting. This server communicates with the voting database server.</td>
<td>See the Security chapter</td>
</tr>
<tr>
<td>Database server for the electronic ballot box</td>
<td>Database server which stores all encrypted votes in the electronic ballot box and the configuration elements for the electronic casting of ballots.</td>
<td>See the Security chapter</td>
</tr>
</tbody>
</table>
3.2 Electronic casting of ballots by voters

3.2.1 Description

The electronic casting of ballots is automatically activated and deactivated by the electoral authority using the parameters set during the configuration process.

Voters access the election and voting portal. They will find the details required for e-voting on their voting cards. To cast a vote, they log in to the election and voting portal. They enter the start voting key and an additional personal detail such as year of birth and cast their vote. The choice return codes are then displayed on the voter’s screen. The voter checks the choice return codes and confirms their accuracy by entering the ballot casting key. The voter receives the vote cast code as a result of this, which needs to be compared against the voting card.

3.2.2 Technical infrastructure used

The infrastructure used for e-voting is divided into three parts. Firstly, the voter uses his or her own infrastructure (workstation, private network etc.). The votes are then cast using the portal hosted by Swiss Post. And finally, the votes are stored in the ballot box which is hosted on Swiss Post’s systems. Swiss Post’s infrastructure is split across two locations.
3.3 Counting of the electronic vote

3.3.1 Description

Once the electoral authority has assembled, the cleansing process is started. Subsequently, the control components, one at a time, mix and partially decrypt the votes. Afterwards, the partially decrypted votes are downloaded. The connection to the e-voting system is made using two-factor authentication with smartcards.

The ballot box is transferred to the post-processing SDM workstation (without network connection). Next, the counting process is undertaken. The members of the electoral authority are first asked for the smartcards, which contain part of the password-protected private key, and the relevant passwords. The votes and the receipt confirmations are then decrypted and the results retrieved. The results of this process are extracted into a signed XML file. The results are also displayed in a PDF report.

The votes cast by the members of the electoral authority (see 3.1 Preparation of the contest) are now audited. The audit takes place in conjunction with the log and is intended to be an additional confidence-building measure.

The XML file is then imported into the canton’s result calculation system, with the e-voting results being added to votes received using other channels.

3.3.2 Technical infrastructure used

To retrieve the encrypted votes, the online SDM is used. This is connected to the e-voting administration server at Swiss Post via a secure Internet connection. Only this server has access to the e-voting database server.

The infrastructure used for the decryption consists of the post-processing SDM workstation (without network connection / no Internet access). The votes are mixed one last time (mixing), decrypted and the counting is carried out.
These workstations that are used are secured and stored under lock. The removal, use and return of the workstations are logged.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Security elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-processing SDM</td>
<td>Workstation that is used for the final mixing and decrypting</td>
<td>Workstation without network connection. The systems are also subjected to a hardening in accordance with specifications</td>
</tr>
</tbody>
</table>

### 3.4 Auditing of the results

After the votes are counted, the contest process is audited. This is undertaken using a separate workstation (verifier) that audits and verifies all data from the SDM workstations (pre-processing, online, post-processing) as well as Swiss Post’s secure logs. The secure logs are made available to the canton using a secure channel. The transfer of the data to the workstation (verifier) is undertaken using a data carrier (see also 5.3.3 Air-gap principle).
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Security elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifier</td>
<td>Workstation that is used solely to verify the accuracy of the results.</td>
<td>Workstation without network connection. The systems are also subjected to a hardening in accordance with specifications</td>
</tr>
<tr>
<td></td>
<td>Installed software:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Verifier</td>
<td></td>
</tr>
</tbody>
</table>
4. IT infrastructure

Various infrastructure in several data centers is used to operate Swiss Post’s e-voting services. The reverse proxy, control component and database infrastructure is run on Swiss Post’s dedicated virtualization platform.

4.1 Data centers & BCM

Swiss Post has two geographically separated data centers. Our data centers are distinguished by the following features:

Features
- FINMA-compliant, TÜV Dual Site Level 3-certified
- The operator is certified under ISO 20000, ISO 22301 and ISO 27001.
- Full redundancies for critical supply systems
- No single point of failure
- Compliance with permitted climatic limits
- Strongly authenticated access control
- Uninterruptible power supply
- Air-conditioning and fire protection
All e-voting systems are situated in both data centers to provide geo-redundancy. If the primary data center fails, the other data center takes over the services. In addition to location redundancy, room redundancy is also guaranteed within a data center. This guarantees business continuity at all times.
4.2 Online voting portal (OVP)

The OVP layer is integrated into Swiss Post’s DCP virtualization platform. The virtualization platform mirrors Swiss Post’s software-defined data center (SDDC). The system consists of computer, network and storage infrastructure and is provided as a service. The system can be set up and expanded on a modular basis.

The following graphic shows the components of the virtualization platform.

From the perspective of the virtualization platform and the SDDC, clients are logical system limits that make it possible to separate virtual systems, data and users.
4.3 Control components layers

As part of the complete verifiability, what are known as control components have been used for various activities.

The following graphic shows how the control components are integrated with the overall system.

All control components are based on dedicated hardware that is designed to be catastrophe-proof. Each control component group (also known as a CC group) has its own hardware. The four CC groups are also based on different operating systems.

By using the four control component groups, the aim is for the cryptographic operations to be verified by several systems and different technologies (e.g. different operating systems). One aspect of this is the fact that the operations are performed in parallel and that the end result is valid only when all four results are identical. Another is that operations such as mixing are conducted in sequence, meaning that the end result is valid only if all four partial results are accurate.
4.4 Database infrastructure

The e-voting database infrastructure comprises three productive and two integrative dedicated systems. Data is therefore triple-mirrored (saved synchronously three times). The infrastructure also ensures that the requirement for zero data loss is met.

The following graphic shows the technical implementation.
4.5 Separation and linking of cantons

4.5.1 Separated infrastructure

Each canton has its own e-voting environment that is logically completely separated from other cantons’ environments. Only the control components are used jointly. As these are stateless and perform calculation operations only, a separation of cantons is not necessary at this level.

In addition to the separation of cantons, there is a dedicated access layer (reverse proxy infrastructure) that has been set up for voters and cantonal administrators. Various demo, test and integration environments are also available.

Key:
- FEV: Frontend e-vote
- BEV: Back office e-vote
- BEA: Back office e-vote admin portal
- RP: reverse proxy
- CC\(_n\): Control component

The e-voting setup for each canton encompasses two separate parts: the public voter part and the admin part. Both are completely separate; interconnections are not permitted and are prevented by firewalls. The admin part is used to create a contest with the SDM (secure data manager). The contest is set up in the voter application via a specially secured channel. The voter part is used for the actual contest for voters. Both the public voter part and the admin part comprise several layered servers in various network areas/layers separated by firewalls.
- Access layer: reverse proxy
- Application layer: frontend server (application server, static file host)
- Application layer: backend server (application server, application logic)
- Database layer: database (storage location of encrypted ballot papers in the encrypted ballot box)

The reverse proxy layer exists in two variants:

- **Variant: Swiss Post IT reverse proxy (model 1)**
  In the reverse proxy variant, the voter's browser or canton's secure data manager (SDM) accesses the reverse proxy infrastructure. The reverse proxy infrastructure carries out a security test and, in the case of the SDM, carries out authentication. The request is then forwarded to the frontend server in Swiss Post's canton layer/application layer.

- **Variant: canton reverse proxy (model 2)**
  The canton provides the access layer for voters itself. From the canton's systems, the requests directly reach Swiss Post's canton layer/application layer via a separate network. The SDM devices use the same channel as for model 1. Model 2 allows a canton portal (e.g. Guichet Virtuel) to be connected securely to Swiss Post's e-voting infrastructure.
4.5.2 Access points for cantons

As described above, there are two access points for cantons. If the canton has its own infrastructure and portal, voters of the relevant canton can vote using this portal. Cantons without their own portal may use Swiss Post’s voter portal for their voters.

The following graphic illustrates the access points.
4.6 E-voting access layer

4.6.1 Reverse proxy infrastructure

Swiss Post’s reverse proxies run on physical hardware. For each data center, there are two physical productive servers and a total of four servers for the e-voting environment. Reverse proxy functionality is ensured through multiple instances of the reverse proxy software for each server. For each hardware server, there is a voter reverse proxy, a voter SDM reverse proxy and an admin reverse proxy per canton. The instances are logically separated from each other. They run on a highly secure operating system as different users with different certificates and separate IP addresses on specially robust servers.

For access via the voter SDM and the admin reverse proxy, connections are authorized using a client certificate.

4.6.2 Security policy

An open-source security policy is used on the reverse proxies. This is a module that offers protection from attacks. The module operates two different security policies. The voting reverse proxy must be accessible to international clients. Access can therefore not be authenticated using a client certificate. For this reason, a bespoke policy has also been developed for the voter reverse proxy that exclusively permits a narrow, pre-defined server access list.

4.7 SDM

The SDM (secure data manager) is the tool that cantons use to initiate and complete the contest. The SDM is therefore used before the start of the contest and after it is completed. It is not used during a contest. The SDM is operated on the infrastructure of the relevant canton. Various workstations (clients) are also used depending on the voting phase, with some of these being used solely offline. For further details, see the chapter “Voting process”.

---

Use only for private, non-commercial audit purposes.
5. E-voting security

Scytl’s e-voting software already provides comprehensive security for the contest and the electronic ballot boxes using a second-generation voting protocol, individual verifiability and end-to-end encryption. Swiss Post ensures the transport of encrypted ballot papers and encrypted ballot boxes. Swiss Post cannot decrypt the data at any time. This transport is secured on Swiss Post’s systems using additional security measures. The following diagram presents a summary of the security-relevant aspects implemented for Swiss Post’s e-voting solution.
5.1 Security measures

5.1.1 Access layer / reverse proxies
A large proportion of security measures are concentrated on the access layer with its reverse proxies and are described in the chapter on the 4.6 e-voting access layer. Essentially, this involves implementing mandatory access control both on the operating system and application levels.
This is undertaken by measures including an Open Source Web Application Firewall. This is operated with various common and established policies.
In the architecture model, in which the canton operates the voter reverse proxies itself, the canton ensures that the same or comparable security checks are carried out before the requests are passed on to the application at Swiss Post.

5.1.2 Firewalls, zones and areas
The zone and area concept separates the servers from each other within the network. This means that the access layer, voter frontend, voter portal, admin portal, admin backend and database are in different network segments. Each zone and each area are protected by firewalls. The connection takes place using regulated and defined firewall rules. The traffic allowed through a firewall and traffic not permitted through a firewall is defined in the firewall policy. The access layer is physically separated from the rest of the e-voting infrastructure.

5.1.3 SDM access
The SDM (secure data manager) with which the contest is set up and with which the election results are collected is connected to the admin reverse proxy and the voter SDM reverse proxy. Access is enabled for authenticated devices only. The SDM client is always used according to the multiple-control principle and is safely stored when not in use.

5.1.4 Operating system
The servers for the online voting portal (OVP) and the reverse proxies are operated using an open source, high-security operating system. The operating system supports the access control mechanism.
This high-security operating system means that an e-voting server process runs in a separate context and is fully encapsulated. This means that a process can only use the system’s designated resources. All other resources are not available to it (mandatory access control).
The operating systems for the control components differ from one another. For details, see chapter 5.2 Special security of the control components.
5.1.5 OS firewalls
In addition to Swiss Post’s own physical network firewall, firewall software is used on the entire e-voting platform and at operating system level. Only access to the necessary system management ports and from defined web server IP addresses is allowed.

5.1.6 DDoS defence strategy
Swiss Post pursues a holistic approach so that it is able to stave off DDoS attacks of any scale. The strategy stipulates that different measures should be taken for different sizes of DDoS attacks. The measures are wide-ranging and include the involvement of the service provider and companies specializing in DDoS, in addition to internal technical measures.

5.1.7 Mutual authentication at SSL/TLS level
All servers communicate in a way that is encrypted. They always authenticate each other using certificates. This ensures full end-to-end encryption (from data entry to vote counting) for e-voting.

5.1.8 Integrity monitoring
For e-voting, Swiss Post uses an open-source solution on the entire platform for operating system integrity monitoring and as an IDS (intrusion detection system). By using this integrity monitoring, every unplanned change to the system is detected.

5.1.9 JS response check (response monitoring)
The reverse proxy validates the JavaScript files that are sent to a client (voter). This means that the reverse proxy checks files’ hashes in the HTTPS response body that are delivered by the backend systems. In the event of a deviation from the configured hash value, it prevents the delivery of a possibly manipulated file. This represents a control measure that ensures the correct JavaScript-based encryption of ballots on the client.

5.1.10 E-voting monitoring
The infrastructure components are monitored in accordance with a standardized and ISO-certified process. Alarming takes place as per defined thresholds by SMS and/or e-mail alerts.

In addition to this monitoring, voter monitoring has been developed for e-voting. The e-voting application generates specific logs with events that can be assigned to individual phases in the voting process. These can be used to monitor the contest in real time. This monitoring is used to verify that the electronic vote casting procedure is carried out properly. Critical situations or anomalies during a contest trigger an alert that is sent to the defined entities. The votes are always fully anonymized and encrypted during this process and accordingly cannot be traced back to the voters.
5.1.11 E-voting deployment process

The deployment process describes the manner in which a new release from the software supplier will be applied to the e-voting platform. It is important to note that the supplied release is checked for integrity using a checksum and deployment will be only possible using the dual-checking principle. Each deployment is recorded in Swiss Post’s change management tool, tracked, and tested and approved following deployment completion.

5.2 Special security of the control components

The control components are subject to special security. In the trust model of universal verifiability, only the control components in their combination are trusted. In addition to the security elements of the e-voting platform already mentioned, additional precautions have been taken to boost security that support the trust model.

5.2.1 Overview

The control components are operated independently of each other, so that any successful attack on one component will not have an effect on other components. As a result, the trustworthiness of a group of control components remains guaranteed.

The operation and monitoring of the control components are the responsibility of different persons. The hardware and the monitoring systems for the control components are distinct from each other. The control components are connected to different networks. They are accessible only to persons who are responsible for the operation and monitoring of a given control component. All attempts at access are detected and are reported to the persons in charge of the corresponding control components.

5.2.2 Physical separation

The control components consist exclusively of physical servers (bare metal approach), are located in different networks and are operated by different teams. The control components also differ from each other physically. This means that different server models with different process architectures are in use.

Each control component is physically present in both data centers. The two components located in both DC1 and DC2 are connected by a load balancer. The primary function of this load balancer is to ensure high availability. If a control component in one data center fails, the other control component located in the other data center takes over the service. Even in the event of a total failure of one of the data centers, this concept ensures seamless operation.
This process also ensures that no control component of the same or another group is physically installed in the same rack.

5.2.3 Different operating systems
To fulfil the differentiated approach, different operating systems are used depending on the control component.

5.2.4 Special zones
A specific area has been established in a dedicated secure zone at Swiss Post for the e-voting control components. This area contains four different zones (1–4), which are connected/protected from each other by a firewall. The e-voting area in turn is separated/protected by a firewall from the other areas in the overall zone. Each additional zone is in turn separated by a firewall.

5.2.5 Access alarms
In addition to the dual-checking principle (see also Chapter 5.4.1 Dual-checking principle), each access of the control component is registered and an alarm is triggered.

5.2.6 Root password principle
The root passwords are changed after initial installation and are stored securely. The release of a root password takes place only after a change has been approved and after the identity of the person requesting the change has been verified. Every release is recorded.

5.3 Security measures for access via the Internet
5.3.1 SDM access to the admin portal
The SDM (secure data manager), with which the contest is set up and with which the election results are collected, is connected to the admin reverse proxy. The secure connection is based on current and secure cryptographic processes.
5.3.2 Voter access to the voter portal

The voter’s access to the voter portal takes place with the voter’s browser and is SSL encrypted. Voters can verify that they are on the correct e-voting page either by using the fingerprint from the SSL certificate (located on the voting card), or by using the hash value from the cryptographic section of the e-voting application (published on the landing page of the relevant canton).

5.3.3 Air-gap principle

The operates several workstations (clients) with the SDM software. These are required to carry out and to verify a contest. A general distinction is made between online and offline devices. An offline device does not have any access to the network at any time. Data is transferred solely using an encrypted data carrier. The following process visualizes the air gap principle for setting up a contest. Devices with a red square are so-called offline workstations. Data is not copied on to these using a network connection, but only by using a medium intended for the process, such as a USB stick.

5.4 Dedicated organizational security measures

5.4.1 Dual-checking principle – Login

The dual-checking principle (more precisely: the segregation of duties principle) controls administrative access to the control components of e-voting. When a Swiss Post IT system administrator wants to access an e-voting component, they require a token number that they receive from another person from another department after their identity and reasons for access have been checked. This token number is valid only once and becomes invalid once the administrator logs out.
5.4.2 Supervised fitting, installation, configuration and maintenance of the control components

In accordance with legislation, the fitting, installation and configuration of the control components must take place in a supervised process. For this, there is a defined process and also corresponding acceptance protocols.

5.4.3 Expanded security screening of e-voting operational employees

Swiss Post IT is organized based on the ITIL framework, certified to ISO 27001, and the separation of responsibilities is clearly defined. Operations staff have been subjected to thorough security screening in accordance with ISO 27001 and can be described as particularly trustworthy and reliable.

The operation of the control components for the e-voting solution calls for higher security requirements for the staff involved.

All members of the affected teams are responsible for the operation of the e-voting solution, in addition to other tasks, and are screened according to the processes.

Swiss Post HR uses the job description to check which employees will be involved in the operation of the e-voting solution, and requests the required supporting documents from them. Staff who cannot provide these supporting documents may no longer be involved in the operation of the e-voting solution. The required permissions will be withdrawn. During the entire employment period, team leaders can contact HR if they have made any observations which call the trustworthiness of an employee into question. All team leaders are informed of the security requirements that employees need to fulfil, and review these before the first deployment of a new staff member.

All Swiss Post employees are trained generally on how to handle data relevant to security, and e-voting staff receive an introduction to the e-voting process that explains the necessity of the increased security requirements.

Team leaders are also made aware by HR on an annual basis of the need to constantly report security-relevant situations involving employees (breaches of duties, unusual behaviour, threats etc.) to the responsible entity.

5.4.4 E-voting threat intelligence

CERT-Post supports the security organization and specialist services by using threat intelligence to deliver early warnings and provide insights that can be used to reduce risks. On the basis of this analysis, a forecast about likely threat situations is created, so that Swiss Post Informatics can proactively react, close security gaps and can adjust its security concept.

The challenge is clear: Internet criminals are operating in a way that is more and more refined and professional. As a company, Post CH Ltd is therefore compelled to constantly adjust and expand the
measures at its disposal. For this reason, Swiss Post IT has co-operated with international CERT organizations for years, and has also taken part in specialist committees. The collaboration is helping security experts to gain a complete picture of the risk situation on the Internet and to take the right measures to protect e-voting.

Post CH Ltd sees e-voting as one of its assets that is most worthy of protection in the Group’s IT architecture. If the CERT network reports new threats, these are analyzed and the risks stemming from these are documented.
6. E-voting operation

6.1 Operational principle of Swiss Post Informatics
Swiss Post IT is organized closely around the ITIL framework, and is certified to ISO 27001, ISO 22031 and ISO 20000. All IT disciplines are split up and are organized in different teams. This operational principle is ideal for achieving a segregation of duties for the operation of an e-voting solution on a 100 percent basis.

6.2 E-voting operation
Swiss Post’s e-voting service is organized in several dimensions in order to meet all customer needs. The graphic below shows this visually. T2P refers to “Transition to Production”. In this process, employees from e-voting support the canton in the move from the transition to the production phase.
6.2.1 E-voting platform operation (e-voting IT service)

The following table indicates which layers of the e-voting platform are present and how they are operated. The individual layers are operated by different operations teams. For control components, several teams which operate the individual groups are involved.

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Operations teams</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reverse proxy</td>
<td>One team</td>
</tr>
<tr>
<td>2</td>
<td>OVP (online voting portal)</td>
<td>One team</td>
</tr>
<tr>
<td>3</td>
<td>Control components</td>
<td>Several teams</td>
</tr>
<tr>
<td>4</td>
<td>Database</td>
<td>One team</td>
</tr>
<tr>
<td>5</td>
<td>DCP (OVP operating platform)</td>
<td>One team</td>
</tr>
</tbody>
</table>

6.2.2 E-Voting Competence Center

The E-Voting Competence Center bundles all services involved in the operating phase of electronic voting. These include specialist and support services in particular. During the project phase, the Competence Center ensures Transition to Production (T2P), and provides specialist support for new set-ups. Release, test and quality management are additional disciplines located within the Competence Center.

Tasks of the Specialist Service:
- Application support
- Specialist support for new set-ups
- Customer advice and requirements management
- Maintenance management for extraordinary elections and votes
- Change management
- Service monitoring and reporting
- Testing
- Support for release management

Tasks of Support:
- SPOC
- Fault and taskforce management
- 24/7 support
- Monitoring
- Access management
- E-voting hardware management and support
- Software tool management
- Field service

Tasks of Transition to Production (T2P):
- Ensuring the interface for onboarding
- Manage canton-specific requirements for software and systems
- Ensure quality assurance for the transition to production
6.2.3 E-voting deployment process
The deployment process describes the manner in which a new release from the software supplier will be applied to the e-voting platform. It is important to note that the supplied release is checked for integrity using a checksum and deployment will be only possible using the dual-checking principle. Each deployment is recorded in Swiss Post IT’s change management tool, tracked, and tested and approved following deployment completion.

6.2.4 Release and change management
New releases are planned and launched by the system operator in accordance with the ITIL release management process. Swiss Post subjects each new release to comprehensive tests for functionality and security. All changes are carried out solely using Change.

6.2.5 E-voting monitoring
Application and middleware monitoring with five monitoring levels exists, with its main role being to monitor the activities of the application and the elements underlying it. The aim of the monitoring is to raise the alarm in the event of failures of the e-voting infrastructure and services and for all other application and middleware components that are involved. The e-voting monitoring team specifies the application and middleware components that need to be monitored and sets the thresholds for raising the alarm.

In e-voting services, all available monitoring services have been implemented:

- Basic component monitoring
- Basic middleware monitoring
- Security monitoring
- Application monitoring
- Service / health monitoring

In addition to this monitoring, the entire platform is monitored using log, monitoring and reporting tools. All application-related and system-technical activities are logged using these tools. In addition, statistical figures for a contest can be given to a canton. The tool can also be used to compile and provide the necessary information for verifying a contest.

6.2.6 E-voting escalation and crisis management
The escalation pathways are specified at Swiss Post in the event of a taskforce or crisis. The graphic below shows this visually.
Swiss Post has a rapid and skilled taskforce and crisis management team. The graphic below shows this visually.

All potential events that may happen are listed with clear guidelines for action and processes in a incident decision matrix.