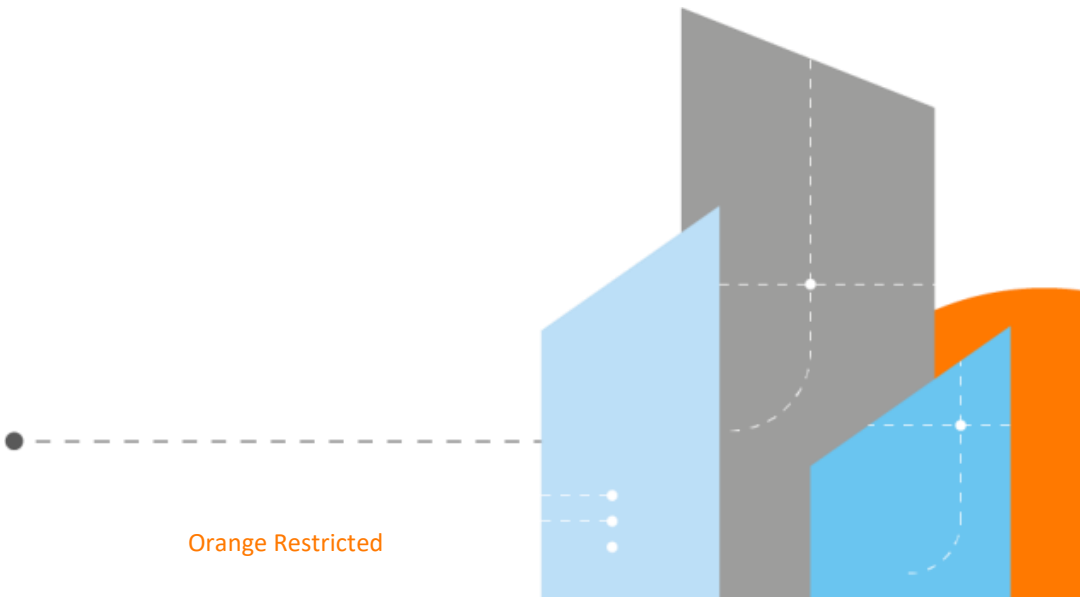
Cyberdefense

Federal Chancellery

Examination of the Swiss Internet voting system

Version: 1.1 / Audit scope: Infrastructure and operations (3) – Measures of the system provider

19 August 2024



Contact information

Address	Contact
Orange Cyberdefense Switzerland SA Rue du Sablon 4 1110 Morges	Stéphane Adamiste Chief Product Officer +41 21 802 64 01 stephane.adamiste@orangecyberdefense.com

Contributor

Name	Date
Stéphane Adamiste	Chief Product Officer, Orange Cyberdefense Switzerland

Document history

Version	Date	Authors	Change details
0.1	2024/07/16	Stéphane Adamiste	Working version
1.0	2024/08/16	Stéphane Adamiste	Released version
1.1	2024/08/19	Stéphane Adamiste	Report improvements, including correction of a mistake in the classification of findings

Contents

Management summary

Context, scope and objective of the examination

This examination work was mandated by the Federal Chancellery following a change operated by the Swiss Post in the e-voting system infrastructure. This change consists in the implementation of dedicated *jumphosts*, used by IT administrators to connect to the e-voting control components. Jumphosts are intermediary servers acting as a gateway to the networks where the control components reside.

The objective of the examination was to assess to which extent the above-mentioned change affects the Post's overall compliance level with the applicable requirements of the Ordinance on Electronic Voting ("VEleS", or "OEV"), audit scope *3 b) Assess the infrastructure and organisational measures of the system provider*.

The examiners did not receive instructions from the Federal Chancellery on which OEV specific requirements to include in the examination. Instead, the scope of their audit was determined at their discretion, focusing on the requirements that might be impacted by the changes made to the infrastructure. A subset of twenty three (23) OEV requirements was selected to form the audit scope.

Results

The introduction of dedicated jumphosts is considered a best practice for network architecture security, and their implementation appears to have been carried out securely. In the examiners' opinion, this evolution in the infrastructure therefore increases the overall security posture of the e-voting environment by strengthening access control to the control components.

However, from a strict compliance perspective, several gaps were identified in relation to the in-scope OEV requirements, including:

- The absence of an operational procedure for the newly deployed jumphosts;
- A lack of a comprehensive, documented threat model for the reengineered network access infrastructure to the e-voting control components;
- The omission of jumphosts in the documents detailing the security monitoring concepts for e-voting infrastructure.

Recommendations

Only succinct recommendations are provided in this document, as the observations formulated are self-explanatory. The implementation of those recommendations requires a small effort at the scale of the e-voting project in the examiners' opinion.

Final note

The examiners conclude this summary by thanking the involved Swiss Post personnel for their cooperation and for the transparency demonstrated throughout the duration of the examination.

1 Context

1. Electronic voting (hereafter referred to as: “e-voting”) was introduced in Switzerland through multiple pilot schemes from 2004 onwards. A total of 15 cantons made e-voting possible in over 300 trials, until early 2019. Two implementations were available: the system provided by the canton of Geneva and the system operated by the Swiss Post (hereafter also referred to as “the Post”), initially developed by Scytl. In June 2019, the canton of Geneva announced the withdrawal of its e-voting system with immediate effect. It was followed in July of the same year by the announcement by the Swiss Post of the withdrawal of its e-voting system from operation to focus on improving the solution. At that point, e-voting was no longer possible in Switzerland.
2. In June 2019, the Swiss Federal Chancellery (hereafter also referred to as “Federal Chancellery”) was commissioned by the Federal Council to redesign a new trial phase, in collaboration with the cantons, using “e-voting systems, which are fully verifiable” [1]. This redesign of the trial phase focused on four objectives:
   a) Further development of the e-voting systems
   b) Effective controls and monitoring
   c) Increased transparency and trust
   d) Stronger connection with the scientific community
3. A taskforce was set up to make proposals for the future of internet voting. To that end, the Federal Chancellery invited experts from academia and industry to engage in a broad dialogue on internet voting in Switzerland. After this dialog, the Federal Chancellery and the cantons published a final report on the redesign and relaunch of internet voting trials, with a catalogue of measures [2].
4. The Federal Council took note of the final report and commissioned the Federal Chancellery to amend the legal bases of the Confederation regarding e-voting. In April 2021, the Federal Council opened a consultation procedure for the redesign of the e-voting trials. The redesign includes both a partial revision of the Ordinance on Political Rights (PoRo) [3] and a complete revision of the Federal Chancellery Ordinance on Electronic Voting (“VEleS”, or “OEV”) [4]. The OEV specifies, among others, the requirements for authorising electronic voting, including the technical and administrative controls for approving an e-voting system.
5. The Federal Chancellery issued an audit concept for the examination of Swiss internet voting systems defining the foundations for assessing the compliance of electronic voting systems with the draft OEV and its annex, as per chapter 26 of the annex of the draft OEV, and for obtaining recommendations for improvements [5].
6. SCRT (now “Orange Cyberdefense Switzerland”) was mandated by the Federal Chancellery to assess the compliance of the Swiss Post’s revamped e-voting system against some of the requirements of the draft OEV. One of the examination scopes covered by SCRT was defined as follows in the audit concept: Scope 3: Infrastructure and operation, b) Assess the infrastructure and organisational

measures of the system provider. The audit report was published in April 2022 on the Federal Chancellery's website [6]

7. In May 2022, the Federal Council enacted the partially revised Ordinance on Political Rights (PoRo) [7], which became applicable from July 1st 2022. The totally revised Federal Chancellery Ordinance on Electronic Voting (OEV) [8] came into force on the same date.
8. In September 2022, an updated version of the audit concept was issued by the Federal Chancellery [9].
9. A second assessment was conducted in mid-September 2022 to follow-up on the findings raised in the initial audit report. The audit report was published in March 2023 on the Federal Chancellery's website [10].
10. A third assessment was conducted in April 2023 to follow-up on the findings raised in the second audit report and to consider changes into the Post's infrastructure, as well as criteria added by the Federal Chancellery to the 3 b) scope [11].
11. Orange Cyberdefense Switzerland ("OCD CH", formerly SCRT) was mandated by the Federal Chancellery to assess the impact of a change initiated by the Post on its infrastructure (i.e., the improvement of access control to the control components through the implementation of jumphosts) on its overall compliance level with the requirements of the OEV.

2 Methodology

2.1 Process

12. The examination was based on OCD CH's information systems audit methodology. The process specifies four-phases, as depicted in the figure below:

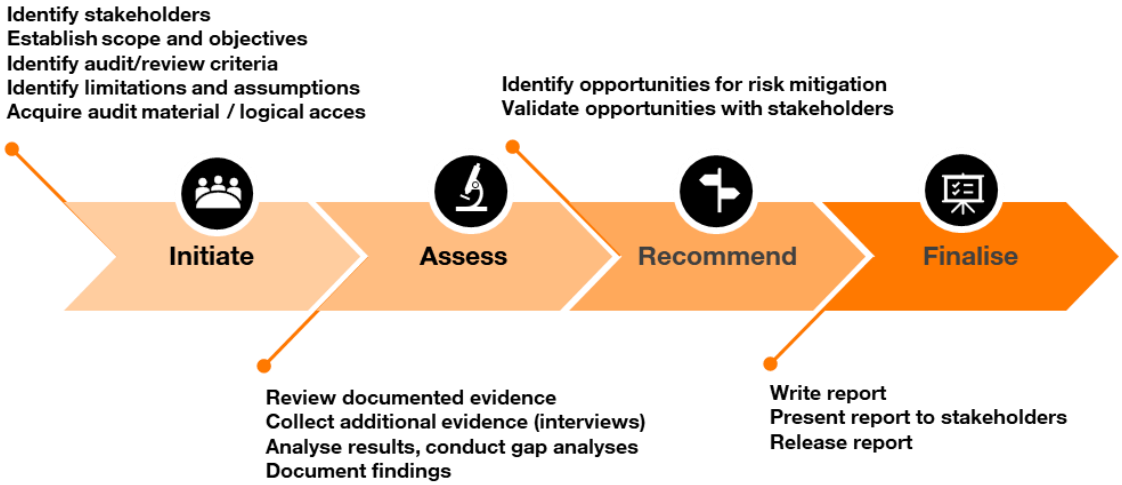


Figure 1: Examination process

2.2 Audit scope definition

13. The examiners did not receive instructions from the Federal Chancellery on which OEV requirements to include in the current examination. Instead, the scope of their audit was determined at their discretion, focusing on the requirements that might be impacted by the changes made to the infrastructure.

2.3 Collection of evidence

14. As a general principle, the examiners aimed at acquiring two types of evidence for each requirement. Types of evidence included: documents (e.g., policies, procedures, reports, etc.) and statements obtained from examinees during interviews.

2.4 Findings

15. The examiners raised a finding when evidence provided by the examinee did not provide satisfying assurance that the requirement is met (implicit miss) or when evidence provided explicitly indicates that the requirement is not or partially satisfied (explicit miss).

2.5 Classification of findings

16. The examiners used the following classification for their findings:

- **Fail** - The finding identifies a failure to produce evidence of satisfying a requirement.

- **Partially fail** - The finding identifies a partial failure to produce evidence of satisfying a requirement.
- **Potential improvement** - The finding identifies a notable opportunity for improvement or optimisation.

17. Readers should note that the classification of findings indicated in this report only reflects the opinion of the examiners and may be subject to re-evaluation from relevant parties.

2.6 Relevance of the assessment criteria

18. The examiners raised an issue when the wording of a given requirement set in the OEV was perceived as unclear, or subject to interpretation, preventing the examiners from performing an objective assessment of the criterion.

2.7 Assumptions

2.7.1 Trustworthiness of statements

19. The examiners assume that the examinees were honest and transparent when providing answers to the examiners' assessment questions. The observation of the actual implementation of the OEV's requirements within the e-voting system was limited to the demo made by the e-voting representatives of the Thurgau canton carried out to verify the accuracy of the examinees' statements.

2.7.2 Enforcement of security measures

20. The examiners assume that the security measures described in the documents provided as evidence in the context of the present examination are implemented and are effective. No observation of the actual implementation of the OEV's requirements within the e-voting system was carried out to verify the accuracy of the statements made in the security documents.

3 Examination criteria

21. This examination focussed on assessing the compliance of the Swiss Post's e-voting system against the following criteria:

Trustworthy components in accordance with Number 2 and for their operation

Key	Requirement
3.6	Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.
3.11	Trustworthy components may not be connected to the internet when installing or updating software.
3.14	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two person principle).
3.15	Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: ■ If a person has physical or logical access to a control component, that person may not have access to any other control component. ■ The hardware, the operating systems and the monitoring systems for the control components should be as distinct as possible from each other. ■ The control components should be connected to different local networks. A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
3.16	Control components must be designed to recognise unpermitted instances of access and to alert the persons responsible. The persons responsible should arrange external monitoring measures, such as the monitoring and the manipulation-resistant logging of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be considered to be particularly trustworthy and reliable.
3.19	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
3.20	Any access to and use of a trusted component or data carrier containing critical data must be logged.

Table 4 - E-voting requirements: Requirements for trustworthy components in accordance with Number 2 and their operation

Tallying votes in the electronic ballot box

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

Table 1 - E-voting requirements: Tallying votes in the electronic ballot box

Threats

Key	Requirement
13.2	The following are considered to be potential threats: ■ Inadvertent or intended electronic or physical threats from internal or external actors; ■ Threats resulting from a malfunction of the system or system-supporting elements.

Table 2 - E-voting requirements: Threats

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

Key	Requirement
14.1	An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required. Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.
14.2	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of preservation of voting secrecy and of the exclusion of premature partial results. The content of the records covers at least the following events: ■ start and end of the audit, identification and authentication processes; ■ start, restart and end of the voting or election phase; ■ start of the tallying with the determination of the results; ■ conduct and results of any self-tests; ■ malfunctions identified in elements of the IT infrastructure that affect the ability to operate. The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented. The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.
14.8	Infrastructure availability must be checked and recorded at selected intervals.
14.10	The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.

Table 3 - E-voting requirements: Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

Use of cryptographic measures and key management

Key	Requirement
15.2	In order to guarantee the integrity of data records that substantiate the accuracy of the result

Key	Requirement
	and ensure that critical data, including the authorities' identification and authentication data, are kept secret, effective cryptographic measures that correspond to the state of the art must be used.
15.3	To ensure that critical data are kept secret, effective cryptographic measures are used in the infrastructure that correspond to the state of the art. Such data is always stored encrypted on data carriers.

Table 4 - E-voting requirements: Use of cryptographic measures and key management

Secure electronic and physical exchange of information

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

Table 5 - E-voting requirements: Secure electronic and physical exchange of information

Organisation of information security

Key	Requirement
18.1	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
18.2	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.

Table 6 - E-voting requirements: Organisation of information security

Management of communication and operations

Key	Requirement
22.1	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
22.2	Appropriate measures must be taken to protect against malware.
22.4	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.

Table 7 - E-voting requirements: Management of communication and operations

Allocation, administration and withdrawal of access and admission authorisations

Key	Requirement
23.1	It must be ensured that, during the ballot, any subsequent change in physical and logical access rights takes place only with the consent of the body responsible at cantonal level.
23.2	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with

Key	Requirement
	the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.

Table 8 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

4 Examination results

22. This section enumerates the results of the examination for each item of the examination criteria.

Key	3.6
Requirement	Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.
Observation	The control components are the only trustworthy components under the sole responsibility of the Post. When performing changes to the control components, the Post implements the notion of “observable process” by: ■ Enforcing the four-eyes principle when accessing the control components (which involves persons from different teams); ■ Thoroughly documenting the accesses to the control components and related operations performed; ■ Forwarding access logs to the Post’s SIEM. Logical access to the control components occurs via jumphosts, which log all actions performed and forward them to the Post’s SIEM. The teams interacting with the control components have no admin access to the jumphosts, nor access to the SIEM and are therefore not able to alter the session recording logs.
Evidence	E-Voting – Zugriffskonzept Kontrollkomponenten v91
Result	Pass
Finding	N/A
Relevance	N/A

Table 9 – Examination results: OEV paragraph 3.6

Key	3.11
Requirement	Trustworthy components may not be connected to the internet when installing or updating software.
Observation	As a default rule, the Post’s servers located in internal zones, such as the control components (i.e. the trustworthy components under the sole responsibility of the Post), are not allowed to communicate with external services (i.e. on Internet). No exception is in place for the control components. No update is performed on control components. They are always reinstalled from scratch, and the process is performed offline. The introduction of dedicated jumphosts for the management of the control components does not compromise the principle that control components do not have Internet access.
Evidence	■ E-Voting Layer 4 Konzept ■ Post HB Network Security Architecture v1.01 ■ Post VOR-Internet Outbound Prozess v02.01
Result	Pass
Finding	N/A

Relevance	N/A

Table 10 – Examination results: OEV paragraph 3.6

Key	3.14
Requirement	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two-person principle).
Observation	Logical access to the control components (i.e. the trustworthy components under the sole responsibility of the Post) is designed in a way that enforces the four-eyes principle (operations are performed in presence of two persons from two different teams) and segregation of duties. Access to the control components by system or database administrators is performed by submitting an access request to a dedicated team (Token Team), which itself has no access to the network zones where the control components reside. Access to the Linux-based control components is allowed through the allocation of a token (under the form of a one-time authentication token) to the requestor, and to the temporary integration to an Active Directory group for the Windows-based control component, once the token team has verified the identity of the requestor and validated the need for access (it verifies the existence of a service or incident ticket, or change request). All logical actions on control components are subject to a formal report signed by the parties involved. Logical access to the control components occurs via jumphosts, which log all actions performed (logs are forwarded to the Post's Splunk SIEM). The control components' administrators have no admin access to the jumphosts. Out-of-Band Management tools (HP's iLO and Cisco's CIMC) are available. Access permissions to these management interfaces are granted following the same authorisation process as depicted above. Teams with logical access to the control components do not have physical access. Only the infrastructure team is allowed to access the components physically, based on a formal change request and while being accompanied. All physical actions on control components are subject to a formal report signed by the parties involved. The Post's employees are not involved in the management of data carriers processing e-voting data, which is the responsibility of the cantons.
Evidence	■ E-Voting collaboration platform - Benutzeranleitungen Release 1.4 ■ E-Voting – Zugriffkonzept Kontrolkomponenten v86 ■ E-Voting - Physical Access Data Center E-Voting Infrastructure concept v26 ■ Operation whitepaper of the Swiss Post voting system
Result	Pass
Finding	N/A
Relevance	N/A

Table 11 – Examination results: OEV paragraph 3.14

Key	3.15
Requirement	Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: ■ If a person has physical or logical access to a control component, that person may

	not have access to any other control component. ■ The hardware, the operating systems and the monitoring systems for the control components should be as distinct as possible from each other. ■ The control components should be connected to different local networks. ■ A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
Observation	Segregation of duties between the Post's operational teams (CC1, CC2, CC3, CC4) enforces the requirement: "If a person has physical or logical access to a control component, that person may not have access to any other control component." Each control component runs on dedicated physical hardware with distinct operating system and is operated in a dedicated network. Access to the control components' networks is disabled by default and must be explicitly granted, based on a formal access request. Logical access to a given control component occurs through a dedicated jumphost. Therefore, compromising one jumphost would not procure any advantage in an attempt to access another control component. From a physical point of view, each control component runs in a dedicated rack located in the most secure zone of the datacentres' provider (Postfinance). The keys to the racks are kept by a dedicated team (Vault-Team), which verifies the identity of the requestor and validates the need for access before handing over the keys. The monitoring systems for the control components include Grafana (general health of the systems) and the Splunk security information and event management (SIEM) platform (focus on security events), which collects access logs and host intrusion detection system (HIDS) logs. Those monitoring tools are common to the whole Post's infrastructure.
Evidence	■ E-Voting – Root Activity Monitoring v12 ■ Operation whitepaper of the Swiss Post voting system ■ Physical Access Data Center E-Voting Infrastructure concept v26 ■ E-Voting – Zugriffkonzept Kontrolkomponenten v86
Result	Pass
Finding	N/A
	N/A

Table 12 – Examination results: OEV paragraph 3.15

Key	3.16
Requirement	Control components must be designed to recognise unpermitted instances of access and to alert the persons responsible. The persons responsible should arrange external monitoring measures, such as the monitoring and the manipulation-resistant logging of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be considered to be particularly trustworthy and reliable.
Observation	Any logical action performed on a control component is monitored, recorded and corresponding alerts are sent to the E-Voting team. After each ballot, local access logs are reconciled with the records of the team granting accesses (Token Team) to ensure consistency. A file integrity verification tool (Samhain) detects modifications of system files on Linux-based control components. Resistance to manipulation of logs during their transfer is provided thanks to the use of TLS with mutual authentication between the e-voting system and the monitoring tools. The rooms where the control components are physically hosted are subject to physical access control and video surveillance.

	The Post applies the following measures to ensure the trustworthiness of its employees: ■ Performance of background checks (as part of the general Post HR process, a criminal record extract is required for joiners and movers and additional elements may be required by the team leaders such as a certificate from the debt enforcement office); ■ Signature by the personnel of non-disclosure agreement (as part of the general Post HR process and e-voting-specific).
Evidence	■ E-Voting – Control Components Monitoring v28 ■ Operation whitepaper of the Swiss Post voting system ■ Physical Access Data Center E-Voting Infrastructure concept v26 ■ E-Voting – Zugriffkonzept Kontrolkomponenten v86 ■ Funktionsweisung Sicherheitsüberprüfung von Mitarbeitenden - Die Schweizerische Post AG ■ Geheimhaltungsvereinbarung im Zusammenhang mit dem Projekt/Vertragsverhältnis: E-Voting der Post
Result	Pass
Finding	N/A
Relevance	N/A

Table 13 – Examination results: OEV paragraph 3.16

Key	3.19
Requirement	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
Observation	All documentation related to the e-voting system is available on the Post's e-voting internal wiki. To ensure completeness, accuracy and readability of the documentation, each wiki page is assigned an owner, in charge of its maintenance. Quality controls are performed once a year. At the time of the examination, no procedure detailing how to access the control components via new newly deployed jumphosts exists.
Evidence	■ 4-eye Principle Access ■ E-Voting Kontrollkomponente Betrieb Handbuch
Result	Partially fail
Finding	At the time of the examination, no procedure detailing how to access the control components via new newly deployed jumphosts exists.
Relevance	N/A

Table 14 – Examination results: OEV paragraph 3.19

Key	3.20
Requirement	Any access to and use of a trusted component or data carrier containing critical data must be logged.
Observation	The Post does not interact with the data carriers involved in the e-voting operations. Every access and action performed on a control component is subject to a formal access request and report. Hardening measures applied on the control components include the activation of local logging functionalities. Accesses performed on control components trigger an alarm which is sent to the

Evidence	corresponding CC team. All interactive sessions initiated from the jumphosts are recorded. After each ballot, local access logs are reconciled with the records of the team granting accesses (Token Team) to ensure consistency.
	■ E-Voting – Control Components Monitoring v28 ■ E-Voting – Root activity monitoring v12 ■ E-Voting Zugriffskonzept Kontrolkomponenten v91
Result	Pass
Finding	N/A
Relevance	The concept of "trusted component" is not defined in the OEV, which prevents an objective interpretation of the examination criterion. The examiners assimilated it to the term of "trustworthy component".

Table 15 – Examination results: OEV paragraph 3.20

Key	11.4
Requirement	From the decryption of votes to the transmission of the result of the ballot, any access to the system or to any of its components must be made jointly by at least two persons; it must be recorded in writing and it must be possible for the examiners to check it.
Observation	The Post is not involved either in the decryption process or in the transmission of the result of the ballot, which are performed by the cantons. It provides the secure logs before the decryption. At the infrastructure level, the Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters in a red phase, where changes are frozen by default. The process allows for emergency changes during the red period, e.g., in case of incident. A four-eyes principle applies for the management of the components (reverse proxy, front-end & back-end servers, databases, control components). All accesses performed are logged.
Evidence	■ E-Voting collaboration platform - Benutzeranleitungen Release 1.4 ■ E-Voting - Change concept v22 ■ Infrastructure Whitepaper of the Swiss Post Voting System v1.6.1.0
Result	Pass
Finding	N/A
Relevance	N/A

Table 16 – Examination results: OEV paragraph 11.4

Threats

Key	13.2
Requirement	The following are considered to be potential threats: ■ Inadvertent or intended electronic or physical threats from internal or external actors; ■ Threats resulting from a malfunction of the system or system-supporting elements.
Observation	Upon request of the auditors, the Post has added a chapter to its *E-Voting – Zugriffskonzept Kontrollkomponenten* document, which maps a number of threats listed in Numbers 13.3-13.40 to corresponding mitigation measures applied to the control components infrastructure.

	However, the examiners note a lack of comprehensiveness in the analysis at several levels: ■ Data flow diagram: For instance, the data flow diagram does not represent the Grafana monitoring platform, which, according to the *Root activity monitoring* document, logs login attempts to the servers supporting the control components; ■ Threats: For instance, threats likely to lead to the unavailability of the newly deployed jumphosts are not considered; ■ Security measures: For instance, existing security measures such as strong authentication, encrypted communication channels, or secure configurations are not mentioned.
Evidence	E-Voting – Zugriffskonzept Kontrollkomponenten v91 §3
Result	Partially fail
Finding	The threat model provided by the Post regarding the control components infrastructure lacks comprehensiveness in terms of graphical representation of the infrastructure and elicitation of applicable threats as well as corresponding security measures.
Relevance	N/A

Table 17 – Examination results: OEV paragraph 13.2

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

Key	14.1
Requirement	An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required. Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.
Observation	The present observation relates to the monitoring means applying to the newly deployed jumphosts. The *Zugriffskonzept Kontrollkomponenten* document specifies that logical access to the control components is performed exclusively through jumphosts, whose session logs are forwarded to the Post's corporate Splunk SIEM. Several documents (i.e., *E-Voting – Monitoring concepts*, *Control components monitoring*, *Root Activity Monitoring*) detail the current ways the e-voting components are monitored. They include security-related monitoring activities, but do not make any mention of the jumphosts. In case of unavailability, the jumphosts are reinstalled from scratch. The list of incidents endured during a ballot are made available to the cantons in a debriefing session that takes place after each voting event.
Evidence	■ E-Voting – Zugriffskonzept Kontrollkomponenten v91 ■ E-Voting – Disaster Recovery concept v31 ■ E-Voting – Monitoring concepts v43 ■ E-Voting – Control components monitoring v28 ■ E-Voting - Root Activity Monitoring v12 ■ Sample debriefing report (shown online)

Result	Partially fail
Finding	The exiting documents relating to the monitoring of the e-voting infrastructure have not been updated to include the jumphosts in their scope.
Relevance	N/A

Table 18 – Examination results: OEV paragraph 14.1

Key	14.2
Requirement	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of preservation of voting secrecy and of the exclusion of premature partial results. The content of the records covers at least the following events: ■ start and end of the audit, identification and authentication processes; ■ start, restart and end of the voting or election phase; ■ start of the tallying with the determination of the results; ■ conduct and results of any self-tests; ■ malfunctions identified in elements of the IT infrastructure that affect the ability to operate. The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented. The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.
Observation	The present observation focusses on the newly deployed jumphosts, which are elements of the IT infrastructure. The *Zugriffskonzept Kontrollkomponenten* document specifies that logical access to the control components is performed exclusively through jumphosts, whose session logs are forwarded to the Post's corporate Splunk SIEM. Several documents (i.e., *E-Voting – Monitoring concepts*, *Control components monitoring*, *Root Activity Monitoring*) detail the current ways the e-voting components are monitored. They include security-related monitoring activities, but do not make any mention of the jumphosts. The logs sent to the Splunk SIEM are transmitted over http and cannot be edited, which ensures their integrity. They are time-stamped using a common NTP source and time zone for consistency purpose. The list Incidents endured during a ballot are made available to the cantons in a debriefing session that takes place after each voting event.
Evidence	■ E-Voting – Zugriffskonzept Kontrollkomponenten v91 ■ E-Voting – Disaster Recovery concept v31 ■ E-Voting – Monitoring concepts v43 ■ E-Voting – Control components monitoring v28 ■ E-Voting - Root Activity Monitoring v12 ■ Sample debriefing report (shown online)
Result	Partially fail
Finding	The exiting documents relating to the monitoring of the e-voting infrastructure have not been updated to include the jumphosts in their scope.
Relevance	N/A

Table 19 – Examination results: OEV paragraph 14.2

Key	14.8
Requirement	Infrastructure availability must be checked and recorded at selected intervals.
Observation	The present observation focusses on the newly deployed jumphosts, which are elements of the IT infrastructure. The documents related to the monitoring activities on the e-voting components make no mention of the jumphosts.
Evidence	■ E-Voting – Monitoring concepts v43 ■ E-Voting – Control components monitoring v28
Result	Partially fail
Finding	The documents related to the monitoring activities on the e-voting components make no mention of the jumphosts.
Relevance	N/A

Table 20 – Examination results: OEV paragraph 14.8

Key	14.10
Requirement	The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.
Observation	The activities of the control components' administrators are recorded on the jumphosts and the records are forwarded to the Splunk SIEM. The documents related to activity monitoring on the e-voting system make no mention of the jumphosts.
Evidence	■ E-Voting – Zugriffskonzept Kontrollkomponenten v91 ■ E-Voting – Monitoring concepts v43 ■ E-Voting – Control components monitoring v28
Result	Partially fail
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 14.10

Use of cryptographic measures and key management

Key	15.2
Requirement	In order to guarantee the integrity of data records that substantiate the accuracy of the result and ensure that critical data, including the authorities' identification and authentication data, are kept secret, effective cryptographic measures that correspond to the state of the art must be used.
Observation	The administrators connect to the control components via SSH (Linux-based control components) or RDP (Windows-based control components) from the jumhosts. Algorithms and key lengths used correspond to current recommended good practices.
Evidence	■ Handbuch Kryptographie ■ E-Voting – Zugriffskonzept Kontrollkomponenten v91

Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – Examination results: OEV paragraph 15.2

Key	15.3
Requirement	To ensure that critical data are kept secret, effective cryptographic measures are used in the infrastructure that correspond to the state of the art. Such data is always stored encrypted on data carriers.
Observation	The administrators connect to the control components via SSH (Linux-based control components) or RDP (Windows-based control components) via the jumhosts. Algorithms and key lengths used correspond to current recommended good practices.
Evidence	■ Handbuch Kryptographie ■ E-Voting – Zugriffskonzept Kontrollkomponenten v91
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 15.3

Secure electronic and physical exchange of information

Key	16.1
Requirement	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.
Observation	The implementation of the e-voting components, including the jumphosts, appears to satisfy the requirements of the Post's Network Security Architecture policy. The policy defines trust zones and the communication rules between the said zones. It requires to filter communications through firewalls at OSI layer 4 level between some zones and forbids communications from specific zones to others (e.g., from the Admin zone to Internet). The jumphosts are the only devices allowed to communicate with the control components. Only the SSH and RDP protocols are allowed.
Evidence	■ Post HB Network Security Architecture ■ Infrastructure whitepaper of the Swiss Post voting system ■ Area-Beschreibung und Platzierungskriterien ESP (E Service Platform) v06.01
Result	Pass
Finding	N/A
Relevance	N/A

Table 24 – Examination results: OEV paragraph 16.1

Organisation of information security

Key	18.1

Requirement	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
Observation	The *Organisation Cluster E-Government* document includes a table which shows which teams within the Post is in charge of which component of the e-voting system, including the newly deployed jumphosts
Evidence	E-Voting – Organisation Cluster E-Government v10
Result	Pass
Finding	N/A
Relevance	N/A

Table 25 – Examination results: OEV paragraph 18.1

Key	18.2
Requirement	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
Observation	The examiners understand that this requirement relates to the authorisation process in case of changes. Change management at the e-voting level follows the Post's general change management process, which bases upon ITIL best practices, and therefore includes an authorisation step. The *E-Voting Change concept* document details the authorisation workflow, which involves both the IT-Post and the e-voting Change Advisory Boards.
Evidence	■ Post change management ■ E-Voting - Change concept v22
Result	Pass
Finding	N/A
Relevance	N/A

Table 26 – Examination results: OEV paragraph 18.2

Management of communication and operations

Key	22.1
Requirement	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
Observation	Risks originating from human resources relating to operations and communications may materialise through physical or logical access to the e-voting system components and include accidental behaviours (e.g., bad manipulation resulting in confidentiality, integrity or availability issues) as well as intentional malicious actions (e.g., fraud attempts, vandalism/sabotage, etc.). The *Organisation Cluster E-Government* document shows how obligations and areas of responsibility related to e-voting operations and communications are split between different teams, and how the four-eyes principle applied for the management of the components (control components, jumphosts, reverse proxy, front-end & back-end servers, databases) limits the risks of frauds. A strict segregation of duties also applies for the management of the control components. People involved in the e-voting operations and communications also follow trainings,

Evidence	which reduces the risk of accidental behaviours. The *E-voting ISDS Konzept* document details the organisation put in place to reduce the risks originating from human resources relating to operations and communications to a residual level.
	■ E-Voting – Organisation Cluster E-Government v10 ■ Whitepaper Infrastructure of the Swiss Post Voting System ■ Schulungskonzept E-Voting ■ E-voting ISDS Konzept V2.01
Result	Pass
Finding	N/A
Relevance	N/A

Table 27 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Protection against malware include a wide range of measures, including user-awareness, end-point protection, management of removable media, rules for software installation, network segregation, patch management, hardening of components, ingress and egress IP communications filtering, content filtering, incident detection and response. All these measures are part of the Post Information Security Management System's standard controls. The Linux-based control components and the jumphosts used to connect to them run a Security-Enhanced Linux version, a rootkit detection tool, and an intrusion detection system. The Windows-based control component and the jump host used to connect to it runs the standard Post antivirus software. The Post's Computer Emergency Response Team (CERT) is in charge of handling malware incidents. A malware outbreak at the infrastructure level is one of the crisis scenarios considered in the Post's emergency manual.
Evidence	■ Post's ISO 27001 certificate ■ Post's ISO 27001 Statement of Applicability ■ Handbuch Network Security Architecture ■ Handbuch HB hardening ■ Function directive IT baseline protection ■ Indikatoren für IT-sicherheitsrelevante Ereignisse
Result	Pass
Finding	N/A
Relevance	N/A

Table 28 – Examination results: OEV paragraph 22.2

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

Observation	The introduction of dedicated jumphosts to manage network access to the control components represents a security enhancement in the e-voting infrastructure. However, it has not been subject to a comprehensive documented risk assessment.
Evidence	E-Voting – Zugriffskonzept Kontrollkomponenten v91
Result	Partially fail
Finding	The introduction of dedicated jumphosts to manage network access to the control components has not been subject to a comprehensive documented risk assessment.
Relevance	N/A

Table 29 – Examination results: OEV paragraph 22.4

Allocation, administration and withdrawal of access and admission authorisations

Key	23.1
Requirement	It must be ensured that, during the ballot, any subsequent change in physical and logical access rights takes place only with the consent of the body responsible at cantonal level.
Observation	Change management at the e-voting level follows the Post's general change management process, which bases upon ITIL best practices. The Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters in a red phase, where changes are frozen by default. The process allows for emergency changes during the red period, e.g., in case of incident. In such a case, the cantons are accountable for the release of the change and therefore consent to it. Physical access requests to the e-voting system's components that may be necessary to handle a change are also dealt with through the change management process.
Evidence	■ Post change management ■ E-Voting Change concept v22 ■ Physical Access Data Center E-Voting Infrastructure concept v26 §2.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 30 – Examination results: OEV paragraph 22.5

Key	23.2
Requirement	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.
Observation	The introduction of dedicated jump hosts represents a change that impacts the way access to the infrastructure is performed, which has not been subject to a comprehensive documented risk assessment.

Evidence	E-Voting – Zugriffskonzept Kontrollkomponenten v91
Result	Partially fail
Finding	The introduction of dedicated jumphosts to manage network access to the control components has not been subject to a comprehensive documented risk assessment.
Relevance	N/A

Table 31 – Examination results: OEV paragraph 23.2

5 Summary of findings and recommendations

23. This section recaps the findings made during the examination, their severity, and provides succinct recommendations to address them.

Key	3.19
Requirement	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
Finding	At the time of the examination, no procedure detailing how to access the control components via new newly deployed jumphosts exists.
Recommendation	Issue an operational procedure for jumphosts to ensure their standardised, efficient, and secure use.

Table 32 – Finding related to requirement 3.19

Key	13.2
Requirement	The following are considered to be potential threats: ■ Inadvertent or intended electronic or physical threats from internal or external actors; ■ Threats resulting from a malfunction of the system or system-supporting elements.
Finding	The threat model provided by the Post regarding the control components infrastructure lacks comprehensiveness in terms of graphical representation of the infrastructure and elicitation of applicable threats as well as corresponding security measures.
Recommendation	Issue a comprehensive threat model for the control components using a formal methodology to ensure comprehensiveness in the analysis. Such a document could be used as a basis to demonstrate compliance with the OEV requirements and assess risks

Table 33 – Finding related to requirement 13.2

Key	14.1
Requirement	An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required. Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.
Finding	The exiting documents relating to the monitoring of the e-voting infrastructure have not been updated to include the jumphosts in their scope.
Recommendation	The documents detailing how incident detection and response is performed should be updated to include the jumphosts.

Table 34 – Finding related to requirement 14.1

Key	14.2
Requirement	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of preservation of voting secrecy and of the exclusion of premature partial results. The content of the records covers at least the following events: ■ start and end of the audit, identification and authentication processes; ■ start, restart and end of the voting or election phase; ■ start of the tallying with the determination of the results; ■ conduct and results of any self-tests; ■ malfunctions identified in elements of the IT infrastructure that affect the ability to operate. The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented. The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.
Finding	The exiting documents relating to the monitoring of the e-voting infrastructure have not been updated to include the jumphosts in their scope.
Recommendation	The documents detailing how malfunctions identified in elements of the IT infrastructure that affect the ability to operate are detected should be updated to include the jumphosts.

Table 35 – Finding related to requirement 14.2

Key	14.8
Requirement	Infrastructure availability must be checked and recorded at selected intervals.
Finding	The documents related to the monitoring activities on the e-voting components make no mention of the jumphosts.
Recommendation	The documents related to the monitoring activities on the e-voting components should be updated to include the jumphosts.

Table 36 – Finding related to requirement 14.8

Key	14.10
Requirement	The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.
Finding	The documents related to activity monitoring on the e-voting components make no mention of the jumphosts.
Recommendation	The documents related to activity monitoring on the e-voting components should be updated to include the jumphosts.

Table 37 – Finding related to requirement 14.10

Key	22.4

Requirement	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
Finding	The introduction of dedicated jumphosts to manage network access to the control components has not been subject to a comprehensive documented risk assessment.
Recommendation	Assess and document risks induced by the deployment of jump hosts in the e-voting infrastructure. A threat model elaborated using a formal methodology could serve as a consistent basis for such a risk assessment.

Table 38 – Finding related to requirement 22.4

Key	23.2
Requirement	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g., opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.
Finding	The introduction of dedicated jumphosts to manage network access to the control components has not been subject to a comprehensive documented risk assessment.
Recommendation	Assess and document risks induced by the deployment of jump hosts in the e-voting infrastructure. A threat model elaborated using a formal methodology could serve as a consistent basis for such a risk assessment.

Table 39 – Finding related to requirement 23.2

6 References

[1] “Swiss Citizens should be able to vote electronically,” Administration numérique suisse, [Online]. Available: https://www.digital-public-services-switzerland.ch/en/implementation/egovernment-implementation-plan/redesigning-evoting. [Accessed 22 May 2024].

[2] “Redesign and relaunch of trials - Final report of the Steering Comittee Vote électronique (SC VE),” Swiss Federal Chancellery, Political Rights Section, 30 November 2020. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Final%20report%20SC%20VE_November%202020.pdf.download.pdf/Final%20report%20SC%20VE_November%202020.pdf. [Accessed 22 May 2024].

[3] “Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials),” Swiss Federal Chancellery, Political Rights Section, 28 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Explanatory%20report%20for%20consultation%202021.pdf.download.pdf/Explanatory%20report%20for%20consultation%202021.pdf. [Accessed 22 May 2024].

[4] “Federal Chancellery ordinance on electronic voting (OEV),” Swiss Federal Chancellery, 21 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/OEV_draft%20for%20consultation%202021.pdf.download.pdf/OEV_draft%20for%20consultation%202021.pdf. [Accessed 22 May 2024].

[5] “Audit concept v1.3 for examining Swiss Internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 18 May 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Audit%20concept,%2018.05.2021.pdf.download.pdf/Audit%20concept,%2018.05.2021.pdf. [Accessed 22 May 2024].

[6] “Examination of the Swiss Internet voting system, Version:1.0 / Audit scope: Infrastructure and operations (3) – Measures of the System Provider,” Swiss federal chancellery, March 2022. [Online]. Available: https://www.newsd.admin.ch/newsd/message/attachments/71144.pdf. [Accessed 16 Juky 2024].

[7] “Ordinance on Political Rights (PoRo). section 6a: Electronic Voting Trials,” Swiss Federal Chancellery, [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf.download.pdf/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf. [Accessed 22 May 2024].

[8] “Federal Chancellery Ordinance on Electronic Voting (OEV),” Swiss Federal Chancellery, 25 May 2022. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2022/336/en. [Accessed 22 May 2024].

[9] “Audit concept v1.5 for examining Swiss internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 15 September 2022. [Online]. Available: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Audit%20concept%20v1.5.pdf.download.pdf/Audit%20concept%20v1.5.pdf. [Accessed 22 May 2024].

[10] “Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider - Round 2,” SCRT, November 2022. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20(Post)%20Final%20Report%20SCRT%2028.11.2022.pdf.download.pdf/Scope%203%20(Post)%20Final%20Report%20SCRT%2028.11.2022.pdf. [Accessed 16 July 2024].

[11] “Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider - Round 3 & changes,” SCRT, June 2023. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2023/Scope%203%20(Post)%20Final%20Report%20SCRT%2016.06.2023.pdf.download.pdf/Scope%203%20(Post)%20Final%20Report%20SCRT%2016.06.2023.pdf. [Accessed 16 July 2024].