Examination of the Swiss Internet voting system

Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider – Round 2

28/11/2022

Work performed for:

Swiss Federal Chancellery
Political Rights Section
Federal Palace West Wing
3003 Bern

Contact information

SCRT SA
Rue du sablon 4
1110 Morges
Switzerland

Stéphane Adamiste
Chief Product Officer
+41 21 802 64 01
stephane.adamiste@scrt.ch

Contributors

Author	Stéphane Adamiste	Chief Product Officer

Version history

Version Number	Author	Date	Version
0.9	Stéphane Adamiste	31.10.2022	Draft for review
1.0	Stéphane Adamiste	28.11.2022	Integration of comments by the Federal Chancellery

Management summary

Scope and objective of the examination

During the period September 2021 – February 2022, SCRT carried out a security compliance audit of the Swiss Post's e-voting system against a subset of requirements set forth by the Federal Chancellery's ordinance on e-voting (audit scope 3 - *Infrastructure and operation, b) Assess the infrastructure and organisational measures of the system provider*).

Twenty-four non-compliances (findings) were identified and reported.

The objective of this examination was to follow up on the findings raised in the initial audit report.

Methodology

The examiners looked for evidence of effort to comply with the criteria that were not fulfilled during the initial examination by performing interviews of the Swiss Post's personnel in charge of the setup and operation of the e-voting system's infrastructure, and by analysing the relating documentation (i.e., policies, procedures, specifications, reports, processes, etc.).

This second examination was performed mostly during the second half of September 2022.

For the sake of consistency, the examiners performed their follow-up audit work on the basis of the requirements set in the draft version of the ordinance on e-voting, although the official version, release in July 2022, includes some modifications. An impact assessment of the changes affecting the audit scope was carried out and integrated into the audit results.

Results

After the second round of audit, five requirements were assessed as not met (*fail* status) or partially not met (*partially fail* status).

Observed non-compliances were found to have the following origins:

- The action plan to meet the OEV's requirement is not implemented yet. Three criteria are concerned;
- One requirement is practically not met, but the examiners consider the newly documented process of the Swiss Post to be aligned with security good practices;
- One requirement, in its current form, lacks precision in its wording and should be reconsidered, as already suggested in the initial audit.

Recommendations

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

This report provides also comments at the attentions of the Federal Chancellery when the examination criteria were perceived as unclear, or subject to interpretation.

Final note

The examiners conclude this summary by thanking the Swiss Post, and more particularly all the personnel that has been involved, for its cooperation and for the transparency demonstrated throughout the entire duration of the examination.

Table of content

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 Swiss Post of the withdrawal of its e-voting system from operation to focus on improving the solution. Since then, e-voting is 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, using “e-voting systems, which are fully verifiable” [1]. This redesign of the trial phase focuses on four objectives:
    1. Further development of the e-voting systems
    2. Effective controls and monitoring
    3. Increased transparency and trust
    4. 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. In April 2021, the Federal Council opened a consultation procedure on the amendment to the legal bases, which was drafted by the Federal Chancellery. A consultation procedure for the redesign of the e-voting trials was initiated in April 2021 by the Federal Council. 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 [5] 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.
6. SCRT 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 Jul. 1st 2022. The totally revised Federal Chancellery Ordinance on Electronic Voting (OEV) [8] came into force on the same date.
8. A second assessment was conducted in mid-September 2022 to follow-up on the findings raised in the initial audit report.

2 Methodology

2.1 Process

10. The examination was based on SCRT's information systems audit methodology. The process specifies four-phases, which are depicted in the figure below:

Figure 1 - Process

2.2 Collection of evidence

11. 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.

12. Part of the examination included reviewing documents classified as confidential by Swiss Post and thus not released to the public. Motives for not disclosing these documents to the public included either or both the a) preservation of the confidentiality of business processes deployed at the organisation level and which may confer Swiss Post a competitive advantage on other actors, and b) the preservation of confidentiality of

operational data (e.g., risk control, infrastructure operations, etc.). Swiss Post confirmed to us that these documents remain accessible to the cantons.

2.3 Findings

13. 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).

2.4 Classification of findings

14. 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.

15. 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.

2.5 Evolution of the audit reference framework

16. The first round of examination was based on the draft version of the revised OEV [4]. The official text released in July 2022 [8] includes changes from the draft version, which modifies the audit reference framework. For the sake of consistency, the examiners kept the requirements' original form. However, they took into account those changes by assessing their impact in a dedicated chapter of this document (See § 3.1 Impact assessment of the OEV changes) and integrating the said impacts in the audit results.

2.6 Relevance of the assessment criteria

17. 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

18. The examiners assume that the examinees were honest and transparent when providing answers to the examiners' assessment questions. 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 examinees' statements.

2.7.2 Enforcement of security measures

19. 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

3.1 Impact assessment of the OEV changes

20. The table below shows the examination criteria that have been subject to changes between the two rounds of examination as well as their impact on the audit process. Potential impacts are mentioned in the examination results section.

Key	Nature of change	Impact of change on the audit process
2.5	Rewording (a *proof -> proof**s***, *the attacker has not -> no attacker has*).	None
3.14	Reduction of the level of requirement (*The hardware, the operating systems and the monitoring systems for the control components should be distinct from each other -> The hardware, the operating systems and the monitoring systems for the control components should be **as** distinct **as possible** from each other*).	This loosening of the requirement allows to consider the principle of a central monitoring system, as implemented by the Post, acceptable.
3.16	Rewording (*Trustworthy components must perform only the intended operations -> Trustworthy components **may** perform only the intended operations*).	None.
13.1	Addition of a threat (***13.28 An internal attacker manipulates the software to reveal the votes***).	The examiners checked whether the additional threat is considered by the Post.
13.1	Rewording (*The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis -> The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis **that must be completed***), (*vulnerabilities of the system -> **system vulnerabilities***), (*the risks are to be specified -> **the list should be updated with full details***).	None.
14.1	Correction of an inaccuracy (*incidents that could endanger the security or the availability -> incidents that could endanger the security, **including availability***).	None.
15.2, 15.3	Rewording (*secret and confidential data -> **critical** data*).	None.

Key	Nature of change	Impact of change on the audit process
18.3	Rewording (*suppliers, service providers -> suppliers **and** service providers*).	None.
20.2	Rewording (*Human resources managers -> **Heads of** human resources*).	None.
21.4	Rewording (*All data must be processed exclusively in Switzerland, including storage -> All data must be processed **and in particular stored exclusively in Switzerland***).	None.
22.1	Adding of a missing word (*Obligations and areas of responsibility must apportioned -> Obligations and areas of responsibility must **be** apportioned*).	None.
24.3.5	Rewording (*in the light of current scientific knowledge and experience -> in the light of current **academic** knowledge and experience*).	None.

3.2 Criteria list

21. This examination focussed on assessing the compliance of the Swiss Post's e-voting system against the following criteria, which were reported to be not fulfilled during the first examination:

Cryptographic protocol: individual verifiability

Key	Requirement
2.5	The voter is given a proof in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that the attacker » has not altered any partial vote before the vote has been registered as cast in conformity with the system; » has not maliciously cast a vote on the voter's behalf which has subsequently been registered as a vote cast in conformity with the system and counted.

Table 1 - E-voting requirements: Requirements for the cryptographic protocol: individual verifiability

Trustworthy components in accordance with Number 2 and 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.
3.14	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 distinct from each other. » The control components should be connected to different networks. » A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
3.16	Trustworthy components must perform only the intended operations.

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

Threats

Key	Requirement
13.1	The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis. They relate to the security objectives and must be taken into account when identifying risks. Depending on the vulnerabilities of the system identified, when the various bodies carry out their risk assessments, the risks are to be specified and considered based on the actual circumstances and depending on the specific threat.

Table 3 - 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 or the 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.

Table 4 - 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
15.1	Electronic certificates must be managed according to the best practices.
15.2	In order to guarantee the integrity of data records that substantiate the accuracy of the result and ensure that secret and confidential 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 secret and confidential 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 5 - E-voting requirements: Use of cryptographic measures and key management

Organisation of information security

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

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

Management of non-material and material resources

Key	Requirement
19.3	Classification guidelines for information must be issued and communicated.

Table 7 - E-voting requirements: Management of non-material and material resources

Trustworthiness of human resources

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

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

Table 8 - E-voting requirements: Trustworthiness of human resources

Physical and environment security

Key	Requirement
21.4	All data must be processed exclusively in Switzerland, including storage.

Table 9 - E-voting requirements: Physical and environment security

Management of communication and operations

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

Table 10 - E-voting requirements: Management of communication and operations

Allocation, administration and withdrawal of access and admission authorisations

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

Table 11 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

Development and maintenance of information systems

Key	Requirement
24.2.1	An operating manual is created that includes the following for each user role: » a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; » a description of how the available interfaces can be used in a secure manner;

	» a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security; » a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions; » a description of the security measures to be implemented in order to achieve the operational security objectives.
24.2.2	The operating manual must identify all possible modes of operation of the software, including the resumption of operation after the detection of errors and the description of the consequences and effects of errors on the maintenance of secure operation
24.2.3	The operating manual must be precise and fit for purpose.
24.3.3	A reliable and verifiable compilation with appropriate security measures must be carried out. This ensures that the executable code is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations. The compilation allows a chain of proofs to be created for the verification of the software and includes in particular: » evidence that the compilation environment is designed as described on the public platform (all tools with the respective version, operating system and any configurations); any derogations must be documented and justified; » evidence that the software has been compiled in accordance with the instructions available on the public platform; if an error in the instructions is found during compilation, this must be recorded and the documentation must subsequently be corrected; » evidence that the source code submitted for public scrutiny and examined is in fact the source code used for compilation; » evidence that no elements other than those provided for in the instructions have been introduced; » evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference (e.g. Maven Central Repository); » evidence that a dependency vulnerability analysis has been performed and that, if vulnerabilities relevant to the software exist, they do not render the software vulnerable to attack; » evidence that the parameters introduced, if any, do not render the system vulnerable.
24.3.4	A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that: 1. the code used in production is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations; and 2. the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The deployment allows a chain of proofs to be created for the verification of the software and includes in particular:

	» evidence that the production environment is the same as that which has been subjected to public scrutiny and independent examinations; any discrepancies (firmware version, configuration files, etc.) must be documented and justified; » evidence that the software deployed in the production environment is in fact that which was created using a reliable and verifiable compilation process; » evidence that the parameters introduced, if any, do not render the system vulnerable.
24.3.5	The quality of the evidence of reliable and verifiable compilation and reliable and verifiable deployment must be confirmed by the presence of at least two witnesses from different institutions or by technical procedures to establish the truth of the evidence in the light of current scientific knowledge and experience
24.3.6	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available

Table 12 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

Operation

Key	Requirement
25.6.2	Persons who operate and use the system must be trained and provided with the necessary documentation
25.6.4	Help on using the system must be readily available.

Table 13 - E-voting requirements: Operation

4 Examination results

7. This section enumerates the results of the examination for each item of the examination criteria. Where applicable, it also details the findings, their severity, and provides succinct recommendations to address them.

Requirement for the cryptographic protocol: individual verifiability

Key	2.5
Requirement	The voter is given a proof in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that the attacker » has not altered any partial vote before the vote has been registered as cast in conformity with the system; » has not maliciously cast a vote on the voter's behalf which has subsequently been registered as a vote cast in conformity with the system and counted.
Initial audit finding	The soundness of the proof in accordance with Article 5 paragraph 2 is based on the trustworthiness of the procedure for distributing the voting papers and the trustworthiness of the procedure for requesting information from the cantons. Therefore, the examiners cannot confirm the exclusive nature of the requirements set in Article 6 letters a and b.
Follow-up audit observation	Following a clarification of this requirement by the Federal Chancellery, it appears that both the procedure for distributing the voting papers and the procedure for requesting information from the cantons are considered as "*trustworthy part of the system*". The examiners thus conclude that the soundness of the proofs under Article 5 paragraphs 2 and 3 is based exclusively on the trustworthiness of criteria listed in Article 6 letters a and b (Article 6 letter a being the "*trustworthy part of the system*").
Evidence	N/A
Result	Pass
Recommendation	N/A

Table 14 – Examination results: OEV paragraph 2.5

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

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.
Initial audit finding	The installation procedure of the e-voting software on the control component is currently not formalised. Therefore, the examiners cannot ascertain that it is performed in an observable manner.
Follow-up audit observation	The installation procedure has been finalised.
Evidence	» 2022-03-30_Protokoll-CC4 » I_E-Voting Trusted Deployment.png
Result	Pass
Recommendation	N/A

Table 15 – Examination results: OEV paragraph 3.6

Key	3.14
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 distinct from each other. » The control components should be connected to different networks. » A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
Initial audit finding	The monitoring systems for the control components are not distinct from each other. The Post's datacentre service team has the keys for all control components' racks.
Follow-up audit observation	The Post has no plan to operate additional monitoring systems. The official version of the OEV includes a change compared to its draft version regarding the requirements for the monitoring systems: "*The hardware, the operating systems and the monitoring systems for the control components should be **as** distinct **as possible** from each other*". In the examiners' opinion, the cost induced by maintaining a dedicated monitoring system by control component (in terms of infrastructure, software and personnel) seems disproportionate in regard to the resulting risk reduction potential. Moreover, centralising logs into a

	common system (i.e., a Security Event Management System) for correlation and comprehensive analysis constitutes a best practice that should be maintained as is, which the rewording of the requirement allows. The Post has modified its organisation in terms of physical key management: The rack keys are no longer held by the datacentre service team, but by the Post's vault teams. The vault teams' personnel are not able to physically access the server rooms, as such access requires keys held by the datacentre service team.
Evidence	E-Voting – Physical Access Data Center E-Voting Infrastructure concept
Result	Pass
Recommendation	N/A

Table 16 – Examination results: OEV paragraph 3.14

Key	3.16
Requirement	Trustworthy components must perform only the intended operations.
Initial audit finding	The current Oracle database hardening reference guide is a rather old document (2014) that covers an older version (i.e., v.11gR2) of the product than the one supporting the e-voting system, in particular its control components. It may therefore not be adapted to the present context.
Follow-up audit observation	The Post has performed a compliance check with the CIS hardening guide for Oracle databases. Observed gaps will be analysed by database and security experts to determine whether the current configuration settings should be further strengthened. A new hardening baseline will then be issued and applied (target deadline: End of 2022).
Evidence	» CIS_EVoting-DB.txt » CIS_EVoting-OL7_ODA.txt
Result	Partially fail
Recommendation	The examiners consider that the completion of the planned action will ensure compliance with the requirement.

Table 17 – Examination results: OEV paragraph 3.16

Threats

Key	13.1

Requirement	The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis. They relate to the security objectives and must be taken into account when identifying risks. Depending on the vulnerabilities of the system identified, when the various bodies carry out their risk assessments, the risks are to be specified and considered based on the actual circumstances and depending on the specific threat.
Initial audit finding	The ISDP concept related to the e-voting system, which serves as a basis for the evaluation of the risks pertaining to the system, is not finalised at this stage. The examiners note that the Post only considers the threats listed in Numbers 13.3-13.39 in the existing document whereas they should be considered as a minimum basis. For instance, threat scenarios involving vandalism or sabotage on physical components of the e-voting system are not considered, nor accidental availability issues / information disclosure resulting from a bad manipulation by an employee.
Follow-up audit observation	The examiners were shown a finalised version of the ISDP concept. It now links applicable threats to countermeasures (listed as ISO27002 chapters). The Post considers additional risks as part of its general risk management process. Risks are reviewed on a regular basis and the risk catalog amended based on the vulnerabilities identified that affect the e-voting infrastructure and its operations. The official version of the OEV integrates an additional threat compared to the draft version, which has been integrated into the ISDP concept.
Evidence	Evidence was presented on-site to the examiners (ISDP concept and risk matrix).
Result	Pass
Recommendation	N/A

Table 18 – Examination results: OEV paragraph 13.1

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 or the 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 to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.
Initial audit finding	No alarm is currently set in case of errors in the registration of votes.
Follow-up audit observation	The Post has implemented an alarm in its monitoring system that spots errors in the registration of votes. It provides the number of sent votes and the number of confirmed votes.
Evidence	evoting_pit_dashboard-2022-08-23.pdf
Result	Pass
Recommendation	N/A

Table 19 – Examination results: OEV paragraph 14.1

Use of cryptographic measures and key management

Key	15.1
Requirement	Electronic certificates must be managed according to the best practices.
Initial audit finding	The e-voting system does not implement the requirements of the Post's security policy on cryptography with regards to certificate pinning.
Follow-up audit observation	The security policy on cryptography has been updated. Certificate pinning is now only recommended for mobile apps.
Evidence	Handbuch Kryptographie V03.02
Result	Pass
Recommendation	N/A

Table 20 – Examination results: OEV paragraph 15.1

Key	15.2 & 15.3

Requirement	15.2: In order to guarantee the integrity of data records that substantiate the accuracy of the result and ensure that secret and confidential 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 secret and confidential 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.
Initial audit finding	The Post has not formally documented how cryptographic controls implemented within the e-voting system mitigate specific threats at the infrastructure level (e.g. in its ISDP concept or in a threat model).
Follow-up audit observation	The ISDP concept has been updated. It integrates cryptographic controls as a mitigation means for certain threats.
Evidence	E-voting ISDS Konzept
Result	Pass
Recommendation	N/A

Table 21 – Examination results: OEV paragraph 15.2 & 15.3

Organisation of information security

Key	18.3
Requirement	The risks in connection with third parties (contractors irrespective of type, such as suppliers, service providers, etc.) must be identified and if necessary reduced by means of suitable contractual agreements. Compliance with the agreements must be appropriately monitored and reviewed throughout their term.
Initial audit finding	No evidence was shown to the examiners that the Post's standard supplier security management process has been applied to the companies involved in the e-voting supply chain. Moreover, the document shown to the examiners fails to mention some suppliers (e.g. Postfinance, as the datacentres' provider, which contract is managed directly by PostIT).
Follow-up audit observation	The Post has initiated the supplier security management process for the suppliers involved in the e-voting initiative. However, no concrete risk assessment has been undertaken so far, and no contractual agreement introduced.

	It seems that the suppliers' list is not exhaustive. As an example, the supplier in charge of the e-voting bug bounty (YesWeHack) is not listed.
Evidence	Supplier Assessment Liste KS_E-Voting Stand 16.09.2022.xlsx
Result	Fail
Recommendation	The Post should keep an inventory of the suppliers involved in the e-voting supply chain and ensure that each supplier undergoes its supplier security management process.

Table 22 – Examination results: OEV paragraph 18.3

Management of non-material and material resources

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.
Initial audit finding	The confidentiality grade mentioned in the *Schutzbedarfanalyse* document for the data processed within the e-voting system does not correspond to the taxonomy used in the information classification policy.
Follow-up audit observation	The *Schutzbedarfanalyse* has been updated and now includes the confidentiality grade specified in the information classification policy.
Evidence	E-voting ISDS Konzept
Result	Pass
Recommendation	N/A

Table 23 – Examination results: OEV paragraph 19.3

Trustworthiness of human resources

Key	20.1
Requirement	Suitable policies and procedures must be devised and promulgated in order to guarantee the trustworthiness of human resources before, during and after termination of employment or in the case of a change of activity.
Initial audit finding	The screening process on human resources interacting with the e-voting system is only performed once, whereas it should be performed every four years, as specified in the Post's guideline.

Follow-up audit observation	The Post is elaborating a new policy that requires employees with high integrity requirements (such as personnel involved in the e-voting project) to deliver a criminal records extract and an extract from the debt collection register every second year. This policy will apply from January 2023 on.
Evidence	Handbuch_Sicherheitsüberprüfung_MA.docx
Result	Fail
Recommendation	The examiners consider that the publication and enforcement of the policy will ensure compliance with the requirement.

Table 24 – Examination results: OEV paragraph 20.1

Key	20.2
Requirement	Human resources managers must accept full responsibility for guaranteeing the trustworthiness of human resources.
Initial audit finding	The examiners did not find any evidence that the Post's human resources department, or any other function assumes the responsibility for guaranteeing the trustworthiness of human resources.
Follow-up audit observation	The Post is developing a new policy (*Handbuch Sicherheitsüberprüfung*) that states the requirements in terms of employees screening. It includes a responsibility matrix for the various tasks forming the process. Several roles are involved in the decision to trust an employee based on a background check. In the case an employee has criminal records or debts, the manager (*Führungsperson*) is responsible for the hiring decision. HR and security staff are consulted. This organisation therefore suggests that human resource managers do not accept full responsibility for guaranteeing the trustworthiness of human resources.
Evidence	Handbuch Sicherheitsüberprüfung von Mitarbeitenden (draft)
Result	Fail
Recommendation	To satisfy the OEV's requirement, human resources managers should be explicitly made accountable for the decision to hire an employee based on the background check's output.
Relevance	In the examiners' opinion, the organisation proposed by the Post to support the employees screening process, where executive managers are accountable for decision making, is in line with information security good practices.

Table 25 – Examination results: OEV paragraph 20.2

Physical and environment security

Key	21.4
Requirement	All data must be processed exclusively in Switzerland, including storage.
Initial audit finding	The source code of the e-voting system being one of its critical information assets, one cannot state that all data is processed exclusively in Switzerland.
Follow-up audit observation	The Post does not plan to change the location of the source code currently stored on Gitlab in the US.
Evidence	Post Audit Response to examination report by SCRT – Scope 3 Infrastructure and operation 29.07.2022
Result	Fail
Recommendation	N/A
Relevance	The OEV should be more specific regarding the expression “all data” by specifying whether it includes the data not directly linked to voting events, such as the source code or technical logs for instance.

Table 26 – Examination results: OEV paragraph 21.4

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.
Initial audit finding	Although good practices in terms of allocation of obligations and areas of responsibility exist, a comprehensive documentation detailing how those practices mitigate the various types of risks originating from human resources does not seem to be available at this stage.
Follow-up audit observation	The Post has now referenced the *Operation Whitepaper of Swiss Post Voting System* document in its ISDP concept. This document details the organisation put in place to reduce the risks originating from human resources relating to operations and communications to a residual level.
Evidence	E-voting ISDS Konzept

Result	Pass
Recommendation	N/A

Table 27 – Examination results: OEV paragraph 22.1

Allocation, administration and withdrawal of access and admission authorisations

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.
Initial audit finding	At the time of the examination, the ISDP concept does not document the detailed risks and countermeasures related to accesses to the e-voting system's infrastructure and software. The examiners cannot conclude that access to infrastructure and software is regulated and documented in detail on the basis of a risk assessment. Moreover, it seems that it is possible to modify the default settings regarding the minimum number of members within the Administration Board. The examiners are therefore not able to ascertain that those manual operations in high-risk areas are conducted by at least two persons.
Follow-up audit observation	The Post has issued a dedicated document describing how access to the e-voting software is performed and what security principles are enforced to mitigate risks of unlawful access to the system. This document has been referenced in the ISDP concept. The operational guide at the attention of the cantons specifies that the operations conducted by the Administration Board members must be subject to the four-eyes principle. As an Election Authority is set up to supervise the operations, a canton would not be allowed to modify the default settings regarding the minimum number of members within the Administration Board.
Evidence	» E-Voting – ISDS Benutzerberechtigungskonzept » E-voting ISDS Konzept

Result	Pass
Recommendation	N/A

Table 28 – Examination results: OEV paragraph 23.2

Development and maintenance of information systems

Key	24.2.1
Requirement	An operating manual is created that includes the following for each user role: » a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; » a description of how the available interfaces can be used in a secure manner; » a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security; » a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions; » a description of the security measures to be implemented in order to achieve the operational security objectives.
Initial audit finding	At the exception of succinct recommendations proposed throughout the operational guide, that may be considered as “a description of the security measures to be implemented in order to achieve the operational security objectives”, the operational guide does not include the elements forming the requirement 24.2.1.
Follow-up audit observation	The operational guide maintained by the Post has been amended to better reflect the present requirements. The examiners noted that: » The document lists the user roles involved in the management of a voting event at cantonal level, i.e. Administrators, Administration Board members, Electoral Authority members, Auditors. By default, steps to manage a voting event are performed by Administrators. The document mentions when other roles must be involved; » A dedicated paragraph lists the main security events likely to occur during a ballot (i.e. the threats) and the associated countermeasures put in place to mitigate them; » A dedicated paragraph recaps the security-relevant actions to be performed.

	From a general point of view, the users have limited options in terms of parametrisation of security functions when managing a voting event. The operational guide advises extensively on security-relevant precautions and good practices to adopt to ensure that the processes occur securely.
Evidence	Benutzeranleitungen Release 0.15
Result	Pass
Recommendation	N/A

Table 29 – Examination results: OEV paragraph 24.2.1

Key	24.2.2
Requirement	The operating manual must identify all possible modes of operation of the software, including the resumption of operation after the detection of errors and the description of the consequences and effects of errors on the maintenance of secure operation.
Initial audit finding	The operational guide itself does not include the elements necessary to satisfy the requirement 24.2.2.
Follow-up audit observation	The operational has been amended to include potential errors likely to occur during a voting event as well as possible solutions to manage the event in secure conditions.
Evidence	Benutzeranleitungen Release 0.15
Result	Pass
Recommendation	N/A

Table 30 – Examination results: OEV paragraph 24.2.2

Key	24.2.3
Requirement	The operating manual must be precise and fit for purpose.
Initial audit finding	Given that the Post's operational guide does not include all the OEV's requirements specified in requirements 24.2.1 and 24.2.2, it can hardly be qualified as "precise" nor "fit for the purpose", although it is subject to continuous improvement and readability efforts.
Follow-up audit observation	The Post having amended the operational guide to better integrate the requirements 24.2.1 and 24.2.2, the examiners estimate that the document can be qualified as "precise" and "fit for the purpose".
Evidence	Benutzeranleitungen Release 0.15
Result	Pass

Recommendation	N/A

Table 31 – Examination results: OEV paragraph 24.2.3

Key	24.3.3
Requirement	A reliable and verifiable compilation with appropriate security measures must be carried out. This ensures that the executable code is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations. The compilation allows a chain of proofs to be created for the verification of the software and includes in particular: » evidence that the compilation environment is designed as described on the public platform (all tools with the respective version, operating system and any configurations); any derogations must be documented and justified; » evidence that the software has been compiled in accordance with the instructions available on the public platform; if an error in the instructions is found during compilation, this must be recorded and the documentation must subsequently be corrected; » evidence that the source code submitted for public scrutiny and examined is in fact the source code used for compilation; » evidence that no elements other than those provided for in the instructions have been introduced; » evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference (e.g. Maven Central Repository); » evidence that a dependency vulnerability analysis has been performed and that, if vulnerabilities relevant to the software exist, they do not render the software vulnerable to attack; » evidence that the parameters introduced, if any, do not render the system vulnerable.
Initial audit finding	At the time of the examination, the trusted build concept developed by the Post to carry out a reliable and verifiable compilation of the e-voting applications' source code with appropriate security measures has not been entirely formalised, nor been subject to an end-to-end execution. The examiners are therefore not able to state that the executable code of the e-voting system is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations, and that its compilation allows a chain of proofs.
Follow-up audit observation	The artefacts forming the front-end of the e-voting software have been integrated to the trusted build concept. The concept has been finalised and successfully executed: Independent observers have reproduced the compilation of the various components of the e-voting software and were able to

	generate the same hash values as the ones published on the publicly available source code repository.
Evidence	Trusted Build of the Swiss Post Voting System
Result	Pass
Recommendation	N/A

Table 32 – Examination results: OEV paragraph 24.3.3

Key	24.3.4
Requirement	A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that: 1. the code used in production is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations; and 2. the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The deployment allows a chain of proofs to be created for the verification of the software and includes in particular: » evidence that the production environment is the same as that which has been subjected to public scrutiny and independent examinations; any discrepancies (firmware version, configuration files, etc.) must be documented and justified; » evidence that the software deployed in the production environment is in fact that which was created using a reliable and verifiable compilation process; » evidence that the parameters introduced, if any, do not render the system vulnerable.
Initial audit finding	There is no process in place to provide evidence that the software deployed into the production environment is the one that has been subject to public scrutiny, nor that the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The examiners did not find any evidence that the technical parameters (relating to the cryptographic protocol) inputted by the cantons during the preparation of an event do not render the system vulnerable.
Follow-up audit observation	A trusted deployment process has been formalised for the e-voting software components. Independent observers witness the release of the software into the production environment to ensure that the code subject to the trusted build process is the code released. The seed entered by the cantons as part of the encryption parameters generation and prime numbers calculation is not likely to render the software vulnerable, as the validity of those cryptographic elements is checked using the *Verifier* software.
Evidence	Trusted Build of the Swiss Post Voting System

Result	Pass
Recommendation	N/A

Table 33 – Examination results: OEV paragraph 24.3.4

Key	24.3.5
Requirement	The quality of the evidence of reliable and verifiable compilation and reliable and verifiable deployment must be confirmed by the presence of at least two witnesses from different institutions or by technical procedures to establish the truth of the evidence in the light of current scientific knowledge and experience.
Initial audit finding	There is currently no documented process to support an independent observation of the deployment process into the production environment, nor any technical procedures guaranteeing a reliable and verifiable deployment.
Follow-up audit observation	The Post has formalised a process to ensure the verifiability of the deployment of the e-voting software. It relies on the involvement of several independent observers.
Evidence	Trusted Build of the Swiss Post Voting System
Result	Pass
Recommendation	N/A

Table 34 – Examination results: OEV paragraph 24.3.5

Key	24.3.6
Requirement	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available.
Initial audit finding	No chain of evidence exists at this stage to ensure the reliable and verifiable nature of the software deployment phase. As the trusted build concept has not been subject to end-to-end execution at this stage, the chain of evidence of reliable and verifiable compilation is not published yet.
Follow-up audit observation	The chain of evidence is formed by the hash values of the e-voting software artefacts generated following the trusted build and trusted deployment processes.
Evidence	https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Trusted-Build/Release-0.15.2.1/checksum.md
Result	Pass
Recommendation	N/A

Table 35 – Examination results: OEV paragraph 24.3.6

Operation

Key	25.6.2
Requirement	Persons who operate and use the system must be trained and provided with the necessary documentation.
Initial audit finding	The document *Schulungskonzept E-Voting* is not up to date (the version provided to the examiners is dated May 2019 and mentions the company Scytl for 3rd level support, whereas this company no longer exists).
Follow-up audit observation	The document detailing the training concept for the cantons has been updated.
Evidence	E-Voting - Training concept canton
Result	Pass
Recommendation	N/A

Table 36 – Examination results: OEV paragraph 25.6.2

Key	25.6.4
Requirement	Help on using the system must be readily available.
Initial audit finding	At the time of the examination, the collaboration platform between the Post and the cantons for e-voting-related topics is under development.
Follow-up audit observation	The collaboration platform between the Post and the cantons is now active. It serves as a central repository for information related to the e-voting system (e.g. release notes, manuals, articles, issue notifications, etc.)
Evidence	E-voting collaboration platform hosted by the Post
Result	Pass
Recommendation	N/A

Table 37 – Examination results: OEV paragraph 25.6.4

5 References

[1] "Reorienting eVoting and ensuring stable trial operation," *www.egovernment.ch*. Accessed Oct. 21, 2021. [Online]. Available: https://www.egovernment.ch/en/umsetzung/schwerpunktplan/vote-electronique/.

[2] Swiss Federal Chancellery, Political Rights Section, "Redesign and relaunch of trials - Final report of the Steering Committee Vote Electronique (SC VE)." Nov. 30, 2020. Accessed: Dec. 06, 2021. [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

[3] Swiss Federal Chancellery, Political Rights Section, "Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials)." Apr. 28, 2021. Accessed: Dec. 06, 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

[4] Swiss Federal Chancellery, "Federal legislation." Accessed Oct. 21, 2021 [Online]. Available: https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html (accessed Oct. 21, 2021).

[5] Swiss Federal Chancellery (FCh) - Political Rights section, "Audit concept for examining Swiss Internet voting systems - v1.3." May 18, 2021.

[6] Swiss Federal Chancellery, "Examination of the Swiss Internet voting system, Version:1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider". March 2022. [Online]. Available: https://www.newsd.admin.ch/newsd/message/attachments/71144.pdf

[7] Swiss Federal Chancellery, "Ordinance on Political Rights (PoRo), section 6a: Electronic Voting Trials". Accessed Jun. 11, 2022. [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

[8] Swiss Federal Chancellery, "Federal Chancellery ordinance on electronic voting (OEV)." Apr. 28, 2021. Accessed: June 11, 2022 [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2022/336/en