SCRT
Information Security

Examination of the Swiss Internet voting system

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

16/06/2023

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	20.04.2023	Draft for review by the Federal Chancellery
1.0	Stéphane Adamiste	16.06.2023	Final report

Management summary

Scope and objective of the examination

During the period September 2021 – November 2022, SCRT carried out two successive security compliance audits 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*).

The first audit (round 1) resulted in the identification and reporting of twenty-four non-compliances (findings).

The second round (round 2) consisted in the follow up of the findings raised in the initial audit report. Five requirements were assessed as not met (*fail* status) or partially not met (*partially fail* status) during this second audit.

The objective of the present examination is to follow up on the round 2 audit findings.

In addition, this audit considers:

- Some changes performed within the Post’s infrastructure that impact the observations reported previously;
- Some criteria added by the Federal Chancellery to the 3 b) scope (i.e. numbers 2.7.1, 2.7.2, 2.7.3).

Methodology

The examiners looked for evidence of effort to comply with the audit criteria 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 third examination was performed during the period April-May 2023.

Results

After the third round of audit, one requirement is assessed as not met (*fail* status) among the five non-compliances reported in the previous round. The said requirement, in its current form, lacks precision in its wording and should be reconsidered, as already suggested in previous reports.

A partial non-conformity has been identified among the newly introduced criteria: the procedure at the attention of the voters to verify that the software provided by the server has not been altered is not exhaustive.

Finally, the examiners noted a partial non-conformity induced by the use of self-signed certificates on the e-voting system components. However, the trust model applied now (direct trust) does not necessarily require a recognised supplier for the provision of certificates.

Recommendations

SCRT recommends adding one step in the procedure at the attention of the voters to verify that the software provided by the voting server has not been altered. The Post is also advised to request an authorisation to use self-signed certificates from the Federal Chancellery to support the digital signature process within the e-voting system, as the adopted trust model is deemed in line with best practices.

Finally, this report provides a comment at the attention of the Federal Chancellery regarding the examination criterion 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.

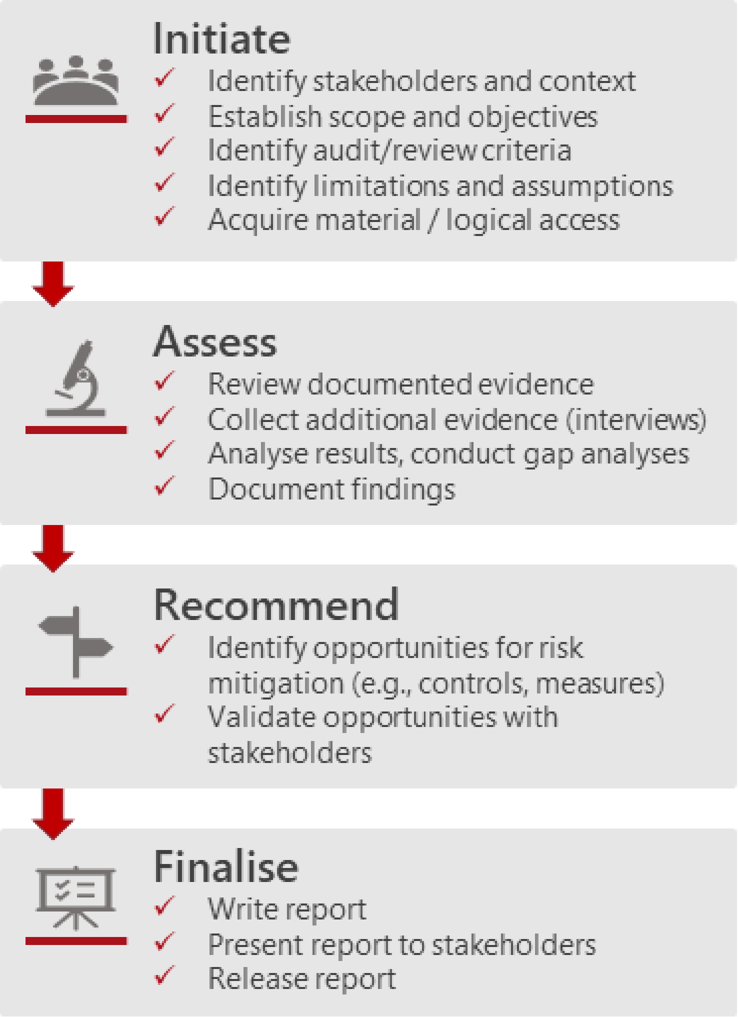
8. A second assessment was conducted in mid-September 2022 to follow-up on the findings raised in the initial audit report. The audit report was published in March 2023 on the Federal Chancellery's website [9].

9. A third assessment was conducted in April 2023 to follow-up on the findings raised in the second audit report, assess changes performed within the Post's infrastructure that impact the observations reported previously, as well as some criteria added by the Federal Chancellery to the 3 b) scope.

2 Methodology

2.1 Process

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



Initiate
- ✓ Identify stakeholders and context
- ✓ Establish scope and objectives
- ✓ Identify audit/review criteria
- ✓ Identify limitations and assumptions
- ✓ Acquire material / logical access

Assess
- ✓ Review documented evidence
- ✓ Collect additional evidence (interviews)
- ✓ Analyse results, conduct gap analyses
- ✓ Document findings

Recommend
- ✓ Identify opportunities for risk mitigation (e.g., controls, measures)
- ✓ Validate opportunities with stakeholders

Finalise
- ✓ Write report
- ✓ Present report to stakeholders
- ✓ Release report

Figure 1 - Process

2.2 Collection of evidence

12. 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.

13. 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

14. 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

15. 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.

16. 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 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.

2.6 Assumptions

2.6.1 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.

2.6.2 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

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

- which were reported to be not fulfilled during the round 2 examination;
- which have been added to the audit scope 3 b) since the round 2 examination;
- which relate to changes reported by the Post to the examiners in its infrastructure.

Criteria not fulfilled during round 2

Trustworthy components in accordance with Number 2 and their operation

Key	Requirement
3.16	Trustworthy components must perform only the intended operations.

Table 1 - E-voting requirements: Requirements for trustworthy components in accordance with Number 2 and their operation

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 2 - E-voting requirements: Organisation of information security

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 3 - 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 4 - E-voting requirements: Physical and environment security

Newly introduced criteria

Requirements for the cryptographic protocol: voting secrecy and absence of premature results

Key	Requirement
2.7.1	It must be ensured that the attacker is unable to breach voting secrecy or establish premature results unless he can control the voters or their user devices.
2.7.2	With the exception of the person voting and his or her user device, system participants who have enough information to breach voting secrecy or to collect premature results are not considered protected against the attacker.
2.7.3	It must be ensured that the attacker cannot take control of user devices unnoticed by manipulating the user device software on the server. The person voting must be able to verify that the server has provided his or her user device with the correct software with the correct parameters, in particular the public key for encrypting the vote.

Table 5 - E-voting requirements: Requirements for the cryptographic protocol: voting secrecy and absence of premature results

Changes performed by the Post

21. Changes reported by the Post in its infrastructure include:

- » A reorganisation of the e-voting teams;
- » A split of the control components' databases;
- » A different way of managing the certificates used to support cryptographic operations within the e-voting system.

22. The following table maps the reported changes performed by the Post with the OEV requirements.

Key	Change	Associated OEV requirement
1	Reorganisation of the e-voting teams	18.1, 22.1
2	Split of the control components' databases	3.14
3	Certificate management practices	15.1, 15.2, 15.3, 15.4

Table 6– Changes performed by the Post since round 2 and associated OEV requirements

Key	Requirement
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.

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.
15.4	Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. NIST, ECRYPT, ESigA). The electronic signature meets the requirements of an advanced electronic signature in accordance with the Federal Act of 18 March 2016[1] on Electronic Signatures (ESigA). The signature must be verified by means of a certificate that has been issued by a recognised supplier of certificate services under the ESigA.
18.1	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
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 7 – OEV requirements associated to infrastructure changes by the Post

[1] SR **943.03**

4 Examination results

23. 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.

Criteria not fulfilled during round 2

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

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.
Round 2 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).
Round 3 audit observation	The Post has established and deployed a security baseline for the Oracle database version it runs on its information systems, in particular on the e-voting control components. The baseline is inspired by the CIS hardening guide applicable to Oracle databases. The document *Konzept Oracle Datenbanken Hardening* justifies which recommendations from the CIS hardening guide have not been applied. The appendix *CIS.xslx* to the *Konzept* document is the step by step procedure to implement the security baseline. Applying a secure configuration baseline reduces the risk of unintended operations on the trustworthy components.
Evidence	» Konzept Oracle Datenbanken Hardening » CIS.xslx
Result	Pass
Recommendation	N/A

Table 8 – Examination results: OEV paragraph 3.16

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).
Round 2 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.
Round 3 audit observation	The Post has updated its list of suppliers involved in the e-voting initiative and has performed a risk assessment of the concerned companies, according to the requirements set in the "*Handbuch Supplier Security Management*" document. Risk assessments include regular on-site audits, remote audits or self-declarative assessments based on a specialised third-party software solution (Bitsight Cyber Risk Analytics & Security Ratings), depending on the criticality of the service supplied. The supplier security management policy mandates the inclusion of a number of security clauses into suppliers' contracts, based on the nature of the service provided. As part of its audit work, the Post verifies the presence of those clauses into the existing agreements with suppliers and notifies the procurement department when it is not the case, so that contracts be updated.
Evidence	» Handbuch Supplier Security Management » List of e-voting suppliers
Result	Pass
Recommendation	N/A

Table 9 – Examination results: OEV paragraph 18.3

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.
Round 2 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.
Round 3 audit observation	The *Sicherheitsüberprüfung von Mitarbeitenden* policy has come into force on January 1st 2023. Internal and external personnel involved in the e-voting project (64 people at the time of the examination) have been formally identified and have been subject to the screening process. Moreover, the personnel has been requested to sign a non-disclosure agreement.
Evidence	Handbuch Sicherheitsüberprüfung von Mitarbeitenden
Result	Pass
Recommendation	N/A

Table 10 – 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.
Round 2 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.
Round 3 audit observation	The *Handbuch Sicherheitsüberprüfung* policy has been updated. It includes a responsibility assignment matrix stating that "HR- Services 1st Level" are accountable for the whole screening process. This allows to conclude that HR managers endorse the responsibility for guaranteeing the trustworthiness of human resources.
Evidence	Handbuch Sicherheitsüberprüfung von Mitarbeitenden - §7.1 Rollen, Aufgaben, Kompetenzen und Verantwortung
Result	Pass
Recommendation	N/A

Table 11 – 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.
Round 2 audit observation	The Post does not plan to change the location of the source code currently stored on Gitlab in the US.
Round 3 audit observation	No change was observed since the previous audit round.
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 12 – Examination results: OEV paragraph 21.4

Newly introduced criteria

Requirements for the cryptographic protocol: voting secrecy and absence of premature results

Key	2.7.1 & 2.7.2
Requirement	It must be ensured that the attacker is unable to breach voting secrecy or establish premature results unless he can control the voters or their user devices (2.7.1). There is no obligation to prevent attacks that limit the number of tallied votes to the degree that all partial votes for a question, list or candidate are the same (2.7.2).
Audit observation	Maintaining voting secrecy and preventing the premature disclosure of a ballot's results are properties enforced through the implementation of a cryptographic protocol within the e-voting application amongst others. The Post has conducted a security analysis of the said cryptographic protocol (See *Swiss Post voting protocol computational proof* document) to demonstrate it meets the intended security requirements when the user device is considered trustworthy and if at least one control component can be trusted. From an infrastructure point of view, an attacker aiming to breach voting secrecy and establish premature results without controlling the voters or their user devices would likely try to execute one of the following threat scenarios: » Introduction of a backdoor in the system via a software dependency; » Introduction of malicious code into the e-voting software directly; » Manipulation of the e-voting software; » Redirection of votes using DNS spoofing; » Reading of votes using man-in-the-middle attacks; » Abuse of the decrypting key to reveal votes; » Exploitation of a weakness in the encryption process. Those scenarios have been taken into account by the Post in its Information Security and Data Privacy concept and have been subject to risk mitigation measures, as required by Number 13.1. In this regard, the document *Leitfaden BK: Risikobeurteilungen – E-Voting-System der Schweizerischen Post* maps the threats listed above with the main associated mitigating controls (OEV requirements). The adequate implementation of those OEV requirements, as stated by the auditors during the previous rounds of examination for the *3 b)* scope proves to reduce risks of breaching voting secrecy or establishing premature results to a residual level.
Evidence	» Swiss Post voting protocol computational proof v1.1.0 » Leitfaden BK: Risikobeurteilungen – E-Voting-System der Schweizerischen Post
Result	Pass
Recommendation	N/A

Table 13 – Examination results: OEV paragraph 2.7.1 & 2.7.2

Key	2.7.3
Requirement	It must be ensured that the attacker cannot take control of user devices unnoticed by manipulating the user device software on the server. The person voting must be able to verify that the server has provided his or her user device with the correct software with the correct parameters, in particular the public key for encrypting the vote.
Audit observation	The voting client application (more precisely, the *GetKey* algorithm) checks that the public key used to encrypt votes submitted by the persons voting corresponds to the key that was inputted by the cantons in the election setup component. An error message is triggered if it is not the case. The algorithm also checks the other input and context arguments from the voting server. The voting client application includes JavaScript files, whose integrity can be checked by the voting persons thanks to the use of the *subresource integrity* tag, a functionality that compares the hash value of the served JavaScript files with the genuine files' hash values, which are made available in the published protocols by the cantons. The procedure is described in the Post's e-voting documentation. This procedure, however, does not provide any means to verify the *html* part of the client software, that can be manipulated on the server to take control of user devices (e.g. by adding a script that captures cursor coordinates at click times and sends them to a remote server controlled by the attacker).
Evidence	» Swiss Post Voting System - System specification v1.3.0 » https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Security-advices/en/hash_browser_manual.md » E-voting demo website: https://demo.evoting.ch/
Result	Partially fail
Finding	Although it is feasible to verify the integrity of the *html* part of the user device software by comparing its source code with the official code on the Post's public Gitlab instance, no such instruction is provided within the security advice at the attention of the voting persons. This gap could be exploited to compromise user devices unnoticed by manipulating the user device software on the server.
Recommendation	The procedure for verifying the user device software should not be limited to JavaScript files but also include the *html* file.

Table 14 – Examination results: OEV paragraph 2.7.3

Changes performed by the Post

Key	1
Change	Reorganisation of the e-voting teams

Associated OEV requirements	» 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. » 18.1: All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated. » 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.
Description	Since October 2022, all employees involved in the operation of the e-voting control components belong to a unique team (devOps e-governemnt), following a reorganisation. To enforce the OEV requirements mentioned here above, the team has been split so that dedicated employees be in charge of the operation of one and only one control component. Therefore, four “split teams” have been constituted. From a technical point of view, members of a split team are able to access SSH-keys that allow connecting to their control component only. Operational tasks are subject to the four-eyes principle and segregation of duties applies to the access right management process (e.g. some people may be in charge of the operation of one control component and the allocation of access rights to another control component, a separate team (i.e. the “token team”) grants access tokens that act as second authentication factor on a discretionary basis.
Evidence	eGovernment – FOM 2.0 neue Teamorganisation
Result	Pass
Recommendation	N/A

Table 15 – Examination results: Change #1 performed by the Post

Key	2
Change	Split of the control components’ databases
Associated OEV requirements	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.
Description	The Post has further increased the isolation of the control components by physically separating their databases. Each control component has now its own database cluster running in the same network as the control component itself. Access to the database requires the activation of a firewall rule between the administration jump host and the database cluster. Administrators must belong to the Windows group that is allowed to access the jump host and to the group that is allowed to access one of the database clusters. Group membership is managed by the token team.
Evidence	E-Voting – Control Components Database Infrastructure
Result	Pass
Recommendation	N/A

Table 16 – Examination results: Change #2 performed by the Post

Key	3
Change	Certificate management practices
Associated OEV requirements	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 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. 15.4: Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. NIST, ECRYPT, ESigA). The electronic signature meets the requirements of an advanced electronic signature in accordance with the Federal Act of 18 March 2016 on Electronic Signatures (ESigA). The signature must be verified by means of an electronic certificate that has been issued by a recognised supplier of certificate services under the ESigA.
Description	Digital signatures are used within the e-voting system to ensure that messages exchanged between the trustworthy parties originate from the expected party and have not been altered. The Post has now opted for a direct trust model to support the e-voting digital signature process. Each trustworthy party

	generates a private signing key and a self-signed certificate containing the related public key, the certificates are transmitted via a secure out-of-band channel, and their authenticity is checked by verifying the files' hash value. The cryptographic material is stored under the form of PKCS#12 keystores on the e-voting system components. key lengths and algorithms used correspond to the current standards According to the requirement of the Post's cryptography handbook, the use of self-signed certificates requires a derogation, which has been granted.
Evidence	» Cryptographic Primitives of the Swiss Post Voting System v1.3.0 (§6) » Direct Trust Keystores – E-Voting collaboration platform » Handbuch Kryptographie v03.02 » Ausnahme 3864 - E-Voting: Direct Trust (Self-Signed Zertifikat innerhalb der Applikation)
Result	15.2, 15.3: Pass 15.1: Pass 15.4: Partially fail
Findings	Certificates used for digital signature on the e-voting system components are not issued by a recognised supplier of certificate services under the ESigA.
Recommendation	The Post should request a derogation from the Federal Chancellery regarding this requirement.
Relevance	The direct model used by the Post to establish trust between the trustworthy parties does not require certificates issued by a recognised supplier of certificate services.

Table 17 – Examination results: Change #3 performed by the Post

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.

[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).” May 25, 2022. Accessed: June 11, 2022 [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2022/336/en

[9] Swiss Federal Chancellery, "Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider - Round 2 " November 2022. Accessed: April 15, 2023 [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