Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

7 February 2025

Audit concept v1.6

For examining Swiss e-voting systems

File reference: 431.0-2/15/4/7

Introduction

This document aims at defining the foundations for assessing the compliance of electronic voting systems with the Federal Chancellery Ordinance of 25 May 2022 on Electronic Voting (OEV) including its annex[1], as per chapter 26 of the annex of the OEV, and for obtaining recommendations for improvements. It describes the rules for preparing, conducting and reporting this examination. It is intended for both examiners and examinees.

Examinations of the system should be carried out at an early stage in order to allow sufficient time before the system is put into operation for non-conformities to be remedied and re-checked.

Context

Internet Voting in Switzerland

Internet voting (also known as 'e-voting') is part of the Swiss e-government strategy. The Confederation and the cantons have agreed to support internet voting and take further steps to introduce it in Switzerland. Since 2004, 15 cantons have offered internet voting to certain sections of their electorate in over 300 trials. At the beginning of 2019, internet voting was offered in ten cantons, either to registered voters living abroad and resident voters, or only to registered voters living abroad. The cantons could choose between two systems: the system offered by the canton of Geneva and the system offered by Swiss Post.

Based on its decision of November 2018, the Canton of Geneva informed in June 2019 that its system would no longer be available with immediate effect.

The Swiss Post system used in trials until February 2019 offered individual verifiability. In order to comply with federal legislation, Swiss Post's new system that aimed for complying with the requirements on complete verifiability underwent a certification procedure, its source code was made accessible and, subsequently, a public intrusion test was conducted. Based on voluntary analysis of the source code and in the course of a subsequent audit mandated by the Federal Chancellery, researchers revealed significant security flaws. In view of this, Swiss Post announced the withdrawal of its individually verifiable system and the focusing on the development of the completely verifiable system.

On 26 June 2019, the Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of e-voting. In 2020, the Federal Chancellery and the cantons have produced a joint final report on the redesign and relaunch of e-voting trials[2]. In the first stage of the redesign, the legislation on e-voting has been revised. The partially revised Ordinance on Political Rights (PoRO) and the totally revised OEV came into force on 1 July 2022.

Since July 2021, the Federal Chancellery is commissioning independent examinations of the redesigned Swiss Post e-voting system aiming for complete verifiability and its operation.[3] In the process and as part of the continuous improvement process, existing need for action is identified and set out in a joint catalogue of measures by the Confederation and the participating cantons in consultation with Swiss Post[4]. The Federal Chancellery monitors the implementation of measures as part of the authorisation procedures.

The Federal Council granted the cantons of Basel-Stadt, St Gallen and Thurgau basic licences for trials with online voting in federal votes in 2023-2025 and in the National Council elections on 22 October

[1] SR **161.116**

[2] www.bk.admin.ch > Political Rights > E-Voting > Reports and studies

[3] www.bk.admin.ch > Political Rights > E-Voting > Examination of systems

[4] www.bk.admin.ch > Political Rights > E-Voting > Trials with e-voting

2023. At its meeting on 22 November 2023, the Federal Council also granted the canton of Graubünden a basic licence for trials with online voting in 2024-2026.

Purpose

In the context of the assessment of the Swiss e-voting system, the experts shall answer the following questions:

- Are the system, its development and operation compliant with the legal requirements?
- Are the measures taken to mitigate risks effective?
- Which improvements could be made for the sake of security, trust and acceptance?

The answers to these questions will be part of the basis used by the Federal Chancellery to prepare its recommendation on whether or not to grant use of the system and also for future actions on the strategic level.

Organisation

The Federal Chancellery mandates a group of experts (examiners) on the basis of the present concept. The group as a whole shall demonstrate expertise in the following areas:

- Cryptography
- E-Voting technology
- Software engineering
- Understanding and experience with IT Frameworks and market best practices, i.e. ISO 27001, COBIT[5], NIST[6] and CIS[7]
- Audit experience in the field of operational security
- Audit education, respectively certification

Experts will be assigned one or several scopes according to their competences. Each scope will be covered by at least 2 experts if appropriate. They can work in groups or individually. When working in groups, one of the experts is responsible toward the Federal Chancellery. The organisation within the group is left to the members.

The Federal Chancellery supervises the work and is available to experts in the event of difficulties or questions.

When the Federal Chancellery receives a draft report covering one scope, the examinees may prepare a response to the examination report prior to its publication. The report and its response can be discussed at a meeting with representatives of the Federal Chancellery, experts and examinees. The experts can then decide whether or not to amend their report, which then become final.

Methodology

For the examination plan to be established, the examinees provide the examiners with a table mapping the OEV requirements with the system and processes from the examinees. The mapping table shall describe each requirement, who takes responsibility for it and what means are used to fulfil it (function of the system, infrastructure item, process and/or documentation). The examiner can then prepare his examination plan on this basis. Should the analysis of this mapping raise questions or reveal gaps, the examiner shall contact the examinee and, if necessary, the Federal Chancellery.

[5] Control Objectives for Information and Related Technology

[6] National Institute of Standards and Technology

[7] Center for Internet Security

The approach for assessing the compliance shall be systematic, objective and structured. It shall be based on the above-mentioned mapping, the risk assessments and the documentation provided by the examinees. Documentation that is not listed in this concept but which the examiner would consider relevant to his or her assessment must be provided by the examinees upon request. The same applies to access to tools. The examinees must designate persons who are able to support the examiner in his work and ensure their availability.

Additionally to the analysis of the documentation and tools, the examiner may conduct interviews with the relevant persons. Interviews can be carried out at the examinee's premises or remotely. If scopes foresee interviews, these must be carried out. The examiner may schedule additional interviews if he or she considers them useful for the examination.

Finally, in some cases, on-site inspections may be necessary to allow a thorough assessment. This is especially the case for infrastructure and operation and printing office. Interviews can be combined with on-site inspections for efficiency. Examinees must guarantee fully transparent access to the examiners and make competent persons available to them during the visit.

Access to the documentation should be organised by the examinees, preferably electronic for efficiency reasons.

Whenever useful to clarify preliminary questions, to present new elements or to define the schedule of the examination, a kick-off meeting can be arranged by the examinee or the Federal Chancellery.

Rights and duties

Of the examiners

- Rights
  - Get access to the documentation, tools, facilities and people needed to conduct the examination
  - Get support from the examinees and the Federal Chancellery
  - Retain the copyright on the report and the right to publish the work related to this examination and to cite analysed documents that must be published by the Cantons and/or the system provider according to Swiss law
- Duties
  - Examining according to the specified method
  - Stay independent and objective
  - Provide an examination report in response to the purpose set out in this document, the report will be published

Of the examinees

- Rights
  - Be assessed fairly and accurately
  - Take a stand on findings
- Duties
  - Provide access and support in investigations
  - Be transparent, proactive and truthful
  - Provide requested information

Scopes

The following chapters describe the different scopes as per defined in the chapter 26 of the annex of the OEV. Together, they cover the entire system, its development and operation. The distribution of experts and their skills must ensure full coverage, free of gaps.

To ensure comprehensiveness and as the cryptographic protocol is the corner stone of the security of the system, experts involved in its verification may be involved in the other scopes.

In addition to the legal bases, the risk assessments of the relevant stakeholders will also be used in the examinations to ensure the effectiveness of the measures taken to mitigate the risks.

Any reports available from the examinee or other sources shall be consulted as far as it serves the purpose.

The detailed scopes presented in this document are intended to provide a basis for a first assessment of the workload. If there are reasons for a requirement not to be assessed in a particular detailed scope, this can be set out within the audit plan. The mapping table provided by the examinees serves as additional guidance within which scope the individual requirements should be examined.

Scope 1: Cryptographic protocol

Criteria

The protocol must fulfil the requirements listed in number 2 of the annex of the OEV.

The requirements comprise:

- a list of abstract system players and a list of abstract communication channels both to be instantiated in protocol definitions;
- a set of security goals to be achieved by executing the protocol. The goals relate to verifiability, secrecy and authentication;
- for each security goal: the strongest permissible assumptions on the trustworthiness of the system players and the communication channels;
- further side-conditions setting boundaries to the definition of the protocol;
- requirements on proofs that demonstrate the conformity of the protocol definition with the requirements (cryptographic and symbolic proof). The proofs may be conducted with respect to cryptographic basic components under generally accepted security assumptions (for example, "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). The protocol should be based as far as possible on existing and proven protocols.

Examinee

System developer

Examiners

Experts in cryptography

Detailed scope

Assess the conformity of the protocol specification, highlight cases of doubt and potential for improvement. Examiners assess the protocol specification document against the requirements in number 2 of the annex of the OEV based on their knowledge and experience with cryptographic protocols and the possible pitfalls. To that end, the argumentation in the proofs must be reviewed.

Documentation

The examinee shall provide at least:

- Cryptographic protocol specification
- Cryptographic proof
- Symbolic proof

Interviews

None

Scope 2: Software

Criteria

The software of the system including the auditor's technical aid must fulfil the requirements listed in numbers 2 to 25 of the annex of the OEV and adequately support the protocol (number 2 of the annex of the OEV). The mapping between a requirement in those paragraphs and the place (functionality in the system, organisational procedure, element of infrastructure, etc.) where it is fulfilled shall be provided by the examinees before the examination. If the mapping table indicates that a requirement is covered in another scope than the one specified here, the examiner shall verify this claim. Functions whose trustworthiness is decisive for the effectiveness of verifiability as per OEV, must be examined in detail on the basis of the source code and the cryptographic protocol.

Examinees

System developer and provider

Examiners

Experts in cryptography and in software development; specifically experts or groups of experts with a high level of knowledge in software engineering and secure development process, possibly with support of experts in cryptography who examined the scope 1.

Detailed scope

	Requirements of the OEV
a) Assess the development process	8.13, 17.1, 17.2, 17.3, 24.1.1, 24.1.2, 24.1.3, 24.1.4, 24.1.14, 24.1.15, 24.1.16, 24.1.17, 24.1.18, 24.1.19, 24.1.20, 24.4.1, 24.4.2, 24.5, 25.13.3, 25.13.4
b) Assess the code quality and security	3.2, 14.1, 14.2, 14.4, 14.5, 14.6, 15.2, 15.3, 15.4, 24.1.5, 24.1.6, 24.1.10, 24.1.12, 25.8.2, 25.8.3, 25.8.4, 25.8.5, 25.9.2, 25.9.3, 25.9.4, 25.10.5, 25.10.6, 25.10.7, 25.10.8, 25.11.2, 25.11.3, 25.11.4, 25.12.2, 25.12.3, 25.12.4, 25.13.2, 25.13.5
c) Asses the documentation quality	24.1.5, 24.1.6, 24.1.7, 24.1.8, 24.1.9, 24.1.12, 24.1.13, 25.2.2, 25.2.3, 25.2.4, 25.2.5, 25.2.6, 25.2.7, 25.2.8, 25.3.2, 25.3.3, 25.3.4, 25.3.5, 25.3.6, 25.4.2, 25.4.3, 25.5.2, 25.5.3, 25.5.4, 25.10.2, 25.10.3, 25.10.4
d) Assess the alignment between software development products	24.1.9, 24.1.11, 25.1.3, 25.2.8
e) Assess the implementation of the protocol	2.5, 2.6, 2.7, 2.8, 2.12.1, 2.12.2, 2.12.3, 2.12.4, 2.12.5, 2.12.6, 2.12.7, 2.12.8, 2.12.9, 2.12.10, 2.12.11, 2.13.1, 2.13.2, 3.17, 25.1.2
f) Assess the functionalities	3.13, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 5.1, 8.11, 9, 10, 11.1, 11.5, 11.6, 25.7.2, 25.7.3

Documentation

The examinees shall provide at least:

- Risk assessment
- Mapping between relevant requirements and way of implementation

- Cryptographic protocol
- Specification and design documentation
- Source code
- Development process documentation
- Configuration management documentation
- Tests documentation
- Build and deployment process documentation
- Quality assurance documentation including audit reports
- Usability concept

Whenever tools are used to support the processes (e.g. Jira, SonarQube, etc.), access to them shall be provided.

A running version of the system with test data shall be available.

Interviews

Interviews shall include at least people from:

- Project management
- Development team
- Test team

Scope 3: Infrastructure and operation

Criteria

The system and its operation must fulfil the requirements listed in numbers 2 to 25 of the annex of the OEV and adequately support the specified objectives. The mapping between a requirement in those paragraphs and the place (functionality in the system, organisational procedure, element of infrastructure, etc.) where it is fulfilled shall be provided by the examinees before the examination. If the mapping table indicates that a requirement is covered in another scope than the one specified here, the examiner shall verify this claim. The core system must be operated in a currently valid ISO 27001 certified infrastructure. Basic components, such as software that serves the secure and independent use of control components, the operating systems used or the servers used must be proven to meet the best standards.

Examinees

System provider, canton and printing office

Examiners

Experts in cryptography and in operating highly secure systems; specifically experts or groups of experts with a high level of knowledge in operational security, possibly with the support of experts in cryptography who examined the scope 1.

Detailed scope

	Requirements of the OEV
a) Assess the certification(s) of the system provider	ISO 27001:2022 certificate + Statement of Applicability (SoA)
b) Assess the infrastructure and organisational measures of the system provider	2.5, 2.6, 2.7, 2.9.1.2, 2.9.2.2, 2.9.3.2, 2.9.4.2. 2.13.3, 3.5, 3.6, 3.7, 3.8, 3.9, 3.11, 3.12, 3.14, 3.15, 3.16, 3.17, 3.19, 3.20, 8.13, 11.1, 11.4, 12.1, 12.2, 12.8, 13, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.8, 14.9, 14.10,

	15.1, 15.2, 15.3, 15.4, 16.1, 16.2, 18.1, 18.2, 18.3, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4, 22.5, 23.1, 23.2, 23.3, 23.4, 23.5, 24.2.1, 24.2.2, 24.2.3, 24.3.1, 24.3.2, 24.3.3, 24.3.4, 24.3.5, 24.3.6, 24.4.1, 24.4.2, 24.4.3, 25.6.2, 25.6.3, 25.6.4
c) Assess the infrastructure and organisational measures of the canton	Art. 11, art. 14, 2.5, 2.6, 2.7, 2.8, 2.9.1.2, 2.9.2.2, 2.9.3.2, 2.13.3, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.20, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 5.1, 5.2, 6.1, 6.2, 6.3, 7.1, 7.2, 7.3, 7.8, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12, 8.13, 8.14, 9, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 13, 14.1, 14.2, 14.3, 14.4, 14.7, 14.8, 14.9, 14.10, 15.1, 15.2, 15.3, 15.4, 16.1, 16.2, 18.1, 18.2, 18.3, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4, 22.5, 23.1, 23.2, 23.3, 23.4, 23.5, 24.3.5, 24.3.6, 24.4.1, 25.6.2, 25.6.3, 25.6.4
d) Assess the infrastructure and organisational measures of the print office	2.9.1.2, 2.9.3.2, 2.9.4.2, 2.13.3, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.17, 3.19, 3.20, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 14.9, 18.1, 18.2, 18.3, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4, 22.5

Documentation

The examinees shall provide at least:

- Relevant organisational process descriptions

Additionally, the system provider shall provide at least:

- Risk assessment
- Mapping between relevant requirements and way of implementation
- Training records
- Current valid ISO 27001 certificate and Statement of Applicability (SoA)
- Operational documentation
- Network schemas
- Logging and monitoring concept

Additionally, the canton shall provide at least:

- Risk assessment
- Mapping between relevant requirements and way of implementation
- Training records
- Tests documentation

Additionally, the printing office shall provide at least:

- Risk assessment (if not already part of the canton’s risk assessment)

- Network schemas

Interviews

Interviews shall include at least:

- Operation team
- Incident response team
- Cantonal responsible

Scope 4: Penetration test

Criteria

Competent attackers from the Internet must not be able to penetrate the infrastructure in order to gain access to important data or to take control of important functions. A penetration test is to be run to assess the effectiveness of the security measures taken to prevent such cases. The tests are carried out on the basis of potential vulnerabilities discovered after a methodical analysis of publicly available documentation, in particular that in article 11 of the OEV.

Examinee

System provider

Examiners

Security experts; specifically experts or groups of experts with high level of knowledge in penetration testing, possibly with the support of experts in cryptography who examined the scope 1.

Detailed scope

a) Search public domain sources to identify potential vulnerabilities
b) Conduct a methodical vulnerability analysis of the system based on its guidelines, functional specifications, architecture description and source code to identify potential vulnerabilities
c) Conduct a penetration test based on the identified potential vulnerabilities to determine whether the system is resistant to attack by an attacker with a moderate attack potential

Documentation

The examinee shall provide at least:

- Architecture documentation
- Data flows
- Description of used technologies
- Documentation provided for the public scrutiny of the source code and bug bounty

Interviews

None

Findings

Findings made during the examinations are to be reported on the Jira platform provided by the Federal Chancellery as they are discovered. If a finding is of particular importance, it shall be reported immediately by email to the Federal Chancellery.

Reports

The examination reports are to be published and shall be written with this objective in mind. In particular, they should be as comprehensive and easy to understand as possible. One report with a consolidated view among members of a same team shall be provided when working in a group. The reports are also to be written in a way allowing to make references to the statements easily (e.g. identifier per findings or indexing of the paragraphs), in particular, the findings shall be described in the reports with the same wording as on the Jira platform.