Examination of the Swiss Internet voting system

Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Baumer print office

29/11/2022

Work performed for:

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

Contact information

SCRT SA	**Stéphane Adamiste**
Rue du sablon 4	Head of Governance division
1110 Morges	+41 21 802 64 01
Switzerland	stephane.adamiste@scrt.ch

Contributors

Author	Stéphane Adamiste	Head of Governance division
Author	Philippe Oechslin	Consultant, OS Objectif Sécurité SA

Version history

Version Number	**Author**	**Date**	**Version**
0.9	Stéphane Adamiste Philippe Oechslin	22.10.2022	Draft for comments
1.0	Stéphane Adamiste	29.11.2022	Integration of comments by the Federal Chancellery

Management summary

Scope and objective of the examination

The objective of this examination was to assess to which extent the infrastructure operated, and the organisational measures implemented by the Baumer print office (in charge of printing and packaging the polling cards, on behalf of the cantons of Basel-Stadt and Thurgau, in the context of electronic voting) satisfy a subset of requirements (audit scope 3 - *Infrastructure and operation, c) Assess the infrastructure and organisational measures of the print office*) set forth by the Federal Chancellery's ordinance on e-voting. In total, the examination included 45 criteria.

Methodology

The examiners looked for evidence of effort to comply with said criteria by performing interviews of the company's personnel in charge of the setup and operation of the infrastructure used to print and package the polling cards, by analysing the relating documentation (i.e., policies, procedures, specifications, reports, processes, etc.) and by observing the printing and packaging process of sample polling cards transmitted by a canton.

The examination was carried out in two phases. Phase 1 consisted in a pre-audit, that took place in mid-June 2022. Resulting intermediary findings were transmitted to the print office and client canton at the end of August, so that they could make improvements to their existing security measures. Phase 2 was conducted in mid-September.

Results

After phase 2 of the examination, the Baumer print office was able to demonstrate a high level of compliance with the requirements of the ordinance on e-voting, as no finding has been identified.

Recommendations

No recommendation is provided within this report, given the absence of non-conformities.

Authors

SCRT is the owner of the present report. The examination work was conducted conjointly by SCRT (represented by Stéphane Adamiste) and OS Objectif Sécurité (represented by Philippe Oechslin).

Final note

The examiners conclude this summary by thanking the Baumer print office, the cantons of Basel-Stadt and Thurgau 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 [6], as per chapter 26 of the annex of the draft OEV, and for obtaining recommendations for improvements.
6. In May 2022, the Federal Council enacted the partially revised Ordinance on Political Rights (PoRo) [6], which becomes applicable from Jul. 1st 2022. The totally revised Federal Chancellery Ordinance on Electronic Voting (OEV) [7] comes into force on the same date.

7. SCRT was mandated by the Federal Chancellery to assess the compliance of the print offices involved in the printing and packaging of the e-voting material on behalf of the cantons, against the applicable requirements of the OEV. The present report focusses on the examination of the perimeter defined as follows in the audit concept [8]: *Scope 3: Infrastructure and operation, c) Assess the infrastructure and organisational measures of the print office.*

2 Methodology

2.1 Process

8. 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

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

2.3 Findings

10. 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

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

12. Readers should note that the classification of indings 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

13. 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

14. 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

15. 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

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

Cryptographic protocol requirements for complete verifiability (Art. 5)

Key	Requirement
2.9.1.2	**For soundness of the proofs referred to in Number 2.5** The following system participants may be considered trustworthy: » set-up component » print component » one of four control components per group, leaving open which one it is
2.9.3.2	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7** The following system participants may be considered trustworthy: » set-up component » print component » user device » one of four control components per group, leaving open which one it is
2.9.4.2	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.8** The following system participants may be considered trustworthy: » set-up component » print component » user device » one of four control components per group, leaving open which one it is
2.13.3	**Requirements for the definition and description of the cryptographic protocol** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.

Table 1 - E-voting requirements: Cryptographic protocol requirements for complete verifiability (Art. 5)

Trustworthy components in accordance with Number 2 and for their operation

Key	Requirement
3.5	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
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.
3.7	Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.
3.8	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
3.9	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
3.10	Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.
3.11	Trustworthy components may not be connected to the internet when installing or updating software.
3.12	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
3.13	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.
3.14	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two person principle).
3.17	Trustworthy components may perform only the intended operations.

Key	Requirement
3.19	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
3.20	Any access to and use of a trusted component or data carrier containing critical data must be logged.

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

Requirements for print offices

Key	Requirement
7.1	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the print office by two persons, who must both stay with the data carrier until it is delivered.
7.2	The encryption must meet the requirements of eCH standard 0014 , Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the print office via a secure secondary channel.
7.3	The person responsible at the print office who receives the data carrier must sign an acknowledgement of receipt.
7.4	For the data carrier containing the print data, the component on which the critical data is decrypted and all components that process the critical data, the provisions for the print component as set out in Number 3 apply.
7.5	The persons responsible at the print office carry out a material quantity check.
7.6	After printing the polling cards, the print office must destroy the data received.
7.7	If the print office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.
7.8	The channel between the print office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.

Table 3 - E-voting requirements: Requirements for print offices

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

Key	Requirement
14.9	All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.

Table 4 - E-voting requirements: Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

Organisation of information security

Key	Requirement
18.1	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
18.2	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
18.3	The risks in connection with third parties (contractors such as suppliers and service providers) 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 5 - E-voting requirements: Organisation of information security

Management of intangible and tangible resources

Key	Requirement
19.1	All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology - Security techniques - Information security management systems - Requirements , relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.
19.2	The acceptable use of intangible and tangible resources must be defined.
19.3	Classification guidelines for information must be issued and communicated.
19.4	Procedures must be devised for the labelling and handling of information.

Table 6 - E-voting requirements: Management of intangible and tangible 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	Heads of human resources must accept full responsibility for guaranteeing the trustworthiness of human resources.

20.3	All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.

Table 7 - E-voting requirements: Trustworthiness of human resources

Physical and environment security

Key	Requirement
21.1	The security perimeters of the various premises of the infrastructure are clearly defined.
21.2	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
21.3	To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.
21.4	All data must be processed and in particular stored exclusively in Switzerland.

Table 8 - E-voting requirements: Physical and environment security

Management of communication and operations

Key	Requirement
22.1	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
22.2	Appropriate measures must be taken to protect against malware.
22.3	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.
22.4	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
22.5	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.

Table 9 - E-voting requirements: Management of communication and operations

4 Examination results

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

Cryptographic protocol requirements for complete verifiability (Art. 5)

The requirements in sections 2.9 describe which components can be considered trustworthy and which can't. These requirements are taken into account when auditing the requirements in section 3, which relate to trustworthy components.

Key	2.9.1.2
Requirement	**For soundness of the proofs referred to in Number 2.5** The following system participants may be considered trustworthy: » set-up component » print component » one of four control components per group, leaving open which one it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 10 – Examination results: OEV paragraph 2.9.1.2

Key	2.9.2.2
Requirement	**For soundness of the proofs referred to in Number 2.6** The following system participants may be considered trustworthy: » one of four control components per group, leaving open which one it is » one auditor in any group, leaving open which auditor it is » one technical aid from a trustworthy auditor, leaving open which aid it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A

Result	N/A
Finding	N/A
Relevance	N/A

Table 11 – Examination results: OEV paragraph 2.9.2.2

Key	2.9.3.2
Requirement	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7** The following system participants may be considered trustworthy: » set-up component » print component » user device » one of four control components per group, leaving open which one it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 12 – Examination results: OEV paragraph 2.9.3.2

Key	2.13.3
Requirement	**Requirements for the definition and description of the cryptographic protocol** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.
Observation	This requirement is taken into account when auditing requirements about the secure distribution of certificates (See Number 7.1, 7.2).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 13 – Examination results: OEV paragraph 2.1.3.3

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

Key	3.5
Requirement	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
Observation	The voting material is printed by specialised external third parties. They only perform operational tasks required for preparation, packaging and delivery.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94
Result	Pass
Finding	N/A
Relevance	N/A

Table 14 – Examination results: OEV paragraph 3.5

Key	3.6
Requirement	Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.
Observation	The trustworthy components of this print office are the following: » The standalone computer used for enriching the PDF documents of the polling cards (i.e. inclusion of a datamatrix code for traceability purpose); » For the canton of Thurgau: A *Ricoh 8320* laser printer and *Ricoh 9210* laser printer (backup) with a *Fiery* Raster Image Processor (RIP); » For the canton of Basel-Stadt: Two *Truepress Jet520HD* printers with an *Equios* RIP, a *Ricoh 9210* laser printer with a *Fiery* RIP (backup/reprints). According to the documented process: » The update of the standalone computer is performed by appointed Baumer employees in respect of the 4-eye principle and traced in the checklist of the printing process. » The setup, update and configuration of the printers are performed by the suppliers' technical staff under the supervision of an appointed Baumer employee. Changes applied to the printers and their servers are documented in tickets.

Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4.2, 4.3 » Interne Checkliste eVotingBASEL V1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 15 – Examination results: OEV paragraph 3.6

Key	3.7
Requirement	Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.
Observation	According to the documented process, original software and updates are downloaded from the official source and their hash value is verified before they are installed on printers or the standalone computer.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4.2, 4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 16 – Examination results: OEV paragraph 3.7

Key	3.8
Requirement	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
Observation	According to the documented process, the certificate used to sign the PDF files of the polling cards are delivered through the same channel as the files themselves, either on a physical data carrier or from a Web portal. The fingerprint of the certificate is either verified in person or transmitted with a secure messaging application (*Threema*) and verified in an online meeting.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.3
Result	Pass
Finding	N/A

Relevance	N/A

Table 17 – Examination results: OEV paragraph 3.8

Key	3.9
Requirement	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
Observation	According to the documented process, the software of the printing devices is updated following the schedule of the concerned manufacturer. No updates are performed during the period were polling cards are printed. The standalone computer is updated just before the polling cards to be printed in the context of a ballot are received.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4
Result	Pass
Finding	N/A
Relevance	N/A

Table 18 – Examination results: OEV paragraph 3.9

Key	3.10
Requirement	Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.
Observation	All steps of the printing process are carried out by at least two persons. Critical data is deleted at the end of the printing process. The cabling of the smaller printing system (*Ricoh*) is visible and evident. As far as the larger printing system is concerned (*Truepress*), several cables connect the print server and the printer. The cables are labelled, and a colour code is used to ensure that the one that connects to the internal network be easily recognisable. The print components are disconnected from the internal network during the printing process.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3 » Visit of the printing facilities
Result	Pass

Finding	N/A
Relevance	N/A

Table 19 – Examination results: OEV paragraph 3.10

Key	3.11
Requirement	Trustworthy components may not be connected to the internet when installing or updating software.
Observation	The documentation mentions that the e-voting infrastructure components are subject to offline installation and updates, i.e. the systems are not connected to the Internet. For the printing systems, the software is downloaded from the Internet at the print office, copied on an SD card and installed on the devices. For the offline computer, updates are downloaded from the editors of the software and copied on USB sticks.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4.2-4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 20 – Examination results: OEV paragraph 3.11

Key	3.12
Requirement	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
Observation	In the cases were the canton deliver the printing data on a USB stick (canton of Thurgau), that stick is destroyed after use. The data is then stored on a PIN protected stick by the print office. Once the polling cards are printed and delivered the USB stick containing the printing data is securely deleted and overwritten upon instruction by the canton. In the case of the canton of Basel-Stadt, the print engine (*Fiery* RIP) uses a mode that guarantees that no data remains on the printer (secure erase). A white paper documents this mode. The *Truepress* print server runs on a dedicated set of hard disks. The disks are plugged into the server after it has been disconnected from the internal network. Once the print job completed, the data is deleted and the disks are swapped out before the server is reconnected to the network. When not in use, the disks are stored in a safe.

	The disk of the offline computer is completely overwritten after its use with a backup made before the stick containing the printing data was plugged into the computer.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94 » EFI Fiery Security White Paper, Fiery FS350 Pro/FS350 Servers 07.2020 » EFI Fiery Security White Paper, Fiery FS300 Pro/FS300 Servers 10.2017 » Interne Checkliste eVotingBASEL V1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 3.12

Key	3.13
Requirement	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.
Observation	USB sticks are used to transfer the print data from the cantons to the print office, in encrypted form to the standalone PC used to enrich the PDF files, where it is decrypted, and in cleartext form to the print servers. The data carrier used to deliver data to the print office is shredded after it has been connected to the standalone computer. The data carrier used to transfer the enriched data to the print server is securely deleted on the standalone computer once the print job is completed.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.6.13
Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – Examination results: OEV paragraph 3.13

Key	3.14

Requirement	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two person principle).
Observation	There are at least two persons involved in each step of the printing process: » Before printing, one person has access to the encrypted data, and another one to the decryption password; » Once the data has been decrypted, enriched and written to the USB stick, the hard disk of the standalone PC is overwritten with a backup, to remove all traces of decrypted data; » During the printing operations, the person transferring the clear-text data to the print server is accompanied by a second person, until the data carrier is stored in a safe; » At the end of the process all critical data is deleted. The deletion process is carried out in respect of the 4-eye principle.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3 » Visit of the printing facilities.
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 3.14

Key	3.17
Requirement	Trustworthy components may perform only the intended operations.
Observation	During the whole e-voting material printing process, the standalone computer, print servers and printers are exclusively dedicated to the intended operations. The printers are disconnected from the network to ensure that no interference occurs. After the printing process, the printers are used for other printing jobs. The trustworthy components are subject to hardening measures to ensure that only necessary functionalities be available.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3, 4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 24 – Examination results: OEV paragraph 3.17

Key	3.19
Requirement	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
Observation	The procedures for setup, update and operation of the components, as well as for the secure deletion of the data they process are documented in the documentation of the printing process.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4
Result	Pass
Finding	N/A
Relevance	N/A

Table 25 – Examination results: OEV paragraph 3.19

Key	3.20
Requirement	Any access to and use of a trusted component or data carrier containing critical data must be logged.
Observation	Each step of the printing process is signed off on a checklist.
Evidence	Interne Checkliste eVotingBASEL V1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 26 – Examination results: OEV paragraph 3.20

Requirements for print offices

Key	7.1
Requirement	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the print office by two persons, who must both stay with the data carrier until it is delivered.
Observation	The canton of Basel-Stadt transmits the encrypted and signed data via a portal (*SharePoint*), the password for decryption being delivered through a separate channel (*Threema* messaging application).

	Two persons of the canton of Thurgau deliver the printing data by hand to the print office.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 27 – Examination results: OEV paragraph 7.1

Key	7.2
Requirement	The encryption must meet the requirements of eCH standard 0014, Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the print office via a secure secondary channel.
Observation	The eCH standard 0014, § 7.5 lists the recommended cryptographic algorithms to be used by Swiss e-government applications. The cantons encrypt the print data with AES-128 (using the *AxCrypt* tool). The encryption password is transmitted via the secure messaging application *Threema*.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.3 » Benutzeranleitung der Post OG Release 0.15 V03.09.2022, §7.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 28 – Examination results: OEV paragraph 7.2

Key	7.3
Requirement	The person responsible at the print office who receives the data carrier must sign an acknowledgement of receipt.
Observation	Canton Thurgau delivers the print data to Baumer on a physical data carrier. The two persons receiving the data carrier sign a receipt.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 29 – Examination results: OEV paragraph 7.3

Key	7.4
Requirement	For the data carrier containing the print data, the component on which the critical data is decrypted and all components that process the critical data, the provisions for the print component as set out in Number 3 apply.
Observation	The data carrier used to transfer the print data from the standalone computer to the print server is subject to the relevant provisions for a data carrier, set in Number 3 (i.e., 3.6, 3.10, 3.11, 3.12, 3.13, 3.14, 3.17, 3.19, 3.20) The data is decrypted on the standalone computer which is subject to the following relevant provisions: 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.14, 3.17, 3.19, 3.20.
Evidence	» See 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.17, 3.19, 3.20 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94
Result	Pass
Finding	N/A
Relevance	N/A

Table 30 – Examination results: OEV paragraph 7.4

Key	7.5
Requirement	The persons responsible at the print office carry out a material quantity check.
Observation	The printers compare the number of documents specified in the original data with the number of documents printed and put in envelopes. A datamatrix code is inserted into the original PDF files and makes it possible to track any losses at each processing step.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 31 – Examination results: OEV paragraph 7.5

Key	7.6

Requirement	After printing the polling cards, the print office must destroy the data received.
Observation	See 3.12
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3 step 13
Result	Pass
Finding	N/A
Relevance	N/A

Table 32 – Examination results: OEV paragraph 7.6

Key	7.7
Requirement	If the print office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.
Observation	The polling cards are packaged immediately after printing.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3 » Visit of he printing facilities
Result	Pass
Finding	N/A
Relevance	N/A

Table 33 – Examination results: OEV paragraph 7.7

Key	7.8
Requirement	The channel between the print office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.
Observation	The voting papers are picked by the postal service.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 34 – Examination results: OEV paragraph 7.8

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

Key	14.9
Requirement	All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.
Observation	The update process of the systems used at the print office is described in the documentation of the printing process.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4
Result	Pass
Finding	N/A
Relevance	N/A

Table 35 – Examination results: OEV paragraph 14.9

Organisation of information security

Key	18.1
Requirement	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
Observation	The documentation contains a list of people and their roles related to e-voting.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §2
Result	Pass
Finding	N/A
Relevance	N/A

Table 36 – Examination results: OEV paragraph 18.1

Key	18.2

Requirement	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
Observation	The documents describing the configuration of the infrastructure and the access rights is signed both by the canton and the print office. Access control and change management are part of the Baumer ISO 27001 certification's scope, which implies that the allocation of access rights and any modification in the configuration of systems is subject to approval.
Evidence	» SOA 27001 V1.06.2001, §A9, A12.1.2 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 37 – Examination results: OEV paragraph 18.2

Key	18.3
Requirement	The risks in connection with third parties (contractors such as suppliers and service providers) 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.
Observation	Baumer carries out a risk analysis of its suppliers. An extract is provided in the documentation. Information security in supplier relationships is part of the Baumer ISO 27001 certification's scope. This implies that risks identified must be mitigated by suitable contractual agreements.
Evidence	» SOA 27001 V1.06.2001, §A15 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §4.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 38 – Examination results: OEV paragraph 18.3

Management of intangible and tangible resources

Key	19.1

Requirement	All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology - Security techniques - Information security management systems - Requirements , relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.
Observation	Asset inventory is part of the Baumer ISO 27001 certification's scope. Moreover, the operational documentation contains specific chapters that list the human resources and the equipment involved in e-voting.
Evidence	» SOA 27001 V1.06.2001, §A8.1.1, A8.1.2 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §2, 4
Result	Pass
Finding	N/A
Relevance	N/A

Table 39 – Examination results: OEV paragraph 19.1

Key	19.2
Requirement	The acceptable use of intangible and tangible resources must be defined.
Observation	Acceptable use of assets is part of the Baumer ISO 27001 certification's scope and is described in the company's acceptable use policy.
Evidence	» SOA 27001 V1.06.2001, §A8.1.3 » Reglement zum Umgang mit Informatikgeräten und Kanälen V1
Result	Pass
Finding	N/A
Relevance	N/A

Table 40 – Examination results: OEV paragraph 19.2

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.
Observation	Classification of information is part of the Baumer ISO 27001 certification's scope and is mentioned in Baumer's information security policy for employees.

	The print data (i.e. the polling cards) has the *vertraulich* (*confidential*) classification level.
Evidence	» SOA 27001 V1.06.2001, §A8.2.1 » Informationssicherheit Leitlinie Baumer AG V1.3, §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 41 – Examination results: OEV paragraph 19.3

Key	19.4
Requirement	Procedures must be devised for the labelling and handling of information.
Observation	Labelling and handling of information are part of the Baumer ISO 27001 certification's scope and is mentioned in Baumer's information security policy for employees.
Evidence	» SOA 27001 V1.06.2001, §8.2.2 » Informationssicherheit Leitlinie Baumer AG V1.3, §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 42 – Examination results: OEV paragraph 19.4

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.
Observation	Personnel security is part of the Baumer ISO 27001 certification's scope. The company's personnel undergo a security check when hired and every year thereafter.
Evidence	» SOA 27001 V1.06.2001, §A7 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §2
Result	Pass
Finding	N/A

Relevance	N/A

Table 43 – Examination results: OEV paragraph 20.1

Key	20.2
Requirement	Head of human resources managers must accept full responsibility for guaranteeing the trustworthiness of human resources.
Observation	Screening is part of part of the Baumer ISO 27001 certification scope. The General Security Policy of the ISMS states that the company's executive management commits to provide the necessary resources to achieve the goals of the ISMS. The documentation describing the polling cards' printing process includes the list of personnel involved in the related tasks. It is signed by the company's CEO. The examiners consider this distribution of responsibilities to be equivalent to the requirement.
Evidence	» SOA 27001 V1.06.2001, §A6 » Informationssicherheitspolitik Baumer AG V1.5, §1.1 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §5
Result	Pass
Finding	N/A
Relevance	N/A

Table 44 – Examination results: OEV paragraph 20.2

Key	20.3
Requirement	All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.
Observation	Information Security Awareness, Education & Training is part of the Baumer ISO 27001 certification's scope. The information security policy of the ISMS specifies that employees follow an internal training regarding information security and are regularly informed of security threats and associated countermeasures applied in the Baumer environment.
Evidence	» SOA 27001 V1.06.2001, §A7.2.2 » Informationssicherheitspolitik Baumer AG V1.5, §1.3, 3.1
Result	Pass
Finding	N/A

Relevance	N/A

Table 45 – Examination results: OEV paragraph 20.3

Physical and environment security

Key	21.1
Requirement	The security perimeters of the various premises of the infrastructure are clearly defined.
Observation	Physical security perimeter is part of the Baumer ISO 27001 certification's scope and is mentioned in the information security policy of the ISMS. The documentation describing the polling cards' printing process provides details regarding the security measures implemented to protect the premises: video surveillance, intrusion alarm system, access control through individual badges.
Evidence	» SOA 27001 V1.06.2001, §A11.1 » Informationssicherheitspolitik Baumer AG V1.5, §3.1 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 46 – Examination results: OEV paragraph 21.1

Key	21.2
Requirement	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
Observation	Physical security perimeter, physical entry controls and access control are part of the Baumer ISO 27001 certification's scope and is mentioned in the general security policy of the ISMS. Physical access controls to assets used for e-voting are listed in the documentation describing the polling cards' printing process: video surveillance, intrusion alarm system, access control through individual badges.
Evidence	» SOA 27001 V1.06.2001, §A9, A11.1.1, A11.1.2 » Informationssicherheitspolitik Baumer AG V1.5, §3.1 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §2.1
Result	Pass

Finding	N/A
Relevance	N/A

Table 47 – Examination results: OEV paragraph 21.2

Key	21.3
Requirement	To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.
Observation	All domains related to the security of devices (e.g., acceptable use of assets, access control, physical security, operations security, etc.) are part of the Baumer ISO 27001 certification's scope. The devices used in the context of e-voting do not leave Baumer's premises.
Evidence	» SOA 27001 V1.06.2001 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 48 – Examination results: OEV paragraph 21.3

Key	21.4
Requirement	All data must be processed and in particular stored exclusively in Switzerland.
Observation	All processing activities related to e-voting data performed by Baumer occur exclusively in Switzerland. The data is stored on local machines or data carriers sited in Islikon, TG.
Evidence	» Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3 » Visit of the printing facilities
Result	Pass
Finding	N/A
Relevance	N/A

Table 49 – 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.
Observation	The document describing the printing process includes a list of people and their roles related to e-voting. The allocation of roles is done in such a way that there are always two people participating to critical steps of the e-voting operations and that the people in a role have the necessary competence.
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §2
Result	Pass
Finding	N/A
Relevance	N/A

Table 50 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Controls against malware are part of the Baumer ISO 27001 certification's scope and documented in the company's acceptable use of assets policy and general information security policy.
Evidence	» SOA 27001 V1.06.2001, §A12.2 » Reglement zum Umgang mit Informatikgeräten und Kanälen V1, §1.7 » Informationssicherheitspolitik Baumer AG V1.5, §3.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 51 – Examination results: OEV paragraph 22.2

Key	22.3
Requirement	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.

Observation	The documentation details the emergency scenarios considered by Baumer with regards to the information processing facilities related to e-voting. It states that the data needed for printing the voting material can be downloaded or delivered again in case it should be lost. Backup is part of the Baumer ISO 27001 certification scope. The control requires to perform data restore tests on a regular basis to check that backups are functioning correctly.
Evidence	» SOA 27001 V1.06.2001, §A12.3 » Informationssicherheitspolitik Baumer AG V1.5, §3.1 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §5
Result	Pass
Finding	N/A
Relevance	N/A

Table 52 – Examination results: OEV paragraph 22.3

Key	22.4
Requirement	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
Observation	Except the machine used for downloading the encrypted data, all machines used for producing the voting material are in a restricted zone that is not connected to Internet. Communications security part of the Baumer ISO 27001 certification's scope.
Evidence	» SOA 27001 V1.06.2001, §A13.1 » Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 53 – Examination results: OEV paragraph 22.4

Key	22.5
Requirement	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.

Observation	The document describing the printing process of the polling cards details the usage made of removable data carriers at the various steps of the process. At the end of the process, those data carriers are either shredded (USB stick containing the encrypted printing data received from the canton of Thurgau) or securely erased (USB sticks used to transfer the printing data to the print servers).
Evidence	Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 54 – Examination results: OEV paragraph 22.5

5 Summary of findings and recommendations

18. No recommendation is provided in this report, given the absence of non-conformities.

6 References

External references

[1] "Reorienting eVoting and ensuring stable trial operation," *www.egovernment.ch*. https://www.egovernment.ch/en/umsetzung/schwerpunktplan/vote-electronique/ (accessed Oct. 21, 2021).
[2] Swiss Federal Chancellery, Political Rights Section, "Redesign and relaunch of trials - Final report of the Steering Committee Vote électronique (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." 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, "Federal Chancellery ordinance on electronic voting (OEV)." Apr. 28, 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/OEV_draft%20for%20consultation%202021.pdf.download.pdf/OEV_draft%20for%20consultation%202021.pdf
[7] Swiss Post, "UP2021 - Mapping List VEleS.xlsx." Jul. 13, 2021.
[8] Swiss Federal Chancellery (FCh) - Political Rights section, "Audit concept for examining Swiss Internet voting systems - v1.4". April 12, 2022. [Offline].

Documentation received from the print office

[9] Prozessbeschreibung für die Produktion von E-Voting-Stimmrechtsausweisen Baumer V0.94
[10] Informationssicherheitspolitik Baumer AG V1.5
[11] SOA 27001 V1.06.2001
[12] Reglement zum Umgang mit Informatikgeräten und Kanälen V1
[13] Informationssicherheit Leitlinie Baumer AG V1.3
[14] Interne Checkliste eVotingBASEL V1.5
[15] EFI Fiery Security White Paper, Fiery FS350 Pro/FS350 Servers 07.2020

[16] EFI Fiery Security White Paper, Fiery FS300 Pro/FS300 Servers 10.2017