Examination of the Swiss Internet voting system

Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Abraxas 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	17.10.2022	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 Abraxas print office (in charge of printing and packaging the polling cards, on behalf of the cantons of Basel-Stadt and St. Gallen, 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 Abraxas 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 Abraxas print office, the cantons of Basel-Stadt and St. Gallen 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 regarding e-voting. In April 2021, the Federal Council opened a consultation procedure for the redesign of the e-voting trials. The redesign includes both a partial revision of the Ordinance on Political Rights (PoRo) [3] and a complete revision of the Federal Chancellery Ordinance on Electronic Voting (“VEleS”, or “OEV”) [4]. The OEV specifies, among others, the requirements for authorising electronic voting, including the technical and administrative controls for approving an e-voting system.
5. The Federal Chancellery issued an audit concept for the examination of Swiss internet voting systems [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. 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 partial 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 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

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)

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 (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 the operational tasks required for the preparation, packaging and delivery.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92
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: » A dedicated physical e-voting server ("*E-Voting-Server*") hosting: ○ a virtual machine running the *Domtrac* software for enriching the polling cards (i.e., inclusion of a datamatrix code for traceability purpose); ○ a virtual *Prisma* server for driving the printer; » A *Canon Colorstream 3500z* printer. According to the documented process, setup up, updates and configurations of trustworthy equipment is performed by two employees of Abraxas or, if necessary, by a technician of the supplier, under the supervision of an Abraxas employee. The equipment is not connected to the Internet. Changes are documented and approved by Abraxas' Change Advisory Board.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §3.3 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §3.3
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, all software is downloaded from the supplier's official source and the integrity is verified with a hash or other control information. The control information is documented in the change report.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §3.3 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §3.3
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 is delivered through the same channel as the files themselves (i.e., a web portal. The fingerprint of the certificate is either verified in person or transmitted using a secure messaging application (*Threema*) and then verified in an online meeting.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.2 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.2
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 documentation, updates are planned before each printing period.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §3.3 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §3.3
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. Several cables connect the *Prisma* print server to the *Canon Colorstream 3500z* printer. The cables are labelled, which allows to understand their function and track their connection status. During the printing process the network cable of the print server is disconnected and the *Domtrac* server is connected to the print server instead.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5 » 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	According to the documentation, the systems are not connected to the internet when installing or updating software. Patches are installed using USB sticks.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §3 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §3
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	The USB stick containing the encrypted critical data (i.e., the polling cards) is stored encrypted in a safe following the 4-eye principle. Secure deletion occurs upon written instruction of the cantons, once they have accepted the printed material. The disks containing the images of the Output Management System (*Domtrac*) and the print server (*Prisma*) are stored in a safe and only inserted into the printing rack when the network connection is removed.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92 » Visit of the printing facilities
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 only used to transfer data in one direction, from the canton to the print office. The encrypted data is copied to the production server. The stick is removed before the data is decrypted. Data on the stick is erased with a specific tool once the printing process is completed.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5 Step 3 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5 Step 3
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	At least two persons are involved in each step of the printing process: » One person holds the encrypted data, and another one has the decryption password or the smartcard containing the decryption key. » The password used to access the Output Management System (OMS) server is split in two halves, held by two different persons. At the end of the process all critical data is deleted.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92 » 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	The printing of the polling cards is performed using a dedicated physical server that hosts only the pieces of software necessary to perform the

	printing operations. The server is disconnected from the corporate network during the printing process.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5
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 secure deletion are detailed in the documentation of the printing process.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92
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	» E-Voting BS _ Checkliste D+V_0.9.1 » E-Voting SG _ Checkliste D+V_0.9.1
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 encrypted and signed data is transmitted through a portal (SharePoint for the canton of Basel-Stadt, SG Connect for the canton of St Gallen). In Basel-Stadt, the password for decryption is transmitted via the secure messaging application *Threema*. In St Gallen, the data is encrypted using a PKI and can be decrypted with the private key stored on a smartcard at the print office.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.2 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.2
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 canton of Basel-Stadt encrypts the print data with AES-128 (using the *AxCrypt* tool). The encryption password is transmitted via the secure messaging application *Threema*. The canton of St Gallen uses an asymmetric algorithm (RSASSA-PSS algorithm with SHA-256 hash and 3072-bit key length) to encrypt the print data and therefore does not need to transmit any password.
Evidence	» Benutzerhandbuch VOTING Stimmunterlagen Offline-Client, § 3.8 » 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	Abraxas does not receive the data on a data carrier.
Evidence	N/A
Result	N/A
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 is decrypted with the offline E-Voting-Server, which is the print component of this print office, and therefore subject to the provisions set out in Number 3. All the components involved in e-voting are subject to the same provisions.
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 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.2 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.2
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 envelope. A datamatrix code inserted into the original PDF files makes it possible to track any potential loss at each processing step.

Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5.11, 2.11 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5.11, 2.11
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	The print data is kept encrypted in a safe (see §3.12) until the cantons provide a written confirmation that it may be destroyed. This occurs once the printed material has been delivered and accepted by the cantons.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5 11) » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5 11) » Visit of the printing facilities.
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	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5.10, 2.8 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5.10, 2.8
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	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5.10, 2.8 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5.10, 2.9 » Visit of the printing facilities
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	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92
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 of the printing process includes the list of people involved in e-voting as well as their role.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.12 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.11
Result	Pass
Finding	N/A
Relevance	N/A

T 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. Access control and change management are part of the Abraxas 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.
Observation	The document detailing the configuration of the infrastructure and the access rights is signed both by the canton and the print office.
Evidence	» SOA Abraxas V2.28, §4 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92
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	Abraxas carries out a risk analysis of its suppliers involved in e-voting (i.e. *Canon*, *Docucom*). An extract is provided in the documentation. Information security in supplier relationships is part of the Abraxas ISO 27001 certification's scope. This implies that risks identified must be mitigated by suitable contractual agreements.
Evidence	» SOA Abraxas V2.28, §4 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §3.1, Annex » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §3.1, Annex
	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	Inventory of assets is part of the Abraxas 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	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5, 2.12 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5, 2.11 » eVoting-Komponenten Owner v1.0 » SOA Abraxas V2.28, §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	Abraxas' security policy describes the acceptable use of information and resources. Acceptable use of assets is part of the Abraxas ISO 27001 certification's scope.
Evidence	» Policy Informationssicherheit v6.8, §5, 6, 7 » SOA Abraxas V2.28, §4
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 Abraxas ISO 27001 certification scope. Abraxas maintains a specific policy on this topic. The print data (i.e. the polling cards) has the *strictly confidential* classification level.
Evidence	» Policy Klassifizierung von Informationen v6.3 » SOA Abraxas V2.28, §4
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 Abraxas ISO 27001 certification scope. The classification policy also specifies how to label and handle information.

Evidence	» Policy Klassifizierung von Informationen v6.3 » SOA Abraxas V2.28, §4
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 Abraxas ISO 27001 certification scope. The company's personnel undergo a security check when hired and every two years thereafter.
Evidence	» Policy Informationssicherheit v6.8, §4 » Policy Personen-Sicherheitsprüfung (PSP) v4.1 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.12 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.11 » SOA Abraxas V2.28, §4
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 the Abraxas ISO 27001 certification scope. A specific policy on background checks describes how the human resources carry out regular background checks to assert the trustworthiness of human resources.
Evidence	» SOA Abraxas V2.28, §4 » Policy Personen-Sicherheitsprüfung (PSP) v4.1

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 are part of the Abraxas ISO 27001 certification's scope. The company relies on an online training system to regularly educate human resources about information security.
Evidence	» SOA Abraxas V2.28, §4 » Demonstration of the e-learning platform
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 Abraxas ISO 27001 certification scope. The perimeter for the printing and packaging activities is considered as a protected zone, subject to reinforced security controls.
Evidence	» SOA Abraxas V2.28, §4 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.1 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.1
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 is part of the Abraxas ISO 27001 certification scope. The security controls applying to the perimeter dedicated to the printing and packaging activities are described in the documentation.
Evidence	» SOA Abraxas V2.28, §4 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.1 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §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 Abraxas ISO 27001 certification scope. The devices used in the context of e-voting do not leave Abraxas' premises. The acceptable use of devices is specified in the security policy.
Evidence	» SOA Abraxas V2.28, §4 » Policy Informationssicherheit v6.8, §6, 7
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 Abraxas occur exclusively in Switzerland. The data is stored on local machines or data carriers sited in St. Gallen-Winkeln, SG.

Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92 » 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 documentation includes the list of people involved in e-voting operations as well as their role. 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	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.12 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.11 » eVoting-Komponenten Owner v1.0
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 Abraxas ISO 27001 certification scope. The security policy also mentions that Abraxas provides an infrastructure that protects against malware.
Evidence	» SOA Abraxas V2.28, §4 » Policy Informationssicherheit v6.8, §7.6.1

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 Abraxas with regards to the information processing facilities related to e-voting. It states that the printing data is stored on the cantons' servers and can be retrieved from those servers in case of loss or disruption. The documentation also declares that the customer is responsible for the backup of e-voting data. Backup is part of the Abraxas 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 Abraxas V2.28, §4 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §4.1.1 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §4.1.1
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, none of the machines used for producing the voting material is connected to Internet. The zone plan describes how the different network zones are interconnected and isolated with firewalls. Communications security part of the Abraxas ISO 27001 certification scope.
Evidence	» SOA Abraxas V2.28, §4 » Netzwerk-Layout ABX Druckerstrasse SG-WKL v1.0

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 removable data carriers are explicitly mentioned in the documents describing the printing process. At the end of the process, they are either shredded or securely erased.
Evidence	» Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92, §2.5.12 » Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92, §2.5.12
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 Federal Chancellery, "Federal Chancellery Ordinance on Electronic Voting (OEV)". (accessed: Jun. 11, 2022). [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/OEV.pdf.download.pdf/OEV.pdf

[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] Ablaufbeschreibung Druck und Verpackung E-Voting Kanton BS V0.92

[10] Ablaufbeschreibung Druck und Verpackung E-Voting Kanton SG V0.92

[11] Policy Informationssicherheit v6.8

[12] SOA Abraxas V2.28

[13] Policy Personen-Sicherheitsprüfung (PSP) v4.1

[14] Policy Klassifizierung von Informationen v6.3
[15] eVoting-Komponenten Owner v1.0
[16] Benutzeranleitung der Post OG Release 0.15 V03.09.2022
[17] Benutzerhandbuch VOTING Stimmunterlagen Offline-Client
[18] Netzwerk-Layout ABX Druckerstrasse SG-WKL v1.0