SWISS CYBER STORM 2026

Auditing the Swiss E-Voting System

Lessons Learned from the Field

Stéphane Adamiste | Principal Consultant, Soluss SA

ABOUT THIS TALK

Three parts

1. (Quick) history of e-voting in Switzerland
2. What my work as an auditor consists of
3. Deep dive into specific threat scenarios

PART 1 OF 3

Three parts

1 **(Quick) history of e-voting in Switzerland**

2 What my work as an auditor consists of

3 Deep dive into specific threat scenarios

Public - Soluss

2004–2019

Three systems, and the cantons that used them

Geneva (CHVote)

Developed, hosted and managed by the canton

2004 first binding trial (Anières)

Nov 2018 development stopped, on cost grounds

19 May 2019 last ballot

Geneva 2004–2019 · **Basel-Stadt** 2009–2017 · **Lucerne** in use 2015 · **Bern** in use 2018 · **Vaud** 2018–2019 · **Aargau, St. Gallen** in use 2018, ex-consortium

Zurich (consortium)

Unisys platform, shared by a consortium of cantons (2009–2015), led by Aargau from 2011

2005 first Zurich trials

2011 Zurich pauses; Aargau leads the consortium

12 Aug 2015 authorisation refused for 9 cantons: ballot-secrecy flaw

Zurich from 2005, paused 2011–2015 · **Consortium refused in 2015:** Zurich, Aargau, Fribourg, Glarus, Graubünden, Schaffhausen, Solothurn, St. Gallen, Thurgau

Neuchâtel, then Swiss Post

Scytl technology; Swiss Post as exclusive Swiss distributor from 2015

2005 first Neuchâtel trials

Sep 2015 Swiss Post/Scytl partnership

29 Mar 2019 withdrawn after flaws

Neuchâtel 2005–2019 · **Fribourg** from Nov 2016, ex-consortium · **Basel-Stadt** from Mar 2018 · **Thurgau** from Sep 2018, ex-consortium

Sources: Serdült et al. 2015 (ZDA/UZH); 20 minutes, 12.08.2015; PRWeb, 01.09.2015; swissinfo.ch, 27.11.2016 and 03.02.2017; Canton of Thurgau, 20.06.2018 and 03.03.2023; ICTjournal, 28.11.2018; bk.admin.ch "Contexte".

2022

A stricter ordinance enters into force

- Total revision of the Federal Chancellery's Ordinance on Electronic Voting (OEV) + partial revision of Federal Council's Ordinance on Political Rights (PoRO), in force 1 July 2022
- Complete verifiability now mandatory (individual + universal)
- Most examinations now commissioned by the FCh (previously: certification by accredited bodies, commissioned by the cantons or the system operator)
- Mandatory bug bounty programme (Art. 13 OEV)
- Mandatory publication of source code, documentation, reports (Art. 10–12)

> *Disclosure of the source code and a subsequent independent evaluation revealed significant security flaws that had not been detected by the previous evaluations and certifications.*
>
> Explanatory Report, on why examination responsibility shifted to the Confederation

Substance delivered by a 23-member Expert Dialog (2020): academic and industry experts, moderated by Christian Folini.

60-question survey (Feb. 2020) + moderated written dialogue (May–Jul. 2020, 700+ statements); its recommendations were carried into the catalogue of measures adopted 30 Nov. 2020.

Source: Explanatory Report §2 and §4.2.1; OEV Art. 5, 10–13. The quoted causal claim is the report's own statement.

AUDIT PERIMETER

The federal examination programme: four scopes

Scope	Subject
1	Cryptographic protocol
2	System software
3	**Security of infrastructure and operation, in four parts: (a) ISO 27001 certificate check, (b) Swiss Post as system provider, (c) each canton, (d) the printing offices**
4	Intrusion testing

This talk sits in Scope 3.

Source: OEV Art. 10 / Annex No. 26; FCh Audit concept v1.6 (7 Feb 2025), Scope 3 a–d; FCh "Examination of systems" page.

PART 2 OF 3

Three parts

1 (Quick) history of e-voting in Switzerland

2 What my work as an auditor consists of

3 Deep dive into specific threat scenarios

THE AUDITOR'S WORK

21 Scope 3 examinations since 2022

Swiss Post, the cantons and the printing offices: the Scope 3 assignment held by SCRT, then Orange Cyberdefense, since 2022.

SWISS POST · 6 REPORTS

26 Mar 2022 · Full audit
First examination

28 Nov 2022 · Follow-up audit
Round 2

16 Jun 2023 · Follow-up + delta audit
Round 3; infra changes + 3 criteria added by the FCh; v2.0 on 3 Nov 2023

19 Aug 2024 · Delta audit
Infrastructure change (admin jumphosts)

16 Dec 2025 · Full audit
Full re-evaluation

CANTONS · 10 REPORTS · 7 CANTONS

17 Feb 2023 · Full audit
Basel-Stadt · St. Gallen · Thurgau

3 Nov 2023 · Full audit (new canton)
Graubünden

12 Jul 2024 · Full audit (new release R1.4)
Basel-Stadt · Graubünden · St. Gallen · Thurgau

23 May 2025 · Full audit
Full re-evaluation: Basel-Stadt · Graubünden · St. Gallen · Thurgau

18 Sep 2025 · Full audit (new canton)
Geneva

9 Jan 2026 · Delta audit (new release R1.5)
Basel-Stadt · Graubünden · St. Gallen · Thurgau

6 Feb 2026 · Full audit (new canton)
Lucerne

20 Apr 2026 · Delta audit (organisational change)
Basel-Stadt

1 May 2026 · Full audit (new canton)
Neuchâtel

4 Aug 2026 · Update (following the Basel-Stadt incident)
Neuchâtel

PRINTING OFFICES · 5 REPORTS · 3 ENTITIES

29 Nov 2022 · Full audit
First examination: Abraxas

29 Nov 2022 · Full audit
First examination: Baumer

23 May 2025 · Full audit
Full re-evaluation: Abraxas

23 May 2025 · Full audit
Full re-evaluation: Baumer

18 Sep 2025 · Full audit (new entity)
First examination: Imprimerie Perfect

Sources: FCh "Examination of systems" page (16 published reports); the speaker's engagement records for the 5 reports not yet published (Geneva and Imprimerie Perfect, Sep 2025; Neuchâtel, May and Aug 2026; Basel-Stadt, Apr 2026).

THE AUDITOR'S WORK

The audit domains, in the ordinance's own words

Domain	Ref.	N°
Cryptographic protocol requirements	§2	**13**
Trustworthy components & their operation	§3	**14**
Information and instructions	§8	**1**
Tallying votes in the electronic ballot box	§11	**2**
Confidential data	§12	**3**
Threats	§13	**2***
Security events & incident handling	§14	**9**
Cryptographic measures & key management	§15	**4**
Secure electronic & physical exchange	§16	**2**

Domain	Ref.	N°
Organisation of information security	§18	**3**
Management of resources	§19	**4**
Trustworthiness of human resources	§20	**3**
Physical and environment security	§21	**4**
Communication and operations mgmt.	§22	**5**
Access allocation & administration	§23	**5**
Development & maintenance of systems	§24	**12**
Operation	§25	**3**

** "Threats" spans 39 individual items (13.2–13.40) behind 2 named rows (see next slide).*

THE AUDITOR'S WORK

How many requirements, exactly?

124

System provider

Swiss Post (3b)
16.12.2025 report

172

Cantons

Current criteria list (3c)
06.02.2026 LU report, recounted

45

Printing offices

Scope 3d
23.05.2025 reports

Sources: Scope 3 final reports, Orange Cyberdefense: Swiss Post 16.12.2025; printing offices 23.05.2025; cantons, LU 06.02.2026 (criteria list recounted). Dossier §2.2b, §2.2c.

THE AUDITOR'S WORK

The evidence wall: one Swiss Post audit, 2025

124
criteria assessed

≈ 200
evidence citations

66
distinct documents

3
languages: EN, DE, FR

PUBLIC SPECIFICATIONS AND PROOFS (17)

- Protocol of the Swiss Post Voting System - Computational Proof of Complete Verifiability and Privacy v1.4.0
- Cryptographic Primitives of the Swiss Post Voting System - Pseudocode Specification
- Swiss Post Voting System - System Specification
- Swiss Post Voting System Architecture Document
- Swiss Post Voting System v1.5.0 - Software Architecture Document
- Infrastructure Whitepaper of the Swiss Post Voting System
- Security Whitepaper of the Swiss Post Voting System
- Secure Software Development Process of the Swiss Post Voting System
- Trusted Build and Trusted Deployment of the Swiss Post Voting System
- Trusted build protocols (R1.4.5.1)
- Technical Specifications of the Main Components of the E-Voting System
- Instructions on how to verify the HTML and JavaScript files of the e-voting portal
- Bug bounty programme
- Swiss Post e-voting community programme
- List of opened issues (GitLab)
- E-voting demo website
- Security advices

E-VOTING OPERATING CONCEPTS (20)

- E-Voting - Organizational concept
- E-Voting - Monitoring concept
- E-Voting - Release Management & Installation Concept
- E-Voting - Change and Maintenance Concept
- E-Voting - Zugriffskonzept Kontrollkomponenten
- E-Voting - Security Elements Control Components
- E-Voting - Security Elements Access Layer
- E-Voting - Emergency Concept
- E-Voting - Data Backup Concept
- E-Voting - Disaster Recovery Concept
- E-Voting Incident Management Concept (EVIMC)
- E-Voting - Schlüssel- und Zertifikatsmanagement Konzept
- E-Voting - Konzept zur Datenvernichtung
- E-Voting - Training concepts
- E-Voting - Threat modeling
- Physical Access Data Center E-Voting Infrastructure concept v26
- ISDS Konzept, ISDS DS E-Voting
- Konzept Information Security Awareness v04.01
- Concept de remédiation à la non-conformité d'accès aux composants de contrôle
- E-Voting collaboration platform - Benutzeranleitung Release 1.5

CORPORATE POLICIES AND HANDBOOKS (20)

- Handbuch Risikomanagement DS v04.01
- Handbuch Supplier Security Management v01.05
- Handbuch Identity and Access Management v02.00
- Change Management - Richtlinie
- Configuration Management - Leitlinien
- Vulnerability treatment - Schwachstellenanalyse durchführen v01.08
- Architecture & Technology - HB Kryptographie
- IT20 Workspace - Network Security Architecture
- HB Sicherheitszonen - Die Schweizerische Post AG v01.00
- Handbuch Zutrittsregelung PostFinance v04.00
- Anhang 1 zu HB Zutrittsregelung: Betriebsstandorte PostFinance AG
- Arbeitsanleitung Zutrittsverhalten Rechenzentren PostFinance AG
- KLA-Weisung Zutrittsmanagement «Die Schweizerische Post AG» v02.00
- Verbindliches Handbuch - Sicherheitsprüfungen von Mitarbeitenden
- Manuel - Contrôle de sécurité du personnel V02.00
- Sécurité de l'information à la place de travail : directive
- Classification of Information Factsheet
- Übersicht Decommissioning von Hardware / Datenträgern
- NDA Vorlage
- Dienstleistungsrahmenvertrag - Anhang A: Servicebeschreibung

OPERATIONAL RECORDS (9)

- ISO 27001:2022 Statement of Applicability (Dec. 2024)
- POST.DS6_Risikenauszug.Kantone
- E-Voting team - Mitarbeiterliste
- Direct Trust Zeremonie - R1.4
- Direct Trust Zeremonie - R1.5
- D4 - Löschung der Daten - R1.4
- Debriefing - UG - 2025-02-09
- Trusted Deployment Acceptance Protocol - July 2025
- E-Voting collaboration platform (wiki)

From a computational proof of the voting protocol to the door-access rules of a data centre, all in one audit.

Source: Scope 3 (Post) Final Report, Orange Cyberdefense, 16.12.2025, "Evidence" fields of the 84 result tables. Document count and grouping by the author; variants of the same title merged.

AUDIT RESULTS

What the Scope 3 reports record, 2022 to 2026

Results marked Partially fail (PF) or Fail (F), per report

SWISS POST (3b)

Report	Round	PF	F
26.03.2022	Full audit, against the draft OEV	**12**	**13**
28.11.2022	Round 2, open points only	**1**	**4**
16.06.2023	Round 3, changes, added criteria	**2**	**1**
03.11.2023	Round 3, version 2.0	**1**	**1**
19.08.2024	Delta audit, admin jumphosts	**8**	0
16.12.2025	Full re-evaluation	**2**	**1**

Open in December 2025, described by the report as resulting "from a strict, literal interpretation of the ordinance":

15.4 certificates of the direct trust model not issued by an ESigA-recognised supplier

21.4 source code and documentation hosted on GitLab in the USA

24.2.1 operating manual without a role/function matrix

CANTONS (3c), FULL AUDITS

Report	PF	F
17.02.2023 BS, SG, TG	**1**	**2**
03.11.2023 GR	**1**	**2**
12.07.2024 BS, GR, SG, TG	**1**	**1**
23.05.2025 BS, GR, SG, TG	**1**	**1**
06.02.2026 LU	**2**	0

Recurring:

Art. 11 source code of the polling-card software and helper scripts not published: F to 2025, PF in LU 2026 (helper scripts only)

15.4 certificates: PF in every report

11.1 tallying before Polling Sunday: F in 2023, Pass from 2024 under a derogation

PRINT OFFICES (3d)

Reports	PF	F
2022 (2)	0	0
2025 (2)	**1**	0

7.7 one office: polling cards not systematically packaged immediately after printing (2025)

Sources: Scope 3 final reports, SCRT / Orange Cyberdefense, published on the FCh "Examination of systems" page. Counts are result tables marked Partially fail or Fail. Canton delta audit of 9 Jan 2026 not shown.

SWISS POST AUDIT FINDING EXAMPLE (2025)

Control components: two rules, on paper and on site

	MARCH 2022 Full audit, documents and interviews	NOVEMBER 2022 Round 2, open points	17 SEPTEMBER 2025 On-site visit, one datacentre room	DECEMBER 2025 Final report
3.14 **Two-person rule** No access to trustworthy components without another person becoming aware of it.	**Pass** "Only the infrastructure team is allowed to access the components physically, based on a formal change request and while being accompanied."	*Not re-examined: round 2 covered the open points only.*	**Non-conformity** "The four-eyes principle had not been applied during the last physical interventions on the control components, as only one name appeared in the corresponding logs."	**Pass** Since 7 October 2025, physical interventions under supervision; staff do not know the codes of the safes holding the rack keys.
3.15 **Segregation between control components** A person with access to one control component may not have access to another.	**Partially fail** "The Post's datacentre service team has the keys for all control components' racks."	**Pass** Rack keys moved to the vault teams, who cannot enter the server rooms.	**Non-conformity** "All six members had access to all four control components."	**Pass** Each control component in its own rack with its own lock; keys in separate safes (implementation report, 2 Dec 2025).

Sources: Scope 3 (Swiss Post) final reports, SCRT 26.03.2022 and 28.11.2022, Orange Cyberdefense 16.12.2025; OEV Annex 3.14 and 3.15 (3.13 and 3.14 in the draft of 28 April 2021).

PART 3 OF 3

Three parts

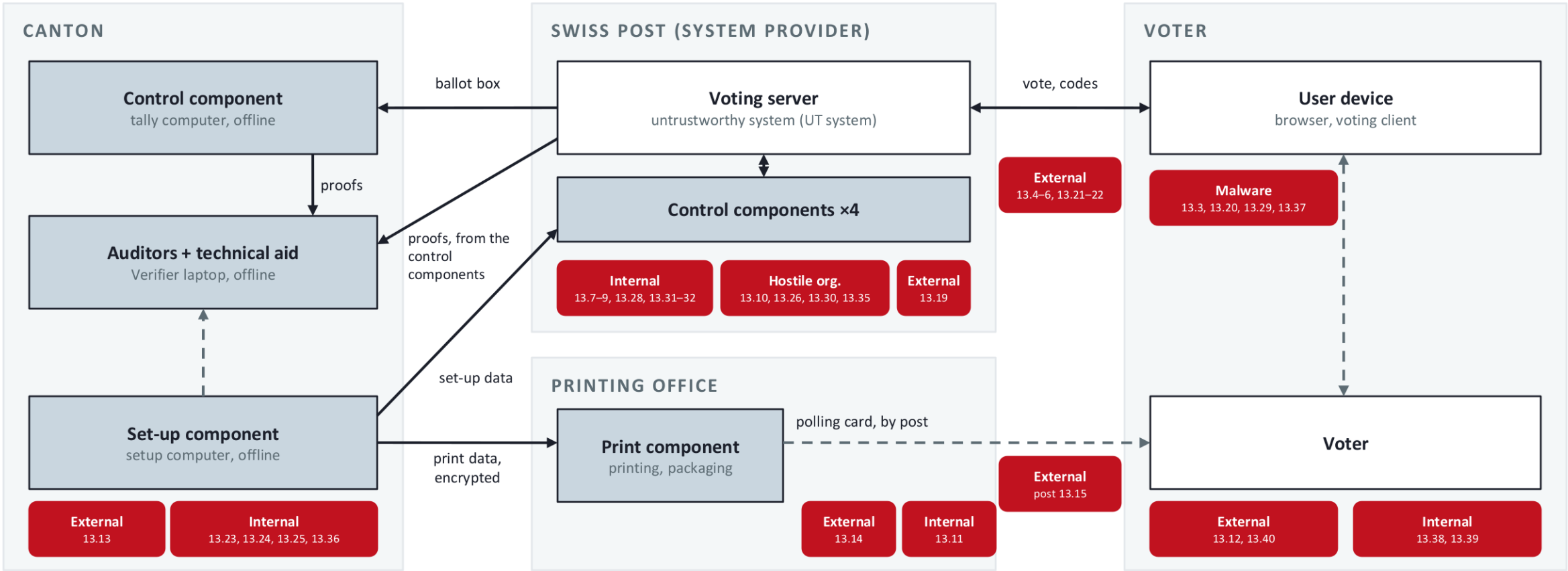
1 (Quick) history of e-voting in Switzerland

2 What my work as an auditor consists of

3 Deep dive into specific threat scenarios

EVIDENCE AND POSITION

Data flows, actors and threat agents in the OEV model

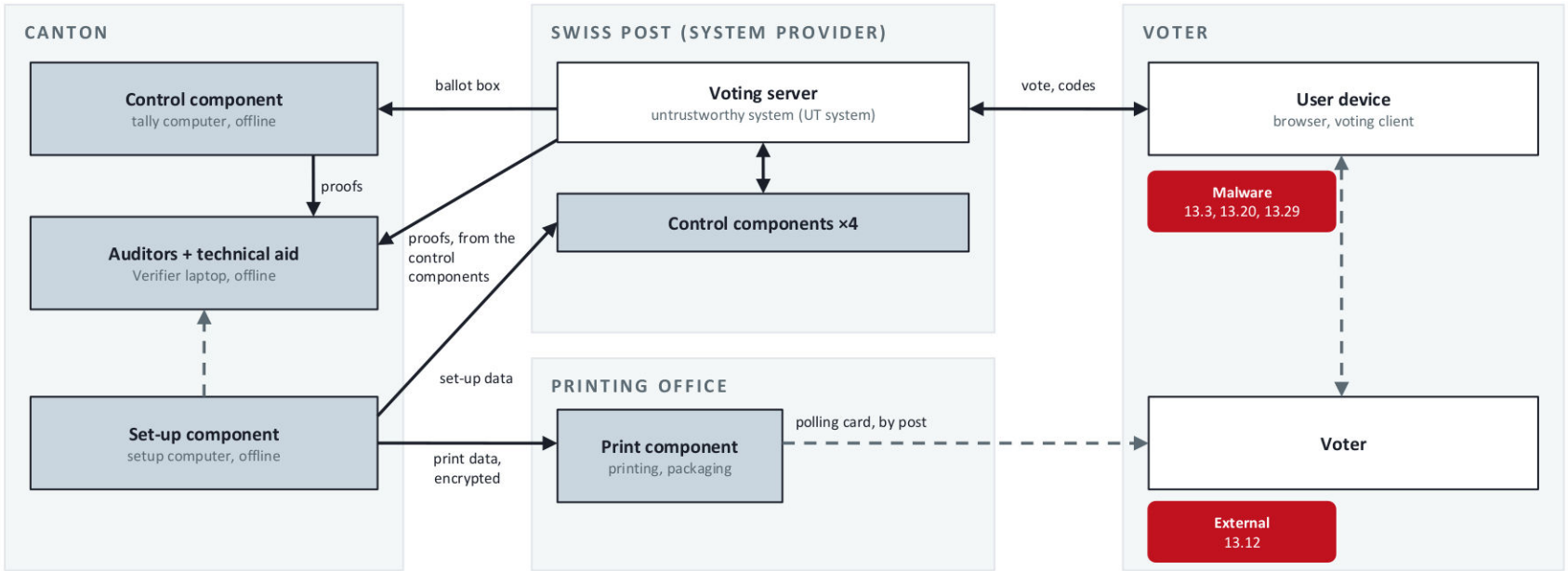


Outside the protocol's attacker model: the trusted components and channels above, and vote secrecy against an attacker who controls the voter or the device (2.7.1).

Sources: OEV Annex 1.4–1.6, 2.1–2.10, 3.1, 7.1, 13 (SR 161.116, in force since 1 Jul 2022); FCh Scope 3 (Cantons) report, 23.05.2025, results for 3.1, 3.4, 3.5, 3.15, 7.1, 16.1.

THREATS IN FOCUS · 1 OF 4

The voter's device: malware and social engineering



WHAT TEXTS, REPORTS AND EXPERTS SAY

- A. Appel (Princeton, 2023): like any internet voting system, it has inherent vulnerabilities; malware on thousands of computers can change votes in transit. B. Schneier: "Online voting is insecure, period."
- On top of this, A. Kuster (2023): verification instructions online only, not on paper, so malware can show a fake procedure. Swiss Post: "falls outside the threat model of individual verifiability".
- Cantons' risk portfolio: P10-R06 (13.12), P10-R13 (13.29): "Gering", accepted. A massive attack can be detected if a small share of voters fully check their codes.

MY OPINION

- Individual verifiability: with the codes on their paper card, voters can check that their vote was registered as entered.
- Voters receive security advice, including in the voting material sent by post.
- Isn't it the voter's responsibility to ensure that their device is not compromised ?

THREATS IN FOCUS (OEV ANNEX 13)

13.3 Malware changes the vote on the user device.

13.12 An external attacker uses social engineering techniques to distract the person voting from following the security measures (individual verifiability).

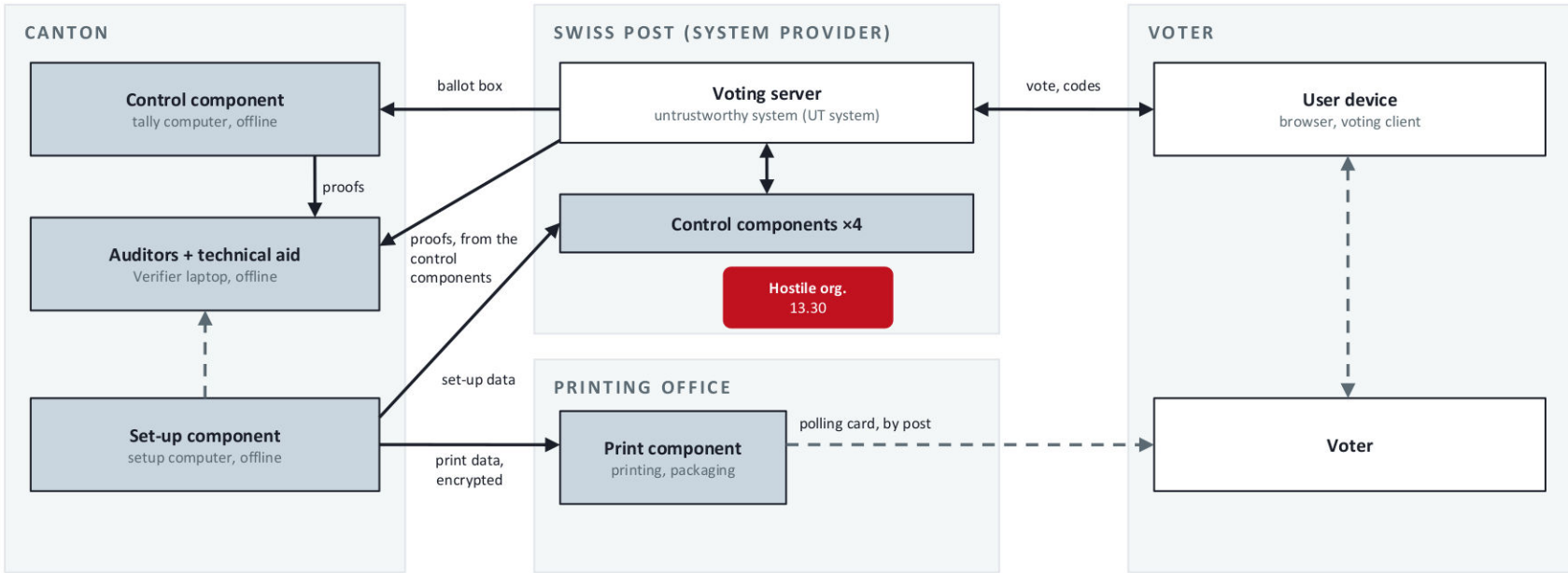
13.20 Malware on the user device sends the vote to a hostile organisation.

13.29 Malware on the user device makes voting impossible.

Sources: OEV (SR 161.116), Art. 5, Annex 2.5, 2.7.1, 13; A. Appel, CITP blog, 06.10.2023; A. Kuster, disclosure write-up, 2023; Schneier on Security, 17.10.2023; cantons BS, GR, LU, SG, TG, E-Voting Risikoportfolio, 30.01.2026.

THREATS IN FOCUS · 2 OF 4

Denial of service on the voting server



WHAT TEXTS, REPORTS AND EXPERTS SAY

- ETH Zurich design review (Scope 4, 2022): "Most of the network-level vulnerabilities that we discuss result in a denial-of-service"; 5 Gbps links shared with other Swiss Post services.
- PIT 2026, high finding: caches created before authentication could impair the voting server's availability; fixed. FCh risk assessment 2026-3: outage by a well-resourced attacker (R8), residual probability "Hoch", under observation.
- Cantons' risk portfolio, GEN-R02 (Swiss Post infrastructure unavailable, incl. 13.30): probability raised to "Mittel" after the DDoS wave of June 2023; accepted. Measures cited: multi-level anti-DDoS set-up, 24/7 team, coordination with the Federal Office for Cybersecurity, geo-blocking.

MY OPINION

- DDoS is a scenario covered by the cantons' emergency plans.
- Fallback: voters switch to the conventional channels, by post or at the polling station.
- Saturating the server for several days is hard to sustain for an attacker.

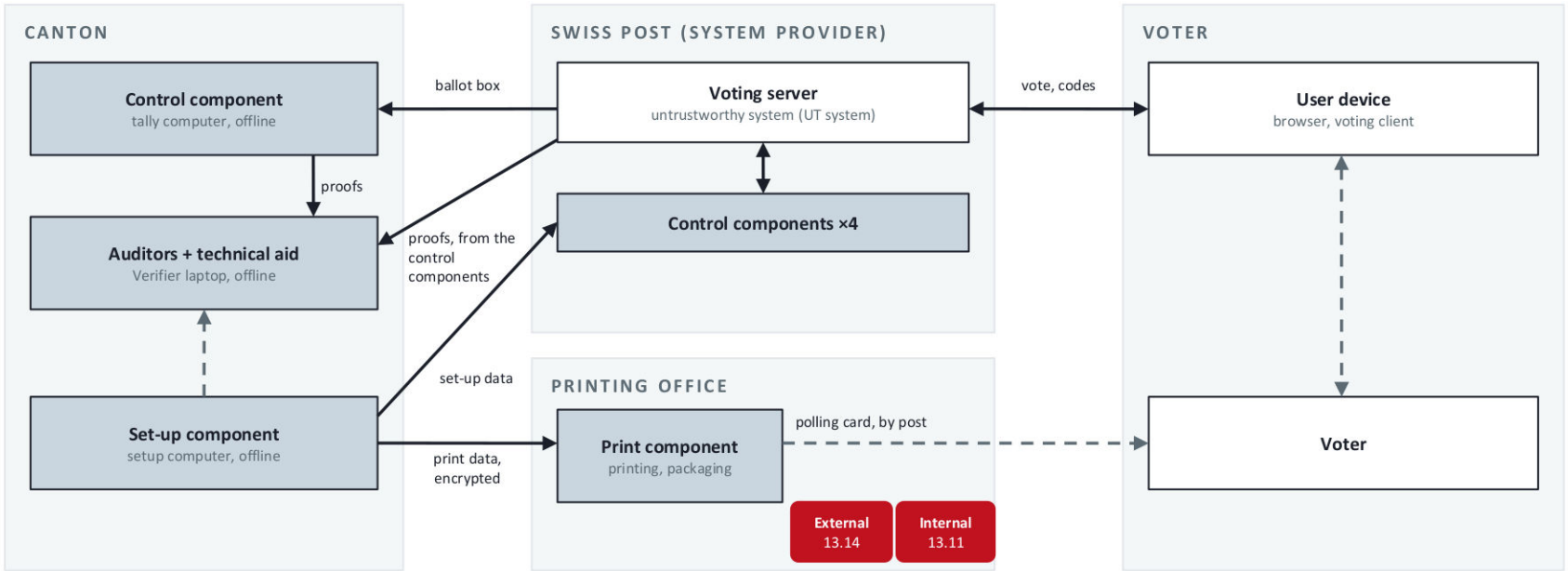
THREATS IN FOCUS (OEV ANNEX 13)

13.30 A hostile organisation carries out a denial-of-service (DoS) attack.

Sources: OEV (SR 161.116), Annex 13.30; Scope 4 reports 2022 to 2026; Swiss Post blog, 28.08.2026; FCh risk assessment 2026-3; cantons BS, GR, LU, SG, TG, E-Voting Risikoportfolio, 30.01.2026.

THREATS IN FOCUS · 3 OF 4

The printing office: Weakest link in the chain?



WHAT TEXTS, REPORTS AND EXPERTS SAY

- Cantons' risk portfolio: P09-R01 (voting cards disclosed at the printing office) and P08-R01 (codes disclosed, incl. 13.11): level "Signifikant", to be monitored; such an attack may be detected "only after the vote, or not at all".
- A. Appel (Princeton, 2022), quoting B. Ford: "if the printing contractor is corrupt, that prints the paper and mails it, then the system is insecure."

MY OPINION

- Small organisations = more vulnerable ?
- Strong culture of physical security.
- Dependence on the suppliers of printing equipment.

THREATS IN FOCUS (OEV ANNEX 13)

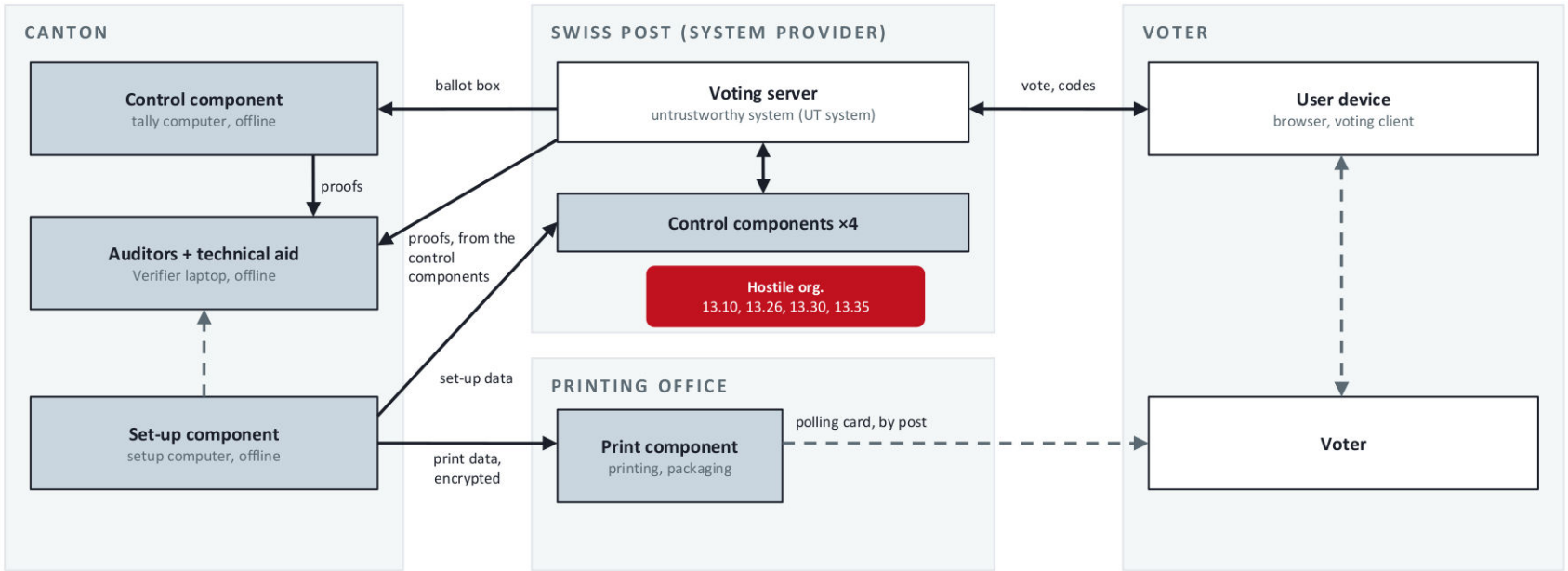
13.11 An internal attacker copies voting papers and uses them.

13.14 An external attacker infiltrates the printing office's infrastructure electronically, physically or by means of social engineering and extracts the codes of the polling cards.

Sources: OEV (SR 161.116), Art. 5, Annex 2.9, 7, 13; Scope 3 (printing offices) reports 2022, 2025; A. Appel, CITP Blog, 01.07.2022; cantons BS, GR, LU, SG, TG, E-Voting Risikoportfolio, 30.01.2026.

THREATS IN FOCUS · 4 OF 4

High-level attacks by a foreign power



WHAT TEXTS, REPORTS AND EXPERTS SAY

- Hostile organisation: "substantial resources and above-average expertise", "may also be supported by a state" (Annex 1.6).
- Verifiability is required to hold even if the online servers and three of the four control components of a group are controlled by an attacker (Annex 2.9); the canton runs at least one control component itself (Annex 3.1).
- FCh risk assessment 2026-3: R8 (outage by a well-resourced attacker) residual probability "Hoch"; R1 (serious security flaw): "Ein Nullrisiko gibt es jedoch nicht."
- Previous system, 2019: four researchers showed that the mixnet's cryptographic design allowed undetectable fraud (A. Appel, Princeton, 2022, citing their IEEE paper).

MY OPINION

- A state-sponsored actor is capable of infiltrating the system.
- But who would want to manipulate Swiss political decisions this way?
- Aren't there simpler ways to influence a vote?
- E-voting results are checked for plausibility against the other channels: a large deviation would be noticed.

THREATS IN FOCUS (OEV ANNEX 13)

13.10 A hostile organisation infiltrates the system with the aim of falsifying the result.

13.26 A hostile organisation infiltrates the system with the aim of breaching voting secrecy or obtaining premature partial results.

13.30 A hostile organisation carries out a denial-of-service (DoS) attack.

13.35 A hostile organisation infiltrates the system with the aim of disrupting operations, manipulating voter information or stealing proofs of the voting behaviour of the persons voting.

Sources: OEV (SR 161.116), Annex 1.6, 2.9, 3.1, 13; FCh risk assessment 2026-3; A. Appel, CITP Blog, 27.06.2022; cantons BS, GR, LU, SG, TG, E-Voting Risikoportfolio, 30.01.2026.

TAKE-AWAYS · PERSONAL VIEW

What I take from it

THE SYSTEM

1 **Over 20 years of experience**
Since 2004, more than 300 trials in 15 cantons, with no relevant security incident according to the Federal Chancellery.

2 **A redesign built on lessons learned**
The current system takes the errors of the previous ones into account and follows the recommendations of independent experts.

3 **Strong technical assurance**
Permanent bug bounty, yearly public intrusion test, audits on four scopes at each change and at planned intervals. Incidents mostly stem from human error, not from the system.

4 **Continuous improvement**
A risk-based approach, with tangible results since 2022.

HOW IT IS DISCUSSED

5 **Demagogy over causality**
Opponents' arguments, politicians' in particular, are often demagogic and sometimes lack any causal link between a weakness and an outcome.

6 **Black-and-white thinking**
Some experts tend to see the system as either secure or insecure. Yet rule zero in the security field is that information security management is risk management.

7 **A vulnerability is not an attack**
A single vulnerability is not, on its own, an attack scenario.

8 **Organisational gaps can lead to issues**
The physical access gaps found on site in 2025, after the 2022 fix, remind us to keep our eyes open.

SWISS CYBER STORM 2026

Thank you!

Questions?

Contact: s.adamiste@soluss.ch