Improving the Swiss Post Voting System: Practical Experiences from the Independent Examination and First Productive Election Event

Olivier Esseiva[1], Audhild Høgåsen[2], Xavier Monnat[3]

Abstract:

The Swiss Post Voting System has undergone over the past few years a rigorous independent examination by experts mandated by the Swiss Federal Chancellery. Following the examination, Swiss Post has made improvements in several areas, including for voter authentication, synchronization, input validation, and universal verifiability. On 18 June 2023, the Swiss Post Voting System was put to trial in its first productive election event. 4,239 voters cast their vote online during the approximately one month that the e-voting channel was open. The adoption rate of the e-voting channel was high, especially among Swiss residents living abroad, with an adoption rate of more than 50%. Swiss Post extensively monitored the voting servers during the whole election period and did not detect any anomalies during the system's operation. The feedback collected regarding the voters' user experience was largely positive. A few voters experienced confusion with regard to the voting process or with browser compatibility issues. Swiss Post has learned important lessons from the independent examination and from the first productive election event, and will continue the work improving the Swiss Post Voting System.

Keywords: Swiss Post Voting System; Electronic Voting; Online Voting; Public Scrutiny; Independent Examination

[1] olivier.esseiva@post.ch All authors are employed by Swiss Post (Switzerland) and work in the E-voting team.
[2] audhild.hoegaasen@post.ch
[3] xavier.monnat@post.ch

doi:10.18420/e-vote-id2023_09

1 Introduction

1.1 Past Experiences

Switzerland has a longstanding tradition of direct democracy, allowing Swiss citizens to vote approximately four times a year in elections and referendums. While mail-in ballots have traditionally been the prevailing method of voting in Switzerland, some cantons have previously introduced e-voting to a portion of their electorate. A survey from gfs-zürich reveals that almost three quarters of the public would welcome online voting.[4]

Swiss Post provided an e-voting system between 2016 and 2019. However, due to substantial criticism from reputable security researchers [Ha19, Ha20, TP19, LHK19], the system was subsequently withdrawn from the market in 2019.

1.2 Relaunch of E-Voting Trials

In 2020, Swiss Post made the strategic decision to internalize the development process and establish a cryptography competence center in Neuchâtel, Switzerland. This center comprises a team of software engineers, cryptographic developers, and mathematicians who possess specialized expertise. Their responsibilities include designing the cryptographic protocol, implementing the specification, and ensuring the secure operation of the Swiss Post Voting System.

Since 2019, Swiss Post has made significant enhancements to the design, documentation, and implementation of the e-voting system. As a result, in March 2023 the Federal Council authorized the cantons of St. Gallen, Thurgau, and Basel-Stadt to employ the Swiss Post Voting System for a specific subset of their electorate.[5] Subsequently, during the federal vote on 18 June 2023, a total of 4,239 voters opted to cast their ballots online using the Swiss Post Voting System.

1.3 Transparent Development and Public Scrutiny

Transparency and public scrutiny is crucial for enhancing trust and acceptance of online voting. Swiss Post strives to achieve this through an open, transparent development process, complemented by the active involvement of a community of security researchers, hackers, and students to perpetually scrutinize its system's documentation and implementation [MO21]. This section presents a concise overview of the initiatives undertaken by Swiss Post to foster this community.

[4] Survey on e-voting from gfs.zürich: https://gfs-zh.ch/schweizer-bevoelkerung-befuerwortet-e-voting/

[5] Federal Council approves resumption of online voting trials: https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-93455.html

1.3.1 Continuous Publication of Documentation

Swiss Post publishes a wide variety of documents on its GitLab platform.[6] Table 1 summarizes the main documents that are particularly relevant for the e-voting community.

Document	Description
Computational proof	Mathematical proof of verifiability and privacy under a minimal set of computational assumptions
Symbolic model	Machine-checkable ProVerif model of the Swiss Post Voting System proving verifiability and privacy in a symbolic setting
System specification	Pseudo-code specification of the cryptographic protocol
Verifier specification	Pseudo-code specification of the auditor's technical aid for verifying the correctnesss of the election result
Crypto-primitives specification	Pseudo-code specification of the cryptographic primitives underpinning the cryptographic protocol
Infrastructure documentation	Documents describing the deployment, testing, and operations of the Swiss Post Voting System

Tab. 1: Overview of published documents on Swiss Post's GitLab platform.

1.3.2 Continuous Publication of Source Code

Swiss Post publishes the source code of the components of the e-voting ecosystem.

Table 2 summarizes the published source code. We publish the verifier and the libraries underpinning the Swiss Post Voting System under a permissive Apache-2 licence. The source code of the Swiss Post Voting System's components is published under a proprietary license granting non-commercial academic use.

Repository	Description	Lines of Code	License
E-voting	Source code of the e-voting system	55,000	Proprietary
Verifier	Source code of the verification software	11,000	Apache-2
Crypto-primitives	Java cryptographic library	9,000	Apache-2
Crypto-primitivies-ts	TypeScript cryptographic library	2,000	Apache-2
E-voting-libraries	Shared functionality and domain objects	11,000	Apache-2
Data-integration-service	Tool to process configuration files	6,000	Proprietary

Tab. 2: Overview of the Swiss Post Voting System's source code repositories.

Furthermore, we provide security researchers with instructions and test data on how to run an end-2-end test locally on their machines using Docker containers.[7]

[6] All documentation is found on GitLab: https://gitlab.com/swisspost-evoting
[7] End-2-end instructions and test data: https://gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev

1.3.3 Reproducible Builds

To guarantee the integrity and intended functionality of the software, Swiss Post employs reproducible builds. There must be a reliable and verifiable software compilation and proof that the source code in the production environments is the same as the publicly available source code, thereby enabling anyone to verify that the binary of the system's component aligns with the inspectable source code published on GitLab. This ensures that the Swiss Post Voting System's components remain untampered with and perform as intended.

The cantons conduct trusted build ceremonies involving mandated experts. The protocols pertaining to these ceremonies are published openly on the GitLab platform.[8]

1.3.4 Permanent Bug Bounty Program

The Swiss Post Voting System is subject to a permanent bug bounty program. The bug bounty program covers the cryptographic protocol, specification, and source code, inviting researchers to identify vulnerabilities. Successful attacks targeting verifiability are eligible for bounties reaching up to EUR 230,000.[9] Through this initiative, to date, 287 reports have been submitted, four significant issues have been discovered, and a total of EUR 170,000 in bounties has been paid out across all bounty reports.[10] All accepted findings are also published on Swiss Post's GitLab. This includes the summary of the report and comments. The reporter of the findings will be credited if the reporter agrees to publication. The hunters can decide if they want to be credited with their name, stay anonymous, or use an alias.

1.3.5 Test Platform

Starting from April 2023, Swiss Post provided a test platform on which anyone could run through the electronic vote casting process.[11] In the span of two months, more than 2,000 votes were cast, and Swiss Post received more than 200 feedback messages through the corresponding feedback form.

[8] Protocols for the trusted build ceremonies: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Trusted-Build

[9] Information about the bug bounty program: https://yeswehack.com/programs/swiss-post-evoting

[10] Overview of received reports: https://evoting-community.post.ch/en/contributions

[11] Swiss Post test platform: https://post-medien.ch/en/how-does-e-voting-work-anyone-can-now-try-out-casting-a-vote-on-swiss-posts-test-platform

1.3.6 Regular Public Intrusion Tests

Swiss Post conducts periodic public intrusion tests, extending invitations to hackers worldwide, with the objective of assessing the security of its e-voting infrastructure. This initiative serves as a valuable complement to the permanent bug bounty program. The public intrusion test offers hackers a designated platform to target a production-like environment.

In 2022, the public intrusion test attracted the participation of 3,400 hackers. Despite their collective efforts, no hacker succeeded in breaching the e-voting system.[12] Nevertheless, the test proved beneficial as it enabled Swiss Post to identify areas for improvement, particularly with respect to voter authentication. In 2023, a public intrusion test took place from 8 to 31 July. As in the year before, no hacker succeeded in breaching the e-voting-system. The activity was similar to the year before. Four reports were submitted, and one was accepted as best practice.[13]

1.3.7 Further Contact with the Community

Regular information to our community is important. Since 2017, Swiss Post has been running a blog that is regularly updated with news about the Swiss Post Voting System.[14] In addition, anyone interested can sign up to the regular infomail from the Swiss Post E-voting team.[15] Since 2021, Swiss Post has held four webinars covering topics such as security by design, trust model, complete verifiability, open source, auditability, and end-to-end testing.[16] In May 2023, Swiss Post organized an event at the cryptography competence center in Neuchâtel especially for IT and math students.[17] Swiss Post engages with the academic community at the conference E-Vote-ID every year. Swiss Post has submitted several papers to this conference. In 2017, the paper *A secure e-voting infrastructure. Implementation by Swiss Post* [SMM17] by Raffaele Stefanelli, Denis Morel and Xavier Monnat was published. In 2021, the paper *The challenges of enabling public scrutiny* [MO21] by Xavier Monnat and Simon Oswald was published. Then in 2023, this paper was published.

[12] PIT 2022: https://www.post.ch/en/about-us/media/press-releases/2022/hackers-put-e-voting-system-to-the-test and https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues/43

[13] PIT 2023: https://post-medien.ch/en/swiss-posts-e-voting-system-to-be-used-for-the-first-time-in-elections-this-autumn-following-further-devel-opment-and-successful-hacker-test/

[14] E-voting blog: https://www.evoting-blog.ch/en

[15] E-voting infomail: https://evoting-community.post.ch/en/community-programme/infomail

[16] E-voting webinars: https://digital-solutions.post.ch/en/e-government/blog/tag/event

[17] E-voting community event 2023: https://digital-solutions.post.ch/en/e-government/blog/exclusive-insight-into-swiss-post-s-e-voting-system

2 Independent Examination

Switzerland's federal law establishes various prerequisites for the approval of e-voting systems to be utilized in elections and referendums. Among these requirements is the mandate that the e-voting system and its operations undergo an independent examination commissioned by the Swiss Confederation.[18] The independent examination is a continuous process, and every new release of the e-voting system triggers a new independent examination.

2.1 Reports by Independent Auditors

Between 2021 and 2023, the Federal Chancellery commissioned renowned experts from academia and industry to examine the Swiss Post Voting System. The examination covered four areas: the cryptographic protocol (Scope 1), the software (Scope 2), the infrastructure and operations at Swiss Post and the cantons (Scope 3), and an intrusion test (Scope 4). The experts produced a total of 28 audit reports. 13 of the reports examined the cryptographic protocol [Es22, Ba22, Ha22a, HPT22, Fo22, Es23c, Es23a, Es23b, RBS23, Ha23, HPT23c, HPT23a, HPT23b], 13 examined the software [HPT22, Fo22, Ha22b, FAD22, Oe23, OH23b, OH23a, OH23c, Fo23, HPT23c, HPT23a, HPT23b, Ha23], six examined infrastructure and operation [Fo22, AFD22, AO23a, AO23b, Ad23, AO23c] and three concerned intrusion testing [SC22, SC23, Kr22]. Several of the reports spanned multiple areas of examination.

In response to the examination reports, Swiss Post summarized the key recommendations, expressed its stance, and provided responses to the major findings and observations highlighted in the reports [Sw22, Sw23d].

Swiss Post is grateful for the extensive reports from the mandated experts and for the opportunity given to improve the Swiss Post Voting System. Numerous issues have already been addressed by Swiss Post, and numerous improvement suggestions have been implemented. However, certain enhancements necessitate a longer timeframe and substantial effort to implement. The Federal Chancellery has outlined a catalogue of measures for these pending improvements and enhancements, including a timeframe for when the measures must be addressed [FC23b].

2.2 Identified Issues and System Improvements

In this section, we highlight a few issues from the examination reports and describe how Swiss Post addressed them in the cryptographic protocol, specification, and code.

[18] Information about the audit concept and all expert reports can be found here: https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html

2.2.1 Voter Authentication

The voting phase comprises two primary stages: firstly, the voter submits the encrypted vote, and secondly, the voter confirms the vote. However, before this, there is a preliminary voter authentication phase, wherein the voter receives an encrypted key store and public keys for vote encryption.[19]

The voter authentication protocol previously used by the Swiss Post Voting System up until April 2023 employed a challenge-response mechanism and did not expose any known security flaws. Nevertheless, various problems concerning the voter authentication were highlighted in the expert reports [Ha23, Section B.3.3] [Ba22, Section Assumptions and Limitations], [Es22, Section 7], [Fo22, Section 5.1]. The criticism highlighted the omission of voter authentication in the symbolic models, the absence of pseudo-code for these authentication algorithms, and an overly complex three-round communication process between the voting server and voting client.

To tackle this issue, Swiss Post rewrote the voter authentication protocol. The new voter authentication protocol is described in pseudo-code in the system specification and included in the symbolic analysis of the cryptographic protocol. The implementation of the new voter authentication protocol significantly simplifies the complexity of the source code. It enabled the retirement of two outdated cryptographic libraries and facilitated the removal of over 20,000 lines of code from the system, thereby streamlining and enhancing its overall efficiency.

Figure 1 shows the workflow of the voter authentication protocol. Importantly, the new voter authentication protocol retains its ability to safeguard against replay attacks from network adversaries, relying on the presence of a trustworthy voting server. The new voter authentication protocol draws inspiration from the TOTP protocol [M'11] and requires only a single round of communication, as opposed to the previous three rounds.

2.2.2 Synchronization

Haenni et al. [Ha22b, Section 2.6] observed that the Swiss Post Voting System lacked a robust mechanism to synchronize the execution of specific operations. This absence of synchronization posed significant concerns, particularly due to the system's deployment across multiple data centers for availability purposes. If an attacker could manage to deceive two instances of the same component into processing two distinct messages simultaneously, this could potentially undermine the system's verifiability.

[19] It is worth noting that this preliminary voter authentication phase holds no relevance for the protocol's security analysis. An attacker with control over the voting client can access the contents of the voter's keystore, whereas an attacker lacking control over the voter or voting client cannot open the keystore.

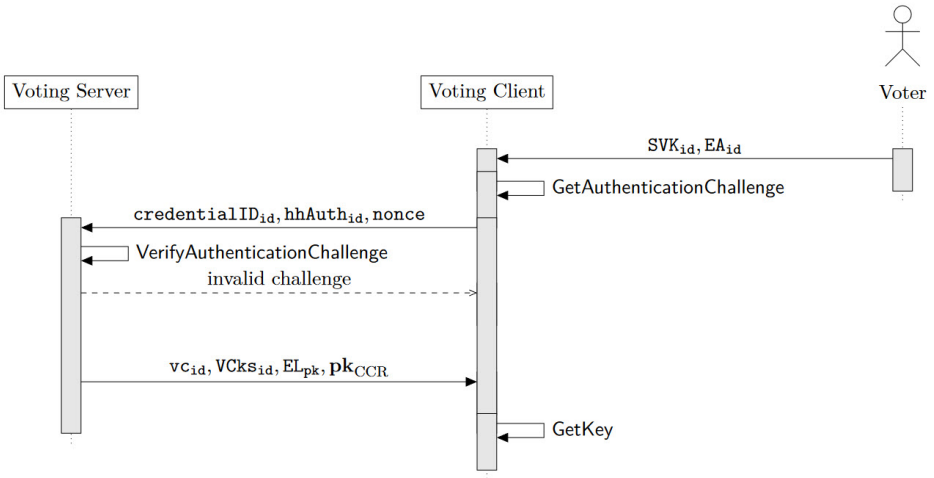

Fig. 1: Sequence diagram indicating the flow of messages in the new voter authentication protocol [Sw23b, page 58].

For instance, the attacker could transmit both a vote corresponding to the voter's selection and a vote containing the attacker's own selections concurrently to a control component. If both instances processed the messages, the attacker could send the expected return codes to the voter while simultaneously storing the manipulated vote in the ballot box—effectively compromising individual verifiability.

To solve this problem and ensure that each component processes every message exactly once, the Swiss Post Voting System now uses the mechanism of an exactly-once processor. The architecture document [Sw23a, Section 10.1.2] outlines this mechanism. The exactly-once processor leverages a widely adopted approach for achieving concurrency control in distributed systems, namely database transactions. The message broker's at-least-once delivery ensures that messages are received by the control components, even in the presence of failures or network issues. Finally, the control component's idempotent handling of messages guarantees that processing a message multiple times always yields the same result.

In the event that two instances of the same component receive different messages for the same voter simultaneously, the system employs a rollback mechanism within the database transactions. This ensures that only one message and response is ultimately saved, and a single response is transmitted to the requester. Consequently, the desired security properties are achieved.

Figure 2 illustrates the scenario in which the same message is delivered near simultaneously to both Control Component 1 instances. As there has been no previously computed response, both copies of the message will be processed. However, the database will detect the consistency violation and force a rollback of one transaction. Furthermore, only one message will be processed successfully, and only one response returned, since the second instance refrains from sending the processed message back to the requester.

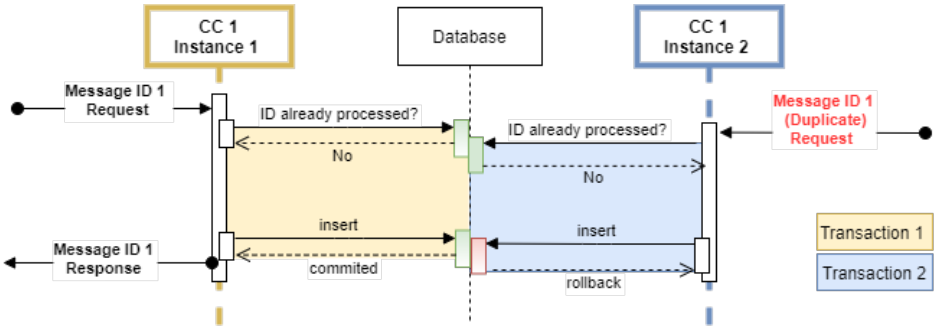

Fig. 2: Diagram showing the mechanism used in the Swiss Post Voting System to handle delayed duplicate messages to ensure exactly-once processing [Sw23a, page 61].

Importantly, the effectiveness of the exactly-once processor was validated during subsequent rounds of the experts' review:

> [Ha23, Section 2.2.6]: They also implemented a property called exactly once processing, which guarantees that external messages are processed exactly once. This prevents not only identical messages from being processed more than once, but also similar messages (of the same type). For example, if a voter sends different ballots simultaneously, then these ballots are recognized as similar messages and only one of them will be processed.

2.2.3 Input Validation

The specification documents offers for each algorithm of the system a comprehensive pseudo-code description, including description of the context, input, operation, and output. The implementation must adhere to these pseudo-code instructions.

Nevertheless, the independent experts emphasized that the source code adhering faithfully to the pseudo-code specification is not sufficient. They stressed the significance of rigorous input validation and the necessity of taking the context from a trusted source:

> [HPT22, Section A.2.1]: For example, the micro services allow the functions to be called many times on a wide range of data, but the security model in the proof assumes most functions can be called only once on a very rigid input. This is a significant discrepancy between the specification and the code, that makes it really hard to decide whether the code does what the specification says, while making it quite possible that the code will lead to many more possible system states than what the specification allows.

Other experts agreed on the importance of rigorous context and input validation [Es22, Section 1.2, Section 8, Section 9.2, Section 9.3] [Ha22b, Section 2.5].

A typical example of the principle of input validation is the group parameters of the ElGamal encryption scheme. These parameters are context for several pseudo-code algorithms in the cryptographic protocol. The algorithms must be instantiated with the group parameters from the component's internal view, where their validity was previously verified during an earlier stage of the protocol. The group parameters must not be taken from adversarially controlled messages.

In response to the criticism, we extensively reviewed the services invoking the protocol's algorithm and ensured that all components properly validate the input and take the context from a trusted source. Input validation involves verifying that the input adheres to the expected format, such as confirming that all elements belong to the designated group and that the vectors contain the appropriate number of elements. Additionally, we took measures to ensure that the context variables originate from the internal view of a component and/or undergo validation against previously encountered values. This approach safeguards effectively against potential attacks that aim to invoke the algorithm with invalid input or unmet preconditions.

The system specification has been enhanced with a subchapter addressing context, state, and input variables [Sw23b, Section 1.5]. This subchapter emphasizes to developers the importance of taking context variables from trusted sources. For certain algorithms in the specifications, we have included an overview which for each variable shows the source and the required input validation. Figure 3 illustrates this approach using the voter authentication algorithms.

2.2.4 Universal Verifiability and Importance of Consistency Checks

Haines et al. emphasized the significance of consistency checks and presented a possible attack on universal verifiability [HPT23c, Section 3.3.4]. The attack involved reordering shuffle payloads between different ballot boxes. To detect such an attack, the verifier needs to examine the consistency of file names associated with the payloads and compare them with

Information	Variable	Source	Use as	Preliminary Validation
Election Event ID	$\texttt{ee}$	Voting Client	Context	Check that $\texttt{ee}$ exists in the internal view.
Authentication step	$\texttt{authStep}$	Voting Client	Context	Check that the authentication step is consistent with the state of the $\texttt{vc}_{\texttt{id}}$.
Derived voter identifier	$\texttt{credentialID}_{\texttt{id}}$	Voting Client	Input	Check in the internal view that $\texttt{credentialID}_{\texttt{id}}$ corresponds to a $\texttt{vc}_{\texttt{id}}$ for this $\texttt{ee}$, that the corresponding ballot box is currently open, and that the $\texttt{vc}_{\texttt{id}}$ is consistent with other information received from the voting client.
Derived authentication challenge	$\texttt{hhAuth}_{\texttt{id}}$	Voting Client	Input	None. Checked within algorithm 5.2.
Base authentication challenge	$\texttt{hAuth}_{\texttt{id}}$	Internal view	Input	None, since retrieved from the trusted internal view.
Authentication nonce	$\texttt{nonce}$	Voting Client	Input	None, other than the implicit domain checks.

Fig. 3: Table from the System Specification [Sw23b, Page 60] showing the context and input validation for the voter authentication algorithms.

the actual payload content. However, the Swiss Post verifier specification only informally described such checks, and the checks were not implemented with sufficient rigor in the code.

To address this concern, the verifier specification has been augmented with more than 40 authenticity and consistency pseudo-code algorithms. These algorithms provide detailed instructions for the verifier to conduct checks aimed at preventing potential attacks and inconsistencies. Further refinements of the verifier specification are planned. An example of such pseudo-code algorithms for consistency verification is depicted in Figure 4.

Verification 3.03 VerifyCCRChoiceReturnCodesPublicKeyConsistency

Input:

The CCR Choice Return Codes encryption public keys ($\mathbf{pk}_{\mathrm{CCR}_j}$) included in the following files from table 2:

- Online Control Component Public Keys ▷ 1 per component
- Setup Component Public Keys

Operation:

1: **for** $j \in [1, 4]$ **do**
2: $\mathrm{ok}_j \leftarrow$ the CCR Choice Return Codes encryption public keys for control component j are identical from both sources
3: **end for**

Output:

$\top$ if all keys are identical, $\bot$ otherwise.

Fig. 4: Pseudo-code algorithm from the verifier specification [Sw23c, Page 19] for one of the consistency verifications.

3 First Productive Election Event

The Swiss Post Voting System, incorporating individual and universal verifiability, was utilized for the first time during the election event on 18 June 2023. The e-voting system was used exclusively for a specific electorate in the cantons of Basel-Stadt, St. Gallen, and Thurgau.

The initial election event was considered a success by the involved cantons and by Swiss Post, with several positive indicators.[20] The open-source verification software successfully verified the correctness of the results, the level of support requests from voters remained low, and the adoption of e-voting demonstrated a high rate.

3.1 Involved Electorate and Participation

In Switzerland, the cantons possess the authority to determine the portion of the electorate eligible to utilize e-voting, provided they adhere to the Federal Chancellery's Ordinance [FC22], which stipulates a maximum limit of 30% of the cantonal electorate and 10% of the national electorate for e-voting participation.[21] For the first productive election event, the cantons chose to offer e-voting to the following segment of the electorate:

- *Basel-Stadt*: Swiss citizens residing abroad and voters with disabilities.
- *Thurgau*: Swiss citizens residing abroad.
- *St. Gallen*: Swiss citizens residing abroad and voters from five pilot municipalities.

A total of 64,869 voters were eligible to vote online in the three cantons. However, voters with disabilities and those from the pilot municipalities are not automatically granted the option to vote online. Instead, they must explicitly register for this service, which adds an additional hurdle to the process. Out of the eligible voters, a total of 4,239 chose to cast their votes online.

[20] A successful premiere for Swiss Post's e-voting system: https://post-medien.ch/en/a-successful-premiere-for-swiss-posts-e-voting-system/

[21] The info page of the cantons explains these requirements in detail (available in German): https://www.evoting-info.ch/themen/politik-gesellschaft/e-voting-in-der-schweiz.html

Table 3 shows the participation in the election event on 18 June 2023 in the cantons of Basel-Stadt and Thurgau.

Description	Basel-Stadt	Thurgau
Eligible Citizens	9,883	4,885
Mail-in/on-site ballots	1,208 (46.5%)	520 (43.8%)
Electronic votes	1,388 (53.5%)	667 (56.2%)
Votes cast in total	2,596 (100%)	1,187 (100%)

Tab. 3: E-voting participation for the cantons of Basel-Stadt and Thurgau in the voting event of 18 June 2023. The numbers originate from the statistics published by the Federal Chancellery [FC23a].

Notable is the high adoption rate of e-voting for the Swiss citizens residing abroad, clearly shown in the cantons of Basel-Stadt and Thurgau. Respectively, 53.5% and 56.2% of the citizens who were eligible for e-voting and chose to cast a vote in the election, chose to do so electronically.

The adoption rate for Swiss residents in the pilot municipalities of the Canton of St. Gallen is challenging to interpret due to the registration process required for online voting. Slightly more than 10% of the citizens who had the potential to register for e-voting and chose to cast a vote in the election, opted to both register and cast their votes electronically.

Worth mentioning is that the total mail-in and on-site ballots in Basel-Stadt, St. Gallen, and Thurgau all included invalid votes, whereas for the e-voting channel an invalid vote is not possible, since the voter portal only allows voters to submit valid votes.

3.2 System Deployment and Security Measures

From mid-May until 17 June, the electronic ballot boxes remained accessible to voters. To ensure seamless operation of the e-voting channel, Swiss Post employs a robust infrastructure, implements restrictions on system modifications, and proactively monitors the system for anomalies. The infrastructure documentation emphasizes key elements of the deployment, including redundancy, access controls, and a layered infrastructure that offers multiple lines of defense against diverse types of attacks.[22]

Throughout the election event period, the system's load remained within normal levels. Additionally, we also monitored the system for any anomalies that might be observed during the election event's execution. Possible anomalies encompass various scenarios, such as:

[22] Infrastructure documentation on GitLab: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Operations

- Unforeseen errors or exceptions occurring in the server backend.
- Excessive utilization of system resources.
- Non-responsiveness exhibited by system components.
- A significant number of failed logins, either originating from the same IP address or in total.
- Lack of successful logins and submissions of votes.
- Substantial quantities of blocked suspicious requests by the web application firewall.
- Unusually elevated traffic levels, suggestive of a potential distributed denial-of-service (DDoS) attack.

The election event proceeded smoothly, with only a minor incident occurring during the voting period when the message broker component experienced a temporary outage. The monitoring system detected the issue and alerted Swiss Post operations, who resolved it within minutes. Although the problem was addressed effectively, there was some ambiguity regarding the communication channels, specifically regarding the responsibility of informing the cantons. As a result of the incident, a few voters encountered difficulties in submitting their votes and reported the issue to the cantonal support hotline, which was initially unaware of the outage.

In the subsequent after-action review of the incident, Swiss Post recognized the need for clearer and more proactive communication with all stakeholders, even in the event of minor incidents. Therefore, we made enhancements to the communication process, aiming to ensure that all relevant parties are informed promptly of potential similar incidents in the future.

During the final week of the election event, the Swiss federal government, along with certain cantonal and municipal governments and state-affiliated companies such as Swiss Post and the Swiss Federal Railways, fell victim to a distributed denial-of-service (DDoS) attack orchestrated by the Russian hacker group known as *No Name*. [23] The Swiss Post Voting System was not on the hacker group's target list and remained accessible throughout. Nevertheless, these attacks served as a reminder of the criticality of robust defense mechanisms against DDoS attacks. Additionally, it emphasized the significance of informing voters about the importance of casting their votes earlier in the election event period, rather than waiting until the final days.

[23] Information from the Federal Council about the DDoS attack: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-95641.html

3.3 User Experience and Feedback

Before the inaugural election event, rigorous testing was conducted on the user interface of the Swiss Post Voting System, resulting in its certification for accessibility level AA[24] according to the Web Content Accessibility Guidelines (WCAG) 2.1.

However, it was during the first productive election event that the system faced its true trial, enabling Swiss Post to observe the system's behavior and the frequency of support inquiries in the three participating cantons.

An essential metric that Swiss Post monitored was the ratio of submitted votes to confirmed votes within the Swiss Post Voting System. The Swiss Post Voting System uses a two-round return code scheme. First, the voter submits their vote and verifies the correctness of the received Choice Return Codes. Secondly, in order for their vote to be counted, the voter confirms their vote by entering the Ballot Casting Key and verifies the correctness of the received Vote Cast Return Code. It is, however, possible for the voter to abandon the process before confirming their vote and opt for an alternative voting channel. It could be expected that the occurrence of such instances is minimal. A higher percentage of unconfirmed votes would suggest voter confusion, forgetfulness in confirming their vote, or, worst-case scenario, potential manipulation by a deceptive voting client. For this first productive voting event, *99.5%* of voters who submitted their vote also proceeded to confirm it. This number aligns with our past experiences with the Swiss Post e-voting system used from 2016 to 2019.

Furthermore, we conducted an analysis of the support requests that the cantons received from voters, examining both their quantity and nature. Encouragingly, the number of support requests remained relatively low, and no support request raised concerns of a potential attack, such as a voting client failing to display the expected return codes. Instead, most support requests pertained to confusion regarding the voting process or browser compatibility issues. For example, there were instances where voters mistakenly confused the start voting key, which needs to be entered into the voter portal, with the voting card identifier. In other instances, voters typed the voter portal's URL into the Google search engine instead of the browser's address bar. Additionally, some voters experienced confusion towards the end of the voting process. Specifically, the voter portal redirected them to the login screen after the voting process ended, leading to uncertainty regarding whether the process had been successfully completed. A very small fraction of voters experienced problems with older versions of iOS and the browser Safari. In response to some of the support requests, Swiss Post has acknowledged the need for targeted enhancements to the voter's user interface, to minimize confusion and enhance the clarity of the voting process.

[24] Access for all: https://access-for-all.ch/leistungen/zertifizierung/zertifizierte-websites/

4 Conclusions

Multiple rounds of independent examination have led to significant improvement in multiple aspects of the Swiss Post Voting System. The improvements encompass all parts of the system: the source code, specification documents, the computational and symbolic proofs. The independent examination rounds in 2021–2023 was an intensive period for Swiss Post, but the effort paid off with the increased quality of the system and the authorization obtained for the relaunch. Furthermore, the continuous activity of the bug bounty program is an indicator that the transparency measures put in place are working.

On 18 June 2023, the Swiss Post Voting System with individual and universal verifiability was used for the first time in a productive election event. Despite the system's inherent complexity involving the user having to input and verify multiple code types, users were able to navigate the voting process with minimal difficulties. The operation of the system proceeded without encountering any significant issues.

Security is a process, and we will continue working on improving the quality of the Swiss Post Voting System. The Federal Chancellery's catalogue of measures outlines the planned improvements and enhancements and specifies the deadlines by which they must be incorporated into the system [FC23b]. Now we are looking ahead to further productive voting events and examination rounds, while ensuring active engagement with the community of security researchers. Our focus remains on increasing security for online voting and continuously enhancing the Swiss Post Voting System.

References

[Ad23] Adamiste, Stephane: Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider – Round 2. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[AFD22] Adamiste, Stephane; Fontes, Antonio; Domingues, Sergio Alves: Examination of the Swiss Internet Voting System Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[AO23a] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet Voting System, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Abraxas print office. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[AO23b] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet Voting System, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Baumer print office. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[AO23c] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the canton. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Ba22] Basin, David: Review of Symbolic Proofs for Swiss Post's Voting System. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Es22] Essex, Alexander: Analysis of the Swiss Post e-Voting System, Audit Scope 1: Cryptographic Protocol. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Es23a] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System (Addendum), Audit Scope 1: Cryptographic Protocol. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Es23b] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System (Addendum II), Audit Scope 1: Cryptographic Protocol. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Es23c] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[FAD22] Fontes, Antonio; Adamiste, Stephane; Domingues, Sergio Alves: Examination of the Swiss Internet Voting System Audit scope 2a: Development process. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[FC22] FCh Swiss Federal Chancellery: Federal Chancellery Ordinance on Electronic Voting (OEV), 01 July 2022. 2022. Available at https://www.fedlex.admin.ch/eli/cc/2022/336/en.

[FC23a] FCh Swiss Federal Chancellery: Eckdaten zum Einsatz der elektronischen Stimmabgabe am 18. Juni 2023. 2023. Retrieved on 2023-07-10 from https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Eckdaten%20Versuch%2018.06.2023.pdf.download.pdf/Eckdaten%20Versuch%2018.06.2023.pdf.

[FC23b] FCh Swiss Federal Chancellery: Vote électronique - Catalogue of mesasures by the Confederation and cantons, 4 August 2023. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsuebersicht.html.

[Fo22] Ford, Bryan: Auditing the Swiss Post E-voting System: An Architectural Perspective. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Fo23] Fontes, Antonio: Examination of the Swiss Internet Voting System, Audit scope 2a (development process), Follow-up audit (round 2). 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Ha19] Haenni, Rolf: Swiss Post Public Intrusion Test: Undetectable attack against vote integrity and secrecy. 2019.

[Ha20] Haines, Thomas; Lewis, Sarah Jamie; Pereira, Olivier; Teague, Vanessa: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020.

[Ha22a] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Examination of the Swiss Post Internet Voting System, Scope 1: Cryptographic Protocol. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Ha22b] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Examination of the Swiss Post Internet Voting System, Scope 2: Software. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Ha23] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Re-Examination of the Swiss Post Internet Voting System, Scope 1 "Cryptographic Protocol" and Scope 2 "Software", Version 1.0.2. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[HPT22] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Report on the Swiss Post e-Voting System. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[HPT23a] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Addendum on the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[HPT23b] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Second Addendum on the Swiss Post e-Voting System*. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[HPT23c] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Examination Report on the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Kr22] Krähenbühl, Cyrill; Wyss, Marc; Burkhard, Robin; Wanner, Joel; Perrig, Adrian: Swiss Post E-Voting Scope 4: Network Security Analysis. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[LHK19] Locher, Philipp; Haenni, Rolf; Koenig, Reto E: Analysis of the cryptographic implementation of the swiss post voting protocol. 2019.

[M'11] M'Raihi, David; Rydell, Johan; Pei, Mingliang; Machani, Salah: TOTP: Time-Based One-Time Password Algorithm. In: RFC 6238, https://www.rfc-editor.org/info/rfc6238. RFC Editor, 2011.

[MO21] Monnat, Xavier; Oswald, Simon: The challenges of enabling public scrutiny. In: Electronic Voting (E-Vote-ID). Springer, 2021.

[Oe23] Oechslin, Philippe: Security audit of the e-voting back-end. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[OH23a] Oechslin, Philippe; Hofer, Thomas: Code review of the Data Integration Service. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[OH23b] Oechslin, Philippe; Hofer, Thomas: Code Review of Voting Card Printing Service. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[OH23c] Oechslin, Philippe; Hofer, Thomas: Code Review of Voting Stimmunterlagen Offline. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[RBS23] Radomirović, Saša; Boureanu, Ioana; Schneider, Steve: Review of the Symbolic Proofs for the Swiss Post Voting System's Cryptographic Protocols. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[SC22] SCRT SA: E-VOTING WEB APPLICATION, SECURITY AUDIT REPORT. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[SC23] SCRT SA: E-VOTING WEB APPLICATION AUDIT, SECURITY AUDIT REPORT. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[SMM17] Stefanelli, Raffaele; Morel, Denis; Monnat, Xavier: A secure e-voting infrastructure. Implementation by Swiss Post. In: E-Vote-ID 2017. TUT Press, 2017.

[Sw22] SwissPost: Swiss Post's reports in response to the expert reports. 2022. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Reports/Examination2021.

[Sw23a] Swiss Post: E-Voting Architecture Document. 2023. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/SwissPost_Voting_System_architecture_document.pdf.

[Sw23b] Swiss Post: Swiss Post Voting System. System Specification. Version 1.3.1. 2023. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/System.

[Sw23c] Swiss Post: Swiss Post Voting System. Verifier Specification. Version 1.4.1. 2023. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/Verifier_Specification.pdf.

[Sw23d] SwissPost: Response to examination reports launched by the federal government. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[TP19] Teague, Vanessa; Pereira, Olivier: Report on the SwissPost-Scytl e-voting system, trusted-server version. 2019.