

# Review of Version 1.5 of the Swiss Post Voting System

Johannes Müller

January 6, 2026

## 1 Overview

**Scope and objective.** This review examines the latest updates (versions 1.5.1 and 1.5.2) of the Swiss Post voting system to determine their impact on the legal security requirements of the regulation.

- I reviewed the changes in the e-voting source code (as summarized in the corresponding [changelog](#) of the Gitlab repository).
- I reviewed the updates of the system specification (as summarized in the corresponding [changelog](#) of the Gitlab repository).

**Summary.** The versions 1.5.1 and 1.5.2 I examined increase the overall security of the electoral system. I have not identified any changes that negatively impact security.

I would particularly like to highlight the improved usability of verification and the implementation of the dispute resolver. I will discuss the proposed dispute resolver in detail in this review because, from a conceptual point of view, it is the most important change in version 1.5.

## 2 Dispute resolution process

From a conceptual point of view, the most important improvement in version 1.5 is the definition and implementation of a dispute resolution process. This extension is intended to fulfill measure A.21 of the catalog of measures. The aim of this measure is to resolve certain cases in which the control components have different views on the ballots to be tallied.

In the following, I evaluate the dispute resolver proposed in version 1.5 based on the definition of measure A.21 in the catalog of measures. First, I report on an obstacle that made this evaluation difficult for me. Then I will argue why I think that the proposed dispute resolution process fulfills measure A.21. However, I will also point out that the dispute resolution process is not presented

and analyzed in a manner that reflects its significance and complexity. Finally, I will outline an alternative to the proposed process, which, in my opinion, is both more efficient and more comprehensive in resolving divergent views.

## 2.1 Obstacle

**Statement.** The objective of Measure A.21 is defined in more general terms in the main section and in the explanatory report than was actually intended. The true objective is much more narrowly defined, but only in the annex of the catalog of measures, and even there it is not particularly emphasized. As a result, I initially based my evaluation on overly strict requirements.

**Details.** Measure A.21 is described as follows in the catalog of measures:

Swiss Post has specified the so-called 'dispute resolver' to eliminate 2024 possible inconsistencies in the control components with regard to the issue of which votes are to be counted (see also explanations on Measure A.24 in the Annex).

The explanatory report describes the challenge as follows:

As a condition for the successful examination of the proof referred to in Number 2.6, all control components must have recorded the same votes as having been cast in conformity with the system. Cases where the control components show inconsistencies in this respect must be anticipated in accordance with Number 11.11 and the procedure determined in advance.

I interpreted these statements to imply that all possible inconsistencies should be resolved, from the casting of individual votes to the determination of the votes to be tallied. I took this interpretation, which seemed obvious to me, as the basis for my evaluation.

However, during my evaluation, I realized that the dispute resolution process designed by Swiss Post has a much narrower focus: this process only considers cases in which the control components have come to the same decision during voting and verification as to whether a vote should be counted later, but the lists of these collected ballots created locally by the control components and ultimately delivered are not identical. This process therefore does not cover the entire voting process, but only one type of divergence that occurs at a specific phase of the process.

Since I couldn't explain this discrepancy, I communicated with Swiss Post via the Jira platform provided. Finally, this discrepancy was clarified. The key sentence in the annex to Measure A.24, which is referred to in the main section of the catalog for Measure A.21 (see above), is as follows:

If a control component indicates an inconsistency between its own list and that of the first control component, an investigation must take place to identify the correct list to be tallied.

This means that the dispute resolution process can be restricted to disagreements regarding the storage/maintenance of these lists.

**Recommendation.** For me, this case shows that, for an evaluation to be effective and efficient, it is important that the target requirements are described clearly and unambiguously, regardless of whether the reader is familiar with the historical background of the measure in detail.

## 2.2 Effectiveness

**Statement.** The proposed dispute resolution process fulfills measure A.21.

**Details.** The dispute resolution process is executed if the lists of confirmed cast votes provided by the control components as input to the tallying phase are not equal. For this process, each control component provides the election event and the verification cards extracted from its internal data.

Essentially, the dispute resolution process then checks the consistency of the election event, of the cast votes, and of the confirmed cast votes:

- If any of the first two consistency checks fails, the dispute resolution process returns an error message.
- If the third consistency check fails, the dispute resolution process uses the individual data received from the control components to compile a list of confirmed votes accepted by all components during the submission phase.

The resulting list of resolved confirmed votes is returned to the control components so that they can check its correctness with their internal records. If the control components accept this list, it becomes the input to the tallying phase.

I intensively studied the details of this dispute resolution process to come to the conclusion that it meets the objective of measure A.21 (see above).

## 2.3 Presentation and analysis

**Statement.** Although the dispute resolution process is an important and complex part of the voting system, its design rationale is not explained, its correctness is not proven, and its impact on security is not reflected in the formal security analysis.

**Details.** While the system specification provides sufficient technical details about the dispute resolution process, it does not present its design rationale or main idea. Readers must figure out why the components were defined the way they were and how they work together properly at a high level. This is a general issue of the system specification.

Despite its complexity and importance, the reason why the dispute resolution process achieves its goal is not explained at a technical level. The reader is left to put the different, deeply connected pieces together.

The dispute resolution process takes an important active part of the voting system (if necessary). In their updated computational proof document, Swiss Post states:

Our security analysis explicitly takes into account an adversary’s attempt to abuse the process for resolving inconsistencies; for instance, by trying to inject an unconfirmed vote into the list of confirmed votes (see section 16.9).

However, comparing the latest version of the security analysis with the previous one shows that no changes have been made. Neither the threat model nor the proofs have been updated to reflect that a potentially critical component was added to the system.

**Recommendation.** Present the design rationale and the main idea of the proposed dispute resolution process. Formally prove the correctness of the dispute resolution process, i.e., why it achieves its goal when all parties behave honestly in the dispute resolution phase. Extend the threat model to include the dispute resolution party and update the formal proofs accordingly.

## 2.4 Alternative proposal

**Statement.** There are more efficient and comprehensive alternatives to the proposed dispute resolution process.

**Details.** Despite its effectiveness, the proposed resolution process has some disadvantages:

- *Late resolution:* It only detects and resolves different views at the end of the voting phase. To minimize the impact of possible discrepancies, it is better to use a dispute resolution process that resolves disputes online as they arise rather than waiting until discrepancies accumulate over the course of the ballot submission phase.
- *Limited scope:* As mentioned above and required by Measure A.21, the proposed dispute resolution process can only resolve disputes relating to the storage or maintenance of confirmed cast votes. However, it is reasonable to assume that discrepancies may also occur during other phases of the ballot submission protocol. Therefore, it would be better if the scope of the dispute resolution process were augmented accordingly.
- *No independent verification:* In principle, the information used in the dispute resolution process can be entirely unrelated to the data that caused the conflict. This is because the control components do not need to share their internal views with the process in a convincing manner. To enable true independent verification, the data submitted to the dispute resolution process must be binding.

**Recommendation.** To improve upon these limitations, I propose the following alternative to, or addition of, the proposed dispute resolution process. The election system already uses real-time monitoring software to control the integrity and conformity of the data during elections (see the Infrastructure Whitepaper). To resolve disputes in a timely manner, the monitoring system should trigger the dispute resolution process directly, if necessary. This would allow disputes to be resolved throughout the entire submission phase, not just in a limited aspect. At the same time, control components should sign their views so that there is no deniability in the event of a dispute, and potential sources of error can be more easily identified.

### 3 Monitoring system

I share my remarks on the monitoring system used. This part of my report is independent of version 1.5. However, I am still writing down my observations here, as they arose in the course of my report on version 1.5.

**Statement.** Although the monitoring system used fulfills an important task for the security of the election system, its use is only described very roughly in the current documents and its significance is not taken into account in the security analysis.

**Details.** Only the following information about the monitoring system can be found in the infrastructure white paper:

The operation and monitoring of the control components are the responsibility of different persons. Specific hardware components and the operating systems of the control components differ. The control components are connected to different networks. They are accessible only to persons who are responsible for the operation and monitoring of a specific control component. Access attempts are detected and reported to the person responsible for the corresponding control components. (Page 10)

1.4.9 Integrity monitoring: Swiss Post uses Grafana and Prometheus solution for e-voting for integrity monitoring of the operating system and as an IDS (intrusion detection system) on the entire platform. (Page 13)

1.4.13 E-voting monitoring: The infrastructure components are monitored according to a standardised and ISO-certified process. Alarms are carried out according to defined threshold values via SMS and/or e-mail alerts. In addition to this monitoring, a so-called voter monitoring was set up for e-voting. The e-voting application generates specific logs with events that can be assigned to individual phases in the voting process. Thus, received and completely anonymised

votes can be observed, searched, filtered, statistically analysed and graphically evaluated in real-time during a ballot. This monitoring primarily serves to control the orderly process of electronic voting. Critical conditions or anomalies during a ballot trigger an alert that is transmitted by SMS to the defined offices. (Page 14)

Only the following information about the monitoring system can be found in the operation white paper:

Storage Team: The Storage Team is the only team that receives monitoring data from the Control Components. It has no system access to any Control Component. (Page 5)

Monitoring collection: Every action on each Control Component will be monitored and recorded and forwarded to the Storage Team.

In particular, this information does not specify which data is collected during monitoring, how it is processed, where and for how long it is stored, and whether there is a regulated emergency plan in place in case the monitoring system triggers an alarm.

Furthermore, this component is not taken into account at all in the security analysis, even though it could have a significant impact on security (from a general perspective), particularly in terms of ensuring data integrity (verifiability) and processing potentially sensitive data (secrecy).

**Recommendations.** The use of the monitoring system should be described in more detail and its significance should be taken into account in the security analysis.