Review of Version 1.4.5 of the Swiss Post Voting System

Johannes Müller

June 17, 2025

1 Overview

Scope and objective. This review examines the latest update (version 1.4.5) to the Swiss Post voting system to determine its impact on the legal security requirements of the regulation.

1. *Updates*: I reviewed the changes in the e-voting source code (as summarized in the corresponding changelog of the Gitlab repository), in the diff files of the system specification and the crypto primitives specification (provided by Swiss post via email).
2. *Measure A.11*: I reviewed the implementation of the Vote Card Print Service (as specified in the corresponding Gitlab repository) from the perspective of measure A.11 (*Disclose source code of software for generating PDF files for printing voting cards*).

Summary.

1. *Updates*: From the security perspective, the most important change from the previous to the latest version 1.4.5 is the hardening of Algorithm 4.9 GenCredDat. In the previous version, there was a small but non-negligible chance that the conversion IntegerToByteArray of a secret key from $\mathbb{Z}_q$ to a byte array could reveal a few bits of information about the key. This issue was fixed in version 1.4.5 by ensuring that the resulting byte array representation has a fixed length.

   I also checked whether similar issues in the system could arise where the algorithm IntegerToByteArray is used without ensuring a fixed length. As far as I can see, at all other places (namely GetAuthenticationChallenge, VerifyAuthenticationChallenge, CreateLCCShare, and CreateLVCCShare), there is no such risk.

   As for the other changes in the update, I didn't find any that would hinder the system's security objectives.

2. *Measure A.11*: The main goal of this measure is to ensure the printing service functions properly and that no sensitive information, especially regarding the verification codes, is leaked.

   Keeping these objectives in mind, I reviewed the provided source code and ran tests with the provided example files. I did not find any issues with the correctness of the operation (i.e., converting raw data files to PDF files) or the secrecy of sensitive information. Using the example files provided in the Dataset folder, I was able to produce PDF files and verify the hashes.

   Therefore, I conclude that Measure A.11 has been implemented correctly.