Final Report on Release 1.4.5

Thomas Haines

19th of June, 2025

Summary

We were asked to review version 1.4.5 of the Swiss Post e-voting system [2]. Our review was limited, covering a bug in the `GenCredDat` algorithm and the newly released `Voting Card Print Service` (`VCPS`). We also reviewed the change logs for all components of the systems. We were satisfied that the changes to `GenCredDat` close the issue (#66); we were likewise satisfied with the other changes we examined.

Our examination of the `Voting Card Print Service` raised a number of issues, which we briefly summarise below:

- We found a bug in the streamable symmetric encryption used for encrypting and decrypting verifier datasets, the data exchanged between different SDM deployments, and the encrypting of the output of the `VCPS`. This bug is of limited impact and has already been patched.
- The input data to the `VCPS` is not encrypted. This is of no consequence if the `VCPS` is considered part of the `Setup component` but violates the requirements of the OEV if the `VCPS` is considered part of the `Print component`. This issue does not seem to be important with the way the system is currently deployed.

1 Examination of Voting Card Print Service

There are two main questions we considered with regards to the `Voting Card Print Service`:

- Does the code prevent a malicious adversary from tampering or reading the input files?
- Does the code deliberately tamper with the voting cards?

1.1 Honest Functionality

We found no evidence of malicious code in the service.

1.2 Security

A2.2 of the OEV [1], lists the channel between `Setup compoment` and `Print component` as untrusted. The untrusted channel means the messages need to be encrypted to avoid leaking the relationship between candidates and return codes to the adversary; this would break both individual verifiability and privacy.

The question is, at the protocol level, is the `Voting Card Print Service` part of the `Setup component` or `Printing component`? In our discussions with Post they argued for the former and in our discussions with the Chancellery they argued for the latter. Post's position is contradicted by the channel security section of the system specification [3] but aligns with the current deployments we are aware of.

Secure transmission from Setup component to the VCPS If the channel is viewed as untrusted the data needs to be protected both from observation and tampering. Authentication is ensured by the signatures verified by `xml-signature` tool.

The secrecy could be ensured by the use of `file-cryptor` tool but this does not occur at present. Since both the `Setup competent` and `VCPS` are dedicated offline computers at the cantons compromising the channel between seems difficult.

Bug in StreamedEncryptionDecryptionService We discovered an issue in `StreamedEncryptionDecryptionService` used by the `file-cryptor`. On line 80 of the class, the nonce for the encryption is constructed with only half of the expected entropy. Given that the nonce is public this only seems an issue if a collision occurred honestly; given the expected low number of times a key would be expected to be reused this remains very unlikely.

1.3 Minor Comments

- The statement in `README.md` that "The output files are encrypted to ensure that the voting cards cannot be altered before printing and signed to verify their authenticity." is unideal since encryption does not provide authentication; the system does use authenticated encryption which combined both encryption and integrity but the reader does not know this at this point of the README. In summary, we would prefer the signatures be highlighted as the reason the voting cards cannot be altered rather than the encryption.

- The link in dataset `README.md` to the package repository (containing the `file-cryptor` and `xml-signature` tools) is broken.

- While `Voting Card Print Service` produces an output following the instructions it still gives errors related to `Municipality Merger and Searcher` and the `FileEncryptor`. This has been discussed with Post and has already been partial addressed.

- At present signature verification is disabled by default in the sample configuration tool. Post has informed us that it is enabled in the configurations used by the Cantons. We have suggested a graphical indication in the tool informing the user if signature verification is disabled.

References

[1] Swiss Federal Chancellery. Federal chancellery ordinance on electronic voting of 25 may 2022. Available from `https://www.fedlex.admin.ch/eli/cc/2022/336/en`, May 2022.

[2] Swiss Post. Swiss post voting system. `https://evoting-community.post.ch/`, 2025.

[3] Swiss Post. Swiss post voting system – system specification – version 1.4.2. `https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/b5fc2da60f373612bc887138966c984da4487dfa/System`, 2025.