Review of the Additions to the Symbolic Proofs Concerning the Authentication Subprotocol of the Swiss Post Voting System

Saša Radomirović, Ioana Boureanu, and Steve Schneider
Surrey Centre for Cyber Security, University of Surrey, UK

30 June 2023

1 Scope and Methodology

We reviewed the extensions made to the symbolic models and proofs of the Swiss Post Voting System's cryptographic protocols. Our work falls into Scope 1 of the Federal Chancellery's (FCh's) Audit concept [AuC22], but *restricted to the Symbolic Proofs*. This means that evaluation of the protocols' *cryptographic proofs* are not in scope of this review, nor are computational cryptography concerns such as resilience to quantum computing.

This review builds on our previous review [RBS22] and concerns the assessment of the updated system specification [Sys23a] and symbolic models [Mod23a, Mod23c] with respect to item A12 of the E-voting catalogue of measures [CM23] approved on 20 February 2023.

While the assessment is primarily concerned with the symbolic modelling of the of the Swiss Post voting protocol, we include in this report our observations and commentary on the cryptographic protocol's design.

Documents Reviewed and Supportive Material. The reviewed material consists of seven ProVerif files. Four of these files concern vote privacy, another two concern individual verifiability of votes and one concerns universal verifiability of votes. A previously reviewed sixth file that demonstrates an attack reported by Haines has not changed and was therefore not reviewed.

Our report is based on the examination of the following documents:

- The documents comprising the symbolic models and proofs of the Swiss Post Voting System's cryptographic protocols [Mod23a] and [Mod23c] as published on 19 April 2023 and the symbolic models [Mod23b] as updated on 16 June 2023.
- Version 1.3.0 of the Swiss Post Voting System Specification [Sys23a] published on 19 April 2023.

- Version 1.3.1 of the Swiss Post Voting System Specification [Sys23b] published on 16 June 2023.
- E-voting catalogue of measures [CM23] approved on 20 February 2023.

The symbolic models and documentation of the Swiss Post Voting System were downloaded from the public repository at the following URL: `https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation`. The links to the specific versions of the files we reviewed are given in the references.

Assessments Undertaken. Our work consisted of

1. Assessment of the correspondence between the aforesaid symbolic models and the system specification in [Sys23a] for the newly specified authentication sub-protocol.
2. Examination of the symbolic proofs of the protocols' privacy, individual verifiability, universal verifiability and effective authentication properties in the symbolic models with respect to the requirements in Article 2 of the Annex of [OEV22].

   In this examination, we verified that the modifications to the symbolic models preserve the following requirements:

   - The symbolic models' trust assumptions with respect to system actors and channels are not stronger than the trust assumptions stated in Article 2 of [OEV22, Annex].
   - The symbolic models' adversary model is not weaker than the attacker assumptions in Article 2.3 of [OEV22, Annex].
   - The security requirements in Article 2 of [OEV22, Annex] are covered by the formalization of the privacy and verifiability security properties in the symbolic models.

   We used ProVerif version 2.04 to verify the correctness of the security claims.
3. Compliance with the requirements in item A12 of [CM23].

   We verified that authentication is modelled as far as is reasonable based on the specification and considered in the symbolic proofs. This is related to measure A9 which requires that the system specification is completed to include the voter authentication protocol which was previously missing.

   There are additional requirements in item A12 which must be implemented by 2025. These have not yet been implemented and therefore have not been considered in this review.

2 Summary of Results

2.1 Symbolic Models

We have not found any major problems with the extended symbolic models. We have found that:

1. In [Mod23a], the privacy models have been extended with an implementation of the voter's authentication steps in order to show that the voting protocol, now including the authentication part, still satisfies the privacy requirements. The models are faithful up to a minor issue which does not affect the validity of the obtained proofs.

2. In [Mod23b] the privacy models are updated to include a nonce and related changes introduced in the updated system specification [Sys23b]. The models remain faithful up to the above mentioned minor issue which does not affect the validity of the obtained proofs.

3. The individual and universal verifiability models have been lightly edited, but do not implement the authentication steps. This is acceptable here, because the model assumes that the `SVK` is leaked to the adversary and requires that individual and universal verifiability still hold. The models did not change between the system specification update from version [Sys23a] to version [Sys23b].

4. Effective Authentication is not proven, but informally reasoned about in the `README.md` document. The given argument is reasonable.

We give further details on our evaluation of the symbolic models in Section 3.

2.2 Design of the Authentication Sub-Protocol

Given the now completed specification of the authentication sub-protocol we observe that the voting protocol uses the same key for authentication as is used later in the voting protocol to decrypt voting material. This is against common security design principles, and we have found that it makes some attacks on vote privacy easier than necessary for the adversary. While we have concerns about the voting protocols' design, we note that the identified issue does not affect the correctness of the symbolic proofs. We expand on this issue in Section 4.

2.3 Compliance with item A12 of the Catalogue of Measures [CM23]

We consider the symbolic models to adequately specify the authentication sub-protocol in fulfillment of the requirement set for the second quarter 2023 in item A12 of [CM23].

With respect to the entire Swiss Post Voting Protocol suite, the models could and should more faithfully represent the system's possible behaviours. These are the aspects that the catalogue of measures envisages for 2025.

3 Symbolic Models

3.1 Privacy Models

The following findings apply to both reviewed versions ([Mod23a] and [Mod23b]) of the symbolic privacy models.

The privacy models have been extended with an implementation of the voter's authentication steps in order to show that the voting protocol, now including the authentication part, still satisfies the privacy requirements. The privacy models are faithful, with the exception of one constant being repeated instead of three different constants being used. Specifically, the `sendVote` and `confirmVote` constants are not used, but should be used instead of the `authenticateVoter` constant in two of the `GetAuthenticationChallenge` calls. This is of no consequence to symbolic privacy.

As reported in our previous analysis [RBS22] in October 2022 the models can be used to show that the privacy property holds unless the start voting key `SVK` leaks. This remains true for the updated models.

The compromise of `SVK` that leads to an attack on privacy is out of scope of the symbolic threat model. The consideration of the consequences of a compromised authentication credential is, we believe, nevertheless useful for further investigations in the context of Section 4 below.

We stress that the points raised in Section 4 do not invalidate the privacy models. Any attack that results from the discussed issue (a voting client's inadvertent leak of `SVK`) is outside the scope of the standard Dolev-Yao adversary model that the symbolic proofs assume. This is because the attack is a consequence of a communication that a trusted voting client is not specified to perform.

3.2 Verifiability Models

The individual and universal verifiability models have been lightly edited, but do not implement the authentication steps. Neither the individual nor the universal verifiability models implement the authentication sub-protocol faithfully. Instead, they prove verifiability under the assumption that the start voting key `SVK` is known to the attacker. This implies that even if the attacker would impersonate any voter in the authentication step, the verifiability property would still hold. This is acceptable here, because the model assumes that the `SVK` is leaked to the adversary and requires that individual and universal verifiability still hold.

3.3 Effective Authentication

Effective authentication requires that *no attacker can cast a vote in conformity with the system without having control over the voters concerned.* [OEV22, Annex, §2.8] This property is not formally proven, but informally reasoned about in the `README.md` document. The given argument is reasonable, but it is not

obvious why the corresponding formal statement is not included in the ProVerif models and proven.

3.4 Future Improvements

The voter's ability to interrupt and later re-authenticate to continue the voting protocol is not modelled in any of the reviewed symbolic models. Our previous criticisms on including all protocol behaviour remain, but are out of scope of the catalogue of measures to be implemented for this assessment.

4 Voting Protocol Design

The assessment of the symbolic models necessitates an understanding of the Swiss Post Voting System Specification. While reviewing the specification with respect to the addition of the authentication protocol, we observed that the start voting key (`SVK`) is used for two different purposes: (1) to authenticate the voter and (2) to decrypt the voter's Verification Card Keystore ($\texttt{VCks}_{\texttt{id}}$) which provides the necessary cryptographic key to submit a vote. This design is in contrast to the better design used in the rest of the system, where independent randomly generated key material is used whenever possible. For example, the ballot casting key (`BCK`) is randomly generated independently of `SVK` rather than one being derived from the other.

The chosen design makes it easier for an attacker to break vote privacy, because knowledge of `SVK` is sufficient to determine how a voter voted. This is discussed in Section 3 above and shown in our previous report [RBS22, Section 3]. The reason this design makes it easier for the adversary to carry out their attack is that it can be expected that some users will inadvertently leak their authentication credentials. For example, if a user connects to a malicious webserver (due to phishing, typosquatting etc.) rather than to the authentic voting server. The users may only notice their mistake after submitting their authentication credential to the malicious server. This risk is exacerbated by the fact that the voting protocol can be interrupted and continued at a later time by the user. The user is asked to authenticate with the `SVK` each time they connect to continue the protocol.

The above `SVK`-stealing attack relies on an initial oversight by the voter and it could be argued that far worse attacks could be carried out in that case. However, it is a relatively simple and cheap attack, as the attacker merely needs to mimic the authentication step of the voting application to obtain the key that can be used to decrypt voting material. In contrast, in a better protocol design the attacker could be forced to accurately replicate more of the voting application's behaviour and perform a man-in-the-middle attack in order to obtain the same amount of information. This would raise the cost of performing the attack and increase the likelihood of being detected.

We note that a protocol redesign to avoid the dual use of `SVK` should be done carefully. A naive improvement to the protocol, following the protocol's

existing design, would require the user to enter and compare more codes than in the current protocol. Such a redesign would therefore decrease the protocol's usability.

References

[AuC22] *Audit concept v1.4 – For examining Swiss internet voting systems.* Swiss Federal Chancellery, 2022.

[CM23] Catalogue of measures by the Confederation and cantons, February 2023. https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/E-voting%20Catalogue%20of%20measures%20by%20the%20Confederation%20and%20cantons,%2020%20February%202023.pdf.download.pdf/E-voting%20Catalogue%20of%20measures%20by%20the%20Confederation%20and%20cantons,%2020%20February%202023.pdf. Accessed 19 June 2023.

[Mod23a] Symbolic Analysis of the Swiss Post Voting System – Vote Privacy, April 2023. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.5.0.0/Symbolic-models/privacy. Accessed 6 June 2023.

[Mod23b] Symbolic Analysis of the Swiss Post Voting System – Vote Privacy, June 2023. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.5.2.0/Symbolic-models/privacy. Accessed 26 June 2023.

[Mod23c] Symbolic Analysis of the Swiss Post Voting System – Individual and Universal Verifiability, April 2023. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.5.0.0/Symbolic-models/verifiability. Accessed 6 June 2023.

[OEV22] *Federal Chancellery Ordinance on Electronic Voting.* Swiss Federal Chancellery, July 2022.

[RBS22] Saša Radomirović, Ioana Boureanu, and Steve Schneider. Review of the Symbolic Proofs for the Swiss Post Voting System's Cryptographic Protocols, October 2022. https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%201%20Final%20Report%20University%20of%20Surrey%2017.10.2022.pdf.download.pdf/Scope%201%20Final%20Report%20University%20of%20Surrey%2017.10.2022.pdf. Accessed 19 June 2023.

[Sys23a] Swiss Post Voting System – System Specification. April 2023. Version 1.3.0. https://gitlab.com/swisspost-evoting/e-voting/

e-voting-documentation/-/blob/documentation-1.5.0.0/System/System_Specification.pdf. Accessed 19 June 2023.

[Sys23b] Swiss Post Voting System – System Specification. April 2023. Version 1.3.1. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/documentation-1.5.2.0/System/System_Specification.pdf. Accessed 26 June 2023.