TECHNICAL SOLUTION OF THE ERROR DISCOVERED AND SOLUTION

Swiss Post published the source code for its e-voting system on 7 February 2019. Since then, 67 messages about the code have been submitted through official channels. International IT experts found a critical error in the source code. Swiss Post requested that its technology partner, Scytl, rectify the error immediately. The modified source code will be published with the next regular release, along with updated documentation.

In order to guarantee voting secrecy and universal verifiability at the same time, Swiss Post's e-voting system relies on so-called verifiable cryptographic mix networks. They play an important role as they enable the vote and voter to be uncoupled (background article (in german) on the role of mix networks in e-voting). Swiss Post's e-voting system uses a Bayer-Groth mix network.

The Bayer-Groth mix network is based on cryptographic commitment schemes. In this specific instance it is based on Pedersen commitments. Pedersen commitments require independent and randomly selected generators G and H. The algorithm currently used does generate these generators randomly. IT experts have however pointed out that the randomness and independence of the generators cannot be verified in the algorithm currently used. The validation of the generators is however a requirement to ensure the validity of the cryptographic proof, upon which the universal verifiability property of the system depends.

Consequence
Universal verifiability could not be guaranteed during the voting process, meaning that potential attempts to manipulate votes could not be discovered beyond all doubt.

To exploit the weak point, however, the attacker had to override numerous protective measures. They needed control over Swiss Post's secured IT infrastructure, for example, as well as help from several insiders with specialist knowledge of Swiss Post or the cantons.

The way individual verifiability works is not affected by the error discovered. The system version currently in use in various cantons functions in accordance with requirements.

Solution
Swiss Post has already had the affected algorithm corrected. The function which generates the random generators was replaced with a verifiable one which is compliant with the recognized standard: NIST FIPS 186-4, appendix 2.3. The problem described has therefore been resolved.

Swiss Post will publish the modification in the next regular source code release, along with other improvements to the code which are implemented thanks to feedback from the community.

Experts who discovered the error
The error was submitted by the following research group and researchers independently in this order:

- Privacy & Anonymity Researcher Sarah Jamie Lewis (Open Privacy Research Society, Canada); Professor Olivier Pereira (Université catholique de Louvain, Belgium); Associate Professor Vanessa Teague (The University of Melbourne, Australia)
- Researcher who wishes to remain anonymous
- Prof. Dr. Rolf Haenni (Bern University of Applied Sciences, Switzerland)

Observations regarding the source code are welcome

Any specialists who are interested still have the opportunity to examine the source code for Swiss Post's e-voting system on the GitLab platform and to submit any observations. Find out more information here.

If findings are reported, Swiss Post will give feedback to the specialists after analysis. Reports which have been fully analysed will be activated on GitLab, provided that the submitter agrees. Reports about the source code which have been fully analysed can be seen on the GitLab account under issues (access possible after registration via www.swisspost.ch/evoting-sourcecode).

In addition, a public intrusion test on the e-voting system is taking place until 24 March 2019. Find out more information here.