The source code of Swiss Post’s e-voting system was not “leaked”

Swiss Post regrets that one-sided information about the publication of its source code has been disseminated. Here is our response.

Has the source code of the e-voting system been leaked?

Nothing was “leaked” that was not already published. The source code is intended to be disclosed.

Swiss Post published the source code of its e-voting system itself on 7 February (www.swisspost.ch/evoting-sourcecode).

Swiss Post fails to understand why one would distribute a source code, that is free and legally accessible, as a pirated copy.

Swiss Post cannot guarantee that the source code, which has been published in other places by unknown persons, has not been tampered with.

Are there access restrictions?

There are no access restrictions: anyone can download, analyse, and work with the source code.

Is there an NDA and a confidentiality obligation?

No, there is no confidentiality obligation.

There is an obligation of responsible disclosure of the weak points. This means that Swiss Post must be informed first when weak points are found. The source code is complex and an observation can lead to a misunderstanding.

After a waiting period, the weak point may be published. This is common in the IT world.

Do the terms of use serve as a muzzle for users?

No. Studies on the source code may be published and one may cite from the source code.

However, the distribution of the source code to third parties who have not accepted the terms of use is prohibited.

Does Swiss Post not allow discussions about the source code?

There is a standard process for submitting notes on the source code. 30 notes have already been submitted (as at 18 February 2019), which are currently being analysed by Swiss Post.

The source code is officially published on GitLab. Notes can be submitted there. You can access the source code via www.swisspost.ch/evoting-sourcecode.

Swiss Post is grateful for any notes, analyses them and gives feedback.

The principles of responsible disclosure apply when weak points are found. After a waiting period, the weak point may be published. This is common in the IT world.

Has the cryptographer Matthew Green really found a weak point, as reported by some media?

It's true that Matthew Green publicly speculated about a weak point.

His observation was submitted a few days ago by a renowned Swiss IT specialist on the process provided for this purpose.

Swiss Post has analysed the observation and has come to the conclusion that this is not a weak point.

The analysis result for specialists:

«As stated in chapter 4.2.2 of the document Scytl sVote Protocol specifications, in a productive environment we are working in the subgroup of quadratic residues of Zp, with p a prime of 2048 bits and q a prime of 2047 bits (p=2q+1). In certain unit tests, smaller values of p and q are used (they are in a folder called test).»

(The referenced document is available on GitLab and is accessible after registration: www.swisspost.ch/evoting-sourcecode)

What happens to the notes that specialists report?

Swiss Post gives feedback to the specialists after analysis. It will publish interim conclusions on all observations at a convenient time.