GI Elections with POLYAS: a Road to End-to-End Verifiable Elections

Bernhard Beckert[3], Achim Brelle[4], Rüdiger Grimm[1], Nicolas Huber[5], Michael Kirsten[3], Ralf Küsters[5], Jörn Müller-Quade[3], Maximilian Noppel[3], Kai Reinhard[4], Jonas Schwab[5], Rebecca Schwerdt[3], Tomasz Truderung[4], Melanie Volkamer[3], and Cornelia Winter[2]

[1] University of Koblenz
[2] Gesellschaft für Informatik e.V. (GI)
[3] Karlsruhe Institute of Technology (KIT)
[4] POLYAS GmbH
[5] University of Stuttgart

Abstract. Starting from 2019, the annual elections of the GI (German Society for Computer Scientists) will be carried out using a new online voting system developed by POLYAS, aiming at providing high, state-of-the-art security guarantees. We describe the steps that POLYAS plans to take together with the GI and academic partners in order to achieve the level of transparency and trust that is expected from modern online voting. The participation of the academic partners is the key factor to make the verification process both practical and meaningful.

Online voting has been used by the GI — German Society for Computer Scientists (*Gesellschaft für Informatik e.V.*) — for its annual elections since 2004. These elections have been so far carried out using the POLYAS 2.3 voting system. Starting from 2019, the GI elections will be carried out using the new POLYAS online voting system, POLYAS 3.0, based on currently available cryptographic methods.

The current state of the e-voting research offers variety of techniques that address the fundamental security concerns of e-voting: *privacy* and *end-to-end verifiability*. However, to fully utilize the potential of those methods, one has to take into account some practical aspects and challenges, such as usability and constraints imposed by the organisation which carries out the elections. Also, as commonly agreed, the desired degree of confidence and trust cannot be achieved without a high level of transparency and without participation of independent experts. In this paper, we discuss the steps already taken and those planned by POLYAS, the GI, and the academic partners, which are designed to result in an election process which satisfies the pragmatics of the GI elections and, at the same time, provides practical and meaningful security guarantees.

Independent verification tools. POLYAS 3.0 implements standard mechanisms aiming at providing universal verifiability: all the important steps of the tallying process (such as shuffling and decryption) produce appropriate zero-knowledge proofs. It is then, in principle, possible for everyone to check those zero knowledge proofs in order to make sure that the tallying process has been carried out correctly. However, in order to utilize this ability in a practical and meaningful way, we have established a cooperation

including academic partners in order to build independent verification tools. The detailed documentation of the tallying process, based on which verification tools can be implemented, has been provided by POLYAS to the GI and to the academic partners for review. POLYAS has also provided a reference implementation of the verification procedure. Both the documentation and the reference implementation will be made publicly available. As of now, one independent implementation of the verification procedure has already been built by Maximilian Noppel from KIT and implementation of two other verification tools have been started in the group of Prof. Küsters from University of Stuttgart, one of which is being funded by POLYAS.

In the election process, an auditor will have an option to choose (one or more of) the verification tools in order to verify the final election data. We have already used the two existing verification tools to verify the tallying process of a test election carried out in July 2019.

Generation of voters credentials and formal verification of some security goals. In order to establish a mechanism preventing ballot stuffing (or to provide, so-called, eligibility verifiability), the process of generating voters' private credentials (used to digitally sign the ballots) is be carried out in a controlled way by an entity designated by the Election Council (GI). Consequently, POLYAS does not know the voters' private credential upfront. The specification of this process, as well as the source code of the credential generation tool has been provided by POLYAS (with the option to build independent implementations in the future). The process of credential generation (carried out by GI using the provided tool) has been part of the mentioned above test election. We plan to make both the specification of this process and the source code of the corresponding tool publicly available.

The central security goals of the credential generation tool is that the randomly generated plaintext passwords are only saved in an encrypted file designated for the trusted distribution facility and they do not leak in any other way (in particular, they should not make it to the file designated for POLYAS which should only contain the corresponding derived public credentials). We plan to use program verification methods to formally prove this property on the implementation level. In this non-trivial task, which has already been started by Michael Kirsten from the group of Prof. Bernhard Beckert (KIT), the KeY tool will be used in combination with techniques from simulation-based security.

Individual verifiability. The known solutions for individual verifiability involve several trade-offs, including the usability aspect: the voters should understand the process and be able to carry out the prescribed steps. Moreover, the election council must establish well define procedures for handling voters' complaints. We plan to address this security requirements in the second step, that is in the GI Elections 2020. The solution which POLYAS offers is based on the optional use of a second device (such as a mobile phone) by the voter. The details of this process are being still discussed.

The **goal of our cooperation between POLYAS and the academic partners** described above is to make the election process offered by POLYAS transparent and auditable in a practical and meaningful way. We believe that opening this process is the best way to build up trust and to improve the offered e-voting solutions.