The highly secure anonymous e-voting system of the Czech Pirate Party

Tomáš Martínek[1][0000−0002−5217−3240] and Lukáš Forýtek[2][0000-0002-2453-4483]

[1] Department of Information Engineering, Faculty of Economics a Management, Czech University of Life Sciences Prague, Czech Republic
martinekt@pef.czu.cz
[2] Department of International and Diplomatic Studies, Faculty of International Relations, Prague University of Economics and Business, Czech Republic

Abstract. The article describes the open-source e-voting system of the Czech Pirate Party including the applications, their modifications and interconnection. Overall, it provides an insight into the highly credible, secure and anonymous voting system used for intra-party direct democracy by the Czech governing party.

Keywords: Internet voting, E-voting, E-democracy, Open-Source.

1 Introduction of the electronic voting system of the Pirates

1.1 The Czech Pirate Party

The Czech Pirate Party [15] is a centrist liberal progressive political party, founded in 2009, inspired by the Swedish Pirate Party. In the parliamentary election to the Chamber of Deputies in 2017, the Czech Pirate Party gained 10.79 per cent of the votes gaining 22 mandates for the first time. The lead author of this article also received one of the mandates. Since 2021 the Pirates have been the governing party in the Czech Republic. The leader of the Czech Pirate Party Ivan Bartoš is the Deputy Prime Minister for Digitalization and the Minister of Regional Development. On 9th September 2022, the Czech Pirate Party had 1193 members [1].

1.2 Systems for intra-party voting of the Czech Pirate Party

The Czech Pirates accent the digitalization, therefore respecting intra-party democracy they have been enabling all discussions and votings online using their systems since their establishment.

Since 2016 the Czech Pirate Party has been using the secure and anonymized Helios system for secret ballots. Combined with other systems of the party, this is a unique electronic voting system that has no comparison among Czech political parties.

Personal voting is available exclusively to the party members. Every member must be accepted by a public vote of the local board in an online forum [4]. Afterwards, each member is verified by an authorized person showing an ID or passport check.

The Forum of the Czech Pirate Party is a general discussion platform that enables the membership base to have free or facilitated discussions and some types of meetings. Technically, this is the phpBB system [9] which is run by the Technical Department on the party servers [4].

The Octopus (Chobotnice) is a system for managing people and teams (regional associations, bodies, etc.). The Octopus is used for the administration of personal registers in compliance with the GDPR. Specifically, it allows the mass management of people and teams, implementation of the agenda of identity verification, registration of supporters and acceptance of members, management of applications and payments of membership fees [3].

The Profile is an application where the members, registered supporters, candidates, volunteers and newsletter subscribers manage their personal information and public profiles, and submit their requests for registration or identity verification. The application is a data source for the Octopus system [2].

The People (the Directory) is a system that provides a public overview of bodies and teams in the party and their members. The Directory is linked to the Octopus and Profile systems [1]. The Octopus, Profile and People systems were developed by the Technical Department of the Czech Pirate Party.

The Auth (the Keycloak) is a central authentication point for other applications of the Pirates. Technically, this is the *Keycloak* system [8] in version 17 which is run by the Technical Department on the party servers and which is linked up to the Octopus system [7].

The LDAP is used as a backend for the Auth. Technically, this is the *OpenLDAP* system [6] which is run by the Technical Department on the party servers.

The Helios [10] is a system for the online secret ballot; however, the ballot is verifiable. Technically, the Helios system is run by the Technical Department on the party servers. Current version 3.1.4 is modified by linking up to the Keycloak for login, to the Octopus for user list integration and other security modifications. The modified version is still open-source and it is stored on the Pirates' GitLab. [5]

Other party technologies related to voting. For HTTPS, the third-party service *Let's Encrypt* is used [12]. The Postfix system is used to create e-mail aliases of the party members in the form "firstname.surname@pirati.cz", where they can receive the information about the election and which is also run by the Technical Department on the party servers. More information on the technical systems is available on the Pirate Wiki [14].
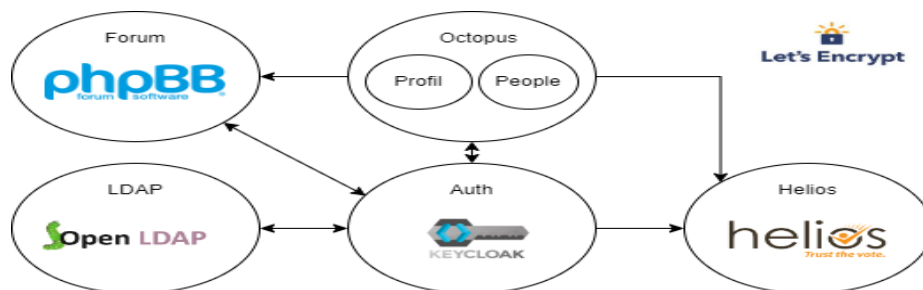

Fig. 1. Simplified scheme of the e-voting system of the Czech Pirate Party

1.3   The intra-party voting process of the Czech Pirate Party

The publicly available discussion and party meetings take place on the online forum of the Czech Pirate Party. The Pirates set an example of using direct democracy, therefore the delegate system is not used for elections, as in other Czech political parties, but all members of the given district can vote. The members usually belong to several levels of districts. The lowest level is the local forum, the middle level is the regional forum corresponding territorially to one of the 14 regions of the Czech Republic, and the highest level is the national forum, which includes all members of the party.

The elected representatives of a certain part or the entire membership base usually vote publicly on the forum of the Czech Pirate Party [4]. For example, a vote of the regional board on the admission of a new member. Personal elections and other important votes are decided by all members of the given district by direct secret electronic ballot.

For calling a vote public support is usually obtained through the forum. Similarly, also for personal elections, the forum is used to get a nomination, where it is possible to get support by supporting a specific nomination post using the "Thanks" functionality of the phpBB forum which displays the names of forum users who support a specific post. In order to start a meeting or a nomination, it is necessary to obtain the support of a group of members. The required member group amount is determined as twice the square root of the number of members in the area.

$$a = 2 * \sqrt{x} \tag{1}$$

a represents a required number of the group of members who supports the proposal

x represents a total number of members of the district

For negotiations that have already started, the required number of the group of members is halved.

In the case of personal elections, members who get the support of a given group of members by the deadline and at the same time accept a nomination or complete a nomination speech can run for the election.

The secret ballot in the voting system of the Czech Pirate Party

The party voting system is usually a two-round system. In the first round, it is possible to vote for none or all options that are acceptable to the voter. All those who receive more than half of the votes go into the second round. The second round is already a majority voting where the voters can choose one or none of the options. The winning option in the second round will be the one that receives the most votes. In case of a draw, the option with the higher support in the first round wins.

At least three trustees are appointed for the election, usually from among the particular departments and forum board. The trustees are responsible for deciphering the voting results. The Helios system itself is the basic automated trustee. Each trustee generates its key pair and uploads the public key to the Helios system [10]. If the results need to be decrypted each trustee uses his private key. The list of voters is uploaded automatically from the party systems after the selection of the district of the members who can vote.

The members are informed about the vote by e-mail, or by a mass SMS. Voting of the Czech Pirate Party can take place after the log-in of the members via the Auth Piráti system [7] using the Keycloak to the Helios party system [10] which takes data from the Octopus party system. The voting takes place on a predetermined date, usually from Friday at 10 a.m. to Monday at 10 p.m.

2 Discussion and conclusion

2.1 Important secret electronic votings of the Czech Pirate Party

The Czech Pirate Party emphasizes direct democracy, thus votings take place quite often. It is not only the election of the board, candidates, and others, but members can also call for a vote to remove them from the party positions. For example, the party statutes changes and other changes are voted on by a referendum. As this is a unique case in the Czech political environment, some votes are closely followed by the national media. The most watched cases are usually the elections of the party leader or, by contrast, calls for the removal of a certain person from a position in a party. In November 2021, all members voted on the entry of the Czech Pirate Party into the coalition government, which was closely followed by the media.

2.2 Conclusion

In contrast to other Czech political parties which vote and make decisions through delegates, or postal ballots, the Pirates allow all members to make decisions online. To increase the credibility, the Pirates exclusively use open-source solutions, making their modifications and applications available on their Gitlab [13]. The e-voting system which is used by the Pirates is comfortable even for mobile voting and guarantees a high degree of credibility, security, and anonymity for qualified decision-making in terms of direct democracy.

References

1. Lidé Piráti, https://lide.pirati.cz, last accessed 2022/09/09.
2. Profil Piráti, https://profil.pirati.cz, last accessed 2022/09/09.
3. Chobotnice Piráti, https://chobotnice.pirati.cz, last accessed 2022/09/09.
4. Fórum České pirátské strany, https://forum.pirati.cz, last accessed 2022/09/09.
5. Piráti: Helios Server, https://gitlab.pirati.cz/to/helios-server, last accessed 2022/09/11.
6. OpenLDAP, https://www.openldap.org/, last accessed 2022/09/09.
7. Auth Piráti, https://auth.pirati.cz/, last accessed 2022/09/09.
8. Keycloak.org, https://www.keycloak.org/, last accessed 2022/09/09.
9. phpBB, https://www.phpbb.com/, last accessed 2022/09/09.
10. Helios Piráti, https://helios.pirati.cz/, last accessed 2022/09/09.
11. Helios, https://vote.heliosvoting.org/, last accessed 2022/09/09.
12. Let's Encrypt, https://letsencrypt.org/, last accessed 2022/09/09.
13. Pirátský GitLab, https://gitlab.pirati.cz/, last accessed 2022/09/11.
14. Piráti: Přehled technických systémů, https://wiki.pirati.cz/to/technicke-systemy, last accessed 2022/09/09.
15. Piráti, http://www.pirati.cz/, last accessed 2022/09/09.