RAD-on: An integrated System of Services for Science - Online Elections for the Council of Scientific Excellence in Poland

Jarosław Protasiewicz, Sylwia Rosiak, Iwona Kucharska, Emil Podwysocki, Marta Niemczyk, Łukasz Błaszczyk, Marek Michajłowicz

National Information Processing Institute, Warsaw, Poland

Keywords
information system; online elections; services for science; open data; web services

1. ABSTRACT

In this study, we demonstrate an information service which supports online elections for the Council of Scientific Excellence in Poland. It is part of an Integrated System of Services for Science, RAD-on (Reports, Analysis, and Data). More specifically, we show the overall architecture of RAD-on, and the most compelling features of the service for use in online elections. The proposed e-voting system implements three phases, namely: (i) candidate nomination; (ii) electorate approval; and (iii) voting, which includes ballot distribution, voting, and result verification. This approach distinguishes itself from a typical e-voting system by paying more attention more carefully to automatic candidate nomination and voter acquisition. Moreover, we have designed processes in the system that strike a balance between security requirements and accessibility to voters. Finally, we present selected statistics from a real online election for the Council of Scientific Excellence in Poland, which took place recently. We hope that our approach, experiences, and the operational challenges which we encountered during this election, may help develop other e-voting solutions.

2. INTRODUCTION

Several countries and organisations have implemented online elections in recent years to make elections more convenient to the public (Yi and Okamoto, 2013). Estonia was the first country that introduced voting on the internet for national elections in 2005 (Vinkel, 2011). Selected government elections or referenda have also been carried out online in countries such as Norway, Switzerland, the United Kingdom, Canada, the United States, and Australia (Kaliyamurthie et al., 2013). We must underline that online voting systems usually do not replace the traditional paper-based method. However, electronic voting provides more opportunities to vote. For example, the iVote system works concurrently with a paper system, and allows remote voting by phone with the use of a call centre or on the internet, or local voting on a special computer (Brightwell et al., 2015).

Each aforementioned country has developed its own electoral system customised to its particular needs and environment: Estonia has been using the i-Voting system (Vinkel, 2011; Springall et al., 2014) since 2005; New South Wales in Australia utilises the iVote System (Brightwell et al., 2015); Norway also has its own voting system (Gjøsteen, 2011). Organisations or smaller governmental bodies may have insufficient funding to develop and maintain a unique voting system. Fortunately, they may access out-of-the-box solutions such as the Helios[1] voting system, which is the most popular open source voting tool (Alonso et al., 2018). The E-note voting system (Pan et al., 2012) and the UVote system (Abdelkader and Youssef, 2012) can also be included in this list, but is currently unclear whether they have been applied in practice.

[1] https://heliosvoting.org

Since online voting systems have now been developed for over a decade, it is now possible to distinguish their typical components. Yi and Okamoto (2013) and Magkos et al. (2017) define five major phases occurring in online voting, namely: (i) the setup in which an encryption method is defined; (ii) the registration of voters and their encryption keys; (iii) voting; (iv) tallying, in which ballots are decrypted; and (v) verification. These phases involve voters; registrants, who authorise the voters; and tallying authorities, who process ballots and publish the final results. However, most online voting approaches distinguish only three phases, normally registration, ballot distribution, and voting, which involve two sides: voters and some kind of an election committee (Alonso et al., 2018; Pan et al., 2012). These phases may be enhanced by the possibility of checking votes by voters (Abdelkader and Youssef, 2012; Brightwell et al., 2015).

In this paper, we present our e-voting system which has recently been developed to support online elections for the Council of Scientific Excellence in Poland. The main goals of our study are the following: (i) to discuss the security issues of e-voting; (ii) to show the unique functions of the system, and how they differ from better-established approaches; and (iii) to share selected statistics of real voting and discuss organisational challenges. The novelty of this study and the presented system are manifested in the following ways:

(i) The system implements three phases of online voting, i.e. candidate nomination, voter verification, and voting, which includes ballot distribution and result verification. As we will demonstrate, our approach differs from the typical systems discussed above due to environmental constraints and requirements (for more, see section 4).
(ii) We attempt to strike a balance between security and accessibility of the system for eligible voters. Since we do not offer alternative paper-based voting, the voters should be able to use the system easily. High security may discourage voters, whereas low security may distort the results (for more, see section 6).
(iii) We discuss unique operational issues and illustrate them with data coming from real rounds of voting. The operational challenges we encountered during this election may help to improve other e-voting systems (for more, see section 5).

The remainder of this paper is structured as follows: section 3 offers the big picture of an integrated system of services for science, RAD-on; section 4 depicts all phases of online elections implemented in the system; section 5 covers selected statistics from the recent election and their analysis; section 6 discusses security issues; and section 7 concludes our work.

3. RAD-on: AN INTEGRATED SYSTEM OF SERVICES FOR SCIENCE

In November 2018, we launched a new project, the Integrated System of Services of Science – Stage II (Michajlowicz et al., 2018). The system[2] aims to integrate several separate databases on science and higher education, and provide public services based on the acquired data. By the end of 2020, we will have delivered five key components, namely:

(i) Knowledge database – offers a deep search service on all data concerning science and higher education in Poland, as well as providing dynamic reports aggregating the data in the warehouse into information, which shows the underlying processes, and helps policymakers to make decisions.
(ii) Sharing data – contains several web services, sharing data either with anonymous users (open data), or authorised users (data protected by law).
(iii) Personal data – is composed of two services: the first assures that every person whose data is processed in our databases can access it; the second supports online elections for the Council of Scientific Excellence in Poland.
(iv) Metadata – publishes a description of all shared data, as well as statistics of service usage.
(v) Editing data - contains several web services for storing and editing data in our databases.

A simplified architecture of the system is presented in Figure 1. Users can use the services through a web portal, whereas information systems can utilise them using web services. A warehouse integrates data coming from several source databases. It must be noted that source systems are fed directly by the web services or their web interfaces. Then the data may be exchanged amongst them through a

[2] https://radon.opi.org.pl

data exchange model, if necessary. All services are authenticated by a central authentication module, except those which offer open data.

The personal data component includes, amongst others, a service implementing online elections for the Council of Scientific Excellence in Poland. The service is presented in detail in the following section.

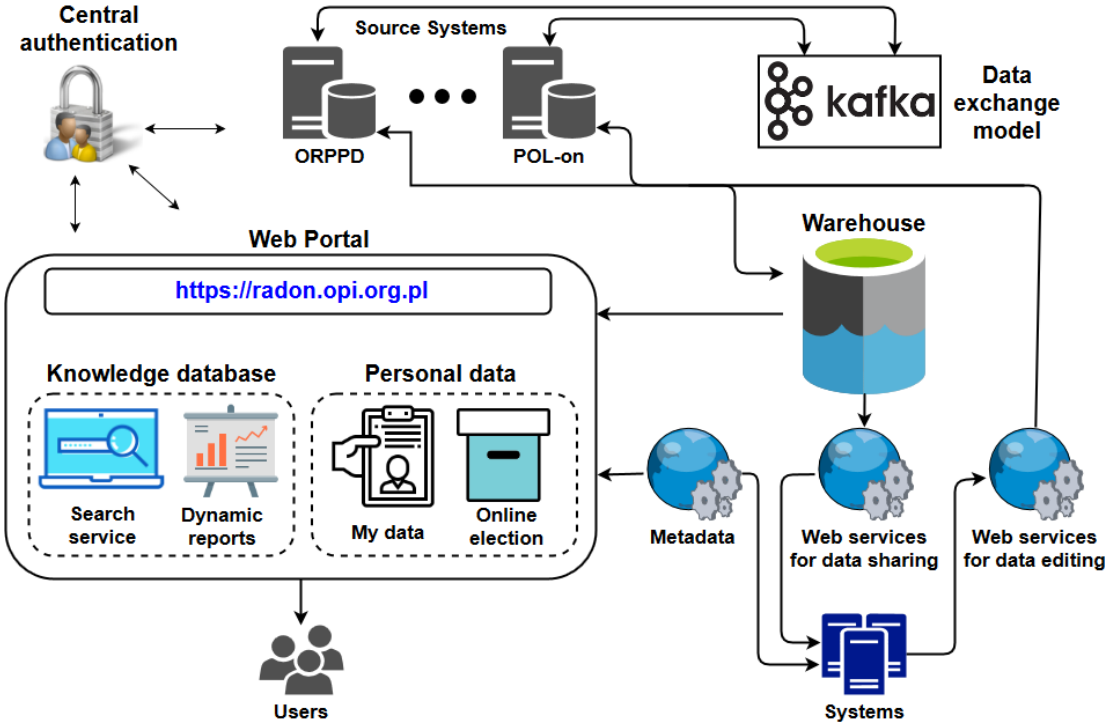

Figure 1. A simplified architecture of the Integrated System of Services for Science.

4. ONLINE ELECTION PROCEDURES

A new bill - the Constitution for Science - has been introduced in Poland, the main aim of which is to improve the quality of science and higher education. Amongst several crucial reforms, it introduces a new body, the Council of Scientific Excellence. The body's members are going to be selected in online elections to be ready for commencement of their duties in June 2019. In this section, we describe our current e-voting system supporting elections for the council of scientific excellence in Poland, which implements three phases, namely: (i) candidate nomination, (ii) electorate approval, and (iii) voting.

4.1. Nomination of candidates

Candidate nomination includes application preparation, verification of nominees, and the decision of the election committee (Figure 2).

Universities or research institutes can nominate candidates representing particular research fields. The list of institutions entitled to do so comes from our information system, POL-on. We notify them that nominations are open. The nominating institution prepares a nomination application. A nominee must sign an agreement to be formally nominated by the institution. When the application is ready, it must be signed via a qualified electronic signature, and may be sent to the election committee.

In the next step, all applications are formally validated to check whether they contain all required documents. This step includes both computer-based and manual work. Then, copies of the applications with optional notes are distributed to members of the committee, who verify the scientific credentials of nominees. Based on previous technical analysis and their own judgement, the members reach an initial verdict on each application, which may be rejected, edited, or accepted.

Finally, the president of the committee makes the final decision on each application. The president may overturn the initial decisions. If an application is rejected, there is no way to appeal or challenge

such a decision. The application may be sent back for editing, and the nominating institution has three days to correct it. All accepted nominees are included in the list of candidates. The committee approves the final list of candidates.

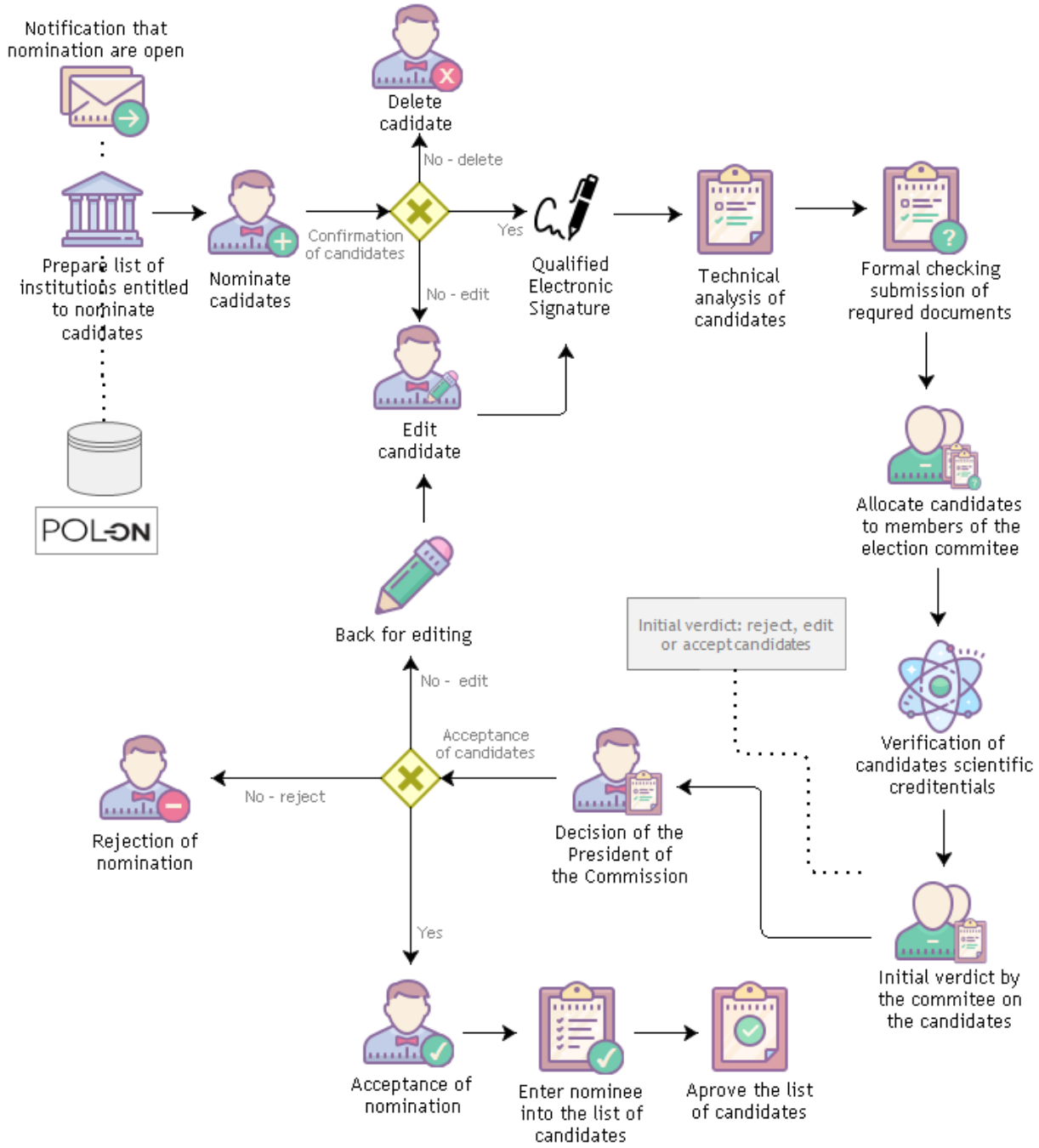

Figure 2. Process of the nomination of candidates implemented in the e-voting service of RAD-on.

4.2. Approval of voters

The service helps to establish the list of people who have the right to vote (Figure 3). The initial list is based on our databases[3][4] of researchers and academic teachers. Any person can check whether he or she appears on the list, and send an application to be added to the electorate, or to have data

[3] http:/nauka-polska.pl
[4] https://polon.nauka.gov.pl

updated. Only institutions can edit the data (name, surname, ID, email address) of potential voters whom they employ. People who are retired or without employment may be added to the list manually by our service desk, if they fulfil all requirements to become a voter. Applications of people who are not included in the initial list are also verified manually by our service desk. All users are automatically notified of the rejection or acceptance of their applications. The final electoral roll is published on the Internet approximately two weeks before the election takes place (Figure 3).

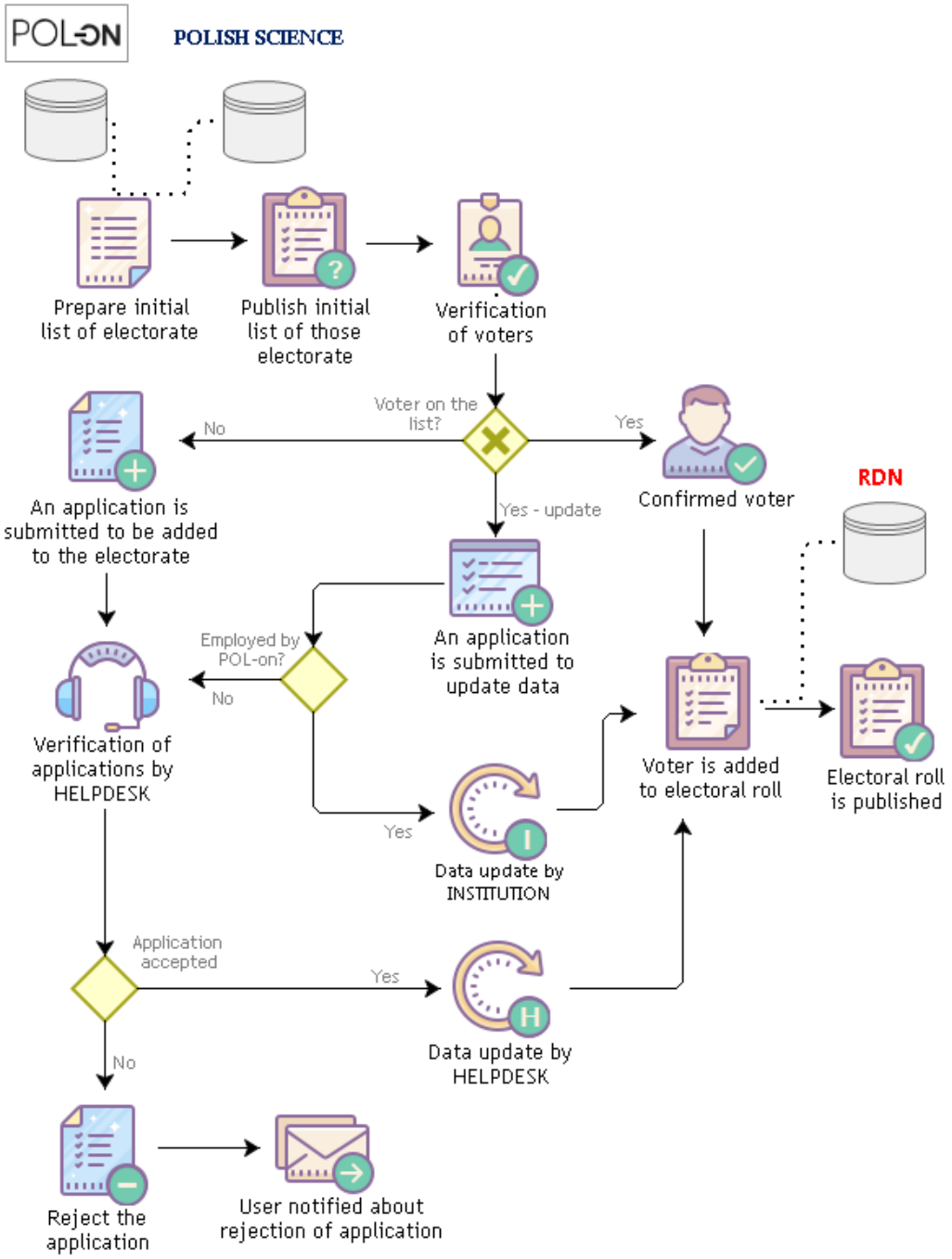

Figure 3. Process of voter approval implemented in the e-voting service of RAD-on.

4.3. Voting

The election lasts two weeks. Each voter receives a link via email to his or her personal voting card. The link is active either until he or she has voted or until the end of the election. The voter must provide some personal data in order to access the voting card. After successful verification, the voter

can fill in the ballot and vote. Voting is encrypted and signed by a blind signature. Thus, it is not possible to recognise who voted for which candidate: only the action of voting will be recorded. It ensures the security and privacy of the election for voters (Figure 4).

The results are calculated automatically immediately after the elections. In case of nominees who received the same number of votes, the winner is drawn. All elected candidates are then notified. If a successful candidate withdraws, the runner-up candidate is notified. Finally, the results are published on the Internet. By the time this article is published the election will have concluded.

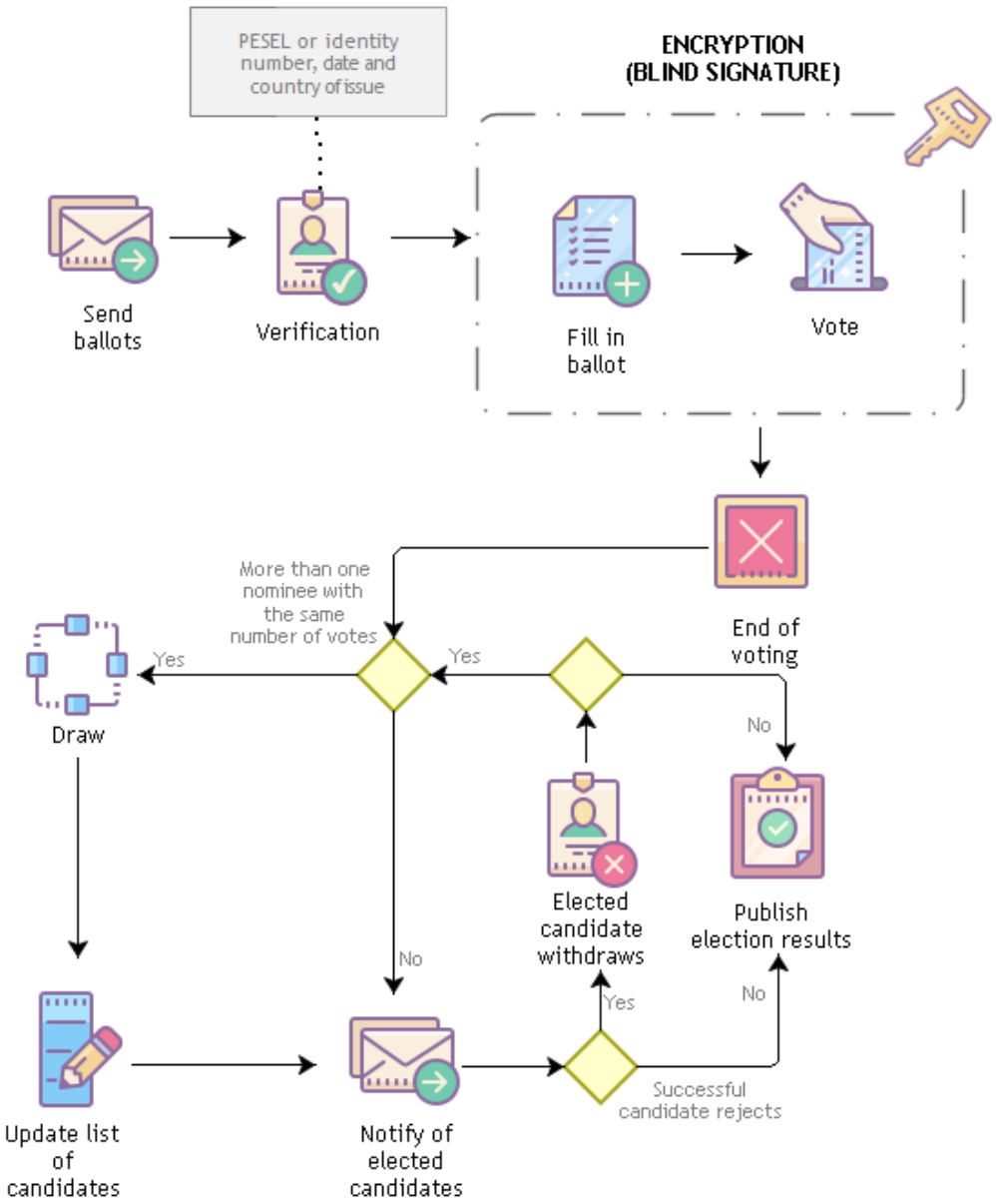

Figure 4. Voting process implemented in the e-voting service of RAD-on.

5. SELECTED STATISTICS AND OPERATIONAL ISSUES

In this section, we present selected statistics of each election phase and discuss the operational challenges which have been encountered.

5.1. Candidates

The candidates' nomination lasted from 8th February 2019 to 14th march 2019. On account of the insufficient number of nominees in two disciplines, the nomination period in these disciplines was extended by two weeks. Polish universities and other institutes nominated 477 candidates in 47 disciplines. Of those, 76% were professors and 24% were PhD holders with '*habilitation*'. Since the nominations had to be approved by university senate, which demanded additional time, the highest number of applications were acquired one month after the nomination process had opened (Figure 5).

The nomination process ran rather smoothly. That being said, some minor issues were encountered. Each application has to be signed by a qualified electronic signature. Each user was able to use a signature issued by any one of a host of providers. Some of them did not work properly depending on the version of the operating system or the web browser on the client side. Although we had prepared e-learning videos and extensive help, we were not able to communicate this information to all users. During verification of nominees it appeared that some applications were formally incomplete. Thankfully, they were able to be supplemented during the correction procedure. The verification of scientific credentials of nominees was a challenging task. For example, the applications included many typing mistakes in journal names, and we should have developed a more sophisticated checking algorithm than the simple one which we used.

5.1. Electorate

Those eligible to vote are professors and PhDs with '*habilitation*'. There are nearly 42,000 such people in Poland. From 1st March 2019 to 1st April 2019 they could verify their data on the initial list of voters or complete an application to be added to the electoral roll. Ultimately, nearly 29,000 voters were included on the final electoral roll. Figure 6 shows the distribution of people eligible to vote in respect to disciplines, degrees, and age. In contrast to candidates, nearly 66% of voters are PhD holders with '*habilitation*'. Over 40% of the electorate is over 60 years of age, and only 3% are under 40 years old. Medical and health sciences are the best represented discipline.

Voter verification is a simple technical process. The issue was how to reach each eligible person, and inform them about this. Although we informed universities, institutions, and all persons having registered email addresses in our databases directly, and made announcements in the press, some members did not verify their data regardless, meaning that they were unable to vote. We believe that the process of establishing the electoral roll must be improved in future.

5.3 Votes

Voting lasted from 12th April 2019 to 30th April 2019. Figure 7 presents the voting statistics. Approximately 60% of the electorate voted within ten hours of the closure of the election. We can observe that more voters vote at the beginning and towards the end of the election period. We did not observe the particular difficulties of users with voting. Security issues are discussed in the next section.

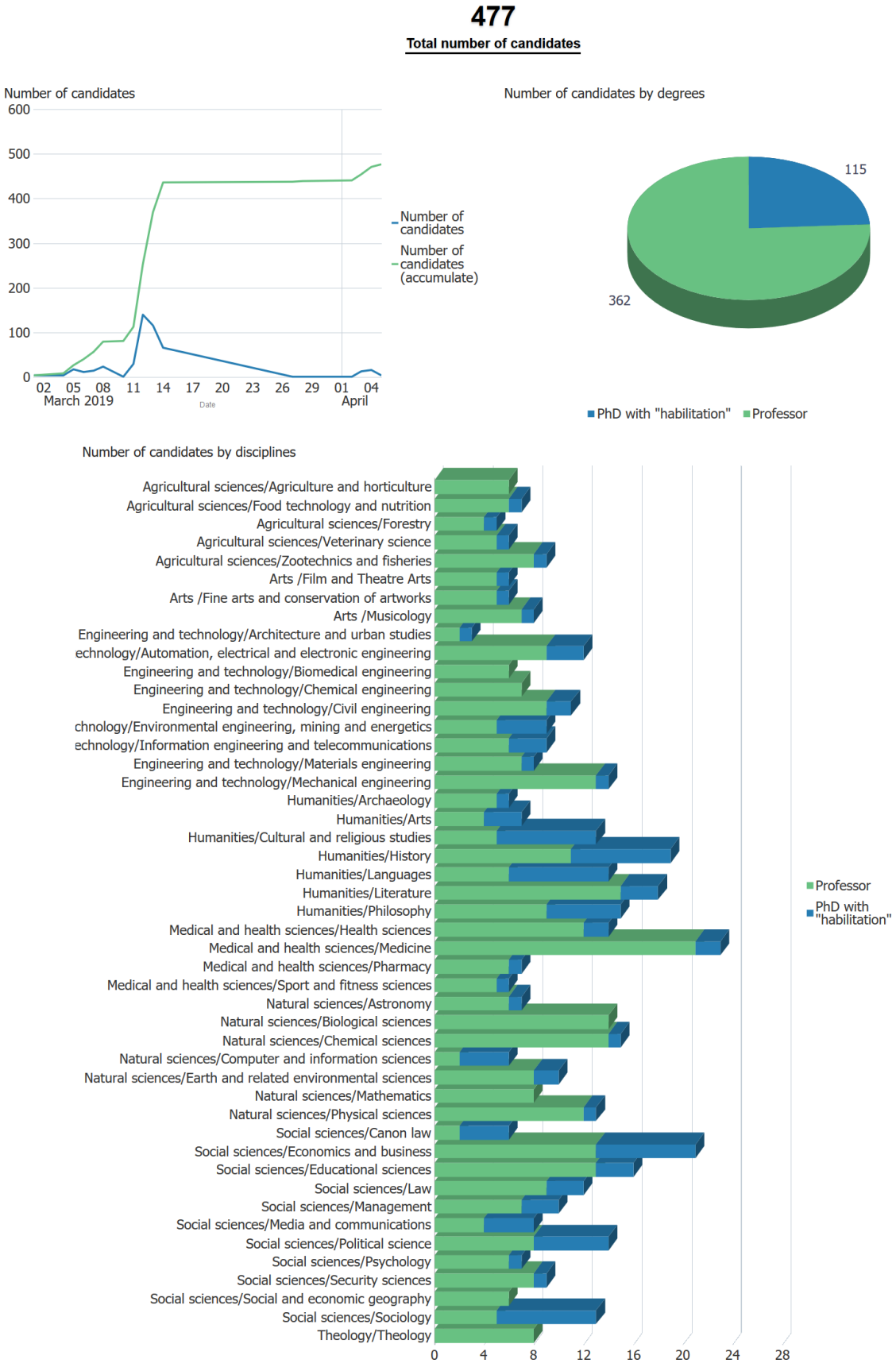

Figure 5. Nominated candidates in disciplines by division of their scientific titles.

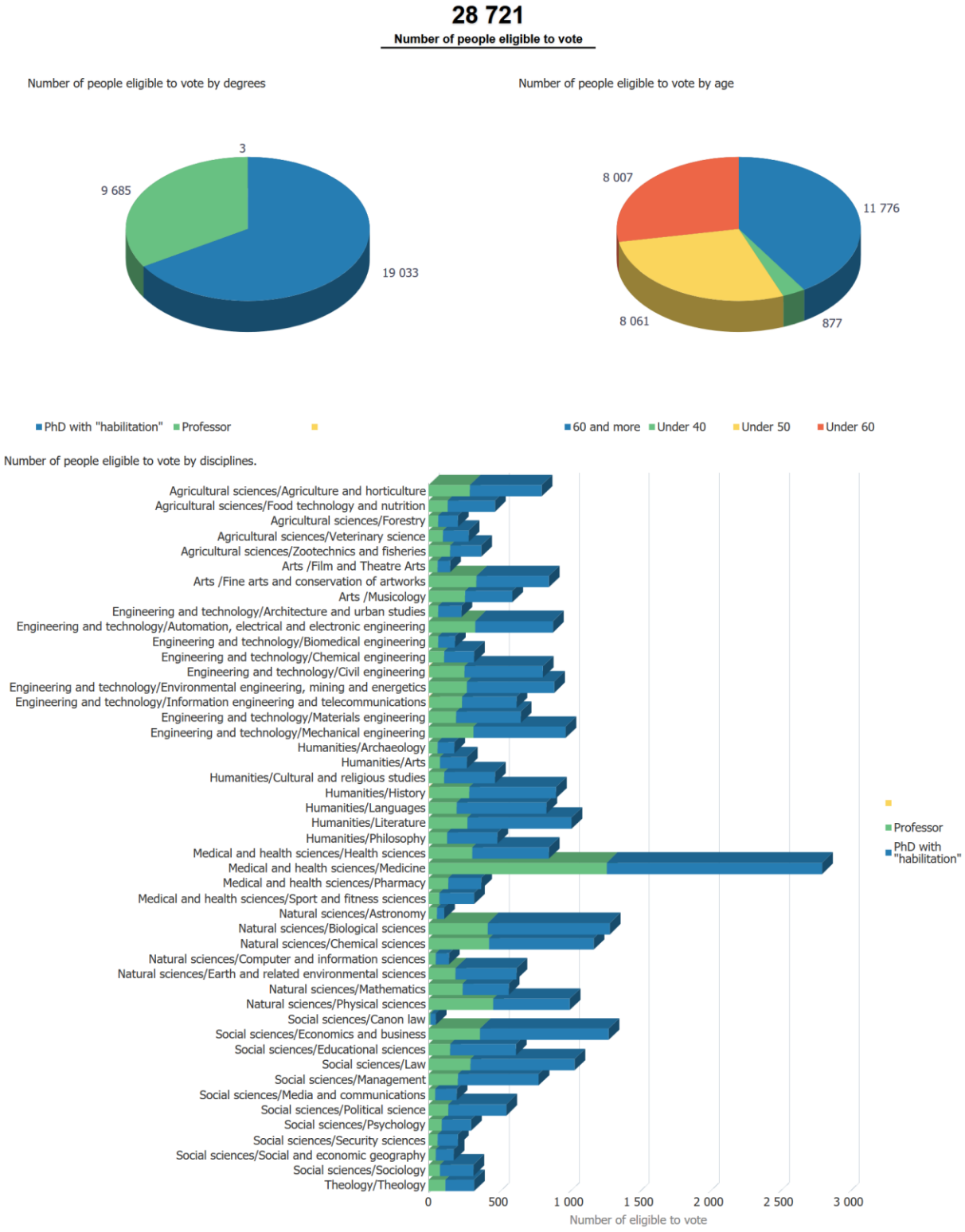

Figure 6. Electorate in particular disciplines, age, and scientific titles.

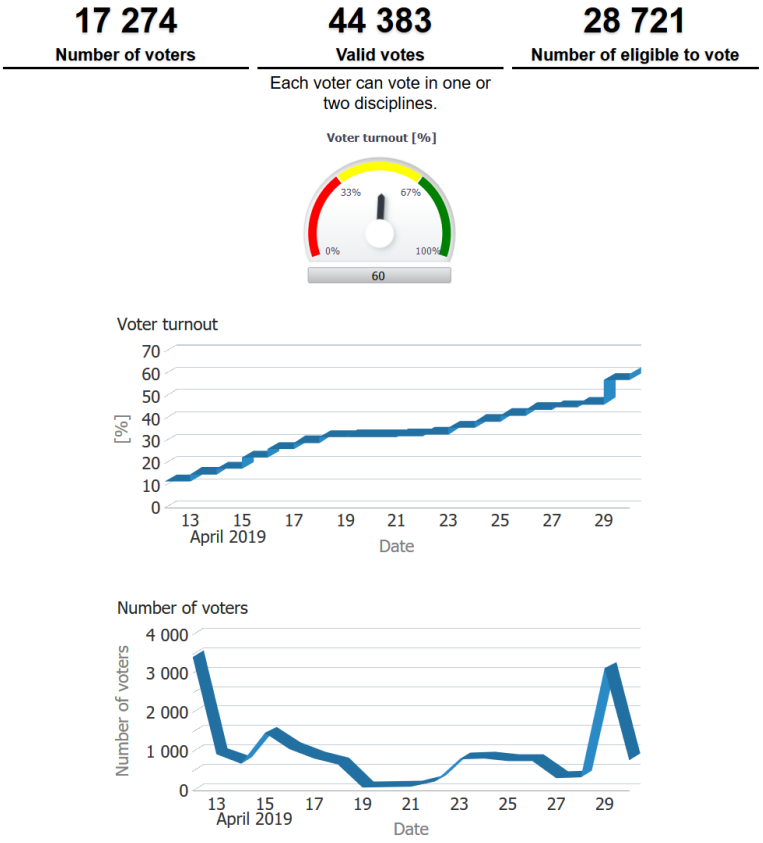

Figure 7. Voting statistics - 10 hours before the end of voting.

6. E-VOTING SECURITY

In this section, we discuss various approaches to the security of e-voting systems based on the literature. Ultimately, we demonstrate our solution, preserving the balance between safety and accessibility.

6.1. Security

There is an ongoing and long-lasting dispute regarding security and privacy, and many issues must be discussed in this section. Registration and verification of voters is a very challenging issue in the case of online voting systems. Usually, some kind of an election committee must accept a voter request for registration (Pan et al., 2012; Brightwell et al., 2015; Ankit and Divya, 2012). Voters may be authenticated using an iVote number and PIN (Brightwell et al., 2015); a login and password (Ankit and Divya, 2012); or codes sent by email and SMS channels concurrently (Gjøsteen, 2011). The most efficient model seems to be the Estonian one. Each Estonian citizen over 15 years old has an ID-card, which includes a personal electronic certificate. This solution requires a card reader. However, it is possible to use a mobile-ID in smartphones which acts as both the ID-card and its reader (Vinkel, 2011). After registration, a voting process is usually encrypted by public and private keys.

Despite undoubted successes, e-voting systems such as Helios, iVote, i-Voting, and the Norwegian voting system, are criticised for their insufficient security. The Committee of Ministers to member States have published recommendation CM/Rec(2017)5 on standards for e-voting[5] (Maurer, 2017). Alonso et al (2018) validated the Helios system in respect of these standards, with particular consideration to integrity, privacy, attacks, and fraud. They concluded that this framework is well-suited to minor elections, but do not recommend it as a system for public governmental elections. The

[5] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f#_ftn1

iVote system was partially used in a recent state general election in New South Wales, Australia (Brightwell et al., 2015). Similarly to Helios, Halderman and Teague (2015) found that iVote was not sufficiently secure. An attacker could expose voters' ballots or compromise the state election results. They suggested that this technology should not be applied to governmental elections again. Springall et al. (2014) have analysed Estonian online elections in 2013. They report insufficient procedures to handle anomalous situations; some operational security issues related to a datacentre and employees involved in maintenance of the voting system; and insufficient measures to fully assess the integrity of election results. A state-attacker or a major criminal organisation could disrupt the voting system and compromise the results. In conclusion, Springall et al., 2014 did not recommend continuing to use the i-voting system for public elections. Koenig et al., 2013 analysed the Norwegian voting system and demonstrated that voters using smartphones or tablets were vulnerable to attacks, and the SMS channel was insecure. Washington D.C. in the United States organised a trial election to check the security of the Digital Vote-by-Mail system. Wolchok et al. (2012) reported that they gained full control of the election system having the possibility to change every vote, and reveal every ballot.

6.2. Promising land of blockchain

The criticism of e-voting because of security issues incentivises us to search for other approaches. Sarker and Islam (2013) suggested using electronic voting machines which incorporate hardware and software in a single device as secure enough for public elections. They suggested this approsch for Bangladeshi pubic elections, but without any proof of its application. Although local voting machines may be helpful for election committees, they may prove inconvenient for voters, who still have to attend a voting location in person. That is why we require a highly secure online solution.

Blockchain technology is one of the most compelling recent advances in IT and demonstrates high potential in e-voting. It can be used for online voting in such a way that each voter gets a wallet with credentials and one or more coins representing ballots. The user votes by transferring the coins to selected candidates' wallets (Kshetri and Voas, 2018). Although blockchain technology is considered as highly secure, it does not solve the problem of authentication of voters on a personal level. This is an issue of biometrical identification (Yavuz et al., 2018). Despite that, some concepts of a blockchain based voting system have been elaborated (Hanifatunnisa and Rahardjo, 2017; Aved, 2017; Pawlak et al., 2018). Recently, Yavuz et al. (2018) proposed the concept of a voting system built on the Ethereum[6] blockchain platform. Its small contracts address the issues of privacy of voters, integrity, verification of votes, and transparency. Osgood, R. (2016) sees blockchain as an efficient tool for future democracy by introducing secure and transparent e-voting.

6.3. Balance between security and availability

With the above discussion about security various e-voting systems in mind, we designed the election system in such a way which preserves the balance between safety and accessibility. Based on other experiences, we had realised that it was impossible to design a system assuring complete security. Moreover, overly strict security procedures would discourage users from becoming a candidate or voter. We also do not think that the newest advances such as blockchain technology are appropriate for such a service, as the service must be as simple as possible, and users must be familiar with the technology used. Therefore, we applied simple technical solutions and relaxed the safety regime to make voting more accessible.

Our security precautions were as follows. Each voter received an e-mail containing a URL address with a unique token, allowing access to his or her voting card. Thus, the key was to have reliable email addresses of all people eligible to vote. That is why we published the initial list of voters, and they could apply for the update either to their employers or our own helpdesk. This registration was aimed to prevent anyone from impersonating another user by adding his or her own email to someone else's profile.

In order to vote, a voter had to have access to his or her email account. In addition, after activating the personal URL, it was necessary to provide some personal data. Only then could the voter fill in the ballot on a web page and submit his or her vote. In order to ensure voting privacy, we applied a blind

[6] https://www.ethereum.org

signature to enclose a ballot, and we did not log which user voted for which candidate at any point in the process. Naturally the transmission between a client machine and the voting server was encrypted.

7. CONCLUSION

We have presented an e-voting service, which was designed to support online elections for the council of scientific excellence in Poland in 2019. The service implements three phases of online voting, namely: (i) candidate nomination; (ii) voter verification; and (iii) voting, which includes ballot distribution and verification of results.

When designing the architecture and processes of the service, we decided to focus on accessibility for users to the same extent as the security of voting. The reason such an approach was that we wanted to involve as many professors and PhD holders with '*habilitation*' in the election as possible. We believe that our model has achieved that objective.

We encountered some operational challenges. For example, the process of establishing the electoral roll should be improved, and the verification of nominees should be more automated than it was. The election results will have been announced by the time this study is published. Then we cannot judge whether the election was a success or otherwise.

If we are given the opportunity to support another election, we will focus more on data verification and even better accessibility. We do not believe that such an election requires highly sophisticated and strict means of security.

8. REFERENCES

Abdelkader, R., & Youssef, M. (2012, June). Uvote: A ubiquitous e-voting system. In *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing* (pp. 72-77). IEEE.

Alonso, L. P., Gasco, M., del Blanco, D. Y. M., Alonso, J. A. H., Barrat, J., & Moreton, H. A. (2018). E-voting system evaluation based on the Council of Europe recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing*.

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), 01-09.

Brightwell, I., Cucurull, J., Galindo, D., & Guasch, S. (2015). An overview of the iVote 2015 voting system. *New South Wales Electoral Commission, Australia, Scytl Secure Electronic Voting, Spain*.

Gjøsteen, K. (2011, September). The Norwegian internet voting protocol. In *International Conference on E-Voting and Identity*(pp. 1-18). Springer, Berlin, Heidelberg.

Halderman, J. A., & Teague, V. (2015, September). The new south wales ivote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity* (pp. 35-53). Springer, Cham.

Hanifatunnisa, R., & Rahardjo, B. (2017, October). Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-6). IEEE.

Kaliyamurthie, K. P., Udayakumar, R., Parameswari, D., & Mugunthan, S. N. (2013). Highly secured online voting system over network. *Indian Journal of Science and Technology*, *6*(6), 4831-4836.

Koenig, R. E., Locher, P., & Haenni, R. (2013, July). Attacking the verification code mechanism in the norwegian internet voting system. In *International Conference on E-Voting and Identity* (pp. 76-92). Springer, Berlin, Heidelberg.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35*(4), 95-99.

Magkos, E., Kotzanikolaou, P., & Douligeris, C. (2007). Towards secure online elections: models, primitives and open issues. *Electronic Government, an International Journal*, *4*(3), 249-268.

Maurer, A. D. (2017, October). Updated European standards for e-voting. In *International Joint Conference on Electronic Voting*(pp. 146-162). Springer, Cham.

Michajłowicz M., Niemczyk M., Protasiewicz J., Mroczkowska K. (2018). POL-on: The Information System of Science and Higher Education in Poland, In *EUNIS 2018 Congress Book of Proceedings*.

Osgood, R. (2016). The future of democracy: Blockchain voting. *COMP116: Information Security*.

Pan, H., Hou, E., & Ansari, N. (2012, June). E-NOTE: An E-voting system that ensures voter confidentiality and voting accuracy. In *2012 IEEE International Conference on Communications (ICC)* (pp. 825-829). IEEE.

Pawlak, M., Guziur, J., & Poniszewska-Marańda, A. (2018, September). Voting process with blockchain technology: auditable blockchain voting system. In *International Conference on Intelligent Networking and Collaborative Systems* (pp. 233-244). Springer, Cham.

Sarker, M. M., & Islam, M. N. (2013). Management of sustainable, credible and integrated electronic voting (E-Voting) system for Bangladesh. *Management of Sustainable Development*, *5*(1), 15-21.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM.

Vinkel, P. (2011, October). Internet voting in estonia. In *Nordic Conference on Secure IT Systems* (pp. 4-12). Springer, Berlin, Heidelberg.

Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. A. (2012, February). Attacking the Washington, DC Internet voting system. In *International Conference on Financial Cryptography and Data Security* (pp. 114-128). Springer, Berlin, Heidelberg.

Yavuz, E., Koç, A. K., Çabuk, U. C., & Dalkılıç, G. (2018, March). Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-7). IEEE.

Yi, X., & Okamoto, E. (2013). Practical internet voting system. *Journal of Network and Computer Applications*, *36*(1), 378-387.

9. AUTHORS' BIOGRAPHIES

Jarosław Protasiewicz (PhD) is an assistant professor at the National Information Processing Institute and the head of the Laboratory of Intelligent Systems. He received a Ph.D. in computer science at the Systems Research Institute of the Polish Academy of Sciences. His areas of interest include agile project management, software design and development, big data, machine learning, and bio-inspired algorithms.
Email: jaroslaw.protasiewicz@opi.org.pl

Sylwia Rosiak (MSc) is a business analyst at the National Information Processing Institute. She received a Masters degree in Management at the University of Warsaw and completed postgraduate studies in designing information systems at the Warsaw University of Technology.
Email: sylwia.rosiak@opi.org.pl

Iwona Kucharska (MSc) received a Masters degree in Computer Science and Econometrics at the University of Computer Science and Economics in Olsztyn. She completed postgraduate studies in Business Processes Engineering and Business Intelligence at the Warsaw University of Technology. She has many years of professional experience as a software tester and as a business analyst, endorsed by certificates. Currently she works as a software designer and business analyst in the National Information Processing Institute.
E-mail: iwona.kucharska@opi.org.pl

Emil Podwysocki (MSc) received a Master degree in Telecommunications Systems at the Technical University of Lodz. He has 10 years of professional experience related to ETL/ELT, data warehouses and Business Intelligence. His areas of interest include Oracle technology, Big Data, Business Intelligence and data visualizations. Currently, he works as a Database and Business Intelligence Team Leader in the National Information Processing Institute.
Email: emil.podwysocki@opi.org.pl
Profile: www.linkedin.com/in/emil-podwysocki

Marta Niemczyk (MSc) received a Masters degree in Mathematics at the University of Warsaw. She has many years of professional experience as a business and systems analyst, endorsed by certificates in methods of IT systems modelling. Currently she works as a software designer and business analyst in the National Information Processing Institute.
E-mail: marta.niemczyk@opi.org.pl

Łukasz Błaszczyk (MSc) is a product owner and business analyst at the National Information Processing Institute. He earned his Masters degree in Forest Information Technology at the University of Applied Sciences in Eberswalde and a master's degree in Forestry at Warsaw University of Life Sciences – SGGW. He finished postgraduate studies in business analysis at SGH Warsaw School of Economics. He has 11 years of experience in business and systems analysis.
Email: lukasz.blaszczyk@opi.org.pl

Marek Michajłowicz (MSc) is the Deputy Head of the Laboratory of Intelligent Systems. He received a Master degree in Sociology at Cardinal Stefan Wyszyński University in Warsaw and a Bachelor of Engineering (B.E.) in computer science at Warsaw School of Information Technology under the auspices of the Polish Academy of Sciences. He has several years of professional experience related to business and systems analysis. Since 2014 he has worked as the project manager of the POL-on system in the National Information Processing Institute. His areas of interest include agile project management, software design and development, big data and warehouses.
E- mail:marek.michajlowicz@opi.org.pl;
Profile: www.linkedin.com/in/marek-michajlowicz