Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 207 (2022) 4359–4368

Procedia Computer Science

www.elsevier.com/locate/procedia

26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2022)

Keeping the secrecy aspect in mass e-voting

Grzegorz Szyjewski[a*]

[a]*University of Szczecin, Institute of Management, ul. Cukrowa 8,71-004 Szczecin, Poland*

Abstract

Two years of the COVID-19 pandemic have pushed society's digitalization forward like nothing ever before. Activities that weren't achievable without personal contact, became present online. Currently, when the COVID-19 restrictions are being lifted and personal meetings are becoming possible, in some cases, it still appeared to be more convenient to "meet" virtually than physically. Some actions proved to be more effective when performed online. That is why some people didn't want to come back to the previous form of communication anymore. Many decision-makers who see all the advantages of online communication have turned to the new possibilities that are served by Internet systems. Hence, they intend to keep it virtual even now, when pandemic restrictions have been lifted in most cases. This situation implies lots of great ideas for virtualization. One of those is online voting and polling conducted on many voters – groups larger than just board members or delegates. Such balloting could be performed using a voting system. Unfortunately, in the case of the decision-making process, which should be treated as a one-time event, using typical solutions is mostly very ineffective. Observations revealed that e-voting procedures conducted on a large number of electors may be challenging for many, not computer-experienced users. The procedure of authentication has to stay present in order to protect the votings against ballot stuffing. Particularly in secret voting, the problem remains the same: how to verify the user for a secret ballot without revealing his data. In mass voting, additional issues appear such as how to complete the procedure on multiple (often not ICT-experienced) voters and how to make the system accessible and credible at the same time.

Keywords: e-voting secrecy; ICT system; mass voting; balloting; confidentiality; online system credibility.

* Corresponding author.
Email address: grzegorz.szyjewski@usz.edu.pl

1877-0509
10.1016/j.procs.2022.09.499

1. Introduction

The COVID-19 pandemic has forced people to limit radically their close contacts. In order to stay safe people needed to stay isolated and were forced to move the majority of their activities online. Now when COVID-19 seems to be less dangerous, due to the vaccinations and virus mutations, some activities still remain to be conducted online. The reason for that situation is that in some cases it appeared to be more convenient to "meet" virtually than physically. Two years of the pandemic have pushed society's digitalization forward like nothing before [1][2][3]. Things that weren't achievable without personal contact, became present online. For some of the activities or services provided, the conversion was easy and quite natural. A good example would be teaching and learning, where in some cases those actions have already been performed online, but were not as popular, as standard classroom meetings [4]. Also, everyday business contacts appeared easy to be kept in the virtual world [5]. Some services had to adapt to the new electronic environment existence. A worth-mentioning example of such rapid evolution would be public administration in some countries, where e-administration wasn't well developed yet [6]. It turned out that a citizen is not obliqued to visit the office to deal with an official matter. In many cases, paper documents used before were easily replaced with their electronic version. Also, citizens' declaration of will began to be accepted when submitted using e-mail or another electronic form. Some activities were not able to exclude personal contact entirely and had to stay conducted traditionally. An example may be extended medical examinations or surgical interventions, which just couldn't have been virtualized. Of all of those activities, some of them proved to be more effective when performed online. That is why some people didn't want to come back to the previous form of communication anymore [7]. They see all of the advantages of online communication, which are mainly: time-saving and accessibility.

Additionally, some decision-makers have turned to the new possibilities that are served by Internet systems. They started to observe that lot of other actions could have been performed online earlier because it's more convenient. So they intend to keep it virtual even now, when pandemic restrictions are in most cases lifted [8]. This situation implies lots of great ideas for virtualization, which should be further well designed within the business processes and adopted into ICT systems to keep them safe and accessible for end-users. One of those activities is online voting and polling conducted on many voters – groups larger than just board members or delegates [9]. Such balloting could be performed using a voting system that supports secret and open elections. Unfortunately, this kind of election or decision-making process must be treated as a one-time event only. Though it was performed again, the poll list would be probably different, due to a large number of electors and natural people rotation within the organization. That is why keeping and reusing voters' authentication keys for the next election would be unreasonable.

2. Secrecy of the ballots

The procedure of keeping online balloting secret, with an anonymous token approach, has been already described in another article [10]. Such a voting system may be effectively used for voting in a group of not more than 150-200 people. Former observations revealed that the procedure of voters' individual keys assignation that keeps voting entirely secret, may be challenging for some not computer-experienced users. That issue may be solved with quick user support, to guide them through the process. Unfortunately, it becomes inefficient when it comes to serving a large number of voters, entitled to take part in an election. The problem remains still the same: how to verify the user for a secret ballot without revealing his data. Considering that the previously described procedure of anonymous token and user identity separation may not be used, due to the possibly large number of individual issues, a new modified approach should have been taken. It was designed for a greater number of voters, to enable them to cast a secret ballot unaccompanied and without the need for additional assistance. Even if the voter is not a computer-experienced person.

To keep the terminology uniform, in this article the names defined by the U.S. Election Assistance Commission in the "Glossary of Election Terminology" were mostly used [11]. The research describes a solution designed and implemented as a reaction to a need stated by a medium-size commercial organization in Poland. This need was probably the result of a change in the approach to virtualization, described earlier as a positive effect of the COVID-19 pandemic. The idea was to provide a solution for mass voting (decision making), concerning that the election system should be ready for both: open and secret balloting. Additionally, the system should have been accessible for all different types of electors from blue-collar workers, to IT-experienced office employees. In this particular research, additional guidelines set that all entitled to vote have been registered in the organizations' database prior the voting.

One of the key factors in the authentication process was that the elections administrator could verify each elector using previously exchanged and stored pieces of information. Every single individual in the organization was identified with his organizational id number, which was known to him, and was often used in an organizational environment. The second element that could have been used in the process of authentication and verification, was a personal cell phone number, assigned to each person on the voters' list. Those two elements allowed for designing an easy to proceed scheme of authentication, used during vote casting that prevents unauthorized voting and ballot stuffing.

It is also worth determining the ballot's exact secrecy level applied in the research. U.S. Election Assistance Commission defines secrecy of the ballot as: "a set of rules and procedures to establish the fundamental right of voters… to cast a secret ballot". Following the definition, the most important aspect is to: "ensure that no ballot can be associated with a voter". This requirement was entirely fulfilled in the procedure described in the earlier approach. Unfortunately, that procedure was not appropriate for a large number of voters, hence had to be modified to be less challenging, especially for less experienced users. Returning to the secrecy definition, it has to be clearly stated, that simplifying the voting procedure required to harm the secrecy level anyway. The research aim was to find an optimal balance between accessibility and voting confidentiality. Reducing the level of secrecy meant that it will not meet all the requirements stated in a definition anymore. That is why the term "secrecy" was replaced with "confidentiality". Such terms as confidential polling were not defined in the U.S. "Glossary of Election Terminology". For this research, the following was presumed: a ballot that has been cast by an entitled elector and may not be easily associated with this person. It means that there is some way to rebuild the relationship between a vote and the voter, but it is not available for everyone, especially for authorities who organize an election. Recovering the connection between the choice and the person who made it, requires deep studies on the different datasets which are available only to the system owner. Such a person or organization becomes a trust institution because potentially has access to all data that enables recovering electors' choices. Under any circumstances, he may not try to find out who has cast particular votes. The difference in meaning between "secret" and "confidential" voting might be misleading, that is the reason why it has been explained as a part of an article.

There are numerous polling/voting IT systems available on the market and most of them are defining themselves as secret balloting prepared. In many cases that is not true, because procedures used in those systems are not meeting the secrecy definition at all. It is obvious that the results are not showing the relation between the elector and the ballot directly, but there is a simple way of challenging the system to find out if it is actually ensuring voting secrecy. First of all, guaranteeing secrecy in ICT is not easy [12][13]. In traditional voting, everything is mostly transparent. There is a paper ballot that before fulfilling is exactly the same for each elector. Only a completed ballot becomes personal and must be protected against disclosure. When it is placed in the ballot box it becomes secret again, because there is no easy way to connect the voting card with the person who placed it in the box. It means that the only way of revealing voters' choices is to see the mark on an official ballot, while it is kept by its owner. Unless there aren't any frauds like ballot marking or disallowing voters to mark their ballots freely without any assistance or supervision, it is almost impossible to reveal the connection between a person and the ballot. Contrary to electronic voting, where the elector can control only the front-end of the system. It is quite clear that taken actions (including elector identification) may be stored at the system back-end and reused to reveal the choices the elector made. That is especially when a user account is used as a system authentication tool. So if the ICT system can show to the particular user the choices he made in secret elections, it means that somehow it can still create a connection between the vote and the voter. Such a situation is the best proof of the system's unreliability because it shouldn't be able to present that information. Even to the person to whom it legally could have been presented. Therefore, if the secret balloting system enables the voting history, based on the user account authentication, that means it does not meet the official secrecy definition.

The verification and authentication procedure for secret or confidential balloting is crucial because in its principle those two aspects are contradictory. Keeping something anonymous means that a person is unrecognizable, although he or she made some actions on their own. In contrast, the authentication process consists first of revealing and confirming someone's identity, then confirming that the person is authorised to take a specified action [14]. To find an optimal level between those two opposites, there is a rate of accessibility that determines the ease of use and also voters' confidence that their ballot choices were recorded correctly. When conducting undisclosed voting the most important objective is to prevent ballot stuffing. That is a matter of authentication to allow ballot casting only to the people entitled to vote, from the registry of electors. Keeping the secrecy of the ballot must be ensured on the level

that voters accept to be strong enough, that they can mark their ballots freely, without fear of repercussion or reprisal. Concerning the second-mentioned element, the right balance between these two opposites should be kept.

3. Research environment

To design and provide a multiple voters election system, an individual balloting procedure was used. The procedure was based on the fact that the election organizer and people entitled to vote knew each other before. It meant that the organizer had enough data to proceed with user verification properly, without additional documents that prove the voters' identity. Exchanging and securing trusted data between the transaction parties provides a possibility to use it as an authentication key in further electronic communication. It means that the multiple users may be identified and verified remotely, without any further preparation and additional credentials exchange. The level of security for authentication procedures should be equal to the transaction significance or straightforwardly to the possible level of harm that could be done by proceeding with a transaction in an unauthorized way. In this particular example, of a multiple voting election system, the transaction had to be secured very properly. It was assumed that the most significant transactions will be workers union authorities' elections. That is why the voting/polling was designed as a set of traditional balloting procedures and authentication similar to an online banking transaction approval [15].

The procedure of vote casting was secured on two different levels. The first was authorizing general access to the voting list and particular voting content. Second, was dedicated to ensuring the credibility of a single vote registered in a system. Such an approach created a two-factor authentication. The first level allowed users only to read the content, and the second to take action like submitting a valid vote. Such an idea was not necessarily implemented to raise the level of security. It should be treated more as an additional function that verifies if a user possesses all the tools that are required for the procedure execution. So the first level of authentication was meant to identify the user as a valid voter, who exists on the poll list. It was also needed to check if the user knows his company's identification number which was used as a primary key that identifies voters in the system. Finally, that stage of authentication was to confirm that the user knows the cell phone number that is assigned as his individual contact phone number. All of these have automatically created the first stage of authentication, which ensured that any person who isn't entitled to vote, will not be able even to preview the votings list or the votings content.

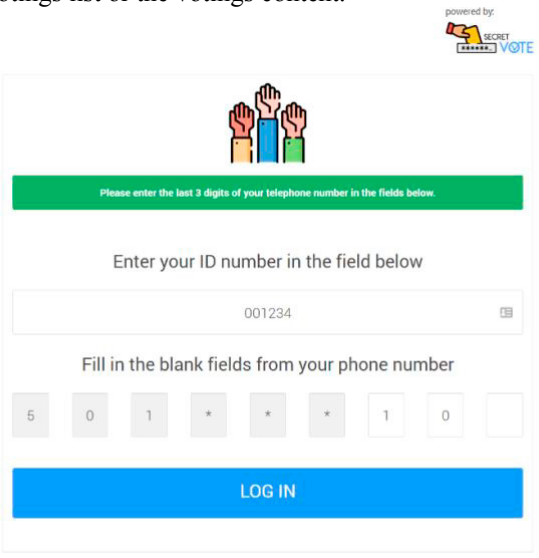

Fig. 1. User verification is based on phone number gaps filling.

The first stage of the authentication procedure assumes that the user should introduce himself to the system, using his individual company's identification number. In this particular environment, where the research was conducted, such a number is assigned to each employee of the company. It is used very often to identify people for multiple

purposes like documents or cases delegation, resources assignment or other HR procedures. The ID consists of 6 digits and to fill all 6 spaces small numbers are predeceased by zeros e.g.: “107634” or “005987”. Considering that the system should be accessible also for not computer experienced people, an additional script that automatically converts the lower numbers to their full versions was applied. So when a user inputs his ID number like “4421”, it automatically appears in an input field as “004421”. For ICT users it may be surprising, but observations showed that such a small change may be a massive improvement in systems accessibility. When the ID number was typed in and sent to the system it has been checked with the poll list to validate if the voter is eligible. If not or in case of any other issue, a user was informed with the alert displayed accordingly to the error event. If the input has been correct, a second screen was displayed. At that stage, the user was obliged to verify if this ID number belong to him. To accomplish that step he had to fill the gaps in the cell phone number, that was officially assigned to the given ID. Polish cell phone numbers structure consists of 9 digits, so the first 3 were displayed on the screen, another 3 were masked, and the last 3 were supposed to be given by the user to verify his identity. 3 digits indeed give only 1000 possible combinations which is not a strong key, but after each failed attempt the procedure was started over and in addition, it was also secured with a captcha mechanism. Concerning that both: the ID and phone number were given correctly and identified user who was allowed to vote, he was redirected to the active votings list. If only one voting at the time was open the list was skipped and users were moved directly to the active voting content. That is another tiny improvement, that makes a big change for not experienced users. At that stage of the procedure, the user was allowed to read the voting contents and see what are the available choices (options). This set of information may be treated also as a preview-only option, which gives a variety of possibilities to enable it outside the company to other authorities.

4. Anonymous authentication for e-voting

Described verification isn’t strong enough to secure the whole voting. The two keys used for authentication are not entirely secret and probably some people may know the ID and phone number of the friend or other person in the company. Moreover, the authentication procedure provides an access to the closed area, based on a link that includes a passkey, sent as a GET variable. That link could be easily copied and used by another person. So this stage of verification should be rather treated as a pre-authentication because it does not secure the voting procedure accordingly to the operation significance. On the other hand, such a method allows providing the secured link to the votings list and votings content for people who may be the authorized observers. The link provides read-only access so in some cases it may be also treated as a useful additional functionality of the system. The actual ballot registration was secured using the method known from other online services and is probably most recognized as a bank operations authorization.

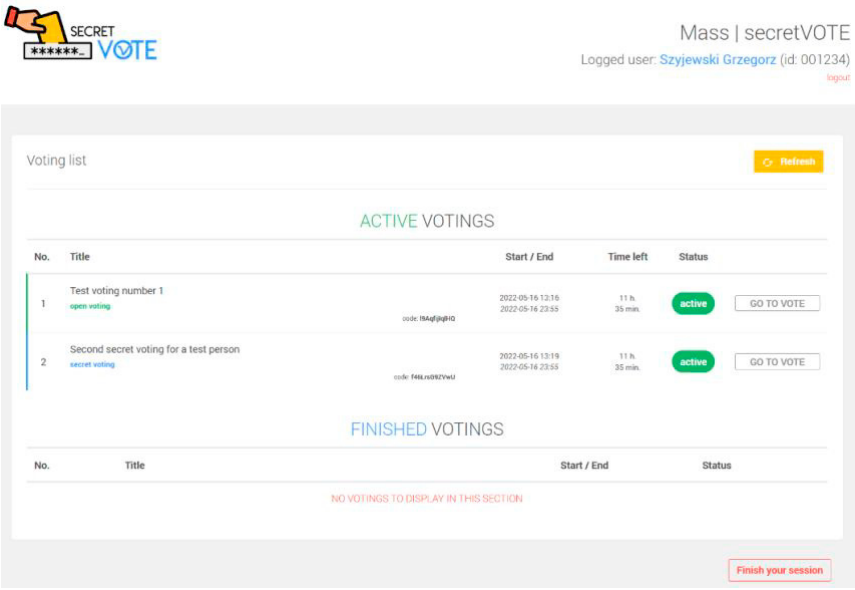

Fig. 2. Users voting interface after successful login.

After successful proceeding with the first level of authentication, the user was allowed to see the active votings and also get into each of them to place his vote. The voting interface itself was made as much similar to the standard ballot as possible. Putting aside regular elements like voting content and available options that may be chosen, there was some more useful information displayed to the user. First and the most important was the type of election that the user is taking part in. It could have been confidential or open voting. The first one was marked with a blue and the second with a green badge. Such an approach allowed the user to immediately realize if his choices will be published or kept confidential. Another useful element was information if the voting allows choosing only one or more (and how many) of the available options. The first condition is used for single-choice voting like being for or against something. The second is commonly used when choosing more than one option from a given set. It may be a list of candidates or other options from which voters are choosing those that convince them most. The result of such multi-option voting is a ranking list, where options are sorted from the most to the least popular one. In both types of voting, the list of the possible choices was also automatically extended with an option for those who want to abstain from voting in this particular election. If such an abstention was selected all other choices (selections) in the voting were cleared. The voting screen has also some more technical information like when the balloting was started and when will be finished or how many electors are entitled to vote in an election. The system was also equipped with a validation mechanism, that does not allow users to select more options than it's allowed to, or not to choose any of the options (except abstention). The voting screen was made as clear and lightweight as possible to make polling easy. Except for the verification elements that validate just voting choices, the most important element of voter authentication was also included.

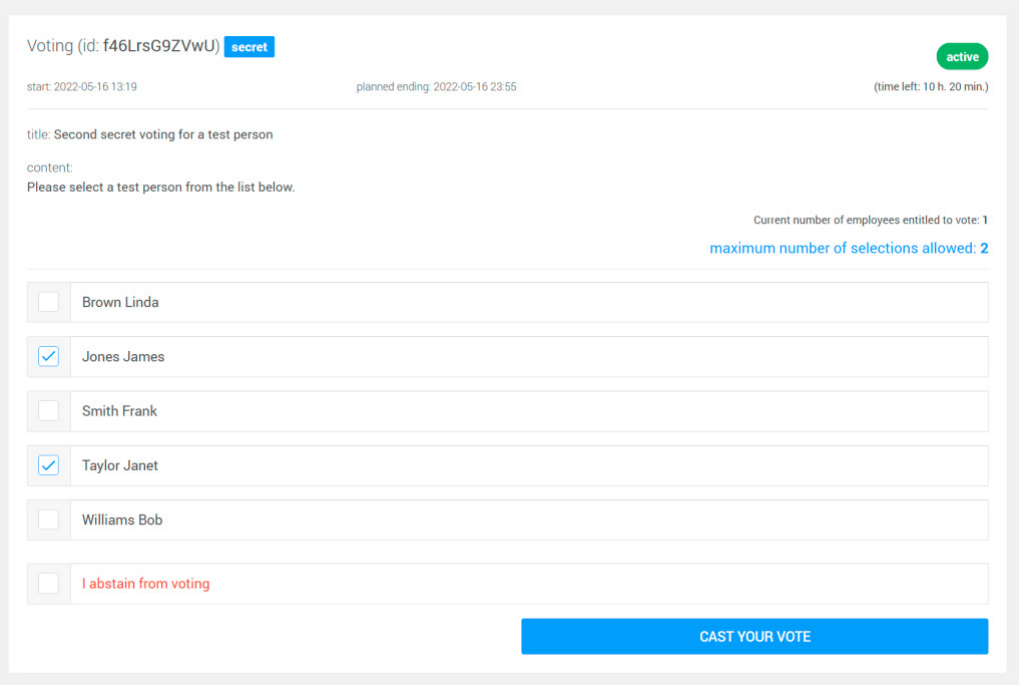

Fig. 3. Balloting screen for secret voting.

The component of user authentication was designed in the process between ballot choice selection and ballot casting. It runs automatically when the user clicks the vote submission button and all given data were properly validated. The screen for the voter and his ballot authentication operation displays only one input field, where the elector is obliged to input an individual secret code, that was sent to his cell phone number as a text message. The code generation and sending procedure is initiated automatically as a background process, so the user is mostly getting the code immediately after the verification screen was displayed. Sometimes due to the increased number of SMS server transactions, it may take a while for the message to be delivered. The SMS code is valid as long as a current voting session. If the user makes a mistake when entering the code, he gets a notification on the screen and he may correct it. During the whole voting session (for a single election) the same code may be used. A new authentication code is generated and sent to the user only when the whole balloting procedure (including the first stage of verification) has been started over. After submitting a valid SMS code, the ballot is saved in the database and the user is marked as the one who has already cast his vote in this particular voting. After getting back into the active voting preview, the elector may see the choices he made, but only for the open votings where the link between the vote and the voter is not undisclosed. For confidential votings, the only information displayed is that the voting for the particular user is finished. When the elections are finished, by entering the voting, the user may preview the final results.

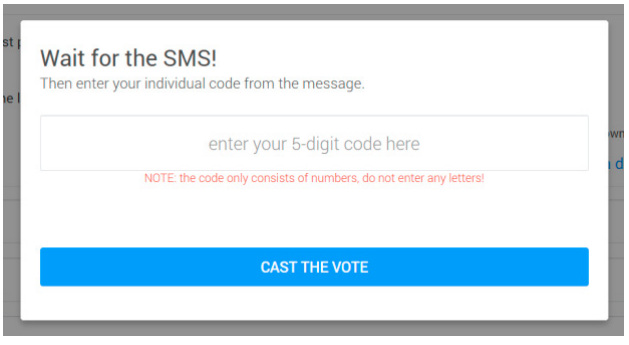

Fig. 4. Final ballot confirmation with SMS code.

The elector's system acceptance requires not only an option of marking their ballots freely and confidentially but also the capability of ballot verification. It is not an issue for open voting where the result shows clearly who voted for which option and how many votes were recorded. The result verification becomes more difficult when such an association between people and their choices may not be revealed. To meet all the requirements for high balloting system acceptance within the electors, some additional approach was taken. The result of confidential voting is displayed not only as a number of votes earned by each option but also as a list of SMS codes that were used to authenticate the ballot. Assuming that each code was individual and was provided only to the phone number of a single elector, it may be used as a post-voting verification key. The code itself becomes unuseful for taking further action like casting an additional ballot when used once. But it still remains as a valid key that may be used for anonymous check, if the ballot was assigned to the right option or was recorded in the closing result at all. Assuming that every single voter may confirm the choices he made by finding his secret code on the list, all electors composed may verify the whole voting result. What is more important, they can easily do it without revealing their ballots so the elections remain confidentially. That aspect ensures more credibility and rises the acceptance rate of the system. Voters are assured that the balloting was conducted fair, and the results cannot be questioned because each person may easily verify them.

An additional aspect that should be mentioned is voter turnout, which is low in many cases. That creates a huge problem if the election requires a specified quorum, which typically is at least 50% of electors entitled to vote. If the turnout does not reach at least half of the entitled voters, the whole election result may be not valid. The electronic voting system makes the whole process of casting a vote easier and more accessible. People may vote from any place using personal devices. The only requirement is Internet access, which generally now is not a difficult condition to meet. Additionally, election organizers may provide voting stations, which are just freely accessible terminals where people may access a voting system. All of the above including high system acceptance of the users is a great prerequisite for increasing voters' involvement in elections. That is another reason why mass elections should be conducted in an electronic form.

The system was implemented in a Polish unit of a company which is a global provider of renewable solutions in packaging, biomaterials, wooden construction and paper. The company requested a solution that improves elections or less demanding poolings within its employees. The open voting or as called “pooling system” was not a challenge, because the only difficult element was an act of multiple voters verification, with the use of existing data, to avoid the necessity of authorizing key distribution in this quite extensive environment. Keeping the mass e-voting secret or relatively, as it was explained earlier, confidential required an individual procedure implementation. The final procedure was an effect of cooperation between the company and an author who made this research and prepared a fully functional online system. Before its first use, this solution was tested on multiple levels. The most demanding, but also the most improving, was the stage of beta-testing. The system has been thoroughly examined by workers’ union representatives, who reported multiple issues that may harm the system acceptance of final users. After that stage, several corrections and changes were applied and the system was put into production. As a final test, the company conducted some elections and poolings on a group of about 1700 employees. The system acceptance and, at the same achieving the research aim, has been confirmed with a high level of employee involvement. The voter turnout appeared to be much better than it was during the traditional votings conducted in the same environment before. People were able to vote anytime (within a given period) and from any device that has an Internet connection. Voting procedure simplicity combined with small improvements implementations that support less computer experienced users, turned out to be a correct approach for mass e-voting solution. The possibility of the publication of the results immediately and automatically after the voting is finished, definitely raised the level of trust for new technologies. Using such tools in times of the greatest pandemic threat was compulsory. But the success of described digital approach for conducting secret elections when the traditional way of voting was also available, means that the aim was fully achieved.

5. Conclusion

Keeping secrecy of the elections conducted using an online system is not easy. Making the system credible for the users is even more difficult. But convincing mass users that online systems (that often is incomprehensible to them) are safe for anonymous voting is the most difficult issue. The presented approach may be successfully applied to other similar mass e-voting surroundings. The only difference that may appear and must be solved is a type of information that is used as a verification and authentication key. It may be changed for different situations and organizations, depending on the data that were already exchanged between the voters and the election organizer. High system acceptance noticed for the given approach, showed that COVID-19 restrictions convinced many people that electronic communication is more efficient than a traditional one. What is more, it appeared to be also as easy or even more achievable, even for not computer-experienced people. Of course only if the procedure and chosen tools are well developed and adapted to the environment in which it operates. This research showed that even such complicated operations as keeping the confidentiality of votes in the computer system, as well as successful conducting balloting, with a high acceptance and trust of multiple users, is possible. It requires only a deep study of the situation and requirements, designing the optimal procedure afterwards, and finally, its' implementation in an online system. When it's ready, applying multi-level testing allows for improving the product, to meet people's expectations. The current post-pandemic time is a great occasion for such modern approach applications. Now it may be called only an occasion, but upcoming years and unpredictable future can change it into an inevitable process and the sooner the process is undertaken, the less severe the consequences of future events will be.

Acknowledgements

The project is financed within the framework of the program of the Minister of Science and Higher Education under the name "Regional Excellence Initiative" in the years 2019-2022, project number 001/RID/2018/19, the amount of financing PLN 10,684,000.00.

References

[1] Manalu, Muditomo, Adriana, Trisnowati, Kesuma, and Dwiyani. (2020) "Role Of Information Technology for Successful Responses to Covid-19 Pandemic." [online] IEEE Xplore.

[2] Sylqa, Neziraj. (2022) "The Relation Between Organizational Learning and Information Technology in Companies with International Activities During the Covid-19 Pandemic." Quality-Access to Success 23(186).

[3] Tortorella, Guilherme Luz, Gopalakrishnan Narayanamurthy, and Paulo A. Cauchick-Miguel. (2021) "Operations Management teaching practices and information technologies adoption in emerging economies during COVID-19 outbreak." Technological Forecasting and Social Change 171(120996).

[4] Benty, Kusumaningrum, Santoso, Prayoga, Ubaidillah, Rochmawati and Wardani. (2020) "Use of Information and Communication Technology in Leaming in the Covid-19 Pandemic Period to Improve Student Learning Outcomes." 6th International Conference on Education and Technology (ICET).

[5] Vardari, Bytyqi, and Lumi, (2022). "The Impact of Information Technologies on Business During the COVID-19 Pandemic Outbreak." Managing Risk and Decision Making in Times of Economic Distress, Part B:143–158.

[6] Tavares, Joia, and Fornazin, (2021). "Digital Transformation Initiatives in Public Administration During the Covid-19 Pandemic in Brazil: Unveiling Challenges and Opportunities." Lecture Notes in Computer Science: 16–28.

[7] Dwivedi, Hughes, Coombs, Constantiou, Duan, Edwards, Gupta, Lal, Misra, Prashant, Raman, Rana, Sharma, and Upadhyay, (2020). "Impact of Covid-19 pandemic on information management research and practice: Transforming education, work and life." International Journal of Information Management, 55(102211).

[8] Barrutia, and Echebarria, (2021). "Effect of the COVID-19 pandemic on public managers' attitudes toward digital transformation." Technology in Society, [online] 67.

[9] Lola, Eugene, Hall, and Gilbert, (2013). "Balloting: Speeding Up the Voting Process." Communications in Computer and Information Science: 373–377.

[10] Szyjewski (2021). "Conducting a secret ballot elections for virtual meetings." Procedia Computer Science, 192: 4448–4457.

[11] www.eac.gov. (n.d.). Glossaries of Election Terminology | U.S. Election Assistance Commission. [online] Available at: https://www.eac.gov/election-officials/glossaries-election-terminology [Accessed 5 May 2022].

[12] Qureshi, Megias, and Rifa-Pous, (2019). "SeVEP: Secure and Verifiable Electronic Polling System." IEEE Access, 7: 19266–19290.

[13] Cranor, Cytron, (1997). "Sensus: a security-conscious electronic polling system for the Internet." [online] IEEE Xplore.

[14] Bailie, Jortberg, (2009). "Online learner authentication: Verifying the identity of online users." Journal of Online Learning and Teaching 5.2: 197-207.

[15] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo and Hoon Jae Lee (2010). "Online banking authentication system using mobile-OTP with QR-code." [online] IEEE Xplore.