



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.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.



25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

# Conducting a secret ballot elections for virtual meetings

Grzegorz Szyjewski<sup>a</sup>

<sup>a</sup>University of Szczecin, Institute of Management, ul. Cukrowa 8, 71-004 Szczecin, Poland

## Abstract

Communication plays a crucial role in business, education, and generally in everyday people's interactions. Face-to-face communication has been banned by the COVID-19 pandemic restrictions and had to be replaced with its electronic remote form. Popular digital applications allowed us to switch to online life quite easily. That conversion wasn't problematic for most (especially young) people. Working online and meeting people virtually became a standard, and people have mostly adapted to the new reality. Moving conventional communication to the Internet wasn't much challenging, because it was only a matter of existing ICT solutions popularization. They have already existed and were functional, but haven't been used much often. COVID-19 pandemic changed it permanently because there was no other way as rapid adoption to this unusual situation. Although most of the actions could have been realized online, some were more problematic to conduct electronically. One of them was secret balloting for virtual meetings. As open voting was not much complicated to arrange using remote communication, conduction the secret type of elections was not so obvious. In open voting electors' data can be revealed and the results may be easily verified when it's finished. Secret voting demands to remain voters' data and their choices confidential. That leads to the question of how to verify the users' identity and voting rights and keep them anonymous at the same time? This paper provides an overview of a person's remote identification and verification methods, also explores the possibilities of using them for secret voting authentication. Results show that conducting a secret ballot with remote voter authentication is possible. The method was widely described and also applied in a authors' digital system. A fully functional ICT solution has been tested in real elections across several organizations in Poland, in which present authorities were elected electronically during the COVID-19 lockdown period.

© 2021 The Authors. Published by Elsevier B.V.

This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0>)

Peer-review under responsibility of the scientific committee of KES International.

*Keywords:* virtual voting, secret ballot, electronic election, digital system, COVID-19 pandemic, remote communication.

## 1. Introduction

The Pandemic has upended human lives across the globe. The way people live, the way people work, and most importantly the way they communicate. It is not a matter of language or words, but the communication channel that is used to pass the information. From day, to day personal meetings and the same personal conversations were replaced with virtual substitutes [1]. This change was forced upon the pandemic situation caused by coronavirus SARS-CoV-

2. COVID-19 used further in the article, is the name given to the disease associated with the virus. The virus has spread dynamically from China to all countries around the world [2], affecting, overloading, and even destroying national healthcare system capabilities. The crucial fact was that the virus spreads across people, increasing the number of affected individuals every day. The only possible option to slow down the infection boost was social distancing [3][4], which meant personal contact restrictions. To support or even force social distancing, most countries announced lockdowns and people had to stay at home. Although all face-to-face meetings were limited, everyday private and business activities had to keep going. The only way for rescue was virtualization, so almost all activities that required personal interaction moved to the Internet. As a consequence, schools pushed out teaching activities to e-learning systems [5] and offices to virtual meetings and remote communication [6]. Working from home became a common way of business performance and phone or online meeting applications the main communication channel [7]. Fortunately, that switch wasn't hard to proceed, because all information and communication technology (ICT) tools have already been in place, just weren't much popular compared to face-to-face meetings [8][9]. A new technology that uses electronic communication became one of the biggest beneficiaries of the pandemic. People were enforced to start using remote communication tools because without them they wouldn't be able to cooperate. Almost all actions demanding interpersonal interaction were banned, so the only way was to virtualize them [10]. Therefore, all virtual meeting applications and other electronic communication software became very popular. For some people, such a change to a remote way of working, teaching/learning, or just living wasn't easy [11], but most managed to do that. More than a year after COVID-19 affected the whole world's reality, most people treat online meetings as a common and natural channel of communication. Online collaboration applications such as Microsoft Teams, Cisco Teams, or ZOOM turned into fundamental working tools. It replaced all meetings and now we can say that it made them even more effective.

Rapid virtualization of everyday activities was generally successful and caused not much inconvenience, corresponding to the global situation seriousness. Personal communication has been replaced with its electronic form and people started to live and work remotely. Unfortunately, some activities occurred to be hard to proceed with using existing ICT tools. One of them was virtual elections when secret balloting had to be processed. The pandemic caused a situation where many boards of directors, shareholders, commissioners, and other meetings had to be arranged online. Such meetings are performed periodically and almost always are associated with decision-making. Final choices are often made based on voting results, where decision-makers are choosing between multiple options. Social distancing forced that those group meetings have been moved to virtual rooms. Each participant was isolated and was communicating using a computer's: camera, microphone, and speakers. That is more than enough for discussion, but regarding voting, standard online communication tools became unsatisfactory. Conducting standard open voting is not much problematic, because conventional electronic survey tools may be used [12]. The only question that may appear is how to control voters with unauthorized access or voting more than once. Nevertheless, that problem could be easily solved unless voting results and voters' choices may be revealed when the voting was finished. The open voting result allows rapid verification if each ballot was submitted by an authorized person. Duplicates (votes submitted by the same person more than once) can be also quickly eliminated. It means that elections involving a small number of voters are fully achievable using a common online survey tool. Visual voting could be another possible option. In such cases, authorized voters are asked to define their choices one after another. As others may see and hear the voter, additional ballot verification is not needed. It's worth mentioning that in both cases the role of the president of the voting (or even the electoral commission) must be appointed. This person or a kind of statutory body is responsible for conduction the elections following applicable regulations, for votes counting, and presenting final results. Such a position must be manned by people who are election independent and bestow the other's trust.

Described techniques are appreciable for online voting only in small groups and few votes. Although they are supported with ICT solutions, verification may be time-consuming because vote review must be handled. Online survey-based solutions are developed for mass questioning, and security is not the most important feature of such software. Moreover, because of the review process, arranging a vote in larger groups of people becomes ineffective, but still possible. The second challenge in a virtual election is secret voting. That type of polling is highly demanded or even required in case of making personal choices. The pandemic caused many complications in both: business and non-profit organizations, operated by any kind of management in which members are elected for a particular period.

After that period, the term of office expires and the organization may end up without necessary governance or management. The process of board or president nomination often requires voting and this must be conducted using a secret ballot. Such a procedure can't be based on an Internet system that is not secured and does not support the secrecy of choice. Especially when comes to a decisive body like the board of directors, which takes decisions having legal effects or financial obligations. Those decisions could be questioned if the representatives were elected using an unappreciated ICT tool, that does not meet the legal requirements. The area of online secret voting is attracting growing attention because when personal group meetings are denied and standard voting is excluded, new management (or other decision body) can't be elected. Therefore the whole process of election may be prepared and discussed using the online meeting tools described before. However, in regard to polling, this part of the process requires a dedicated voting system. The tool that supports the security and anonymity of voters' choices [13].

The main issue of using online polling tools for the professional and binding election process is the lack of results verifiability and secret balloting option. The problem is how to provide anonymity and verification of the electors at the same time. Each user authentication process consists of two core elements: identification and verification. The goal of users' authentication is to ensure that a remote user is someone that is identifying himself as that certain person [14]. The authentication procedure must also support keeping the originally authenticated user in for some period, to ensure that it is still the same person [15][16]. The question is, how the user can be identified and stay anonymous at the same time? How to verify and keep user identity without revealing it? This paper describes the design and implementation of a secure voting ICT system, that provides secret ballot support for virtual election. The aim of this work is to investigate the problem of user verification and authentication for online secret voting purposes, which ensures confidentiality for members of the electorate and verifiability of voting results. Knowledge of the presented subject is needed for authentication procedure and voting algorithms development. This study aims to determine the set of rules, that may be used for handling secret ballot elections for virtual meetings. The rules are used in the authors' ICT system, which provides all needed functionalities for conducting and supervising online open and secret voting.

## 2. Voters authentication

Remote user authentication is generally regarded as the main cause of many issues in remote services that are accessed across the Internet. Standard identity verification is based on physical objects like ID cards or other personal documents issued by the government. That simple action becomes more problematic in virtual communication because physical objects can't be transferred over that channel. Moreover, operations in digital services are mostly automated, without the involvement of a person who could verify the identity using i.e. a computer camera [17]. There are some researches on automated identity verification using multiple approaches and techniques, that may solve the problem [18][19][20]. Although these approaches are interesting, at the same time they may be too complicated for a common voting system application. It is important to use the verification method which is adequate to the process importance. Another way the whole voting procedure will be blocked because of the verification stage complicity. In that case, it is important to prove voters' identity in a way, that does not create an access barrier that can't be passed for most of the users [21]. On the other hand, a verification process must also meet voting secrecy conditions if needed. To achieve this goal dedicated algorithm for user authentication was built. The algorithm undertakes user verification, based on a trusted individual communication channel, which was verified before. Such an approach is well known from other digital system solutions and a key element is trust inheritance. It can be described using a simple triangle where each vertex is one part of the authentication process. One is a user who must be authenticated, the second is a service (or person) who needs to verify the user, and the third is a person or service that already knows the user and may act as an authority that may vouch for the user. The guarantee given for the user is delivered from an authority, that is trusted by both: the verifying entity and one that is being verified. This kind of external identity provider is commonly used for account creation or signing in to digital services. The question is if the identity provider is trusted enough to be treated as a reliable source of information. For the services where user identity isn't a key value, a provider such as Facebook or Google may be used [22]. Unfortunately, that solution isn't it's secure enough to be applied in a professional electronic voting system.

The algorithm which was the subject of performed study, uses an individual trusted communication address of the voter, provided by an authority such as the voting chairman or institution that is organizing the election. Generally, the algorithm and the whole voting process relate to the typical voting procedure. The reason is to make it simple and natural for users to use. Giving an authority of allowed user selection to the voting supervisor or organizer is one of the analogies. Who may be more suitable to point users that are allowed for polling, than a voting organization entity? Electors are in most cases well-known (and verified) by the organizer, so he may easily define a list of people that are allowed to make decisions in form of balloting. Each person should be identified by his name and an individual target for a communication channel. This can be a personal phone number for sending a text message or an e-mail address that is assigned only to this particular person. That target is further used for initial user authentication and registration. The second key element of the approach is the use of individual keys, provided to each person who is allowed for the voting. Again, relating to the parallels of the “paper” voting procedure, each elector gets his own key, which may be compared to a paper ballot card. That identifies his right for submitting a vote and cannot be transferred to another person. If lost or destroyed, cannot be issued even to the same person again. Such voting card is represented in the algorithm with a pair of personal keys. Each person gets two different keys which are a set of characters that creates individual unique code. One key is designated for open votings and is related to a person who owns it. The second one is an anonymous token, that has no relation with its owner but provides the right to submit a single vote.

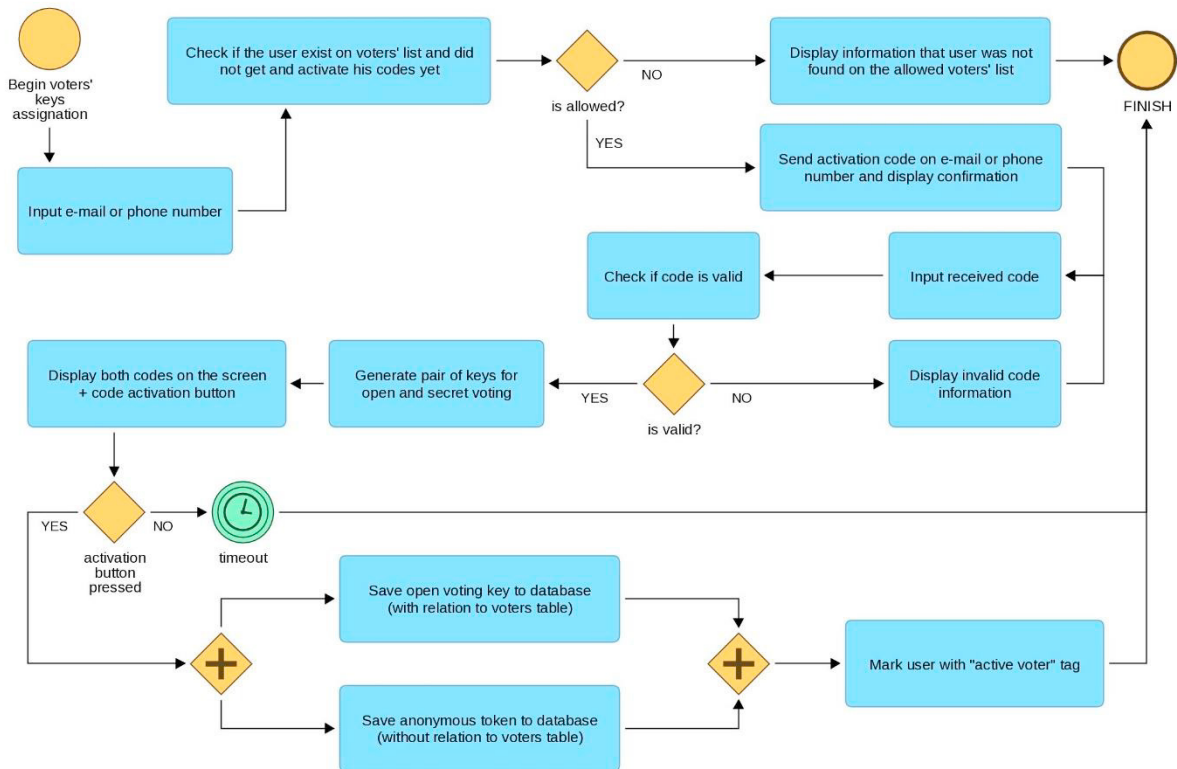


Fig. 1. The algorithm of voters' individual keys assignment.

The method assumes that anonymous tokens are provided to the users allowed to vote only once when they are registered. Another important aspect is that each issued token is not related to a person, which is crucial to keep voting secret and results verifiable. In case of secret voting, all events are always verified and controlled with a individual and private token. The owner of the token has the right to submit a ballot, and the system may also limit number of accesses to avoid votes duplication. When it's finished, final results may be verified by each individual, because given

votes are associated with anonymous tokens. Each voter may check if the vote was indeed qualified for a chosen option. When all individuals verify their votes, there is no place for voting frauds or mistakes and the ballots still stay secret. Such an approach provides security of voting procedure, allows anonymity and full results verifiability. For open voting, a different user key type is used. It is to control users against multiple ballot submissions during single voting. Since the second key is related to a person, results may be verified and choices taken by the voters are revealed. In that case, result verification is even easier, because each vote is tagged with a voter's name. This solution may be easily applied to a digital election system and used as support for virtual meetings and polling. A block description of the algorithm of voters' individual keys assignment was presented in Fig. 1.

The whole idea of online polling and keeping it secret (if needed) is based on the individual codes, that voters are using to authenticate themselves when voting. To get the codes each voter must go through the procedure of code assignment and activation. This procedure is available only for allowed voters registered by the authority. Each registration has separate electors' data and individual contact target for verification. To obtain the keys, a voter needs to trigger the procedure, by inputting his e-mail or phone number. When this data is submitted the algorithm checks if such target contact exists and hasn't obtained his keys yet. If any of these conditions are not met, the user should get a proper notification. If both conditions are fulfilled procedure may be continued. In the next steps, the voter should get his unique activation code which is sent to the target contact address or a phone number. That is the stage of user authentication. It is based on the common idea, that only verified users have access to obtain the code from a private mailbox or short text message. If the user inputs the activation code and the code is correct and matches the current procedure, two unique keys are generated. There should always be two different codes for one voter. The first one is a personal key used in open votings, related to the voter's registry and the owner of the code is always known. The second code is an anonymous token, which is used for secret voting. That code is stored only in an active tokens registry, which is not related to the users' database.

Each token allows to submit a single vote in each voting, but the owner of the token is unknown. This approach assumes that the secret token was possessed during the code assignment procedure and its owner is allowed to vote. Who exactly owns the token is unknown because the only information that is needed to proceed with secret voting, is if the owner is allowed to submit a ballot. That is a key element for keeping elections secret but still has the capability to verify voters. At that stage of the procedure, both codes are displayed to the user but are not saved to the database yet. The user must confirm that he has collected the codes and saved them in a secure way. That part is crucial, because anonymous tokens may not be recreated. Of course, there is a registry of active tokens in the database, but there is no relation to the certain user. If a voter has lost his token after activation, it wouldn't be possible to replace it with a new one. Such an operation would need to deactivate a previous token first, then put a new one into the registry. The first step is impossible to proceed without knowing which one belongs to the user. Registering only a new code wouldn't be safe, because the old one is still active and could be used in voting. That is a reason why the voter is asked to double-check if his codes were properly saved. Pushing the activation button saves the codes to the database and locks the procedure for the single voter against a second use. Unless the activation button isn't pushed, the user may cancel the procedure and start it over again later. Codes that were generated are deleted, so during the next procedure run, the voter will get new codes. When the whole procedure is finished and codes are activated, the user is marked as an "active voter" that may submit ballots in further elections.

### 3. Voting procedure

The most important limitation of virtual communication lies in the fact that users may not be verified using traditional ways of authentication. It is caused by limitations described in the first part of the article. Fortunately, some ways of remote verification are known and commonly used in ICT systems. However, in the context of secret balloting, the major weakness of remote authentication is that users' identity is uncovered while being verified. That is why it can not be applied for secret polling purposes. The algorithm of user verification and registration described earlier in this paper supports both: authentication and anonymity. When the registration procedure is done, voters are equipped with codes that may be used to verify voters when voting. Thanks to a personal key and anonymous token, it applies equally to open and secret voting. Thanks to the one-time registration procedure, the algorithm of polling may effortlessly verify voters. Although the first voter registration procedure is quite demanding, further votings are

much more simple and less time-demanding. It means that meetings that include multiple voting may be proceeded more efficiently, and referring to the secret balloting – they may be conducted at all.

The voting procedure was presented in Figure 2 and consists of few tasks and conditions. Such approach allows registered voters to place the ballot easily and securely at the same time. The first activity in the procedure is starting a particular voting. It means that the voter needs to select voting that is currently running, to take part in it. When the voting is loaded, the voter gets access to the content that consists of a title, subject matter, and offered options to choose from. There may be some more technical information displayed such as voting type (open or secret), number of available options that may be selected (if multiple-choice voting), starting and ending time, etc. Each person that has an access to the voting (it depends on the voting ICT system if the voting is also enabled to observers), may see the whole content but only registered voters may submit a valid ballot. That can be easily controlled with a code, that was given to allowed users in the registration and activation procedure. Each submitted ballot may be also validated against common errors. This means an exceeded number of chosen options or exclusive choices like abstention and another option simultaneously. When the choice was not validated, suitable information may be presented and the procedure reversed to be reviewed.

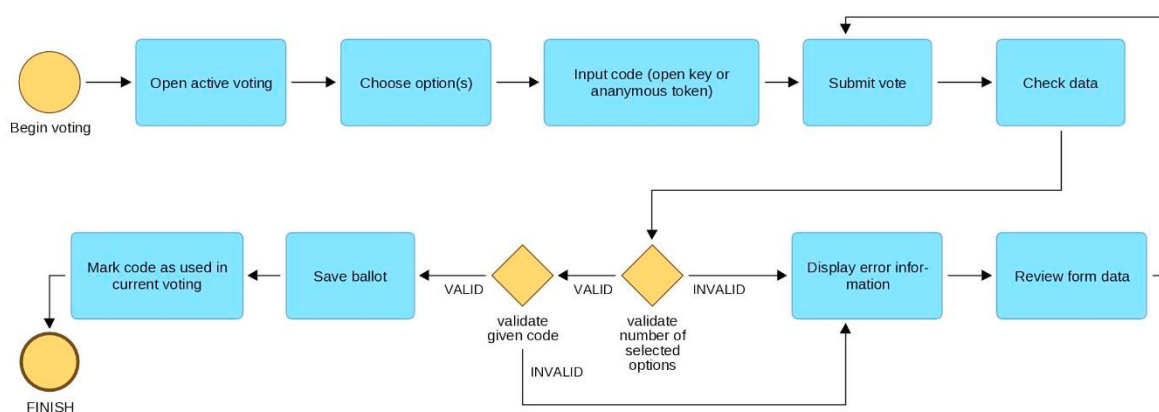


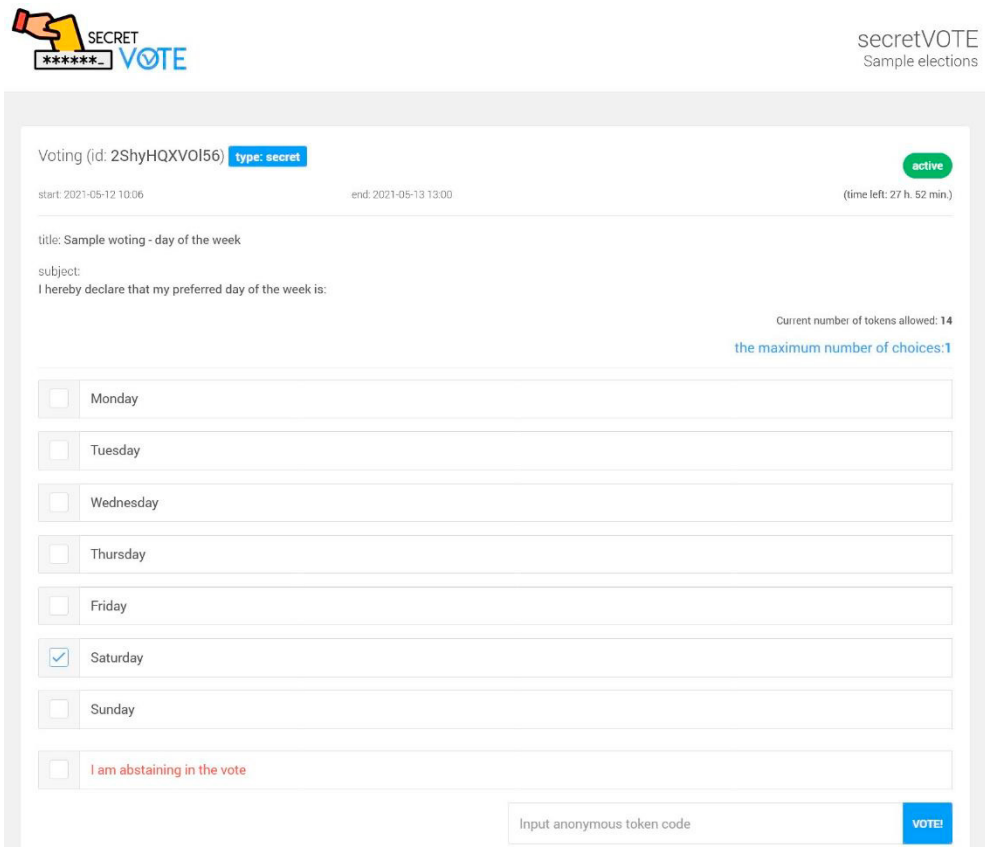
Fig. 2. The procedure of ballot submission and voter verification

Next and the most important element is code validation. The code must not only be valid but also must fit the voting type and must not be used in the particular voting earlier. That is to avoid using a personal overt key (not anonymous token) for secret voting and opposite. When the code is invalid on any of the validations levels, the ballot cannot be placed. Conversely, when the vote validation and code verification didn't reveal any errors, the vote may be saved. It is also critical to mark code as used at the end, to prevent double voting. That action may be served in several ways, depending on the digital system solution. When the operation of voting for a single user is finished, he may still access the voting content and see which of the options he has selected. Ending the whole voting by the chairman means that all voters (and observers if allowed) are available to see the results immediately. If needed, some additional calculations may be proceeded and displayed automatically. That means voting attendance or results presented in percentage concerning final turnout and/or allowed voters number. As a consequence, all voter's choices may be also presented, but according to a voting type, name or anonymous tokens should be revealed. Such an evident approach leaves no misunderstandings on polling results dishonesty because each vote and option relation may be verified and the number of submitted votes for each option revised.

#### 4. The procedure implementation

This paper provides new insights into electronic voting that is offering both: secrecy of choices and secure authentication of the voters. To confirm the findings of this study author has created a digital voting system. The

system uses algorithms described in the article and offers digital support for online elections. This stage of research was to confirm that a given approach can be applied in a real application and that the application can support secret ballot elections for virtual meetings. The system was developed by the author of this article as an online web application. It can be accessed remotely from many kinds of digital devices equipped only with a basic web browser and Internet connection. Data transferred between the users' device and the application is encrypted using an SSL certificate and HTTPS protocol. The application was named “secretVOTE” and was registered under secretvote.pl domain. This solution provides a wide range of possibilities to conduct virtual voting. On the contrary, it was still kept with a minimum required functionality, to make it easy to use. It allows creating and managing allowed voters list, by inputting each person into the system manually or just by importing a batch of data from a simple spreadsheet. Each person put onto the voters' list, may run the registration procedure. The procedure was based on the algorithm described earlier in this article and finishes with generating two personal codes and their activation. Each active voter may check his code's validity or take part in votings that are announced on the voting list. A sample voting screen from the “secretVOTE” system was presented in Figure 3. It applies to single voting where ballots are kept secret. There is a sample voting title, subject, and 7 possible options to chose from. Only one option may be selected because the voting was defined as a single-choice one. On the bottom of the screen input field for anonymous code has been placed. The user should select one of the options, insert his anonymous token and press the green button to submit his vote securely. The final decision is confirmed with an additional question window if the user is sure that he wants to submit a vote. After the second confirmation vote is saved and anonymous token deactivated for the particular voting.



The screenshot displays the 'secretVOTE' interface for a voting session. At the top left, there is a logo with a hand holding a ballot and the text 'SECRET VOTE'. At the top right, the text 'secretVOTE Sample elections' is visible. The main content area shows the following details:

- Voting (id: 2ShyHQXV0I56) type: secret
- start: 2021-05-12 10:06 end: 2021-05-13 13:00 (time left: 27 h. 52 min.)
- title: Sample voting - day of the week
- subject: I hereby declare that my preferred day of the week is:
- Current number of tokens allowed: 14
- the maximum number of choices: 1

The voting options are presented as a list of radio buttons:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- I am abstaining in the vote

At the bottom, there is an input field labeled 'Input anonymous token code' and a blue button labeled 'VOTE!'.

Fig. 3. Virtual ballot - screenshot from “secretVOTE” digital system

The system and applied verification methods make virtual voting easy and accessible even for not digital experienced users. The algorithm and its conditions allowed to describe actions or errors clearly so all needed



information is displayed to a user on the screen. A virtual ballot presented on the screen in Figure 3 displays also some additional information about the voting like the type of voting (which is secret in this case), beginning and ending, and also time which is left until the end of the voting. Users may see also a current number of tokens that are allowed in voting. That is the number of active users, so those who have already obtained and activated their codes. There is also one important piece of information displayed above the options that tell the user how many choices can be selected on the list. That is verified during vote submission, exactly like it was defined in the procedure. Users may also leave the voting and come back later, to submit the vote. When the ballot was successfully placed, it is confirmed with a green alert displayed on the screen. The vote may be later verified, even when the voting is running. To do that, the user needs to input his code again, to see which options were previously chosen. The main results of the balloting are available immediately after voting comes to the end. The results can be also accessed remotely using the application votings list. When one of the finished votings is selected, its final results are displayed. Such a view from “secretVOTE” systems screenshot and sample voting was presented in Figure 4.

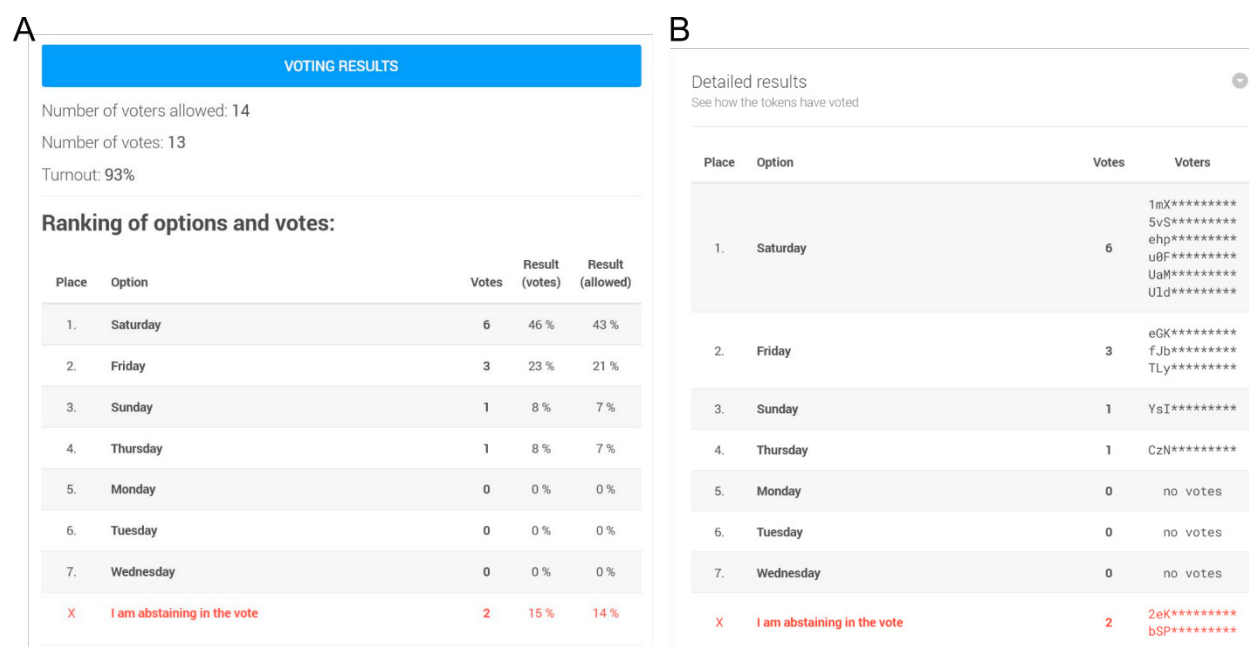


Fig. 4. Finished voting results - screenshots from “secretVOTE” digital system

A sample voting aim was to select one preferred day of the week using the voting ICT tool. Voters were choosing between seven available options, from Monday to Sunday. The voting was defined as a secret, so the results cannot reveal voters' and their choices. That is why anonymous tokens were used. Screenshots with the results were presented in Figure 4. The A view (on the left) displays general polling results in a form of options rank. The ones with the biggest number of votes were placed at the top and those without the votes at the bottom. Such a view allows identification which option was the most popular. Others, with a smaller number of votes, were placed in the next places in the ranking. Each voting has an abstaining option which is added automatically. The user should always have an alternative to take part in polling without selecting any option. In such a case the vote is counted for the turnout but does not affect the results. Each position in the ranking has a number of votes won and also achieved results presented as a percent of all votes submitted and all votes that could have been cast. Such information may be very useful especially when internal organization rules, require to win at least half (or more/less) of the votes.

The second view marked as B section of Figure 4, shows detailed results of the voting. This allows users and observers to verify general numbers presented in the Ranking. Regarding that the voting type was secret, only anonymous tokens are displayed. What is more, the tokens are partially masked, not to reveal a full code. If the full code was shown, there would be a possibility to use it in an unauthorized way during the next voting. That is the

reason why only part of the code is presented. Such a small part allows its owner to locate it on the list but does not allow others to possess the code for further use. Additionally, the masking scheme changes in each voting. Each time other three signs of the code are presented and the other masked. To make it even more secure, some signs are not shown in any of the scheme combinations. It secures the system against fraud based on trying different combinations of revealed code parts, to find a valid token and use it illegally for the next voting. That is the crucial element of the secret ballot verification. Each person may verify his own and only own vote, but can't see the others' choices. If every single person confirms his vote-option assignation, there is no place for fraud or mistake, because the number of votes won is presented and the total sum must match. It proves that taken approach reconciles two mutually exclusive elements which are anonymity and virtual authentication.

## 5. Conclusion

This paper has shown the significance of virtual services during a pandemic when social distancing is a key to fight against COVID-19 disease. Unfortunately, not all services were prepared enough to handle all people's needs when personal communication must be entirely replaced with its electronic form. One of such needs was online voting and especially secret virtual balloting. The most important limitation lies in the fact that the user can't be authorized and stay anonymous at the same time. Conducting elections and verification procedures remotely brings even more complications. Presented results provide a significant step towards online voting that becomes available and achievable for all organizations and individuals. The described algorithm shows how to verify the user for a secret ballot without revealing his data.

The presented method has been applied to a digital system to verify its functionality and usability. The system has been developed as a fully functioning internet application. It has been examined in several actual elections, conducted during virtual meetings. Several organizations in Poland, during the pandemic lockdown, have elected their authorities using "secretVOTE" application and described algorithms. The system has proved the approach usability in practice and now is supporting other organizations in this uncertain time. SecretVOTE application has been now enabled for commercial use, as a solution for COVID-19 pandemic restrictions. For now, it provides excellent support to the organizations but in the future, when hopefully restrictions will be gone, it may be successfully used for hybrid and standard elections. The whole idea simplifies the process of digital balloting. The possibility to use own voters' devices as an electronic ballot card is even more promising. It's worth emphasizing that the COVID-19 pandemic already changed the world in terms of electronic services use. Some things will never return to their traditional analog form whether we want it or not.

## References

- [1] Fisher, J., Languilaire, J.-C., Lawthom, R., Nieuwenhuis, R., Petts, R. J., Runswick-Cole, K., & Yerkes, M. A. (2020). Community, work, and family in times of COVID-19. *Community, Work & Family*, 23(3), 247–252. <https://doi.org/10.1080/13668803.2020.1756568>
- [2] Velavan, T. P., & Meyer, C. G. (2020). The COVID-19 epidemic. *Tropical Medicine & International Health*, 25(3), 278–280. <https://doi.org/10.1111/tmi.13383>
- [3] Milne, G. J., & Xie, S. (2020). The Effectiveness of Social Distancing in Mitigating COVID-19 Spread: a modelling analysis. *MedRxiv*. <https://doi.org/10.1101/2020.03.20.20040055>
- [4] McGrail, D. J., Dai, J., McAndrews, K. M., & Kalluri, R. (2020). Enacting national social distancing policies corresponds with dramatic reduction in COVID19 infection rates. *PLOS ONE*, 15(7), e0236619. <https://doi.org/10.1371/journal.pone.0236619>
- [5] Mishra, Dr. L., Gupta, Dr. T., & Shree, Dr. A. (2020). Online Teaching-Learning in Higher Education during Lockdown Period of COVID-19 Pandemic. *International Journal of Educational Research Open*, 1(), 100012. <https://doi.org/10.1016/j.ijedro.2020.100012>
- [6] DeFilippis, E., Impink, S., Singell, M., Polzer, J. T., & Sadun, R. (2020). Collaborating During Coronavirus: The Impact of COVID-19 on the Nature of Work. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3654470>
- [7] Gabbiadini, A., Baldissarri, C., Durante, F., Valtorta, R. R., De Rosa, M., & Gallucci, M. (2020). Together Apart: The Mitigating Role of Digital Communication Technologies on Negative Affect During the COVID-19 Outbreak in Italy. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.554678>
- [8] Bottanelli, F., Cadot, B., Campelo, F., Curran, S., Davidson, P. M., Dey, G., Raote, I., Straube, A., & Swaffer, M. P. (2020). Science during lockdown – from virtual seminars to sustainable online communities. *Journal of Cell Science*, 133(15). <https://doi.org/10.1242/jcs.249607>
- [9] Anderson, D., & Kelliher, C. (2020). Enforced remote working and the work-life interface during lockdown. *Gender in Management: An*

- International Journal, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/gm-07-2020-0224>
- [10] Jones, R. E., & Abdelfattah, K. R. (2020). Virtual Interviews in the Era of COVID-19: A Primer for Applicants. *Journal of Surgical Education*, 77(4). <https://doi.org/10.1016/j.jsurg.2020.03.020>
- [11] Wagner, N., & Strulak-Wójcikiewicz, R. (2020). Concerns about the technology used by collaborative platforms - a challenge for managers. *Procedia Computer Science*, 176, 2536–2545. <https://doi.org/10.1016/j.procs.2020.09.319>
- [12] Van Selm, M., & Jankowski, N. W. (2006). Conducting Online Surveys. *Quality and Quantity*, 40(3), 435–456. <https://doi.org/10.1007/s11135-005-8081-8>
- [13] Qureshi, A., Megias, D., & Rifa-Pous, H. (2019). SeVEP: Secure and Verifiable Electronic Polling System. *IEEE Access*, 7, 19266–19290. <https://doi.org/10.1109/access.2019.2897252>
- [14] NERMEND, K., ALSAKAA, A., BORAWSKA, A., & NIEMCEWICZ, P. (2017). Emotion recognition based on eeg signals during watching video clips. *Studies & Proceedings of Polish Association for Knowledge Management*, 40–52. [http://pszw.edu.pl/images/publikacje/t086\\_pszw\\_2017\\_nermend\\_alsakaa\\_borawska\\_niemcewicz\\_-\\_emotion\\_recognition\\_based\\_on\\_eeg\\_signals\\_during\\_watching\\_video\\_clips.pdf](http://pszw.edu.pl/images/publikacje/t086_pszw_2017_nermend_alsakaa_borawska_niemcewicz_-_emotion_recognition_based_on_eeg_signals_during_watching_video_clips.pdf)
- [15] Braz, C., & Robert, J.-M. (2006). Security and usability. *Proceedings of the 18th International Conference on Association Francophone d'Interaction Homme-Machine - IHM '06*. <https://doi.org/10.1145/1132736.1132768>
- [16] Patel, V. M., Chellappa, R., Chandra, D., & Barbelo, B. (2016). Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4), 49–61. <https://doi.org/10.1109/MSP.2016.2555335>
- [17] Szyjewski, G. (2010). Remote authentication as a gateway to automate process of non-electronic service offering. in information systems in management. In *INFORMATION SYSTEMS IN MANAGEMENT VII* (pp. 86–94). WULS Press. [http://isim.wzim.sggw.pl/resources/ISIM\\_VII\\_2010.pdf](http://isim.wzim.sggw.pl/resources/ISIM_VII_2010.pdf)
- [18] Cresitello-Dittmar, B. (2016). Application of the Blockchain For Authentication and Verification of Identity. <http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf>
- [19] Isobe, Y., Seto, Y., & Kataoka, M. (2001). Development of personal authentication system using fingerprint with digital signature technologies. *IEEE Xplore*. <https://doi.org/10.1109/HICSS.2001.927272>
- [20] Blythe, S. (2005). Issue 2 Article 3 2005 of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security, 11 *Rich. J.L. & Tech*, 11(2). <https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1238&context=jolt>
- [21] Królikowski, T., & Susłow, W. (2019). A Concept of a Training Project IT Management System. *Procedia Computer Science*, 159, 1468–1478. <https://doi.org/10.1016/j.procs.2019.09.317>
- [22] Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013). A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. *Proceedings of the 2013 ACM Workshop on Digital Identity Management*. <https://doi.org/10.1145/2517881.2517886>