Agris on-line Papers in Economics and Informatics

Volume XVI Number 3, 2024

Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe

Tomáš Martínek, Martin Pelikán, Jan Tyrychtr, Jakub Konopásek

Department of Information Engineering, Faculty of Economics a Management, Czech University of Life Sciences Prague, Czech Republic

Abstract

Lockdowns and social progress have increased hours of work from home, often requiring remote methods of communication. Agricultural organizations from associations to cooperatives to joint stock companies must prepare to carry out more activities online. This article proposes a procedure for the possible implementation of a remote electronic election in personnel matters of the organization using the Belenios system, based on an evaluation of expectations from a questionnaire survey of agricultural college students and graduates. The proposed procedure is subsequently verified based on an evaluation of compliance with the Council of Europe recommendation on standards for electronic voting.

Keywords

Internet voting, E-voting, E-democracy, Open-Source, Belenios, E-elections.

Martínek, T., Pelikán, M., Tyrychtr, J. and Konopásek, J. (2024) "Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe", *AGRIS on-line Papers in Economics and Informatics*, Vol. 16, No. 3, pp. 59-73. ISSN 1804-1930. DOI 10.7160/aol.2024.160305.

Introduction

Online voting is becoming an increasingly prevalent method of casting a ballot. In Estonia, 51% of participating voters cast a ballot online in the 2023 Parliamentary elections (Valimised.ee, 2023). While the COVID-19 pandemic has promoted the use of ICT tools for remote communication, i-voting has not developed as much in national politically binding elections (Driza Maurer et al., 2023). Remote electronic dialing is one of the possibilities of using ICT. So that the members of the institution do not have to all meet in one place for the elections, but elections can be instead conducted remotely.

If it is a public election without the secrecy of individual ballots, such an election can be carried out in many ways. The problem arises if the principle of secrecy of elections is to be observed, i.e. the secrecy of ballots so that even the administrator of the election system cannot find out the form of individual ballots. I-voting is developing in its use in the primary elections of political parties (Blanchard et al., 2022) and their other intra-party decision-making (Martínek and Malý, 2024), in academic elections (Adida et al., 2009) and in other institutions. In our paper, we focus on secret personnel ballots in agricultural enterprises, which can be agricultural or food production cooperatives, or limited liability companies or joint stock companies with a focus on agriculture and food production. The proposed methodological procedure may also be suitable for agricultural unions and associations.

Food cooperatives began to be established in the Czech Republic in the first half of the 19th century, and agricultural cooperatives were also established in the second half. Among the basic principles of cooperatives is democratic control, requiring also voting by cooperative members (Kořínková et al., 2017). After 1989, other types of agricultural enterprises using voting within the ownership structure began to emerge in the Czech Republic in the form of limited liability companies or joint stock companies. The Act on Companies and Cooperatives (Czech Republic, 2012) allows voting using technical means. The voting conditions must ensure that the identity of the voting person is verified and that the shares or stocks associated with the voting right are identified. These conditions are determined by the articles of association or the articles

of association and are set out in the invitation to the general meeting or in the draft resolution. In the case of a cooperative, each member has 1 vote in the voting and secret ballots are generally permitted. In the case of limited liability companies, a secret ballot is excluded in certain cases, for example when the law requires the voting members to be named in the notarial deed. A secret ballot is required for the election and removal of employee members of the supervisory board.

In the Czech Republic, agrarian enterprises already use a number of digital services, which include e-mail, electronic signature, the Ministry of Agriculture's eAgri portal, data box, public administration portal, tax portal, electronic procurement, e-customs and others (Rysová et al., 2013). Agricultural enterprises are also gradually starting to use social networks (Kánská et al., 2013). Secret ballot via the Internet is not among the commonly used systems. With the use of information and communication technologies (ICTs), farms can enjoy benefits that may include better accessibility of elections, greater voter interaction, voter time savings, and others. At the same time, however, potential threats and risks must be addressed where the security of the constitutional principles of personal elections, which commonly include universal, equal, free and secret suffrage, may be compromised. Legislative documents that should be considered when i-voting in the Czech Republic include the recommendations of the Council of Europe, of which the Czech Republic is a member (Driza Maurer et al., 2023).

Council of Europe Recommendation on standards for e-voting

The Council of Europe's core legislative document for i-voting is Recommendation CM/Rec(2017) 5 of the committee of ministers to member states on standards for e-voting (Council of Europe, 2017). While the Recommendation is not binding on members, compliance with it is expected. Norway and Sweden have voluntarily adopted the Recommendation, the Supreme Court in Estonia has referred to the Recommendation, and in Belgium the Recommendation has been used as a benchmark in the evaluation of e-voting (Rodríguez-Pérez, 2022).

Based on the results of a questionnaire survey among students and graduates of agricultural colleges, this paper aims to propose a sufficiently transparent and verifiable methodological procedure using the open source Belenios system for conducting a secret remote electronic election in an agricultural enterprise or union. The methodological procedure should be subsequently validated using the requirements of the Council of Europe (2017) recommendations.

Materials and methods

In this article, a methodical procedure for the implementation of a secret remote electronic election using the Belenios test system was proposed. To achieve the goal of the article, a survey of professional literature was conducted from the scientific databases Web of Science and Scopus. To process the literature search, the article further focuses on professional texts, legislation and other sources related to agricultural enterprises.

Questionnaire survey on the characteristics of remote electronic voting

In order to find out the opinions on the features of remote electronic voting, a questionnaire survey was conducted among students and graduates of Czech universities with agricultural specialization. We assume that these are people with higher technical literacy who may be potential users of i-voting systems on farms in the near future. The Agbesi et al. (2023) framework with identical questions was used to construct the questions, which explored dimensions of Internet voting transparency, supplemented with a few specific questions. Agbesi et al. (2023) identify five core dimensions, namely Information Availability, Understandability, Monitoring and verifiability, Remedial Measures, Testing, these dimensions affect the perception of transparency which in turn affects the trustworthiness in the whole system. The anonymous questionnaire survey was conducted online via the Dotaznik.czu.cz platform operated by the Czech University of Life Sciences Prague. The invitation to participate in the survey was extended primarily to Czech students and graduates of agricultural universities. The survey was conducted from 24 October 2023 to 12 May 2024. Participants were shown all information including consent to data processing on the survey homepage.

Respondents answered questions on a seven-point Likert scale ranging from Strongly Disagree (0) to Strongly Agree (6) on five defined dimensions. A total of 177 people were recorded as completing the questionnaire. A total of 108 questionnaires were completed in full. Of these, 8 more questionnaires

were removed because the control question "This question is not part of the survey and just helps us to detect bots and automated scripts. To confirm that you are a human, please choose 'Strongly agree' here" was answered differently than Strongly agree. Out of the 100 responses, 64 were male, 35 were female and 1 respondent did not indicate their gender. 72 respondents are aged 18-30, 18 aged 31-40, 5 aged 41-50, 2 aged 51-60 and 3 aged 61-70. 72 respondents have completed secondary education, 10 have a Bachelor's degree, 12 have a Master's degree and 6 have a PhD.

The questionnaire survey is evaluated in aggregate according to the defined dimensions and transparency, which consist of individual questions. The rating describes the average frequency of responses on a Likert scale and the degree of expectation of fulfilling a given dimension on a scale from 0 (not at all expected) to 1 (fully expected), where from 0.5 upwards a given characteristic is expected. The level of expectation for a given attribute is the ratio of the average rating to the maximum possible rating within the aggregate of the whole dimension. The value is rounded to 2 decimal places.

The Statistica 14 software was used to do the descriptive statistics. We calculated fundamental information such as the mean, minimum, and maximum values, various measures of variation, and data regarding the shape of the variable's distribution (including the standard deviation and the standard error). An important aspect of the description of a variable was the shape of its distribution, which indicates the frequency of values within different ranges of the variables. More precise information was obtained by performing normality tests to determine the probability that the sample originated from a normally distributed population of observations, specifically using the Shapiro-Wilk test. These statistics were included in the dataset (Martínek and Tyrychtr, 2024).

Methodology for the testing the software used

Our methodology was developed to be used with the Belenios system, which, according to Cortier et al. (2019), offers a compromise between simplicity and security. Belenios is based on the Helios system (Adida et al., 2009). For the testing purposes of this article, the Belenios system installation at *https://volba.odvolit.cz* is used, which also verifies the correct functionality of the open-source code of the official system installation at *https://vote.belenios.org*. To specify the new methodological procedure, the general characteristics of the organization's information systems and their requirements were considered. The proposed methodological procedure combines the instructions of the Belenios voting system (Belenios team, 2023) embedded in the practical paper voting common in Czech organizations.

Methodology for the design of the election procedure

The methodological procedure is designed to meet the expectations identified in the questionnaire survey. The methodological procedure is tested by experimental voting in the form of a secret personnel election of a model organization. In our case, the model organization is a medium-sized agricultural cooperative, which has its information system for members and which uses the procedure for the election of the board. The cooperative thus uses an ERP system that enables the display of personalized information for individual members of the cooperative as well as communication through encrypted messages.

Methodology for verification of the proposed methodological procedure

Subsequently, the proposed methodological procedure of the election was verified by checking against the fulfillment of Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for electronic voting of the Council of Europe (Council of Europe, 2017) through answers created based on the methodological evaluation of the Helios electronic system (Panizo Alonso et al., 2018), professional literature, security analysis (Cortier et al., 2020) created by the authors of the Belenios system, by testing the system. Considering the limitation of the length of the paper, the basic 49 standards (Brunet and Essex, 2023) are evaluated descriptively. Each requirement is also evaluated in brackets as fulfilled (○), not fulfilled (✗), or fulfilled under certain conditions - partial according (Δ) to the symbols in the framework of Panizo Alonso et al. (2018).

Results and discussion

Based on the evaluation of the questionnaire survey, it can be determined that students and graduates of agricultural colleges expect the i-voting system to meet all 5 defined dimensions and transparency, so in the proposal of the methodological procedure of e-voting of agricultural organizations, we will try to meet the expectations (Table 1).

Dimensions (number of questions within a dimension)	Average frequency of responses							Level of expectation
	0	1	2	3	4	5	6	
Information Availability (4)	1.25	1.75	3.25	9	15	25.5	44.25	0.81
Understandability (5)	0	0.2	0.8	3.4	17	33	45.6	0.86
Monitoring and verifiability (5)	0.4	0.4	1.8	8	17.2	30	42.2	0.83
Remedial Measures (5)	0.6	1.6	4	9.6	15	30.8	38.4	0.80
Testing (4)	0.75	0.75	1.75	8	16.5	27.25	45	0.83
Transparency (4)	1.5	0.75	2.25	12.5	19.25	29	34.75	0.79

Source: Authors (Martínek and Tyrychtr, 2024)

Table 1: Evaluation of a questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges.

Methodical procedure for remote secret electronic election

The basis for the possibility of conducting an electronic election is to use a trusted electoral system under an administration that voters trust. For the purposes of this article, we use the open-source system Belenios, the functionality of which was verified by our installation. The following method of conducting an election is designed to be conducted, for example, during a remote meeting via an online conference of the membership to participate in the election.

Voters should be informed in advance of the plan to conduct electronic elections, for example in an invitation to a meeting. In accordance with the GDPR, voters should be informed about the way personal data is protected within the organization's information system. The organization should prepare or refer to detailed instructions for using the voting system. In the first phase, it is necessary to designate an election administrator who, as a member of the election commission, will ensure the technical setup and administration of the election. This can be the secretary of the membership body, in the case of ensuring greater credibility, it can be, for example, the independent IT administrator of the given organization.

The administrator can create a new option after logging in. Access codes and authentication are important in the system, which can be via email and password or a trusted third-party system (CAS). In the basic mode, access codes and passwords are sent by the election server; to increase security, access codes should be sent to voters in a different way than by e-mail sent by the election server. This activity can be ensured by an authorized authority, which could distribute the access codes to invited voters in a paper invitation to the meeting, or send them, for example, via the organization's internal communication system. If access codes or passwords are transmitted in a way other than those sent by the election server to the voter's e-mail, there is less chance of discrediting the election, as the potential risk of "eavesdropping" on encrypted e-mail communication or breaking access to the voter's e-mail box is reduced. The administrator thus enters the name of the authorized authority and gives it a link for generating access codes. In the case of a test election, the individual personal access codes are imported by an authorized authority, which can be the election administrator, into the organization's internal system, which then displays the specific access code after logging in to the given voter with a link to the specific election. The authorized authority has at its disposal a list of voters, which it can also provide to other members of the electoral commission. After the end of the elections and their successful audit verification, this information is removed from the internal system in order to increase the long-term security of the secrecy of the vote.

After setting the voter authentication methods, the administrator further enters a clear name and description of the election, sets questions and answers for the first round of the election, and adds his name and contact, which should be on the authorized identity in case of obtaining a lost access code. It also sets the language of choice, in the Czech Republic the default is Czech (cs), or for people who do not know Czech, they can add other languages of choice, including English (en).

The administrator further populates the voter register by adding a voter email list with one email per line. The system allows you to enter the login of each user in case of using a more sophisticated method of authentication connected to the central authentication service (CAS). The number of whole votes of a given voter can be added to the third place

of the line, separated by a comma, in the case of, for example, different ownership shares of the voters. The same vote weight is used in the experiment. Members of the electoral commission should also have access to the list of voters, including information about their participation in the vote, before the start and after the end of the vote.

As in the case of paper elections, it is necessary to choose persons who will take care of the security of the election in the given institution. In the case of using Belenios, at least two other members of the electoral commission can be elected by public election, who will also be guarantors of the election. The guarantors should not have a personal interest in the outcome of the election so they have no motivation to influence the election after the agreement. Alternatively, the guarantors could be appointed by each of the candidates so that each candidate has one trustworthy person in the electoral commission without whose participation the election results cannot be influenced. After selecting the guarantors, the administrator enters their names and e-mails into the selection settings of the Belenios system. Subsequently, the administrator gives the guarantors, for example, using a confidential secure communication system, their links for generating keys.

When preparing for the election, it is necessary to fill in the voting questions and answers by the administrator. Although the Belenios system allows for various alternative voting methods, including ranking and scoring, for testing purposes, traditional two-round voting, which is often used in organizations as well, will be used. Thus, all nominated candidates participate in the first round. The method of nomination is determined by each organization itself, just as it is already done in paper elections. If any of the candidates receives more than half of the votes, they will be elected in the first round. Otherwise, the two candidates with the highest number of votes advance to the second decisive round. In order to reduce the risk of a tie election in the second round, it is possible to define a condition in the approved voting procedure that in case of equality of votes in the second round, the number of votes in the first round is taken into account.

Before starting the election, the guarantors carry out its encryption, when they save and enter a private key and a unique fingerprint. Immediately after the election is started by the administrator after it has been encrypted, the guarantors will verify the identity of their unique fingerprint with the publicly displayed fingerprint on the front page of the given election next to their name.

The Electoral Commission shall determine in advance the beginning and end of the voting, which shall be clearly announced to the voters, and the administrator shall set the given times. If an event occurs that may limit voters' access to casting their vote in the electronic ballot box, the electoral commission may agree to extend the deadline for voting.

The voter accesses the election at the URL sent by email with the password or displayed together with the access code. First, he enters the access code, then he fills in the ballot when it should be possible to submit an empty ballot. After it has been encrypted, the voter should save a printout of the ballot for verification and then insert it into the electronic ballot box by logging in using the password sent. At any time after that, he can verify the presence of the ballot in the ballot box using the stored fingerprint.

After the end of the election, the administrator has the encrypted result calculated and then waits for the decryption of the result by all the guarantors. The administrator will provide the guarantors with a URL to enter their private keys to decrypt the election. Admin can also postpone the publication of the result to the exact time. After the evaluation of the elections, the administrator should hand over to the members of the electoral commission the list of voters, including information on participation in the vote. The members of the electoral commission should subsequently audit the voting results (Belenios team, 2023), and anyone else can also do this.

After the audit, both the administrator and the members of the election commission should delete all stored keys and voter lists from their PCs and the organization's internal systems. The choice itself is subsequently archived and deleted after a longer period of time. If all verifications are carried out, the choice can be immediately deleted to ensure the greater long-term security and secrecy of votes.

In the event of an incident or violation of the procedure, in any part for which the members of the election commission are responsible, they immediately inform their superiors - the presiding organization, so that correction can take place. Similarly, voters or auditors should immediately inform the electoral commission of any suspicious event.

Verification of the electoral methodological procedure with the Recommendation CM/Rec(2017)5 of the Committee of Ministers of Member States on standards for electronic voting of the Council of Europe (2017)

1. *The voter interface of an e-voting system shall be easy to understand and use by all voters. (○)*

The Belenios system has already been used in many elections and thousands of different users have managed the election (Cortier et al., 2019). The election process is intuitive and is supplemented with instructions that help less technically literate election participants.

2. *The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently. (Δ)*

The Belenios system achieves a rating of 72 % in the accessibility test (Accessibility Checker, 2023), but at the same time, it is open source, which, if necessary, allows modifications for greater accessibility to electronic voting.

3. *Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting. (○)*

The proposed method takes into account the availability of the voting system online via the Internet. A classic paper election is not excluded for users who do not want to vote online.

4. *Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum. (○)*

In the proposed procedure, information regarding the meaning of the election is passed on to the voters within the given meeting and the organization's internal information system, which is related to the election.

5. *All official voting information shall be presented in an equal way, within and across voting channels. (○)*

In the proposed procedure, all voters receive the same information using the organization's internal information system or e-mail communication. Basic information about the election is displayed on the initial page of the vote and in the public data for the election.

6. *Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result. (○)*

The proposed procedure allows for electronic voting. If it is necessary to hold a non-electronic election, a classic paper election could be held for voters who do not participate in an electronic election. To ensure that voters are not influenced, the publication of electronic results must be set only after the end of the paper election. Subsequently, the results of the electronic and non-electronic election commissions would have to be merged. Since the Electoral Commission has information about the participation of individual voters, it can allow paper voting for those who did not participate in the electronic election, in which case it is assumed that the non-electronic election will take place only after the end of the electronic election.

7. *Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured. (○)*

The list of voters is compiled based on the identification of voters using a defined e-mail address. Each email address will receive its authentication information. Members of the electoral commission, including the administrator, have access to the list of voters' e-mails, including information about the voter's turnout. Belenios provides authorization verifiability, where anyone can check that votes come from eligible voters (Cortier et al. 2019). According to Baloglu et al. (2021a), it has been shown to satisfy formal requirements for the verifiability of elections, both in the symbolic model for a particular variant (Cortier et al., 2019) and in the computational model (Cortier et al., 2018). Still, there are issues regarding possible attacks on verifiability in case of registrar corruption. Even if the registrar and server are not compromised, individual verifiability can be compromised (Baloglu et al., 2021a).

8. *The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote. (○)*

The voter is authenticated using two elements, the login name and password on the one hand and the voting code on the other. These two elements

are transmitted separately, one by the voting server, and the other by the voting code generator. In case of loss or theft, the voter can request a new password. In this case, the old password is invalid. The voting code can also be sent back to the voter by the voting code generator (without change) - possibly by the authorized authority. If in the meantime the voting documents were used by a usurper, the voter can vote again with his new identifiers and the old vote will be canceled. In addition, identity theft voting generates an automatic receipt sent to the legitimate voter, greatly increasing the likelihood of detection of potential fraud (Cortier et al., 2020).

9. *The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box, and included in the election result. (○)*

The ballot containing the choice confirmed by the voter and signed with his valid code is completely prepared on the client side, including encryption. Registration to the ballot box is performed by the server on the condition that the ballot is valid (cryptographically) and that the voter's authentication has been successful. In this case, and only in this case, the attendance register is updated, the voter is sent a confirmation email with a tracking number that serves as a receipt, and the public ballot box also provides a way for the voter to check that their vote has been counted (Cortier et al., 2020).

10. *The voter's intention shall not be affected by the voting system, or by any undue influence. (○)*

The Electoral Commission should ensure that questions are asked impartially and correctly. The voting system itself is then displayed to all voters in the same way.

11. *It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter. (○)*

The voter will receive the voting URL of the election in e-mail and in the organization's internal information system. The voter can always verify that he is voting at the correct URL, and that the tracking code of his ticket is inserted in the correct ballot box, which is at the same URL of the sent election extended by "/ballots". The voter can check the submitted form of the ballot after authentication in publicly accessible election data.

12. *The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation. (○)*

The voting process has several steps that can always be repeated. It is even possible to submit a completely new ballot before the end of voting, which invalidates the originally submitted one.

13. *The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options. (○)*

After the voter's identity is verified, he is redirected to the blank ballot. A voter can also hand in a blank ballot. The neutral form of the ballot is ensured by the electoral commission through settings by the administrator. The resulting form can be verified using publicly available election data. Alternatively, the form of the ballot can be challenged and the electoral commission can be forced to correct it, including repeating the election in a correct form. The system does not allow you to set a benefit in the form of a pre-selection of one of the options.

14. *The e-voting system shall advise the voter if he or she casts an invalid e-vote. (○)*

After casting a valid vote in the ballot box, this information is displayed to the voter on the last page of the election and an information e-mail is sent. The system does not allow an invalid vote to be inserted into the ballot box. It is possible to allow the submission of a blank ballot, which is not inherently a validity error, but an opportunity to express the voter's will.

15. *The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable. (○)*

The confidentiality of the ballot during its processing and storage in the ballot box is ensured by the encryption used. Its integrity is ensured by double protection. On the one hand, the signature associated with the slip becomes invalid if the slip is modified (Cortier et al., 2020).

After the ballot is encrypted, a unique tracking code is displayed, which is also sent to the voter's e-mail after it is inserted into the ballot box. The ballot box publicly displays a list of tracking codes, according

to which the voter can verify the counting of his vote in the original encrypted form.

16. *The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed. (○)*

Information about the successful submission of the ballot is displayed on the last page of the voting process, information about the submission of the vote is also sent to the voter's e-mail address.

17. *The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system. (○)*

Voters can check the presence of their ballot in the ballot box, and external audits ensure that the ballot box only grows. By auditing, anyone can verify, based on public data, that the cryptographic data is consistent (for example, consistency between the public keys of decryption authorities and the public key of elections). After counting, it is possible to make sure that the result corresponds to the encrypted ballots of the ballot box, thanks to the cryptographic evidence provided by the decryption authorities (Cortier et al., 2020). In the Belenios system, no single party needs to be fully trusted, as verifiability is ensured as long as neither the election server nor the registrar is compromised. The registrar generates public credentials, posts them on a bulletin board, and distributes the associated private credentials to voters. The public login serves as the authentication key of the newly created signature key pair, while the private login is the corresponding signature key. The votes are signed and the election authorities can verify on the bulletin board that all votes have been cast by the expected eligible parties (Baloglu et al., 2020).

18. *The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system. (○)*

The voting server does not have a signing key, so it cannot create a valid signature. In theory, only unauthorized vote deletion could occur. But this would be revealed because voters can check the presence of their ballot in the ballot box and external audits ensure that the ballot box is only growing. The ballot box (that is, the list of encrypted ballots), the public election key, the list of questions, and the list of public parts of the election codes can be viewed publicly by anyone who knows the election URL. Automatic programs, apart from the voting server, regularly monitor this data (external auditors can also perform this monitoring). Modification of election data (deletion of the ballot paper, change of the list of public voting codes, etc.) would therefore be detected immediately (Cortier et al., 2020).

19. *E-voting shall be organized in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure. (○)*

The ballot is encrypted and sent to the server via an HTTPS channel, which adds a second layer of encryption and ensures integrity. On the other hand, the ballot is authenticated thanks to the signature derived from the voting code, it is not possible to modify the ballot while maintaining a valid signature. Finally, the integrity of the ballot is again ensured by the fact that the voter can verify the presence of his own ballot in the ballot box with his tracking number (Cortier et al., 2020). The open-source election system Belenios allows the use of homomorphic programming (Glondu, 2023) to carry out an election by keeping individual ballots secret, enabling their verification and simultaneously displaying the overall election results.

Currently, there is no formal, universal definition for End-to-End Verifiability (E2Ev) because the associative and commutative operators are inaccessible to symbolic analysis tools, which for example makes it impossible to analyze the following homomorphic property as stated in (Cortier, 2015):

$$enc(pk; v_1) * enc(pk; v_2) = enc(pk; v_1 + v_2) \quad (1)$$

where * and + are associative and commutative operators. Thanks to them it is possible to sum the contents of votes (v_1 and v_2) encrypted (*enc*) with the public key (*pk*) without further decrypting them individually.

After the election results have been evaluated and confirmed, voter lists including access codes as well as decryption keys should be deleted. The choice itself is archived and subsequently deleted.

20. *The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election. (○)*

Voter lists are separate from the ballot box. After the election is over and the results are confirmed, the entire election, including voter lists containing email addresses, can be deleted.

21. *The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. (○)*

Authentication data is encrypted on the election server, or on a third-party server in the case of using CAS. The voter will receive the password by e-mail, in case of losing the password, they can have a new password generated by the administrator.

22. *Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties. (○)*

The voter register is not public. It is updated by the server and made available to election administrators. In case of doubts about its integrity, the compliance of the voter registers with the ballot box can be checked by the voting code generator (authorized authority), which knows the link between the codes used to sign the ballot boxes and the voters. The voter list is accessible to the administrator and authorized authority, who should make it available to the electoral commission for review.

23. *An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties. (Δ)*

The system does not allow you to find out the content of the submitted vote. The voter can only verify that the vote in the ballot box is the same as the one he cast.

The system is not resistant to coercive voting, when the voter would be influenced by the participation of a third person to make the election, if he voluntarily gave the third person a public imprint of the ballot submitted in front of him to verify the counting of the given vote in the ballot box (Cortier et al., 2019).

24. *The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period. (○)*

The counting option can only be activated after the voting is closed. Each decryption authority then performs the calculation on its own computer using its private key. After reaching the contribution threshold, the result is announced. Partial counting cannot be done during the election, because the counting operation can only be activated once and requires the active participation of the decryption guarantors.

25. *E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected. (○)*

The content of the voter's previously submitted ballot is always overwritten by the newly submitted ballot. The results of earlier elections are not archived for a long time.

26. *The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous. (○)*

Tightness between the voter's identity and the expression of his vote is ensured by two means. The keys needed for decryption are generated and stored on separate, independent machines, managed by different persons or entities, as it is on the one hand the server and on the other hand the decryption authorities chosen by the electoral commission. It is even unlikely that they all have the same operating system, for example. Thus, while a link is established between the voter and his encrypted ballot, it is not possible to establish a link between the voter and the cast of the vote. During analysis, the keys necessary for decryption remain on separate, independent computers managed by different people or entities. Voters' encrypted ballots are never deciphered. Belenios uses two decryption solutions depending on the voting method used: homomorphic counting or verifiable mixnets. In both cases, no link can be established between the expression of the vote and the voter (Cortier et al., 2020).

27. *Member States that introduce e-voting shall do so in a gradual and progressive manner. (Δ)*

In the Czech Republic, it is not possible to vote electronically in major political national elections, on the other hand, it is not prohibited to vote electronically in elections of private or public organizations. As electronic voting is only possible in minor elections, the rollout can be considered gradual and progressive.

28. *Before introducing e-voting, member States shall introduce the required changes to the relevant legislation. (Δ)*

Electronic voting in national elections has not yet been introduced in the Czech Republic. Electronic voting within organizations should be governed by statutes and other legal regulations.

29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them. (○)

Within the organization, responsibility can be defined by its own statutes, regulations or resolutions, including the designation of the election commission. In the event of a possible future introduction to national elections, a significant change in the country's laws will be needed.

30. *Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process. (Δ)*

The decryption of the tallied results is carried out by guarantors who are part of the electoral commission. Anyone with access to the election URL can verify the data used in the census based on publicly available data.

31. *Member States shall be transparent in all aspects of e-voting. (Δ)*

In the event of the eventual introduction of nationwide electronic voting, the state must be transparent, similar to the proposed procedure for electronic voting in organizations.

32. *The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: any steps a voter may have to take in order to participate and vote; the correct use and functioning of an e-voting system; the e-voting timetable, including all stages. (○)*

The organization informs voters of the plan for conducting electronic elections in the invitation to the meeting, the voter obtains information using the internal information system and e-mail. Detailed instructions should also always be available.

33. *The components of the e-voting system shall be disclosed for verification and certification purposes. (○)*

Belenios is open source, which is free to download and verify the code. Likewise, certain election data required for certification is publicly available.

34. *Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results. (Δ)*

Anyone who knows the election URL can view the ballot box and public data. After the election result is decrypted, anyone can perform verification based on public data and third-party tools.

35. *Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate. (Δ)*

Belenios is open source, and it also offers a tool for calculating a unique fingerprint as open source. The system allows the development of other third-party control systems.

36. *Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date. (Δ)*

State assessment and certification requirements should be developed for possible national elections in the future.

37. *Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control. (○)*

We checked the functionality of the Belenios system by testing our own installation. A security analysis (Cortier et al., 2020) compares the fulfillment of the technical requirements

of the CNIL (La Commission nationale de l'informatique et des libertés, 2019). The Belenios voting platform meets levels 1 and 2 defined by the CNIL as well as level 3 depending on the chosen implementation (Cortier et al., 2020).

38. *The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.* (✗)

Belenios allows anyone who knows the election URL to audit voting results. The standards for issuing the certificate have not yet been defined.

39. *The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats. (Δ)*

The auditor regularly downloads the contents of the ballot box and checks its consistency. These tests ensure that no votes have disappeared and that only legitimate (properly signed) votes have been added. This audit is performed at least by an automatic program set up by the Belenios team, but it can also be performed by third parties. Software tools enabling these tests are available in the open-source Belenios code. On the other hand, the detailed specification of Belenios also allows to reprogram all the tests. In addition, voters can check at any time whether their ballot is in the ballot box. This last point means that security does not rely as much on attendance as with a traditional system. However, verification that this is consistent with the ballot box can be permanently done by the voting code generator (Cortier et al., 2020).

Belenios has an active academic community working on updates as well as third-party solutions for greater control and auditing of the elections made. Belenios publishes public data that allows for an audit. The Belenios system, compiled in the object-oriented programming language OCaml, is open source, including the auditing part. The academic community also informs about potential problems and threats in professional publications (Baloglu et al., 2021b).

40. *The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system. (○)*

The electoral commission is responsible for the correctness of the election, which may also have tools for correction, including the possibility of extending the vote or repeating it.

41. *Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated. (Δ)*

In the case of using the official Belenios installation, the server of the Belenios platform is hosted by the LORIA high-security laboratory. It thus benefits from associated services: controlled physical access, activity monitoring, and logical separation with other hosted services. The system is a stable version, with a limited number of services and regular updates. The list of people with physical and logical access to the server is limited and controlled (Cortier et al., 2020).

Only members of the elected electoral commission have access to voter lists including e-mails, the connection with the access code is handled by the authorized authority.

42. *Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly. (Δ)*

We verified the correct functionality of the system by installing it ourselves. Before the start of the election, the functionality of the system is verified by the administrator and other members of the election commission.

43. *A procedure shall be established for regularly installing updated versions and corrections of all relevant software.* (✗)

In the case of using the official Belenios installation, the system developers themselves ensure that the system is kept up-to-date.

44. *If stored or communicated outside controlled environments, the votes shall be encrypted. (○)*

All ballots are encrypted.

45. *Votes and voter information shall be kept sealed until the counting process commences. (○)*

Only members of the election commission have access to personal information in the form of e-mail. Votes are encrypted, the electoral commission

only obtains information about the participation of individual voters in the vote.

46. *The electoral management body shall handle all cryptographic material securely. (○)*

Guarantors whose private keys are needed to decrypt the election results are advised to store the decryption keys securely. The authorized authority is informed of the need to handle voters' access codes with care.

47. *Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body. (Δ)*

Voters and auditors immediately inform the electoral commission of suspicious events, in case of a suspicious event with a member of the electoral commission, the superior/chairman of the given organization should be informed immediately.

48. *The authenticity, availability, and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected. (○)*

The list of voters is entered into the systems by the administrator based on e-mails delivered, for example, from the organization's internal systems. The list of voters does not change throughout the election and, including personal data in the form of e-mail, is available exclusively to members of the electoral commission. Voters should be familiarized with the protection of personal data under the GDPR, the organization can extend its personal data protection conditions beyond the requirements of the Belenios system itself, for example within the registration conditions for the organization's internal information system.

49. *The e-voting system shall identify votes that are affected by an irregularity. (○)*

As part of the audit carried out by the electoral commission, which can be carried out by anyone who has access to the URL of the given election, possible irregularities should be identified.

Discussion

Even though the recommendation of the Council of Europe is important for the member states, the verification of the internet voting system or the proposed method of the voting procedure following the Recommendation of the Council of Europe is not a common part of the documentation. Even the documentation (Cortier et al., 2020) of the investigated French Belenios system evaluates its security only in accordance with the national requirements for electronic voting. The methodological procedures for evaluating electronic elections focus more on the system itself (Panizo Alonso et al., 2018) and only exceptionally evaluate the entire methodological procedure of real elections.

As evidenced by the assessment, elections in Ontario would not meet the requirements of the Council of Europe recommendations (Brunet and Essex, 2023). Token and envelope protocols are evaluated in more detail by academic staff often not directly connected to the development of the given system, while for example evaluating their strengths and weaknesses in relation to the recommendations of the Council of Europe CM/Rec(2017)5. The findings show that envelope protocols do not meet the requirements of the recommendation, while token protocols can meet the requirements if certain technical provisions are met (Bagnato, 2022).

The independent evaluation of voting procedures using the electronic voting system by a trusted authority is fundamental in terms of its application use by the general public, therefore it is advisable to strive for greater standardization of the evaluation and the way it is made available to all users of the system. The transparency of the i-voting system is important in terms of the Council of Europe (2017) recommendations and for building credibility. Similarly, research on the Swiss electoral system (Driza Maurer, 2019) calls for an emphasis on the transparency of the system. The requirement for public source code is also highlighted by Buckland et al. (2012) who conclude that the lack of transparency in the Australian e-voting system may negatively affect voter attitudes towards e-voting. Volkamer et al. (2011) also rate the transparency of an electoral system as crucial with respect to credibility. Few countries have developed adequate legislation or standards for online voting systems (Brunet et al., 2022).

Conclusion

From the described analysis, it follows that the proposed method of conducting a remote electronic secret election can to a certain extent meet most of the requirements

of the Council of Europe (2017) recommendation in the case of a less important election within the agricultural organization. The proposed procedure methodology does not provide for the certification required by Requirements 38 and 43. The proposed methodological procedure does not meet requirement 23, which requires the prevention of the possibility of transferring information about the choice to a third party. On the other hand, this requirement is better addressed by the possibility of repeated voting than in the postal elections that operate in many EU countries, and is less essential for elections in private institutions, since the verification of the voter's choice in this case can be legitimate. For example, in the case when a cooperative member/shareholder delegates a representative to express his will when electing the board. BeleniosRF should bring an improvement in resistance to coercion (Chaidos, 2016). Points 27, 28, 29, 31, and 36, which deal primarily with requirements for the state, are obviously relevant to national elections to the Parliament, etc., even so, they are fulfilled to a certain extent for electronic voting in the organization. A greater level of security could be provided by the use of a third-party authentication system (CAS), which will simultaneously require two-factor authentication.

Acknowledgments

This work was conducted within the project “Smart environments - modeling and simulation of complex decision-making problems in intelligent systems” (2022B0010) funded through the IGA foundation of the Faculty of Economics and Management, Czech University of Life Sciences in Prague.

Corresponding author:
Ing. Tomáš Martínek
Department of Information Engineering, Faculty of Economics and Management
Czech University of Life Sciences Prague, Kamýcká 129, 165 00, Prague, Czech Republic
E-mail: martinekt@pef.czu.cz

References

[1] Accessibility Checker (2023) "*Audit*", Accessibility Checker. [Online]. Available: https://www.accessibilitychecker.org/audit/ [Accessed: Feb 20, 2024].

[2] Adida, B., de Marneffe, O., Pereira, O. and Quisquater, J. -J. (2009) "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios", *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections, EVT/WOTE*. [Online]. Available: https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/adida-helios.pdf [Accessed: Feb 20, 2024].

[3] Agbesi, S., Budurushi, J., Dalela, A. and Kulyk, O. (2023) "Investigating Transparency Dimensions for Internet Voting", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2023, Lecture Notes in Computer Science, Conference paper, Vol. 14230. Springer, Cham, pp. 1-17. ISBN 978-3-031-43756-4. DOI 10.1007/978-3-031-43756-4_1.

[4] Bagnato, D. (2022) "Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols", *Proceedings of the Central and Eastern European eDem and eGov Days*, pp. 169-178. ISBN 9781450397667. DOI 10.1145/3551504.3551519.

[5] Baloglu, S., Bursuc, S., Mauw, S. and Pang, J. (2021a) "Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios", *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, pp. 1-15. ISBN 978-3-030-86941-0. DOI 10.1109/CSF51468.2021.00019.

[6] Baloglu, S., Bursuc, S., Mauw, S. and Pang, J. (2021b) "Provably Improving Election Verifiability in Belenios", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting.* E-Vote-ID 2021, Lecture Notes in Computer Science, Conference paper, Vol. 12900, Springer, Cham. DOI 10.1007/978-3-030-86942-7_1.

[7] Belenios team (2023) "*Who does what during a Belenios election?*", Belenios. [Online]. Available: https://www.belenios.org/instructions.html [Accessed: Feb 20, 2024].

[8] Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D. and Walter, J. (2022) "An Analysis of the Security and Privacy Issues of the Neovote Online Voting System", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2022, Lecture Notes in Computer Science, Conference paper, Vol. 13553, Springer, Cham, pp. 1-18. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_1.

[9] Brunet, J. and Essex, A. (2023) "Online Voting in Ontario Municipalities: A Standards-Based Review", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting,* E-Vote-ID 2023, Lecture Notes in Computer Science, Springer, Cham, Conference paper, Vol. 14230, pp. 52-68. ISBN 978-3-031-43756-4. DOI 10.1007/978-3-031-43756-4_4.

[10] Brunet, J., Pananos, A. D. and Essex, A. (2022) "Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting,* E-Vote-ID 2022, Lecture Notes in Computer Science, Springer, Cham, Conference paper, Vol. 13553, pp. 36-52. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_3.

[11] Buckland, R., Teague, V. and Wen, R. (2012) "Towards Best Practice for E-election Systems", In: Kiayias, A., Lipmaa, H. (eds) *E-Voting and Identity.* Vote-ID 2011, Lecture Notes in Computer Science, Vol. 7187. Springer, Berlin, Heidelberg pp. 224-241. ISBN 978-3-642-32746-9. DOI 10.1007/978-3-642-32747-6_14.

[12] Cortier, V. (2015) "Formal verification of e-voting: solutions and challenges", *ACM SIGLOG News*, Vol. 2, No. 1, pp. 25-34. ISSN 2372-3491. DOI 10.1145/2728816.2728823.

[13] Cortier, V., Dragan, C. C., Dupressoir, F. and Warinschi, B. (2018) "Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios", *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, Oxford, UK, pp. 298-312. ISSN 2374-8303. DOI 10.1109/CSF.2018.00029.

[14] Cortier, V., Gaudry, P. and Glondu, S. (2019) "Belenios: A Simple Private and Verifiable Electronic Voting System", In: Guttman, J., Landwehr, C., Meseguer, J., Pavlovic, D. (eds) *Foundations of Security, Protocols, and Equational Reasoning,* Lecture Notes in Computer Science, Springer, Cham, Vol. 11565, pp. 214-238. ISBN 978-3-030-19052-1. DOI 10.1007/978-3-030-19052-1_14.

[15] Cortier, V., Gaudry, P. and Glondu, S. (2020) "*Analyse de sécurité de la plateforme de vote Belenios Conformité avec les recommandations 2019 de la CNIL*", Belenios. [Online]. Available: https://www.belenios.org/analyse-secu.pdf [Accessed: Feb 20, 2024].

[16] Council of Europe (2017) "*Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*". [Online]. Available: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f [Accessed: Feb 20, 2024].

[17] Czech Republic (2012) "*Zákon č. 90/2012 Sb. - Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)*", Sbírka zákonů. [Online]. Available: https://www.e-sbirka.cz/sb/2012/90/2023-07-01 [Accessed: Feb 20, 2024]. (In Czech).

[18] Driza Maurer, A. (2019) "The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting,* E-Vote-ID 2019. Lecture Notes in Computer Science, Vol. 11759, pp. 83-99. ISBN 978-3-030-30625-0. DOI 10.1007/978-3-030-30625-0_6.

[19] Driza Maurer, A., Volkamer, M. and Krimmer, R. (2023) "Council of Europe Guidelines on the Use of ICT in Electoral Processes", In: Katsikas, S., et al. *Computer Security. ESORICS 2022 International Workshops*, Lecture Notes in Computer Science, Springer, Cham, Vol. 13785, pp. 585-599. ISBN 978-3-031-25459-8. DOI 10.1007/978-3-031-25460-4_34.

[20] Glondu, S. (2023) "*Belenios specification: Version 2.1*". [Online]. Available: https://www.belenios.org/specification.pdf [Accessed: Feb 20, 2024].

[21] Chaidos, P., Cortier, V., Fuchsbauer, G. and Galindo, D. (2016) "BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme", *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, pp. 1614-1625. ISBN 978-1-4503-4139-4. DOI 10.1145/2976749.2978337.

[22] Kánská, E., Jarolímek, J., Hlavsa, T., Šimek, P., Vaněk, J. and Vogeltanzová, T. (2012) "Using social networks as an integration tool in rural areas of the Czech Republic - agricultural enterprises", *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, Vol. 60, No. 4, pp. 173-180. ISSN 1211-8516. DOI 10.11118/actaun201260040173.

[23] Kořínková, J., Čížková, Z. and Němčík, L. (2017) "*170 COOP*". ISBN 978-80-87118-11-5.

[24] La Commission nationale de l'informatique et des libertés (2019) "*Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet: NOR: CNIL1917529X*", Légifrance. [Online]. Available: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239 [Accessed: Feb 20, 2024]. (In French).

[25] Martínek, T. and Malý, M. (2024) "Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party", *Acta Informatica Pragensia*, Vol. 13, No. 3, pp. 395-417. ISSN 1805-4951. DOI 10.18267/j.aip.249.

[26] Martínek, T. and Tyrychtr, J. (2024) "A questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges [Data set]", Zenodo. [Online]. Available: https://zenodo.org/records/11234690 [Accessed: May 21, 2024].

[27] Panizo Alonso, L., Gascó, M., Marcos del Blanco, D. Y., Alonso, J. Á. H., Barrat, J. and Moreton, H. A. (2018) "E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting", *IEEE Transactions on Emerging Topics in Computing*, Vol. 9, No. 1, pp. 161-173. ISSN 2168-6750. DOI 10.1109/TETC.2018.2881891.

[28] Rodríguez-Pérez, A. (2022) "The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update?", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2022, Lecture Notes in Computer Science, Conference paper, Vol. 13553. Springer, Cham, pp. 90-105. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_6.

[29] Rysová, H., Kubata, K., Tyrychtr, J., Ulman, M., Šmejkalová, M. and Vostrovský, V. (2013) "Evaluation of electronic public services in agriculture in the Czech Republic", *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, Vol. 61, pp. 473-479. ISSN 1211-8516. DOI 10.11118/actaun201361020473.

[30] Valimised.ee (2023) "*Statistics about Internet voting in Estonia*", Valimised.ee. [Online]. Available: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia [Accessed: Feb 20, 2024].

[31] Volkamer, M., Spycher, O. and Dubuis, E. (2011) "Measures to establish trust in internet voting", *ICEGOV '11: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, Tallinn, Estonia, pp. 1-10. ISBN 978-1-4503-0746-8. DOI 10.1145/2072069.2072071.