Electronic Voting and Its Use - E-elections

Juraj Fabus
Department of Communications
University of Zilina
Zilina, Slovakia
email: juraj.fabus@fpedas.uniza.sk

Iveta Kremenova
University of Zilina

Viktoria Fabusova
University of Zilina

***Abstract*— The paper is devoted to the issue of electronic signature in the Slovak Republic. It identifies perspective area for electronic signature use - electronic voting. It discusses possible factors that are essential for the introduction of e-elections to life for citizens of the Slovak Republic.**

***Keywords*-Electrocic voting; security; national ID card.**

I. INTRODUCTION

The subject of this paper is the possibility of using an electronic signature within the concept of e-voting. The aim is to raise awareness of electronic signature, to increase interest in its use, as well as to describe the conditions necessary for the introduction of e-voting.

For example, Estonia is the only country in the world that relies on Internet voting in a significant way for legally-binding national elections — up to 25% of voters cast their ballots online. Independent evaluation [1] of the system urgently recommends that Estonia discontinue use of the system.

The reason for which e-election should be introduced is so, that the Slovak citizens, who live abroad, and the number of which is estimated at around 250,000, can also participate in elections. Today they need to handle long and difficult election by post and mainly for this reason, their voter turnout is so low.

In Section 2 we describe why it would be good to use e-voting in Slovakia. In Section 3, the requirements for protocol used in electronic voting are introduced. Section 4 is about the up and downs of e-elections. Last section – Section 5 – is about eID card project and the possibilities of implementation of e-elections in the Slovak republic.

II. ELECTRONIC VOTING

With regard to electronic voting, the most asked question is its application in national elections. The benefits is particularly in financial savings, speeding-up of results counting, simplification of act of election and to increase participation of younger generation. The field of its use is much broader, ranging from regional elections through referendum, various selection procedures up to the polls. Such use of electronic elections in Slovakia requires the necessary legislative amendments.

On the other hand, the electronic voting as a cheap and quick way to vote could lead to the creation of new institutions. The use of e-voting could be quickly fastened in the university environment, where we can expect computer-proficient people, and where complicated legislative changes are not necessary [2].

III. SECURITY PROTOCOL OF E-ELECTIONS

Implementation of e-voting protocol consists of several phases (Figure 1), which must be performed in a prescribed order.

In the Constitution of the Slovak Republic, it is stated that suffrage is universal, equal, direct and conducted by secret ballot. Electronic voting should be able to enable citizens to realize this right. Possible election fraud and particularities of electronic voting deliver additional requirements:

- Eligibility - Only eligible voters who meet certain well-defined criteria may participate in the vote. Verification of the eligibility to participate in the elections together with mechanisms to avoid multiple counting of voters' votes, must be part of an electronic election scheme. If not, dishonest participant can manipulate with the election results.
- Election verifiability - voter should be able to verify that his vote was recorded and counted correctly in the election results. We distinguish between individual and universal verifiability. This requirement is important for the confidence of voters in the electoral system, including the results. Then, uncontrolled authorities would not be able to manipulate the election results without verification of voters or others.

ISBN: 978-1-61208-485-5

- Repudiation of vote - Scheme should have mechanisms to deal with inconsistencies in the various stages. For example, if voter finds that his vote was not counted in the election results despite the fact that he participated in the voting, there should be a mechanism that would be able to demonstrate his legitimate complaint against the electoral authorities.
- Justice - No one should have access to partial results if the elections are still ongoing. This information can be misused in a pressure on voters who have not yet participated in the election.
- Secrecy of voting - in electronic voting envelope, the selected option must not identify the voter. Each links between the ballot and the voter has to be deleted. This requirement protects the privacy of the voter in the election, so that he cannot be penalized in any way for the vote.
- Urgency of elections – after the vote, voter would not be able to obtain the document, with which would be able to prove his choice to someone else. This requirement is to impede vote buying [2].

In technological terms, system for electronic voting could operate in different ways. To prevent abuse of the system, the system should be based on qualified electronic signatures. It is a condition for online communication between authorities and citizens.

There are two basic types of protocols in an e-election - a scheme based on blind signature, and a scheme based on homomorphic encryption [3]. Blind signature, as introduced by David Chaum [4], is a form of digital signature in which the content of a message is blinded before it is signed. A homomorphic encryption scheme is a crypto system that allows computations to be performed on data without decrypting it.

With qualified electronic signature, the voters would encrypt the vote by the public key and add the proof of the correctness of the encrypted message, i.e., it comprises a vote of one of the possible candidates only. After signing this report it will be sent to registration server. It checks the voter's eligibility to participate in the election, verifies the signature and fairness of accompanied evidence. If all is well, encrypted vote of the voter can be published.

IV. Benefits and risks of e-election

For young people who are accustomed to work with the Internet, e-elections would represent a more comfortable alternative that reflects their lifestyle. Any qualified voter would be able to vote from anywhere with internet access. On the other hand, especially for representatives of the older generation who are not adept in using computers, there should still be a space to participate in public affairs in classical way.

There are real technical risks of e-voting over the internet, which should not be overlooked. As a threat, we consider an attack to disrupt the election services with a consequent avoidance of the vote. It is desirable to describe the possible internal and external attacks on individual components of the electoral system. Creating and maintaining people's confidence in the accuracy and security of the electoral process is the basis for the use of electronic voting [2].

V. Situation in Slovakia

Implementation of e-elections in the Slovak Republic should be realized on a long-term concept of informatisation of society and should not be done quickly, because currently our country is not ready for such elections yet.

The first major step toward introducing of e-elections into practice was disclosure of the call for project on a national electronic ID card by the Ministry of Finance. This card should contain components to implement qualified electronic signature. Legal acts carried with it by a citizen, will be then unquestionable. So, the state would provide (and delivered as well) an electronic signature free of charge to every citizen to communicate with other bodies. Such identification card creates good starting conditions for the nationwide e-voting use.

The price of ID card with electronic-signature and the costs associated with its use can influence Slovaks on whether or not to use public services online, and decide whether the vicious circle will finally break, as the weak extension of the qualified electronic signature hinder the use of services. Lack of services on the other hand, inhibits expansion of e-signature [5].

By the end of April 2016, more than 804,000 Slovak citizens had eID cards. Less than 39,000 of them requested also the certificates that enable the creation of advanced electronic signature. The Ministry of Finance is responsible for the implementation of eID cards. It is not clear why people do not apply for advanced electronic signature (free for first five years). Research in this area will be needed.

In [6], the authors proposed a concept of academic election system that can provide voting services for different university applications, e.g., university information system portal, virtual collaboration, video conferencing system, etc. This election system was tested in the project “Modern European elections” [7]. Background process of e-elections is technically highly complex. But for voters casting votes it looks like a simple task. During the simulation, the students inserted the voter card into the chip reader and then entered the PIN. After that, from a desktop application, they selected a party for which they wanted to vote and with a click their choice was sent.

Other, not less important conditions are legislative changes, expanding the availability of broadband Internet, the political will and other factors. Also it is appropriate to establish an expert commission which will assess the social, technical and legal aspects of the use of computerized elections in Slovakia in the context of the development of eGovernment. In view of all the conditions to be met, it seems unrealistic to put the nationwide elections into practice prior 2017 [2].

VI. Conclusion

Current state of the electronic signature has positive and also negative effect on the situation in the Slovak Republic.

The electronic signature is not exerted nowadays because of the small extension. It is assumed that these problems will soon be removed, and the competent authorities will pursue the main idea of an electronic signature. Research projects, such as the “Academic election system” and “Modern European elections”, which are initiated from bottom, can help to gain the necessary experience with the creation and use of electronic elections. They open public discussion on the future of e-voting in Slovakia.

REFERENCES

[1] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine. J. Halderman, “Security Analysis of the Estonian Internet Voting System”, In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS ’14), November 2014.

[2] M. Novotný, “Electronic voting - a sci-fi or near future?”, Available from: http://www.itnews.sk/tituly/infoware/free-clanky/2009-11-09/c130130-iw-elektronicke-volby-sci-fi-alebo-blizka-buducnost, [retrieved: may, 2016].

[3] R. Sampiegethaya, R. Poovendran, “A Framework and Taxonomy for Comparison of Electronic Voting Schemes”, Elsevier Computers & Security, vol. 25, 2006.

[4] D. Chaum, “Blind signatures for untreaceable payments”, Crypto 82, 1982.

[5] G. Jarosova, “Online election at the earliest in 2014”, Available from: http://fwd.etrend.sk/vsetko/online-volby-najskor-v-roku-2014.html, [retrieved: may, 2016].

[6] M. Novotny, “Design and analysis of a practical e-voting protocol”, in the Proceedings of FIDIS/IFIP Internet Security & Privacy Summer School 2008, Springer IFIP, vol. 298, 2009.

[7] Modern European elections Project Website. Avaliable from: http://ics.upjs.sk/evolby, [retrieved: may, 2016]

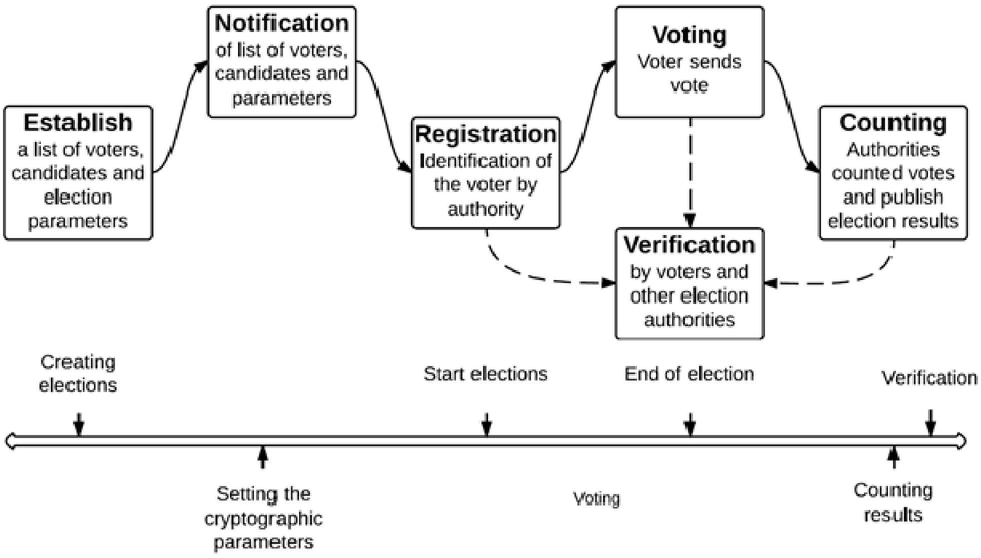
Establish
a list of voters, candidates and election parameters
Notification
of list of voters, candidates and parameters
Registration
Identification of the voter by authority
Voting
Voter sends vote
Verification
by voters and other election authorities
Counting
Authorities counted votes and publish election results
Creating elections
Start elections
End of election
Verification
Setting the cryptographic parameters
Voting
Counting results

Figure 1. Phases of an implementation of security protocol in electronical election implementation (Source: own processing).