NEW E-VOTING TECHNOLOGIES PRESENTING A DEMOCRATIC ALTERNATIVE TO MASS RIOTS

Sergei Ablameiko [1], Nikolai Kalosha [2], Sergei Bratchenya, Vitaly Lipen [3]

Abstract

Characteristics of different types of electoral technologies are considered, as well as their impact on their uses in different countries. A new approach to organization of election events based on a system of external monitoring of elections is proposed. Model implementation of the severs and the web portal of the proposed 'Guarantor' system is presented, as well as the results of an ongoing effort to create a complete prototype of an Internet voting system.

1. Introduction

The preparation of the current paper coincided with tragic events in North Africa as well as many other countries. According to analysts social and political outbursts in this group of countries is caused by several reasons. One major cause is that usually these countries can be characterized by a long-standing monopoly on power held by a single political party, clan or an authoritarian ruler. Inevitably, there appears a movement opposing the regime, which quickly exhausts the few available constitutional instruments at its disposal, and instead starts rallying the citizens to unsanctioned mass manifestations, which in turn are brutally subjugated by police and army forces loyal to the current rulers. At the same time, even popular protests numbering hundreds of thousands of demonstrators cannot be used to gauge the number of people opposing the current regime since the voices of the majority of the citizens remain unheard. The exact number of supporters and opponents of the ruling power can only be established by holding free election events or properly conducted polls, which should necessarily guarantee the anonymity of the electors or respondents.

It is most unfortunate that for a number of authoritarian regimes both country-wide and local elections are more of a ritual serving to achieve a degree of legitimization in the eyes of the international community. These regimes are in a position to falsify the results of the elections in any way they want, which can be explained by non-transparent voting technologies, lack of political education in the society at large, and, last but not least, the repressive actions of the government stifling any and all efforts of the opposition. In the described scenario, the electors become either apathetic to election events, often ignoring them completely, or are driven to desperate protest actions. Examples of Zimbabwe, Kenya, Nigeria, Iran, Cote d'Ivoire, Kirgystan, Egypt, Tunisia, Yemen, Haiti, Albania Kosovo and a number of post-Soviet republics show that mass protest are mostly a consequence of

[1] Belarusian State University, Nezavisimosti av. 4, 220030 Minsk, Republic of Belarus
[2] Institute of Mathematics, National Academy of Sciences of Belarus, Surganova 11, 220072 Minsk, Republic of Belarus
[3] United Institute of Informatics Problems, National Academy of Sciences of Belarus, Surganova 6, 220012 Minsk, Republic of Belarus

discontent of a certain part of the electors with the organization and the results of elections held in these countries. For instance, the results of the elections held in Egypt on the 28th November of 2010 were that out of the 35% of the citizens participating in the elections 92% voted for the ruling national-democratic party led by President Mubarak. A few weeks later rioting Egyptians burned down the headquarters of that party, expressing their actual attitude towards its members, who formed the backbone of Mubarak's bureaucratic administration. Similar events have been observed in many other authoritarian countries.

Is the community of developed countries able to offer the citizens and the rules of the countries discussed above an alternative way, one that is different from a long-time conservation of despotic regimes and an attempt to overthrow them in a bloody uprising similar to the events in Egypt and Tunisia? It is clear that the cost of passiveness in that matter is thousands of victims, hundreds of thousands of refugees and billions of euros spent on relief and peacekeeping efforts. A number of politicians, for example in Russia, have been heard saying that it's time to reconsider the matters of elections and legitimization of the government being a sovereign right of national governments. Perhaps an experiment should be conducted, offering technological aid to the countries where both governments and the citizens express interest in highly transparent elections controlled by international bodies. As shown in the authors' previous work [7], today's Internet technologies know no borders, and most services, including facilitation of electronic elections, can be provided to multiple countries from a single centre.

It can be expected that the governments confident of popular support would be receptive to an offer to be legitimized by an international committee using advanced information technologies certified by OCSE and the UN. Once the technology becomes available, it is natural to assume that governments of Morocco, Algiers, Bahrain and many other countries would approve voting events being monitored by an outside international guarantor organization, as independently verified election results would protect the government from accusations of election fraud. Provided that the proposed 'Guarantor' system of elections is being used, the citizens will also have an opportunity to verify their votes over the Internet or by SMS without compromising vote secrecy. Additionally, use of advanced technologies has the potential of making election events more cost-effective by reducing the number of personnel involved in the elections.

There are several examples of leaders viewed as authoritarian by the international community being open to modern electronic voting technologies. In 2003 Nursultan Nazarbaev, the President of Kazakhstan, has started the development of 'Sailau' electronic voting system, which was subsequently approbated and today is used at many of the Kazakh polling stations. In a recent interview [8], the Russian President Dmitri Medvedev has confirmed his intention to replace paper bulletin voting by a modern e-voting system. Before the recent elections, the President of Venezuela Hugo Chaves has stated that he completely trusts the e-voting system deployed in his country and will accept any results of the elections. Evidence of cost-efficiency of electronic voting can be found in India and Brazil, where inexpensive mobile e-voting stations have been used for several years. As a rule, e-voting systems are also capable of producing electronic reports on election events which can be presented to international observers (for example, the reports created by the Kazakh 'Sailau' system have been analyzed by OSCE experts).

Viability of the idea of offering a system of outside control and verification of election results to trouble countries can only be guaranteed if such system guarantees full automation of the elections, vote secrecy, transparency and reliability, ability to verify the results and protection from fraud and human error, also conforming to the guidelines set by organizations such as OCSE and the UN. A

centralized system of facilitating and supporting electronic elections internationally could also provide increased cost-efficiency due to virtual lack of downtime which is inevitable in election systems limited to a single nation.

The goal of the current research is to analyze the existing election technologies in order to incorporate the best known approaches to creating a voting systems with the properties outlined above, as well as justification of the concept and the architecture of the proposed 'Guarantor' system of election event monitoring, which is offered as a prototype of such systems.

2. Issues with existing voting technologies in troubled countries n

One can envision the general events leading to the society's inability to freely elect the governments in troubled countries. The less educated part of the population will generally trust the official propaganda, voting for the current government by rote. The socially active and politically educated citizens, seeing the evidence of fraud during previous elections, will often demonstratively ignore elections, becoming apathetic to political life in general. These people are well aware of the methods that can be used by state-appointed election committees to influence local election results, as well as the instances when local government representatives were reprimanded or even fired from the jobs because of unfavorable election outcomes. This knowledge leads to the obvious conclusion that local election committees have not only opportunity to commit election fraud, but also a very strong motivation, making foul play at the elections a near certainty.

It should be noted that many democratic instruments such as 'primaries', polls, free debates on the television and in printed media, collection of signatures in support of petitions or collection of exit poll data are either unused or similarly controlled by the governments of troubled countries. Additionally, any procedure that doesn't protect the respondents' anonymity is affected by the citizens' fear of invoking the displeasure of the government or local authorities. This becomes evident, for example, during the nomination of presidential candidates, when many citizens express their concerns about supporting an opposition candidate.

The troubled countries that are being discussed usually hold elections using traditional paper ballots. The ballots are marked by the electors and cast into sealed receptacles to be subsequently counted by local election committees. As stated in the report [9], the only issues arising during traditional voting in long-established democracies are ones related to the tediousness and inefficiency of the procedure. In troubled countries, on the other hand, the biggest problem of traditional paper ballot voting is its lack of transparency and susceptibility to fraud, as evidenced by routine post-election protests.

Neither winners nor losers of election events held by using paper ballots can prove beyond reasonable doubt to the society, media or an impartial court if the data gathered by local election committees (which is eventually aggregated to determine the nationwide election outcome) was accurate or falsified. Indeed, the election protocols are signed by heads of local election committees, which answer to local administration; there's no guarantee that the ballots have been marked by electors themselves and the signatures supposedly left by the voters during registration could just as well have been falsified, whilst at the same time a number of ballots has been 'thrown in' by the election committee. This type of fraud cannot be discovered by mandated procedures for verifying the election results, such as recounting the ballots. Numerous reports of dead people having been registered as voters during elections in ex-soviet countries are a testament to frequent 'throwing in' of fraudulent ballots.

It must be noted that despite the widespread expectations to resolve the issues identified with traditional voting by implementing electronic voting protocols, the actual results of introducing electronic elections are not entirely encouraging. Despite quick acceptance of electronic voting in USA, Canada, Switzerland, Australia, India, Brazil, Venezuela and several other countries, Ireland, the Netherlands and Germany have halted their e-voting programs. Somewhere in between these extremes lies Estonia, where every citizen was issued a personalized smart card capable of authentication generation of electronic signatures, which was subsequently used in an e-voting protocol. The 2008 elections have shown that the number of Estonians voting online has risen to 15% compared to 1% in 2005 (the year when the system was introduced). Still, a recent poll established that about 67% percent of the populace believe that internet voting does not guarantee vote secrecy and fairness of the elections. Prof. Thad Edward Hall, who is one of the leading researchers in the area of e-voting, has harshly criticized the approach in [10]. Criticism of the approach can be also found in [11], where it is emphasized that personal ID cards shouldn't be used in e-voting protocols due to public concerns about vote secrecy. Several Estonian activists have spoken against electronic voting in the press. Similar results have been observed in Kazakhstan, where only 14% of the voters chose electronic voting instead of using a paper ballot.

It is interesting to note that despite public concerns about vote secrecy, many e-voting protocols feature the same immediate depersonalization of votes as during traditional voting, leaving no opportunity to demonstrate to an individual voter that his choice has been properly recorded. This situation is analyzed in depth in [1–2]. An in-depth analysis of implementations of e-voting in developing and transitional countries can be found in [3], and proposals toward trusted voting can be found in [4]. A recent e-voting experiment in Austria was supervised by Robert Krimmer [13].

3. Key problems and the proposed solutions

As shown in the introduction, use of non-transparent paper-based technologies can lead to conflicts since neither the dominant political power (represented by local administrations and election committees) nor opposition candidates or parties have access to a reliable mechanism or a "drill-down" procedure to prove beyond reasonable doubt that the results of an election event (the recorded votes and voter registration data) are accurate or fraudulent. Observers present at polling stations can only confirm that they didn't see any deviations from the usual procedure. However, they normally can't access the primary data recorded on the ballots as well as the intermediate results which are used by the election committee to compile the final protocol of the election event at a given polling station. Thus, the observers find it nearly impossible to collect any evidence of the elections being dishonest. As shown by e.g. past election events in Moldova and Russia, once the protocol has been finalized and signed, the unused ballots have been destroyed and the ballots removed from the ballot boxes have been packed and sealed, the chances to nullify the numbers recorded in the protocol are almost zero.

At the same time, personal makeup of local election committees often leaves much to be desired. Members of these committees are tasked with manually registering electors, manual counting of ballots and compiling the final protocol of the election event at the polling station they've been assigned to. They're clearly in a position to influence election results, yet members of organizations and parties not affiliated with the government will often be prevented from joining local election committees. This fact is yet another reason to doubt the fairness of traditional elections under authoritative governments.

Thus, the fundamental requirement for an e-Voting technology that would replace traditional paper ballot voting in transitional and emerging democracies is to enable transparency of all stages of election events for the electors, members of the local elections committees, local and remote observers. This necessitates also recording and trusted electronic storage of every vote as well as the intermediate results obtained at the different polling stations. The e-Voting framework should prevent not only modification of the preliminary results, but also early access to these results by including a fully automated system that collects, processes and displays the voting data without any human participation.

The problem of increasing voter trust in electronic technologies, which would lead to eventually abandoning the traditional paper ballot voting, can be solved by offering to the electors cardinally new possibilities to verify voter registration and the vote without compromising vote secrecy. In order to realize such services, we propose that the traditional approach of immediate depersonalization of the results is replaced by a protocol where polling stations send to the election server data on the registration and the votes of electors using the proposed 'hidden' personalization technique. It is important to note that in Russia and Kazakhstan such 'hidden' personalization could be realized by modifying the internal software of the e-Voting equipment that is already used at some of the polling stations. Internet voting can incorporate this 'hidden' personalization through a specially designed protocol of interaction between the web-portal of the election event, the authentication/registration server and the vote casting server.
The proposed methodology of increasing voter trust in the official results of the elections is based on introducing, in addition to the electorate and the various election committees, an outside system of election event monitoring acting as a trusted third party. The functions of this system would include the following:

- performing the necessary cryptographic routines during the elections;
- processing of a request to hold an election event;
- generation of secure identifiers (SIDs) for all electors;
- presenting the electors with the information on the subjects of the voting;
- support of elector registration and on-line voting;
- off-line collection of local personalized results from standalone polling stations;
- displaying the results of an election event on the web-portal, including the individual results with 'hidden' personalization that can be verified by the electors.

Thus, the responsibility for aggregation of voting event results is shifted from election committees to an impartial automated system of monitoring and supervision that can be certified both by the government and the independent specialists. In addition, both electors themselves and remote election observers can use the web portal to monitor the collection and aggregation of votes. The results of an election event are then accepted if no protests have been raised during a certain period of time after the elections or if a satisfactory response to such protests was given by the administrators of the system or the organization holding the election event. This approach is similar to the principles of establishing the results of major sports events, where certified automated systems are used for measuring the performance of the contestants and displaying the intermediate and final results in real time.

Introduction of the "Guarantor" system or its analogue in the electoral process as the trusted third party requires a certain legal agreement between the organization supervising the system and the government body or other organization that holds the election event, which can take form of a con-

tract to provide an electronic service. Following that, the web portal of the future election event receives the complete information about the event, and after the election event is concluded its outcome is presented on the web portal as both the aggregated and local results, including the individual votes with 'hidden' personalization. A demonstration version of the portal, including the vote verification service, is available at http://e-vote.basnet.by/demo/eng.

As discussed at the authors' previous presentations at international conferences, the proposed technology can be considered suitable for elections in 'problem countries' with a universally trusted international organization, such as the European Council, assuming the role of the trusted third party. In such cases it may be wise to refrain from publishing the local outcomes so that the local administration cannot be held responsible for unfavorable results by the central government. One other feature to prevent tampering with the election results can be placing the servers responsible for authentication and aggregation of votes, as well as electronic voting, outside the country holding the elections.

We believe that such organization of the election event will leave the losing side with no grounds to dispute the results of the elections, and the winning side will have their victory confirmed by a trusted international organization. The polling station equipment proposed in the earlier publications by the authors makes it possible to organize both stationary and mobile polling stations that will enable deployment of the system in the countries with poor telecommunication networks. This offline mode of voting is well integrated in the system and retains the ability to verify individual votes. Approbation of the proposed autonomous voting equipment shows that it can be made very compact and extremely inexpensive. This would allow the trusted organization contracted to supervise the election event to provide this equipment for the duration of the election event and collect it after the event is finished.

4. Realization of the principles of trusted elections using the 'Guarantor' system

The proposed system is based on the authors' previous experience in developing electronic voting technologies for emerging democracies. Notable developments include the mock-up designs of electronic polling stations made for the Central Election Committee of Belarus as well as development of the prototype of 'Sailau' election system currently used in Kazakhstan [12]. The principles used in designing the latter have been patented [5].

In the previous year the authors have finalized the development of the complex of equipment to be used at the polling stations in the proposed voting system. The complex has been approbated and can be manufactured on demand [6]. It is designed to be fully integrated with the 'Guarantor' system, employing the same authentication procedure based on SIDs and personal data and the 'hidden' personalization of votes by a transaction authentication number (TAN). Below we have reproduced the approach to election events described in detail in [7] that supports voting at polling stations, over the Internet, by mail and by SMS. Authentication of the electors, as well as collection and aggregation of votes, is facilitated by the 'Guarantor' servers, allowing for centralized publishing of election event results and individual vote verification.

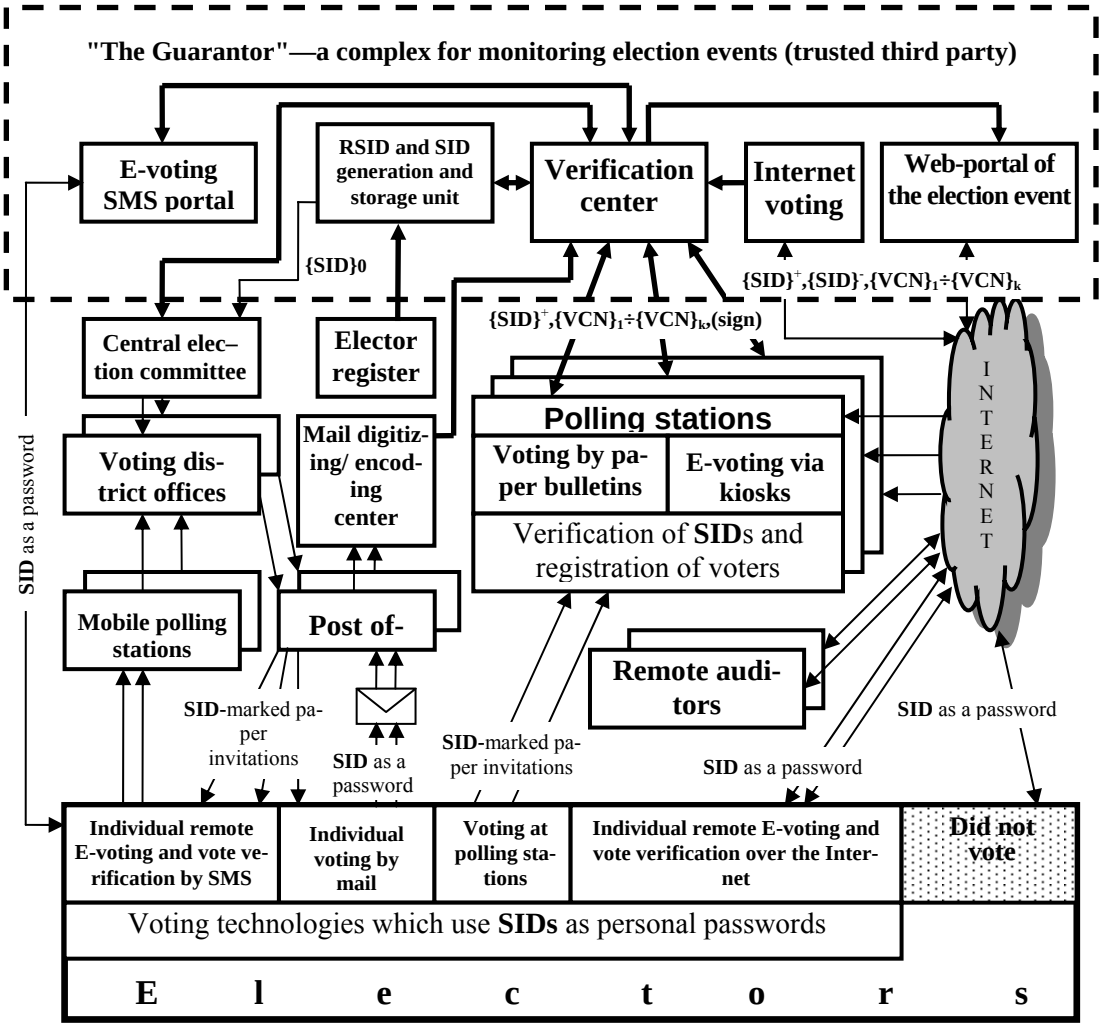

Figure 1 : Structure of an integrated state-scale voting systems

Lately the authors have focused their attention on Internet voting, considering that it's accessible to over 4 million Belarusians (even more if one considers the public Internet access points provided by schools and post offices) and that a wide-scale approbation can be organized much more easily over the Internet. Similar advantages of Internet voting have been pointed out in the newspaper article [8], which contains a number of proposals for the president of Russia Dmitry Medvedev concerning reforms of the election system. The authors feel that it is important to have a prototype of the 'Guarantor' system ready in short order so that its advantages can be directly compared to the technologies that will be developed by our Russian colleagues.

Presented below is an outline of the interactions between the subjects of the electoral process with the 'Guarantor' system acting as the trusted third party.

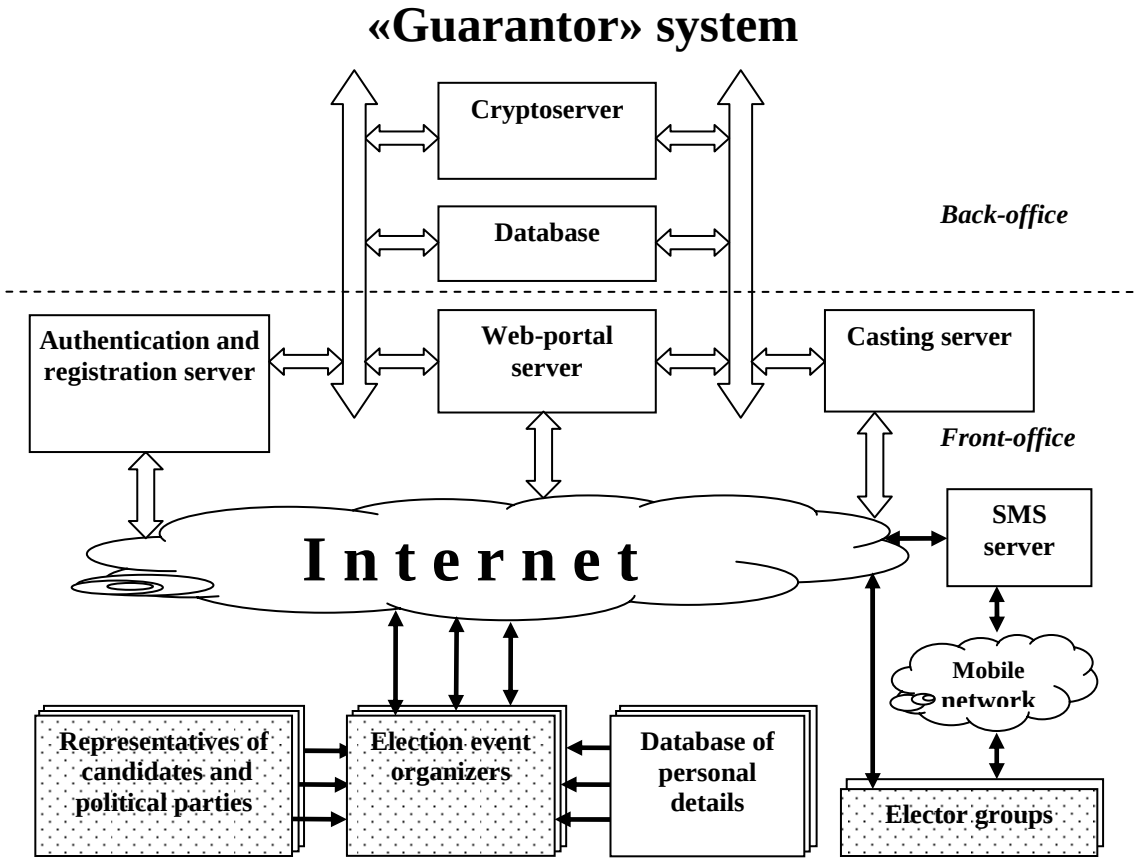

Figure 2 : Internet voting using the 'Guarantor' system

An important feature of the proposed voting scheme is the mechanism used to authenticate the electors. Our proposal consists of using personal data in conjuction with SIDs (secure identifier) distributed to the electors in confidence before the elections. A detailed description of SID generation can be found in [7]. To briefly describe the properties of SID, we will note that each SID is generated as $SID_i = EID_i \oplus F_{crypt}(EID_i, K, R_i)$, where EID_i is a unique number identifying the elector, $\oplus$ is the concatenation operator, and F_{crypt} is a secure cryptographic function taking as arguments the identifier EID_i, the secret key K, and a randomly generated number R_i, which is stored in a remote database accessible only to the cryptoserver. The function F_{crypt} is designed so that generation of valid SIDs requires not only the knowledge of the secret key K, but also the random numbers used in the procedure (and thus access to the database storing these numbers). These properties make generation of counterfeit SIDs unfeasible. At the same time, secrecy of SIDs is only essential before voting has ended. After the voting server has been closed and the results of the election event have been published and made final, it is possible to allow public access to the cryptoserver, the key K and the database of random numbers R_i so that every remote observer can verify that only valid SIDs have been used in the voting.

Presented below is a formal description of all stages of the elections.

i. Pre-election stage.

Input: complete information about the election event, personal data of the electors.
Output: credentials for managing the election event.

At the pre-election stage, the organizer of the election event uses the administrative interface of the 'Guarantor' system to create a new election event and to submit the complete information about the event and the personal data of the electors. He then receives the login and password valid for managing the election event.

ii. Preliminary stage.

Input: confirmation of the data input during the pre-election stage.
Output: a set of SIDs used for voter authentication.

The preliminary stage of the election event is started immediately after the information gathered in the pre-election stage has been processed by the 'Guarantor' system. A web portal of the election event is created, containing the information about the election event. The organizer reviews the web portal and authorizes publishing it online. From this moment the information about the election event becomes accessible to the public and is recorded by the voting server.
At the same time, a request is placed for the cryptoserver to generate an SID for each of the electors. The generated SIDs are randomly assigned to electors and delivered to them in confidence.

iii. Voting stage.

Authentication/registration server input: SID.
Authentication/registration server output: randomized voting token and password.

Voting server input: randomized voting token and password, vote.
Voting server output: confirmation that the vote has been received.

Voting begins and ends at a time set by the organizer of the election event. In order to place his or her vote, the elector must perform the following steps:

1. Input the SID received at the preliminary stage using the web interface of the authentication/registration server. The SID is sent to the cryptoserver for verification. If the SID hasn't yet been used for voting, a set of 8 randomized voting tokens (RVTs), which are random numbers not linked to the EIN or the personal data of the voter, is generated (or reused) together with the passwords corresponding to them.
2. Record one of the eight RVT/password pairs.
3. Access the voting server and input a valid RVT/password pair. The remaining 7 pairs that were shown to this voter then become invalid. The invalidated RVTs can be used by a different voter later.
4. Place the vote and confirm it.

4. Post-election stage.

Input: RVTs or RVT/password pairs received by the electors.
Output: votes corresponding to the RVTs used in the elections, SIDs submitted to the authentication/registration server, election event results.

Post-election the authentication/registration and voting servers become inactive. Preliminary results of the elections are tallied and published at the web portal of the election event. Lists of RVTs used in the elections appear together with the corresponding votes.

At the post-election stage every elector can:
1. Check the published lists of RVTs to verify that their votes have been correctly tallied.
2. Input the RVT/password pair used for placing the vote. In that case the RVT is highlighted in the list, indicating that it has been verified by the elector. Assuming that enough electors perform this procedure and no instances where an elector saw his or her RVT highlighted prior to entering the RVT/password pair have occurred, this proves that each unique RVT corresponds to a unique vote.

The organizers of the election event resolve the possible disputes raised by the voters and the observers. After all of the disputes have been resolved, the results of the election become final and are published as such at the web portal.

Once the results have been finalized, the entire database of SIDs used in the elections is published, allowing anyone to verify that every SIDs received by the authentication/registration server is valid and that the total number of votes doesn't exceed (or significantly differ) from the number of recorded SIDs, proving that no 'ghost voters' have participated in the elections.

Presented below is a more formal description of the verification mechanisms available to the public.

Let us assume that N electors are participating in the event and that SID set $\boldsymbol{S} = \{S_1, S_2, \ldots, S_N\}$ has been generated at the pre-election stage. Some of the electors may choose not to vote, leaving a set $\boldsymbol{S'} \subseteq \boldsymbol{S}$ of SIDs that have been used by electors to authenticate themselves at the authentication/registration server, and the size of set $\boldsymbol{S'}$, which will be denoted as N', satisfies $N' \leq N$. Again, it is possible that not every elector who has registered will choose to vote. Therefore, the set of votes $\boldsymbol{V} = \{V_1, V_2, \ldots, V_{N''}\}$ recorded by the voting server must satisfy $M \leq N'' \leq N$. After the raw data collected by the authentication/registration server and the voting server is published, any remote observer can verify this relation and ensure that every SID in the set $\boldsymbol{S'}$ as recorded by the authentication/registration server is valid. This relation can be presented differently. Let us number the available choices in the voting from 1 to M, and let $C_1, \ldots, C_M$ be respectively the total numbers of votes given in support of each of the choices. Then $C_1 + \ldots + C_M = M \leq N'' \leq N$.

It must be noted that in the proposed scheme every honest voter can use the RVT used for voting to ensure that his or her vote has been tallied correctly. Unfortunately, unless every vote is accompanied by an elector's electronic signature, it is impossible to prevent dishonest voters from claiming that the system doesn't work as intended. However, the authors believe that such dishonest voters will be a small minority, and that their efforts will be wasted. After all, unlike the case of traditional paper ballot voting, every honest voter can use his RVT to see that the vote has been properly recorded, and every honest elector who didn't vote can verify that his or her SID has not been captured by the authentication/registration server.

6. Conclusion

The main concern of the authors is that, despite widespread use of information technologies in the modern world, traditional paper ballot voting, despite its numerous flaws, is still widely utilized. Numerous well-known and well-documented techniques of committing fraud in paper ballot elections are one of the reasons why citizens of developing countries and emerging democracies lose

their faith in elections, leading to either elector apathy or, on the contrary, anger at the ruling government manifested in various forms of civil unrest. In many countries it has become customary for the losing side to declare the elections fraudulent after the results have been announced, rallying their supporters for actions of mass protest. It is characteristic of paper ballot elections that nobody, including the ruling government, is aware of the exact extent of the machinations and, consequently, the true results of the voting. This situation leads to political instability, delegitimization of the government in the eyes of the citizens and, ultimately, doubts in the very principles of democratic government.

The proposed alternative is the use of modern transparent electronic voting technologies specifically designed to address the issues that have become identified with traditional technologies. The authors realize that they don't have the manpower or the resources required to develop a working state-scale election system based on the principles outlined in the paper. Nonetheless, it is our hope that the presented ideas and the prototypes that have been developed will lead to a joint project by various IT experts to create a pilot e-Voting framework that would fully comply with the OSCE requirements and which could be approbated under international supervision. It is our firm belief that realizing the proposed ideas could benefit not only the troubled countries of Africa, Asia and Middle East, but also the ex-soviet countries and even the countries of the European Union where use of electronic voting has been limited or banned legally (Ireland, the Netherlands, Germany) or where electors have shown mistrust or lack of interest in electronic voting (Estonia).

References

[1] S. Ablameyko, V. Lipen, Electronic voting systems: experience of creation and new projects, in: 5th Eastern European e-Gov Days 2007: Best Practice and Innovation, Session 5A "e-Participation", Österreichische Computer Gesellschaft, Wien 2007.

[2] S. Ablameyko, N. Kalosha, V. Lipen, D. Lipen, Organizing and monitoring election events with «The Guarantor», in: EDEM, 2010. – Conference on Electronic Democracy 2010: proc. of EDEM 2010, 2010, P. 299–310..

[3] S. Caarls, From e-voting to paper ballot voting, in: Modern Democracy—the Electronic Voting and Participation Magazine, February 2010, available from http://www.e-voting.cc/static/evoting/files/modem_2_2010_web.pdf

[4] Making voting systems transparent through open-source development. http://www.trustthevote.org

[5] EAPO patent № 006712 "Electronic voting system". http://www.eapo.org/rus/reestr/patent.php3?id=6712

[6] S.Ablameyko, V.Lipen, D.Lipen, New technologies for transparent and trusted e-voting and results sizing, in: Tagung fur Elektronische Demokratie: Tagungsband der EDem2008, Krems, Osterreichische Computer Gesellschaft, 2008, S. 271–279.

[7] S. Ablameyko, N. Kalosha, V. Lipen, D. Lipen, New technologies for remote observation and verification of electronic votes: foundations of a better E-voting system, in: EDEM 2009 – Conference on Elektronic Democracy: Proceedings of EDEM 2009, Osterreichische Computer Gesellschaft, Wien 2009.

[8] Electronic democracy from the party of the government (in Russian). http://www.ng.ru/politics/2010-11-16/3_electrodemocracy.html

[9] M. Kripp, Trust, certification, verification, in: Modern Democracy—the Electronic Voting and Participation Magazine, February 2010, available from http://www.e-voting.cc/static/evoting/files/modem_2_2010_web.pdf

[10] T. Hall, R. Alvarez. Point, Click and Vote: The Future of Internet Voting, 2004, Brookings Institution Press.

[11] http://www.slaw.ca/2010/10/25/electronic-voting-and-the-law-its-not-like-e-banking/

[12] S.Ablameyko, V.Lipen, Electronic voting systems: experience of creation and new projects, 5th Eastern European e-Gov Days 2007: Best Practice and Innovation, 11-13 April 2007, Prague, 2007.

[13] R. Krimmer, A. Ehringfeld, M. Traxl, The Use of E-Voting in the Austrian Federation of Students Elections, The 4th International Conference on electronic voting, 2010, Bregenz, Austria.