

Key Factors Influencing Electronic Voting Design

by Silhavy R.¹

This contribution focuses on the opportunity of the setting accurate level of security and Privacy, comparing to the level of security and privacy in common paper-based voting processes. The electronic voting is probably one of the most important improvements of the direct democracy. Probably the most important topics in electronic voting research are connected with security and privacy. The fundamental technical principles of the e-solutions are nearly the same. Therefore, there is no difference between electronic voting solution and commonly used solutions like internet banking. This level of the security and privacy should be sufficient in comparing to the traditional voting process. The aim of this contribution is to analyse electronic voting process and its security and offer electronic voting design.

Introduction

Many countries have been researching the benefits of e-voting solutions. Every country uses individual ideas to solve e-voting problems. The range nowadays is from electronic ballot reading devices to ballot boxes installed in polling stations. The second electronic voting system is electronic voting. The electronic voting solution allows voting through the internet network. Very few countries have been working on the internet based voting system. Electronic voting has been attracting considerable attention during the last few years. There is nowadays a great deal of interest in e-solutions. There are two more practical reasons for the interest in e-voting solutions. The first an interest in an e-voting, system which can help to solve problems with domestic election systems e.g. lacking flexibility with respect to time frames (not in Europe, but e.g. in the USA) Also the physical accessibility of polling stations, which may possibly prevent citizens from casting their votes. The second reason is connected to the number of elections during the year. People do not usually want to visit polling stations very often. In a time when referendum is becoming increasingly popular, it is the right time to research other possibilities of practicing democracy.

¹ Tomas Bata University in Zlin, Faculty of Applied Informatics. Email: rsilhavy@fai.utb.cz.

Basis Voting Process Description

Electronic voting is similar to classic "paper-form" voting. In classical "paper-form" voting voters entering the polling station have to be identified. If identification is passed, they are able to vote. The whole scenario of classical voting can be seen in Figure 1.

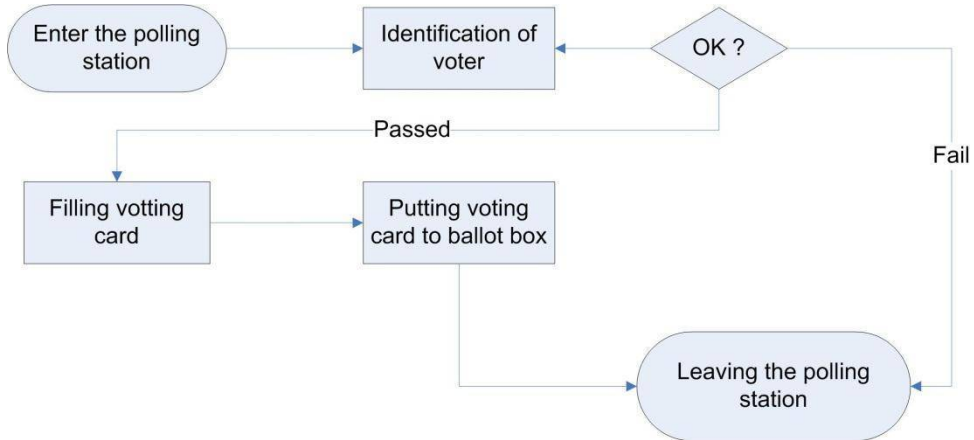


Figure 1: The classical "paper-form" voting process

There are two recognised types of electronic voting systems. The first one is based on visiting a polling station. In this case voters are still identified by using identification cards. Voters do not fill voting cards in the paper form but push buttons on various electronic devices. Then voters use the electronic device to vote.

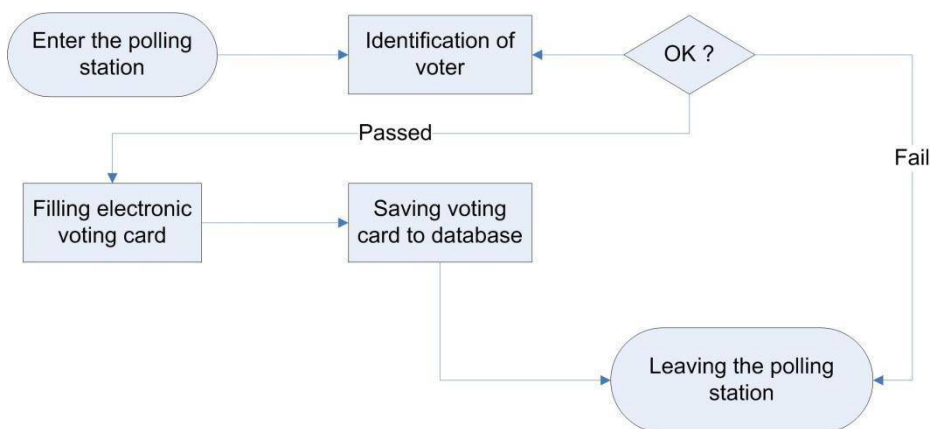


Figure 2: The in-site electronic voting system

Usually voters have the chance to vote by using computers at remote locations or at polling stations. They use computer and internet networks for voting. Voters can vote out with the normal interval for voting (usually office hours). They can also vote from abroad. These constitute the most important advantages of the remote-based voting system. This idea is usually called electronic voting.

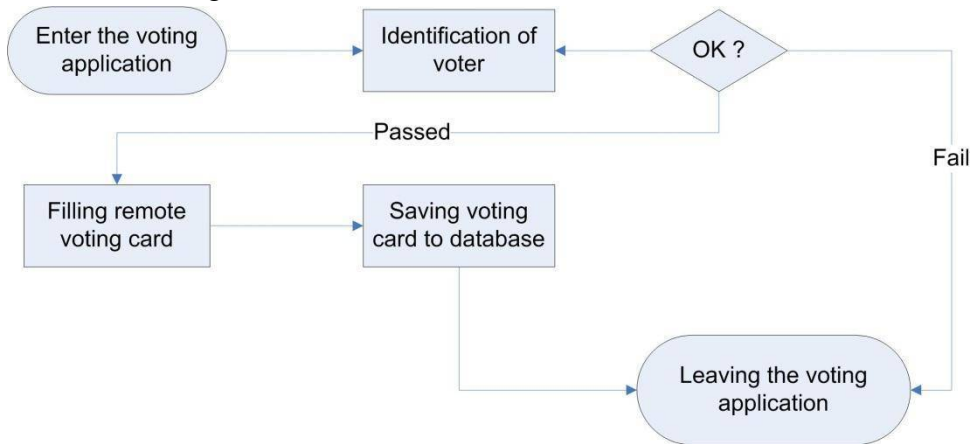


Figure 3: The remote voting process

Generic Voting System Architecture

The main point of this contribution is the utilisation of an internet application solution for remote electronic voting, because it is a solution, which allows the connection of electronic voting and internet.

By using an electronic voting system you are not merely limited to electronic voting. Electronic voting is useful in electronic voting too. The internet platform can be useful and helpful for every electronic voting system. If the e-voting system uses a internet-based solution, it can be used by individual voters through the internet network or it can be used in polling stations. In the polling station touch-screen terminals can be utilised.

The electronic voting solution can be divided into four parts:

1. The voting application for individual voters
2. The voting application for polling stations
3. The database of votes
4. The results of elections

The voting application for individual voters would be used in internet explorer (web browser). The voter has to be identified and will be able to access the voting application. The voter identification has to be done by using the list of voters. The list of voters has to be in electronic form. When access is granted the process of vote casting can start. Each voter is permitted to access a list of candidates in his election district only.

The voter uses web-based applications for the voting process. The first step is choosing and editing a ballot. Then the ballot is secured by cryptophytic method (e. g. public key). The secured ballot is saved into a database. Each ballot has an individual transaction ID. Each voter receives a ticket with the transaction ID and results of their voting. This is necessary for voting control and maintaining anonymity.

At the polling station the application is used without electronic identification of voters. Voters are identified by the election committee and process of voting continues as for electronic voting (Figure No. 2). The election committee has to control the voter if the voter does not vote by the internet channel.

The third part - database of votes - can be registered and monitored by various database technologies. Every vote is saved only once. During the process of identification, the system has to check voter status. It means that the system will recognise if voter already log in or not. If the voter had previously logged-in the voter is not allowed to log-in again.

The result of elections can be prepared automatically. The system has to support the algorithm(s), which are used in the country. Results are controlled by an election committee or directly by voters.

Electronic Voting Trials in Europe

There are two examples of using web-based voting in Europe. The first one describes a project prepared in Switzerland. The situation in Geneva - Switzerland is a good example for using electronic voting systems. Voters are called 4 to 6 times to the elections.

Lots of voters in Geneva used to vote by postal message and 2/3 of citizens have internet access. The electronic ballot box is locked by two independent digital keys. In Geneva a "paper-form" voting card is used. Each card has a transaction number. Transaction numbers are stored in the database. Voters have to insert a number into the system as an authorisation code. Then they

can vote. Each voting card has a PIN code too, which is used for confirmation of vote.

The second example is taken from Estonia. Identification cards are used in electronic voting system in Estonia. This smart card has a chip. The chip contains data about the holder and two certificates, two private keys. Smart cards can be used for various applications, not only for eGovernment services. Smart cards were important for starting the project of electronic voting in Estonia. These cards are used for identification of voters and for authorization of votes. Each voter can change their vote several times.

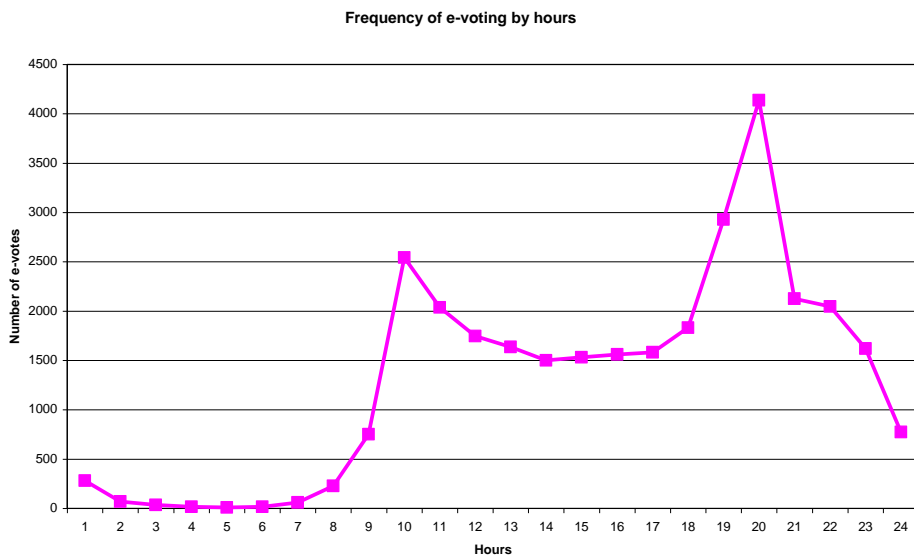


Figure 4: Frequency of e-voting in Estonia, 2007

The National Electoral Committee of Estonia (NEC) organised parliamentary elections in 2007. This was the first occasion that an e-voting system was used on a national scale. Figure Frequency of e-voting by hours shows the number of e-votes cast per hour during a typical day of the election which due to e-voting took place over several days. The first peak appeared at 9. 30 a. m. and the second peak at 8 p. m. Between these two peaks numbers of votes cast was relatively levelled, although there was a significant steady rise in the number of voters between 5.30p.m and 8p.m. As can be seen the casting of votes during the evening remains high and is indicative of a strong possible future for e-voting. From 12.00p.m. to 8.00a.m only a very small

percentage of votes were cast. The sharp increase at 8:00a.m may have been caused by voter's daily regime.

Key Factor for Electronic voting System Design

There are several conditions for electronic voting systems. The law in the country has to support the electronic voting systems. The electronic voting solution has to follow the technical and process conditions listed below:

1. Participation in the voting process is granted only for registered voters.
2. Each voter has to vote only once.
3. Each voter has to vote personally.
4. Security and anonymity of voters and voting.
5. Security for the electronic ballot box.

The first condition for electronic voting means, the voter should be registered by voting committee in the list of voters. This list is used as the basis for distribution of log-in information. If the voter is registered, they will be able to display the relevant list of parties and candidates.

Voters could also vote more than once, but only the last attempt will be included in the final results of the election. This possibility varies in different e-voting systems. If it is not possible to vote more than once, there should be more complicated protection for the election against manipulation and assisted voting.

The third condition – Right to vote personally – is closely connected to the previous. On the other hand this is the basic responsibility of each voter to protect his private zone for voting – in the case of the internet-based remote voting. In the “in-site” voting the system of privacy protection will be similar to the current situation.

Security and anonymity of voters and voting is probably the most important issue in the electronic voting process. The appropriate voting system should be realized in two separate parts. The first part should be responsible for authorization of the voter and the second for storing votes. Therefore the system will support anonymity. The voter should check his vote by the list of collected votes. The unique identification of vote will be known by the voter only. The voting process will be protected by using a cryptographic principle.

One of the many applicable solutions is Private Key Infrastructure. This approach deals with two pairs of keys in the first part of voting system – for authorization. In the second part of voting system – storing votes – it should deal with a public key for protection of the vote in the transport canal.

The electronic ballot box should form as a database. Votes in the database will be ciphered by the public key of the election committee. The private key, which is necessary for decrypting votes, will be held by members of the committee. Each member will hold only part of the key.

By investigation of these conditions and by the determination of the initial technological principles, authorities will be able to establish law to support the electronic voting system. The voting public's consensus to the electronic voting is quite important for the parliament process too.

Voting Workflow Design and System Architecture Overview

The internet technology is useful for electronic voting systems. This technology is based on a client-server. The client-server technology has advantages in the field of support and installation. There is only one central server, which is the main part of the solution. Application development can use several technologies. Web services can be used for communication between various areas of the solution. Web services are very useful especially in the decentralisation of the client-server system. A demonstration of the solution can be found on figure No. 5

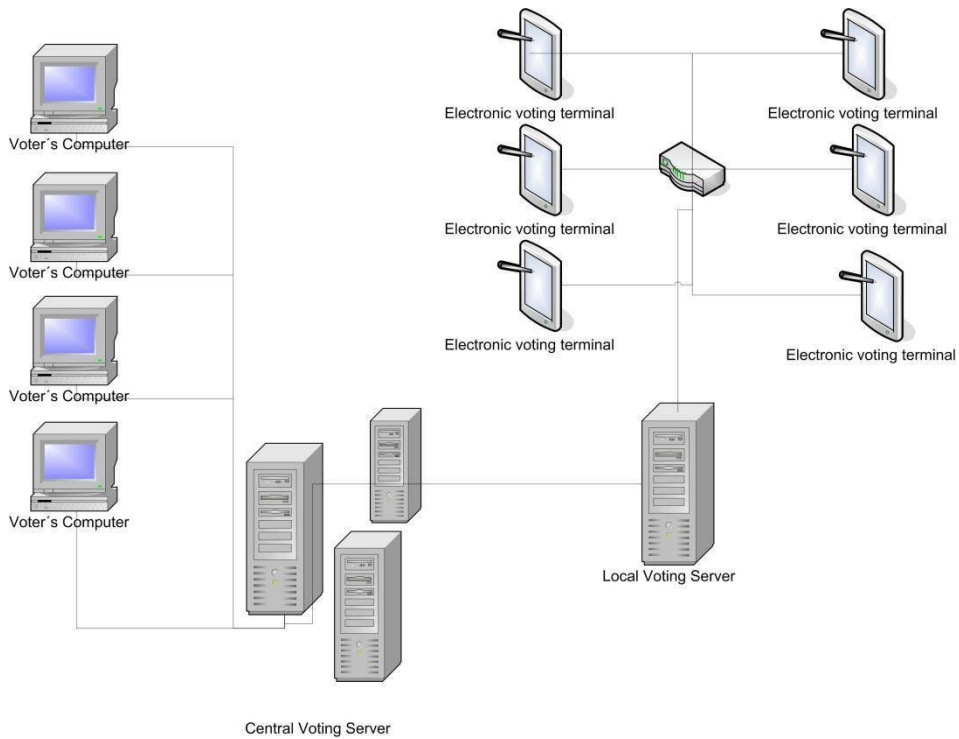


Figure 5: The basic idea of architecture web-based voting system

Proposed system design is based on four basic blocks:

- Voting Client Subsystem (VCS)
- Voting Application Subsystem (VAS) and Ballot Database Subsystem (BDS).
- Voting Backend Subsystem (VBS) and Tallying Database Subsystem (TDS).
- Voting Results Subsystem (VRS)

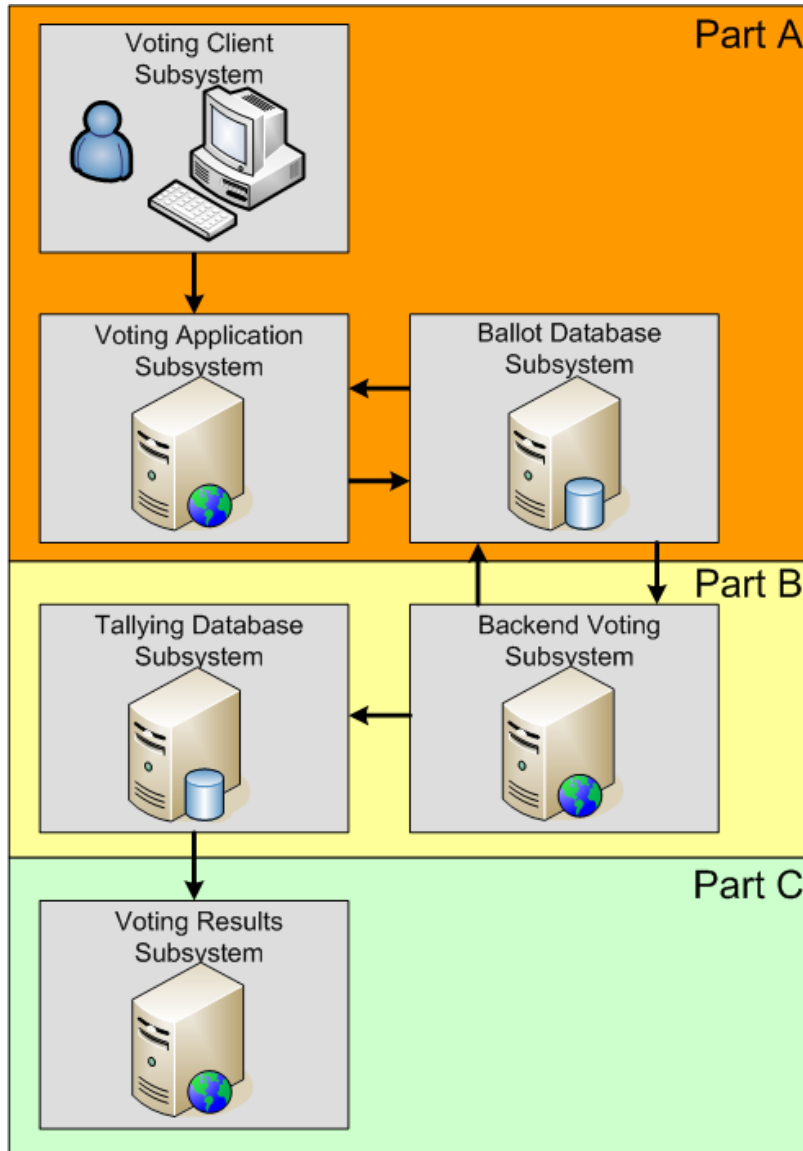


Figure 6: The Basics System Design Blocks

In the Figure 6 can be seen system design architecture. It has three separate parts are recognized. Part A is used for casting votes and contains Voting Client Subsystem, Voting Application Subsystem and Voting Database Subsystem. Voting clients represent voting terminal in elections rooms, kiosk voting or voters own computers.

Voting Application Subsystem is represented by web-based application, which contains user interface for voters, voter validation services and communication interface for Ballot Database Subsystem.

There are two most significant tasks for BDS. Votes are cast there and default ballots are generated for individual voter. Votes are cast in encrypted form, which depends on cryptographic methodology adopted for the election. For the protection against manipulation with votes in BDS HASH algorithm is implemented. HASH value is calculated irregularly based on votes, which are cast. Default ballots are generated for individual voter with respect to the election district he belongs to.

Part B represents Backend Voting Subsystem and Tallying Database Subsystem. The part B is securely connect to BDS from part A. The BVS is used by electoral committee. The BDS is responsible for auditing elections by comparing HASH based on votes and stored HASH value. The BVS deals with decryption of votes, validating of them and storing in TDS. The TDS is used for storing votes in open form. Part B is realized as web-based application and relational database server. Final part – part C – is responsible for counting final Results of the election. Part C is realized as web-based application.

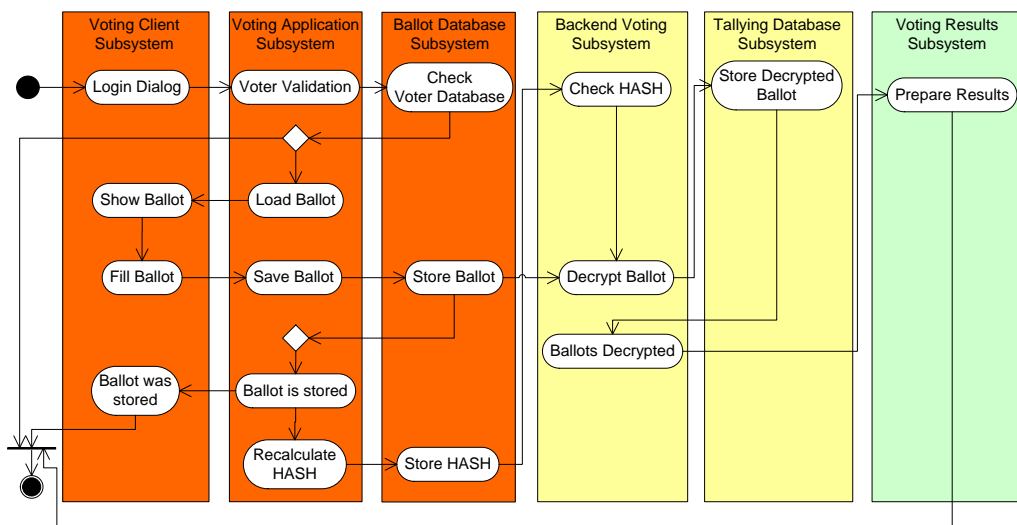


Figure 7: Vote pass-through in system design

In the figure 7 is shown workflow description of individual vote through the proposed system design.

Conclusion

The main task of this contribution was to key factors, which influenced e-Voting system design.

Many countries have researched the benefits of e-voting solutions. Every country uses individual ways to solve e-voting problems. Only a few are seriously studying electronic voting. Electronic voting solutions represent the future of electronic voting in Europe.

Increasing internet access supports the e-Government and e-Democracy. People are used to communicating through the Internet. In the future people will be used to electronic elections too.

References

1. Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July, 7th-9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance, Austria, Proceedings. GI 2004, ISBN 3-88579-376-8
2. Leenes, R., Svensson, K.: Adapting E-voting in Europe: Context matters. Proceedings of EGPA, 2002.
3. Commission on Electronic Voting: Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Dublin, 2006, available at http://www.cev.ie/htm/report/download_second.htm accessed on 2007-06-06.
4. Chevallier, M.: Electronic voting: Status; perspectives and Issues, ITU E-Government Workshop, Geneva, 6 June 2003, available at: http://www.geneve.ch/chancellerie/EGovernment/doc/UIT_6_6_03_web.ppt accessed on 2007-06-06.
5. VVK [online]. 2007 [cit. 2007-11-02]. Accessible on WWW: <<http://www.vvk.ee/english/results.pdf>>.