Internet Voting: Experiences From Five Elections in Estonia

Conference Paper · April 2012

CITATIONS
4

READS
1,343

1 author:

Priit Vinkel
Tallinn University of Technology
22 PUBLICATIONS **211** CITATIONS

SEE PROFILE

Internet Voting: Experiences From Five Elections in Estonia

Priit Vinkel
Estonia

Abstract: Estonia has been one of the pioneers of Internet Voting by introducing Internet Voting in binding elections in 2005. Since then this novelty method has been used in five elections. Although Internet Voting is just one of many voting methods, the number of Internet voters has grown exponentially throughout the years. The reasons of relative success in the process include for example the size of the country and positive experiences with previous e-services. The role of a secure online authentication — the e-ID-card is crucial in implementing an idea of remote online voting in an uncontrolled environment. Changing the i-vote with another i-vote and the supremacy of the paper ballot serve as main strongholds against vote buying and other infringements of the principle of free elections.
In addition, the main issues that have emerged throughout the years are addressed.

Keywords: Internet Voting, Electronic Voting, E-voting, I-voting, elections, e-government, e-services, remote authentication

1. Introduction

In 2005, Estonia was the first country in the world to have remote voting over the Internet in pan-national binding elections. Since then the number of Internet voters has grown more than 14 times. This short paper looks at the essential principles of the Estonian Internet Voting system and addresses some of the emerged problems.

Most likely Internet Voting in Estonia is there to stay as already a quarter of voters vote over the Internet. However, the constant struggle of improving the system and the surrounding processes is crucial in preserving the trust of the voter in online voting.

2. Estonian Internet Voting system

2.1 Pillars of Success

Statistical overview. Using Internet Voting for pan-national elections is not a very widespread practice. Only Switzerland, Estonia and Norway allow legally binding remote Internet Voting at least on the wider local level. Therefore, the understanding of the factors that help for implementing this system is quite important. The current concept of Internet Voting that has been used for voting in two general (Riigikogu) elections (2007 and 2011), in two local elections (2005 and 2009) and one European Parliament election (2009). The number of Internet voters has grown rapidly through the years, reaching its peak of 140 000 in 2011 Riigikogu elections (see Table 1).

Table 1. Internet Voting statistics in Estonia from 2005 to 2011

	2005 LE	2007 PE	2009 EP	2009 LE	2011 PE
Number of Internet votes	9 681	31 064	59 579	106 786	145 230
Number of repeated Internet votes	364	789	910	2 373	4 384
Number of Internet voters	9 317	30 275	58 669	104 413	140 846
Internet votes cancelled by paper ballot	30	32	55	100	82
Internet votes counted	9 287	30 243	58 614	104 313	140 764
Internet votes among participating voters	1.9%	5.5%	14.7%	15.8%	24.3%
Internet votes among advance votes	7.2%	17.6%	45.4%	44%	56.4%

Source: Estonian National Electoral Committee

The number of changed votes either by giving a repeat vote over the Internet or going to the polling station could be seen as considerably moderate, reaching up to 3% of the overall Internet votes and only up to 100 cancellations in the stations. In addition, there are two important factors that could be observed. Firstly, Internet Voting is just one of over ten voting methods in Estonia. However, it has secured second highest popularity with almost a quarter of votes being given electronically. The most popular method has always been the Election Day (Sunday) voting with half of the votes. Nevertheless, the emergence of Internet Voting has spiked the turnout in advance voting equalizing the voting periods before and during the Election Day. Secondly, Internet Voting has also achieved vast popularity among advance voting as such, where more than half of the advance votes were given by electronic means in 2011.

A widely discussed topic has always been the influence of Internet Voting on overall turnout, because this goal has been one of the main reasons of adopting this voting method. Estonia has had a steady experience in e-enabled elections and one of the scientific reviews has stated a real positive influence of Internet Voting on turnout estimated up to 2.6%. Nevertheless, the actual role of remote electronic voting on voter activity is under discussion.

When thinking of the reasons of the voter for choosing such a new voting method, one factor has emerged all these years — accepting Internet Voting relies heavily on the trust of the voters. Without a doubt, trust is a key factor for almost all crucial e-solutions but the direct connection with remote Internet Voting has been reiterated in all according scientific surveys. The three most important factors of keeping and building this trust could be summarized as put on Figure 1.

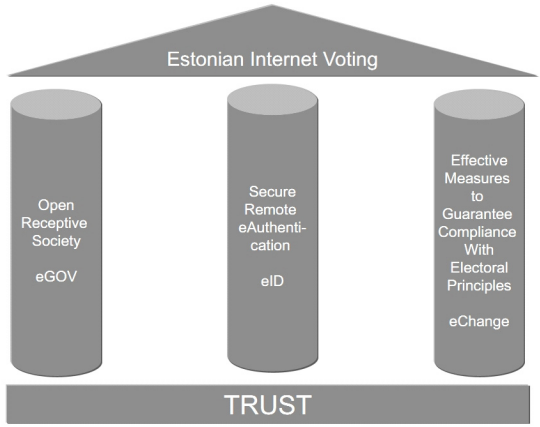

Fig. 1. Three pillars of Estonian Internet Voting

Open receptive society. The Republic of Estonia currently has about 1.35 million inhabitants, dispersed over 45.227 km^2 . According to the Global Information Technology Report 2012, in the category of government success in ICT promotion Estonia lies on 9th place forerunning such IT giants as US, Finland or Japan. In the field e-participation Estonia shares position 9 with Singapore. In the category of presence of ICT in businesses, the top three countries are Korea, Sweden and Estonia. Since 1 June 2010, even the official publication of legal acts, *State Gazette*, is entirely electronic, all legal acts are published only on the Internet. An important factor explaining the possibility to launch totally new solutions like the official virtual identity or Internet Voting is the smallness of the country. Lennart Meri, the late president of the Republic of Estonia compared in his speech at St. Olaf College in Minnesota on 6 April 2000 Estonia with a small boat: "A super tanker needs sixteen nautical miles to change her course. Estonia, on the contrary, is like an Eskimo kayak, able to change her course on the spot."

Therefore, as the number of actual voters is around 1 million and there is generally a positive notion towards innovation, such ideas as Internet Voting could be addressed more easily.

Secure remote e-authentication. The cornerstone of Estonian e-services, public as well private, is e-ID. Since 2002, ID card is the new generation's mandatory primary identification document. The ID cards are issued by the Government and contain certificates for remote authentication and digital signature. All Estonian citizens and resident aliens older than fifteen must have an ID card.

Each ID card contains two discreet PKI-based digital certificates — one for authentication and one for digital signing. The certificates contain only the holder's name and personal code and have two associated private keys on the card, each protected by a unique user PIN. The certificates are not restricted of any use: they are by nature universal and meant to be used in any form of communications, whether between private persons, organizations or within the government. The e-ID card can be also used for encryption of documents so that only the person intended to view the document can decrypt it. This is an efficient means for secure transfer of documents using public networks. In addition to that, each ID card contains all data printed on it also in electronic form, in a special publicly readable data file.

The number of issued ID-cards has in June 2010 exceeded 1.1 million. Over two-thirds of cardholders have used the e-ID card for remote personal identification and over one-third — for digital signature. It is to be noted that Internet Voting has strongly promoted the electronic use of ID card. Another important promoting factor has been the agreement between banks to allow unlimited Internet banking only with ID-card or PIN-calculator. The old password-cards can be used only for very small transactions.

In order to use the ID card, the smart-card reader and a computer with relevant software (free to download) plus Internet connection and Windows, Mac or Linux operating system are needed. A couple of years ago a new solution was brought to the market: m-ID, where a mobile telephone acts as an ID-card and a card reader at the same time. In addition to functionality of an ordinary SIM, a Mobile-ID SIM also holds a person's mobile identity that enables providers of internet services to identify the person and to give digital signatures. Personal identification and digital signature functionality are secured by up-to-date security technology and corresponding Personal Iden-

tification Numbers. What makes the solution more convenient is the fact that an ID-card reader in the computer is not needed any longer — instead, it enables making electronic transactions, just like an ID-card: it makes it possible to log into e-services, internet banks etc. and sign contracts digitally.

Parliamentary debate over e-ID card raised several privacy and security questions, but the parties supporting compulsory e-ID commanded over majority of votes. The most controversial questions were the possible risk of identity theft and overall IT security. To prevent the use of the ID-card issued to another person, respective provisions were added to the Penal Code. According to the law, fraudulent use of the ID card is punishable by a pecuniary punishment or up to three years of imprisonment.

In practice e-ID is used for user authentication in several Databases, the State Portal serving as an e-service-centre; e-ticket in the public transportation; loyal customer identification tool in several private companies; and even used be there to insert comments to the online daily newspaper *Eesti Päevaleht*, which was to prohibit anonymous comments to prevent libel cases.

Effective measures to guarantee compliance with electoral principles. The secrecy of voting has traditionally been viewed in Estonia as the right and obligation to cast the vote alone in a voting booth. In the case of the Internet Voting the state is not in the position to secure the privacy aspect of the procedure. Legislators proceeded from the interpretation of the Constitution according to which secrecy of voting, drawing on its two sub-principles — the private proceeding of voting and the anonymity of the vote — is required to ensure free voting and is not an objective per se. Consequently, instruments aimed at securing secrecy can be adapted, provided that voters are given the opportunity to vote freely for their preferred choice without fearing condemnation or expecting moral approval or material reward.

The voter's right to anonymity during the counting of the votes is guaranteed to the extent to which it can be secured in the case of absentee ballots by mail; the so-called "system of two envelopes" (visually seen on Figure 2), used for absentee ballots by mail, is both reliable and easy to understand for the e-voters.

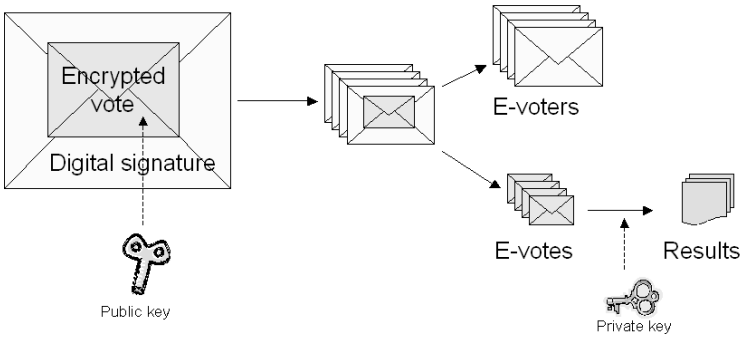

Fig. 2. Double envelope system used in Internet Voting

A double-envelope scheme known from the postal voting in some countries guarantees the secrecy of the vote. The voters' choice is encrypted by the voting application (i.e. voter seals the choice into an inner blank envelope) and then signs it digitally (i.e. he puts the inner envelope into the bigger one and writes his name/address on it). The signed and encrypted votes (outer envelopes) are collected to the central site to check and ensure that only one vote per voter will be counted. Before counting, digital signatures with personal data (outer envelopes) are removed and anonymous encrypted votes (inner envelopes) are put to the ballot box for counting.

The scheme uses public key cryptography that consists of a key pair — a private and a public key. Once the vote is encrypted with a public key then it can only be decrypted with the corresponding private key. The National Electoral Committee, holding the private key, collegially opens the encrypted I-votes on Election Day.

In order to guarantee the freedom of voting, e-voters have been granted the right to re-vote electronically an unlimited number of times and replace the vote cast on the Internet by a paper ballot. However, this can only be done within the advance polling days. In case of several I-votes the last one is counted; in case of contest between an I-vote and a paper ballot, the paper ballot is counted. In the highly unlikely case where several paper-ballots are cast, all votes are

declared invalid. Thus, the "one vote — one voter" principle is ostensibly guaranteed.

In Internet-based voting, the possibility to change the I-vote is not just permissible; it is considered a constitutional obligation. According to the opinion of the Supreme Court of Estonia, the principle of the freedom of vote gives rise to the obligation of the state to protect voters from persons attempting to influence their choice. With regard to that principle, the state has to create necessary prerequisites in order to carry out free polling and to protect voters from undesired pressure while making a voting decision.

In the judgment, the Supreme Court maintains the following:

> The voter's possibility to change the vote given by electronic means, during the advance polls, constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting upon voting by electronic means. A voter who has been illegally influenced or observed in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influences. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, the possibility to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, besides the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The penal law sanctions do have their preventive meaning but subsequent punishment — differently from the possibility of changing one's electronic vote — does not help to eliminate a violation of the freedom of election and secrecy of voting.

The Supreme Court thus confirmed the constitutionality of one of the main premises of the Estonian remote Internet Voting project. Moreover, the corresponding principle has been acknowledged and adopted also by the Norwegian Internet Voting project.

2.2 System architecture

The main components of the Estonian I-voting system (seen on Figure 3) are the Voter Application; the Vote Forwarding Server; and the Back-office, which is divided in two: the Vote Storing Server and the Vote Counting Application. The Voter Application is a stand-alone application in voters' personal computers to cast and encrypt votes.

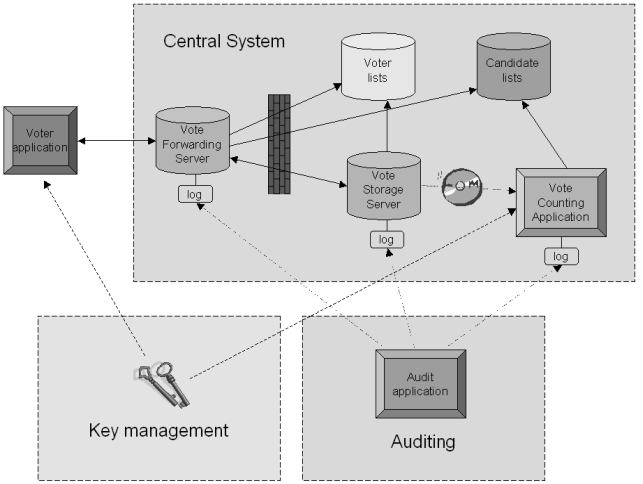

Fig. 3. The general architecture of the Internet Voting system

The processes of the Vote Forwarding Server (a network server) are authentication, the checking of franchise, sending a candidates' list to voters, receiving signed and encrypted ballots. The network server immediately transfers the received encrypted ballots to the Vote Storing Server and transposes the acknowledgements of receipt from the Votes Storing Server to the voters. The network server completes the work when the I-voting period finishes. The Vote Storing Server receives encrypted ballots from the network server and stores them until the end of voting period. The Votes Storing Server has also a responsibility of votes' managing and cancelling. The Vote

Counting Application is an offline program, which summarizes all encrypted ballots. The encrypted ballots are transferred from Vote Storing Server to Vote Counting Application by using offline data carriers. Vote Counting Server does not receive voters' digital signatures and so, does not know voters' personal data.

Additionally, the I-voting system delivers independent log files, which consist of trace of the received encrypted ballots from the Vote Forwarding Server, all annulled encrypted ballots, and all encrypted ballots sent to the Vote Counting Application and all counted encrypted ballots. The used cryptographic protocol links all records in the log files. The National Electoral Committee has the right to use the log files to resolve disputes. Hence, there is an independent audit trail to verify the I-voting process and help solve problems should they appear.

3. Emerged issues and future trends

3.1. Main issues after five elections

Security. It is impossible to prove security, but only the opposite. This popular IT proverb has kept its ground in the Estonian Internet Voting case. Moreover, e-enabled elections from 2005 to 2009 had only limited concerns regarding security issues tied explicitly to one way of voting — over the Internet. The National Electoral Committee had no complaints presented and the overall notion had been fairly positive. However, after 2011 Riigikogu elections, a discussion flared up about the mere possibility of infringement of security. Most probably the growingly prominent position of Internet Voting among other voting methods has played a significant role in this fact. A thorough discussion about the technical issues emerged in 2011 has been covered by Heiberg *et al*.

Verification of the I-vote. Norway entered the circle of countries providing e-enabled elections in September 2011 by introducing Internet Voting in ten local government units. In addition, a possibility to verify the cast I-vote by using customary SMS and paper

polling cards was offered for the voters. Lifted by this example the discussions of offering this possibility in Estonia have emerged as well. So far, the Estonian system has not foreseen a separate possibility to verify the I-vote. In case of re-voting the Voter Application shows a message of the fact that the person has voted before and it could actually be seen as first-level verification (stating the arrival of the vote). Nevertheless, the discussions of introducing the concept of vote verification to the Estonian Internet Voting system are still ongoing. A perfect solution looks for a balance between security, usability, accessibility and feasibility.

Uniformity of elections. This issue has been imminent from the very beginning of the concept. The Estonian I-Voting system put a lot of effort in fulfilling all universal principles of election. Nevertheless, the very fact that Internet Voting is fundamentally different from traditional voting is grounds enough to have doubts in equal conduct of matters. The actual conundrum is that Internet Voting can never have all the same characteristics as paper voting. The main issue within the complex of uniformity is whether changing the vote should be exclusively an e-matter. As already stated before, changing the e-vote is not about changing the ticket but rather changing in order to be free. Therefore, constitutionally I-voting must be conducted in an un-uniform matter.

Role of "soft laws". Not all provisions fit in the narrow limitations of a legal act. There are some principles concerning I-voting that need to be agreed upon by the players — the parties — themselves. The agreement includes aspects from prohibiting I-voting parties to persuading voters to change their vote for other reasons than guaranteeing the secrecy of the vote. However, there were some parties that did not agree with these soft provisions which started a discussion of integrating the agreement further into "hard law". So far the discussion is still in process.

4. Conclusions

In order to increase the competitiveness of the Estonian society, the government places more emphasis on the development of

citizen-centred and inclusive e-society based on virtual identity and e-solutions in all possible fields. Internet Voting is, on the one hand, an essential public e-service in the Estonian information society; on the other hand, it is a revolutionary tool in electoral administration, where its impact deserves permanent attention and sustainable scientific research.

The Estonian Internet Voting system benefits from three factors. First, the Estonian ID-card — a secure and widely accepted way of remote electronic identification. Second, that e-services are widely accepted in the Estonian society. And third, that we have managed to build the Internet Voting system as similar to the traditional voting principles as possible, including means to guarantee secure and anonymous voting (the virtual voting booth or possibility to change the i-vote and the virtual twin envelope system). Therefore, Internet Voting is prominently seen as just another e-service in communicating with the government (state), as a part of the modern information society.

In all the five elections where e-enabled voting has been implemented, the factor of trust has been of the utmost importance. Without a doubt, trust will stay the most important factor of choosing Internet Voting also in the future and building and stabilizing trust is the most important but also one of the most difficult tasks of the state.

About the Author

Mr. Priit Vinkel has been member of the secretariat of the Estonian National Electoral Committee since 2005, working for the legal and constitutional committees of the Estonian parliament and since 2007 in the elections department of the chancellery of parliament. He is a PhD student at Tallinn University of Technology, has graduated from Tallinn University of Technology (2008) master studies (*cum laude*) in public administration and from Tartu University (2005) in political science. His academic interests involve new voting technologies, electoral systems and effective electoral administration.