

Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of

- Seminar
- Proceedings
- Dissertations
- Thematics

current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

ISSN 1617-5468

ISBN 978-3-88579-225-3

The 2008 Conference on Electronic Voting took place in Castel Hofen near Bregenz at the wonderful Lake Constance from 6th to 9th August.

This volume contains 17 papers selected for the presentation at the conference out of more than 30 submissions. To assure a scientific quality, the selection was based on a strict and anonymous double-blind review process.



Robert Krimmer, Rüdiger Grimm (Eds.): Electronic Voting 2008

GI-Edition

Lecture Notes in Informatics

Robert Krimmer, Rüdiger Grimm (Eds.)

3rd international Conference on **Electronic Voting 2008**

**Co-organized by Council of Europe,
Gesellschaft für Informatik and E-Voting.CC**

August 6th- 9th, 2008

In Castle Hofen, Bregenz, Austria

Improving the Transparency of Remote E-Voting: The Estonian Experience

Epp Maaten¹, Thad Hall²

¹National Electoral Committee
Lossi pl 1a, 15181 Tallinn, Estonia
epp.maaten@riigikogu.ee

²Institute of Public and International Affairs, University of Utah
260 South Central Campus Drive, Room 252
Salt Lake City, UT 84112, USA
thadhall@gmail.com

Abstract: Pilot projects in the area of remote e-voting have been carried out in several countries but the number of those projects in which the Internet-cast votes are legally binding remains small. Estonia, indeed, has been the first country to introduce Internet voting in which legitimate results were obtained at the national level. In local government elections in October 2005 and March 2007 parliamentary elections, Internet balloting was used without controversy. The number of I-voters was three times higher in 2007 compared to 2005.

Elections need to enjoy broad public confidence to be a legitimate, meaningful democratic exercise. Remote e-voting has twice been offered as an additional channel to Estonian voters, and in both cases the system's operation has been considered successful, both technically and politically. Technically, all systems and procedures functioned well and there were no security problems. Politically, the election results were legitimate and there were no proceedings initiated to challenge the Internet voting option.

This paper gives an overview about tools for voters that reduce the negative effects of remote e-voting and improve confidence in the new voting system. A question will be proposed how the observation of remote Internet voting can be put in practice in order to resolve the transparency problems. After two Internet-enabled elections, international observers and researchers have made many recommendations regarding how to improve the transparency of the electoral administration. The paper discusses whether the recommendations focusing on testing, auditing and certification of the voting system are applicable in the light of Estonian experiences.

1 Introduction

Internet voting (I-voting) represents new opportunities for improving the electoral process, but it also presents new challenges. In particular, it is critical that I-voting is introduced in a manner that safeguards the transparency of the elections, which is one of the fundamental principles for democratic elections⁶. I-voting, like other changes in the mechanisms used to capture votes—from paper ballots to voting machines—is a technology that changes the direct means of participation but not the nature of democracy itself. We should, therefore, seek to determine how we can integrate this new technological solution into the old traditions of voting.

The basic question in electoral administration no longer focuses on whether new technology developments are acceptable in electoral processes but rather on what kind of technology is suitable for a specific country, taking into account its political and social culture, level of technological infrastructure, and its electoral system. In the Estonian case, the preconditions were favourable for introducing the most ambitious change in the nature of voting – voting over Internet. It can be clearly said that the Public Key Infrastructure (PKI), the digital signature, and the existing process of authentication have served as absolute prerequisites for the creation of an efficient e-country. Internet voting is just part of the overall concept of e-governance in Estonia [Ma07]. Good communications infrastructure, voters' high e-readiness, the widespread use of the national ID card, which enables securely to authenticate on-line voter, and its relatively small population of 1.3 million complete the list why I-voting has been a success in Estonia.

The argument in this paper is that Estonia's current election system—which includes I-voting as a mechanism for voting—has a high level of legitimacy and transparency on three levels: political/legal legitimacy, voter transparency, and system transparency. At each level, the legitimacy can be measured through the actions of government, the actions of voters, or the actions of the electoral administrators in charge of elections. At each level, participants have been able to engage the system in the most transparent ways possible. The next sections detail the importance of transparency in elections, providing a theoretical framework for appreciating the importance of transparency in elections.

2 Transparency in Elections

Transparency is an internationally recognized principle for elections. The Administration and Cost of Elections (ACE) Project⁷ has developed a set of standards for elections, with transparency a critical component. As they note⁸:

⁶ See HW08a and HW08b for a summary of the literature on electoral transparency.

⁷ The eight entities who are ACE Partner Organizations are: Elections Canada, EISA, Instituto Federal Electoral (Mexico), IFES, International IDEA, United Nations Development Programme (UNDP), the United Nations Department of Economic and Social Affairs (UNDESA), and the United Nations Electoral Assistance Division.

⁸ <http://aceproject.org/ace-en/topics/ei/ei20> accessed February 22, 2008.

”Transparency makes institutional systems and the actions/decisions they take widely accessible and understood... Electoral administrators and election officers should be held accountable for decisions they make when administering elections; legislators should be held accountable for the content of the laws they pass and the level of funding allocated for elections...[It] builds understanding of the process, the difficulties encountered, and why electoral administrators and election officers make certain decisions. Transparency increases the credibility of the process and the legitimacy of the results. If the electoral process is free and fair, accurate, transparent and monitored, and if laws and regulations are enforced, it is difficult for participants and voters not to accept the election results or the legitimacy of the newly elected representatives.”

ACE is not the only organization that is concerned about transparency. The Organization for Security and Co-operation in Europe’s (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) is also focused on transparency through their efforts related to election monitoring and observation. Like the ACE Project, the OSCE/ODIHR has a strong interest in ensuring that elections are run in a free and fair manner; in fact, this organization monitored the 2007 Estonian Parliamentary Elections [OSCE07].

The rationale for transparency in elections is simple; when elections are not transparent, individuals may engage in some sort of fraud or electoral manipulation that cannot be observed. In addition, even if nothing nefarious happens, a lack of transparency creates a situation where government officials cannot answer questions about the election in a way that satisfies either political parties or the citizenry. Erin Peterson notes that transparency has been closely tied to the idea of accountability and legitimacy in both the public and private sectors because it provides the public with important information about how institutions function⁹. Other scholars have found that transparency, especially in the vote counting process and the ability of observers to follow the election and watch key actions, are critical to confidence in the election process [Hy08]. In evaluating the legitimacy of an election system, transparency is a key attribute in the overall evaluation of the electoral process [Hy08].

In evaluating legitimacy, there are key features to examine based on international principles¹⁰. In order to evaluate the Estonian electoral system with Internet voting, it is important to determine whether the system has legal legitimacy among the public, the government, third-party election monitors, and the electoral administrators that implement election. It is also important that there are procedures in place that facilitate election observation and electoral transparency.

⁹ Pe07 cites the works of Be95; BO99; FS02; Mo98; PR96; and SL01 as leading scholars in the area of transparency.

¹⁰ See HW08a and HW08b for a review of this literature.

Our review of the Estonian case utilizes these international norms as a framework for understanding the way in which the Estonian government fosters transparency and legitimacy in the electoral process. We begin our evaluation by considering whether the political process that allowed for Internet voting is viewed as legitimate and was developed in a transparent political process (i.e., one in which I-voting was not adopted in a politically-motivated fashion to introduce bias into the system). Second, we are interested in examining whether the voters themselves view the Internet voting system as legitimate and fair. Third, we consider the administrative environment in which Internet voting is implemented and whether that system promotes transparency. Fourth, we consider how Internet voting is observed and audited. A transparent system should be one that promotes openness and is viewed as legitimate; by using international norms for election transparency as a framework, we can see how well Estonia's system fares.

3 The Legitimacy of the Estonian I-voting System

The legitimacy of I-voting in Estonia comes from the fact that the nation has relatively strong political support and an excellent legal framework that provides for Internet-related government services generally, including I-voting [DM02, DM04; MMV06]. The backbone to the entire system is the Digital Signature Act (DSA) of 2000. This Act provides for Estonians to be able to authenticate themselves during online transactions, including I-voting, and to use a digital signature. In 2002, Estonia began providing its citizenry with an identity card that had two individual's digital certificates embedded in it. When a user inserts the card into a standard smart card reader affixed to a computer and then connects to the websites enabling different services via the Internet, the individual can then enter their first personal identification number (PIN1) and the user is authenticated and can access an array of governmental and private services online. In order to give electronic signature the second certificate is activated by giving PIN2. According to Administrative Procedure Act, public sector is obliged to accept digitally signed documents and a digital signature has the equal legal value as a handwritten signature.

The DSA links closely with the set of laws enacted in 2002 that allow for I-voting in various electoral settings: the Local Communities Election Act, European Parliamentary Election Act, and the Riigikogu Election Act. After significant amendments in 2005, these laws detail the manner in which I-voting is to be administered. The statutes detail when voters can cast ballots over the Internet, the use of the DSA in voter authentication, the process for allowing I-voters to cancel their vote using an early-vote paper ballot, reconciling voter registries so that I-voters cannot cast a ballot on election day, and the ballot reconciliation process for I-votes on election night. The strong authentication requirement for I-voters i.e. the usage of ID card, is also for mitigating the risk of vote selling. Forwarding one's ID card will compromise a person's identity in all transactions not only in elections.

Electoral laws were sponsored and supported by the Prime Minister and the Minister of Justice and continue to be supported by the Parliament. In addition, the Estonian ministries have been supporters in I-voting and have championed its success in talks around the world. The most controversial issue of guaranteeing secrecy of remote I-voting by allowing people to vote repeatedly is also supported by the Estonian Supreme Court, which has ruled that repeated I-voting is constitutional because the technological benefits outweigh any deficiencies. Specifically, the court stated that “the infringement of the right to equality and of uniformity, which the possibility of electronic voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to outweigh the aims of increasing the participation in elections and introducing new technological solutions.” [Court05]. If these laws were no longer deemed legitimate by either the political parties or the public, the Parliament would obviously be in a position to change them but there has been no reason to do so. No election results have been challenged during the I-voting elections and no parties have officially questioned the transparency of the process in the political or legal setting.

One reason why the system is deemed to be transparent is that the laws governing I-voting ensure that the Internet is but one way that voters can cast ballots in Estonia. Voters can also vote in person during the early voting period on a paper ballot or they can vote on a paper ballot in person on Election Day. Internet voters can use the early voting period to ensure that their vote was secret. On the early voting period the election law allows an I-voter to cast multiple I-votes, with only the last vote counted and included in the reconciled election totals. In addition, if an I-voter casts a paper ballot during the early voting period, no I-vote is counted, only the paper ballot. By re-voting, the voter who was illegitimately influenced is able to cast a new vote once the influence is gone. Thus, an I-voter has multiple means of ensuring that their vote counted is a secret, un-coerced vote.

The legal framework for the Estonian I-voting system provides the system with legitimacy because the decision to move to I-voting was made in an open, deliberative process. The government carefully considered the issues associated with I-voting and ensured that there was an appropriate set of legal mechanisms in place to fulfil this expectation. The timing of I-voting, concomitant with early voting, allows an I-voter the opportunity to cast a secret, un-coerced ballot.

4 Voter Legitimacy: Options for Dealing with Negative Effects of I-Voting

As was noted previously, the improper influence of remote voters by others is a theoretical but potentially significant problem, although such threats are tolerated with vote-by-mail in numerous jurisdictions. As Alvarez and Hall have noted, the threats that exist with I-voting are similar to the threats that exist in almost all other modes of voting [AH04, AH08]. In order to reduce the potential threat of coercion or a problem with a perceived loss of privacy in remote I-voting, reversible voting during the early voting period is allowed under Estonian electoral law.

If we consider the experience of voters in the two I-voting experiences, we see that there is little evidence of coercion or concerns about privacy, based on the behaviour of voters. The number of I-voters who decided to go to the polling station in order to replace their I-vote with a paper ballot has decreased from 0.3% in 2005 to 0.1% in 2007 (see Table 1). Also, the percentage of repeated votes compared to the total number of I-votes diminished accordingly from 3.8% to 2.5%. The small percentages of repeated votes as well as the significant increase of the total number of I-voters indicate that the confidence in the existing I-voting system has grown. These two statistics suggest that few voters have felt the need to use the various reversible voting mechanisms that exist to guard against coercion. However, it is valuable that the small percentage of voters who have used the system, for whatever reason, have had a system in place to allow them to change their vote and avoid this concern. Likewise, the reporting of these data by the Estonian government provides voters with confidence that their votes were reversed in the process and their replacement vote tabulated.

	Local elections 2005	Parliamentary elections 2007
Number of I-votes	9 681	31 064
Repeated I-votes	364	789
Number of I-voters	9 317	30 275
I-votes cancelled by paper ballot	30	32
I-votes counted	9 287	30 243
% of I-votes among total votes given	1,9%	5,4%
% of I-votes among total advance votes given	7,2%	17,6%
% of I-votes cast abroad (51 countries in 2007)	n.a	2 %

Table 1: Internet voting statistics of 2005 and 2007 elections [NEC2007].

In addition, we see a large growth in the percentage of voters who used the I-voting channel from 2005 to 2007. In its first use, 1.9% of voters used I-voting; in 2007, 5.4% used the system. In a survey of voters and non-voters in both elections, respondents who cast I-votes in 2005 reported having also I-voted in 2007. I-voters were very loyal to the technology, suggesting that their experience in 2005 convinced them of the system's effectiveness [TSB07]. By comparison, other voters were not loyal to their voting method; election day voters tended toward early voting and early voter to I-voting. In addition, there was some evidence that I-voting brought a small but potentially significant number of non-voters into the electoral process. This is important because studies in the United States have suggested that a lack of confidence in the electoral process can lead individuals to decide not to vote [AHL08]. Internet voting in Estonia seems to have the reverse effect, potentially drawing in some voters who previously did not participate in the electoral process. A survey of voters after the 2007 parliamentary elections found that 1 in 10 internet voters suggested that they might not have voted if the internet option had not been available [TSB07]. The contrast between America and Estonia can be seen here between the relatively low level of technology trust in the United States and the high I-government support in Estonia.

The Estonian government has also used simple methods to increase voter understanding of and confidence in the I-voting system in an attempt to overcome any concerns about the lack of transparency and complexity. In both elections in which I-voting has been used, prior to the voting period, the government allowed all individuals eligible to vote the opportunity to test out the I-voting system in order to encourage people to see how the system worked. This helped the voters detect any problems they might encounter before the real I-voting period started. In Estonia, the primary concerns among the country's election officials, outside observers, political parties, and citizens, relate to the cost and acquisition of the hardware and software needed to read an ID card on a personal computer, updating expired ID card certificates and the renewal of PIN codes needed for electronic use of the ID card. The government engaged in a nationwide pre-election information campaign to inform voters about these potential issues and to encourage voters to try the system before the voting period started. In 2007 elections, about 4,000 voters did test the system.

5 Transparent Election Administration

In addition to having voters test the system so that they would know how the electronic equipment worked during the voting period, there were also other issues about which the national election officials wanted to educate I-voters. Specifically, in order to raise the confidence of voters, they were informed that they should ensure that the file of the voting application had not been modified in transmission or intercepted by untrusted parties. This was done by explaining to voters how, once the live voting period had started for I-voting, they could verify the authenticity of the voting application. Before the start of the I-voting period for some operational systems, the election officials published information about the cryptographic hash functions that were used, and during voting period voters could examine the checksums.

As an additional element of transparency, the number of I-voters who had cast ballots was updated regularly on the I-voting website during the early voting period. This very simple process allowed the wider national audience, as well as the political parties, to know how many i-voters had voted and to determine if the trend in the number of i-voters casting ballots seemed reasonable. At the end people were also able to compare the number of I-voters with the number of I-votes counted. The transparency of the election process was not mere window-dressing on the part of either election officials or voters. One real example that illustrates that the importance of allowing voters and the political parties to monitor the I-voting should not be underestimated. As the i-voting system was closed at the end of the early voting period, the final number of I-voters disappeared from the I-voting website for a couple of minutes. This incident caused immediate and intense feedback from voters.

A high level of transparency is appealing because it provides the voters as much data as they need so that each voter is convinced that her vote has been correctly registered. One key question is to know how much information can be reflected back to the voter without creating other problems. For example, one possibility is to let the voter inspect the ballot as it is registered in the trusted part of an Internet voting system (analogous to checking the statement of account in Internet banking). The ballot can only be inspected, not modified [Sk06] and the possibility for inspection may give the voter even greater trust in the system.

This idea has been thoroughly discussed during the development process of the Estonian Internet voting system but the realization of it was postponed. Therefore, other methods were used in order to convince the voter. If the voter decided to replace the I-vote with a new one, he got a notification of an earlier recorded I-vote. A second option for verifying the correctness of electoral administration was offered on election day in the polling station of voter's residence, where the fact of an valid I-vote had to be reflected on the polling lists in order the prevent voting more than once.

The I-voting system actually provides I-voters with more assurance that their ballots were included in the final tabulation and were tallied accurately compared to the traditional paper ballot system. The I-voter has two mechanisms that could increase the confidence of voters. First, voters who use the I-voting mechanism know that there is no misinterpretation of their ballot by a third-party. They do not have to worry whether the polling place workers can read their writing on election night and properly count their ballot; by contrast, all I-votes were counted. Second, the voter can check acceptance of an electronic I-vote during the I-voting period or after the end of the advance poll as described earlier.

6 Transparency and Observation in Practice

In the case of Internet voting, observation is of particular importance for several reasons. First, the introduction of new technologies can influence public opinion with regard to the ability of the election process to produce honest, verifiable results. In Estonia the electoral administration enjoys broad confidence of the electorate. This confidence is reflected in the fact that, even with the implementation of this new voting mechanism, the interest of domestic observers in observing the Internet voting was quite modest in last elections. Second, the introduction of such a new technology can influence international opinion about Estonia. This interest is reflected in the high interest that international observers have had towards Estonian I-voting and their efforts to assess whether Estonian elections using I-voting are conducted in line with international standards for democratic elections, provide an opportunity to identify potential concerns, and enhance the integrity of the elections process not only for Estonian public opinion but internationally. Third, there are also theoretical concerns that, given the electronic nature of the voting, the system is inherently less transparent than is traditional precinct based balloting.

According to the Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting and tabulation of results. Internet voting has been no different. All significant documents describing the I-voting system have been made available for all, including observers. In order to enhance the observers' knowledge about the system, political parties were invited to take part in a training course before each election in which I-voting was used. Besides political parties, auditors and other persons interested in the I-voting system also took part in the training. The training was followed by surveys of concrete procedures that were necessary for a set up of the I-voting system. Observers were invited also to a test of the counting process. However, few political parties exercised their opportunity to observe the I-voting procedures.

Throughout the I-voting observation period of one month, the main observation tool was the checking of the activities of electoral administrators against written documentation describing the necessary procedures. The key management function required extra attention, as the security and anonymity of I-votes was predicated on the encryption and decryption of votes. During counting event - the highlight of the election period - the management of the private key was demonstrated to observers. NEC mastered this key, and its members collegially could open the anonymous encrypted votes. The process of conducting the counting of ballots was all conducted with observers able to watch all ballot counting activities on large screens in the observation area. The process was fully narrated and observers were able to follow each step.

It is important that observers are deployed for a length of time necessary to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, the conclusions about the integrity of the system can not be made. In last elections of March 2007, I-voting procedures started several weeks before the elections day. Especially for casual foreign observers, the length of the observation period appeared to be a challenge. The OSCE did audit the 2007 elections and, in its report, it states that "election administration implemented the [Internet voting] system in a fully transparent manner, and appeared to take measures to safeguard the conduct of internet voting to the extent possible" [OSCE07].

The Estonian NEC has also been very supportive of analyses of its voting system by academic observers. In both 2005 and 2007, the NEC provided support to studies conducted by the Council of Europe that evaluated public confidence in the I-voting system. These two studies both found that there was a high level of public confidence in I-voting and provided an independent audit of public attitudes toward the I-voting system. Given the fact that transparency and confidence are not tangible but are attitudinal, these studies of public opinion in Estonia allowed the NEC and others involved in the elections to have additional knowledge that the I-voting system was effective and the procedures being used were acceptable to the public.

7 Validating the Voting Systems – Audit, Certification, Testing

The Estonian I-voting system was developed with the underlying principle being that all components of the system should be transparent for audit purposes. Procedures should be fully documented and critical procedures should be logged, audited, observed, and videotaped as they are conducted.

Specifically, during last elections, NEC has conducted audits on the source code and on the electoral procedures. A common requirement is that the source code of the voting system should be available for auditing. In Estonia, though, the code is not universally available but it can be audited if agreed to by the NEC. In order to rule out any manipulation by insiders, every election and audit by external auditing company had been ordered and it covered all of the technical and operational activities controlled by electoral committee. The audit was conducted by KPMG Baltics, which reviewed and monitored security sensitive aspects of the process continuously, such as updating the voters list, preparation of hardware and its installation, loading of election data, maintenance and renewal of election data and the process of counting the votes. The auditors' report about the 2007 Parliamentary election was released after all procedures, including the deletion of I-votes, were carried out. The report stated that the I-voting followed the rules described in the system's documentation and the integrity and confidentiality of the system were not endangered.

The I-voting system produces a wealth of system log information that can be used to monitor the work of the system thoroughly. In its different production functions, the I-voting system produces different logs on received, cancelled, and counted votes, also invalid and valid votes. The Audit Application enables to determine what happened to an I-vote given by a concrete person without revealing the voter's choice. These logs provide external auditors as well as observers with information that they can use to ensure that the system is working correctly.

The OSCE, in its report about the 2007 Parliamentary elections, recommended that, in addition to the audits of the process now conducted, all components of the system should be audited by an independent body in accordance with publicly available specifications, with all reports made public [OSCE07]. NEC has not published the audit reports referring to the contracts and given the consideration that publishing reports could make the system more vulnerable to attacks. In the future, the NEC should consider asking its auditors to produce both an internal audit report, intended for the NEC, and a report that can be made public, with certain information redacted.

In order to validate the electronic voting system, certification procedures could be established and other measures like testing and audits of different aspects should be taken. The Council of Europe has stated that it is necessary to promote the development of certification and accreditation schemes for e-voting systems in the member countries [CoE06]. A certification process will be very useful if there are a number of e-voting systems available. It might become very hard for any electoral authority to make sure a particular product is ready to be used, will operate correctly and will produce accurate, reliable results [Rec04].

Currently there is no domestic or international body that is ready to certify Estonian I-voting system. Estonia instead uses a system similar to that used in other countries, where a third-party audits the source code to ensure that the system operates as is specified. In addition to the audits discussed previously, system testing was also done on separate operation and functional components of the system in order to test the functionality and accuracy. Two weeks prior to the advance electronic voting period, the I-voting system was also tested by the public and contracted testers.

8 Conclusions

It is critical all election systems have fundamental safeguards for transparency in place because without them the public confidence necessary for legitimating elections cannot be ensured. Tools like observation, independent auditing, and system testing are suitable for assessing the actions of the electoral administrators. In addition, third party evaluations of public confidence in the process also serve to enhance our understanding about whether the public views the election with confidence and sees that the election administration was in fact transparent. These tools might not be easily accessible or of interest to the average person; however, it should be simple for those individuals who do want to participate.

The two Estonian I-voting experiences seem to prove that it is possible to solve the legal as well technological obstacles inherent for remote e-voting concerning the transparency of elections. The high degree of public confidence enjoyed by electoral administrators in last elections, as well as the fact that the legitimacy of the whole election process—including Internet voting—has not been questioned, strongly suggest that the elections have been carried out transparently. Moreover, the electoral administrators have provided procedural mechanisms that educate voters and the political parties about the process and allow each, through simple activities, to be an active participant in the election observation and evaluation process. The test voting process, the ability to re-vote, and the ability to determine that their vote was accepted all provide voters with a chance to evaluate and check the I-voting system.

In order to increase public awareness about IT security and teach people how to use the Internet safely, new initiatives, like public-private project “Computer Security 2009” and state’s Information Society Awareness Program have been started. The aim at further increasing the use of e-services with due attention to security issues and application of ID-card, will most probably raise the popularity of Internet voting in the future. Based on researches success of Internet voting is clearly linked to the overall ICT awareness [TSB07]. Next elections using I-voting as an option will take place in the year 2009.

ICT has already dramatically changed the way elections are conducted in many countries, and it must be accepted that this process will go on and affect more and more countries. Even if Estonia is still the only one practicing Internet voting countrywide on legally binding elections, it could be a matter of time when people in other countries also overcome their native conservativeness against new solutions. To get experiences, the first step has to be taken and trust can be built only based on experiences. Insecurity is the part of every IT system, but in order to reduce the insecurity a lot can be done. And learning from experience is highly valuable in making the I-voting transparent and confident

References

- [AHL08] Alvarez, R., Hall, T., Llewellyn, M.: Are Americans Confident Their Ballots Are Counted? *Journal of Politics* 2008 [Forthcoming].
- [AH04] Alvarez, R., Hall, T.: *Point, Click, and Vote: The Future of Internet Voting*. Washington, DC. Brookings Press 2004.
- [AH08] Alvarez, R., Hall, T.: *Electronic Elections: The Perils and Promise of Digital Democracy*. Princeton University Press 2008.
- [Be95] Bell, A.: Constitutional Aspects. *The International and Comparative Law Quarterly*. Vol. 44, No. 3. (Jul., 1995), pp. 700-705.
- [BO99] Bloomfield, R. and M. O'Hara.: Market Transparency: Who Wins and Who Loses? *The Review of Financial Studies*. Vol. 12, No. 1. (Spring, 1999), pp. 5-35.
- [CoE06] Remmert, M.: *E-Voting in Europe: Standards, policy practice*, 2006.
- [Court05] Decision of the Supreme Court of Estonia of Electronic Voting, <http://www.nc.ee/klr/lahendid/tekst/RK/3-4-1-13-05.html>.
- [DM02] Drechsler, W., Madise, Ü.: "E-Voting in Estonia." *Trames*, 2002, 6(56/51), 3, 234-244.
- [DM04] Drechsler, W., Madise, Ü.: Electronic Voting in Estonia. In: N. Kersting and H. Baldersheim (eds.) *Electronic Voting and Democracy. A Comparative Analysis*. Basingstoke: Palgrave Macmillan 2004, pp. 97-108.
- [FS02] Faust, J., Svensson, E.O.: The Equilibrium Degree of Transparency and Control in Monetary Policy. *Journal of Money, Credit and Banking*, 2002, vol. 34, No. 2., pp. 520-539.
- [HW08a] Hall, T., Wang, T.: Show Me the ID: International Norms and Fairness in Election Reforms. *Public Integrity*, 2008, 10, 2: pp. 97-111.
- [HW08b] Hall, T., Wang, T.: Normative Principles for Evaluating Election Fraud. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): *Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives*. Washington, D.C., Brookings Institution Press 2008.
- [Hy08] Hyde, S.: How International Election Observers Detect and Deter Fraud. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): *Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives*. Washington, D.C., Brookings Institution Press 2008.
- [Ma07] Maaten, E.: Practicing Internet Voting in Estonia. In *Baltic IT&T Review 2007*, <http://www.ebaltics.com/00704985?PHPSESSID=f5849c543bdc4a1b621bd4c73eb62fc0>.
- [MMV06] Maaten, E., Madise, Ü., Vinkel, P.: Internet Voting at the Elections of Local Government Councils in October 2005. Report on Internet Voting to the National Election Committee, Tallinn 2006, <http://www.vvk.ee/english/report2006.pdf>.

- [Mo98] Moncrieffe, J.M.: Reconceptualizing Political Accountability. *International Political Science Review / Revue internationale de science politique* 1998, Vol. 19, No. 4. (Oct.), pp. 387-406.
- [NEC07] National Electoral Committee of Estonia: Parliamentary Elections 2007 – Statistics of e-voting, http://www.vvk.ee/english/Ivoting_stat_eng.pdf.
- [OSCE07] OSCE/ODIHR Election Assessment Mission Report, Republic of Estonia, Parliamentary Elections, 4 March 2007, <http://194.8.63.155/item/25385.html>.
- [PR96] Pagano, M., A. Roell.: Transparency and Liquidity: A Comparison of Auction and Dealer Markets with Informed Trading. *The Journal of Finance*, 1996, Vol. 51, No. 2, pp. 579-611.
- [Pe07] Peterson, E.: Transparency In United States Election Law. Thesis Manuscript, University of Utah.
- [Rec04] Recommendation No. R (2004) 11 of the Committee of Ministers to members states on E-Voting, [http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec\(2004\)11_Eng_Evoting_and_Expl_Memo.pdf](http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec(2004)11_Eng_Evoting_and_Expl_Memo.pdf).
- [SHN06] Skagestein, G., Vegard Haug, A.V., Nødtvedt, E., Rossebø, J.: How to create trust in electronic voting over an untrusted platform. In: Krimmer, R. (Ed.) *Electronic Voting 2006*, Bonn: Gesellschaft für Informatik 2006, pp. 107-116.
- [SL01] Stirton, L., Lodge, M.: Transparency Mechanisms: Building Publicness into Public Services. *Journal of Law and Society* 2001, Vol. 28, No. 4., pp. 471-489.
- [Tr06] Perspectives e-voting. Presentation made at the E-Voting Conference in Tallinn, October 2006, http://www.ega.ee/files/27.10.06_Michael_Remmert_e-haaletamise%20konv.pdf.
- [TSB07] Trechsel, A.H., Schwerdt, G., Breuer, F., Alvarez, M., Hall, T.: Report for Council of Europe - Internet voting in the March 2007 Parliamentary Elections in Estonia. http://www.coe.int/t/e/integrated_projects/democracy/EVoting/Report_Evoting_Estonia_for_the_CoE_2007.doc.