Tallinn University of Technology Doctoral Theses
Series I: Social Sciences, No. 24

Remote Electronic Voting in Estonia: Legality, Impact and Confidence

PRIIT VINKEL

TUT
PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
Ragnar Nurkse School of Innovation and Governance
Faculty of Social Sciences

The thesis was accepted for the defense of the degree of Doctor of Philosophy in Public Administration on 20 July 2015.

Supervisors: Professor Dr Ülle Madise (University of Tartu, Estonia)
Professor Dr Robert Krimmer (Tallinn University of Technology, Estonia)

Opponents: Professor Dr Norbert Kersting (University of Münster, Germany)
Professor Dr Magdalena Musiał-Karg (Adam Mickiewicz University in Poznań, Poland)

Defense of the thesis: 24 August 2015

Declaration: Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology, has not been submitted for any other degree or examination.

Priit Vinkel

Publication of this thesis is granted by the Doctoral School of Economics and Innovation created under the auspices of European Social Fund

ISSN 1406-4790
ISBN 978-9949-23-827-9 (publication)
ISBN 978-9949-23-828-6 (PDF)

CONTENTS

LIST OF ORIGINAL PUBLICATIONS

This dissertation is based on the following original publications:

I Priit Vinkel. 2012. "Internet Voting in Estonia." In P. Laud (ed.). *Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011, Tallinn, Estonia, 26-28 October 2011, Revised Selected Papers.* Berlin: Springer, 4-12. (1.1)

II Ülle Madise and **Priit Vinkel**. 2011. "Constitutionality of Remote Internet Voting: The Estonian Perspective." *Juridica International* 18, 4-16. (1.2)

III Ülle Madise and **Priit Vinkel**. 2015. "A Judicial Approach to Internet Voting in Estonia." In Jordi Barrat and Ardita Driza Maurer (eds). *E-Voting Case Law: A Comparative Analysis*. Farnham: Ashgate Publishing, 1-35 (*forthcoming).* (3.1)

IV Ülle Madise and **Priit Vinkel**. 2014. "Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections." In Tanel Kerikmäe (ed.). *Regulating eTechnologies in the European Union*. Cham: Springer International, 1-19. (3.1)

APPENDIX

V Priit Vinkel. 2012. "Internet Voting: Experiences from Five Elections in Estonia." In T. Jundzis (ed.). *Proceedings of the International Conference: Democracy and Development – Taiwan and Baltic Countries in Comparative Perspective, 27-28 April 2012*. Riga: Latvian Academy of Sciences, 176-188. (3.1)

VI Ülle Madise and **Priit Vinkel**. 2010. "TIC, votacions per Internet i altres serveis electronics a Estonia." In J. Vall (ed.). *EINES 12, Politica 2.0*. Barcelona: Fundacio Josep Irla, 59-67. (3.2)

VII Ülle Madise, Epp Maaten and **Priit Vinkel**. 2014. "Voto por Internet en Estonia." In A. Ayala Sanchez (ed.). *Nuevas Avenidas de la Democracia Contemporanea*. Serie Docrina Juridica 707, Institutio de Investigaciones Juridicas. Mexico: Universidad Nacional Autonoma de Mexico, 575-601. (3.2)

VIII Ülle Madise, **Priit Vinkel** and Epp Maaten. 2006. *Internet Voting at the Elections of Local Government Councils on October 2005*. Report. Tallinn: Estonian National Electoral Committee. (6.7)

INTRODUCTION

Scope and aim

We live in a time where information and the development of information and communication technologies (ICT) – most importantly the Internet – have shaped the understanding of communication. As Manuel Castells (2007) has put it "The diffusion of Internet, mobile communication, digital media, and a variety of tools of social software have prompted the development of horizontal networks of interactive communication that connect local and global in chosen time." These networks build connections among persons and enhance the communication with the public as Internet-based transactions have grown to be a part of both private and public conduct. We see this tendency in commerce, where online business is growing stronger (Statista 2015a); likewise in online banking where the usage numbers in Europe reach up to 91% (Statista 2015b), and in the public sector where ICT-enabled services have also found growing acceptance (WE Forum 2015).

The nature of one country's democratic processes takes many influences from the development of the country and its democratic and legal culture (Venice Commission 2010). Therefore, the conduct of elections has many unique features in every country – e.g. the choice of voting channels or the time of voting. However, democratic elections have to adhere to a set of core principles – universality, freedom, equality (uniformity) and secrecy (ICCPR 1976, Art 25b). Guaranteeing these principles in all different electoral procedures (including electronic ones) is the challenge that is important to uphold the legitimacy of elections.

The transformation of electoral procedures has been seen as a part of the development of e-democracy, which has gained considerable interest since the dawn of the 21st century. According to Krimmer (2012) circumstances like decreasing voter turnout, continuing disconnection of the citizen and the representative and general implications of globalization have driven the process.

Introducing remote electoral methods (also, e.g., postal voting) serves the citizen in providing an easily accessible and comfortable means of voting. In addition, remote voting is also considered a viable alternative for disenfranchised voters whose participation in elections has always been dependent on the methods they are offered – voters living or residing permanently abroad, voters who are living in conditions which make it difficult for them to attend elections for geographical reasons and voters with disabilities. All these voters need to make extra efforts in participating in the democratic process, and in all these cases, the principle of universality (or general elections) prevails over the possible concerns connected with the way of voting (Gronke et al. 2008).

Remote state-citizen communication has been implemented in many communities, but Estonia has been one of the most eager countries to actively pursue electronic services and procedures (Drechsler 2006; Madise 2007). Estonia has featured a remote online

voting method since 2005, and has been the only country in Europe (not to say the world) to have it without limitations in all types of elections. However, despite the widespread acceptance of ICT in the Estonian society, the constant development of the system has to guarantee the accordance with up-to-date security and usability recommendations.

Researchers all over the world have early on tried to find suitable solutions to fit the criteria set by universal electoral principles and tackle the questions posed by different fields of interest. The research fields could be divided into four categories – computer science, legal science, social science and political science (Prosser and Krimmer 2004).

Theoretical literature in the computer science is often related to voting from an uncontrolled environment and connected technical risks (e.g. security of the voting device and voting channel). Most of the papers and new scientific thought are being channeled to the vision of finding the safest, tamper-proof, mathematically sound system currently possible (e.g. Joaquim et al. 2013 or Mohammadpourfard et al. 2014). This field of study looks for the ideal solution to answer all possible theoretical risks and practical acceptance. The theoretical literature, however, is by and large explored and tested in laboratory conditions and unfortunately is not often viable or feasible in practical implementations. Nevertheless, all these studies also help the operational researchers (including those in Estonia) to further improve systems that are used in practice (e.g. Springall et al. 2014 or Spycher et al. 2012). Additionally, many articles are devoted to a topic that has been seen as the number one confidence builder in remote Internet Voting systems – verification. In theory, verification can be seen in several categories – individual verification, where only the voter is able to verify the trail of the vote, and universal verification, where any person or institution is able to verify the overall results of the I-voting – and in multiple stages – cast as intended (ballots are well-formed), recorded as cast and tallied as recorded– depending on the level of assurance (Popoveniuc et al. 2010). Estonia has implemented the recorded as cast level in 2013 (Heiberg and Willemson 2014); however, discussions about possible additional steps in this field are ongoing. The verification scene is very rich and filled with different ideas to offer credible ways towards higher verifiability (e.g. Nestås and Hole 2012 or Volkamer et al. 2011). Historically, in the early 2000s, the domain of trust building in (remote) electronic voting solutions was dominated by the concept of certification (Council of Europe 2004). Over the years, and with the growing possibilities of different solutions, verifiability has grown to be the main factor in guaranteeing the theoretical trustworthiness of an electronic voting solution.

Legal science discussions form the basis for the implementation of a remote electronic voting system, as the question of constitutionality is the first issue to be answered (e.g. Braun 2006; Mitrou et al. 2003). Additionally, legal scientists are worried about judicial review of the election results and the legitimization of election outcomes (e.g. Loncke and Dumortier 2004; Meagher 2008).

In social and political sciences, Internet Voting has been researched from a wide variety. The main interests are summarized by the effect of Internet Voting on effective turnout (e.g. Bochsler 2009; Vassil and Weber 2011; Solop 2004), experiences of various implementations, as in Switzerland or Norway (e.g. Driza Maurer et al. 2012; Stenerud

and Bull 2012), or more general discussions on the democratic implications of novel ideas in the electoral field (e.g. Reiners 2013; Mendez 2010). However, since most of the papers are bound to the context of the appropriate countries, the field lacks social-science papers about the possible introduction of remote electronic voting in other countries and the implications of their use on a more theoretical level.

Moreover, the international community is looking for the best practices in different countries. The most prominent process being the work of the Organization of Security and Co-operation in Europe (OSCE) and its institution in charge of the human dimension, the Office for Democratic Institutions and Human Rights (ODIHR). The organization has intensified its observation of countries that are using alternative remote-voting methods (OSCE/ODIHR 2007; 2011; 2012a; 2012b; 2013b; 2015). Recently it has published a handbook on observing elections using new voting technologies (OSCE/ODIHR 2013a).

Literature about the Estonian Internet Voting experience was more concentrated in the early years, right after its adoption (e.g. Drechsler and Madise 2002; 2004; Maaten 2004; Madise and Martens 2006; Drechsler 2006), with some more specialized articles in the last five years (e.g. Alvarez et al. 2009; Musiał-Karg 2011; Heiberg et al. 2012; Reiners 2013; Heiberg and Willemson 2014). The Estonian experience has previously been analyzed in two dissertations (Krimmer 2012 and Madise 2007).

Consequently, a gap in the scientific literature concerning a holistic interdisciplinary approach of a remote electronic-voting experience over a longer period could be seen. This dissertation aims to address the issue by offering an evidence-based approach with insight from electoral practice into the experience of the Estonian Internet Voting program.

The theoretical framework of this dissertation is built on studies of election and constitutional law, the existing literature on the Estonian implementation and applicable studies in other countries.

The core assumption of this dissertation is that in order to establish the principle of universal elections (ultimately freedom of vote), additional complementary methods of voting should be offered for the citizens in addition to Election Day voting. Therefore, an experience-based approach on Internet Voting has been presented in the articles. Moreover, especially in a small country like Estonia, it is commonly understood that as many voters as possible (and feasible) are to be engaged in voting. Therefore, innovative, comfortable and attractive ways of voting are created. However, the catch for the lawmaker is to find a suitable balance between the principle of universal elections and the rest of the core principles.

The main question this dissertation aims to answer is:

- How has Estonia managed to implement remote electronic voting as an established and credible voting channel?

In order to answer the main research question it is necessary to further break this question down into three main areas and sub-questions:

- How constitutionally and legally sound are the Estonian solution and the implementation practices?
- How has the Estonian Internet Voting system developed over the course of its implementation, and what impact did it have?
- What factors have helped building confidence into the Estonian system?

The articles that compose this thesis hold interdisciplinary features, tackling the proposed questions among others from the perspectives of constitutional review, institutional development and technical understandability. The legal and constitutional aspects of the Estonian I-voting solution are looked upon in **II** and **III**. The development and experience of the Estonian Internet Voting solution are covered in **I**, **IV**, **V**, **VII** and **VIII**. The factors and measures of confidence are discussed in **I**, **V** and **VI**.

The main part of the dissertation is based on articles, out of which one paper is single-authored and rated 1.1 (**I**), three (**II**, **III** and **IV**) have been co-published with one of the doctoral advisors with a balanced input in all papers (rated 1.2 and 3.1). The thesis features a report (**VIII**), rated 6.7, which has been added to the appendix to give a detailed insight into the implementation of Estonian Internet Voting in its maiden use. Additionally, two (**VI** and **VII**) non-English publications (in Catalan and in Spanish) for supporting the dissemination of the Internet Voting research in the according region (both 3.2) and a single-authored article (**V**) on the Estonian Internet Voting experience featured in Latvia, rated 3.1, have been added to the appendix.

The author has extensive experience with the topic of elections, having worked at the Estonian National Electoral Committee (the central electoral management body, EMB, in Estonia) for 10 years (of which the last 2 years as chief executive). Additionally, he has taken part in the development of international standards at OSCE/ODIHR and Council of Europe and has been presenting the Estonian experience at numerous international conferences. Therefore, this thesis presents contemporary research on Internet Voting based on a rich set of practical experiences.

The following introduction is divided into three chapters, each addressed to answer one of the sub-questions proposed earlier.

1. The discussion over constitutionality

Before the first implementation of electronic voting, including Internet Voting, it is common to ask whether there is also a need to change the country's constitution (see Braun 2006; Heindl et al. 2003; Rüß 2000). Similarly, in the Estonian experience, adding a new voting method in addition to paper voting and the introduction of a fully remote way of voting raised several questions in constitutional law (**III**).

1.1 The constitutional review of 2005

The Constitutional Chamber of the Estonian Supreme Court has analyzed in its review process the accordance of Internet Voting with constitutional principles, mainly with the principle of equality (uniformity) (Supreme Court 2005). The President launched the case in 2005, just before the first e-enabled elections and adoption of the refined stipulations in the electoral law. The center of the argument lay in the question whether the Internet Voters' ability to change the Internet Vote by voting again electronically or on paper (for a general description of the Estonian I-voting system, see NEC 2015a) would give unconstitutional advantages when compared to the traditional voter (**II**).

A possible lack of legitimacy of the election results could stem from either of the following situations: The privacy of an individual I-voting procedure cannot be supervised or observed by authorities. Therefore, large-scale buying and selling of votes, as well as exercising other influence or pressure on the voter, could be possible. The people themselves cannot verify the I-voting results, and people need to have absolute faith in the accuracy, honesty and security of the electoral system (its organizers, procedures, software and hardware). For people who did not take part in developing the system, the computer operations could be verified only by knowing the input and comparing the expected with the actual output (similar to a black box). In a secret-ballot system, there is no known input, nor is there any expected output with which to compare the electoral results (**II**).

Additionally, guaranteeing the freedom and secrecy of vote in an uncontrolled environment was examined in the review process. Based on the remote nature, one of the cornerstones of free voting – mandatory privacy in the voting process – is not possible in Internet-based remote voting. The two sub-principles of secrecy of voting were analyzed by the Supreme Court: privacy of voting and the anonymity of the vote. The court explained that to be found constitutional, Internet Voting should especially have the "virtual voting booth" – the possibility to change the I-vote in the voting process. It is important to emphasize that the constitutionality of the Internet as a communication channel, together with possible threats on anonymity and secrecy, was not analyzed in that particular case and has not yet been analyzed by the Estonian Supreme court (**III**).

1.2. Understanding secrecy in Internet Voting

The secrecy of voting has traditionally been understood in Estonia, and elsewhere, as the right and obligation to cast the vote alone in a voting booth. In the case of Internet Voting, it is impossible to ensure the privacy aspect of the voting procedure. The voter's right to anonymity during the tallying of the votes can be guaranteed, indeed to the extent to which this can be secured in the case of remote postal voting (Kersting 2004a). Therefore, remote electronic voting requires a rethinking of the privacy principle (**II**).

The principle of privacy is there to protect a person from any pressure or influence acting against his or her free expression of a political preference. Such a teleological approach to the principle was the basis of the I-voting provisions from the very beginning of the whole project. Consequently, the provisions enabling Internet Voting are based on the premise that the government has to trust the citizen and avoid, whenever possible, interference with decision-making at the individual level. The voter has to be aware of the risks, and he or she has to have the right to decide whether to use the opportunity of Internet Voting (**II**). Therefore, Internet Voting cannot, under the same conditions, replace traditional paper voting and should be considered a complementary solution (Council of Europe 2004). The 2005 ruling of the Supreme Court agreed with this position (Supreme Court 2005).

1.3 Electoral complaints and Internet Voting

The second broader category of discussions on Internet Voting have taken place in the Constitutional Chamber of the Supreme Court following specific electoral complaints. Complaints in Estonian elections (both on paper voting and on Internet voting) can be issued via a fast-track appeal system, where institutions have only a limited period to reach a verdict (electoral committees five working days, Supreme Court seven working days). In addition to the Supreme Court, appeals have to be scrutinized in two tiers (county-level and national) of electoral committees. Altogether, there are three tiers, so the maximum duration of dealing with an electoral complaint in all instances is about one month (Heinsalu et al. 2012). The principles of equality, secrecy, technical uniformity, procedural soundness and security of Internet Voting have been raised in the different complaints. The effect of the possible shortcoming on the overall election results is the overarching question that has to be analyzed based in the complaints. By 2015, all of the complaints concerning Internet Voting have been dismissed (**III**). However, the complaints issued after the 2011 parliamentary elections have a strong influence on the parliamentary debates of 2012 (see chapter 2.2).

Additionally, an issue that has arisen in these complaint debates is how to obtain applicable and sufficient evidence, which is by concept difficult, due to the anonymity of the vote. So far the Supreme Court has been quite innovative and liberal in the I-

voting electoral complaint judgments, however, always stating that the election organizers should have done their best in avoiding any malpractice (**III**).

1.4 Assessing the constitutionality

On a broader note, the question whether remote Internet Voting with binding results in public political elections complies with the constitutional principles of sound and fair voting cannot be answered simply with a "yes" or a "no". Instead two questions could be proposed. The first sub-question should be whether the legal norms in the abstract comply with the constitutional provisions of the state, and the second whether the technical solution used to conduct voting procedures in a certain election guarantees constitutionality (**II**).

The first sub-question can be answered based on theoretical analysis and could be researched in a constitutional review process, but the second should be examined before and after the actual elections. The fact that it is not possible to fulfil all of the theoretical and conceptual requirements set for an (originally paper-based) voting system is not enough for declaring I-voting as a solution to be unconstitutional. The second sub-question can be answered with "yes" only if sufficient measures are in place to check whether the IT solutions work properly. This leads to the requirement that auditing, verification and evaluation of the results be stipulated in the law and electoral regulation (**II**).

In the case of Estonian, the legal norms comply with the constitutional provisions, because eID enables secure remote identification, eID has overall penetration, all advance voters (both electronic and paper voters) are placed in the same conditions, and the "virtual voting booth" (the right to replace an I-vote with another I-vote or a paper ballot) and the virtual double-envelope system ensure freedom of voting and the uniformity of elections. Therefore, the answer to the first sub-question is "yes". Moreover, the system is justified by the target to guarantee universal (general) suffrage in an information society where e-services (including Internet Voting) are demanded by a significant proportion of the electorate. Whilst formal equality can be provided, the questions of material equality (the access to computers and Internet) and the issue of the digital divide remain. In addition, complying with the principle of secrecy poses new obstacles for many countries. According to the teleological interpretation of the principle of secrecy, the voting act is to be seen not as an aim but as a measure to guarantee freedom of voting, and the anonymity aspect of the principle of secrecy can be guaranteed (**III**). The analysis of the compliance of the Estonian I-voting system with the ICCPR (1976) has given positive results as well, but also emphasized the importance of special procedures to facilitate auditing and observation of I-voting (Meagher 2008).

The answer to the second sub-question is more complicated. Internet Voting in concrete elections is constitutional if the provisions of the law are fulfilled in practice: only people who are entitled to vote can vote, I-votes cast over the Internet are recorded and tallied

properly, and only one vote per voter is counted (OSCE/ODIHR 2013a). Independent IT auditing that covers all aspects of the system can prove its soundness. The proper performance of the IT system should be verified and audited before, during and after voting. Personal computers and the Internet remain the weakest links of the system. Additional changes of 2012 introduced the first steps of individual verification to the Estonian system and therefore opened new possibilities to minimize the threats from personal computers. Nevertheless, remote online voting as a concept is never absolutely ready and secure. Constant development of the system needs to be maintained to stay ahead of possible risks and threats. To date, the courts answer the second sub-question with a tentative "yes". Nevertheless, confidence and trust are the most important factors in judging the reliability of the system and they should be built and maintained by effective practical measures (**III**).

1.5 Summary of the legal debate

In conclusion, the 2005 constitutional debate has maintained its position throughout the years of Internet Voting implementation in Estonia. The principle of the "virtual voting booth" as a guarantee for freedom and the understanding of teleological secrecy of voting have become the cornerstones of the Estonian system and are also adopted in other Internet Voting systems (see chapter 2.5). The electoral complaints hold an important role in surfacing possible challenges with the use of Internet Voting. During the first ten years, complaints on equality, secrecy, technical uniformity, procedural soundness and security of the system have been raised. However, no violations have been found.

The constitutionality of an Internet Voting system can be assessed on levels of the general compliance with the electoral principles and the soundness of the implementation of the system in actual elections. The first-level question in the Estonian case could be answered positively, the system is in general compliance with the constitutional provisions. The answer to the second-level question in Estonia could also be seen in a positive light, but it depends heavily on the processes of verification and auditing. In addition, the appropriate measures need constant upgrading and development.

2. The development and impact of the Estonian Internet Voting

This chapter aims to analyze the Estonian remote electronic voting experience throughout the years of its implementation. For this, the development of the Estonian system has been divided into three periods – (1) the setup and implementation phase, (2) the years of increasing participatory numbers and additional legal debates and (3) the introduction of verifiability and stable use of the method. Additionally, the impact of the added voting method will be analyzed and parallels with two other I-voting countries – Switzerland and Norway – will be drawn.

2.1 Setup phase

The year 2002 marked the start of the setup phase, when a very general principle of remote electronic voting was stipulated in the electoral law (LGCEA 2002), allowing the election authorities to start with the project preparations, find a vendor and prepare for the 2005 local elections. Legal debates on the topic were restarted in 2005 to broaden the regulations in the law (LGCEA 2005). This period also holds the discussions about the constitutionality of the system in the Constitutional Chamber of the Estonian Supreme Court (see chapter 1.1). To test the features of the system a limited pilot was held in Tallinn in January 2005 (**VIII**). The first e-enabled elections (for the local government councils) were held in October 2005. A more in-depth discussion and report can be found in **VIII**.

2.2 Pivotal discussions in the parliament and amendments in electoral law

The second phase entails a steady rise in user numbers and diffusion of the solution in elections. The legal stipulations had not been changed between the years 2005 and 2011. However, the technical solution was constantly updated for every implementation; the Mobile-ID support and a new voter-application interface were developed for the 2011 general elections (Heiberg et al. 2012). The end of this phase is marked by a report by OSCE/ODIHR (2011), where several key features of the Estonian Internet Voting system and the regulation were revised and recommendations were made. This process was the main engine to launch renewed discussions in the parliament to look over the Internet Voting regulations and amend the procedures to bring more transparency and introduce additional steps on verifiability (**IV**).

After the 2011 general elections, where almost a quarter of all votes were given electronically, the parliament decided to specify the norms of I-voting in electoral law in order to improve the legitimacy and transparency of I-voting. Until 2011, the I-voting procedures had only very brief legislative regulations (despite the discussions in 2005). The parliament established a special working group (Constitutional Committee 2011)

that, in addition to detailed procedures, had to propose a solution for raising transparency and accountability in the I-voting system (**III**).

At the same time the technical community, which had been involved by the EMB in discussions about the security and transparency of I-voting, came to the conclusion that a new mechanism for some level of verification was needed in Estonia (Draft law 186SE 2012). The perceived aim was to detect possible malicious attacks on the I-voting system. The EMB has a better chance to discover attacks and react to those if I-voters, even a relatively small amount of them, verify their vote. If somebody finds out and reports that his/her vote is not stored correctly, measures can be taken immediately (Heiberg et al. 2012). In addition, a second channel for executing the verification had to be found, because if voters use the same personal computers for voting and verification, it will only add a limited amount of additional information regarding the voting computers. Therefore, an independent channel, like a mobile phone or a mobile device, was introduced for verification (Heiberg and Willemson 2014).

In 2012, the parliament adopted several amendments (Draft law 186 SE 2012) to the electoral law, stating that a new electoral committee – the electronic voting committee – was to be created for the technical organization of I-voting.

The first elections where the committee was in charge were the 2013 local elections. The law also regulates that before every implementation the I-voting system must be tested and audited. The most significant change of the law was the statement that, from 2015 on, voters have to have the possibility to verify that their vote has reached and is stored at the central server of the elections and reflects the choice of the voter correctly (**IV**).

The main lesson that can be learnt from this period is that together with the development of the technical environment, also the legal regulation has to be kept up. As Drechsler and Kostakis (2015) argue, technology is constantly evolving, but the law is not updated immediately. This allows for a process of consideration where only sustainable and desirable technologies are implemented. Verifiability was not implemented when it was available (years before the actual introduction) but when there was a concrete need due to the recent discussions in the country. Moreover, only the quiet period between elections allowed these discussions to take place where a reasonable system was selected and implemented. Additionally, widely accepted reports and input from the specialists' community have shown to be strong initiators in the 2011-2012 legal processes. Moreover, the timing of possible reforms has to be taken into account, as the election-free period from 2011 to 2013 came after a long period of back-to-back elections and was the only time where EMB and the parliament could take up a larger reform of the system.

2.3 Recent years

The third phase of development could be defined in the last three elections, where the share of I-voters among all voters has stayed high and additional steps of individual verification – recorded as cast – were implemented (**IV**). The number of I-voters who verified their vote has grown through the years, reaching 4.3% in the 2015 elections (Table 1). Despite the relatively small number of verifiers, mathematically the absence of any large-scale attacks or manipulations is notable (Heiberg and Willemson 2014).

The discussion about transparency and verifiability in a remote electronic voting system has clearly defined the general Internet Voting discussion in the past (Krimmer 2012; Spycher et al. 2012, Volkamer et al. 2011) and will define it in the nearer future. The same is true for Estonia, despite introducing the first stages of verification (Springall et al. 2014 and predicted in **I**). The OSCE/ODIHR election specialists' report (OSCE/ODIHR 2015) emphasizes the need for added verifiability, and the electronic voting committee is actively seeking contributions from the ICT community (EVC 2015) to bring added knowledge into the analysis of the solution; the fact that the next elections are in 2017 offers enough time for bolder development.

Table 1**.** Detailed data on Internet Voting in Estonia 2005-2015 (Data: National Electoral Committee)

	2005 Local Elections	*2007 Parlia-mentary Elections*	*2009 European Parliament Elections*	*2009 Local Elections*	*2011 Parlia-mentary Elections*	*2013 Local Elections*	*2014 European Parliament Elections*	*2015 Parliamentary Elections*
Eligible voters	1,059,292	897,243	909,628	1,094,317	913,346	1,086,935	902,873	899,793
Participating voters (voter turnout)	502,504	555,463	399,181	662,813	580,264	630,050	329,766	577,910
General voter turnout	47.4%	61.9%	43.9%	60.6%	63.5%	58.0%	36.5%	64.2%
I-voters	9,317	30,275	58,669	104,413	140,846	133,808	103,151	176,491
I-votes counted	9,287	30,243	58,614	104,313	140,764	133,662	103,105	176,329
I-votes cancelled (replaced with paper ballot)	30	32	55	100	82	146	46	162
I-votes invalid (not valid due to a nonstandard of vote)	n/a	n/a	n/a	n/a	n/a	1	n/a	1
Multiple I-votes (replaced with I-vote)	364	789	910	2,373	4,384	3,045	2,019	4,593

	2005 Local Elections	*2007 Parlia-mentary Elections*	*2009 European Parliament Elections*	*2009 Local Elections*	*2011 Parlia-mentary Elections*	*2013 Local Elections*	*2014 European Parliament Elections*	*2015 Parliamentary Elections*
I-voters among eligible voters	0.9%	3.4%	6.5%	9.5%	15.4%	12.3%	11.4%	19.6%
I-voters among participating voters	1.9%	5.5%	14.7%	15.8%	24.3%	21.2%	31.3%	30.5%
I-votes among advance votes	7.2%	17.6%	45.4%	44%	56.4%	50.5%	59.2%	59.6%
I-votes cast abroad among I-votes	n/a	2% 51 countries	3% 66 countries	2.8% 82 countries	3.9% 105 countries	4.2% 105 countries	4.69% 98 countries	5.71% 116 countries
I-voting period	3 days	3 days	7 days	7 days	7 days	7 days	7 days	7 days
Share of I-votes that were verified by the voter	n/a	n/a	n/a	n/a	n/a	3.4%	4.0%	4.3%

2.4 The impact of Internet Voting

Estonia has implemented Internet Voting in eight consecutive elections. It was the first country, in 2005, to introduce remote electronic voting in pan-national binding elections and was leading a kind of "race" at the beginning of the 2000s for introducing remote electronic methods in elections (Maaten 2004; Kersting 2004b; Madise and Martens 2006). The number of Internet Voters has been rising from the beginning, reaching more than 176,000 voters and comprising more than 30% of all given votes in the 2015 parliamentary elections.

Internet Voting started low, with only 9,317 I-voters, but began to grow in the following implementations. The low start and the following step-by-step rise in numbers could be explained by Rodgers' theory on the diffusion of innovation (Vassil et al. 2014). The number of eligible voters and turnout numbers are distinctively different per election type. For example, European Parliament election turnout is also by general measures (Ehin et al. 2013) lower than in other election types, like local or national elections. Therefore, the absolute numbers as seen in Figure 1 have fluctuated per election type after reaching the highest level in the 2015 parliamentary elections.

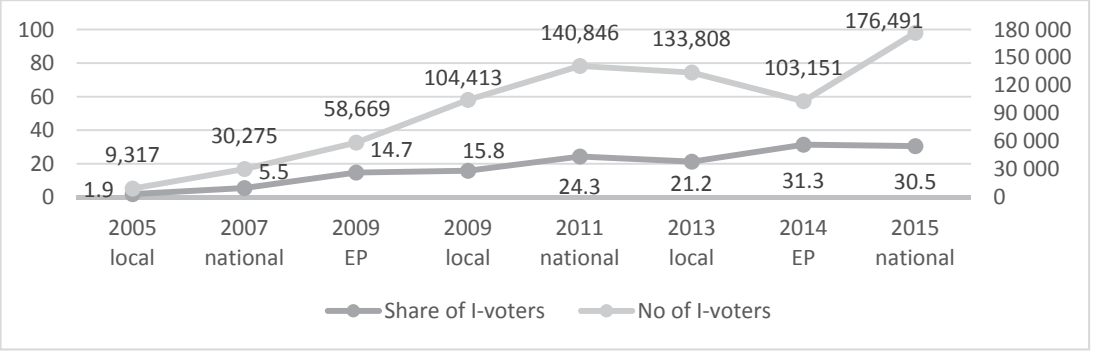


Figure 1. Number of I-voters and share of I-voters from all voters in 2005-2015

However, the share of Internet Voters among all voters has shown a steady rise despite the absolute number fluctuations, having risen to over 30% in the last two elections. Moreover, Internet Voting is offered for a seven-day period during advance voting, and since 2011, there have been more electronic advance voters compared to paper advance voters (Heinsalu et al. 2012 and Table 1). This process has had an impact on the paper-voting organization by putting the local governments under pressure to reduce the number of polling stations, as the attendance numbers have decreased, especially in rural areas. The effect is emphasized by the finding that the relative distance from the polling station has a clear correlation to the use of Internet Voting (Vassil and Solvak 2015).

When looking at the impact of the Internet Voting results, at least three categories could be distinguished: firstly the impact on the election turnout, whether adding a new voting method raises the turnout; secondly the effect of socio-demographic factors on the use of Internet Voting; and thirdly the relation of Internet Voting and the election results. Scientific reports on Estonian Internet Voting have been compiled after all eight elections (Trechsel and Vassil 2011; Vassil and Solvak 2015), and the results have been publicly discussed and are available on the EMB webpage.

One of the most frequent questions with any novelty electoral solution is the impact on turnout. Without a doubt, the hope to have a positive influence on the general turnout was one of the claimed aims in the early discussions of I-voting in Estonia (**VIII**). Nevertheless, it is difficult to assess the actual impact of Internet Voting on turnout because a direct comparison of the same election with and without I-voting is not possible. Perhaps a better question to be asked is what share of the electorate would not have participated in the voting, if the Internet Voting opportunity had not been provided. Unfortunately, only voter survey results can be used here. One exception is the case when Internet Voting is the only possibility for the voter and he/she uses this possibility**.** In the local elections, Estonia does not provide for voting from abroad by postal ballot or at a diplomatic representation, therefore voting over the Internet is the only voting method abroad (**IV**). The number of I-voters from abroad has grown after every election (Table 1).

The relation of the absolute number of I-voters and the general turnout has not been a linear one. Scientific surveys (Trechsel and Vassil 2011 and Vassil and Solvak 2015) have shown that most Internet Voters are actually paper voters who decide to switch the voting method; only a relatively small number of voters have started voting because of such a possibility. In 2005, I-voting seems to have had a slight effect on the increase in the turnout of voters who sometimes vote and sometimes do not. In 2007, already approximately ten percent of the questioned I-voters said that they certainly or probably would not have voted without having had the possibility to vote via the Internet (Trechsel 2007). Trechsel and Vassil show (in 2011) that the percentage of the I-voters questioned who certainly or probably would not have voted without having had the possibility to vote via the Internet has risen to 16.3%, which allows for the conclusion that the overall turnout might have been as much as 2.6% lower in the absence of such a method of voting. That is already a significant marker when one looks at the impact of Internet Voting on the overall turnout (**IV**).

Another interesting question is whether Internet-based voting shows any difference of representation within social groups. Remote electronic voting removes physical barriers hindering participation in elections of the aged, disabled or other groups with restricted mobility or ones that have difficulty in attending polling stations (e.g. persons having tight work schedules or working, studying or travelling abroad, parents of small children and persons living in regions with poor infrastructure), assuming, of course, that these people have access to the Internet.

Trechsel et al. and later Vassil and Solvak have concluded in their reports following the experience of Internet Voting from 2005 to 2015 that education and income, as well as type of settlement have been insignificant factors when choosing the Internet instead of other voting channels (Trechsel and Vassil 2011; Vassil and Solvak 2015). One of the most important findings of the studies researching I-voting predictors until the 2009 elections has been that it is not so much the cleavage between the Internet access haves and have-nots, but clearly computing skills and frequency of Internet use. However, since the 2009 local elections, where more than 100,000 voters used Internet Voting, those factors have become non-detectable (Trechsel and Vassil 2011). Confidence (trust) in the I-voting system and procedure has been the most significant factor throughout the years that directs the voters' choice in using a remote electronic voting method (Carter and Campbell 2011; Volkamer et al. 2011; Spycher et al. 2012). Vassil et al. (2014) have also claimed that based on empirical analysis at least a three-election period has to be studied to have adequate results for assessing the impact of different features on Internet Voting.

The question for political parties is whether the use of I-voting has an influence on the overall election results. Estonian parties that have favored I-voting in their campaigns and supported this voting method, have received more I-votes compared to those parties not supporting the use of I-voting. However, studies have shown that political left-right auto-positioning does not play an important role when choosing a voting channel

(Trechsel and Vassil 2011). In a separate study on the possible bias of I-voting on election results a similar conclusion was drawn – I-voting is politically neutral and does not have a direct impact on the election results (Vassil 2014).

In conclusion, a steady rise in the use of Internet Voting in Estonia was seen until the 2011 general elections; after that, the absolute number of voters has been fluctuating because of the nature of the elections it is used in, but the share of I-voters has kept on rising. Additionally, in advance voting, since 2011 I-voting has been more popular than traditional paper voting. When looking at the impact factors it can be seen that only a small amount of I-voters are completely new voters, the majority of I-voters are converted paper voters. A stronger impact could be made out in local elections, where I-voting is the only voting method from abroad. Additionally, socio-demographic features in determining the use of I-voting have been fading since the 100,000-voter hurdle was broken in 2009. Nevertheless, the factor of confidence (trust) in the system and procedures has stayed the most important determinant of I-voting use. Finally, several studies have looked into the political influence of I-voting and have found that I-voting is politically neutral and does not bring about biased results in elections. However, one should refrain from drawing conclusions on the impact of Internet Voting based solely on one execution of the method. At least three elections have to be analyzed to see the effects unfolding (Vassil and Solvak 2015).

2.5 Comparison with experience from Switzerland and Norway

The Internet Voting landscape has been quite active (E-Voting.CC 2015; Stein and Wenda 2014; Kersting 2004b; Barrat et al. 2012b; Krimmer and Kripp 2009). Remote electronic voting has been utilized on some level in more than twenty countries, and several countries analyze possible implementation (Faraon et al. 2015). The largest steps in Europe and maybe even worldwide have been made (beside Estonia) in Switzerland and Norway. Therefore, the experience of these two countries is analyzed next.

Switzerland, as a confederation, hosts its online elections mainly in the cantons. With postal voting being a long-time favorite in a country where elections and referendums are held often, the step to online solutions was not far-fetched. Different cantons have had pilots and try-outs since the early 2000s. Currently three different technical voting systems are in use, and more than half of the Swiss cantons use Internet Voting on some level of their electoral activity. Identification is based on unique passwords, and individual verification is offered. Since 2008, voting is also offered for Swiss expatriates. Similar to Estonia, the Swiss reached a stable user experience at the beginning of the 2010s and are today looking for possibilities to enhance their (different) systems by making them more transparent, observable and verifiable. The Swiss experience has also been studied by Schweizer Bundesrat (2002; 2006; 2013), Kersting (2004b), Gerlach and Gasser (2009), Driza Maurer et al. (2012), OSCE/ODIHR (2012b) and Serdült et al. (2015).

Norway started its Internet Voting project with two pilots, the first in the 2011 local elections and the second in the 2013 general elections. Both pilots were held in a small number of local-government units. Norway implemented the system after rigorous constitutional analysis and an international public tender (Ansper et al. 2009). From the beginning, recorded as cast verifiability was implemented, and a large effort was deployed to ensure public trust with the latest security solutions for the system. Technically and from the public perspective, both pilots were perceived as successful. However, after some evaluation, the Norwegian government decided to discontinue Internet Voting pilots due to possible risks in the system's security with the underlying reasons being the change in political leadership and the lack of trust the politicians held for the system. The Norwegian pilots are discussed in detail by OSCE/ODIHR (2012a; 2013b), Stenerud and Bull (2012), Barrat et al. (2012a) and Markussen et al. (2014).

As seen in Table 2, there is no single working solution for introducing Internet Voting. The compared countries show differences across the board and are/were nevertheless able to implement Internet Voting in their respective countries.

Table 2. Comparison of main features in the Estonian, Swiss and Norwegian I-voting experience.

	Estonia	**Switzerland**	**Norway**
Authentication method	eID	Passwords through postal system	Unique ID tied with mobile phones
Implementation style	Snap implementation, nationally	Step-by-step, canton-based	Step-by-step, only limited pilots
Verifiability	Individual	Individual	Individual and universal
Multiple vote casting	Yes	No	Yes

2.6 Summary of the Estonian implementation experience

To sum up this chapter, the Estonian experience in implementing Internet Voting could be seen in three stages, where firstly constitutional debate and introduction of the novelty system took place, after five elections a refreshment of the legal stipulations was in order and additional measures for more transparency and accountability in the system were debated about, and lastly a three-election period could be distinguished where a new level of verifiability was applied and a gap between elections ushered in a new discussion about additional measures of confidence.

What can be learnt from the Estonian experience to date is that the build-up of Internet Voting turnout takes time, as does looking at the diffusion of any innovative solution.

Additionally, the effects and impact of the added voting method will not appear after the first application; it has been claimed that at least three elections have to be taken into account. As for the impact of the Estonian system, it has been found that introducing Internet Voting has had a slightly positive influence on the general turnout, but most Internet Voters are former paper voters who started using a different method of voting. However, in specific groups (like abroad voters) the effect on turnout is present. Different socio-demographic values, like type of settlement or rate of computer use, were important determinants of I-voting before the 2009 elections, but they have become irrelevant since. The principal important factors for voters to choose I-voting through all elections have been trust and confidence in the solution.

When comparing the Estonian experience and solution to Switzerland and Norway, it can be seen that no single characteristic makes up a working system, and verifiability and trustworthiness are features other implementers are investing in as well. Each Internet Voting system has been developed in line with the needs of the actual context it was implemented in. Therefore, this does not allow for generalizing based on individual features; it is the complete solution that needs to be looked at. What can be learnt from Norway is that the ways of implementation are irrelevant if the politicians are not convinced that the election results would remain the same regardless of the new voting channels.

3. Building voter confidence in Estonian Internet Voting

Trust and confidence have been shown to be the top determinants of Internet Voting use (see chapter 2.4). Therefore, we have to look at the factors that enhance the belief of the user that the solution at hand is trustworthy. The voter, who in the case of Internet Voting is the actual user, has to be confident that the system cannot be manipulated and the election organizers follow the prescribed rules and operate the system correctly so that the systems' results reflect the actual will of the voters and thereby mirror the aggregated results of the elections correctly. In article **I** a model, consisting of three factors has been developed: (1) confidence in the overall e-government system, (2) confidence in the token of identification and (3) confidence in the EMB. The terms used in the articles have been further developed, in particular by redefining trust as a factor of confidence in the various stakeholders and used tokens.[1] In the following, the revised and extended factors are presented.

3.1 Confidence in the e-government

The first factor of the model takes into account an open and receptive society and discusses the relation of the general reception of the society of an e-solution provided by the state. With its re-independence at the beginning of the 1990s, Estonia started many processes anew, forcing the Estonian society to adapt to rapid changes and an open vision. This gives the Estonian society a slight advantage in adopting new solutions (Kalvet 2012).

According to the latest Global Information Technology Report (WE Forum 2015), the overall ranking of Estonia in the Networked Readiness Index is 21st; in the category of government success in ICT promotion Estonia ranks in 13th place, ahead of such IT giants as the US, Finland, Korea or Japan. In the category of assessed quality of governmental e-services, Estonia reaches a high fifth place. Since 2010, the official publication of Estonian legal acts, *State Gazette*, is electronic, which means that legal acts are published only on the Internet. In addition, tax declarations in Estonia are issued fully electronically in up to 95% of the cases (Estonian Tax and Customs Board 2015), and online banking has taken full precedence over traditional banking. All these are signs of acceptance of e-services in the society (**I**).

An important factor explaining the possibility to launch wholly new solutions like the official virtual identity or Internet Voting is the smallness of the country. Lennart Meri, the former president of Estonia compared Estonia to a small boat in one of his speeches: "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." (Meri 2000). Therefore, as the number of actual voters is around 1 million (Table 1), and there is

[1] The meaning of the term "trust" in the articles was adopted from the survey design of Trechsel and Vassil (2011) and can be understood as confidence in the different stakeholders involved in Estonian Internet Voting.

generally a positive notion towards innovation, such ideas as Internet Voting could be addressed more actively. In addition, the use of online ICT solutions in alternative democratic measures (e.g. participatory budget initiatives) further enhances the citizens' commitment and confidence in using e-methods in general (see Peixoto 2009; Raudla and Krenjova 2013). In the context of this model, this first factor could be summarized as confidence in the general governmental environment where the I-voting solution is implemented.

3.2 Confidence in the token of authentication

The second factor of confidence is formed by secure online authentication methods. The cornerstone of Estonian e-services, public as well as private, is eID. Since 2002, the ID card (together with other eID tokens) is the new generation's primary identification document. All Estonian citizens and residents above fifteen must have an ID card, which is issued by the government and contains certificates for remote authentication and digital signature (Identity Documents Act 1999).

The number of issued eIDs has exceeded 1 Million, providing all Estonians with the possibility to use secure online services. Approximately half of the cardholders (507,606 persons in May 2015) actively (during January-May 2015) use the eID functionality of their ID cards (Certification Centre 2015). Here it has to be noted that Internet Voting has strongly promoted the electronic use of ID cards (**VI**). Another important promoting factor has been the agreement between banks to allow Internet banking only with an ID card or a PIN calculator. The old one-time password cards can be used only for relatively small (in case of Swedbank 200 EUR per day) transactions (Schreiber and Kosienkowski, 2015). Therefore also international banks trust eID as a credible method of online authentication.

Parliamentary debate over eID cards raised several privacy and security questions, but the parties supporting compulsory eID commanded the majority of votes (**VIII**). The most controversial questions were possible risks 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 legislation. According to the law, fraudulent use of the ID card is punishable by a fine (Penal Code 2001). Therefore, confidence in the token of identification and in the authorities and services connected with the token are crucial in the overall confidence-building of a remote electronic system.

3.3 Confidence in the electoral principles and the EMB

The third, and arguably the most important factor can be understood as the effective measures to guarantee compliance and similarity with traditional electoral principles, as well as the confidence that the election organizers (in the Estonian case the National Electoral Committee) are able to guarantee these principles. The I-voting procedure has

been adapted to similar schematic rules compared to traditional voting. The double-envelope system (**V**), known from many voting systems (in particular postal voting) around the world, has been implemented as a logical structure in the electronic form of voting. The similar nature and the ability for the voter to relate to this system helps building trust to a novelty idea such as I-voting (Maaten and Hall 2008).

Evidently, confidence in the EMB is the strongest indicator in showing voters they can confidently use the system. Therefore, additional emphasis is laid in the thesis on offering an insight into the possibilities that were used in Estonia for guaranteeing the confidence of the voter in the EMB and the used I-voting solution.

The methods that have been used in Estonia 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 are diverse. Eight particularly important features could be differentiated.

As the first measure, in order to validate an electronic voting system, certification or verification procedures, testing and auditing can be considered (Council of Europe 2004). The development and importance of Internet Voting verifiability has been discussed earlier (see chapter 2.2). In 2013, first steps of verifiability were added to the system, and it has been used for three consecutive elections. Additional measures of verifiability are likely to be added to the system in the future. Verifiability, especially individual verifiability, where the voter can personally get information about the safe acceptance of the vote, helps the voter to understand the inner procedures of the voting solution and allows for the EMB to claim widespread soundness of the election conduct and results (Heiberg and Willemson 2014). However, the risk of receiving false-positive malignant claims of unsuccessful verifications might occur so that the EMB has to have a procedure at hand to take appropriate measures.

Secondly, in most of the e-enabled elections in Estonia, the EMB has allowed all voters to test out the I-voting system prior to the voting period in order to encourage people to see how the system works, calling them mock or demo elections. This has helped the voters detect any problems they might encounter before the real I-voting period has started. In Estonia, the primary concerns among the country's election officials, outside observers, political parties and citizens relate to the acquisition of the hardware and software needed to use an ID card on a personal computer, updating expired ID card or Mobile-ID certificates and the renewal of PIN codes needed for the electronic use of the ID card or Mobile-ID. System-testing prior to elections is also an important factor in order to control the functionality and accuracy by contracted testers, auditors, observers and by the public (**IV**).

Thirdly, the Estonian I-voting system was developed with the principle that all components of the system should be transparent for audit purposes: procedures are fully documented, and critical procedures are logged, audited, observed and videotaped (since

2013 also published on Youtube) as they are conducted. A separate procedural audit by Certified Information Systems (CISA) auditors is procured by the EMB for every election. The scope of the audit is to ensure the validity of performed procedures compared to the handbooks and technical documentation of I-voting. Additionally, auditors review and monitor security-sensitive aspects of the process, 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 (**VII**).

Fourthly, it is a common requirement that the source code of an information system is available for public audit (Council of Europe 2004). In Estonia, though, until 2013, the source code of the I-voting solution was not universally available, but one could access it by signing a non-disclosure agreement with the EMB. However, after the second legal debates of 2012, the source code of all central servers of the voting system as well as the software of the vote verification application has been made available on the Internet (EVC 2013).

Fifthly, according to the Estonian electoral law, all procedures related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting procedures, counting and tallying of results. Internet Voting has been no different. All significant documents describing the I-voting system have been made available for the public (NEC 2015b), including observers. In order to enhance the observers' knowledge about the system, political interlocutors are invited to take part in a training course before each election. Besides political parties, auditors and other persons interested in the I-voting system can take part in the training. Observers are also invited to participate in test elections during the setup phase (**V**).

Sixthly, it is important that observers be deployed for a length of time to allow meaningful observation. If some important stages influencing the correctness of the final results have not been observed, the conclusions about the integrity of the system cannot be made. Especially for foreign observers, the length of the observation period appears to be a challenge. The OSCE reported on Estonian Internet Voting in 2007, 2011 and 2015 (OSCE/ODIHR 2007; 2011; 2015) and in the 2011 report states, "The OSCE in general found widespread trust in the conduct of the Internet Voting by the NEC [National Electoral Committee]. However, … more detailed and formal control of software installation and reporting on testing of the Internet Voting system could further increase transparency and verifiability of the process." (OSCE/ODIHR 2011). As a direct result in 2012 the process of added transparency was created. Therefore, international observation is an influential and important source for getting feedback and peer review from the international community, which helps building general confidence in the EMB and the used voting methods.

Seventhly, as an additional element of transparency, the number of I-voters was regularly published on the I-voting website (www.valimised.ee). This very simple process allowed the wider audience, as well as political parties and media to follow how many I-voters

had voted and to determine if the trend in the number of I-voters casting ballots seemed reasonable.

Eighthly, in order to convince voters that their votes had been correctly registered, they had the option to check whether their I-voting fact had been reflected on the polling lists on Election Day in order to prevent voting more than once. In addition to verification itself, a second option for confirming the arrival of an I-vote has been possible during the I-voting period. If the voter decided to replace the I-vote with a new one, he was notified in the voting application of a previously recorded I-vote being stored in the central system (**IV**).

There are many different possibilities to give the wider audience additional confidence in the procedures and organization of remote electronic elections. In summary, eight important features could be distinguished:

I Technical features

(1) Introducing stages of verifiability (both individual and universal)

(2) Introducing procedural audit measures

(3) Publishing the source code of the system

II User experience features

(4) Providing mock elections for the public

(5) Providing safeguarding procedures for the voter to check the I-voting fact

(6) Publishing the number of I-voters during the voting process

III Observation related features

(7) Inviting and training domestic I-voting observers

(8) Inviting and accepting international observers

3.4 The House of Confidence

To conclude, the topic of confidence-building in the Estonian Internet Voting experience was looked at in three distinctive factors. It is important to reiterate the importance of each of the three sets of features, as functioning in a complex structure provides for the necessary confidence.

Based on the previous discussion, an original concept model called The House of Confidence (HoC) was developed for this thesis (Figure 2). This is the first attempt to conceptualize the features of confidence-building based on the actual Estonian

experience. The theoretical essence of the HoC touches upon the concept of the "E-voting Mirabilis", developed by Krimmer (2012).

From the Mirabilis four-way categorization, the first pillar of HoC stands for politics/technology, the second pillar for technology/society and the third pillar, the broadest one, for the technology/law/society aspects of the contextual factors presented by Krimmer (2012).

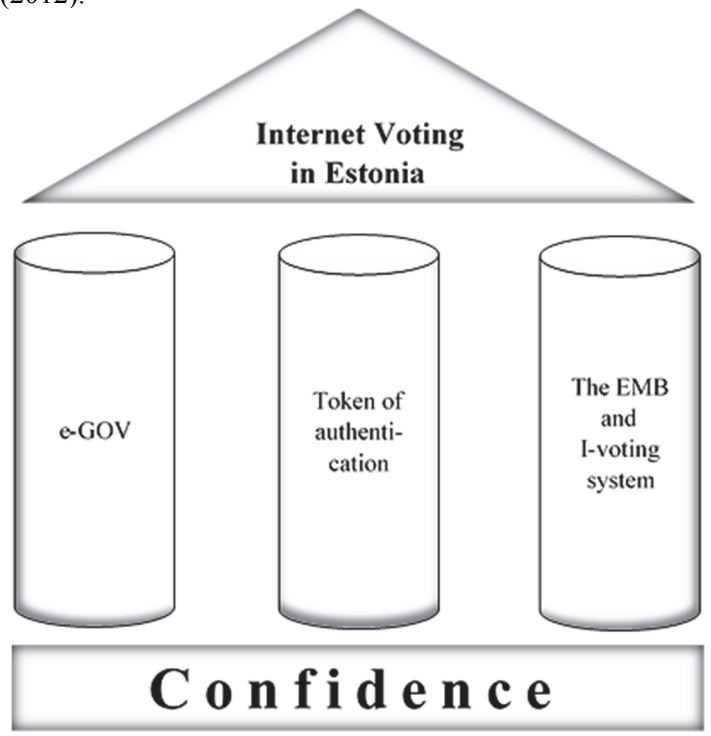


Figure 2. House of Confidence (further developed from **I** and **V**)

Confidence in the Internet Voting system stands on three pillars where the first two – the general e-government environment and the e-identity – are more underlying components, whereas the third – EMB and I-voting system – forms the backbone of confidence in the concept of Internet Voting. The third pillar offers the most possibilities to enhance public confidence by smart procedural and system-related choices listed in the previous sub-chapter.

Similarly, former OSCE/ODIHR Director Lenarčič has compared electoral processes to a house (Lenarčič 2010). He discussed that if elections [electoral processes] are fraudulent, i.e. the foundation of the house is not solid, then no matter how well the house is built, it will crumble. Therefore, if any of the three pillars show signs of weakness and do not guarantee the confidence of the voter, the House of Confidence, supporting the nominal Internet Voting "roof" concept, could be in danger of collapsing.

Conclusion and outlook

In conclusion, what the Estonian experience, so far, has shown is that it has been implemented as a credible voting method. The channel has also become a solid part of the Estonian so-called "e-stonia" narrative. Many news articles about Estonia in the international media define the country by its e-capability in the electoral field (e.g. NY Times 2014; BBC News 2013). Nevertheless, in order to see beyond the shiny surface presented in the newscasts, questions that are more detailed need to be asked.

Therefore, the main question in this dissertation, how Estonia has managed to implement remote electronic voting as an established and credible voting channel, was looked at by means of three sub-questions.

- How constitutionally and legally sound are the Estonian solution and the implementation practices?
- How has the Estonian Internet Voting system developed over the course of its implementation, and what impact did it have?
- What factors have helped building confidence into the Estonian system?

The constitutional foundation of the Estonian Internet Voting lies in the 2005 constitutional debate, which has maintained its position throughout the years of the implementation of Internet Voting in Estonia. The principle of the "virtual voting booth" as a guarantee for freedom and the understanding of teleological secrecy of voting have become the cornerstones of the Estonian system. The electoral complaints hold an important role in presenting possible challenges with the use of Internet Voting. During the first ten years of implementation, complaints on equality, secrecy, technical uniformity, procedural soundness and security of the system have been raised. However, so far no violations have been found in the complaints process.

According to the assessment of the Supreme Court, the Estonian I-voting system is in general compliance with the constitutional provisions. The soundness of the implementation practices depends heavily on the undertaken measures – like processes of verification and auditing – for single elections. It is important to emphasize that the Internet Voting system and the appropriate measures need constant upgrading and development to fit constitutional criteria.

The Estonian experience in implementing Internet Voting could be seen in three chronologic stages – firstly the constitutional debate and the introduction of the I-voting system; secondly a refurbishing of the legal stipulations after five elections and additional measures for a more transparent and accountable system; and lastly a three-election period where a new level of verifiability was applied and a gap between elections ushered in new discussions about additional measures of confidence.

What can be noted from the Estonian experience to date is that Internet Voting turnout build-up takes time; the development is the same as looking at the diffusion of any innovative solution. Additionally, the effects and impact of the added voting method will not implicitly show after the first application; it has been claimed that at least three

elections have to go by to make any conclusions. As for the impact of the Estonian system, it has been found that introducing Internet Voting has had a slight positive influence on the general turnout, but mostly Internet Voters are paper voters who started using a different voting method. However, a positive effect on turnout in specific groups, like abroad voters, could be brought out. Different socio-demographic values, like type of settlement or rate of computer use, were important determinants of I-voting before the 2009 elections, but have lost its importance since. The principal significant factors for voters to choose I-voting through all elections have been trust and confidence in the solution.

The short comparison with two other implementing countries (Switzerland and Norway) shows that there is no unified understanding of how a remote electronic voting solution should be implemented. For instance, using the postal system to send vital parts of the identification scheme would be unthinkable in Estonia. Therefore, context matters in the way every country finds its best practice in introducing such a novelty solution.

As trust and confidence have been found to be the most important factors for the voter to choose I-voting over other voting methods, a model called House of Confidence was designed. Confidence in the Internet Voting system stands on three pillars, where the first two – the general e-government environment and the e-identity – are more underlying components, whereas the third – EMB and the I-voting system – forms the backbone of confidence in the concept of Internet Voting. The third pillar also offers the most possibilities to enhance public confidence by smart procedural and system-related choices like verifiability, emphasis on auditing, testing and overall transparency and domestic and international observation. However, if any of the three pillars show signs of weakness and do not guarantee the voters' confidence in elections, the House of Confidence, supporting the nominal Internet Voting "roof" concept, could be in danger of collapsing. Therefore, all of the pillars should be equally important in sustaining the confidence of the voter in Internet Voting.

The topics discussed in the thesis will undoubtedly be analyzed also in the future. The ten-year period of continuous application of such voting method offers great opportunity for research and every added implementation shall provide additional data and possibilities for more complex analysis for the researchers. Estonia serves as a benchmark for any other country to come, therefore, continuous and comparable research should follow all elections that make use of Internet Voting in the future.

The most interesting avenues of further research lie in the implementation of added verifiability and the perceived impact of the solutions. Every step of added verifiability beyond the currently implemented recorded as cast level offers valuable insight into the practical applicability of theory-driven solutions of verification. Moreover, the relation of added verifiability and the voters' confidence and trust should be examined. Sociological research on the topic of voters' confidence could also be more specified, providing better insights into the separate factors of the House of Confidence and possibly identifying additional reasons for the voters' confidence in Internet Voting.

Additionally, the role of international standards, especially the applicability of the renewed recommendation Rec(2004)11 (Council of Europe 2004) in the legal process of those countries which are adding provisions of remote electronic voting to their electoral legislation, should be researched. This would give insight into the possibility of harmonization of principles in different legal structures and democratic environments. In addition, from the legal perspective, a comparative analysis on appeal and complaint stipulations and case practice in different I-voting countries would allow for a more detailed look on how and with what limitations constitutional principles are guaranteed in different systems.

On a more general note, in order to get invaluable feedback on the possibility of implementing Internet Voting, it could be taken from the realm of the idealistic drawing boards of scientists and engineers and put to the test in the actual environment. The context in which this system is launched has to have at least the basic prerequisites to successfully build the confidence of the society.

Internet Voting is by essence a solution that divides the interested parties. A solution that redefines hundred-year-long perceptions of acceptable democracy has to do as much. Discussions about the acceptability of such a solution started earlier than the Estonian system was implemented and surely influenced the development of the system (e.g. Buchsbaum 2004; Buchstein 2004).

Nevertheless, the criticism of the system could be motivated by different reasons. The politicians' understanding of the impact of remote electronic voting can never be underestimated. The biggest fear is to be suspected of unwanted influence on their electorate, e.g. the fear of lost votes. However, although the bias question has been answered scientifically, fear stays. The IT specialists and scientists are more likely to be influenced by the yearning for the perfect system, for a solution where most of the theoretical threats would be neutralized. However, in practice the perfect system exists only on paper. Legal scientists have to protect the core principles of elections. Although, as put forward in the beginning, universal suffrage demands new and innovative solutions, these solutions have to be balanced over universality and other principles like equality, secrecy etc. An interesting question comes to mind, whether not offering the best possible access to elections, i.e. implementing remote voting solutions, would be unconstitutional and not in compliance with the constitutional principles.

Therefore, imagine the election organizer fitted with the task of organizing remote e-enabled elections; all these different aspects have to be considered, and these theoretical implications are vital. The context in which elections are organized matters. Because without taking into account the democratic environment of the country, the solutions would not evolve in the right direction, of becoming more transparent, more observable and more in balance with all of the electoral principles. This thesis aims to add information to all fields of interest, to any other scientist or any other country considering such solutions.

References

Alvarez, M., T. Hall and A. Trechsel. 2009. "Internet Voting in Comparative Perspective: The Case of Estonia." *PS: Political Science & Politics* 42, 497-505.

Ansper, A., S. Heiberg, H. Lipmaa, T.A. Øverland and F. Van Laenen. 2009. "Security and Trust for the Norwegian E-Voting Pilot Project E-valg 2011." In A. Jøsang, T. Maseng, S.J. Knapskog (eds.). *Identity and Privacy in the Internet Age*. Berlin/Heidelberg: Springer, pp. 207-222.

Barrat, J., M. Chevalier, B. Goldsmith, D. Jandura, J. Turner and R. Sharma. 2012a. "Internet Voting and Individual Verifiability: The Norwegian Return Codes." In M. Kripp, M. Volkamer, R. Grimm (eds.). *Proceedings of the 5th International Conference on Electronic Voting (EVOTE2012)*. Bonn: GI, 35-45.

Barrat, J., B. Goldsmith and J. Turner. 2012b. *International Experience with E-Voting*. Stockholm: IFES Foundation.

BBC News. 2013. "How Estonia became E-stonia." Available at http://www.bbc.com/news/business-22317297 (last accessed 31 May 2015).

Bochsler, D. 2009. "Can the Internet Increase Political Participation? An Analysis of Remote Electronic Voting's Effect on Turnout." Available at http://pdc.ceu.hu/archive/00005913/01/bochsler-web_1.pdf (last accessed 31 May 2015).

Braun, N. 2006. *Stimmgeheimnis: Eine rechtsvergleichende und rechtshistorische Untersuchung unter Einbezug des geltenden Rechts*. Bern: Stämpfli Verlag.

Buchsbaum, T. 2004. "E-Voting: International Developments and Lessons Learnt." In Alexander Prosser and Robert Krimmer (eds). *Electronic Voting in Europe Technology, Law, Politics and Society*. LNI P-47, Bregenz: GI, 31-34.

Buchstein, H. 2004. "Online Democracy, Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory." In N. Kersting and H. Baldersheim (eds). *Electronic Voting and Democracy: A Comparative Analysis*. Basingstoke: Palgrave Macmillan, 39-58.

Carter, L. and R. Campbell. 2011. "The Impact of Trust and Relative Advantage on Internet Voting Diffusion." *Journal of Theoretical and Applied Electronic Commerce Research* 6(3), 28-42.

Castells, M. 2007. "Communication, Power and Counter-Power in the Network Society." *International Journal of Communication* [S. l] 1, 29.

Certification Centre. 2015. Response to a query about the latest statistics of the electronic use of ID cards, issued 19 June 2015 via e-mail.

Constitutional Committee. 2011. Minutes of the session of 9 June 2011 of the Constitutional Committee of the Estonian Parliament. Available at http://www.riigikogu.ee/download/6ca49b18-e6ec-b9f7-8e88-826d5d8ef5a4 (last accessed 31 May 2015).

Council of Europe. 2004. Recommendation Rec (2004) 11 "Legal, Operational and Technical Standards for I-voting" of the Council of Europe. Available at http://www.coe.int/t/dgap/democracy/activities/ggis/evoting/key_documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf (last accessed 31 May 2015).

Draft law 186 SE. 2012. The draft law for amending the election acts, number 186 SE, Estonian Parliament, adopted 17 October 2012. Available at http://www.riigikogu.ee/tegevus/eelnoud/eelnou/abc6bd69-0c8f-4012-8616-9277a7cbfec8/Riigikogu%20valimise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus/ (last accessed 31 May 2015).

Drechsler W. 2006. "The Estonian E-Voting Laws Discourse: Paradigmatic Benchmarking for Central and Eastern Europe." *NISPAcee Occasional Papers in Public Administration and Public Policy* 5(2), 11-17.

Drechsler, W. and V. Kostakis. 2015. "Should Law Keep Pace With Technology? Law as Katechon." *Bulletin of Science, Technology & Society* 0270467615574330.

Drechsler, W. and Ü. Madise. 2002. "E-Voting in Estonia." *Trames* 6(3), 234-244.

Drechsler, W. and Ü. Madise. 2004. "Electronic Voting in Estonia." In N. Kersting and H. Baldersheim (eds). *Electronic Voting and Democracy: A Comparative Analysis*. London: Palgrave Macmillan, 97-108.

Driza Maurer, A., O. Spycher, G. Taglioni and A. Weber. 2012. "E-Voting for Swiss abroad: A Joint Project between the Confederation and the Cantons." In M. Kripp, M. Volkamer, R. Grimm (eds.). *Proceedings of the 5th International Conference on Electronic Voting (EVOTE2012)*. Bonn: GI, 173-187.

Ehin, P., Ü. Madise, M. Solvak, R. Taagepera, K. Vassil and P. Vinkel. 2013. *Independent Candidates in National and European Elections: Study*. Brussels: European Union. Available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493008/IPOL-AFCO_ET(2013)493008_EN.pdf (last accessed 31 May 2015).

Estonian Tax and Customs Board. 2015. "Electronic Filing of Income Tax Returns is now Open." Available at http://www.emta.ee/index.php?id=36597&tpl=1026 (last accessed 31 May 2015).

EVC. 2013. “The Source Code of the Estonian I-voting Solution.” Available at https://github.com/vvk-ehk/evalimine (last accessed 31 May 2015).

EVC. 2015. “The Electronic Voting Committee Call for Proposals for Amending the Internet Voting Solution by 2017 Elections.” Available at http://www.vvk.ee/valimiste-korraldamine/vvk-uudised/kutse-ideepaev-e-haaletamise-parenduseks/ (last accessed 2 June 2015).

E-Voting.CC. 2015. “Map of E-Voting Usage in the World.” Available at http://www.e-voting.cc/en/it-elections/world-map/ (last accessed 31 May 2015).

Faraon, M., G. Stenberg, J. Budurushi and M. Kaipainen. 2015. “Positive but Skeptical: A Study of Attitudes towards Internet Voting in Sweden.” In: P. Parycek, M. Sachs and M. M. Skoric (ed.). *CeDEM Asia 2014: Proceedings of the International Conference for E-Democracy and Open Government*. Hong Kong, 4-6 December, 2014. Krems: Edition Donau-Uni Krems, 191-205.

Gerlach, J. and U. Gasser. 2009. *Three Case Studies from Switzerland: E-Voting*. Internet & Democracy Case Study Series. Harvard: Berkman Center Research Publications. Available at http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf (last accessed 31 May 2015).

Gronke, P., E. Galanes-Rosenbaum, P. A. Miller and D. Toffey. 2008. “Convenience Voting.” *Annual Review of Political Science* 11, 437-455.

Heiberg, S. and J. Willemson. 2014. “Verifiable Internet Voting in Estonia.” In R. Krimmer and M. Volkamer (eds.). *Proceedings of Electronic Voting 2014 (EVOTE2014)*. Tallinn: TUT Press, 7-13.

Heiberg, S., P. Laud and J. Willemson. 2012. “The Application of I-voting for Estonian Parliamentary Elections of 2011.” In A. Kiayias and H. Lipmaa (eds). *E-Voting and Identity: Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*. Berlin/Heidelberg: Springer, 208-223.

Heindl, P., A. Prosser and R. Krimmer. 2003. “Constitutional and Technical Requirements for Democracy over the Internet: E-Democracy.” In R. Traunmüller (ed.). *Electronic Govenment*. Berlin: Springer-Verlag, 417-420.

Heinsalu, A., A. Koitmäe, M. Pilving and P. Vinkel. 2012. *Elections in Estonia 1992-2011*. Tallinn: National Electoral Committee.

ICCPR. 1976. *United Nations International Covenant on Civil and Political Rights*. Available at http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (last accessed 31 May 2015).

Identity Documents Act. 1999. Art 5 of the Identity Documents Act. Available at https://www.riigiteataja.ee/en/eli/513042015004/consolide (last 31 accessed May 2015).

Joaquim, R., P. Ferreira and C. Ribeiro. 2013. "EVIV: An End-to-End Verifiable Internet Voting System." *Computers & Security* 32, 170-191.

Kalvet, T. 2012. "Innovation: A Factor Explaining E-Government Success in Estonia." *Electronic Government* 9(2), 142-157.

Kersting, N. 2004a. „Briefwahl im internationalen Vergleich." *Österreichische Zeitschrift für Politikwissenschaft 33(3),* 341-351.

Kersting, N. 2004b. „Online-Wahlen im internationalen Vergleich." *Aus Politik und Zeitgeschichte B18,* 16-23.

Krimmer, R. 2012. *The Evolution of E-Voting: Why Voting Technology is Used and How it Affects Democracy*. Tallinn: TUT Press.

Krimmer, R. and M. Kripp. 2009. "The Use of Electronic Voting Around the World." *Modern Democracy 2*, 8-9.

Lenarčič, J. 2010 Address by Ambassador Janez Lenarčič, Former Director of the OSCE/ODIHR, at the OSCE Chairmanship Expert Seminar on the "Present State and Prospects of Application of Electronic Voting in the OSCE Participating States", in Vienna, Austria on 16 September 2010. Available at http://www.osce.org/odihr/71361 (last accessed 31 May 2015).

LGCEA. 2002. Local Government Council Election Act, passed on 27 March 2002. Electronic Voting regulation in Art. 50. Available at https://www.riigiteataja.ee/ akt/95225 (last accessed 31 May 2015).

LGCEA. 2005. Amendments to the Local Government Council Election Act passed on 28 June 2005. Available at https://www.riigiteataja.ee/akt/938241 (last accessed 31 May 2015).

Loncke, M. and J. Dumortier. 2004. "Online Voting: A Legal Perspective." *International Review of Law, Computers & Technology* 18, 1.

Maaten, E. 2004. "Towards Remote E-Voting: Estonian Case." In Alexander Prosser and Robert Krimmer (eds). *Electronic Voting in Europe Technology, Law, Politics and Society*. LNI P-47. Bregenz: GI, 83-90.

Maaten, E. and T. Hall. 2008. "Improving the Transparency of Remote I-voting: The Estonian Experience." In R. Krimmer and R. Grimm (eds). *Electronic Voting 2008*. Bonn: Gesellschaft für Informatik.

Madise, Ü. 2007. *Elections, Political Parties, and Legislative Performance in Estonia: Institutional Choices from the Return to Independence to the Rise of E-Democracy*. Tallinn: TUT Press.

Madise, Ü and T. Martens. 2006. "E-Voting in Estonia 2005: The First Practice of Country-Wide Binding Internet Voting in the World." In R. Krimmer (ed.). *Electronic Voting 2006*. LNI P-87. Bregenz: GI, 27-35.

Markussen, R., L. Ronquillo and C. Schürmann. 2014. "Trust in Internet Election: Observing the Norwegian Decryption and Counting Ceremony." In R. Krimmer and M. Volkamer (eds.). *Proceedings of Electronic Voting 2014 (EVOTE2014). Tallinn: TUT Press,* 24-31.

Meagher, S. 2008. "When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights." *American University International Law Review* 2008, 23.

Mendez, F. 2010. "Elections and the Internet: On the Difficulties of 'Upgrading' Elections in the Digital Era." *Representation* 46(4), 459-469.

Meri, L 2000. Speech at the University of St Olaf Minnesota, U.S., 6 April 2000. Available at https://vp1992-2001.president.ee/est/k6ned/K6ne.asp?ID=3675 (last accessed 31 May 2015).

Mitrou, L, D. Gritzalis, S. Katsikas and G. Quirchmayr. 2003. "Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications." In D.A. Gritzalis (ed.). *Secure Electronic Voting*. Boston + Dordrecht: Kluwer Academic Publishers, 43-60.

Mohammadpourfard, M., M. Doostari, M. Bagher Ghaznavi-Ghoushchi and H. Mikaili. 2014. "Design and Implementation of a Novel Secure Internet Voting Protocol Using Java Card 3 Technology." *International Journal of Business Information Systems* 17(4), 414-439.

Musiał-Karg, M. 2011. "The Theory and Practice of Online Voting. The Case of Estonia (selected issues)." *Athenaeum. Polish Political Science Studies* 29, 180-198.

NEC. 2015a. "Estonian Internet Voting: General Description." Available at http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf (last accessed 31 May 2015).

NEC. 2015b. "Internet Voting Procedural Documents on the Estonian National Electoral Committee Webpage." Available at http://www.vvk.ee/valijale/e-haaletamine/e-dokumendid/ (last accessed 31 May 2015).

Nestås, L.H. and K.J. Hole. 2012. "Building and Maintaining Trust in Internet Voting." *Computer* 45(5), 74-80.

NY Times. 2014. “Estonians Embrace Life in a Digital World.” Available at http://www.nytimes.com/2014/10/09/business/international/estonians-embrace-life-in-a-digital-world.html (last accessed 31 May 2015).

OSCE/ODIHR. 2007. *OSCE/ODIHR Election Assessment Mission Report. Estonia. Parliamentary Elections 4 March 2007*. Available at http://www.osce.org/odihr/elections/estonia/25925 (last accessed 31 May 2015).

OSCE/ODIHR. 2011. *OSCE/ODIHR Election Assessment Mission Report. Estonia. Parliamentary Elections 6 March 2011*. Available at http://www.osce.org/odihr/77557 (last accessed 31 May 2015).

OSCE/ODIHR. 2012a. *OSCE/ODIHR Election Expert Team Report. Norway. Internet Voting Pilot Project Local Government Elections 12 September 2011*. Available at http://www.osce.org/odihr/88577 (last accessed 31 May 2015).

OSCE/ODIHR. 2012b. *OSCE/ODIHR Election Assessment Mission Report. Swiss Confederation. Federal Assembly Elections 23 October 2011*. Available at http://www.osce.org/odihr/87417 (last accessed 31 May 2015).

OSCE/ODIHR. 2013a. *OSCE/ODIHR Handbook for the Observation of New Voting Technologies*. Available at http://www.osce.org/odihr/elections/104939 (last accessed 31 May 2015).

OSCE/ODIHR. 2013b. *OSCE/ODIHR Election Assessment Mission Report. Norway. Parliamentary Elections 9 September 2013*. Available at http://www.osce.org/odihr/elections/109517 (last accessed 31 May 2015).

OSCE/ODIHR. 2015. OSCE/ODIHR Final Report on Estonian Parliamentary Elections 1 March 2015. Available at http://www.osce.org/odihr/elections/estonia/160131 (last accessed 31 May 2015).

Peixoto, T. 2009. “Beyond Theory: e-Participatory budgeting and its promises for eParticipation.” *European Journal of ePractice, 7(5)*, 1-9.

Penal Code. 2001. Chapter 19 Division 2 in the Penal Code. Available at https://www.riigiteataja.ee/en/eli/519032015003/consolide (last accessed 31 May 2015).

Popoveniuc, S., J. Kelsey, A. Regenscheid and P. Vora. 2010. “Performance Requirements for End-to-End Verifiable Elections.” In D. Jones, J.-J. Quisquater and E. Rescorla (eds.). *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections.* Berkeley: USENIX Association, 1-16.

Prosser, A. and R. Krimmer. 2004. “The Dimensions of Electronic Voting: Technology, Law, Politics and Society.” In A. Prosser and R. Krimmer (eds.). *Proceedings of the Workshop* on *Electronic Voting in Europe*. Bonn: GI, 21-28.

Raudla, R. and J. Krenjova. 2013. “Participatory budgeting at the local level: Challenges and opportunities for new democracies.” *Administrative Culture, 14-1*, 18-46.

Reiners, M. 2013. “E-Revolution. Actor-Centered and Structural Interdependencies in the Realization of Estonia’s Democratic Revolution.” Available at http://dr-markus-reiners.de/cms/files/Texte/ZPol-eRevolution.pdf (last accessed 31 May 2015).

Rüß, O.R. 2000. “Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen.” *Multimedia und Recht* 3(2), 73-76.

Schreiber, W. and M. Kosienkowski. 2015. *Digital Eastern Europe*. Wroclaw: Kolegium Europy.

Schweizer Bundesrat. 2002. “Bericht über den Vote électronique. Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte.” In *Bundesblatt* 2002. Bern.

Schweizer Bundesrat. 2006. “Bericht über die Pilotprojekte zum Vote électronique.” In *Bundesblatt* 2006. Bern.

Schweizer Bundesrat. 2013. “Bericht des Bundesrates zu Vote électronique. Auswertung der Einführung von Vote électronique (2006–2012) und Grundlagen zur Weiterentwicklung.” In *Bundesblatt* 2013. Bern.

Serdült, U., M. Germann, F. Mendez, A. Portenier and C. Wellig. 2015. “Fifteen Years of Internet Voting in Switzerland [History, Governance and Use].” In L. Teran and A. Meier (eds.). *Proceedings of the Second International Conference on eDemocracy & eGovernment (ICEDEG), 2015*. Quito: IEEE, 126-132.

Solop, F. 2004. “Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election.” In Norbert Kersting and Harald Baldersheim (eds). *Electronic Voting and Democracy: A Comparative Analysis*. London: Palgrave Macmillan, 242-254.

Springall, D., T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J.A. Halderman. 2014. “Security Analysis of the Estonian Internet Voting System.” In G.-J. Ahn (ed.). *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York: ACM, 703-715.

Spycher, O., M. Volkamer and R. Koenig. 2012. “Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting.” In A. Kiayias and H. Lipmaa (eds). *E-Voting and Identity: Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*. Berlin/Heidelberg: Springer, 19-35.

Statista. 2015a. “More of the Same from Amazon.” Available at http://www.statista.com/chart/1299/amazons-revenue-and-profit-growth/ (last accessed 31 May 2015).

Statista. 2015b. “Online Banking Penetration in Selected European Markets in 2014.” Available at http://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/ (last accessed 31 May 2015).

Stein, R. and G. Wenda. 2014. “The Council of Europe and E-Voting: History and Impact of Rec(2004)11.” In R. Krimmer and M. Volkamer (eds.). *Proceedings of Electronic Voting 2014 (EVOTE2014)*. Tallinn: TUT Press, 1-6.

Stenerud, I. and C. Bull. 2012. “When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting.” In M. Kripp, M. Volkamer, R. Grimm (eds.). *Proceedings of the 5th International Conference on Electronic Voting (EVOTE2012)*. Bonn: GI, 21-33.

Supreme Court. 2005. “Judgment Number 3-4-1-13-05 of the Constitutional Review Chamber of the Supreme Court.” Available at http://www.nc.ee/?id=381 (last accessed 31 May 2015).

Trechsel, A. 2007. *Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe*. Available at http://www.vvk.ee/public/dok/CoE_and_NEC_Report_E-Voting_2007.pdf (last accessed 31 May 2015).

Trechsel, A. and K. Vassil. 2011. “Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005. Council of Europe and European University Institute, 2011.” Available at http://www.vvk.ee/public/dok/ Internet_Voting_Report_20052011_Final.pdf (last accessed 31 May 2015).

Vassil, K. 2014. “Does Internet Voting Bias Election Results?” A Working Paper, accessible at http://kodu.ut.ee/~wass/wp-content/uploads/Bias_report.pdf (last accessed 31 May 2015).

Vassil, K. and M. Solvak. 2015. “Ten Years of Internet Voting in Estonia: Overview of research on Internet Voting in 2005-2014.” Seminar on 22 January 2015. Seminar material published at http://www.vvk.ee/public/dok/Event_2015_print.pdf (last accessed 31 May 2015).

Vassil, K., M. Solvak and P. Vinkel. 2014. “E-valimiste levik Eesti valijate hulgas.” *Riigikogu Toimetised* [Parliamentary Journal] 30, 116-128. Available at http://www.riigikogu.ee/rito/index.php?id=16791 (last accessed 31 May 2015).

Vassil, K. and T. Weber. 2011. “A Bottleneck Model of E-Voting: Why Technology Fails to Boost Turnout.” *New Media & Society* 13(8), 1336-1354.

Venice Commission. 2010. Report CDL-AD on Constitutional Amendment adopted by the Venice Commission at its 81st Plenary Session (Venice, 11-12 December 2009). Available at http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2010)001-e (last accessed 31 May 2015).

Volkamer, M., O. Spycher and E. Dubuis. 2011. "Measures to Establish Trust in Internet Voting." In E. Estevez and M. Janssen (eds). *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV '11)*. New York: ACM, 1-10.

WE Forum. 2015. "Global IT Report 2015, Sections 10.1 and 10.3." In S. Dutta, T. Geiger and B. Lanvin (eds.). *World Economic Forum Global IT Report 2015*. Geneva: World Economic Forum. Available at http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf (last accessed 31 May 2015).

KOKKUVÕTE

Elektrooniline hääletamine Eestis: õiguspärasus, mõju ja usaldus

Valimistel legitimeerib kõrgeima võimu kandja – rahvas – seadusandliku võimu. Valimiste aususe kindlustamiseks vajalikud üldised põhimõtted on demokraatlike riikide vahel kokku lepitud: valimised peavad olema üldised, vabad ja ühetaolised, hääletamine peab olema salajane. Demokraatlikud protsessid, sh valimised, on oma detailides riigiti eripärased, kuivõrd nad on võrsunud riigi ajaloolisest ja kultuurilisest taustsüsteemist. Nõnda sisustatakse ka loetletud põhimõtteid riigiti erinevalt: on riike, kus valimistel osalemine on kohustuslik, teised loevad mitteosalemisõigust valimisvabaduse osaks; ette võib olla nähtud väga pikk eelhääletamise aeg või hääleõiguse volitamine; lubatud võib olla kontrollimata keskkonnas täidetud hääletamissedeli saatmine tavaposti teel. Mõned riigid, sh Eesti, lubavad Interneti teel elektroonilist hääletamist. Mainitud erinevused on lubatavad seni, kuni mahuvad demokraatlikes riikides üldtunnustatud valimisprintsiipide raamidesse. Ühelt poolt muutuvad valimisõiguslike inimeste käitumis- ja liikumismustrid, teiselt poolt lisandub tehnilisi võimalusi ka valimiskorralduses inimkäitumise muutumisega arvestamiseks. Muutuste kavandamisel tuleb hoolikalt ja pigem konservatiivselt kaaluda muudatuste eesmärkide tähtsust ja uuendustega võetavaid riske ning meeles pidada, et valimiste aususe kahtluse alla sattumine murendab ühiskonnas kehtivaid aluskokkuleppeid.

Käesolev teadusartiklitest ja nende ülevaateartiklist koosnev väitekiri käsitleb Eesti kogemust elektroonilise hääletamisviisi juurutamisel alates 2005. a kohaliku omavalitsuse volikogu valimistest 2015. aasta Riigikogu valimisteni, otsides vastust küsimusele, kuidas Eesti on saavutanud Interneti teel kontrollimata keskkonnast elektroonilise hääletamise ausa hääletamisviisina tunnustamise valdavas osas ühiskonnast.

Sellele küsimusele põhistatud vastuse andmiseks on uuritud kolme küsimusteringi:
1. Milliste võtetega on tagatud ja kuidas argumenteeritud Eestis kasutatava e-hääletamise süsteemi ja selle kasutuspraktikate põhiseaduspärasust, sh kooskõla üldiste valimisprintsiipidega?
2. Millised on olnud Eestis kasutatava e-hääletamise süsteemi arenguetapid ning milline on olnud süsteemi mõju Eesti ühiskonnas?
3. Kuidas on Eestis tagatud e-hääletamise süsteemi usaldusväärsust?

Väitekiri tugineb neljale töö põhiosas esitatud artiklile ning neljale töö lisasse kantud artiklile. Esimesele alaküsimusele pakuvad vastuse artiklid **II** ja **III**, analüüsides Eestis kasutatava e-hääletamise kontseptsiooni põhiseadusõiguslikku mõõdet. Eesti e-hääletamise süsteemi arengut ning empiirilist kogemust vaadeldakse artiklites **I**, **IV**, **V**, **VII** ja **VIII**. Usaldusväärsuse tagamise meetmeid analüüsitakse aga artiklites **I**, **V** ja **VI**.

Käesoleva väitekirja autoril on pikaajaline kogemus valimiste korraldamisel. Töökogemus Vabariigi Valimiskomisjoni sekretariaadis on kümne aasta pikkune, sellest

viimased kaks juhi rollis. Autor on saanud vahetult jälgida e-hääletamisega seotud teemade arutelu Riigikogus ja Vabariigi Valimiskomisjonis ning tunneb üksikasjalikult senist rakendus- ja kohtupraktikat. Lisaks on autor osa võtnud ja tutvustanud Eesti kogemust arvukatel elektroonilise hääletamise teemalistel konverentsidel ning osalenud OSCE/ODIHR (Euroopa Koostöö- ja Julgeolekuorganisatsiooni valimiste teemaga tegelev organ) ja Euroopa Nõukogu rahvusvaheliste juhiste ja soovituste väljatöötamisel.

Väitekiri püüab siduda kaasaegse, teiste samateemaliste uurimustega sidestatud elektroonilise hääletamise teemalise teoreetilise käsitluse empiiriliste uuringutega Eesti näitel, tuues piiratud ulatuses paralleele Norra ja Šveitsiga.

Eesti elektroonilise hääletamise arutelu algas Riigikogus 2002. aastal ja oma põhiseaduslikkuse mõõtmes kulmineerus põhiseaduslikkuse järelevalve menetlusega vahetult enne esmarakendamist 2005. aasta linna- ja vallavolikogude valimistel. Riigikohtu 2005. aasta otsuses kinnitati elektroonilise hääletamise sõlmküsimuste põhiseaduspärast lahendamist ja tollased seisukohad on õigusteaduslikus argumentatsioonis senini domineerivad. Kohus andis vastuse küsimusele, kas hääletamise salajasus on eesmärk iseeneses või ennekõike vahend valimisvabaduse tagamiseks, ja kas vajadus tagada valija õigus hääletada vabalt, anonüümselt ning privaatselt, kaalub üles e-hääletaja õiguse eelhääletamise vältel elektrooniline hääl teise e-hääle või pabersedelil häälega muuta. Elektrooniliselt antud hääle muutmise instituut on kohtu hinnangul oluline valimiste vabaduse tagamiseks ning seetõttu vajalik valimiste aususe garanteerimiseks. Täiendavat või uut juriidilist debatti põhiseaduslikku järku väärtuste üle pärast 2005. aastat peetud ei ole. Küll on teistsuguseid vaatenurki esitatud poliitilise võitluse käigus ja sotsiaalteaduslikes ning infotehnoloogiaalastes vaidlustes.

Elektroonilise hääletamise praktika kontrollimiseks on võimalik ja on ka kasutatud Eestis valimiskaebuste lahendamise süsteemi. Tegemist on olemuselt haldusasjade lahendamisega kiirkorras põhiseaduslikkuse järelevalve kohtus. Kümne aasta jooksul, mil elektroonilist hääletamist on Eestis korraldatud, on seda tüüpi kaebused käsitlenud küsimusi nii ühetaolisusest, salajasusest, tehnilisest turvalisusest kui ka protseduurilisest kindlusest üksiknäidete varal. Kõik elektroonilise hääletamise teemalised valimiskaebused on seni jäänud rikkumiste mittetuvastamise tõttu rahuldamata või kohtu pädevusse mittekuulumise tõttu läbi vaatamata.

Õiguspärasust ja põhiseaduslikkust saabki hinnata kahel tasandil: abstraktselt, normide põhiseaduslikkuse kontrolli teel, ning konkreetselt, üksikjuhtude kaebuste lahendamise kontekstis. Esimesel tasandil saab järeldada, et on saavutatud tasakaal tehnoloogiliste ja protseduuriliste lahenduste vahel, tagamaks Põhiseaduses kehtestatud valimispõhimõtete kaitse ja järgimine. Teisel tasandil ei ole seni põhistatult seaduserikkumisele viitavaid kaasusi olnud, ent selgeks on saanud vajadus korraldada elektroonilise hääletamise protsess selliselt, et süsteemi korrakohast toimimist on võimalik usaldusväärselt tõendada ka kohtumenetluses. See tähendab valimishalduse pideva täiustamise vajadust, uute protseduuride loomist, nende korrektset dokumenteerimist jpm. Nii kohtuliku kontrolli kui üldise ühiskondliku usaldatavuse seisukohalt on oluline pidev auditeerimise, testide ja kontrollitavuse arendamine.

Teisele uurimisküsimusele vastamisel saab Eesti elektroonilise hääletamise rakendamise ajaloo jaotada kolme faasi. Esimeses faasis toimus üldpoliitiline ja põhiseaduslik debatt ning ettevalmistus uudse hääletamisviisi esmakordseks rakendamiseks. Teises faasis toimusid viis hääletamist, kus toimus järkjärguline e-hääletajate arvu tõus ning osakaalu kasv kõigi hääletajate hulgast. Antud faasi lõpuaastatel, kui saavutati kriitiline neljandik e-hääletajaid valijaskonna koguhulgast, algas teine põhjalikum õiguslik debatt läbipaistvuse ja kontrollitavuse suurendamiseks e-hääletamise süsteemis. Valimiste vaheaastatel peetud debatt päädis e-hääletamise põhjalikuma sätestamisega valimisseadustes, protseduuriliste normide laiendamise ning valijatele pakutava kontrollimisvõimaluse rakendamisega 2013. a valimistest. Kolmandas faasis näeme valija poolt kasutatava kontrollitavuse meetme rakendamist valimistel, mõõdukat valijate arvu kasvu ning e-hääletajate osakaalu tõusmist ligi kolmandikuni koguhääletajatest. Oluline on rõhutada ka hääletamise struktuurseid muutusi eelhääletamise perioodil, kus e-hääletajad moodustavad juba üle poole kõikides sel ajavahemikul hääletanud valijatest. Kolmanda faasi lõpul alanud valimiste vaheline aeg juhatab aga järjekordselt sisse debati täiendava läbipaistvuse ja kontrollitavuse rakendamiseks, juhtides tähelepanu valimiste vahelise vaheaja olulisele seosele diskussioonide pidamise võimalustega.

Mõjude osas valimistele ja ühiskondlikele protsessidele, saab kokkuvõtvalt järeldada, et elektroonilise hääletamise kasvatav mõju üldisele valimistest osavõtule on olnud pigem tagasihoidlik, omades olulist rolli eelkõike väljaspool Eestit hääletamisel ning valijate seas, kellel võib olla raskusi valimisjaoskonda pääsemisega. Teaduslike analüüside kohaselt on pärast 2009. aastat toimunud protsess, mille tulemusena ei ole võimalik ühiskondlike tunnuste abil elektroonilist hääletajat eristada. Puuduvad seosed nii vanuse, soo, elukoha, arvutioskuse kui poliitilise eelistuse jms osas. Ainuke väärtus, mis selgelt läbi aastate määratleb hääletaja valikut e-hääletamise kasuks otsustamisel, on usaldus kasutatava e-hääletamise süsteemi vastu.

Võrdlusel kahe Interneti teel hääletamist rakendanud riigi – Šveitsi ja Norraga – selgub, et süsteemid on erinevad isikutuvastamise, verifitseerimise ja elektroonilise hääle asendamise (nn virtuaalse valimiskabiini) osas. Eestis ei oleks näiteks posti teel valija tuvastamiseks vajalike koodide saatmine mõeldav. E-hääletamise süsteemide rakendamisel on tähtis järgida igas konkreetses riigis aktsepteeritavaid ja usaldusväärseid reegleid, millega selle riigi ajalugu ja demokraatlik kultuur kokku sobib.

Nagu eelnevalt sedastatud, usaldus e-hääletamise süsteemi ja veendumus, et valimiskorralduslik organisatsioon seda korrektselt ja õiguspäraselt rakendab, on üks kõige olulisemaid faktoreid, mille alusel valijad e-hääletamise kasuks või kahjuks otsustavad. Seetõttu on väitekirjas käsitletud autori poolt Eesti e-hääletamise süsteemi näitel arendatud kolmesambalist meetmete mudelit.

Esimese samba moodustab valijate veendumus, et üldine e-valitsemise korraldus ja uute e-lahenduste juurutamine on tagatud korrektselt ja õiguspäraselt. Teise samba moodustab valijate usaldus elektroonilist identiteeti tagavate vahendite vastu, Eesti näitel usaldus ID-kaardi ja mobiil-ID elektrooniliste funktsioonide vastu. Kolmas sammas on kõige mahukam ning hõlmab endas valija usaldust valimisi läbiviiva

organisatsiooni ja valimistel kasutatava e-hääletamise süsteemi vastu. Konkreetsemalt on tegemist meetmetega, mis hõlmavad tehnilisi aspekte, valija kogemusest tulenevaid asjaolusid ning vaatlejate rollist tulenevaid küsimusi. Kokkuvõtvalt moodustavad usalduse tagamise meetmed kontseptsioonilise Usalduse Maja, kus kõik kolm sammast on tervikliku usalduse tagamiseks olulise tähtsusega. Keeruliseks teeb avalikkuse usalduse võitmise ja säilitamise see, et ka veatu organisatsiooni ja tehnilise korrektsuse korral pole võimalik välistada alusetuid, ent edukaid rünnakuid usaldatavuse vastu. Seega tuleb vaeva näha ka selle nimel, et e-hääletamine mitte üksnes ei oleks, vaid ka paistaks aus.

Eesti ja ka teised riigid on näidanud, et Interneti teel elektroonilise hääletamise juurutamine on võimalik, arvestades seejuures iga riigi poliitilisi ja kultuurilisi eripärasid. Rakendada tuleb põhjalikku mitmekülgset analüüsi ning arvestada igale riigile omase kontekstiga, ainult nii on võimalik saavutada erinevaid aspekte arvestav tasakaalustatud lahendus.

ACKNOWLEDGEMENTS

I am lucky to be part of a complete scientific family, to have a *Doktormutter*, Professor Dr Ülle Madise, and a *Doktorvater*, Professor Dr Robert Krimmer.

Ülle has been my closest ally and colleague throughout my scientific endeavors, has believed in me in good and not so good times and has simply been a great friend. Her vision and relentless support have always been very inspiring and helped me tremendously in my journey. Thank you!

Robert has been an excellent colleague and visionary in the academic and practical fields. His wide-ranging understanding of the topic, punctuality and great academic sense have been irreplaceable in finalizing this dissertation. Thank you!

I would like to give my special appreciation to the Ragnar Nurkse School for an inspiring and supportive academic environment for my PhD studies. My thanks go to Professor Dr Rainer Kattel, Professor Dr Wolfgang Drechsler, Professor Dr Ringa Raudla, Dr Illimar Ploom and all the faculty and fellow students for meaningful years of study. Special thanks go to Piret Kähr and all her colleagues for creating a support network throughout the studies that actually works. Thank you!

Additionally, my thanks go to Dr Kristjan Vassil and Dr Mihkel Solvak from the University of Tartu, whose passion and energy in the research of Internet Voting has been remarkable and inspiring. Moreover, I would like to thank my BA thesis advisor, Professor *emeritus* Dr Rein Taagepera, who introduced me to the world of elections and electoral systems and encouraged me to study it further, which gave a push to my academic and professional journey more than ten years ago. Thank you!

Particularly kind thanks for their support and encouragement belong to my dear colleagues at the Estonian electoral organization "kitchen" – Tarvi Martens, Epp Maaten, Mihkel Pilving, Arne Koitmäe, Leino Mandre and Helena Stepanov. Distinctive appreciation has to be given to my supervisors throughout the years – Dr Alo Heinsalu, Aaro Mõttus and Heiki Sibul – who have encouraged me to see further and beyond and have supported me in every instance in achieving my academic goals. Thank you!

Finally, yet importantly, I would like to thank my family and friends. My wonderful wife Kadri and my children Joosep Oliver and Johanna Matilda have always believed in me, supported me and have had my back throughout any difficult times. Thank you!

ORIGINAL PUBLICATIONS

I Priit Vinkel. 2012. "Internet Voting in Estonia." In P. Laud (ed.). *Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011, Tallinn, Estonia, 26-28 October 2011, Revised Selected Papers.* Berlin: Springer, 4-12. (1.1)

Internet Voting in Estonia

Priit Vinkel

Estonian National Electoral Committee,
Lossi plats 1a,
Tallinn, Estonia
priit.vinkel@vvk.ee

Abstract. Estonia was the first country in the world to introduce Internet Voting pan-nationally in binding elections in 2005. Although Internet Voting is only one of many ways of voting in Estonia, the number of voters has grown exponentially. The short paper explores the topic of Internet Voting based on the six-year experience of the pioneer country Estonia. The factors of success in the process include for example the relative small size of the country and the positive experiences with previous government e-services. The role of a secure online authentication token — ID-card — would also be crucial in implementing the idea of remote voting in an uncontrolled environment.

Voter's right to change the I-vote with another I-vote or with paper-ballot and the supremacy of the paper ballot serve as main strongholds against vote buying and other infringements of the principle of free elections.

Possible future developments and expansion of technical platforms will be addressed.

Keywords: Internet Voting, elections, e-government, e-services, remote authentication.

1 Introduction

Estonia is a parliamentary democracy, the 101 members of the unicameral parliament Riigikogu are elected under proportional electoral system, the governing coalition usually comprises of two or more political parties. Head of state is the President with mainly representative duties. Estonian reform-readiness might be explained with the state history (after Soviet occupation and being part of the Soviet Union, Estonia regained its independence in 1991 and had to rebuild an effective governance under rule of law, restore private property and market economy etc). Since 2004 Estonia is member of European Union and NATO[1].

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 risen more than 14 times. This short paper looks at the building blocks

[1] More about history, culture, society etc in an encyclopedia about Estonia: http://www.estonica.org/en/

P. Laud (Ed.): NordSec 2011, LNCS 7161, pp. 4–12, 2012.

of the Estonian Internet Voting system, addresses some emerged problems and future plans. 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 The Estonian Internet Voting System

2.1 Pillars of Success

Using Internet Voting for national elections is not a very widespread practice. Only Switzerland, Estonia and Norway allow legally binding remote Internet Voting [1]. Therefore, the understanding of the factors that help for implementing this concept is quite important. The current concept of Internet voting that has been used for voting in two general elections (2007 and 2011), in two local elections (2005 and 2009) and one European Parliament election (2009). The number of Internet Voters has grown sharply from less than 10,000 in 2005's local elections to over 140,000 in the 2011 general elections. The latter account for 24.3% of all votes cast and 56.4% of the advance votes [2]. And one red line has always followed through 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 according scientific surveys [3]. The three most important factors of keeping and building this trust could be summarized as put on figure 1.

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 2009-2010 [4], in the category of government success in

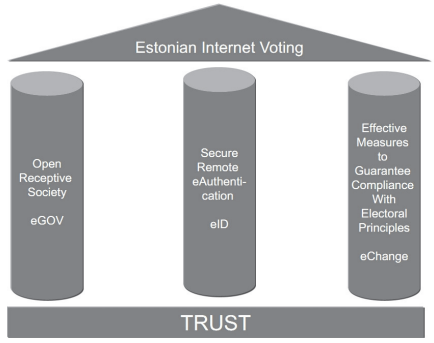


Fig. 1. Three pillars of Estonian Internet Voting

ICT promotion Estonia lies on 11th place forerunning such IT giants as US, Korea or Japan. In the field of providing quality online public services Estonia shares the positions 26–28 with Hungary and Ireland. In the category of presence of ICT in government agencies, the top three countries are Singapore, Sweden and Estonia. Since 1st June 2010 even the official publication of legal acts — The State Gazette — is entirely electronic, it means the legal acts are published only on the Internet[2].

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 eID[3]. Since 2002, ID card as 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 above 15 years old must have ID-card.

Each ID card contains two discrete 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 contain no restrictions of 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 eID 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 2/3 of cardholders have used the eID card for remote personal identification and over 1/3 for digital signature. Here has to be noted, that Internet voting has strongly promoted electronic use of ID card. Another important promoting factor has been the agreement between banks to allow 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); an 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

[2] The Estonian State Gazette. `https://www.riigiteataja.ee/tutvustus.html?m=1`

[3] More info about the Estonian ID-card can be found at `http://www.id.ee/?lang=en`

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 Identification 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 databases, internet banks etc and sign various contracts digitally.

Parliamentary debate over eID card raised several privacy and security questions, but the parties supporting compulsory eID commanded over majority of votes. The most controversial questions were possible risk of identity theft and the general 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.

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 one's vote alone in a voting booth. In the case of the Internet voting, the state is not in a 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 party without fearing condemnation or expecting moral approval or material reward [5].

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" (see Figure 2), used for absentee ballots by mail, is both reliable and easy to understand for the I-voters.

A double-envelope scheme known from the postal voting in some countries guarantees the secrecy of the vote. The voter's choice is encrypted by voting application (i.e. voter seals the choice into an inner blank envelope) and then signed 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 [6].

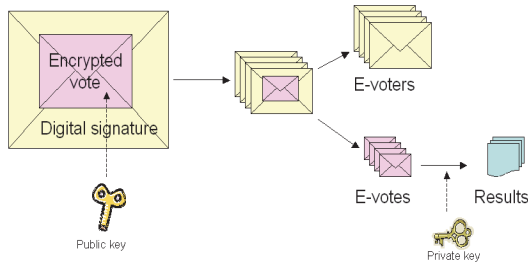


Fig. 2. Double envelope system used in Internet Voting

In order to guarantee the freedom of voting, I-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. If several paper-ballots are cast, all votes are declared invalid. Thus, the "one vote — one voter" principle is ostensibly guaranteed.

In case of the Internet-based voting, the possibility to change a vote is not just permissible; it is a constitutional obligation. According to the opinion of the Supreme Court of Estonia [7], 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.

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 Storage Server and the Vote Counting Application. The Voter Application is a stand-alone application in voters' personal computers to cast and encrypt votes.

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 Storage Server and transposes the acknowledgements of receipt from the Votes Storage Server to the voters. The network server completes the work when the I-voting period finishes. The Vote Storage Server receives encrypted ballots from the network server and stores them until the end of voting period. The Votes Storage Server has also a responsibility of votes' managing and cancelling. The Vote Counting Application is an offline app which summarizes all encrypted ballots. The encrypted ballots are transferred from Vote Storage Server to Vote Counting App by using offline data carriers.

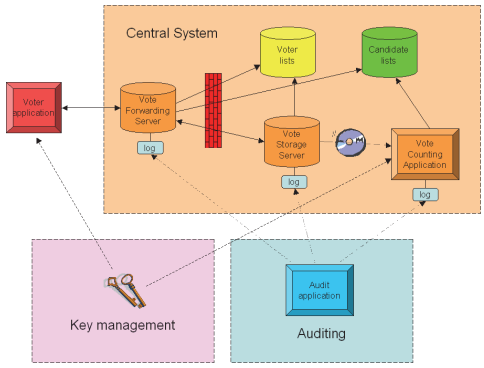


Fig. 3. The general architecture of the Internet Voting system

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 App 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 [8].

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. As a matter of fact e-enabled elections from 2005 to 2009 have had quite little publicly exposed concerns regarding security issues tied explicitly to one way of voting — over the Internet. The usual topics: why I-voting, compliance with principles of free and fair voting, the possible impact on the election results etc were discussed in the parliament and in scientific circles, less in the media. The National Electoral Committee had no complaints presented and the overall notion had been fairly positive. However, after 2011 general elections, discussions about the possible the infringement of principles of security flared up again. 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* [9].

Verification of the I-vote. Norway entered the circle of countries providing e-enabled elections in September 2011 by introducing Internet Voting in local elections. In addition, a possibility to verify the I-vote by using SMS and paper polling cards was offered for the voters[4]. Lifted by this example the discussions of offering this possibility in Estonia have emerged as well. To date, the Estonian system has not foreseen a separate possibility to verify the I-vote. Only 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 lever verification (stating the receiving of the vote). Nevertheless, the discussions currently held in the parliament have yet to come to a conclusion, but most probably the 2013 local e-enabled elections will have some additional level of verification used.

Uniformity of elections. This issue has been imminent from the very beginning of the concept. The Estonian I-Voting system has 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 I-vote is not about changing the ticket but rather voting again in order to be free. Therefore, constitutionally, I-voting even has to be conducted in a non-uniform manner [10].

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. The soft laws include things like prohibiting I-voting parties or encouraging voters to change their vote for other reasons than guaranteeing the secrecy of the vote[5]. However, there were some parties that did not agree with these soft provisions and started a discussion of integrating the agreement further into hard law. To date the discussion is still in process.

3.2 Future of I-Voting — Where to?

Finally, some points considering future development in the field of Internet Voting in Estonia.

To replace paper voting. As stated before, Internet Voting is only one of many possibilities of voting in Estonia and at the moment it can be said that it shall be so also in the nearer future. The purpose of e-enabled voting has always been supplementary. It offers new possibilities but does not take away existing ones. Although the eID rollout has been completed, only roughly a half of the population has ever used the ID-card electronically. So, I-voting will most probably stay a successful e-government service meant to keep existing voters and offer a

[4] Norwegian Internet Voting Project `http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658`

[5] Good Practice of Internet Voting: `http://www.ega.ee/files/Good%20Practice%20of%20E-voting%202009.pdf`

convenient voting method for possible new ones. It will not replace paper-ballot, at least in the near future, and if at all, it would probably replace postal-voting from abroad.

To have e-kiosks in polling stations. There might be questions of as having implemented one e-solution, why not a similar one. Most probably Estonia will not enable electronic voting in polling stations (in form of voting machines). We have a simple and fairly linear ballot, few questions and quite small electorate. All this indicates that Internet Voting will be sufficient for our needs. Moreover, as the concept of Internet Voting is not limiting the place and environment of voting, so offering Internet Voting in polling station grounds during advance voting might be possible.

To match the voting periods. At the moment Internet Voting is possible during advance voting for 7 days, traditional voting for 3 days. This discrepancy has been seen as an infringement of uniformity since adopting the provisions. The main problem is seen in the political environment the voter makes his or her decision. Moreover, the voting situation is already different during the long advance voting period compared to voting Sunday. Therefore, I-voting and traditional voting periods shall be equalized. The effects of shortening the I-voting period have been also discussed in the 2011 EUI report [3].

To move to smart phones. At the moment the Internet Voting Application is a stand-alone program designed for use in a computer environment (Windows, Mac and Linux platforms supported). Voting with a smart phone is not possible. Although there have been some ambitious ideas from some political parties of entering this uncharted territory, the most likely scenario will not include smart phones in Internet Voting. The relative lack of a strong cost benefit factor is underlined by the broad heterogeneity of smart phone platforms. For the foreseeable future Internet Voting will stay exclusively with computers.

4 Conclusions

Being a sparsely populated Northern state with few strong traditions when it regained independence in 1991, Estonia was and still is able to benefit from excellent opportunities for successful exploitation of new ideas. The unique chance to rebuild the state has offered wide opportunities to take contemporary, functional and logical decisions. Internet Voting is on the one hand an essential public e-service in the Estonian information society, on the other hand an innovation in electoral administration which impact deserves permanent attention and scientific research.

The Estonian Internet Voting system stands literarily speaking on three pillars. First, the Estonian eID — a secure and widely accepted way of remote e-identification. Second, e-services are widely accepted in the Estonian society. And third, we have managed to build the Internet Voting system as similar to the traditional voting logic as possible, incl. means to guarantee secure and anonymous voting (the virtual voting booth or possibility to change the I-vote)

and a virtual twin-envelope system. Internet Voting is not a separate concept but prominently seen as just another e-service for the citizen for communicating with the government (state), as part of the modern information society.

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

References

1. Competence Center for Electronic Voting and Participation. E-voting database, http://db.e-voting.cc/
2. Estonian National Electoral Committee. Internet Voting — Voting Methods in Estonia, http://www.vvk.ee/voting-methods-in-estonia/engindex/
3. Trechsel, A.H., Vassil, K.: Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005. Report for the Estonian National Electoral Committee, European University Institute (October 2011). http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf
4. Dutta, S., Mia, I.: The Global IT Technology Report 2009–2010: ICT for Sustainability. World Economic Forum (2010)
5. Drechsler, W., Madise, Ü.: Electronic Voting in Estonia. In: Kersting, N., Baldersheim, H. (eds.) Electronic Voting and Democracy. A Comparative Analysis, pp. 97–108. Palgrave Macmillan, Basingstoke (2004)
6. Estonian National Electoral Committee. E-Voting System: General Overview (2010), http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf
7. Constitutional Review Chamber of the Supreme Court of Estonia. Constitutional Judgement 3-4-1-13-05 (September 1, 2005), http://www.nc.ee/?id=381
8. Madise, Ü., Maaten, E., Vinkel, P.: Internet Voting at the Elections of Local Government Councils on October 2005. Report for the Estonian National Electoral Committee (2006), http://www.vvk.ee/public/dok/report2006.pdf
9. Heiberg, S., Laud, P., Willemson, J.: The Application of I-voting for Estonian Parliamentary Elections of 2011. In: Kiyaias, A., Lipmaa, H. (eds.) Postproceedings: 3rd International Conference on E-voting and Identity, Tallinn, September 29-30, 2011. LNCS. Springer, Heidelberg (forthcoming, 2012)
10. Madise, Ü., Vinkel, P.: Constitutionality of Remote Internet Voting: The Estonian Perspective. In: Juridica International. Iuridicum Foundation, vol. XVIII (forthcoming, 2011)

II Ülle Madise and **Priit Vinkel**. 2011. "Constitutionality of Remote Internet Voting: The Estonian Perspective." *Juridica International* 18, 4-16. (1.2)

Ülle Madise

Professor of Constitutional Law
University of Tartu

Priit Vinkel

Assistant, University of Tartu
Advisor, Elections Department
of the Chancellery of Riigikogu

Constitutionality of Remote Internet Voting:

The Estonian Perspective

1. Introduction

Estonia has used remote Internet-based voting in five elections: twice each in municipal and Riigikogu (parliamentary) elections and once in European Parliament elections. The number of 'I-voters' has grown sharply from less than 10,000 in 2005's municipal elections to over 140,000 in the 2011 parliamentary elections. The latter account for 24.3% of all votes cast and 56.4% of the advance votes. Initially, no individual complaints claiming unconstitutionality of I-voting were filed in court. In 2011, the situation has changed: critical public debate has re-emerged, followed by several complaints.

Only Estonia, Switzerland, Norway and a few other countries allow legally binding remote I-voting, though some countries are on their way toward its countrywide use. The list of countries that have abandoned the use of e-voting in various forms is much longer, including the US, Germany, Finland, and the Netherlands.[*1] France, for example, tries to keep alive the tradition of voting only at the polling station, as this ritualises citizenship[*2], but has allowed proxy voting and recently remote I-voting from abroad. The reasons for allowing or giving up on I-voting are different, but constitutional questions of whether fair and free voting can be secured in the case of remote I-voting have always been raised.

We are facing the pressure of the information society[*3]: people require e-services, yet, on the other hand, cyber-threats are more serious than ever before.[*4] Social changes have already forced countries to allow remote postal or proxy voting.[*5] We have to admit that holding on to old traditions (one single elec-

---

1 See the database for the Competence Center for Electronic Voting and Participation, at http://db.e-voting.cc/. German constitutional court decision to declare the use of voting machines unconstitutional: BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1-163). Available at http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html (9.10.2011). The core of the decision in German:

Der Grundsatz der Öffentlichkeit der Wahl aus Art. 38 in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen.

Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.

2 L. Monnoyer-Smith. How I-voting technology challenges traditional concepts of citizenship: An analysis of French voting rituals. – R. Krimmer (ed.). Electronic Voting 2006: 2nd International Workshop Co-organised by the Council of Europe, ESF TED, IFIP WG 8.6, and E-Voting.CC. Bonn: Gesellschaft für Informatik 2006, pp. 63–64.

3 W. Drechsler. Dispatch from the Future. – The Washington Post, 5.11.2006.

4 J. Farwell, R. Rohozinski. Stuxnet and the Future of Cyber War. – Survival 2011 (53) 1, pp. 23–40.

5 See, e.g., the thorough overview of remote postal voting in N. Kersting. Briefwahl im Internationalen Vergleich. – Österreichische Zeitschrift für Politikwissenschaft 2004 (33) 3, pp. 325–328.

tion day, casting of paper ballots in a controlled environment as the only option, etc.) will not be possible in the future, but free and fair elections, anonymity of the vote, and the principle of uniformity must be guaranteed. The Council of Europe has adopted recommendation[*6] and guidelines[*7] for electronically enabled elections, and the OSCE/ODIHR is looking for ways to observe and evaluate various forms of e-voting, including I-voting. Estonia's I-voting experience is internationally followed with special attention; any failures would have very negative consequences not only for Estonian democracy but for all I-voting projects, worldwide.

The concept of the Estonian I-voting system is described and analysed here in the light of theoretical literature, judgements of the Supreme Court of Estonia, and the empirical data available. In addition to statistics, the results of sociological surveys are used.

2. Description of the concept of Estonian I-voting

Estonia's I-voting system is based on an electronic roll of voters, a compulsory e-ID, the public/private key infrastructure ('virtual double-envelope scheme'), and the right to change a vote given online ('virtual voting booth'). The elements of the system are meant to guarantee the compliance of the I-voting with constitutional principles of elections: only people entitled to vote can vote, access to voting shall be equal, one vote per voter shall be counted, free voting shall be granted, and both counting of the voting results and election results shall be fair and sound. Brief description of the elements of the Estonian I-voting system is given in this section; the constitutional analysis follows in Section 3.

2.1. Electronic Population Register

The Estonian Population Register is a uniform database of personal data of Estonian citizens and foreigners with Estonian residence permits. The Estonian voter roll is held on the basis of the Population Register, and voters do not have to enrol specially before elections. The Estonian electoral law[*8] states that electoral rolls are drawn up 30 days before election day but additions to the list can be made until the very end of elections. This gives the list the property of being constantly up to date in practice. During Internet voting, the voting roll is updated daily.[*9]

2.2. ID card and m-ID

The cornerstone of most e-services, public as well as private, is the e-ID.[*10] Since 2002, an ID card has been 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. Every Estonian citizen or resident alien above age 15 must have an ID card.

Each ID card contains two discrete 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 have no restrictions of use: they are by nature universal and meant to be used in any form of communication, whether between private persons or organisations or within the government. The e-ID card can be used also for encryption of documents so that only the person intended to view the document can decrypt it. This is an efficient means for

6 Recommendation on legal, operational, and technical standards for e-voting, Rec(2004)11; Recommendation on electronic democracy, Rec(2009)1. Available on the Council of Europe Web site.

7 Certification of E-voting Systems, GGIS(2010)3E; Guidelines on transparency of e-enabled elections, GGIS(2010)5E. Available on the Council of Europe Web site.

8 Up-to-date translations of election laws are available on the National Electoral Committee Web site: http://www.vvk.ee/?lang=en (9.10.2011).

9 For more information, visit the Web site of the Ministry of Internal Affairs, specifically http://www.siseministeerium.ee/35796/ (9.10.2011).

10 Detailed information about e-IDs, the areas of their use, etc. can be found at http://www.id.ee/?lang=en (9.10.2011).

secure transfer of documents over public networks. In addition, each ID card has all data printed on it also in electronic form, in a special publicly readable data file.

The number of ID cards issued grew in June 2010 to exceed 1.1 million. Over 2/3 of cardholders have used the e-ID card for remote personal identification and more than 1/3 for digital signature. Here it has to be noted that Internet voting has strongly promoted electronic use of ID cards. Another important promoting factor has been the agreement among banks to allow Internet banking only with an ID card or PIN calculator. The old password cards can be used only for very small transactions.

To use the ID card, one needs a smartcard reader and a computer with the relevant software installed (free for download from the Web page https://installer.id.ee/); an Internet connection; and a Windows, Mac, or Linux operating system.

A couple of years ago, a new e-ID solution was brought to the market: the m-ID, where a mobile telephone (via its SIM card) acts as an ID card and a card reader at the same time. In addition to having the functionality of an ordinary SIM, a mobile-ID SIM holds a person's mobile identity that enables providers of Internet services to identify the person and to issue digital signatures.[*11] Personal identification and digital signature functionality are secured by up-to-date security technology and corresponding personal identification numbers. Making the solution more convenient, with this, one does not need an ID card reader for the computer any longer; instead, one can perform electronic transactions just as one would with an ID card: it enables logging in to databases, Internet banks, etc. and signing various types of contracts digitally. The m-ID certificate is issued by the state and is thereby an equally e-enabled document to the ID card. The m-ID can be used as a means of authentication and digital signature in elections from 2011.

In practice, an e-ID is used for user authentication with several databases[*12]; the above-mentioned state portal serving as an e-service centre, e-tickets for public transportation, a customer loyalty programme identification tool in several private companies, and even insertion of comments for the online daily newspaper *Eesti Päevaleht*, which has prohibited anonymous comments in order to prevent libel cases. The use of e-ID is steadily widening, although the initial aim of combining e-ID with all possible other documents, such as driving licences, and replacing all possible password-based solutions has not been fulfilled yet.[*13]

2.3. System architecture

The Estonian IT security experts in their security analysis[*14] published in 2003 and revised in 2010 declared that in a **practical sense** the Estonian I-voting system was secure enough for implementation. In absolutely secure systems, unexpected events are not possible. One may dream about such systems, but they can never be realised in practice. This applies particularly to I-voting systems. Considering the security level of personal computers, it is impossible to design I-voting systems that are absolutely secure for every user. The most important security goal of voting is not to affect the final results and not to abuse the constitutional principles. Single incidents with users are still important, but they do not have an influence on the final result. Moreover, small-scale incidents are acceptable even in traditional voting systems.[*15]

The part of I-voting in the whole process of organising elections is relatively small. The system uses existing information systems—the Population Register for the polling list, election information system of the National Electoral Committee (hereinafter referred to as the NEC) for the collection and publication of information on candidates and voting results, and the infrastructure of Certification Centre Ltd. for checking ID card (or m-ID) certificates.

The main components of the Estonian I-voting systems are the voter application; the Vote Forwarding Server; and the back office, which is divided in two: the Vote Storage Server and the Vote Counting Application. These components support the following processes:

---

11 More about the m-ID project can be found at http://id.ee/?id=10995.

12 For example, the Estonian Research Portal, at https://www.etis.ee/index.aspx?lang=en, which compiles information on all Estonian researchers and their scientific projects, publications, and activities.

13 Comprehensive coverage of the ID card can be found in the work of T. Martens and E. Maaten. E-voting is here to stay. – Baltic IT&T Review 2006 (1).

14 Available from the NEC Web site at http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf.

15 T. Mägi. Practical Security Analysis of I-voting Systems. Master's Thesis 2007. Available at http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf.

- The voter application is a Web-based application or an application on voters' personal computers.
- The Vote Forwarding Server is responsible for authentication, checking of enfranchisement, sending a list of candidates to voters, and receiving signed and encrypted ballots.
- The network server immediately transfers the received encrypted ballots on the Vote Storage Server and transfers the acknowledgements of receipt from the Vote Storage Server to the voters. The network server completes the work when the I-voting period finishes.
- The Vote Storage Server receives encrypted ballots from the network server and stores them until the end of the voting period. The Vote Storage Server is responsible for cancellation and management of votes.
- The Vote Counting Application is an off-line program that summarises all encrypted ballots. The encrypted ballots are transferred from the Vote Storage Server to the Vote Counting Application via data carriers. The Vote Counting Application does not receive voters' digital signatures, and it does not know voters' personal data.

Additionally, the I-voting system delivers independent log files, which consist of tracing data for the received encrypted ballots from the Vote Forwarding Server, all annulled encrypted ballots, all encrypted ballots sent to the Vote Counting Application, and all counted encrypted ballots. The cryptographic protocol used links all records in the log files. The NEC has the right to use the log files to resolve disputes. Hence, there is an independent audit trail to verify the e-voting process and help solve problems should they appear.[*16] The legality of all elections depends on the presence and proper functioning of these components.

2.4. Measures used to ensure voting secrecy

In order to understand how the I-voting system guarantees secret and equal voting, we should briefly describe the envelope voting method used in Estonia for advance paper voting. The latter gives the voter the possibility to vote outside the polling station for the voter's residence in any rural municipality or city. A voter presents a document for entry in the list of voters and then receives the ballot and two envelopes. The inner envelope has no information about the identity of the voter, and the ballot paper is put in it. The inner envelope is placed in an outer envelope, on which the voter's details are written, so that, after the end of the advance poll, the envelope can be delivered to the voter's polling station of residence. There it is verified whether the voter has the right to vote; then, the inner envelope is taken out and placed unopened into the ballot box. The two-envelope system guarantees that the voter's choice remains secret. The same system but electronically built is used in Internet voting.[*17]

Asymmetric cryptography is used to guarantee the secrecy of votes. A pair of keys is generated for the system in a special safety module so that its private component never leaves this environment. The public component of the pair of keys is integrated into the voter application and is used to encrypt the votes. The private component of the pair of keys is used in the vote-counting application to open the votes on the evening of election day. The NEC can open the votes—i.e., use the private component—only collegially. After the period for dealing with any complaints has elapsed, the private key is destroyed.

2.5. 'Virtual voting booth'

In order to guarantee the freedom of voting, I-voters have the right to replace the vote cast on the Internet by means of another I-vote or a paper ballot. However, this can be done only on advance polling days. In the case of several I-votes being cast, only the last one is counted; in the event of contradiction between an I-vote and paper ballot, the paper ballot is deemed definitive. If multiple physical ballots are cast, all votes are declared invalid.[*18] Thus the 'one voter—one vote' principle is guaranteed.

16 General description of the Estonian Internet voting system, 2010. Available at http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf (9.10.2011).

17 Details of the double-envelope scheme and description can be found in the General Overview document (Note 16).

18 Riigikogu Election Act (Riigikogu valimise seadus), §40 (6). – RT I 2002, 57, 355; RT I, 10.12.2010, 1 (in Estonian).

3. Analysis of the constitutionality of Internet voting

According to the Estonian Constitution[*19], members of the Riigikogu, as well as local government councils and the European Parliament shall be elected in free, general, equal, and direct elections, and voting shall be secret. There is no special regulation of I-voting in the Constitution. The legal framework for I-voting is laid down in electoral law. The provisions are almost the same in all legal acts regulating voting procedures. In the case of I-voting, almost all principles of democratic elections give rise to several questions in constitutional law and, more broadly, in social sciences.

3.1. A teleological interpretation of the principle of secrecy

The secrecy of voting has traditionally been viewed in Estonia as the right and obligation to cast one's vote alone in a voting booth. In the case of Internet voting, it is impossible to ensure the privacy aspect of the voting procedure. The voter's right to anonymity during the counting of the votes **can** be guaranteed, indeed to the extent to which this can be secured in the case of remote postal voting. Therefore, remote Internet voting requires rethinking of the privacy principle.

The principle of privacy is there to protect a person from any pressure or influence acting counter to his or her free expression of political preference. Such a teleological approach to the Constitution was the basis of the I-voting provisions from the very beginning of the whole project. In short, the provisions enabling Internet voting are based on the premise that the government has to trust the individual and avoid, whenever possible, interference with decision-making at the individual level.[*20] The individual has to be aware of the risks—e.g., technical risks—and he or she has to have the right to decide whether or not to exercise the Internet voting opportunity. The Supreme Court has agreed with this teleological approach to the principle of secrecy.[*21]

Buchstein, on the other hand, does not agree:

> Mandatory secrecy is a principle which goes beyond constitutional law, its fundaments are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption. In this concept, it is not the individual him- or herself, but a warranted outside agent or authority—normally the state—that is responsible for providing the necessary means to allow for the secret ballot.[*22]

Indeed, postal voting as another form of absentee ballot is widespread and is becoming accepted in Germany. There, the Federal Constitutional Court has twice declared remote postal voting to be constitutional, arguing that facilitation of voter turnout outweighs, in this case, the problems possible in relation to security and public scrutiny of electoral processes.[*23] In France, by contrast, postal voting was abolished in 1975 because of incidents of fraud.[*24]

19 Translations of Estonian legal acts can be found at http://www.just.ee/6906. Up-to-date official versions of all legal acts are available from the State Gazette, at http://www.riigiteataja.ee/ (in Estonian).

20 The ideological foundation and parliamentary debates are explored by W. Drechsler, Ü. Madise. E-voting in Estonia. – Trames 2002 (6) 3, pp. 234–244; W. Drechsler, Ü. Madise. Electronic Voting in Estonia. – N. Kersting, H. Baldersheim (eds.). Electronic Voting and Democracy: A Comparative Analysis. Basingstoke: Palgrave Macmillan 2004, pp. 97–108.

21 Available at http://www.nc.ee/?id=381 (9.10.2011).

22 H. Buchstein. Online Democracy. Is It Viable? Is It Desirable? Internet Voting and Normative Democratic Theory. – N. Kersting, H. Baldersheim (eds.). Electronic Voting and Democracy: A Comparative Analysis, Basingstoke: Palgrave Macmillan, pp. 39–58.

23 BVerfGE 21, 200 (15.02.1967); BVerfGE 59, 119 (24.11.1981). Available at http://www.wahlrecht.de/wahlpruefung/index.htm (9.10.2011).

24 L. Monnoyer-Smith (Note 2), p. 63.

3.2. Increase of turnout

One of the declared aims of launching online voting in Estonia was to increase voter turnout, which perhaps could be described more realistically as broadening access possibilities and stopping the decrease in participation. Scholars point out on the positive side of I-voting also that I-voting could and should better accommodate the needs of disabled voters.[*25]

The actual impact of Internet voting on the turnout does not lend itself to objective analysis. One can determine the variations of turnout in different election years (comparing equivalent types of elections) and attempt to clarify the causes underpinning variations with the aid of sociological studies. Perhaps the most important question is what proportion of the electorate would not have participated in the voting had the Internet voting opportunity not been provided. There does not exist a way of obtaining empirical evidence. We must, therefore, come to terms with unverifiable claims made by the voters themselves. The only exception is the case where Internet voting provides the only possibility for the elector to vote and he or she takes advantage of this possibility. For example, the local government council elections in Estonia do not provide the possibility of voting abroad by postal ballot or at a diplomatic representation. Nonetheless, it is possible to vote over the Internet when abroad.[*26]

Table 1. I-voting statistics for 2005–2011[*27]

	2005 LE	2007 PE	2009 EPE	2009 LE	2011 PE
Number of I-votes	9,681	31,064	59,579	106,786	145,230
Repeated I-votes	364	789	910	2,373	4,384
Number of I-voters	9,317	30,275	58,669	104,413	140,846
I-votes cancelled by paper ballot	30	32	55	100	82
I-votes counted	9,287	30,243	58,614	104,313	140,764
Total number of votes cast	502,504	555,463	399,181	662,813	580,264
I-votes out of all votes cast	1.9%	5.5%	14.7%	15.8%	24.3%
I-votes among total advance votes	7.2%	17.6%	45.4%	44%	56.4%
I-votes cast abroad (no. of countries)	n.a.	2% (51)	3% (66)	2.8% (82)	3.9% (105)

Source: National Electoral Committee

I-voting seems to have had, in 2005, a slight effect on the increase in the turnout of voters who sometimes vote and sometimes not.[*28] In 2007, approximately 10% of those I-voters questioned said that they certainly or probably would not have voted without having had the possibility to vote via the Internet. Moreover, Trechsel and Vassil show that the percentage of the I-voters questioned who certainly or probably would not have voted without having had the possibility to vote via the Internet has risen to 16.3%, which allows the conclusion that the overall turnout might have been as much as 2.6% lower in the absence of such a method of voting. That is already a significant marker when one looks at the impact of Internet voting on the overall turnout.[*29]

25 See, e.g., M. Loncke, J. Dumortier. Online voting: A legal perspective. – International Review of Law, Computers & Technology 2004 (18) 1, pp. 60–61.

26 Ü. Madise, E. Maaten. Internet Voting in Estonia. – D. R. Insua, S. French (eds.). Advances in Group Decisions and Negotiation Vol 5 e-Democracy: A Group Decision and Negotiation Perspective. Dordrecht, Heidelberg, New York, London: Springer 2010, pp. 314–316.

27 LE—Local Elections, PE—Parliament Elections, EPE—European Parliament Elections.

28 F. Breuer, A. Trechsel. E-voting in the 2005 local elections in Estonia: Report for the Council of Europe 2006, available at the Council of Europe Web site.

29 A. Trechsel, K. Vassil. Internet Voting in Estonia: A Comparative Analysis of Four Elections Since 2005. Council of Europe and European University Institute 2010. Available at http://www.vvk.ee/public/dok/Report_-_E-voting_in_Estonia_2005–2009.pdf (9.10.2011).

3.3. Uniformity

3.3.1. The digital divide and equal opportunities for representation

Trechsel *et al.* concluded in the report prepared for the Council of Europe following the experience of the Internet voting in 2005 and 2007 that education and income, as well as type of settlement, are insignificant factors in the choice of Internet voting over other voting methods. One of the most important findings of that study was that it is not so much the divide etc. between the Internet access 'have's and 'have-not's as, clearly, computing skills, frequency of Internet use, and trust in the I-voting procedure that direct voters' decisions to use or not use I-voting. Age has remained a significant factor for some years.*[30] Moreover, some interesting conclusions have been drawn in the latest report by Trechsel and Vassil, in 2010, where they state that the ICT variables (computing knowledge and frequency of Internet usage) have disappeared since the 2009 elections as predictors of Internet voting usage.*[31]

In the discussion of equal access to the place of voting, some authors*[32] ignore the fact that in Estonia there are quite many different voting methods; for example, if a voter is unable to vote at a polling place as a result of his or her state of health or for another good reason, he or she may apply to vote by paper ballot at home on the day of election day (Riigikogu Election Act, §46 (1)).

The Estonian Supreme Court has stated:

> The principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons with the right to vote. In fact, those who use the different voting methods provided by law (advance polls, voting outside the polling division of residence, voting in custodial institutions, home voting, voting in a foreign state, etc) are in different situations. For example, the voters who have to use the possibility of advance polls, are in a situation different from that of the voters who can exercise their right to vote on the election day. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the Constitution.*[33]

In the future, the number of people without Internet access will probably decrease, but the digital divide is going to be even deeper than before. People without Internet access will have significantly less information, no access to voting-advice applications, etc. In this case, it is not the access to I-voting (as long as other methods of voting remain) but access to the candidates' and parties' information that might be the constitutional problem.

3.3.2. Impact on the voting results

The most intriguing question for political parties is probably that of the impact of the use of I-voting on results. Impact on the voting results can result from the fact that votes cast by those voters who would not participate if I-voting did not exist may not be distributed proportionally over the political spectrum. However, studies have shown that the left–right auto-positioning of the voter does not play any important role in the choice of a voting channel. The same applies to the 2009*[34] and 2011 elections.

30 A. Trechsel. Internet voting in the March 2007 Parliamentary Elections in Estonia: Report for the Council of Europe, 2007. Available at http://www.vvk.ee/public/dok/CoE_and_NEC_Report_E-Voting_2007.pdf.

31 A. Trechsel, K. Vassil (Note 29).

32 See, e.g., S. Meagher. When Personal Computers Are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights. – American University International Law Review 2008/23, pp. 374–376.

33 CRCSCd, 1.9.2005, 3-4-1-13-05, paragraph 24. Available at http://www.nc.ee/?id=381 (9.10.2011).

34 A. Trechsel, K. Vassil (Note 29).

Table 2. Relationship of I-votes to all votes cast for a political party

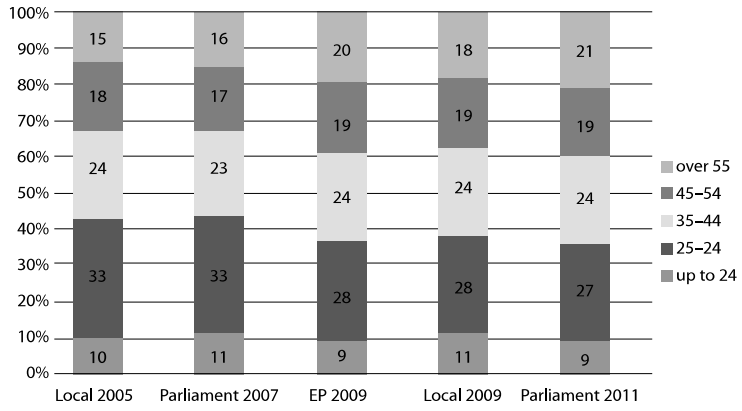
	2005 LE		2007 PE		2009 EPE		2009 LE		2011 PE	
	a)	**b)**	**a)**	**b)**	**a)**	**b)**	**a)**	**b)**	**a)**	**b)**
RP	32.7	3.6	34.5	6.8	20.1	19.3	25.1	23.7	37.0	**31.7**
PRU	10.4	2.3	26.7	**8.2**	17.3	**20.9**	22.5	25.5	25.4	30.3
PP	17.5	**3.8**	-	-	-	-	-	-	-	-
SD	9.9	2.9	13.3	6.9	10.4	17.6	10.7	22.6	18.0	25.8
GP	-	-	10.7	**8.2**	3.3	17.9	2.0	**27.4**	4.3	28.0
CP	8.7	0.6	9.1	1.9	10.9	6.2	14.7	7.4	9.9	10.4

Data: National Electoral Committee

a) = Percentage of I-votes
b) = Proportion of I-votes to total votes, in per cent
RP = Reform Party
PRU = Pro Patria and Res Publica Union (in 2005 only Res Publica)
PP = Pro Patria Union (merged with Res Publica to form PRU since 2007)
SD = Social Democratic Party
GP = Green Party
CP = Centre Party

In comparison of the overall distribution of votes in Internet voting or e-votes with that for total votes, not only the growing proportion of e-votes could be observed. According to Table 2, the party that is most popular in electronic voting is not always the one that profits the most from e-voting. The PRU (PP) and the GP (instead of the winner, RP) have been the greatest beneficiaries of Internet voting. The small numbers of e-votes on the account of the otherwise popular CP can be explained by that party's strong opposition to Internet voting from the very beginning[*35] but probably also by specifics of the electorate.

The hypothesis that I-voting rewards advantages to urban voters found no proof. Gender is also not an important factor when one chooses I-voting from among the possible voting channels. Age, by contrast, is quite an important factor in choosing Internet voting.[*36] Yet still, as can be seen in Figure 1, no age group is clearly dominant. The 55+ age group, with up to 20% of all Internet voters, is worthy of note here. So, while being younger correlates with use of the Internet as a means of voting, age does not give all the answers.



(Source: National Electoral Committee)

Figure 1. Age of I-voters in 2005 to 2011

35 Ü. Madise, E. Maaten, P. Vinkel. Internet Voting at the Elections of Local Government Councils on [sic] October 2005, Report on Internet voting to the NEC, 2006. Available at http://www.vvk.ee/public/dok/report2006.pdf (9.10.2011).

36 A. Trechsel, K. Vassil (Note 29).

It is, nevertheless, very interesting to compare the age groups taking part in Internet voting with the general electorate. For lack of a more comprehensive reference, we examine survey data from an exit poll conducted at the 2007 parliamentary elections by the Tartu University Department of Political Science.*[37] According to the poll the age groups break down as follows: ages up to 24 accounting for 12.3%, 25–34 for 16.3%, 35–44 for 19.5%, 45–55 for 16.5%, and over-55s for 35.4%. When comparing these figures to the Internet voting results for 2007, we see a strong over-representation in the under-35 group and under-representation in the over-55 age group. This appears to be consistent with the importance of age in the decision to choose Internet voting as a voting method.

3.3.3. The right to change one's I-vote

The President refused to promulgate amendments, which allowed I-voting and gave to the I-voter the right to replace I-vote once given with another I-vote or paper-ballot, to the Local Government Council election act*[38], arguing that I-voters are in a better position when compared to other voters, who do not have any right to change their vote once cast.*[39] The initial version of the I-voting law included the possibility of changing the I-vote with a paper ballot not only during advance voting but also on election day. To solve some of the problems indicated by the President, the Riigikogu restricted the time of I-voting to advance voting days. The chance to change their election preferences on Sunday after receiving additional information about candidates in the second half of the week had really placed I-voters in a better position. After this change, all voters who take advantage of advance poll possibilities were formally acting in the same conditions. The President did not see these changes as sufficient and initiated constitutional review.

The Supreme Court Chamber of Constitutional Review pointed out that, despite repeated electronic voting, there was no possibility of an I-voter affecting the voting results to a greater degree than can those voters who use other voting methods. From the standpoint of the voting results, this vote was deemed in no way more influential than a vote cast by paper ballot.

The most important arguments of the Supreme Court were the following. The principle of freedom of the vote gives rise to the obligation of the state to protect voters from persons attempting to influence their choice.

The aim of increasing voter turnout is without any doubt legitimate. The measures the state takes for ensuring the opportunity to vote for as many voters as possible are justified and advisable. Another aim in allowing I-voting is the modernisation of voting practices that coincides with the aims of I-voting listed in the recommendation Rec(2004)11, on legal, operational, and technical standards for I-voting, of the Council of Europe.

In accordance with the Penal Code, preventing a person from freely exercising his or her right to elect or be elected in an election or to vote in a referendum, if such prevention involves violence, deceit, or threat or takes advantage of a service, economic, or other dependency relationship of that person with the offender, is punishable by a pecuniary punishment or up to one year of imprisonment. The possibility for the voter to change the vote cast by electronic means throughout the advance polling period 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 watched 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 via a ballot paper, after having been freed from the illegal influence. In addition to the possibility of subsequently rectifying a vote given under such influence, the possibility of voting again serves an important preventive function.

---

37 R. Toomla. Results of 2007 Riigikogu elections exit polls. Conducted by the Department of Political Science of Tartu University. Unpublished, available to the authors.

38 Draft No. 607 SE in X Riigikogu proceedings. The draft, information regarding parliamentary procedures, and motions to change the draft are available on the Parliament Web site at http://www.riigikogu.ee/?page=eelnou2&op=ems&eid=607&assembly=10&u=20110420131938 (9.10.2011) (in Estonian). The I-voting provisions were first adopted as a law in 2002; see drafts 747 SE, 748 SE, 771 SE, and 906 SE in IX Riigikogu proceedings. Right before the very first use of I-voting in 2005 municipal elections, the Riigikogu decided to change some I-voting provisions and the President used his suspensive veto foreseen in §107 of the Constitution of Estonia.

39 Decision No. 873, 22.6.2005. Available at http://vp2001-2006.president.ee/et/ametitegevus/otsused.php?gid=64640 (in Estonian).

When the law guarantees a voter who is voting electronically the possibility of changing a vote cast by electronic means, the motivation to influence him or her illegally decreases.

There are no measures as effective as the possibility of changing a vote cast by electronic means for guaranteeing the freedom of election and secrecy of voting upon electronic voting by means of an uncontrolled medium. The infringement of the right to equality and of uniformity, which the possibility of I-voters to change their vote an unlimited number of times can be regarded as amounting to, is not sufficiently intensive to outweigh the aim of increasing participation in elections and introducing new technological solutions.*[40] Norwegian scholars arrived at similar principles independently before obtaining in-depth knowledge of the Estonian Internet voting system.*[41]

In fact, the number of changed and replaced votes has been low in all elections. The maximum number of replaced votes has been 100, and the percentage of repeated votes does not exceed 4% of total e-votes.*[42] So, any fears of misuse of these opportunities cannot be validated.

In short, the fact that the Internet voter is in a somewhat different position from the traditional voter does not in itself indicate an infringement of the constitutional values. The Supreme Court thus confirmed the constitutionality of one of the main premises of the remote Internet voting project.

3.3.4. Computing skills and security of the voter's computer

It has been noted that good computing skills have been an important factor in choosing Internet voting as a mode of voting in the 2005 and 2007 elections. Since 2009, the ICT variable has lost its meaning in defining the reasons behind the choice of using e-enabled voting. However, since the absolute number of Internet voters has steadily risen, the question of technical uniformity and usability emerges. I-voting has been offered in a variety of environments and on several platforms claiming to cover the maximum number of possible voters. In addition, comprehensive informational materials and a 24-hour help line are available.*[43] However, a peculiar issue arose in the 2011 elections. There were a few voters who used a very rare combination of screen resolution, Windows 7, and font sizes on their computer. When these people used the Internet voting application, some of the interface and control buttons were left behind the Windows taskbar. This would not have been a greater problem unless some of the candidates' names too were covered by the taskbar. One of the candidates brought a complaint to the Supreme Court that stated:

> The chamber adds that in organising Internet voting the state has to guarantee the accordance of the application with most common hardware, operating systems, resolutions, and fonts. In some cases, compliance cannot be guaranteed. In the event of such problems, the voter has the option of contacting the technical support staff. If the issues cannot be resolved, the voter can use the traditional means of voting.*[44]

Therefore, ensuring the compatibility of the computer with the Internet voting application is clearly left to the user.

The security analysis of the Internet voting concept*[45] states clearly that one of the fundamental security problems with electronically enabled voting is the necessity of trusting the voters' computer. The central system can be, and is, protected by the state. The spread of malware on private computers, on the other hand, cannot easily be limited—either by the state or through private efforts. The analysis even says that the modern personal computer is a 'black box' that nobody is able to control. Therefore, the security of the computer on which the voting application is run remains an issue in actuality. The user—the voter—can, of course, take actions to protect the computer, but, nevertheless, this cannot resolve all possible consequences. Accordingly, the security of the voting application is a topic that is being given extra attention.

---

40 CCRSCd, 1.9.2005, 3-4-1-13-05 (Note 33).

41 G. Skagestein, A. V. Haug, E. Nodtvedt, J. Rossebo. How to create trust in electronic voting over an untrusted platform. – R. Krimmer (ed.) (Note 2), p. 108.

42 See Table 1 for further data.

43 Available at http://www.valimised.ee/internet_eng.html (9.10.2011).

44 In 3-4-1-6-11. Available at http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-6-11 (in Estonian).

45 See Note 14.

However, the issue of secrecy became prominent during the 2011 elections when a computer enthusiast hacked his own vote in the voting application on his own computer. He was able to modify the vote and create an illusion of the vote not having been sent to the central system. He was also keen to go public with his discovery (to national media) and later bring the issue up to the Supreme Court. It is important to state that all of the problems and situations discovered were monitored in the central system and that the threats revealed had been discussed already in the 2003 security analysis.

Subsequently, the Supreme Court, in its judgement No. 3-4-1-4-11[*46], stated that knowingly manipulating one's own vote cannot be seen as grounds for indictment of the overall security of the Internet voting system. In an analogy with traditional voting, a voter could easily go to the polling booth and make the polling paper invalid (by scrapping or doodling on the paper, etc.). That is a conscious decision and is completely legitimate.

However, the debate about secrecy is never resolved. Another issue that was raised by the computer enthusiast described earlier is the traceability of a vote. The reasoning behind this is that the online environment cannot be trusted and additional external proof of compliance has to be generated. A very interesting Internet voting pilot project is to be introduced in late 2011 in Norway.[*47] In this project, external means of confirming one's choices are used. Namely, voters receive a special printed polling card (by post) with all candidates who are running for election represented by code names. After voting, the voter can request the code name matching the vote cast, via independent channels. This should, in theory, guarantee that the vote can be traced and that it has been accepted.

However, some additional concerns arise with this. Firstly, new channels of communication have to be built and secured between the state and the voter. Secondly, issues with the principle of anonymity come up where the voter has to understand that under some circumstances the state knows how he or she has voted. Thirdly, how does this traceability affect the possibility of buying or selling one's vote over the Internet?

4. Certification and auditing

Certification is, in broader term, a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes provisions for ascertaining that the system is functioning as intended. This can be done through measures ranging from testing and auditing to formal certification. The end result is a report and/or a certificate. An audit is an independent pre- or post-election evaluation of a person, organisation, system, process, entity, project, or product, which includes quantitative and qualitative analysis.[*48]

Currently, there is no domestic or international public body that would be ready to certify and audit all the elements of an entire I-voting system before, during, and after election procedures. In Estonia, hired specialists performed comprehensive tests in order to check the functionality and accuracy of the system both as experienced by testers and in public (in demo voting). A third party audits the source code and the procedures that have been carried out.

The Estonian I-voting system was developed to follow the principle that all components of the system must be transparent for audit purposes. Procedures should be fully documented, with those that are critical being logged, audited, observed, and videotaped as they are conducted. A common requirement is that the source code of the voting application be available for auditing. In Estonia, though the code is not universally available, it could be audited if so agreed by the NEC.

As a rule, the process audit is ordered from external internationally certified IT auditors. The audit reviews and monitors sensitive aspects of the process, such as updating of the list of voters, preparation of hardware and its installation, loading of election data, maintenance and updating of election data, and the process of counting the votes etc. At the counting event on election day, auditors publicly declare their opinion about the soundness of the procedures of the electoral administration to that point. The report of the auditors, released after all procedures are complete (including the destruction of all voting equipment—

46 Available at http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-4-11 (9.10.2011) (in Estonian).

47 For more information about the Norwegian Internet voting system, see http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658 (9.10.2011).

48 Council of Europe Rec(2004)11 and guidelines based on that recommendation (see Note 7).

I-votes along with it), states whether the I-voting procedures followed the rules described in the system's documentation and whether the integrity and confidentiality of the system was not endangered. To date, all reports have been positive.

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 stages, the I-voting system produces a variety of logs concerning received, cancelled, and counted votes, also invalid and valid votes. The audit application enables determining what happened to an I-vote cast by a specific 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.

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, the counting, and tabulation of results. Internet voting is no different. All significant documents describing the I-voting system are public. In order to enhance the observers' knowledge of the system, the political parties are invited to take part in a training course before each election, in which I-voting is used. Besides political parties, auditors and other persons interested in the I-voting system take part in the training. In addition, observers are invited to follow the testing of the whole process and take part in other preparatory procedures. However, few political parties have so far exercised their opportunity to observe the I-voting procedures.[*49] It is important that observers be deployed for an amount of time that suffices to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, conclusions cannot be made as to the integrity of the system.

The OSCE did audit the 2007 elections, and in its report it states that the "election administration implemented the [I-voting] system in a fully transparent manner, and appeared to take measures to safeguard the conduct of Internet voting to the extent possible".[*50] Professional, independent, reliable, and comprehensive IT audit and certification procedures should compensate for the lack of simple public scrutiny.

5. Conclusions

In Estonia, as well as in many other countries that have prepared systems for, and allowed, postal voting, advance voting, and other supplementary voting methods, voting at a polling station has virtually lost its significance as a ritual of transforming people into a nation-state and a carrier of sovereign nationhood.

In discussion surrounding the introduction of I-voting, the classical arguments concerning the conformity of I-voting with the principles of fair elections (including the reliability of the electronic voting systems) have gained renewed force. For example, one of the typical arguments against I-voting is that people who have no commitment to go to the polling station to execute their citizen's duty should not participate in governing at all, which contradicts the axiom that the higher the turnout the better.

A possible lack of legitimacy of the election results could result from either of the following situations:

- The privacy of individual I-voting procedure cannot be supervised by authorities or observed in a traditional way. Therefore, massive buying and selling of votes, as well as exercise of other influence or pressure on the voter, is possible.
- The people themselves cannot verify the I-voting results, and people need to have absolute faith in the accuracy, honesty, and security of the whole electoral system (its people, procedures, software, and hardware) if it is to be legitimate. For people who didn't take part in developing the system, the computer operations can be verified only by knowing the input and comparing the expected with the actual output. In a secret ballot system, there is no known input, nor is there any expected output with which to compare the electoral results.[*51]

Therefore, the question of whether remote Internet voting with binding results in public political elections complies with the constitutional principles of fair voting cannot be answered simply with a 'yes' or

49 E. Maaten, T. Hall. Improving the Transparency of Remote I-voting: The Estonian Experience. – R. Krimmer, R. Grimm (eds.). Electronic Voting 2008, Gesellschaft für Informatik. Bonn 2008, pp. 31–43.

50 OSCE/ODIHR 2007. Election Assessment Mission Report, Republic of Estonia, Parliamentary Elections, 4 March 2007. Available at http://vvk.ee/public/dok/OSCE_report_EST_2007.pdf (9.10.2011).

51 Ü. Madise, T. Maaten (Note 26).

'no'. Actually, the question and answer should be divided into two parts. The first sub-question should be whether the legal norms in the abstract comply with the constitutional provisions and the second whether the technical solution used to conduct voting procedures in a certain election guarantees constitutionality.

The first sub-question can be answered on the basis of theoretical analysis, but the second should be examined before and after the relevant elections. The fact that it is possible not to fulfil the legal requirements set for an I-voting system is not enough *per se* for declaring I-voting as a concept unconstitutional. As a matter of fact, this underscores the importance of qualified certification and auditing of the system as well as the need for a new approach in electoral observation. The second sub-question can be answered with a 'yes' only if sufficient measures are in place to check whether the IT solutions work properly. This leads to a requirement that auditing, certification, and evaluation as required in the Council of Europe guidelines[*52] be foreseen by law or NEC regulation.

In the Estonian case, the first sub-question could be answered 'yes', as e-ID enables secure remote identification, e-ID has wide penetration, all advance voters are placed in the same conditions, and the 'virtual voting booth' (the right to replace an I-vote with another I-vote or a paper ballot) and 'virtual double-envelope system' ensure freedom of voting and uniformity of elections. Moreover, the system is justified by the aim to guarantee universal suffrage in an information society where e-services (including Internet voting) are demanded by a significant proportion of the electorate. Whilst formal equality can be provided, the questions of material equality and the issue of the digital divide remain. In addition, complying with the principle of secrecy poses new obstacles for many countries. According to the above teleological interpretation of the principle of secrecy, the voting act is to be seen not as an aim but as a measure to guarantee freedom of voting, and the anonymity aspect of the principle of secrecy can be guaranteed. The analysis of the compliance of the Estonian I-voting system with the United Nations International Covenant on Civil and Political Rights has given positive result as well[*53] but emphasises the importance of special procedures to facilitate auditing and observation of I-voting.[*54]

The answer to the second sub-question is more complicated. Internet voting in concrete election is constitutional if the provisions of the law are fulfilled in practice: only people entitled to vote can vote, e-votes cast over the Internet are recorded and counted properly, and only one vote per voter shall be counted. Independent IT auditing that covers all aspects of the system can prove its soundness. The proper performance of the IT system should be certified and audited before, during, and after voting. The personal computer and the Internet remain a weak point of the system. The scholars are probably right in saying that "[a]lthough perfect real-time knowledge of all cyber threats is an impossible goal, it *is* realistic to do mach better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber attack".[*55] Both new threats and I-voting are part of the information society.

52 See Note 7.

53 S. Meagher (Note 32), pp. 349–380.

54 *Ibid.*, pp. 384–386.

55 Th. C. Wingfield, E. Tikk. Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen. – International Cyber Security. Legal & Policy Proceedings. Tallinn: CCD COE Publications 2010, p. 21.

III Ülle Madise and **Priit Vinkel**. 2015. "A Judicial Approach to Internet Voting in Estonia." In Jordi Barrat and Ardita Driza Maurer (eds). *E-Voting Case Law: A Comparative Analysis*. Farnham: Ashgate Publishing, 1-35 (*forthcoming).* (3.1)

Chapter 6

A Judicial Approach to Internet Voting in Estonia

Ülle Madise and Priit Vinkel

Introduction

Estonia is a small nation in Northern Europe, a Member of the European Union and NATO and has one of the most advanced e-governments in the world. It is the only country where all adult inhabitants are obliged to possess electronic identity and where countrywide remote I-voting[1] with binding results in all elections and referendums has been allowed since 2005. The share of online voters has risen to 24.3 per cent in the 2011 *Riigikogu* (Estonian Parliament) elections and 30.5 per cent in the 2015 *Riigikogu* elections. The compulsory e-ID as a universal access key to public and private e-services is a critical success factor for I-voting, advanced e-Health[2] solutions, digital signature, electronic tax board etc.

Using the Internet for public services raises several constitutional and cyber security problems. Neither abandoning e-services nor simply denying threats is a proper solution. Netizens[3] require the redesigning and rethinking of many institutions, concepts and principles to protect values of democracy in the Internet era. Indeed, using new technologies is just a means, not an end. Thus the benefit should outweigh the cost and risks; and judicial control over the executive,

1 The Estonian concept of remote I-voting does not limit the environment of the voter, so, contrary to the concept of electronic voting used in many countries (kiosk voting, voting machines etc.), I-voting is not offered in polling stations. However, many public and private establishments like banks or libraries offer internet access to the public during elections.

2 Estonian e-Health comprises four systems: an electronic health record, digital registration, digital prescriptions and a digital image.

3 The term 'netizen' was coined by Michael Hauben in 1992 while studying at Columbia University. See also Michael Hauben and Ronda Hauben, Netizens: On the History and Impact of Usenet and the Internet (Los Alamitos, CA: IEEE Computer Society Press, 1997). As pointed out by several thinkers like James Fishkin, there is a need for some new approaches and tools to improve decision-making and participation. See e.g. The Centre for Deliberative Democracy website http://cdd.stanford.edu/ (accessed 1 August 2014). For opposing statements see Hubertus Buchstein 'Online Democracy, Is it Viable? Is it Desirable? I-voting and Normative Democratic Theory' in Norbert Kersting and Harald Baldersheim (eds), *Electronic Voting and Democracy: A Comparative Analysis* (Basingstoke: Macmillan 2004).

including electoral administration in the case of Internet Voting, must be real and possible.

The chapter starts with brief overview of Estonian electoral law, and the electoral system, administration and experience. Some light is then shed on the technical solution chosen as well as the testing, auditing and verification of the system. This serves as an introduction to the discussion of court procedure and judgements in cases related to the Internet voting scheme.

Electoral Law, System and Administration

Electoral Law

According to the Estonian Constitution[4] members of the *Riigikogu*, as well as local government councils and European Parliament, shall be elected in free, general, equal and direct elections, and voting shall be secret. There is no special regulation for I-voting in the constitution. The legal framework for I-voting is given in electoral law. The provisions are almost the same in all legal acts regulating voting procedures, whereas the most detailed provision is stipulated in the Riigikogu Election Act.[5] In addition, the National Electoral Committee adopts a decree[6] on the detailed provisions concerning the organization of I-voting. After the first adoption processes in 2002 and 2005, the I-voting regulation was furthermore enhanced in 2012 when a special committee of the parliament worked out regulations containing the formation of the electronic voting committee, adding detailed procedural provisions to the law etc.

Furthermore, different Council of Europe guidelines and the OSCE/ODIHR observing and assessing reports on e-voting (including I-voting)[7] have served

4 Translations of Estonian legal acts can be found at https://www.riigiteataja.ee/en/. The updated official versions of all legal acts are available at the State Gazette, www.riigiteataja.ee (in Estonian).

5 See Chapter 7, 'Electronic Voting', https://www.riigiteataja.ee/en/eli/ee/510032014001/consolide/current.

6 It is named 'the procedure for the organisation of electronic voting and the ascertaining of the results of electronic voting', it can be found here: https://www.riigiteataja.ee/akt/118032014016 (in Estonian).

7 Council of Europe recommendation on legal, operational, and technical standards for e-voting, Rec(2004)11, available at https://wcd.coe.int/ViewDoc.jsp?id=778189; Recommendation on Electronic Democracy, Rec(2009)1, available at https://wcd.coe.int/ViewDoc.jsp?id=1410627; Guidelines on Certification of E-voting Systems, GGIS(2010)3, available at http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf; and Transparency of e-enabled elections, GGIS(2010)5, http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf. OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, available at

as examples and sources of best practice in developing the Estonian solutions and regulations.

Although not a part of legal norms' hierarchy, the recommendation[8] issued by the Council of Europe has been referred to by the Supreme Court of Estonia.[9]

Electoral System

The Estonian parliament consists of 101 members who are elected in 12 electoral districts comprising five to 14 mandates each. The voter chooses a party-list candidate or an independent candidate. The electoral results are determined based on both election district results and national list results by a proportional electoral system. The number of parties in the parliament had fallen to four by 2011, but got back to six in 2015. The proportional system is used at local and European Parliament elections as well.

As Estonia is a small country with around 1 million eligible voters, many of those residing temporarily or permanently abroad,[10] the number of voting channels has been high in Estonia throughout the years. Every vote counts and every voter should have the possibility to vote in the most convenient way. Beside the traditional Election Day voting, there are several additional voting channels ranging from embassy and postal voting for voters permanently residing abroad and voting on ships flying the Estonian flag, to different channels of voting outside the voting district of residence and home voting for those voters unable to visit the polling place.[11] In this large mix of channels, I-voting is just one additional possibility for the voter.

---

http://www.osce.org/odihr/elections/104939?download=true. The OSCE/ODIHR Election Assessment Mission has observed Internet voting in Estonia (parliamentary elections 2011) http://www.osce.org/odihr/77557, in Norway (municipal election 2011) http://www.osce.org/odihr/88577, and in Switzerland (Federal elections 2011) http://www.osce.org/odihr/87417, all accessed 1 August 2014.

8 The Estonian Supreme Court case 3-4-1-13-05 [2005] (http://www.nc.ee/?id=381 in English).

9 See p. 17 of the judgement: 'Although the Recommendation of the Council of Europe is not a legally binding document, it summarises the understanding of the democratic states of Europe of the conformity of electronic voting with the election principles inherent to democratic states, and it is thus an appropriate tool for interpreting the Constitution'.

10 For the latest data see Ene-Margit Tiit 'Estonian Census 2011' [2013] *Papers on Anthropology*, 22, 234.

11 The complete list of voting channels in the 2015 *Riigikogu* elections will be: voting on Election Day, home voting on Election Day, voting abroad (by mail or in embassies, by temporal or permanent abroad residents), voting on ships, Internet voting, advance voting in special locations (penitentiaries, nursing homes, hospitals etc.), advance voting in all polling stations, advance voting in special polling stations (voters outside residence), advance voting in county centres.

In Estonia, voting is not compulsory and there is no required minimum turnout. The overall turnout rates are quite standard in Eastern European terms; in parliamentary elections the turnout ranges from 57 to 68 per cent.[12]

Electoral Administration

The National Electoral Committee (NEC) manages electoral administration in Estonia. This seven-member politically independent body consists of high public officials. Other electoral committees are built up hierarchically starting from voting district (polling place) committees and ranging to municipal and county committees. In 2012 the parliament decided that a new electoral committee – electronic voting committee – would be established for the technical administration of I-voting. All committees are subordinated to the NEC which organizes training for electoral officials and resolves electoral complaints in the first instance. The rulings of the NEC can be contested directly in the Supreme Court.

The Estonian I-voting Solution

For I-voting, the voter needs an Internet connected computer (Windows, Linux and iOS are supported) and any type of e-ID (either ID-card, electronic-ID or mobile-ID).[13]

All Major Principles of Traditional Voting are Followed

The Estonian concept seeks to follow all the principal steps of traditional voting in order to maintain the connection with traditional elections and to make the concept more understandable for the voter. This includes basic electoral principles such as freedom, universality, uniformity and secrecy (anonymity) of the vote. In addition, and in order to include familiar values from traditional elections, a 'virtual double envelope' scheme is used. This means, similar to paper voting, the Internet vote is encrypted in the voter's computer (put in a blank envelope) and marked with the voter's data using a digital signature (put in a larger envelope with the voter's data on it).[14]

12 A detailed overview of Estonian elections can be found in Alo Heinsalu, Arne Koitmäe, Mihkel Pilving and Priit Vinkel, 'Elections in Estonia 1992–2011' [2012] National Electoral Committee and National Library, http://issuu.com/vabariigi_valimiskomisjon/docs/elections_in_estonia_1992-2011_eng/1, accessed 1 August 2014.

13 See also: Priit Vinkel, 'I-voting in Estonia' in Peeter Laud (ed.), *Lecture Notes in Computer Science: NordSec 2011, Tallinn, Estonia 26–28 October 2011* (Berlin: Springer, 2012).

14 See also: Sven Heiberg, Peeter Laud and Jan Villemson, 'The Application of I-voting for Estonian Parliamentary Elections of 2011' in Aggelos Kiyaias and Helger Lipmaa (eds), *E-voting and Identity* (Dordrecht: Springer, 2012).

Virtual Voting Booth[15]

In order to prevent coercion and possible breaking of the freedom and secrecy of voting, it is possible to change (replace) the I-vote an unlimited number of times during advance polling days. Only the last vote is counted. Another option is to go to the polling place and submit a paper vote during advance voting. In this case the paper ballot is counted. In this way the so-called virtual voting booth is created. A voter who has experienced undue influence while voting via the Internet can make her or his independent electoral choice.

I-voting Is Held for a Seven-Day Period

The voting period starts 10 days before Election Day at 9 a.m. and is closed four days before Election Day at 6 p.m. Voting is possible throughout the whole period, i.e. 24 hours a day for seven days.

Digital Voter's Register

The Estonian Population Register is used for obtaining the voter lists. The same lists are used as printed lists in polling places and electronically on the Internet. The correct, timely and efficient compiling of these lists allows for the easy introduction of remote voting.

Voter Identification with Electronic-ID

The Estonian ID card and the Mobile-ID solutions offer a secure, proven and sophisticated means for identification of the voter in the electronic environment. The e-ID solution is used throughout the private and governmental sector to identify the person and for digital signing.[16]

Verifiable Vote

Since 2013, a system that allows the voter to get information regarding whether the vote was cast as intended and accepted by the central system as cast has been implemented, it being legally binding from the 2015 parliamentary elections. Secondary channels, like smart phones are used in that matter.[17]

15 Also 'voter's right to replace the I-vote'.

16 More can be found in: Ülle Madise and Epp Maaten, 'I-voting in Estonia' in David Rios Insua and Simon French (eds), *E-Democracy: A Group Decision and Negotiation Perspective* (Dordrecht: Springer, 2010) and Ülle Madise and Priit Vinkel, 'Constitutionality of Remote I-voting: The Estonian Perspective' [2011] *Juridica International*, 18.

17 See a short description of the verification scheme at http://www.vvk.ee/public/Verification_of_I-Votes.pdf, accessed 1 August 2014.

I-Voting Experience 2005–2015

Estonia-wide remote I-voting with binding results was used for the first time in municipal elections 2005.[18] Since 2005 this way of voting has been used in eight elections, the 2015 *Riigikogu* elections being the most recent (see Table 6.1). But, as already emphasized, I-voting is one of many voting channels and will not replace the traditional paper based solutions in the foreseeable future.

Table 6.1 I-voting statistics for 2005–2015

	2005 ME	2007 PE	2009 EPE	2009 ME	2011 PE	2013 ME	2014 EPE	2015 PE
Number of I-votes	9,681	31,064	59,579	106,786	145,230	136,853	105,170	181,084
Repeated I-votes	364	789	910	2,373	4,384	3,045	2,019	4,593
Number of I-voters	9,317	30,275	58,669	104,413	140,846	133,808	103,151	176,491
I-votes cancelled by paper ballot	30	32	55	100	82	146	46	162
I-votes counted	9,287	30,243	58,614	104,313	140,764	133,662	103,105	176,329
Total number of votes cast	502,504	555,463	399,181	662,813	580,264	630,050	329,766	577,910
I-votes out of all votes cast	1.9%	5.5%	14.7%	15.8%	24.3%	21.2%	31.3%	30.5%
I-votes among total advance votes	7.2%	17.6%	45.4%	44.0%	56.4%	50.5%	59.2%	59.6%
I-votes cast abroad (no. of countries)	n.a.	2% (51)	3% (66)	2.8% (82)	3.9% (105)	4.2% (105)	4.7% (98)	5.7% (116)

Note: ME – municipal government elections; PE – parliamentary elections; EPE – European Parliament elections

Source: National Electoral Committee.

18 Political and legal debates are analysed in: Wolfgang Drechsler and Ülle Madise, 'Electronic Voting in Estonia' in Norbert Kersting and Harald Baldersheim (eds), *Electronic Voting and Democracy: A Comparative Analysis* (Basingstoke: Macmillan, 2004).

One of the declared aims of launching online voting in Estonia was to increase voter turnout, which perhaps could be described more realistically as broadening access possibilities and stopping the decrease in participation. Scholars point out on the positive side that I-voting also could and should better accommodate the needs of disabled voters.[19]

The actual impact of Internet voting on the turnout does not lend itself to objective analysis.[20] One can determine the variations of turnout in different election years (comparing equivalent types of elections) and attempt to clarify the causes underpinning variations with the aid of sociological studies. Perhaps the most important question is what proportion of the electorate would not have participated in the voting had the Internet voting opportunity not been provided. There does not exist a way of obtaining empirical evidence. We must, therefore, come to terms with unverifiable claims made by the voters themselves. The only exception is the case where Internet voting provides the only possibility for the elector to vote and he or she takes advantage of this possibility. For example, the local government council elections in Estonia do not provide the possibility of voting abroad by postal ballot or at a diplomatic representation. Nonetheless, it is possible to vote over the Internet when abroad.[21]

Trechsel and Vassil concluded, in the report prepared for the Council of Europe following the experience of Internet voting, that education and income, as well as place of residence, are not important factors in the choice of Internet voting over other voting channels.[22] Moreover, Trechsel and Vassil have drawn some interesting conclusions in the 2011 report, where they state that the ICT variables (computing knowledge and frequency of Internet usage) which were important predictors of Internet voting usage in 2005 and 2007 have disappeared since the 2009 elections.[23]

19 See, e.g.: Mieke Loncke and Jos Dumortier, 'Online Voting: A Legal Perspective' [2004] *International Review of Law, Computers and Technology*, (18)1.

20 See e.g.: Kristjan Vassil and Till Weber, 'A Bottleneck Model of E-voting: Why Technology Fails to Boost Turnout' [2011] *New Media and Society*, 13(8).

21 Ülle Madise and Epp Maaten, 'I-voting in Estonia' in David Rios Insua and Simon French (eds), *E-Democracy: A Group Decision and Negotiation Perspective* (Dordrecht: Springer, 2010).

22 Alexander Trechsel, *Internet Voting in the March 2007 Parliamentary Elections in Estonia: Report for the Council of Europe, 2007*, available at http://www.vvk.ee/public/dok/CoE_and_NEC_Report_EVoting_2007.pdf, accessed 1 August 2014.

23 Alexander Trechsel and Kristjan Vassil, *Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005* (Council of Europe and European University Institute, 2011), available at http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf, accessed 1 August 2014.

An Overview of the Estonian Judicial and Constitutional Review System

Pursuant to the Constitution, the highest court in Estonia, the Supreme Court, is also the court of constitutional review. Besides Administrative, Criminal and Civil Chambers, there is also a Constitutional Review Chamber. This Chamber consists of nine judges elected by the Supreme Court for five years. Members of the Chamber shall not be elected for longer than two terms of office. The Chief Justice of the Supreme Court shall be the chairman and presiding judge of the Chamber and at least one member from the Civil, Criminal and Administrative Chambers of the Supreme Court shall belong to the Chamber. Usually constitutional review cases are decided by a panel of five justices, in exceptional cases *en banc*.[24]

The organization of constitutional review in Estonia differs from the system of separate Constitutional Courts established in most European countries. However, the Estonian model has some significant advantages compared to other European countries. Besides diminishing expenses, the system ensures the uniformity of judicial practice and excludes possible conflicts between the highest instances of the administrative and general court system and the constitutional court in the interpretation of law and the Constitution. The Estonian system also decreases the possibility of constitutional review becoming politicized: the instance of constitutional review belongs to the highest court of the state judicial system, the members thereof being appointed from among the justices by the highest court itself.

The most important function of the Constitutional Review Chamber is to check that the laws adopted by the parliament are in compliance with the norms and principles established by the Constitution.

Pursuant to the Constitution, the Supreme Court has the right to declare any legal act invalid that is in conflict with the provisions or essence of the Constitution.[25]

Election complaints, in their essence administrative cases, have been given a special regulation in the electoral acts. All such complaints are discussed in the first two instances, in county and national electoral committees respectively. The procedure is swift, the complaint has to be filed within three days and the committee has five working days to reach a verdict. The third instance is the Constitutional Chamber of the Supreme Court where a swift course is also paved, with only seven working days provided for the court to reach a verdict.

24 All 19 judges sitting.

25 General constitutional review can be initiated by the President of the State, the Chancellor of Justice, a local government council (in specific matters) and the courts. Specific review of a provision could also be achieved through the election complaints procedure.

The Judicial Approach to I-voting

Types of Cases in I-voting Issues

The cases on the matter of I-voting can be divided into three broad categories: general constitutional review; complaints against electoral administration; and criminal offences. In Estonia the court procedure is different for each of these categories.

General constitutional review

The question of the constitutionality of legal acts (in this case electoral acts) and single provisions concerning the general concept of I-voting is the subject of the regular constitutional review procedure as described above. The most prominent case in this category is the discussion about the principle of uniformity and secrecy in the case of I-voting.[26] The President of the Republic issued a petition to the Supreme Court in order to declare the component of multiple voting unconstitutional.

In addition to this process, one direct complaint to the Supreme Court was issued by Tallinn City Council, again on the premise of the infringement of the principle of uniform municipal elections.[27] Both cases are discussed further below.

Complaints against electoral administration

Specific issues concerning the technical or operational functioning and preparation of I-voting are raised through the procedure of complaints against the electoral administration (elaborated in the previous section) during or after the electoral procedures in given elections. Until 2012, the Estonian National Electoral Committee was the *de iure* organizer of I-voting, therefore the complaints were issued directly to the Supreme Court. However, since the introduction of the Electronic Voting Committee, a specialists' committee formed by the National Electoral Committee, all disputes are settled in the first instance by the NEC, and after that it is possible to file a complaint with the Supreme Court.

After the 2011 parliamentary elections, five cases of this type were initiated, and after the 2013 municipal elections, one more: a complaint of P.P. for annulment of all Internet votes based on security issues in the system,[28] a complaint of a candidate, H.P. for annulment of all Internet votes because of a technical glitch

26 The Estonian Supreme Court case 3-4-1-13-05 [2005] (http://www.nc.ee/?id=381 in English).

27 The Estonian Supreme Court case 3-4-1-16-11 [2011] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-16-11 in Estonian).

28 The Estonian Supreme Court case 3-4-1-4-11 [2011] (http://www.nc.ee/?id=1243 in English).

involving too large font sizes and a non-transparent Windows taskbar,[29] a complaint of T.R for annulment of all given votes, based on security issues in the system that was used,[30] two complaints of the Centre Party to annul election results because of shortcomings in I-voting,[31] and in 2013 a complaint of an election coalition against I-voting and other basics of the electoral system in general.[32] After the 2015 Riigikogu elections, one specific I-voting related complaint was issued, by V.K for annulment of all given votes because of a changed Election Day procedure, but as the complaint did not affect the subjective rights of the complainant, the case was dismissed.[33]

Criminal offences

Cases of selling or buying Internet votes, violence against or influence of an I-voter, cyber-attacks against the I-voting system, misuse of another person's e-ID in electoral matters and similar are not processed by the electoral administration and fall under the jurisdiction of the police; thus they are taken to standard criminal court. By 2014, no criminal cases tied specifically to I-voting have been discussed in court.

A Constitutional Review of I-voting[34]

The most important case in this category concentrated on the equality aspect of I-voting. The court did not evaluate all aspects of I-voting and has thus left the door open for further constitutional disputes.

In 2005, just a few months before the planned first launch of online voting, the President of the Republic refused to promulgate amendments to the Local Government Council election act[35] arguing that I-voters are in a better position

29 The Estonian Supreme Court case 3-4-1-6-11 [2011] (www.nc.ee/?id=1255 in English).

30 The Estonian Supreme Court case 3-4-1-7-11 [2011] (www.nc.ee/?id=1256 in English).

31 The Estonian Supreme Court cases 3-4-1-10-11 [2011] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-10-11) and 3-4-1-11-11 [2011] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-11-11 in Estonian).

32 The Estonian Supreme Court case 3-4-1-57-13 [2013] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-57-13 in Estonian).

33 The Estonian Supreme Court case 3-4-1-5-15 [2015] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-5-15 in Estonian)

34 For a more detailed view see also Ülle Madise and Priit Vinkel, 'Constitutionality of Remote I-voting: The Estonian Perspective' [2011] *Juridica International*, 18.

35 Draft nr. 607 SE in X *Riigikogu* proceedings. The draft, information regarding parliamentary procedures as well motions to change the draft are available on the parliament's website (http://www.riigikogu.ee/?page=eelnou2&op.=ems2&eid=607&assembly=10&u=20140811113307 in Estonian, accessed 1 August 2014). The I-voting provisions were first adopted as a law in 2002, see drafts nr. 747 SE, 748 SE, 771 SE

when compared to other voters who do not have any right to change the vote once given. The Law sent back to the parliament by the president contained the possibility to replace the I-vote with a paper-ballot not only during advance voting days but also on the Election Day. Therefore, the I-voters were indeed in a favourable position when compared to other advance voters and voters who cast their vote on Election Day. The Estonian parliament *Riigikogu* agreed with the President and restricted the time of I-voting to advance voting days. The option of changing election preference on Sunday, after receiving additional information about candidates in the second half of the week, really put I-voters into better situation. After this change, all voters who use advance poll possibilities are formally in the same position. However, the President did not consider these changes sufficient and he initiated a constitutional review.

The Constitutional Review Chamber of the Supreme Court decided that the right to replace I-vote by another I-vote or by ballot-paper does not unconstitutionally infringe the equality of I-voters and voters who vote in advance by paper ballot. Due to the virtual double envelope scheme, it is guaranteed that only one vote by the I-voter is counted. The right to change the vote does not give any advantages to the I-voters in any way.

The Estonian Supreme Court uses for the analysis of the constitutionality of the infringement of basic rights the so-called proportionality test, best known in the German theory of rational argumentation in legal discourse.[36]

The legal norm limiting a fundamental right is considered to be constitutional, if there is a legitimate aim for a constraining measure; the measure is suitable to achieve the aim; the measure is necessary to achieve the aim; and there is no other, less limiting measure available.

The rational argumentation of the Estonian Supreme Court was the following.

Legitimate aim

The aim declared by the parliament to increase, or at least to stop the decrease in, voter turnout is without any doubt legitimate. The measures the state takes to ensure the possibility to vote for as many voters as possible are justified and advisable. Another aim of allowing I-voting is the modernization of voting practices that coincides with the aims of I-voting listed in the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting.[37]

---

and 906 SE in IX *Riigikogu* proceedings. Right before the very first use of I-voting in 2005 municipal elections the *Riigikogu* decided to change some I-voting provisions and the President used his suspensive veto mandated in § 107 of the Constitution of Estonia.

36 The proportionality test originated systematically with the jurisprudence of the German Constitutional Court. Its variations are currently used by the European Court of Justice as well.

37 See footnote no. 7.

Suitability and necessity

The court stated that the voter's option to change the vote given by electronic means during the advance polling days constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting when voting by electronic means.

A voter who has been illegally influenced or watched 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 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.

Lack of alternative measures

There are no other equally effective measures, beside the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting when voting electronically in an uncontrolled medium. The infringement of the right to equality and of uniformity, which is what the I-voters' option to change their votes an unlimited number of times can be regarded as amounting to, is not sufficiently intense to outweigh the goals of increasing the participation in elections and introducing new technological solutions.[38]

Norwegian scholars arrived at similar principles independently before obtaining detailed knowledge about the Estonian I-voting system[39] or the work of Estonian scholars.

In short, the fact that the I-voter is in a somewhat different position compared to the traditional voter does not in itself create an infringement of the constitutional values. The Supreme Court thus confirmed the constitutionality of one of the main premises of the remote I-voting project. Without the virtual voting booth (the right to replace the I-vote) it would be impossible to guarantee the freedom of electoral choice, and without guaranteeing this freedom, I-voting would be unconstitutional and could not be used in Estonia.

Another case of general constitutional review did not bring any new important arguments related to the constitutionality of I-voting.[40] This case was initiated

38 The Estonian Supreme Court case 3-4-1-13-05 [2005] (http://www.nc.ee/?id=381 in English).

39 See Gerhard Skagestein, Are Vegard Haug, Einar Nodtvedt and Judith Rossebo, 'How to Create Trust in Electronic Voting over an Untrusted Platform' in Robert Krimmer (ed.), *Electronic Voting 2006: 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.cc* (Bonn: Gesellschaft für Informatik, 2006).

40 The Estonian Supreme Court case 3-4-1-16-11 [2011] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-16-11 in Estonian).

by the Tallinn Municipal Council six years later, in 2011.[41] Tallinn City Council referred in its petition to the alleged inequality of I-voters and other advance voters and lack of security. The first question was already the subject of constitutional review in 2005. Tallinn did not bring up either new theoretical arguments or new evidence. The municipal council has the right to initiate constitutional review only if there has been an infringement of the constitutional guarantees of local government autonomy. According to the constitution, local government is entitled to manage independently all local issues. The Supreme Court stated that electoral law does not belong to local issues, and therefore the municipal council's petition was declared inadmissible.

As discussed above, the Supreme Court has judged on only some of the constitutional aspects of I-voting. The variety of problems is much broader.

a. The privacy of individual I-voting cannot be supervised by authorities or observed in a traditional way. Therefore, massive buying and selling of votes as well as exercise of other influence or pressure on the voter are possible.
b. The people themselves cannot fully verify I-voting results, and people need to have absolute faith in the accuracy, honesty and security of the whole electoral system (people, procedures, software and hardware). For people who didn't develop the system, only knowing the input and comparing the expected with the actual output can result in verification of the computer operations. Under a secret ballot system, there is no known input, nor is there any expected output with which to compare the electoral results.[42]
c. It is difficult to prove the possible breach of the rights of I-voters and it is difficult to find evidence for arguing the opposite. The electoral administration and courts face new challenges.

The first sub-question should be whether the legal norms comply with the constitutional provisions; and the second, whether the norms are properly implemented using the technical solution. The third question is: how to prove it in court?

41 Tallinn is the Estonian capital led by the Centre Party which opposes I-voting and uses any possible methods to compromise or challenge it. Besides its fair concern regarding the security of I-voting, the problem for this party might be that I-voting is not useful to them or any other party whose supporters are ready to turn out on Election Day and use the paper ballot. Behind that calculation could be the knowledge that if I-voting did not exist, some voters could not or would not vote, which would increase such parties' share of the votes in a proportional system. However, as this approach contradicts the principle of universal suffrage, it has never been publicly declared.

42 See also Ülle Madise and Tarvi Martens, 'E-voting in Estonia 2005: The First Practice of Country-wide Binding I-voting in the World' in Robert Krimmer (ed.), *Electronic Voting 2006: 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.cc* (Bonn: Gesellschaft für Informatik, 2006).

The first sub-question can be answered based on abstract analysis but the second one requires formalized procedures, IT audit results and observation reports. This underlines the importance of qualified certification and auditing of the system as well the need for new approaches in electoral observation.

In the Estonian case the first sub-question could be answered 'Yes', as e-ID enables secure remote identification, e-ID penetration is wide, all advance voters are in the same position, the 'virtual voting booth' (the right to replace an I-vote with another I-vote or a paper ballot) and 'virtual double envelope system' ensure freedom of voting and uniformity of elections. Moreover, it is justified by the aim to guarantee universal suffrage in an information society where e-services (also I-voting) are required by a significant part of the electorate.

According to the teleological interpretation of the principle of secrecy, the privacy of the voting act cannot be seen as an aim but as a measure to guarantee freedom of voting; and the anonymity aspect guarantees the principle of secrecy. An analysis of the compliance of the Estonian I-voting system with the United Nations International Covenant on Civil and Political Rights has given a positive result as well,[43] but emphasizes the importance of special procedures to facilitate the auditing and observation of I-voting.[44]

The answer to the second sub-question is more complicated. The second sub-question could be answered 'Yes' only if there are sufficient measures to check that the IT solutions work properly. This leads to the requirement that auditing, certification and evaluation as required in the Council of Europe guidelines should be foreseen by law or electoral administrative regulation. I-voting in a concrete election is constitutional if the provisions of the law are actually fulfilled: only people entitled to vote can vote, votes given over the Internet are recorded and counted properly, only one vote per voter is counted. Independent IT audit covering all aspects can prove the soundness of the system. The proper performance of the IT system should be certified and audited before, during and after voting.

The personal computer as well as the Internet remain the weak points of the whole system. The scholars are probably right when they say: '[a]lthough perfect real-time knowledge of all cyber threats is an impossible goal, it *is* realistic to do much better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber-attack'.[45]

43 See also: Sutton Meagher, 'When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights' [2008] *American University International Law Review*, 23.

44 Ibid., pp. 384–6.

45 See Thomas C. Wingfield and Eneken Tikk, 'Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen' [2010] *International Cyber Security: Legal and Policy Proceedings* (Tallinn: CCD COE Publications).

The answer to the third sub-question is derived from what was said above: all aspects of the I-voting system will be documented, an independent reliable IT audit is required, and in constitutional review cases the results of other sciences will be used.

Constitutional review proceedings put greater weight in rational argumentation, based on well-established theoretical research, opinions presented in the past and to a limited extent the results of other scientific disciplines. The number and the weight of the abstract facts to be proven in these disputes is smaller and lighter. However, it is important to include factors of electoral behaviour analysis and sociological studies – for example, the argument that the possibility of I-voting exists in the information society to ensure the universality (general nature) of elections. In addition to the abstract arguments, 'hard data' studies should be included in the method of research, including studies on voting behaviour.

The impact of I-voting on turnout can evidently be proven only in cases where it is clear that without the I-voting option the voter would not objectively have been able to participate in the elections. For instance, in Estonia postal voting from abroad is allowed only in general and European Parliament elections and referendums. In municipal elections, postal voting is not used and voters staying abroad can only vote via the Internet. Therefore, all the votes received from abroad constitute an increase in turnout.

As for the remainder of the problem, properly devised studies would be in order that explain how many voters would not have voted had I-voting not existed. Of course, these results reflect the reality only to a limited extent, because you can rely only on the testimonies of the people themselves, a matter that is intrinsically impossible to verify.

If the court finds that the disputed act or provision is unconstitutional, it declares the relevant provision invalid.

Complaints against Election Administration

Procedure

Disputes and complaints arising during the preparation and organization of elections are settled according to the procedure for review of complaints provided in the Estonian election acts and the Referendum Act. In Estonia all electoral complaints must be solved before confirmation of the official election result. The only exemption is European Parliament elections as the confirmation of the results is partially regulated by EU law.

The procedures of the Electronic Voting Committee are reviewed on appeal by the National Electoral Committee. Only a person who finds that their (subjective) rights have been violated in the voting process is entitled to file a complaint. A complaint cannot be filed in the public interest.

A complaint must be filed with the electoral committee within three days of the contested resolution or act. The electoral committee reviews the complaint within five working days of the receipt of the complaint.

The electoral committee either satisfies or denies the complaint, or satisfies it partially. If the complaint is satisfied, the electoral committee may decide to revoke the contested resolution of the electoral committee as well as to perform further acts, e.g. initiate supervision of the activities of the electoral committee or issue precepts to electoral committees. Furthermore, the National Electoral Committee has the right to declare (I-)voting results invalid and call for a repeat vote.[46]

If the interested party does not accept the resolution made by the National Electoral Committee after having reviewed the complaint, or finds that the resolution of the National Electoral Committee violates their rights, they may file a complaint with the Supreme Court pursuant to the procedure provided in the Constitutional Review Court Procedure Act. As already stated, the procedure of an electoral complaint in the Supreme Court is different from standard proceedings. The court, in a standard-three-member formation, has only seven working days, with a possibility of an extension, to come to a decision.[47]

Complaints in I-voting cases

The case of H.P. vs National Electoral Committee[48]

I-voting has been offered in a variety of environments and platforms claiming to cover the maximum number of possible voters. In addition, comprehensive information materials and a 24-hour helpline are available.[49] However, a peculiar issue was brought up in the 2011 elections. A few voters used a very rare combination of screen resolution, Windows 7 and font sizes on their computer. Consequently, when using the I-voting application a portion of the interface and control buttons were left behind the Windows taskbar. This would not have been a serious problem unless some of the candidates' names weren't also covered by the taskbar. One of the candidates brought a complaint to the Supreme Court and the judgement stated.[50]

> The Chamber adds that upon organising e-voting, it is the state's responsibility to ensure the compatibility of the software used in elections with the most common

46 See Art 15 and Art 73 of the Riigikogu Election Act, available at https://www.riigiteataja.ee/en/eli/510032014001/consolide (English).

47 The basis of the procedure is stipulated in the main electoral act, Riigikogu Election Act (see Art 72, available at https://www.riigiteataja.ee/en/eli/510032014001/consolide in English) but relies heavily also on the Constitutional Review Court Procedure Act (available at https://www.riigiteataja.ee/en/eli/521012014004/consolide in English).

48 Complaint of H.P for annulment of electronic votes cast in the *Riigikogu* elections 2011. 23.03.2011 Judgement 3-4-1-6-11 (available at www.nc.ee/?id=1255 in English).

49 See also a description of the Internet Voting procedure at https://www.valimised.ee/eng/juhis, accessed 1 August 2014.

50 On page 12 of the judgement of the Estonian Supreme Court case 3-4-1-6-11 [2011] (available at www.nc.ee/?id=1255 in English).

> hardware, operating systems, screen resolutions or fonts. However, achieving such compatibility may be complicated in isolated cases. In case of problems, the voter has the possibility to seek advice from the e-voting technical support. If the technical problems arising during e-voting cannot be eliminated in isolated cases, the voter has the possibility to vote by means of a ballot paper.

Therefore, ensuring the compliance of the computer with the I-voting application is clearly left to the user. Indirectly the court approved the parliament's liberal approach to voting: the voters themselves decide whether to vote, how to vote and which channels to use. The state's responsibility is to offer a possibility, an alternative, but keeping in mind that it is just one of the possible ways.

The same idea of procedural liberty is also found in the first constitutional review case in 2005 and has been accepted not only in matters of elections. Overall, this idea takes note of the general notion of digital solutions in a society where a traditional form of conduct (like the paper based signature) is enhanced by an e-version (like the digital signature). Both forms are equally legally accepted and it is up to the user to find the most suitable method at a given time and place.

The case of P.P vs National Electoral Committee[51] *and the case of T.R. vs National Electoral Committee*[52]

The security analysis of the I-voting concept[53] states clearly that one of the fundamental security problems with e-enabled voting is the necessity to trust the voters' computer. The central system is and can be protected by the state. The spread of malware in private computers on the other hand cannot easily be limited – either by state or by private efforts. The analysis even states that the modern personal computer is a 'black box' that nobody can or is able to control. Therefore, the security of the computer where the voting application is run remains a real issue. The user themselves can of course take actions in protecting their computers, but nevertheless this cannot solve all possible consequences. Consequently the security of the voting application is a topic that requires extra attention.

The issue of security thus stood out prominently during the 2011 elections where a computer enthusiast (P.P) hacked his own vote in his own voting application on his own computer. He was able to modify his own vote in his own computer and create an illusion that the vote was not sent to the central system. He was also keen to go public with his discovery (to national media) and later bring the issue up to the Supreme Court. It is important to say that all the discovered problems and

51 The Estonian Supreme Court case 3-4-1-4-11 [2011] (http://www.nc.ee/?id=1243 in English).

52 The Estonian Supreme Court case 3-4-1-7-11 [2011] (www.nc.ee/?id=1256 in English).

53 The security analysis is available at the NEC website, http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf, accessed 1 August 2014.

situations were monitored in the central system by the administrators and were noticed. Moreover, the revealed threats had been discussed already in the 2003 security analysis.

Subsequently, the Supreme Court looked at the issue of the security of the technical solution of I-voting in two separate but similarly motivated judgments.

In the case of P.P (3-4-1-4-11) the court makes a compelling statement[54] that knowingly manipulating his own vote cannot be seen as proof of the overall lack in security of the I-voting system. Looking at an analogy with traditional voting, a voter could easily go to the polling booth and turn in an invalid polling paper (by scrapping or doodling on the paper etc.). That is a conscious decision and is totally legitimate. Here are some excerpts from the decision.[55]

> As it appears from the memorandum, P.P. has conducted an experiment with the full awareness and consent of the test subjects proving, according to P.P., that the electronic voting in Riigikogu elections was unsafe as described above. The Chamber presumes that P.P. participated as a test subject in the experiment organised by himself. As it appears from the circumstances described by P.P., the test subjects had to, in the opinion of the Chamber, be aware that they were casting their vote via a computer infected with a virus.
>
> Pursuant to Art 72 and Art 70 of the Riigikogu Election Act, a complaint can be filed only for the protection of the person's own violated rights. Therefore, the 8 March 2011 complaint of P.P. cannot be filed for the protection of the rights of the other persons who participated in the experiment.
>
> On the basis of the circumstances presented in the memorandum and the 8 March complaint of P.P., the possible participation of P.P. himself in the described experiment cannot violate his right to vote. Namely, a person with the right to choose a voting channel has, by infecting his or her computer with a virus blocking the transmission of 'a vote unsuitable for the virus', put him or herself knowingly in a position where the electronic vote cast by him or her will not be delivered to the National Electoral Committee.

The case presented by T.R (3-4-1-7-11) is based on the same arguments presented by P.P but with more emphasis on the general implication of the security of

54 The Estonian Supreme Court case 3-4-1-4-11 [2011] (http://www.nc.ee/?id=1243 in English).

55 Points 16–18 of the judgement.

I-voting.[56] The general notion of the court is similar to that in the case of P.P, however noting,[57]

> Regarding the argument of T.R. about the non-safety of the e-voting, a hypothetical possibility that someone has monitored, changed or affected in any other way his voting during the election process, as well as a similar hypothetical possibility that the electronic vote cast by him has not been delivered to the specified destination or has not been received, cannot be the reason for satisfaction of the complaint of T.R. even if he himself voted electronically. A prerequisite for declaring the voting results invalid is an established violation of the voter's rights.

The same reasoning was used by the court in a similar case in 2013,[58] where similar arguments were presented.

The problem with evidence

Finding evidence to prove the breach of I-voters' rights is as difficult as in all areas covered by anonymity of the vote. The aspect of verification gives rise to additional case handling problems. On the one hand the electoral administration receives additional information about possible attacks against networks and individual computers; on the other hand it evokes a lot of confusion and may generate questions about the secrecy of the vote.

Consider claims such as: it was not possible for the voter to vote for the desired candidate because of administrative errors; votes were counted incorrectly or not tallied at all; the voting or election result is ascertained incorrectly. These all have to be proven by documents, statements, survey results etc. For those claims the applicant has to be able to credibly demonstrate the violation of his/her rights. On the other hand, the National Electoral Commission and the Supreme Court have to be able to check the election administration activities, including the fact that the I-voting system is operating correctly. Therefore, it has to ensure that the accuracy and stability of the system have been reliably established based on an audit and/or inspection (testing) prior to the start, during and after voting. In the future, the handling of incidents in a more thorough implementation of vote verification[59] has to be able to produce court-approved evidence.

---

56 E.g. the IP address of the voter is at some point tied to the person's vote whereas it could not be ruled out that such information would be used by the organizers; also no specific verification method is available.

57 In point 9 of the judgement.

58 The Estonian Supreme Court case 3-4-1-57-13 [2013] (http://www.nc.ee/?id=11&tekst=RK/3-4-1-57-13 in Estonian).

59 Although first steps with 'cast as intended' and 'accepted as cast' verification as a pilot were introduced in 2013.

We have to agree to the fact, or even the paradox of electoral disputes, that because of the anonymity and secrecy of voting it is often very difficult or even impossible to assess the accuracy of the presented claims. This problem affects not only I-voting, but also paper ballot voting. You can check the correct functioning of the overall system, however not the operation and 'destiny' of a single vote. For example, statements that a vote sent by mail has been lost or somehow altered can only be proven based on information collected under covert surveillance in a criminal investigation or proven by actual witnesses.

A vote shall be annulled only if the infringement found affected or could have affected the election results.

The Supreme Court has emphasized that hypothetical (unproven) suspicions are not enough to declare any results invalid, as this would violate the rights of other voters and candidates. The court has also emphasized the responsibility of the voter: the number of the candidate written on the ballot has to be clearly understandable; the ballot must be equipped with the required information etc. In the case of I-voting, the voter must take care of the computer and the security settings, and, if necessary, ask for technical support in case of problems, or ultimately use the option to vote in the traditional way at a polling station.

Taking into account the tight time-frame between elections, it would be difficult to find a domestic or international public body that would be ready to certify and audit all the elements of the entire I-voting system before, during and after election procedures. In Estonia, the electoral organization performs operational tests in order to check the functionality and accuracy of the system. Furthermore, independent and public testing (demo voting) takes place, and a third party audits the operational procedures that have been carried out.[60]

The Estonian I-voting system was developed following the principle that all components of the system must be transparent for audit purposes. Procedures should be fully documented and critical procedures should be logged, audited, observed and videotaped as they are conducted. A common requirement is that the source code of the voting application should be available for auditing. The source code of the Estonian I-voting system was made public in 2013.[61] It was not universally available before but could have been audited[62] if agreed by the NEC.

As a rule the process audit is carried out by external internationally certified IT auditors. The audit reviews and monitors sensitive aspects of the process, such as updating the voter list, the preparation of hardware and its installation, the loading

60 There has been a computer-science based study on the risks of Estonian I-voting (see Springall, et al, 2014) that was, however, heavily criticised by the Estonian authorities (see e.g. http://www.vvk.ee/valimiste-korraldamine/vvk-uudised/vabariigi-valimiskomisjoni-vastulause-the-guardianis-ilmunud-artiklile/, accessed 1 May 2015 or https://www.ria.ee/e-voting-is-too-secure/ , accessed 1 May 2015)

61 The source code can be found at: https://github.com/vvk-ehk/evalimine, accessed 1 August 2014.

62 Although this possibility was not used before the publication of the source code.

of election data, the maintenance and renewal of election data and the process of counting the votes, etc. At the counting event on Election Day, auditors publicly declare their opinion about the soundness of the procedures used by the electoral administration up to that point. The auditors' report, released after all procedures (including the destruction of all voting equipment including I-votes) have been completed, states if the I-voting procedures followed the rules described in the system's documentation and the integrity and confidentiality of the system was not endangered. To date all reports have been positive.

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 stages, the I-voting system produces different logs on received, cancelled and counted votes, also invalid and valid votes. The Audit Application enables one 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 they can use to ensure that the system is working correctly.

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. I-voting is no different. All significant documents concerning the I-voting system are public. In order to enhance the observers' knowledge of the system, political parties are invited to take part in a training course before each election in which I-voting is used. Besides political parties, auditors and other persons interested in the I-voting system take part in the training. In addition, observers are invited to follow the test of the whole process and to take part in other preparatory procedures. However, few political parties have so far exercised their opportunity to observe the I-voting procedures.[63] 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, then conclusions cannot be made about the integrity of the system.

Conclusion

In the case of I-voting almost all principles of democratic elections give rise to several questions in constitutional law and broader questions in social sciences.

In Estonia, as well as in many other countries that have created and allowed postal voting, advance voting and other supplementary voting channels, voting at a polling station has virtually lost its significance as a ritual of transforming people into a nation-state and a carrier of sovereign nationhood.

63 See Epp Maaten and Thad Hall, 'Improving the Transparency of Remote I-voting: The Estonian Experience' in Robert Krimmer and Rüdiger Grimm (eds), *Electronic Voting 2008* (Bonn: Gesellschaft für Informatik, 2008).

The Estonian Supreme Court has analysed in its constitutional review process the accordance of Internet voting with the principle of equality. The centre of the argument lies in the question whether the I-voters' ability to change the I-vote by voting again electronically or on paper would give unconstitutional advantages.

Additionally, guaranteeing the freedom and secrecy of vote in an uncontrolled environment was examined. Based on the remote nature, one of the cornerstones of the freedom of vote – mandatory privacy in the voting process – is not applicable in Internet-based remote voting. The two sub-principles of secrecy of voting were analysed – privacy of the voting act and anonymity of the vote. The court explained that to be found constitutional, Internet voting should include a 'virtual voting booth' alternative, the possibility to change the vote in case of infringement of the secrecy of the voting act. It is important to emphasize that the constitutionality of the Internet as a communication channel, together with possible threats on anonymity and secrecy, has not yet been analysed by the Estonian Supreme court.

The second broader category of discussions on Internet voting have taken place in the Constitutional Chamber of the Supreme Court following specific electoral complaints. The principles of equality, secrecy, technical uniformity and security of online voting have been raised in the complaints. One of the main issues that has arisen in these cases is how to obtain applicable and sufficient evidence, which is conceptually difficult due to the anonymity of the vote. New forms of evidence were raised in those cases, like documented test runs of the system, audited processes and verification of the vote.

So far the Supreme Court been quite innovative and liberal in its I-voting electoral complaint judgements, however, granting that the election organizers have done their best in avoiding any malpractice. It remains to be see whether this balance will continue in future cases.

Estonia is one of the (yet) few countries that has had a lot of experience in conducting e-enabled elections, the most important reason being the presence of a working e-ID solution but also the overall support of the general public. The case history in Estonia, both in constitutional review and electoral cases, has after seven successful applications of the concept shown support for the chosen principles. However, although Internet voting has so far been immune to some incremental flaws compared to some otherwise very popular voting channels (e.g. postal voting), the rapid development of the Internet as a communication channel could possibly bring new concerns that could also be held up in court.

Consequently, any new threats and I-voting itself belong both to the information society and it is the task of election organizers and courts to adjust the solutions to netizens' needs.

References

Hubertus Buchstein, 'Online Democracy, Is it Viable? Is it Desirable? I-voting and Normative Democratic Theory' in Norbert Kersting and Harald Baldersheim (eds), *Electronic Voting and Democracy: A Comparative Analysis* (Basingstoke: Macmillan, 2004).

Wolfgang Drechsler and Ülle Madise, 'Electronic Voting in Estonia' in Norbert Kersting. and Harald Baldersheim (eds), *Electronic Voting and Democracy: A Comparative Analysis* (Basingstoke: Macmillan, 2004).

Michael Hauben and Ronda Hauben, *Netizens: On the History and Impact of Usenet and the Internet* (Los Alamitos, CA: IEEE Computer Society Press, 1997).

Sven Heiberg, Peeter Laud and Jan Villemson, 'The Application of I-voting for Estonian Parliamentary Elections of 2011' in Aggelos Kiyaias and Helger Lipmaa (eds), *E-voting and Identity* (Dordrecht: Springer, 2012).

Alo Heinsalu, Arne Koitmäe, Mihkel Pilving and Priit Vinkel, 'Elections in Estonia 1992–2011' [2012] National Electoral Committee and National Library, http://issuu.com/vabariigi_valimiskomisjon/docs/elections_in_estonia_1992-2011_eng/1, accessed 1 August 2014.

Mieke Loncke and Jos Dumortier, 'Online Voting: A Legal Perspective' [2004] *International Review of Law, Computers and Technology*, (18)1.

Epp Maaten and Thad Hall, 'Improving the Transparency of Remote I-voting: The Estonian Experience' in Robert Krimmer and Rüdiger Grimm (eds), *Electronic Voting 2008* (Bonn: Gesellschaft für Informatik, 2008).

Ülle Madise and Epp Maaten, 'I-voting in Estonia' in David Rios Insua and Simon French (eds), *E-Democracy: A Group Decision and Negotiation Perspective* (Dordrecht: Springer, 2010).

Ülle Madise and Tarvi Martens, 'E-voting in Estonia 2005: The First Practice of Country-wide Binding I-voting in the World' in Robert Krimmer (ed.), *Electronic Voting 2006: 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.cc* (Bonn: Gesellschaft für Informatik, 2006).

Ülle Madise and Priit Vinkel, 'Constitutionality of Remote I-voting: The Estonian Perspective' [2011] *Juridica International*, 18.

Sutton Meagher, 'When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights' [2008] *American University International Law Review*, 23.

OSCE Office for Democratic Institutions and Human Rights, Estonia Parliamentary Elections; OSCE/ODIHR Election Assessment Mission Report (March 6, 2011).

Gerhard Skagestein, Are Vegard Haug, Einar Nodtvedt and Judith Rossebo, 'How to Create Trust in Electronic Voting over an Untrusted Platform' in Robert Krimmer (ed.), *Electronic Voting 2006: 2nd International Workshop Co-*

organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.cc (Bonn: Gesellschaft für Informatik, 2006).

Springall, D.; Finkenauer, T.; Durumeric, Z.; Kitcat, J.; Hursti, H.; MacAlpine, M.; Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security'. 703-715.

Ene-Margit Tiit, 'Estonian Census 2011' [2013] *Papers on Anthropology*, 22.

Alexander Trechsel, *Internet Voting in the March 2007 Parliamentary Elections in Estonia: Report for the Council of Europe* (2007), http://www.vvk.ee/public/dok/CoE_and_NEC_Report_EVoting_2007.pdf, accessed 1 August 2014.

Alexander Trechsel and Kristjan Vassil, *Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005* (Council of Europe and European University Institute, 2011), http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf, accessed 1 August 2014.

Kristjan Vassil and Till Weber, 'A Bottleneck Model of E-voting: Why Technology Fails to Boost Turnout' [2011] *New Media and Society*, 13(8).

Priit Vinkel, 'I-voting in Estonia' in Peeter Laud (ed.), *Lecture Notes in Computer Science: NordSec 2011, Tallinn, Estonia 26–28 October 2011* (Berlin: Springer, 2012).

Thomas C. Wingfield and Eneken Tikk, 'Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen' [2010] *International Cyber Security: Legal and Policy Proceedings* (Tallinn: CCD COE Publications).

IV Ülle Madise and **Priit Vinkel**. 2014. "Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections." In Tanel Kerikmäe (ed.). *Regulating eTechnologies in the European Union*. Cham: Springer International, 1-19. (3.1)

Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections

Ülle Madise and Priit Vinkel

Abstract Remote Internet voting has been allowed in Estonia since 2005 in all types of public elections. The share of online voters has risen to 20–25 %. According to surveys, Internet voting slightly increases general voter turnout, contrary to common expectations does not favor well-educated young urban population and is politically neutral. Significant factors predicting the use of Internet as a voting channel are computer skills and trust. The constitutionality of online voting and of postal voting lends itself to similar analysis with the exception of Internet as a channel. We argue that Internet voting is constitutional, if reliable remote authentication, electronic voter roll, and control mechanisms preventing from any kind of manipulation are in place: the I-votes must be cast as intended, stored as cast, and counted as recorded. In an advanced information society, online voting could be even seen as a required means of guaranteeing universal suffrage and voting equality. On the other hand, the impact of remote e-services on human psychology and behavior needs further research. The results of such scholarly work might lead to new arguments in legal analysis as well.

1 Introduction

Estonia is credited as a front-runner country in matters of e-governance with its universal electronic key to all e-services (e-ID), digital signature, e-Health, e-taxboard, etc. According to the latest *Global Information Technology Report 2013*,

Ü. Madise (✉)
Institute of Constitutional and International Law, University of Tartu, Tartu, Estonia
e-mail: ylle.madise@ut.ee

P. Vinkel
Ragnar Nurkse School of Innovation and Governance, Tallinn University of Technology, Tallinn, Estonia
e-mail: priit.vinkel@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_4

Estonia ranks as the highest Central and Eastern European country, in 22nd place.[1] The use of electronic means for claiming different services has steadily risen in the country, and a large amount of e-services are provided both by the public and the private sectors. About 77 % of Estonian inhabitants aged 16–74 use regularly Internet and 80 % of households have access to the Internet.[2]

While, in many states, the first step toward some form of electronic vote was to use voting machines in polling stations in order to facilitate voting or counting, in Estonia, from the beginning, there was the aim of creating conditions for public and accessible remote Internet voting. Similar projects of introducing binding remote electronic voting for general elections have evolved the most in Switzerland[3] and Norway,[4] but also in Catalonia, United Kingdom, Finland, Canada, and other.[5]

I-voting has stood beside a number of other voting methods in Estonia since 2005.[6] For six times, Estonian voters have had the choice of casting a paper vote or vote over the Internet at parliamentary, municipal, and European Parliament elections.

The declared aim of the launching of online voting in Estonia was to increase voter turnout, which perhaps could be described more realistically as widening access possibilities and stopping the decrease in participation, especially among younger voters.[7] The participation rate at local government council elections in Estonia is usually ~50 % and at parliamentary elections ~10 % higher. Voter turnout never exceeded 70 %, even at the 1992 constitutional referendum. By facilitating electoral participation, it seemed likely that voter turnout, and hence the overall legitimacy of the results, would improve.

Another reason behind the I-voting project was the wish of exploiting the existing infrastructure more efficiently. The widespread use of the national e-ID card was vital for starting the Internet voting project, as only e-ID card owners had the option of voting through the Internet. In 2012, the national ID card celebrated its 10-year anniversary and currently 1.2 million people possess a valid ID card, of those 85 % are Estonian citizens; thus, most of the eligible voters (~1 million) hold the card.

Moreover, according to some commentators, an important factor explaining the possibility to launch totally new solutions like I-voting in Estonia is the smallness of the country.[8]

---

[1] See the World Economic Forum (2013).

[2] As shown by Eurostat (2013).

[3] They have had numerous trials both on cantonal and federal levels. For an overview, see Maurer et al. (2012) and Gerlach and Gasser (2009).

[4] Norway has used Internet voting in two elections. See the OSCE report on Norwegian parliamentary elections 2013 at http://www.osce.org/odihr/elections/109517.

[5] The concept on electronic voting harbors both machine e-voting and remote Internet voting. An overview of the use cases can be found in Barrat et al. (2012).

[6] For a complex overview of Estonian elections after the restoration of independence, see Heinsalu et al. (2012).

[7] See Drechsler and Madise (2004).

[8] For context, see Kalvet (2012) and Kattel et al. (2011).

2 Starting Out

In 2001, discussions among political and academic groups started about whether or not Estonia should introduce Internet voting. At the same time, the Ministry of Justice announced intentions to introduce Internet voting as soon as possible.

A political agreement was reached in 2002, and in 2003, the National Electoral Committee (NEC) started the electronic voting project. At the beginning of the project, the NEC involved as many IT security specialists as possible to elaborate a commonly acceptable approach and, thereby, raise public trust in Internet voting. Good cooperation between different parties, public or private, was crucial in launching the successful and apolitical I-voting project.

I-voting project's executive group was formed by NEC, a project manager was elected, and the roles between the NEC, executive group, and project manager were distributed. In accordance with the project organization, the NEC approved the more relevant decisions. The task of the executive group was to make proposals and recommendations to the NEC and control the achieving of set objectives. The project manager was in charge of the implementation of the project, and he summoned project groups formed by experts upon necessity, directed their work, and checked the results.

At this stage, the I-voting concept was essentially complete. After that, the security analysis of the concept was carried out by a working group formed of IT security specialists. Proceeding from the recommendations of the security analysis, changes were made to the concept and the document entitled General Description of Estonia's E-Voting Project was presented.[9]

Early in 2004, the technical description of the I-voting software was produced. In March 2004, three tenders were submitted and the NEC chose the Cybernetica Ltd as a software developer, a cooperation that has lasted until today. In autumn, the software was ready for the first public pilot. The pilot offered the possibility of I-voting in a Tallinn residents' poll, it took place in January 2005. About 703 voters were participated, and 697 votes were counted. The system worked without failures. After the pilot was completed, the I-voting system seemed in place and ready to be used in the local elections of autumn 2005.[10]

3 Laying the Legal Ground

3.1 Parliamentary Debates About I-Voting

The scope of the parliamentary debate before launching I-voting was quite wide, ranging from clear ideological questions to detailed technological issues.[11] The most discussed question was the exact meaning and purpose of the principle of

[9] Latest version available at www.vvk.ee.

[10] For detailed elaboration of project management, see Madise and Maaten (2010).

[11] See about the genesis of the Estonian I-voting project with references to the minutes of *Riigikogu* plenary sessions, party structure, etc., in Drechsler and Madise (2004).

secrecy. Other important questions were the digital divide and the value of the ritual of walking into a polling station.

In Estonia, as well as in many other countries that have created and allowed remote voting possibilities (e.g., postal voting), advance voting, and other supplementary voting methods to meet contemporary mobile voters requirements, voting at a polling division has virtually lost its significance as a ritual transforming people into a nation-state and the carriers of sovereign nationhood.[12]

In the discussion about the introduction of I-voting, classical arguments about conformity of the I-voting with the principles of fair elections including the reliability of electronic voting systems were changed, whereby one of the arguments against I-voting was that people who have no commitment neither to prepare themselves for election nor go to the polling station to execute their citizen's duty should not participate in governing at all,[13] which contradicts the axiom that the higher the turnout, the better.[14] Indeed, the discussions were dominated by clear liberal democracy approach in the way as Robert A. Dahl puts it: if we accept the desirability of political equality, then every citizen must have an equal and effective opportunity to vote and all votes must be counted as equal. Viable democracy requires not only constitutional right to vote but also factual freedom of information and expression, civic education, etc.[15]

The principles of free and fair elections—especially universal suffrage and equality—cannot be followed if electoral administration is not adapted to changes in the society.

The legislative process in the Estonian parliament concerning Internet voting has had three stages. In 2002, only the concept of remote voting possibility was adopted. The main idea was to have enough in the law to guarantee public funding for the early-stage project. In 2005, right before the first implementation at the local government council elections, detailed provisions were entered into electoral acts. In 2012, after five cases of using Internet voting in different elections, more precise and accustomed regulations based on the previous experience were adopted. Additionally, the concept of verification was introduced.

It is likely that while deciding whether to support electronic voting, political parties took into account the potential effect of remote Internet voting over their election results. Parties suppose that I-voting brings persons to vote who would by traditional means not participate, and additional votes will not be distributed proportionally among political parties. So it seems likely that increased turnout changes the share of votes between political parties.[16] Of course, such kinds of considerations contradict the principle of universal suffrage and are rare if at all

[12] About the importance of the voting ritual, see, e.g., Monnoyer-Smith (2006).

[13] For reasons of the attitude that it might be better for democracy if some of votes were not cast at all, see, e.g., Buchstein (2004, p. 55).

[14] Explaining electoral turnout is never a simple task, see, e.g., Rolfe (2012).

[15] Dahl (1998, p. 80 and p. 95).

[16] See Madise (2008).

publicly exposed. One hint to calculations of that kind could be the condition added to electoral legislation that I-voting cannot be launched before the year 2005. In 2003, Estonian people voted in a referendum on EU accession.

3.2 Teleological Interpretation of the Principle of Secrecy

According to the Estonian Constitution, members of the *Riigikogu*, as well as local government councils shall be elected in free, general, equal and direct elections, and voting shall be secret.[17] The same principles apply to European Parliament elections. There is no special regulation for I-voting in the constitution.

The secrecy of voting has traditionally been viewed in Estonia as the right and obligation to cast one's vote alone in a voting booth. In the case of Internet voting, the state is not in a 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 subprinciples—private proceeding of voting and anonymity of vote—is required to ensure free voting and is not an objective per se.

The voter's right to anonymity during the counting of the votes is guaranteed to the extent to which this can be secured in the case of absentee ballots by mail; the so-called system of two envelopes used for absentee ballots by mail is both reliable and easy to understand for I-voters (see Sect. 5.2).

Remote Internet voting requires rethinking the privacy principle. The principle of privacy is there to protect an individual from any pressure or influence against her or his free expression of political preference. Such teleological approach to the constitution was the basis of the I-voting provisions from the very beginning of the whole project. In addition to the teleological interpretation of the constitution, the Ministry of Justice, led by the liberal Reform Party, based provisions enabling Internet voting on the premise that the state has to trust the individual and avoid, whenever possible, interference with decision making at the individual level. The individual has to be aware of risks, i.e., technical risks, and he or she has to have the right to decide whether or not to use the Internet voting opportunity.[18]

This teleological interpretation of the principle of secrecy is clearly divergent from the traditional approach generally adopted in the scholarly literature. For instance, Buchstein[19] remarks that

> Mandatory secrecy is a principle which goes beyond constitutional law, its fundaments are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption. In this concept, it is not the individual him- or herself, but a warranted outside agent or authority – normally the state – that is responsible for providing the necessary means to allow for the secret ballot.

[17] Articles 60 and 156.

[18] See Drechsler and Madise (2004).

[19] In Buchstein (2004).

> Indeed, in many countries, the privacy of voting act is not required nor protected in such a strict way: the voters are not required to hide their choice and traditionally they do not; in some countries, proxy voting is allowed.

In Estonia, unlike in some countries, the fact whether a person entitled to vote did participate in voting or not is not regarded as a part of the principle of secrecy. The voter lists that contain information about participation and chosen voting method (voting on voting day or advance vote in or outside polling stations of one's place of residence, in case of advance vote paper ballot or I-vote) are preserved in an archive and can be used for research purposes. Researchers have made use of this possibility, including for the I-voting survey, what unfortunately weakened somewhat the public trust against I-voting. The fact that the official questioner had knowledge about the actual fact of I-voting made some people suspect about the secrecy of their voting decision. These suspicions were discussed in public media but due to satisfying explanation, the common trust was not harmed.[20] The explanation was that voters' lists have always had the stated information about who participated and what voting method was used. The voting decision itself has always been and will remain secret. There is no possibility to obtain any knowledge about how the voter voted.[21]

3.3 Virtual Voting Booth as a Required Guarantee for Free Elections

In order to guarantee the freedom of voting, I-voters were granted the right to replace the vote cast on the Internet by another I-vote or a paper ballot. However, this could be done only within the advance polling days. In case of several I-votes, only the last one is counted; in case of contest between I-vote and paper ballot, the paper ballot was counted. If several paper ballots are cast, all votes are declared invalid. Thus, the "one vote—one voter" principle is ostensibly guaranteed.

This approach caused perplexity among the audience of the report presented by Madise at the Worldwide Forum on e-Democracy in Paris in 2001, and even in 2005. However, at the International Seminar held in Bregenz in 2006, Norwegian scholars remarked *inter alia* that they had arrived at similar principles before obtaining detailed knowledge about the Estonian Internet voting system[22] and expressed clear support for the vote replacement aspect of this idea.

---

[20] The survey results are encompassed in the Council of Europe study report accessible here: http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/evoting_documentation/PDF-FinalReportCOE_EvotingEstonia2005.pdf.

[21] Due to the technical and procedural aspects explained in Chap. 4.

[22] See Skagestein et al. (2006).

Some months before the municipal elections in 2005, the President of Estonia brought I-voting provisions to the Supreme Court for constitutional review, arguing that the possibility to change I-votes gives advantages to I-voters in comparison with non-I-voters. I-voters can change their vote for an unlimited number of times but only during I-voting and advance poll days. The initial version of the I-voting law contained the possibility to change the I-vote with a paper ballot on the actual voting day. This provision was left out of the law, because this could have given real advantage to I-voters: they would have had the chance to change their election preference on Sunday after receiving additional information about candidates in the second half of the week. All voters who use advance poll possibilities (either paper- or I-voting) were now formally in the same conditions.

The Supreme Court Chamber of Constitutional Review pointed out that despite "virtual voting booth," there was no possibility of the voter affecting the voting results to a greater degree than those voters who used other voting methods. From the point of view of the voting results, this vote was in no way more influential than the votes given by paper ballot. According to the Estonian Election law, each voter shall have one vote.

The court said that this interpretation renders the principle of uniform elections a special case of the general right to equality. In the legal sense, I-voting is equally accessible to all voters. The ID card necessary for I-voting is mandatory for all inhabitants of Estonia; thus, the state has created no legal obstacles for anyone to I-vote, including to changing one's vote during the advance poll days. It is a fact that due to factual inequality the possibility to change one's vote through I-voting is not accessible to all voters can be regarded as an infringement of the general right to equality and the principle of uniformity.

The principle of equal treatment in the context of electing representative bodies does not mean that factually equal possibilities for performing the voting act in equal manner should be guaranteed to all persons entitled to vote. In fact, those who use different voting methods provided by law are in different situation. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the constitution. The aim to increase voter turnout is without any doubt legitimate. The measures the state takes for ensuring the possibility to vote for as many voters as possible are justified and advisable. Another aim of allowing I-voting is the modernization of voting practices that coincides with the aims of I-voting listed in the OSCE Recommendation.[23]

According to the opinion of the Supreme Court of Estonia, the principle of 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 the necessary prerequisites to carry out free polling and to protect voters from undesired pressure while making a voting decision. In paragraph 30 of the aforementioned judgment, the Supreme Court maintains the following:

[23] Rec (2004).

> The voter's possibility to change the vote given by electronic means, during 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 watched 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 of changing 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 have a 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.[24]

The Supreme Court thus confirmed the constitutionality of one of the main premises of the remote Internet voting project. The concept of teleological approach and acceptance of the used methods of I-voting has stood the bar also in subsequent cases in the Estonian Supreme court.[25]

3.4 Second Round of Parliamentary Debates: Stored as Intended Verification of I-Votes from 2015

As in 2011 the percentage of I-votes had risen to almost a quarter of valid votes, Parliament decided to specify the norms of I-voting in electoral laws in order to improve the legitimacy and transparency of I-voting. Until 2011, the I-voting procedures had only very brief legislative regulations. Parliament established a working group that, in addition to detail procedures, had to propose a solution, how to raise auditability and how to verify the correctness of I-votes.

At the same time, technical community, which has been involved by NEC in discussions about the security of I-voting, came to conclusion that a new mechanism for some level of verification is needed, in order to detect malicious attacks on the I-voting system. NEC and electronic voting committee (EVC) have better options to discover attacks and react to those if I-voters, even a relatively small amount of them, verify their votes. If somebody finds out and reports to NEC or EVC that his/her vote is not stored correctly, measures could be taken immediately. If voters would only have access to their personal computers and use them for verification, no security could be achieved at all. Therefore, some independent

---

[24] Chamber of Constitutional Review of the Estonian Supreme Court, Decision Nr 3-4-1-13-05. See http://www.nc.ee/?id=11&tekst=RK/3-4-1-13-05 (in Estonian).

[25] Namely cases 3-4-1-10-11 from March 31, 2011, see http://www.nc.ee/?id=11&tekst=RK/3-4-1-10-11 (in Estonian) and 3-4-1-4-11 from March 21, 2011 http://www.nc.ee/?id=11&tekst=RK/3-4-1-4-11 (in Estonian).

channels like mobile phones or mobile devices, which are easily accessible by the voters, are needed for verification.[26]

In the end of 2012 Parliament adopted, the amendments to the electoral law stating that a new electoral committee—EVC—to be created for technical conducting of I-voting. The first elections where the EVC was active were 2013 local elections. The law also regulates that before every implementation the I-voting system must be tested and audited. Most significant change in the law was the statement that from 2015, voters have to have possibility to check that their vote has reached and is stored at the central server of elections and reflects the choice of the voter correctly.

4 Technical Solution and Practical Experience

4.1 e-ID Card as an Universal Access Key to e-Services

Some of the biggest challenges in the sphere of e-Government are the reliable remote identification and authentication of citizens.[27] Simple password-based authentication methods are not secure enough.[28] Estonia chose the electronic ID card as main authentication tool. Although many states across the world already have some form of identity card schemes in place, few are based on electronic cards. However, in Estonia ID card, enabling secure personal authentication and digital signing, as well as the public key infrastructure (PKI) necessary for using ID cards electronically, had been developed already by the end of 2001.

Issued by the Estonian Government since January 2002, national ID cards represent the primary source of personal identification for people living within Estonia and are mandatory for all citizens and resident aliens above 15. The ID card carries two functions: physical identity as a regular ID and electronic identity that enables citizens to use the same card to electronically authenticate to Web sites and networks, and/or digitally sign communications and transactions as required.

Each 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 contain no restrictions of 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. As mentioned before, the card can be also used for the 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.

---

[26] See Heiberg et al. (2010).

[27] See also Chap. 3 in Nyman-Metcalf (2014).

[28] See also Heiberg et al. (2012).

In 2007, a new e-ID solution was brought to the Estonian market: the Mobile-ID, where the mobile telephone (via its SIM card) acts as an ID card and a card reader at the same time. In addition to having the functionality of an ordinary SIM, a Mobile-ID SIM holds a person's certificates that enable providers of Internet services to identify the person and issue digital signatures. From 2011, Mobile-ID certificates have governmental guarantee and the solution can be used in Internet voting.[29]

4.2 Technical Measures Used to Ensure Voting Secrecy

One of the main interests of those interested in the security of Internet voting systems is the obvious contradiction of security and secrecy properties. On one hand, the votes must remain anonymous. On the other, voters must be identified in order to guarantee that only the eligible voters are able to vote and that they vote only once.

In order to understand how the I-voting system guarantees the secrecy and singularity of vote, we should describe shortly the envelope voting method used in Estonia for advance paper voting.[30] The latter gives the voter possibility to vote outside the polling station of the voter's residence in any rural municipality or city. A voter presents a document to be entered in the list of voters and then receives the ballot and two envelopes. The inner envelope has no information about the identity of the voter, and the ballot paper is put in it. The inner envelope is put into an outer envelope and the voter's details are written on it, so that, after the end of the advance poll, the envelope could be delivered to the voter's polling station of residence. There it is verified whether the voter has the right to vote; then, the inner envelope is taken out and put unopened into the ballot box. The two-envelope system guarantees that the voter's choice remains secret. Additionally, recording the data about envelope I-voting in the list of voters in the polling station of residence prevents voting more than once (Fig. 1).

Upon I-voting, a voter makes her or his choice, which is encoded (placed in a virtual inner envelope). Thereafter, the voter shall approve the choice through his or her digital signature, which means that personal data are added to the encoded vote (the outer envelope). The personal data and the encoded vote are stored together until the counting of votes on Election Day, with the aim of ascertaining that the person has given only one vote.

The personal data of a voter and the vote given by the voter are separated after the fact that the voter has given only one vote has been checked and repeated votes

[29] See also Heiberg et al. (2012), and for the statistical use of mobile-ID in elections, see http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/.

[30] A system very similar to the advance voting procedure in Sweden (see http://www.val.se/pdf/Elections_in_sweden_2014_webb.pdf) and Finland (see http://www.finlex.fi/fi/laki/kaannokset/1998/en19980714.pdf).

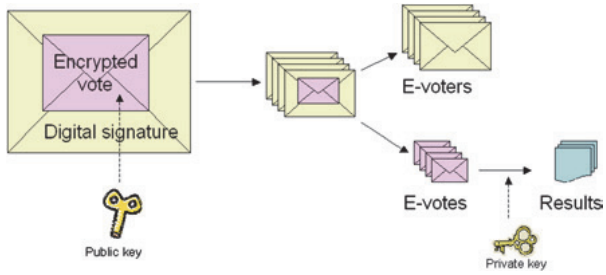


Fig. 1 Double-virtual envelope PKI-based method for I-voting

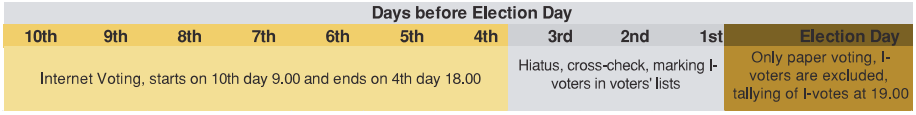


Fig. 2 I-voting event cycle

have been eliminated. It is then possible to open the inner envelope only after the personal data added to the encoded vote have been separated.

I-voting, like voting outside the polling station of residence, is possible only during advance polls. This is necessary to guarantee that, in the end, only one vote is counted for each voter. During the I-voting process, the voter's right to vote is checked. If the voter makes use of the possibility to replace his or her I-vote by paper ballot during the advance poll, then it has to be guaranteed that finally only one vote is counted. For that, all polling stations are informed of the I-voters on their voters' rolls after the end of advance polling and before the Election Day on Sunday. If it is found at the polling station that the voter has voted both electronically and with paper ballot, the information is sent to the central system and the voter's I-vote is cancelled by the EVC (Fig. 2).

Before the tallying of voting results in the evening of the Election Day, the encrypted votes and the digital signatures with personal data or inner and outer envelopes are separated. Then, all I-votes are opened by the EVC and counted. The system opens the votes only if they are not connected to any personal data.

4.3 System Architecture

The Estonian IT security experts in their security analysis[31] published in 2003 declared that in *practical sense* the Estonian I-voting system was secure enough for implementation. In absolutely secure systems, unexpected events are not

[31] Available at www.vvk.ee.

possible. One may dream about such systems, but they can never be achieved in practice.[32] This applies particularly to I-voting systems. Considering the security level of personal computers, it is impossible to design I-voting systems, which are absolutely secure for every user. The most important security goal of voting is not to affect the final results and not to abuse the principles of democracy. The single incidents with users are still important, but they do not have influence to the final result. Moreover, even in traditional voting systems, small-scale incidents are acceptable.[33]

I-voting part in the whole process of organizing elections is relatively small. The system uses existing information systems—population register as basis for voters' lists,[34] election information system of the NEC for the collection and publication of information on candidates, and voting results and the infrastructure of Certification Centre Ltd for checking the validity of the ID card certificates.

The main components of the Estonian I-voting systems are a stand-alone voter application for casting the vote; the vote forwarding server; the vote storing server; the vote counting server; and the monitoring (log-file) server.[35]

Asymmetric cryptography is used to guarantee the secrecy of votes. A pair of keys is generated for the system in a special hardware security module so that its private component never leaves it. The public component of the pair of keys is integrated into the voter application and is used to encrypt the votes. The private component of the pair of keys is used in the vote counting application to open the votes on the end of the Election Day. The NEC can decrypt the votes, i.e., use the private component, only collegially. After the end of the period of dealing with possible complaints, the private key is destroyed.

4.4 Users' Perspective

The Internet voting system takes advantage of the existing infrastructure and governmental databases. To vote electronically, a voter does not need to register himself or herself additionally. The voter needs an ID card and a computer connected to the Internet and with an installed card reader (not necessary if using Mobile-ID). The voter also needs PIN codes for authentication and signing. He can use the same tools for other transactions, including governmental e-services and Internet banking.

---

[32] As stated by Mägi (2007).

[33] See also Madise and Martens (2006).

[34] In Estonia, voters' lists are generated based on Population Register data, no separate registration procedures are necessary.

[35] More on the technical structure of the system can be found in the General Description (2010) at http://www.vvk.ee/voting-methods-in-estonia/engindex/reports-about-internet-voting-in-estonia/ and various technical documents (in Estonian) at http://www.vvk.ee/valijale/e-haaletamine/e-dokumendid/.

From the user's perspective, the voting procedure looks like this:

1. The voter opens the voting page www.valimised.ee.
2. The voter must choose how to identify him/herself (by using an ID card or Mobile-ID).
3. After that, voter inserts the ID card into the universal card reader and inserts PIN1 of the ID card or enters PIN1 on the mobile phone in case of Mobile-ID.
4. The server checks whether the voter is eligible (using the data from the population register).
5. The candidate list of the appropriate electoral district is displayed.
6. The voter makes his/her voting decision; the system encrypts it.
7. The voter confirms his/her choice with a digital signature by entering PIN2 of the ID card or Mobile-ID. The system checks whether the same person who authenticated him/herself during the start of the session gave the according digital signature. Also, the validity of the digital signature is confirmed by the validity confirmation server.
8. The system confirms that the vote has been stored in the vote storing server.

In the 2013 municipal elections, the NEC and EVC ran a pilot on verification: for the first time, voters had the possibility to verify whether their I-vote arrived in the central server as intended. In order to check the vote, voter must have a smart device (mobile phone or a tablet) that has a camera, Internet connection, and a special application downloaded from the Internet. Right after the voting procedure, a QR code will be displayed on the voting computer screen. The voter must now open the special application in the smart device and point the camera at the QR code on the screen. After reading the code, the application contacts the central server of elections and downloads the encrypted (secret) e-vote of the voter. In a few seconds, the voter's choice appears on the smart device screen and the voter can check whether his vote has reached the central server of elections and reflects the choice correctly.[36]

4.5 Impact and Analysis After Six Cases of I-Voting

The impact of I-voting and other important e-services (signing digitally contracts without seeing each other, etc.) on human behavior and psychology needs further research.[37]

[36] More on the pilot on I-voting Web page www.valimised.ee and on the Norwegian experience with verification see Ansper et al. (2009) and the OSCE mission report 2013 at http://www.osce.org/odihr/elections/109517.

[37] For a first insight with the topic, refer to Anu Realo's work in the latest survey by Trechsel and Vassil (2011).

So far, we can use statistics and the results of surveys conducted at European University Institute and Tartu University.[38]

One cannot avoid the question of whether Internet-based voting exacerbates the difference in representation possibility within social groups. What is clear is that Internet-based voting removes physical barriers hindering participation in elections of the aged, disabled or other groups with restricted mobility, or who have difficulty in attending polling stations (e.g., persons having tight work schedules or working, studying or traveling abroad, parents of small children, and persons living in regions with poor infrastructure), assuming, of course, that these people have access to the Internet.

Trechsel et al. concluded in their reports prepared for the Council of Europe following the experience of the Internet voting from 2005 to 2011 that education and income, as well as type of settlement, have been insignificant factors while choosing the Internet from other voting channels. One of the most important findings of the studies until the 2009 elections has been that it is not so much the cleavage between the Internet access haves and access have-nots, but clearly computing skills and frequency of the Internet use have been important predictors of choosing Internet voting. However, since 2009 local elections where more than 100,000 voters used Internet voting, those factors have faded away. Trust in the I-voting procedure has been throughout the years the most significant factor that directs voters' decisions to use or not I-voting.[39]

The actual impact of Internet voting on the change in turnout does not lend itself to objective analysis. One can determine the variations of turnout in different election years (comparing equivalent types of elections) and attempt to clarify the causes underpinning variations with the help of sociological studies. Perhaps, the most important question is what share of the electorate would not have participated in the voting, had the Internet voting opportunity not been provided. There is no really reliable way of obtaining empirical evidence. We must, therefore, come to terms with unverifiable claims made by the voters themselves. The only exception is the case when Internet voting is the only possibility for the elector to vote and he or she uses this possibility. For example, the local government council elections in Estonia do not provide for voting abroad by postal ballot or at a diplomatic representation. Nonetheless, they do envisage the possibility of voting on the Internet (Table 1).[40]

The most intriguing question for political parties is probably the impact of the use of I-voting on results. Although parties favoring I-voting have gathered through the years, most of the I-votes,[41] the studies show that left–right auto-positioning does not play any important role while choosing a voting channel.[42]

---

[38] For the full list of reports, turn to http://www.vvk.ee/voting-methods-in-estonia/engindex/reports-about-internet-voting-in-estonia/.

[39] See Trechsel and Vassil (2011).

[40] See Madise and Vinkel (2011).

[41] Ibid.

[42] In Trechsel and Vassil (2011).

Table 1 I-voting statistics 2005–2013

	2005 LE	2007 PE	2009 EPE	2009 LE	2011 PE	2013 LE
I-votes	9,681	31,064	59,579	106,786	145,230	136,863
Repeated I-votes	364	789	910	2,373	4,384	3,045
I-voters	9,317	30,275	58,669	104,413	140,846	133,808
I-votes cancelled by paper ballot	30	32	55	100	82	146
I-votes counted	9,287	30,243	58,614	104,313	140,764	133,662
Valid votes cast	496,336	550,213	396,982	658,213	575,133	625,336
% of I-votes	1.9 %	5.5 %	14.8 %	15.8 %	24.5 %	21.4 %
I-votes among advance votes	7.2 %	17.6 %	45.4 %	44 %	56.4 %	50.5 %
I-votes cast abroad	n.a	2%	3%	2.8 %	3.9 %	4.2 %

LE—local (municipal) elections
PE—parliamentary elections
EPE—elections to the European parliament

In 2005, the I-voting seems to have had a slight effect on the increase in the turnout of the voters who sometimes vote and sometimes not.[43] In 2007, already approximately 10 % of the questioned I-voters said that they certainly or probably would not have voted without having had the possibility to vote via the Internet. Trechsel and Vassil show (in 2011) that the percentage of the I-voters questioned who certainly or probably would not have voted without having had the possibility to vote via the Internet has risen to 16.3 %, which allows the conclusion that the overall turnout might have been as much as 2.6 % lower in the absence of such a method of voting. That is already a significant marker when one looks at the impact of Internet voting on the overall turnout.

Three cases of Estonian I-voting in 2013 (LE), 2014 (EP), and 2015 (PE) will also be analyzed by experts of the University of Tartu. This research offers unique prolonged insight into the development of such voting method throughout the years

Approximately one-fifth of the questioned non-I-voters pointed out that a reason for not I-voting was the sufficiency of the paper ballot system. Lack of trust with 3.2 % and absurdity of I-voting with 1.9 % were not dominant reasons. Prior to the actual I-voting, there was a concern that the possibility to change the I-vote is going to be misused. It was not the case. The general statistics shows that the number of amended I-votes was insignificant. 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. If we consider the experience of voters in the I-voting experiences, we see that there is little evidence of coercion or concerns about privacy, based on voters' behavior. The small percentages of repeated votes as well

[43] See Breuer and Trechsel (2006).

as the significant increase on the total number of I-voters throughout the years indicate that the confidence in the existing I-voting system has grown.

The hypothesis that I-voting rewards advantages to urban electorate found no proof. Gender is not an important factor when choosing I-voting from possible voting channels. Age, on the contrary, is quite an important factor: most I-voters in all elections belong to the age group 18–39. Furthermore, an interesting analysis of the impact of I-voting on turnout and the role of voters who otherwise do not engage in public matters has been composed by Vassil and Weber.[44]

However, the legitimacy of Internet voting cannot be judged solely on the basis of its impact on political alienation. The legitimacy and constitutionality of Internet voting as well as its impact on democracy are only briefly discussed. It is too early to make strong statements on that topic—on one hand, the remote Internet voting experience has too thin a basis for that, and on the other, the socio-political environment is steadily changing.

4.6 Challenges: Transparency

How to create trust and guarantee the transparency of electronic voting? Although the risks mentioned above are handled, one should take into account that it is always possible to threaten legitimacy of the voting result without any objective cause. Therefore, it is crucial to shape I-voting procedures as transparent and simple as only possible and foresee several reliable control methods.

Simple methods have been used in Estonia to increase voter understanding and confidence on the I-voting system in an attempt to overcome any concerns about the lack of transparency and complexity. In all elections in which I-voting was 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 acquisition of the hardware and software needed to use an ID card on a personal computer, updating expired ID card or Mobile-ID certificates, and the renewal of PIN codes needed for electronic use of the ID card or Mobile-ID.

As an additional element of transparency, the number of I-voters who had cast ballots was updated regularly on the I-voting Web site. This very simple process allowed the wider national audience, as well as the political parties and media, know how many I-voters had voted and determine whether the trend in the number of I-voters casting ballots seemed reasonable. In the end, people were also able to compare the number of I-voters with the number of I-votes counted.

---

[44] See Vassil and Weber (2011).

In order to convince voters that their votes had been correctly registered, voters had an option to check whether their valid I-vote had been reflected on the polling lists on Election Day in order the prevent voting more than once. A second option for verifying the correctness of a valid I-vote was possible during I-voting period. If the voter decided to replace the I-vote with a new one, he got a notification of an earlier recorded I-vote.

4.7 Challenges: Observation

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 were 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. Besides political parties, auditors and other persons interested in the I-voting system also took part in the training, which was followed by surveys of concrete procedures that were necessary for a setup of the I-voting system. Observers were invited also to a test of the counting process.

Throughout the I-voting observation period of 1 month, the main observation tool was the checking of activities of the EVC 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 the counting event—the highlight of the election period—the management of the systems' private key, which is the warranty of the electoral secrecy, was demonstrated to observers. This key, split in seven pieces, was hold by the NEC, and its members opened collegially the anonymous encrypted votes. The process of counting of ballots was 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 cannot be made. Especially for foreign observers, the length of the observation period appears to be a challenge. The OSCE did audits in the 2007 and 2011 elections and in its last report states "The OSCE in general found widespread trust in the conduct of the Internet voting by the NEC. However, /…/ more detailed and formal control of software installation and reporting on testing of the Internet voting system could further increase transparency and verifiability of the process."[45]

[45] The OSCE/ODIHR Election Assessment Mission Report, Estonia, Parliamentary Elections, March 6, 2011 is available at http://www.osce.org/odihr/77557.

4.8 Challenges: Validating the Voting Systems and Procedures

In order to validate the electronic voting system, certification procedures, testing, and audits should be considered. Currently, there is no domestic or international body that is able to certify the Estonian I-voting system. Estonia instead uses a system similar to that used in other countries (and similar cases), where the source code of the system is auditable and the operational procedures have been under keen supervision of auditors. System testing prior to elections is also an important part in order to control the functionality and accuracy by contracted testers, observers, and by public.

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 are fully documented and critical procedures are logged, audited, observed, and videotaped[46] as they are conducted. The procedure-audit,[47] conducted in every election, reviews and monitors security sensitive aspects of the process, 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.[48]

A common requirement is that the source code of a voting system should be available for public auditing. In Estonia, though, until 2013, the code was not universally available but one could access it if signing a NDA with the NEC. However, after the second legal debates mentioned earlier, in 2013, the source code of all central servers of the voting system as well as the software of the vote verification application was made available in Internet.[49] This is an important step for bringing more transparency and thus more trust toward the very concept of I-voting.

5 Conclusions

Estonia has been one of the first countries in the world where Internet voting with binding results has successfully been used countrywide. The whole Estonian electorate has had six times the possibility of casting the vote via Internet in local (2005, 2009, and 2013), parliamentary (2007 and 2011), and European Parliament elections (2009). Having I-voting constitutes a genuine qualitative change in the development of the electoral system and electoral administration. The Estonian I-voting experience shows that it is possible to ensure the conformity of remote I-voting with all constitutional electoral principles, including the principle of secrecy.

---

[46] Since 2013 also published on Youtube at http://www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ.

[47] The scope of the audit is to ensure the validity of performed procedures compared to the handbooks and technical documentation of I-voting. The audit is procured separately for every election by the NEC, the auditors must present a CISA certificate.

[48] See also Vinkel (2012).

[49] You can access the source code at https://github.com/vvk-ehk/evalimine.

The e-ID card, being a primary identification document in Estonia with its two mandatory functions—remote authentication and digital signature—as universal access key to all e-services has been the cornerstone of Internet voting. Reliable identification of the voter as well the anonymity of the vote and correct counting of the votes can thus be secured.

As long as universal Internet access and secure authentication of the voters is not guaranteed, the doubts related to the political neutrality of this technique will probably remain. Nevertheless, I-voting should be regarded as an essential public service in an information society. Issues related to voting machines (as faced in many countries like United States, Germany, or the Netherlands) should certainly not be extended to remote Internet voting.

In an advanced information society, online voting could be even seen as a required means of guaranteeing uniformity of voting. It gives access in elections to citizens who are temporarily working, living, traveling, or studying abroad. Therefore, it might be an important general e-service for guaranteeing free movement inside European Union. Would returning to the traditional voting channels harm free movement of Estonian people, goods and services inside EU?

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 any specific country, taking into account the political tradition and social culture, level of technological infrastructure, and the electoral system of the respective country. In the Estonian case, the preconditions were favorable and time was just right for introducing the most ambitious change in the nature of voting—voting over Internet.

References

Ansper, A., Heiberg, S., Lipmaa, H., Øverland, T. A., & van Laenen, F. (2009). Security and trust for the Norwegian E-voting pilot project E-valg 2011. In A. Jøsang, T. Maseng, & S. J. Knapskog (Eds.), *Lecture notes in computer science*, *5838, NordSec 2009, Oslo, October 14–16, 2009* (pp. 207–222). Berlin: Springer.

Barrat, J., Goldsmith, B., & Turner, J. (2012). *International experience with E-voting*. Washington: IFES foundation.

Breuer, F., & Trechsel, A. H. (2006). E-*voting in the 2005 local elections in Estonia: Report for the council of Europe*. Available at the Estonian National Electoral Committee website www.vvk.ee. Accessed January 2014.

Buchstein, H. (2004). Online democracy, is it viable? Is it desirable? Internet voting and normative democratic theory. In N. Kersting & H. Baldersheim (Eds.), *Electronic voting and democracy. A comparative analysis* (pp. 39–58). Basingstoke: Palgrave Macmillan.

Dahl, R. A. (1998). *On democracy* (p. 95). New Haven and London: Yale University Press.

Drechsler, W., & Madise, Ü. (2004). Electronic voting in Estonia. In N. Kersting & H. Baldersheim (Eds.), *Electronic voting and democracy. A comparative analysis* (pp. 97–108). Basingstoke: Palgrave Macmillan.

Eurostat. (2013). *Survey on individuals regularly using the Internet and on households—level of Internet access*.

Gerlach, J., & Gasser, U. (2009) *Three case studies from Switzerland: E-voting*. Internet and democracy case study series. Berkman Center Research Publications.

Heiberg, S., Laud, P., & Villemson, J. (2012). The application of I-voting for Estonian parliamentary elections of 2011 In: A. Kiyaias & H. Lipmaa (Eds.), *Postproceedings of the 3rd International Conference on E-voting and Identity, Tallinn, September 29–30, 2011. Lecture Notes in Computer Science, 7187* (pp. 208–223). Berlin: Springer.

Heiberg, S., Lipmaa, H., & van Laenen, F. (2010). On E-vote integrity in the case of malicious voter computers. In D. Gritzalis & B. Preneel (Eds.), *Computer security—ESORICS 2010: Esorics 2010*, Athens, September 20–22, 2010 (pp. 373–388). Berlin: Springer.

Heinsalu, A., Koitmäe, A., Pilving, M., & Vinkel, P. (2012). *Elections in Estonia 1992–2011*. Tallinn: National Library of Estonia.

Kalvet, T. (2012). Innovation: A factor explaining e–government success in Estonia. *Electronic Government, An International Journal, 9*(2), 142–157.

Kattel, R., Randma-Liiv, T., & Kalvet, T. (2011). Small states, innovation and administrative capacity. In V. Bekkers, J. Edelenbos & B. Steijn (Eds.), *Innovation in the public sector: Linking capacity and leadership.* Basingstoke: Palgrave Macmillan.

Madise, Ü. (2008). Legal and political aspects of the Internet voting: Estonian case. In J. M. Reniu (Ed.), *E-voting: the last electoral revolution* (pp. 45–59). Barcelona: Institut de Ciències Politiques i Socials.

Madise, Ü., & Maaten, E. (2010). Internet voting in Estonia. In D. R. Insua & S. French (Eds.), *e-Democracy: A group decision and negotiation perspective* (pp. 301–321). Berlin: Springer.

Madise, Ü., & Martens, T. (2006). I-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 15–26). Bonn: Gesellschaft für Informatik.

Madise, Ü., & Vinkel, P. (2011). *Constitutionality of remote internet voting: The Estonian perspective*. In *Juridica International*, *18*, 4–16.

Mägi, T. (2007). *Practical security analysis of I-voting systems*. Available at http://triinu.net/e-voting. Accessed January 2014.

Maurer, A., Spycher, O., Taglioni, G., & Weber, A. (2012). E-voting for Swiss abroad: A joint project between the confederation and the cantons. In *Electronic voting 2012* (pp. 173–187). Bonn: Gesellschaft für Informatik.

Monnoyer-Smith, L. (2006). How I-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 61–68). Bonn: Gesellschaft für Informatik.

Nyman-Metcalf, K. (2014). E-governance in law and by law. The legal framework of e-governance. In *E-technology in the EU: Normative Realities and Trends.*

Rolfe, M. (2012). *Voter turnout: A social theory of political participation*. Cambridge: Cambridge University Press.

Recommendation Rec. (2004). '*Legal, operational and technical standards for I-voting' of the council of Europe*. Available at http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/key_documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf. Accessed January, 2014.

Skagestein, G., Haug, A. V., Nødtvedt, E., & Rossebø, J. (2006). How to create trust in electronic voting over an untrusted platform. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 107–116). Bonn: Gesellschaft für Informatik.

Trechsel, A. & Vassil, K. (2011). *Internet voting in Estonia: A comparative analysis of five elections since 2005*. European University Institute 2011. Available at the Estonian National Electoral Committee website www.vvk.ee. Accessed January, 2014.

Vassil, K., & Weber, T. (2011). A bottelneck model of E-voting: Why technology fails to boost turnout. *New Media & Society,* 1–19. Accessed 23 Jun 2011

Vinkel, P. (2012). Internet voting in Estonia. In p. Laud (Ed.), *Lecture notes in computer science, NordSec 2011, Tallinn, Estonia October 26–28, 2011* (pp. 4–12). Berlin: Springer.

World Economic Forum. (2013). *The global information technology report 2013*. Available at World Economic Forum website http://www.weforum.org/reports/global-information-technology-report-2013. Accessed January, 2014.

V Priit Vinkel. 2012. "Internet Voting: Experiences from Five Elections in Estonia." In T. Jundzis (ed.). *Proceedings of the International Conference: Democracy and Development – Taiwan and Baltic Countries in Comparative Perspective, 27-28 April 2012*. Riga: Latvian Academy of Sciences, 176-188. (3.1)

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.

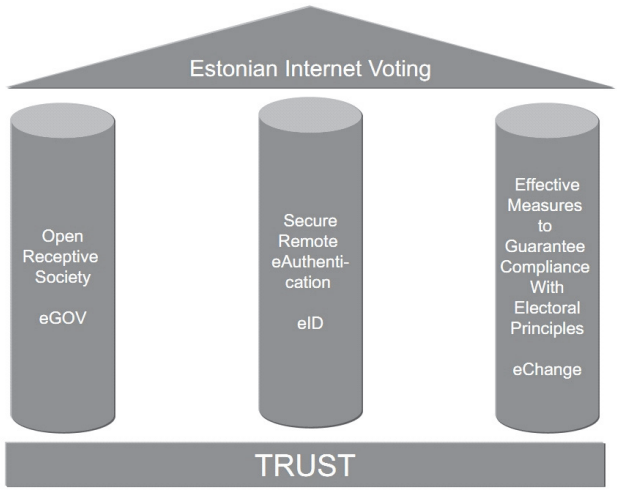


Fig. 1. Three pillars of Estonian Internet Voting

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.

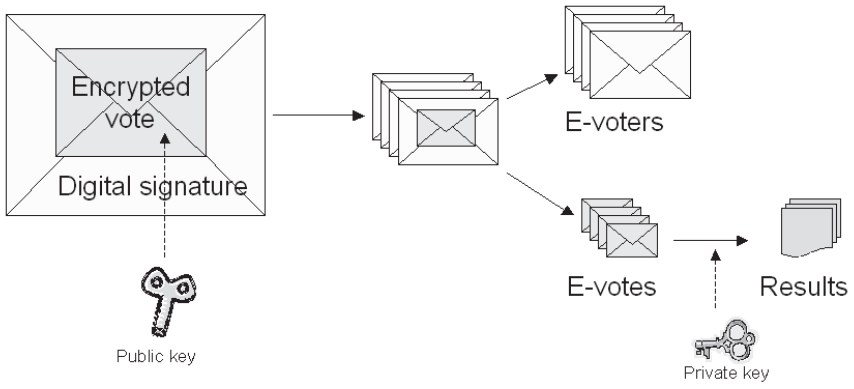


Fig. 2. Double envelope system used in Internet Voting

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.

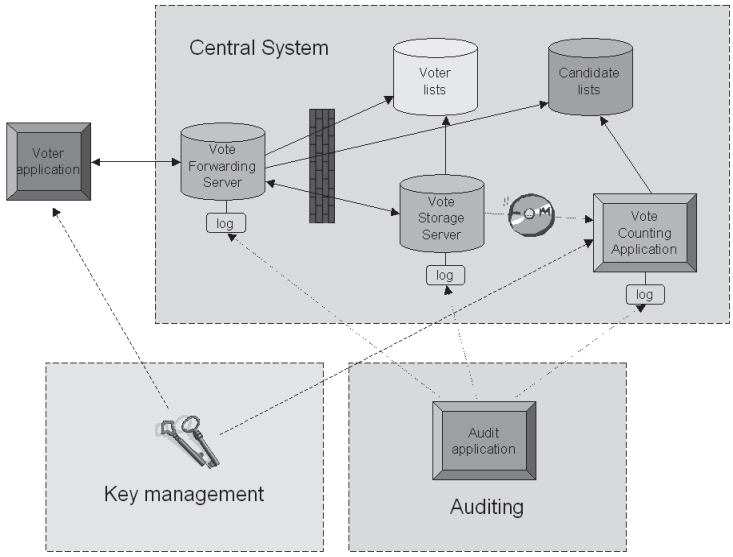


Fig. 3. The general architecture of the Internet Voting system

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.

VI Ülle Madise and **Priit Vinkel**. 2010. “TIC, votacions per Internet i altres serveis electronics a Estonia.” In J. Vall (ed.). *EINES 12, Politica 2.0*. Barcelona: Fundacio Josep Irla, 59-67. (3.2)

TIC, votacions per Internet i altres serveis electrònics a Estònia

VISTA PRÈVIA

La ciutadania electrònica i la identitat virtual són la base d'un dels països més joves de la UE. I és que amb menys de 20 anys, Estònia ha passat de ser una república asfixiada per la Unió Soviètica a ser un dels països capdavanters en la introducció de les tecnologies de la informació i la comunicació en els afers públics, esdevenint tot un referent en l'administració i el vot electrònic.

Nota: Els autors agraeixen els bons consells del professor Jordi Barrat de la Universitat d'Alacant.

Introducció

Per als que no estiguin familiaritzats amb Estònia, pot ser-los útil saber que va ser una república independent entre 1919 i 1940, i que després de l'ocupació soviètica va formar part de la Unió de Repúbliques Socialistes Soviètiques (URSS), fins que recobrà la independència el 1991. Des del 2004 el país és membre de la Unió Europea (UE) i de l'Organització del Tractat de l'Atlàntic Nord (OTAN).[1]

Estònia és una democràcia parlamentària, els 101 membres del parlament monocameral —Riigikogu— són elegits a través d'un sistema electoral proporcional, donant lloc normalment a governs de coalició de dos o més partits. El cap d'Estat és el President, que té les principals obligacions representatives.

La República d'Estònia actualment té aproximadament 1.350.000 habitants, repartits en 45.227 km^2.[2] Segons *The Global Information Technology Report 2009-2010*,[3] en la categoria d'èxit governamental en la promoció de les TIC, Estònia es disputa l'onzè lloc amb altres gegants de les tecnologies de la informació com els Estats Units d'Amèrica (EUA), Corea del Sud o el Japó; pel que fa a proveir qualitat en línia en els serveis públics, Estònia comparteix

1 Per a més informació sobre la història, la cultura i la societat vegeu *Estonica*, l'enciclopèdia electrònica d'Estònia.

2 L'*State Portal* ofereix informació oficial sobre la República d'Estònia i l'accés a molts serveis electrònics públics. http://www.eesti.ee/eng/

3 http://www.weforum.org/documents/GITR10/index.html

Ülle Madise
Professora de Dret Públic
a la Tallinna Tehnikaülikool
ylle.madise@vpk.ee

Priit Vinkel
Professor ajudant de Dret Públic
a la Tallinna Tehnikaülikool
priit.vinkel@ttu.ee

» Estònia és l'onzè país en la categoria d'èxit governamental en la promoció de les TIC i el tercer en presència de les TIC en agències governamentals

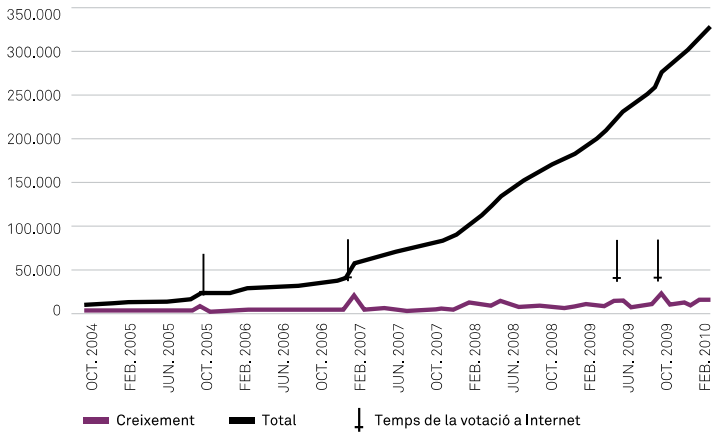
les posicions 26-28 amb Hongria i Irlanda; en la categoria de presència de les TIC en agències governamentals, els tres primers llocs són per a Singapur, Suècia i Estònia. De fet, des de l'1 de juny de 2010, fins i tot el butlletí oficial de l'Estat —*State Gazette*— és totalment electrònic, fet que significa que totes les decisions legals es publiquen només a Internet.[4]

Un factor important que explica la possibilitat d'apostar per solucions totalment noves com la identitat virtual oficial o la votació electrònica és la dimensió del país. Lennart Meri (1929-2006), l'últim president de la República d'Estònia, el 6 d'abril del 2000, va comparar Estònia, en un discurs que va donar al St. Olaf College de Minnesota, amb un vaixell petit: «Un supervaixell cisterna necessita setze milles marines per a canviar el seu curs. Estònia, al contrari, és com un caiac d'esquimal, capaç de canviar el seu curs a l'instant».

4 https://www.riigiteataja.ee/ert/ert.jsp

Gràfica 01

Creixement de la funcionalitat de la identificació electrònica



Font: Elaboració pròpia

Identitat oficial virtual: la identificació electrònica

La pedra angular de la majoria de serveis electrònics, tant públics com privats, és la identificació electrònica.[5] Des del 2002, la targeta d'identificació és el principal document d'identificació de nova generació, esdevenint obligatori. Les targetes d'identificació són creades pel Govern i contenen certificats d'autentificació remota i la signatura digital. Tota la ciutadania estoniana i els residents estrangers que tenen més de quinze anys han de tenir una targeta d'identificació electrònica.

Cada targeta d'identificació conté dos certificats d'infraestructures de claus públiques digitals bàsics —un per a l'autentificació i l'altre per a la signatura digital. Els certificats només contenen el nom i el codi personal del titular i tenen dues claus privades associades a la targeta, cadascuna protegida per un únic PIN d'usuari. Els certificats no contenen cap restricció d'ús: són de caràcter universal i poden ser utilitzats en qualsevol tipus de comunicació, ja sigui entre

5 Vegeu informació detallada sobre la identificació electrònica a http://www.id.ee/?lang=en

Un factor important que explica la possibilitat d'apostar per solucions totalment noves com la identitat virtual o la votació electrònica és la reduïda dimensió del país «

particulars, organitzacions o en l'àmbit del govern. La targeta d'identificació electrònica també es pot utilitzar per a l'encriptació de documents de manera que només la persona a qui va adreçat el document pugui descodificar-lo. Aquest és un mitjà eficaç per al trasllat segur de documents que utilitzen xarxes públiques. A més a més, cada targeta d'identificació conté totes les dades que s'han publicat en relació a aquella identitat.

El nombre de targetes d'identificació va excedir el juny del 2010 el 1.100.000. Més de dues terceres parts dels titulars han utilitzat la targeta d'identificació electrònica per a la identificació personal remota i més d'un ters per fer una signatura digital. Cal tenir en compte que la votació per Internet ha promogut molt l'ús electrònic de la targeta d'identificació —veure gràfica 1. Un altre factor de promoció important ha estat l'acord entre bancs per permetre moviments bancaris per Internet només amb la targeta d'identificació.

Per utilitzar la targeta d'identificació, a més d'un lector de targetes intel·ligents i d'un ordinador amb el programari pertinent —que es pot descarregar lliurement des d'una pàgina web[6]—, es necessita una connexió a Internet i el sistema operatiu de Windows, Mac o Linux. Fa un parell d'anys es va presentar una nova proposta al mercat, la identificació mòbil, a partir de la qual un telèfon mòbil actua com a targeta d'identificació i lector de targetes al mateix temps. A més de la funcionalitat d'una SIM corrent, una SIM d'identificació mòbil també aporta una identitat mòbil de les persones que permet als proveïdors dels serveis d'Internet identificar la persona i donar-li signatures digitals. La funcionalitat de la identificació personal i de la signatura digital queden assegurades mitjançant l'actualització de la tecnologia de la seguretat i el número d'identificació personal corresponent. Amb aquesta proposta ja no és necessària una targeta de lectura connectada a un ordinador alhora que permet realitzar les mateixes funcions: escriure en bases de dades, bancs virtuals... i signar diversos contractes digitalment.

A la pràctica, la identificació electrònica s'utilitza per a l'autentificació de l'usuari en diverses bases de dades com: el portal de recerca estonià, que reuneix tots els investigadors, els seus projectes científics, les seves publicacions...; l'*State Portal*, que ofereix un centre de serveis electrònics; com a tiquet electrònic en el transport públic; com a eina legal d'identificació de clients en unes quantes empreses privades; i, fins i tot, per a la introducció de comentaris al diari en línia *Eesti Päevaleht*,[7] que ha prohibit comentaris anònims per evitar casos de difamació.

El debat parlamentari sobre la targeta d'identificació electrònica va generar alguns dubtes sobre la privacitat i la seguretat, però els partits que donaven suport a la identificació electrònica obligatòria van obtenir la majoria de vots. Les preguntes més controvertides eren el possible risc de robatori d'identitat i la seguretat de les tecnologies de la informació en general. Per a evitar la utilització de la targeta d'identificació per part d'una altra persona, es van afegir les corresponents modificacions del Codi Penal. Segons la llei, l'ús fraudulent de la targeta d'identificació és punible amb una sanció pecuniària o fins a tres anys de presó. L'ús de la identificació electrònica s'està eixamplant constantment, encara que no s'hagin portat a terme els propòsits inicials de combinar la identificació electrònica amb tots els altres documents possibles, com el permís de conduir.

Votació per Internet[8]

Estònia és el primer país del món on s'ha implementat amb èxit la votació re-

6 https://installer.id.ee

7 www.epl.ee

8 Per una exposició més detallada, vegeu MADISE, «Legal and political aspects of Internet voting: Estonian case», p. 45-59.

» Tota la ciutadania estoniana i els residents estrangers que tenen més de quinze anys han de tenir una targeta d'identificació electrònica

mota per Internet amb resultats vinculants en les eleccions municipals (2005 i 2009), legislatives (2007) i al Parlament Europeu (2009).[9] La raó per implementar la votació per Internet a Estònia no era tant la necessitat de millorar el procés de recompte de vots —el qual ja era suficientment ràpid i transparent—, sinó la voluntat de proporcionar un canal addicional i convenient per votar, per mantenir els votants existents i per captar els dels més joves.[10]

Enfocament teològic del principi de la inviolabilitat de la identitat

El secret de votació s'ha vinculat tradicionalment a Estònia amb el dret i l'obligació d'emetre el vot de manera individual en una cabina electoral. En el cas de la votació per Internet, l'Estat no pot assegurar la privacitat del procediment. Els legisladors van interpretar la Constitució en relació al secret de votació i, atenent als seus dos subprincipis —el procediment privat de votació i l'anonimat del vot—, s'exigeix assegurar la votació lliure, sense que es tracti d'un objectiu *per se*. Conseqüentment, es poden adaptar instruments destinats a assegurar el secret, amb la condició que es doni als votants l'oportunitat de votar lliurement a favor del seu partit preferit sense témer que se'l condemni o sense esperar-ne una aprovació moral o una recompensa material.

El caràcter anònim del votant és garantit durant el recompte de vots fins al punt que es pot assegurar tant com en el cas de les votacions per correu postal; l'anomenat «sistema de dos sobres», utilitzat per a les votacions per correu postal, és tan fiable com fàcil d'entendre per als votants electrònics. L'esquema de sobre doble conegut a través de la votació per correu en alguns països garanteix el secret de vot. L'elecció dels votants és encriptada per l'aplicació de votació (per exemple el votant segella l'elecció en un sobre en blanc interior) i llavors el signa digitalment (per exemple, fica el sobre interior dins del més gran i hi escriu el seu nom i la seva adreça). Els vots signats i encriptats (sobres exteriors) es recullen al lloc central per comprovar i assegurar que es comptarà només un vot per votant. Abans de comptar-los, es treuen les signatures digitals amb les dades personals (sobres exteriors), i els vots encriptats anònims (sobres interiors) es posen a l'urna per tal de fer el recompte.

L'esquema utilitza una criptografia d'accés públic que consta d'un parell de claus —una clau privada i una pública. Quan el vot s'encripta amb una clau pública llavors només es pot descodificar amb la clau privada corresponent. El Comitè Electoral Nacional, que té la clau privada, col·legialment obre els vots encriptats d'Internet el dia de l'elecció.

Per garantir la llibertat de vot, es concedeix als votants electrònics el dret de tornar a votar electrònicament un nombre il·limitat de vegades i de rectificar el vot emès per Internet per un vot en paper. Tanmateix, això només es pot fer durant la votació anticipada. En cas de diversos vots electrònics, només es dóna per vàlid l'últim; en cas de vot electrònic i un vot en paper, el vot en paper és el que es dóna per vàlid. Si s'emeten uns quants vots en paper, tots els vots es declaren nuls. Així, es garanteix, aparentment, el principi «un votant - un vot».

En el cas de la votació per Internet, la possibilitat de canviar un vot no és només permissible, sinó que és una obligació constitucional. Segons l'opinió de la Cort Suprema d'Estònia, el principi de la llibertat de vot genera l'obligació de l'Estat de protegir als votants de les persones que intenten influir en la seva elecció. Pel que fa a aquest principi, cal que l'Estat creï els requisits previs ne-

9 Tota la informació sobre la votació per Internet, inclosos els articles, enquestes, decisions legals, estadístiques... estan disponibles a la web del Comitè Electoral Nacional: http://www.vvk.ee

10 Les discussions parlamentàries es descriuen a Drechsler i MADISE,«Electronic Voting in Estonia», p. 97-108.

Estònia és el primer país del món on s'ha implementat amb èxit la votació remota per Internet

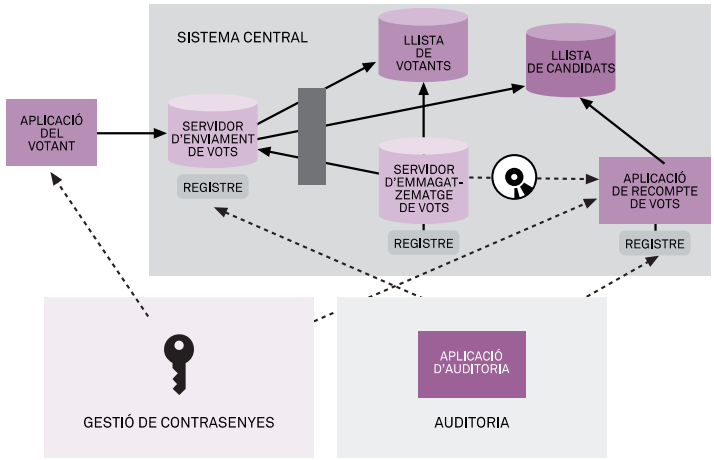
cessaris per tal de garantir la votació lliure i protegir als votants de qualsevol pressió indesitjada mentre prenen la decisió de votació. En el judici, la Cort Suprema manté la següent postura: «La possibilitat del votant de canviar el vot emès electrònicament durant les votacions anticipades, constitueix una garantia suplementària essencial per a l'observança del principi d'eleccions lliures i de votació secreta emesa electrònicament. Un votant que ha estat influït il·legalment o que ha estat observat durant una votació electrònica, pot restaurar la seva lliure elecció i el secret de votació votant una altra vegada, tant electrònicament com mitjançant un vot en paper, un cop alliberat de les influències. A més de la possibilitat de posteriorment rectificar el vot emès sota influència, la possibilitat de votar una altra vegada ofereix una funció preventiva important. Si la llei dóna garanties a un votant amb el vot electrònic, la possibilitat de canviar el vot emès electrònicament comporta que la motivació per influir-lo il·legalment disminueix. No hi ha altres mesures que siguin igual d'eficaces, apart de la possibilitat de canviar el vot emès electrònicament, per garantir la llibertat d'elecció i el secret de votació a través de la votació electrònica en un mitjà incontrolat. Les sancions de dret penal tenen el seu vessant preventiu i el subsegüent càstig —a diferència de la possibilitat de canviar el vot electrònic de cadascú— no ajuda a eliminar una violació de la llibertat d'elecció i del secret de votació.» La Cort Suprema confirmava així la constitucionalitat d'una de les principals premisses del projecte de votació remota per Internet.

Configuració del sistema de vot electrònic

Els principals components del sistema de votació per Internet estonià són l'aplicació del votant, el servidor d'enviament de vots i la gestió interna, que es divideix en dos espais: el servidor d'emmagatzematge de vots i el servidor de recompte de vots. L'aplicació dels votants és una aplicació web per

Diagrama 01

Sistema de votació electrònica



Font: Elaboració pròpia

» La raó per implementar la votació per Internet a Estònia és la voluntat de mantenir els votants existents i per captar els més joves

emetre vots. Els processos del servidor d'enviament de vots són l'autentificació, la comprovació del dret de vot, l'enviament de les candidatures als votants, i la recepció signada i encriptada dels vots. El servidor de xarxa immediatament transfereix els vots encriptats rebuts al servidor d'emmagatzematge de vots i transposa el reconeixement de recepció del servidor d'emmagatzematge dels vots als votants. El servidor de xarxa completa la feina quan el període de votació per Internet s'acaba.

El servidor d'emmagatzematge de vots rep els vots encriptats del servidor de xarxa i els emmagatzema fins al final del període de votació. El servidor d'emmagatzematge de vots té la responsabilitat d'administrar i cancel·lar els vots. El servidor de recompte de vots és un servidor fora de línia, que aglutina tots els vots encriptats. Els vots encriptats es transfereixen des del servidor d'emmagatzematge de vots al servidor de recompte de vots a través d'uns transmissors de dades. El servidor de recompte de vots no obté les signatures digitals dels votants i no en sap les dades personals. Addicionalment, el sistema de votació per Internet reparteix fitxers de registres independents, que consten dels vots encriptats rebuts des del servidor d'enviament de vots: tots els vots encriptats anul·lats, tots els vots encriptats enviats al servidor de recompte de vots i tots els vots encriptats recomptats. El protocol criptogràfic utilitzat connecta tots els registres amb els fitxers. El Comitè Electoral Nacional pot utilitzar l'historial de fitxers per resoldre situacions difuses. Per això, hi ha una auditoria independent per verificar el procés de votació electrònica i ajudar a resoldre els problemes que puguin aparèixer —veure diagrama 1.[11]

L'impacte de la participació i la representació de la votació per Internet

No es pot evitar l'assumpte de la fractura digital, la qüestió de si la votació per Internet agreuja la diferència de la possibilitat de representació dins de determinats grups socials. El que és evident és que la votació per Internet elimina les barreres físiques que obstaculitzen la participació en les eleccions de grups de persones grans, invàlides o d'altres amb mobilitat reduïda, o que tenen dificultat per assistir a les meses electorals —com les persones que tenen horaris de feina estrictes o que treballen a l'estranger, pares de nens petits i persones que viuen en regions amb una infraestructura pobra—, suposant, és clar, que aquesta gent tingui accés a Internet.

Alexander Trechsel conclou a un article elaborat per al Consell Europeu, seguint l'experiència de la votació per Internet portada a terme a Estònia entre el 2005 i el 2009, que l'educació i els ingressos, així com el tipus d'ubicació, són factors insignificants a l'hora d'escollir Internet entre els diversos canals de votació. Un dels descobriments més importants de l'estudi és que no és tant la divisió entre els que tenen accés a Internet i els que no en tenen, ni tampoc les tècniques informàtiques o la freqüència d'ús d'Internet, sinó la confiança en el procediment de votació per Internet, que fa que els votants s'encaminin a utilitzar o no la votació per Internet. L'edat és un factor significatiu però no dominant en aquest cas.

L'actual impacte de la votació per Internet en el canvi de participació no s'observa en una anàlisi objectiva. Es poden determinar les variacions de participació en diversos anys d'eleccions —comparant els tipus equivalents d'eleccions— i intentar aclarir les causes que apunten les variacions amb l'ajuda d'estudis sociològics. Potser la pregunta més important és quina porció de l'electorat no hauria participat en la votació si no s'hagués proporcionat la possibilitat de votació per Internet . No hi ha cap

11 MADISE, MAATEN, i VINKEL. *Internet Voting at the Elections of Local Government Councils on October 2005.*

El caràcter anònim del votant és garantit durant el recompte de vots fins al punt que es pot assegurar tant com en el cas de les votacions per correu postal «

manera d'obtenir-ne una evidència empírica més enllà de les dades aportades pels mateixos votants que Trechsel ha recollit pel seu estudi. L'única excepció és quan la votació per Internet és l'única possibilitat perquè l'elector voti com passa en el cas de la votació des de l'estranger en les eleccions municipals.

El 2005, la votació per Internet sembla que va tenir un lleuger efecte a l'alça pel que fa a l'assistència dels votants que a vegades voten i a vegades no. El 2007, aproximadament un 10% dels votants per Internet enquestats asseguraren que veritable o probablement no haurien votat si no haguessin tingut la possibilitat de votar a través d'Internet. L'estudi començava dient que fins i tot el Consell Europeu afirma que sense la votació per Internet, la participació en les eleccions municipals del 2009 hauria estat un 2,6% més baixa. Això és ja un impacte visible.

La qüestió més intrigant per als partits polítics és probablement l'impacte de l'ús de la votació per Internet en els resultats. Encara que els partits que estan a favor de la votació per Internet van reunir entre el 2005 i el 2009 molts dels vots per Internet, l'estudi mostra que l'autoposicionament en l'eix esquerra – dreta no juga cap paper important a l'hora d'escollir un canal de votació.

Aproximadament una cinquena part dels no votants per Internet pregun-tats assenyalaven que una raó per a la no votació per Internet era la suficiència del sistema del vot en paper. La manca de confiança, que era del 3,2%, i l'absurditat de la votació per Internet, de l'1,9%, no eren raons dominants. Al marge d'això, hi havien dubtes sobre un mal ús de la possibilitat de canviar el vot per Internet. No va ser el cas. L'estadística general mostra que el nombre de vots per Internet esmenats va ser insignificant. Tal com estava fixat prèviament, la influència impròpia d'altres persones en els votants remots és un problema teòric però potencialment significatiu, encara que tals amenaces es toleren amb el vot per correu en nombroses jurisdiccions. Si considerem l'experiència dels votants en els quatre casos de votació per Internet, veiem que hi ha poca evidència de coerció o de preocupació sobre la intimitat, basada en el comportament dels votants. Els petits percentatges de diversos vots així com l'augment significatiu sobre el nombre total de votants

Taula 01

Estadístiques de la votació per Internet (2005-2009)

	Municipals 2005	Parlament 2007	Parlament Europeu 2009	Municipals 2009
Nombre total d'e-votants	9 287	30 243	58 614	104313
Nombre total de votants	496 336	550 213	396 982	658 213
% d'e-votants	1,9%	5,5%	14,8 %	15,7%
E-vots sobre el vot anticipat	7,2%	17,6%	45,4%	44%
E-vots emesos a l'estranger	Dades no disponibles	2 %	3 %	3%

1 Dades de 2004 2 Dades entre 2000 i 2007

Fonts: PNUD, *Human Development Reports*, 2010.

» El Consell Europeu afirma que sense la votació per Internet, la participació en les eleccions municipals del 2009 hauria estat un 2,6% més baixa

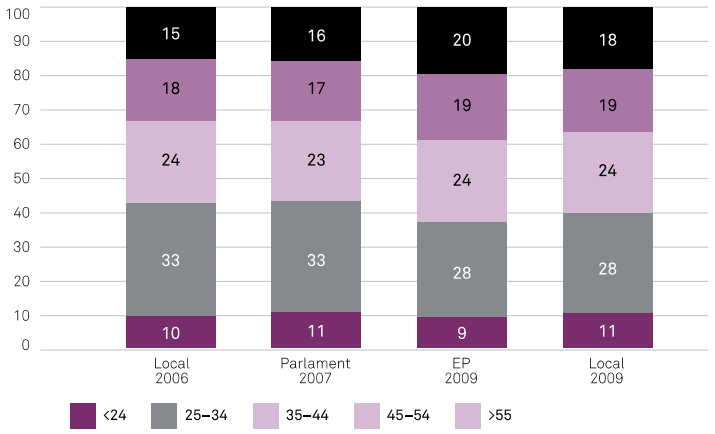
per Internet des de 2005 fins al 2009 indiquen que la confiança en l'existència del sistema de votació per Internet ha augmentat —veure taula 1.

El mateix estudi afirma que la hipòtesi que la votació per Internet dóna avantatge a l'electorat urbà no es sustentaven. El gènere no és un factor important a l'hora d'escollir la votació per Internet d'entre els possibles canals de votació. L'edat es pot veure com un factor important, ja que el grup d'entre 25 a 34 anys aglutina la majoria dels votants per Internet, però si el comparem amb els votants globals i amb la composició d'edat tradicional dels votants, la votació per Internet no destaca com a solució per als votants més joves, tal com els crítics han sostingut —veure gràfica 2.

Tampoc es pot jutjar la legitimitat de la votació per Internet només sobre la base del seu impacte en l'alienació política. La legitimitat i la constitucionalitat de la votació per Internet així com el seu impacte en la democràcia són només meres discussions. És massa d'hora per fer declaracions fermes en aquest sentit. D'una banda, l'experiència de la votació remota per Internet té una base massa feble per fer-ho; i d'altra banda, l'ambient sociopolític està canviant constantment.

Gràfica 02

Percentatge d'e-votants per edat (2005–2009)



Font: Elaboració pròpia

Conclusions

Pel fet de ser un Estat del nord esparsament poblat i amb poques tradicions assentades quan va recobrar la independència el 1991, Estònia es podia beneficiar d'unes oportunitats excel·lents per a l'explotació reeixida de noves idees com les que ofereixen les tecnologies de la informació i la comunicació. La singular possibilitat de reconstruir l'Estat ha ofert grans oportunitats de prendre decisions contemporànies, funcionals i lògiques. Per tal d'augmentar la competitivitat de la societat, s'ha posat més èmfasi en el desenvolupament d'una societat electrònica inclusiva basada en la identitat virtual i en solucions electròniques en tots els camps possibles. Algunes d'aquestes solucions, com el tiquet electrònic, substitut de contrasenyes per a la targeta d'identificació, la signatura digital, el procedi-

La votació per Internet no destaca com a solució per als votants més joves

ment administratiu digital... són només serveis electrònics convenients sense riscs pel que fa a la intimitat.

Altres, com un programa de salut electrònica que reculli tota la informació mèdica, o simplement l'electrònica *State Gazette*, requereixen unes mesures de seguretat serioses. Encara que els escenaris descrits per George Orwell a *1984* o per Florian Henckel von Donnersmarck a *Das Leben der Anderen* són altament improbables a Estònia, la legitimitat d'establir un Banc Genètic que contingui dades de tota la població exigeix una reflexió. Té l'Estat el dret de crear uns requisits previs per produir una imatge completa d'una persona amb uns quants clics de ratolí? Aquestes discussions sorgeixen de tant en tant dins d'un petit cercle d'experts, mentre que l'interès de la majoria de l'audiència en aquests assumptes és bastant modest. La conveniència d'unes noves solucions supera dubtes i riscos.

Un cas a part és la votació per Internet. D'una banda és un servei electrònic públic essencial en la societat de la informació estoniana; i d'altra banda és una revolució en l'administració electoral, l'impacte de la qual mereix una atenció permanent i una recerca científica. ◂

MÉS INFORMACIÓ

DRECHSLER, Wolfgang i MADISE, Ülle. «Electronic Voting in Estonia». A KERSTING, Norbert i BALDERSHEIM, Harald (eds.). *Electronic Voting and Democracy. A Comparative Analysis*. Basingstoke: Palgrave Macmillan, 2004, p. 97-108.

Global Information Technology Report 2009-2010. http://www.weforum.org/documents/GITR10/index.html

MADISE, Ülle. «Legal and political aspects of the Internet voting: Estonian case». A RENIU, Josep M. (ed.). *E-voting: the last electoral revolution*. Barcelona: Institut de Ciències Polítiques i Socials, 2008, p. 45-59.

MADISE, Ülle, MAATEN, Epp i VINKEL, Priit. *Internet Voting at the Elections of Local Government Councils on October 2005* [en línia]. Tallinn: Comitè Electoral Nacional d'Estònia, 2008 [Consulta: juny de 2010]. Disponible a: http://vvk.ee/public/dok/report2006.pdf

TRECHSEL, Alexander H. i VASSIL, K. *Internet voting in Estonia: Report for the Council of Europe*. Tallinn: Comitè Electoral Nacional d'Estònia, 2010 [Consulta: juny de 2010]. Disponible a: http://vvk.ee/public/dok/Report_-_E-voting_in_Estonia_2005-2009.pdf .

ENLLAÇOS

Comitè Electoral Nacional
http://www.vvk.ee

Estonica
http://www.estonica.org/en/

State Portal
http://www.eesti.ee/eng/

VII Ülle Madise, Epp Maaten and **Priit Vinkel**. 2014. “Voto por Internet en Estonia.” In A. Ayala Sanchez (ed.). *Nuevas Avenidas de la Democracia Contemporanea*. Serie Docrina Juridica 707, Institutio de Investigaciones Juridicas. Mexico: Universidad Nacional Autonoma de Mexico, 575-601. (3.2)

VOTO POR INTERNET EN ESTONIA*

Ülle MADISE**
Epp MAATEN***
Priit VINKEL****

SUMARIO: I. *Introducción*. II. *Gestión de proyectos*. III. *Creación de la base jurídica*. IV. *Solución técnica*. V. *Análisis del impacto*. VI. *Retos*. VII. *Conclusiones*. VIII. *Bibliografía*.

I. INTRODUCCIÓN

Estonia es ampliamente reconocida como un país pionero en gobierno electrónico. De acuerdo al *Global Information Technology Report 2013*, Estonia se encuentra clasificada como la mejor entre los países de Europa Central y del Este, en el lugar 22.[1] El uso de medios electrónicos para diferentes servicios se ha ampliado de manera constante en el país y una gran cantidad de servicios electrónicos son proporcionados tanto por el sector público como por el privado. El 77% de los estonios entre los 16 y los 74 años de edad usan regularmente Internet y el 80% de los hogares tiene acceso a la misma.[2] El entusiasmo con el que los estonios aplican las nuevas soluciones tecnológicas de la información, apunta claramente a un alto nivel de preparación electrónica de las personas.

Mientras que en muchas naciones el primer paso hacia alguna forma de voto automatizado fue utilizar las máquinas de votación en los colegios electorales a fin de facilitar el sufragio o el conteo, en Estonia, desde el principio, existía el objetivo de crear las condiciones para el voto público remoto por Internet. Proyectos similares de introducción del voto electrónico vinculante a distancia para elecciones generales han evolucionado mucho más en Suiza y Noruega.

El sufragio por Internet ofrece nuevas oportunidades para mejorar el proceso electoral, pero también presenta nuevos retos.

* Traducción de Alfonso Ayala Sánchez y Daniel Martínez Vinzoneo.

** University of Tartu, *ylle.madise@vpk.ee*.
*** Estonian Electronic Voting Committee, *epp.maaten@eesti.ee*.
**** Estonian National Electoral Committee, *priit.vinkel@vvk.ee*.

1 Foro Económico Mundial, *The Global Information Technology Report 2013*.

2 Eurostat 2013, *Survey on Individuals regularly using the Internet and on Households - Level of Internet Access. General Description of e-Voting*, 2004, NEC.

En particular, es fundamental que el voto por Internet (*I-voting*) sea introducido de una manera que salvaguarde la transparencia de las elecciones, un principio democrático fundamental. El *I-voting*, al igual que otros cambios en los mecanismos utilizados para captar votos —desde las papeletas hasta las máquinas de votación— es una tecnología que modifica el medio directo de la participación, pero no la naturaleza de la propia democracia. Por lo tanto, ha sido un reto para Estonia el integrar esta nueva solución tecnológica a las viejas tradiciones de votación.

¿Por qué votar por Internet?

La explosión de Internet a finales de la década de 1990 llevó a muchos a especular sobre la posibilidad de utilizar este nuevo medio público para mejorar la eficiencia, eficacia y legitimidad de las elecciones democráticas. Hemos llegado a una nueva era en la que Internet es una parte integral de la vida cotidiana y el principal medio de información para un número creciente de ciudadanos. Drechsler está probablemente en lo cierto cuando afirma que "el impulso para mejorar continuamente la tecnología de la información y comunicación es tan irresistible que gran parte del mundo seguirá el ejemplo del voto por Internet de Estonia. Es el futuro de la política, a pesar de las advertencias de algunas personas como el teórico de Internet Manuel Castells, quien sostiene que el *I-voting* presenta riesgos para la legitimidad democrática".[3] El objetivo declarado del lanzamiento de la votación en línea en Estonia fue aumentar el número de votantes, lo que tal vez se podría describir de manera más realista como ampliar las posibilidades de acceso y detener el descenso de la participación (especialmente entre los votantes más jóvenes). La tasa de participación ciudadana en las elecciones del consejo local de gobierno en Estonia se encuentra usualmente cercana al 50% y en las elecciones parlamentarias aumenta aproximadamente un 10%. La participación electoral nunca excedió el 70%, incluso en el referendo constitucional de 1992. Al facilitar la participación electoral, parecía probable que el número de votantes, y por lo tanto la legitimidad global de los resultados, mejorarían. Otra razón detrás del proyecto de votación por Internet fue el deseo de aprovechar la infraestructura existente de manera más eficaz. El uso generalizado de la tarjeta nacional de identidad electrónica (*e-ID card*) fue vital para iniciar el proyecto de voto por Internet, ya que solo los propietarios de tarjetas de identidad tenían la opción de votar a través de

[3] Drechsler, Wolfgang, "Dispatch from the Future", *The Washington Post*, The Washington Post Company, 5 de noviembre de 2006.

este medio. En 2012, el documento nacional de identidad celebró su décimo aniversario, y actualmente 1.2 millones de personas poseen una tarjeta de *e-ID* válida, de los cuales, 85% son ciudadanos; por tanto, la mayoría de los votantes elegibles (~1 millón) ya poseen la tarjeta.

II. Gestión de proyectos

En 2001 las discusiones entre los grupos políticos y académicos comenzaron acerca de si Estonia debía o no introducir el voto por Internet. Al mismo tiempo, el Ministerio de Justicia anunció la intención de introducir la votación por Internet tan pronto como fuera posible. Con el fin de evaluar la idea, dos informes fueron encargados por el gobierno.

Se llegó a un acuerdo político en 2002, y en 2003 el Comité Electoral Nacional (CEN) comenzó el proyecto de votación electrónica. Al inicio del proyecto, el CEN involucró a tantos especialistas en seguridad de tecnologías de la información como fue posible a fin de elaborar un enfoque común aceptable y, por lo tanto, aumentar la confianza del público en el voto por Internet. La buena cooperación entre las distintas partes, públicas o privadas, fue crucial en el lanzamiento del exitoso y apolítico proyecto de *I-voting*.

El grupo ejecutivo del proyecto de voto por Internet fue formado por el CEN, se eligió a un gerente del proyecto y los roles entre el CEN, el grupo ejecutivo y el gerente del proyecto se distribuyeron. De acuerdo con la organización del proyecto, el CEN aprobó las decisiones más relevantes. La tarea del grupo ejecutivo era hacer propuestas y recomendaciones al CEN y controlar la consecución de los objetivos fijados. El gerente del proyecto estuvo a cargo de la implementación del mismo, convocó a grupos del proyecto formados por expertos cuando fue necesario, dirigió sus trabajos y revisó los resultados.

En esta etapa, el concepto del *I-voting* estaba esencialmente completo. Después de esto se llevó a cabo el análisis de la seguridad del concepto por un grupo de trabajo formado por especialistas en seguridad de tecnologías de la información. Partiendo de las recomendaciones del análisis de seguridad, se realizaron cambios al concepto y se presentó el documento titulado "Descripción general del proyecto de voto electrónico de Estonia".[4]

A principios de 2004, se produjo la descripción técnica del *software* para la votación por Internet. En marzo de 2004 se presentaron tres ofertas y el CEN eligió a Cybernetica Ltd. como el desarrollador del *software*, una cooperación que ha continuado hasta la actualidad. En otoño, el *software*

[4] La última versión está disponible en *www.vvk.ee*.

estaba listo para la primera prueba piloto en público. La prueba ofreció la posibilidad de votar por Internet en una encuesta a los residentes de Tallin, que tuvo lugar en enero de 2005; 703 electores participaron y 697 votos fueron contados. El sistema funcionó sin fallas. Una vez completada la prueba piloto, el sistema de *I-voting* parecía estar en posición y listo para ser utilizado en las elecciones municipales de otoño de 2005.[5]

III. Creación de la base jurídica

1. *Los debates parlamentarios sobre el* I-voting

El alcance del debate parlamentario antes de lanzar la votación por Internet fue bastante amplio, abarcando desde claras cuestiones ideológicas hasta problemas tecnológicos detallados.[6] El asunto más discutido fue el significado exacto y propósito del principio de secrecía. Otras cuestiones importantes eran la brecha digital y el valor del ritual de caminar a un centro de votación.

En Estonia, así como en muchos otros países que han creado y permitido el voto por correo, la votación anticipada y otros métodos de votación complementarios, votar en una casilla electoral ha perdido prácticamente su significado como un ritual de transformación de las personas en un Estado-nación y en los portadores de la soberanía nacional (comparar con Monnoyer-Smith, 2006).[7] La pregunta retórica de los adversarios del *I-voting* en el *Rüigikogu* era en cierta forma emblemática: "¿Estamos hundiéndonos en el pantano liberal?" Esta pregunta probablemente estaba inspirada en la suposición de los partidarios de la votación por Internet de que el Estado debe confiar en la gente y, de ser posible, no interferir con ninguna de sus decisiones.

En la discusión acerca de la introducción del *I-voting*, los argumentos clásicos acerca de la conformidad de la votación por Internet con los principios de elecciones justas, incluyendo la confiabilidad de los sistemas de vo-

[5] Madise, Ülle y Maaten, Epp, "Internet Voting in Estonia", en Ríos Insua, David y French, Simon (comp.), *E-Democracy: A Group Decision and Negotiation Perspective*, Nueva York, Springer Science+Business Media, 2010, pp. 301-321.

[6] Véase lo concerniente al origen del proyecto estonio de *I-voting* en las referencias a las actas de las sesiones plenarias del parlamento estonio (*Rüigikogu*), la estructura partidista, etcétera, en Drechsler y Madise, 2004.

[7] Monnoyer-Smith, Laurence, "How e-Voting Technology Challenges Traditional Concepts of Citizenship: An Analysis of French Voting Rituals", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006, pp. 61-68.

tación electrónica, se cambiaron, y por tanto uno de los argumentos típicos contra *I-voting* fue que las personas que no tienen ningún compromiso de ir a la mesa de votación para ejecutar su deber ciudadano, no deberían de participar en el gobierno en absoluto, lo que contradice el axioma de que cuanto mayor sea la participación el día de la elección, mejor.

Una posible falta de legitimidad de los resultados de las elecciones podría derivarse de lo siguiente:

- El procedimiento individual de votación por Internet no puede ser supervisado por las autoridades u observado de la manera tradicional. Por lo tanto, la compra y venta masiva de votos, así como el ejercicio de otro tipo de influencia o presión sobre el votante es posible.
- Las propias personas no pueden verificar los resultados del *I-voting*, y la gente necesita tener una fe absoluta en la precisión, honestidad y seguridad de todo el sistema electoral (personas, *software*, *hardware*). Para quienes no programan el sistema, la operación de las computadoras puede ser verificada solo conociendo lo que se introdujo, y comparando el resultado esperado con el resultado de salida. Bajo un sistema de voto secreto, no se puede saber lo que el votante introdujo, ni tampoco existe un resultado esperado con el que se puedan comparar los resultados electorales obtenidos.[8]

Aunque los riesgos antes mencionados son manejables, se debe de tener en cuenta que siempre es posible amenazar la legitimidad del resultado electoral sin ninguna causa objetiva. Es probable que al decidir si apoyaban el voto electrónico o no, los partidos políticos tomaran en consideración el efecto potencial del voto remoto por Internet sobre los resultados electorales. Los partidos suponen que el *I-voting* le permite votar a personas que por los medios tradicionales no participarían, y los votos adicionales no se distribuirían proporcionalmente entre los partidos políticos. Por lo tanto, parece probable que el aumento de la participación cambie la distribución de los votos entre los partidos.[9] Por supuesto estos tipos de consideraciones contradicen el principio de sufragio universal.

[8] Madise, Ülle y Martens, Tarvi, "E-Voting in Estonia 2005. The First Practice of Country-wide binding Internet Voting in the World", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006, pp. 15-26.

[9] Madise, Ülle, "Legal and Political Aspects of the Internet Voting: Estonian Case", en Reniu, Joseph M. (ed.), *E-voting: The Last Electoral Revolution*, Barcelona, Institut de Ciències Politiques i Socials, 2008, pp. 45-59.

2. *Interpretación teleológica del principio de secrecía*

De acuerdo a la Constitución de Estonia, los miembros del *Riigikogu* así como los consejos locales de gobierno deben ser elegidos en elecciones libres, generales, iguales y directas, y la votación debe de ser secreta. No existe una regulación especial para la votación por Internet en la Constitución.

La secrecía del voto ha sido considerada tradicionalmente en Estonia como el derecho y la obligación del ciudadano de emitir su voto de manera solitaria en una casilla de votación. En el caso del voto por Internet, el Estado no está en condiciones de asegurar el aspecto privado del procedimiento. Los legisladores procedieron con la interpretación de la Constitución, según la cual la secrecía del voto, sobre la base de sus dos sub-principios —el procedimiento privado de la votación y el anonimato del voto—, es necesaria para garantizar una votación libre y no es un objetivo *per se*.

El derecho del elector al anonimato durante el conteo de los votos se garantiza en la medida en que esto puede ser asegurado en el caso de las papeletas de voto ausente por correo; el denominado "sistema de dos sobres", usado para el caso del voto ausente por correo, es tanto confiable como fácil de entender para los votantes por Internet (véase *infra* epígrafe IV).

El voto remoto por Internet requiere repensar el principio de privacidad. Este principio está ahí para proteger a las personas de cualquier presión o influencia en contra de la libre expresión de sus preferencias políticas. Tal enfoque teleológico de la Constitución fue la base de las disposiciones del voto por Internet desde el principio de todo el proyecto. Además de la interpretación teleológica de la Constitución, el Ministerio de Justicia, encabezada por el liberal Partido de la Reforma, basó disposiciones permitiendo el voto por Internet sobre la premisa de que el Estado tiene que confiar en las personas, y evitar siempre que sea posible, la interferencia con la toma de decisiones a nivel individual. La persona tiene que ser consciente de los riesgos (como los riesgos técnicos), y debe de tener el derecho de decidir si utiliza o no la oportunidad de votar por Internet.[10]

Esta interpretación teleológica del principio de secrecía es claramente divergente del enfoque tradicional generalmente adoptado en la literatura académica. Por ejemplo, Buchstein señala que: "la secrecía obligatoria es un principio que va más allá de la ley constitucional, sus fundamentos se basan en la idea de auto paternalismo y se entiende como un mecanismo

[10] Drechsler, Wolfgang y Madise, Ülle, "Electronic Voting in Estonia", en Kersting, Norbert y Baldersheim, Harald (comp.), *Electronic Voting and Democracy. A Comparative Analysis*, Basingstoke, Palgrave Macmillan, 2004, pp. 97-108.

de sujeción propia de los ciudadanos autónomos a fin de evitar situaciones de presión externa o corrupción. En este concepto, no es la persona misma, sino un agente o autoridad externo autorizado —normalmente el Estado— el responsable de proporcionar los medios necesarios para permitir el voto secreto".[11]

En Estonia, a diferencia de otros países, el hecho de si una persona con derecho a votar participó en los comicios o no, no es considerado como parte del principio de secrecía. Las listas de votantes que contienen la información sobre la participación y el método de votación elegido se conservan en un archivo y pueden ser utilizados para fines de investigación. Los investigadores han hecho uso de esta posibilidad, incluyendo la encuesta sobre *I-voting*, lo que desafortunadamente debilitó un poco la confianza pública en la votación por Internet. El hecho de que el entrevistador oficial tuviera conocimiento sobre hechos concretos del *I-voting* hizo que algunas personas sospechan sobre la secrecía de su decisión de voto. Estas sospechas se filtraron en los medios de comunicación públicos, pero más o menos pasaron inadvertidos. La explicación fue que las listas de votantes siempre han tenido información sobre quiénes participaron y qué método de votación utilizaron. La propia decisión del votante siempre se ha mantenido en secreto.

3. *El derecho a cambiar el voto por Internet como garantía necesaria para elecciones libres*

Con el fin de garantizar la libertad de voto, a los votantes por Internet se les otorgó el derecho a sustituir el voto emitido en Internet por otro electrónico o por una boleta de papel. Sin embargo, esto se puede hacer solo dentro de los días de votación por adelantado. En caso de existir varios votos por Internet, solo el último se toma en cuenta; en caso de presentarse un voto electrónico y una boleta de papel, la boleta se contabilizaba. Si varias boletas se emitían, todos los votos se declaran nulos. Por lo tanto, el principio de "un voto: un votante" está ostensiblemente garantizado.

Este enfoque causó perplejidad entre la audiencia del informe presentado por Madise en el Foro Mundial sobre E-Democracia en París, en 2001, e incluso en 2005. Sin embargo, en el Seminario Internacional celebrado en Bregenz en 2006, los académicos noruegos comentaron *inter alia*, de que

[11] Buchstein, Hubertus, "Online Democracy. Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory", en Kersting, Norbert y Baldersheim, Harald (comp.), *Electronic Voting and Democracy. A Comparative Analysis*, Basingstoke, Palgrave Macmillan, 2004, pp. 39-58.

ellos habían llegado a principios similares antes de obtener un conocimiento detallado acerca del sistema de votación por Internet de Estonia,[12] y expresaron un claro apoyo al aspecto de sustitución del voto de esta idea. Ya sea que uno esté de acuerdo con este principio o no, sin duda vale la pena considerarlo de manera más profunda.

Algunos meses antes de las elecciones municipales de 2005, el presidente de Estonia llevó disposiciones sobre el voto por Internet ante la Corte Suprema para una revisión constitucional, argumentando que la posibilidad de cambiar el voto por Internet le da ventajas a este tipo de votantes en comparación con quienes votan de manera distinta. Los votantes por Internet pueden cambiar su voto un número ilimitado de veces, pero solo durante los días de votación por internet y votación anticipada. La versión inicial de la ley sobre *I-voting* contenía la posibilidad de cambiar el voto por Internet por una boleta de papel el día de la votación. Esta disposición fue derogada, porque esto podría haber dado una ventaja real a los votantes por Internet: ellos habrían tenido la oportunidad de cambiar su preferencia electoral el domingo después de recibir información adicional acerca de los candidatos en la segunda mitad de la última semana. Después de este cambio, todos los votantes que utilizaran las posibilidades electorales anticipadas, estaban formalmente en las mismas condiciones.

La Sala de Revisión Constitucional de la Corte Suprema señaló que a pesar de la votación electrónica repetida, no había ninguna posibilidad de que el elector afectara los resultados de la votación en un mayor grado que aquellos votantes que utilizaron otros métodos de votación. Desde el punto de vista de los resultados electorales, este voto no tenía de ninguna manera una mayor influencia que los votos emitidos en las papeletas. De acuerdo con la Ley Electoral de Estonia, cada elector debe de tener un voto.

La Corte dijo que esta interpretación transforma el principio de elecciones uniformes en un caso especial del derecho general a la igualdad. En sentido legal, el *I-voting* es igualmente accesible a todos los votantes. La tarjeta de identificación necesaria para el *I-voting* es obligatoria para todos los habitantes de Estonia, y por lo tanto, el Estado no ha creado ningún obstáculo legal para que cualquier persona vote por Internet, incluido el cambiar el propio voto durante los días en que se realizan las votaciones anticipadas. Es cierto que, debido a desigualdades de hecho, la posibilidad de cambiar el propio voto a través de Internet no sea accesible a todos los votantes, y

[12] Skagestein, Gerhard *et al.*, "How to Create Trust in Electronic Voting over an Untrusted Platform", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006, pp. 107-116.

esto pueda ser considerado como una violación del derecho general a la igualdad y al principio de uniformidad. El principio de igualdad de trato en el contexto de la elección de los órganos de representación no significa que se deba garantizar a todas las personas con derecho a voto posibilidades absolutamente iguales de realizar el acto de votación de igual manera. De hecho, aquellos que utilizan los diversos métodos de votación previstos por la ley se encuentran en situaciones diferentes. La garantía de una igualdad realmente absoluta entre las personas en el ejercicio de su derecho a votar es inviable en principio y no lo requiere la Constitución. El objetivo de aumentar el número de votantes es sin lugar a duda legítimo. Las medidas que el Estado adopte para garantizar la posibilidad de votar para el mayor número posible de votantes están justificadas y son aconsejables. Otro objetivo de permitir el voto por Internet es la modernización de las prácticas de votación, lo que coincide con los objetivos del *I-voting* que figuran en la Recomendación Rec (2004) "Legal, Operational and Technical Standards for I-voting" del Consejo de Europa.

De acuerdo con el dictamen de la Corte Suprema de Estonia, el principio de la libertad de voto da lugar a la obligación del Estado de proteger a los votantes de personas que intenten influir en su elección. Con respecto a este principio, el Estado debe de crear las condiciones necesarias para llevar a cabo elecciones libres y proteger a los votantes de presiones indeseadas mientras deciden su voto. En el párrafo 30 de la citada sentencia, la Suprema Corte mantiene lo siguiente:

> La posibilidad del votante de cambiar el voto emitido por medios electrónicos, durante las votaciones anticipadas, constituye una garantía complementaria esencial para el cumplimiento del principio de elecciones libres y la votación secreta al emitir el sufragio por medios electrónicos. Un votante que ha sido influenciado u observado ilegalmente durante su votación electrónica, puede restaurar su libertad de elección y la secrecía de su voto mediante una nueva votación, ya sea electrónicamente o con una boleta de papel, después de haberse liberado de las influencias. Además de la posibilidad de rectificar posteriormente el voto emitido bajo influencia, la posibilidad de votar de nuevo tiene una función preventiva importante. Cuando la ley le garantiza a un votante que utiliza el voto por Internet la posibilidad de cambiar el voto emitido por medios electrónicos, la motivación para ejercer una influencia ilegal sobre la persona disminuye. No existen otras medidas igualmente efectivas, además de la posibilidad de cambiar el voto emitido por Internet, que garanticen la libertad de elección y la secrecía del voto sobre el voto electrónico en un medio sin control. Las sanciones del derecho penal tienen un sentido preventivo, pero el castigo posterior —a diferencia de la posibilidad de cambiar

> el voto electrónico propio— no ayuda a eliminar una violación de la libertad de elección y el secreto del voto. (Cámara de Revisión Constitucional de la Suprema Corte de Estonia, Decisión núm. 3-4-1-13-05)

Así, el Tribunal Supremo confirmó la constitucionalidad de una de las principales premisas del proyecto de voto remoto por Internet.

Mientras que Drechsler y Annus aseveraban (bastante razonablemente para el periodo de 1992 a 2001) que en su interpretación de la Constitución, la Suprema Corte de Estonia evita el método de interpretación teleológico y sistemático junto con el punto de vista de la ciencia social,[13] el caso del voto remoto por Internet es evidencia de un cambio. Es cierto que la tradición de pertenecer al espacio jurídico alemán y la influencia de las ideas de Kelsen en *Reine Rechtslehre* sobre la jurisprudencia de Estonia,[14] han reforzado el énfasis en la pura discusión de las normas en lugar de enfocarse en la realidad social. Sin embargo, al menos las ideas de las reformas del derecho público ya se han alejado del método técnico positivista de subsunción. Ya en 2001, Narits trató la discusión sobre el objetivo del significado y la norma de la ley como una clara tendencia en las últimas prácticas de la Suprema Corte.[15] El concepto del enfoque teleológico y la aceptación de los métodos utilizados por la votación por Internet se han mantenido en casos subsiguientes en la Corte Suprema de Estonia (los casos 3-4-1-10-11 del 31 de marzo de 2011 y 3-4-1-4-11 del 21 de marzo 2011).

4. *Segunda ronda de debates parlamentarios. Verificación de que los votos por Internet se almacenen como se pretende a partir del 2015*

Debido a que en 2011 el porcentaje de votos por Internet había aumentado a casi un cuarto de los votos válidos, el Parlamento decidió especificar las normas del *I-voting* en las leyes electorales con el fin de mejorar la legitimidad y la transparencia de la votación electrónica. Hasta 2011 los procedimientos de votación por Internet tenían muy pocas regulaciones legislativas.

[13] Drechsler, Wolfgang y Annus, Taavi, Die Verfassungsentwicklung in Estland von 1992 bis 2001, en Häberle, Peter (ed.), *Jahrbuch des öffentlichen Rechts der Gegenwart*, Tübingen, Mohr Siebeck, 2002, pp. 473-492.

[14] Mälksoo, Lauri, "Von der Demokratie bis zur Diktatur: ein verborgener Dialog zwischen Artur-Tõeleid Kliimann und Carl Schmitt", *Der Staat*, vol. 43, núm. 1, 2004, pp. 57-82.

[15] Narits, Raul, "Rechtssprache und juristische Semantik im sozialen Kontext der estnischen Rechts - und Lebensordnung", en Krawietz, Werner y Narits, Raul, (eds.), *Rechtstheorie. Internationales Symposium der Estnischen Juristischen Fakultät in Tartu. Sonderheft Estland*, vol. 31, núm. 3-4, 2001, pp. 535-551.

El Parlamento estableció un grupo de trabajo que, además de detallar los procedimientos, tenía que proponer una solución de cómo elevar la auditabilidad y cómo verificar que los votos por Internet estuvieran correctos.

Al mismo tiempo, la comunidad técnica, que había estado involucrada por el CEN en los debates sobre la seguridad de la votación electrónica, llegó a la conclusión de que se necesitaba un nuevo mecanismo para tener un cierto nivel de verificación, con el fin de detectar ataques maliciosos en el sistema de *I-voting*. El CEN tiene una mejor opción para descubrir ataques y reaccionar a ellos si los votantes por Internet, incluso una cantidad relativamente pequeña de ellos, verifica sus votos. Si alguien descubre y reporta al CEN que su voto no está almacenado correctamente, se pueden tomar medidas inmediatamente. Si los votantes solo tienen acceso a sus computadoras personales y utilizan las mismas para la verificación, no se podría lograr ninguna seguridad en absoluto. Por lo tanto, algunos canales independientes como los teléfonos móviles o los dispositivos móviles, que son fácilmente accesibles para los votantes, se necesitan para la verificación (Heiberg, Lipmaa, van Laenen 2010).[16]

A finales de 2012, el Parlamento aprobó las enmiendas a la ley electoral que indicaban que un nuevo comité electoral —el comité de votación electrónica— debería crearse para la realización de la votación por Internet. La ley también regula que antes de cada utilización, el sistema de *I-voting* debe ser probado y auditado. El cambio más importante de la ley fue la afirmación de que, a partir de 2015, los votantes tienen que tener la posibilidad de comprobar que su voto ha llegado y está almacenado en el servidor central de las elecciones, y refleja la elección del votante correctamente.

IV. Solución técnica

1. *La tarjeta de identificación como una herramienta para la interacción segura en Internet*

Durante la última década, los gobiernos de todo el mundo están utilizando cada vez más el potencial de las tecnologías de la información y comunicación (TIC) para aumentar la eficiencia de sus servicios. Esto, a su vez, ha traído consigo nuevos retos. Algunos de los más grandes en el ámbi-

[16] Heiberg, Sven *et al.*, "On E-Vote Integrity in the Case of Malicious Voter Computers", en Gritzalis, Dimitris *et al.* (eds.), *Computer Security – ESORICS 2010*, *15th European Symposium on Research in Computer Security*, 20-22 de septiembre de 2010, Atenas, Springer-Verlag Berlin Heidelberg, Lecture Notes in Computer Science, 2010, pp. 373-388.

to de la gobernanza electrónica son la identificación y autenticación de los ciudadanos. Los métodos de autenticación basados simplemente en contraseñas no son lo suficientemente seguros. Estonia eligió la tarjeta de identificación electrónica como la principal herramienta de autenticación. A pesar de que muchos Estados alrededor de todo el mundo ya tienen algún tipo de sistemas de tarjetas de identidad funcionando, pocos están basados en tarjetas electrónicas. Sin embargo, en la tarjeta de identificación de Estonia, lo que permite la autenticación personal segura, y la firma digital, así como la infraestructura de la clave pública (ICP) necesaria para el uso de tarjetas de identificación electrónica, ya se habían desarrollado a fines de 2001.

Emitidas por el Gobierno de Estonia desde enero de 2002, las tarjetas de identificación nacionales representan la principal fuente de identificación personal para las personas que viven dentro de Estonia, y son obligatorias para todos los ciudadanos y residentes extranjeros mayores de quince años. La tarjeta de identificación tiene dos funciones: la identificación física como una credencial normal y la identificación electrónica, que le permite a los ciudadanos utilizar la misma tarjeta para autentificarse electrónicamente en sitios web y redes, y/o firmar digitalmente comunicaciones y transacciones, según se requiera.

Cada credencial contiene dos certificados digitales discretos basados en la ICP: uno para la autentificación y otro para la firma digital. Los certificados contienen solo el nombre y el código personal del titular, y tienen dos claves privadas asociadas en la tarjeta, cada una protegida por un PIN de usuario único. Los certificados no contienen restricciones de uso: son por naturaleza universales y están destinados a ser utilizados en cualquier tipo de comunicación, ya sea entre particulares, organizaciones o dentro del gobierno. Como se ha mencionado antes, la tarjeta puede también ser utilizada para cifrar documentos, de modo que solo la persona destinada para ver el documento puede descifrarlo. Este es un medio eficaz para la transferencia segura de documentos a través de redes públicas. Además de eso, cada credencial de identificación contiene todos los datos impresos en ella de forma electrónica, en un archivo especial de datos legible públicamente.

En 2007, una nueva solución de identificación electrónica fue introducida en el mercado estonio: la identificación móvil (*Mobil-ID*), donde el teléfono móvil (a través de su tarjeta SIM) actúa como una credencial de identificación y un lector de tarjetas a la vez. Además de tener la funcionalidad de una tarjeta SIM normal, una SIM de identificación móvil contiene los certificados personales que permiten a los proveedores de servicios de Internet identificar a las personas y emitir firmas digitales. A partir de 2011,

los certificados móviles de identificación tienen garantía gubernamental y la solución se puede utilizar en el voto por Internet.

2. *Medidas empleadas para garantizar la secrecía del voto*

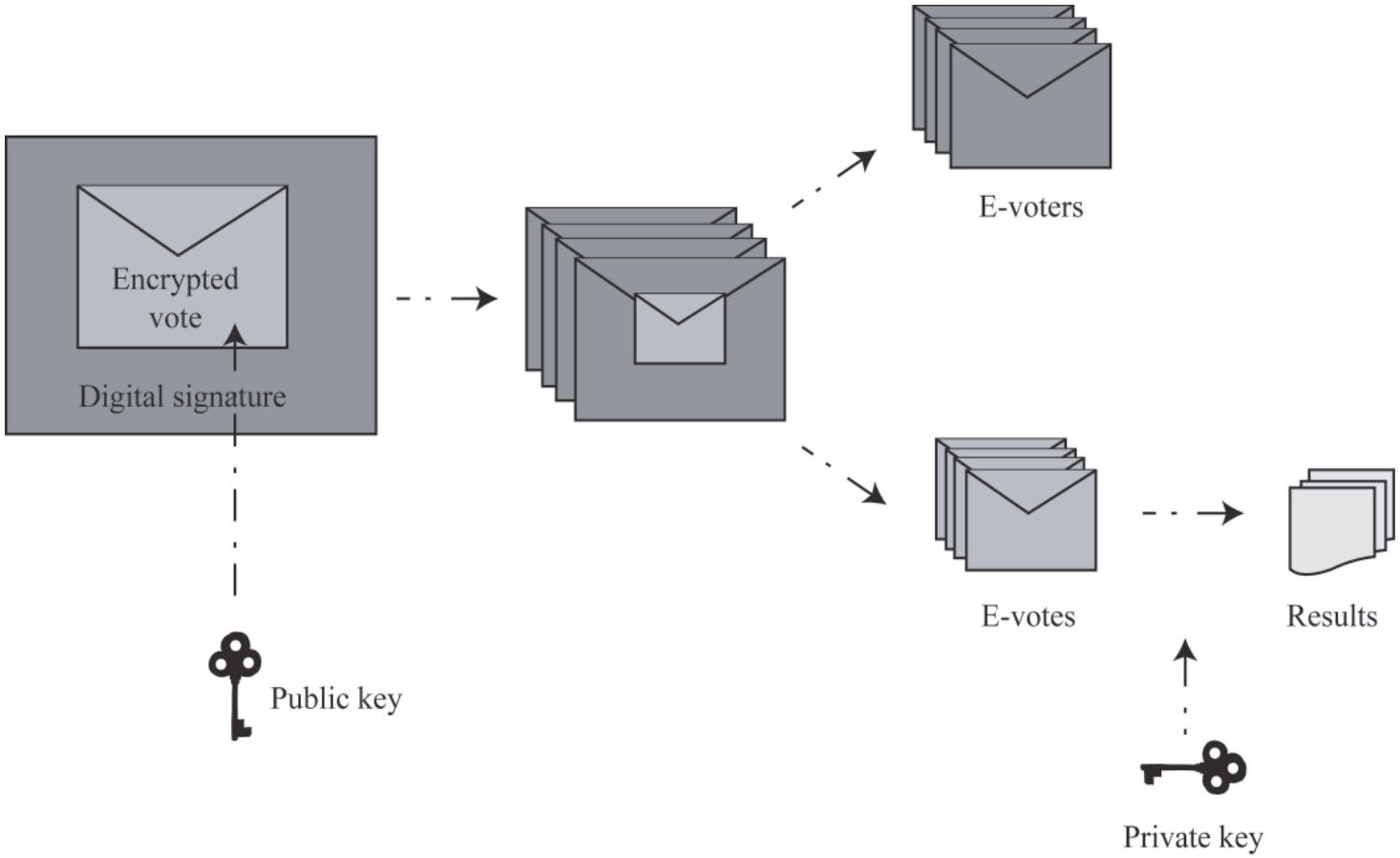
Una de las principales preocupaciones de los interesados en la seguridad de los sistemas de voto por Internet es la contradicción evidente entre las propiedades de seguridad y confidencialidad. Por un lado, la votación debe ser privada y los votos deben de permanecer anónimos. Por el otro, los votantes deben de ser identificados con el fin de garantizar que solo quienes son elegibles pueden votar y que lo hagan solo una vez.

Con el fin de entender cómo el sistema de *I-voting* garantiza la secrecía y la singularidad del voto, debemos describir brevemente el método de votación mediante sobres utilizado en Estonia para la votación anticipada con papel. Este método le da la posibilidad al votante de emitir su sufragio fuera de la casilla de votación de su zona de residencia en cualquier municipio rural o ciudad. El votante presenta un documento para su incorporación a la lista de votantes, y a continuación recibe la papeleta y dos sobres. En el sobre interior no tiene ninguna información sobre la identidad del votante y la papeleta de votación se introduce en este. El sobre interior se introduce a su vez en un sobre exterior y los detalles del votante se escriben sobre este último, de manera que, después del final de la votación anticipada, el sobre pueda ser entregado a la casilla de votación donde reside el elector. Allí se verifica si el votante tiene derecho a votar; después, el sobre interior se saca y se coloca sin abrir en la urna. El sistema de dos sobres garantiza que la elección del votante permanezca secreta. Adicionalmente, el registro de los datos acerca del sobre de votación por Internet en la lista de electores en la casilla electoral de residencia impide votar más de una vez.

Tras la votación por Internet, el elector realiza su elección, la cual es codificada (colocada en un sobre interior virtual). Después de eso el votante debe de aprobar su elección a través de su firma digital, lo que significa que se añaden sus datos personales al voto codificado (el sobre exterior). Los datos personales y el voto codificado se almacenan juntos hasta el conteo de los votos el día de la elección, con el propósito de comprobar que la persona ha emitido un solo voto.

Los datos personales del votante y su voto emitido se separan después de comprobar que el elector ha votado solo una vez y los votos repetidos han sido eliminados. Entonces es posible abrir el sobre interior solo después de que los datos de carácter personal añadidos al voto codificado han sido separados.

Esquema. Método de votación por Internet con doble sobre virtual



El *I-voting*, al igual que la votación fuera de la casilla electoral de residencia, es posible solo durante las elecciones anticipadas. Esto es necesario para garantizar que, al final, solo un voto es contabilizado por cada votante. Durante el proceso de votación por Internet, el derecho del elector a votar ha sido revisado, pero si el votante utiliza la posibilidad de anular su voto al ir a votar a la casilla electoral durante las elecciones anticipadas, entonces tiene que garantizarse que finalmente solo un voto se contabilice por cada votante. Para ello, a todos los centros de votación se les informa de los votantes por Internet, en su lista de electores al final de la votación anticipada y antes del domingo, el día de la elección. Si se encuentra en el centro de votación que el elector ha votado tanto por vía electrónica como con boleta de papel, la información se envía al CEN, que cancela el voto por Internet del elector. Antes de la verificación de los resultados de la votación, en la noche del día de la elección, los votos encriptados y las firmas digitales, con los datos personales o los sobres interior y exterior, se separan. Entonces todos los votos son abiertos por el CEN y contados. El sistema abre los votos solo si no están asociados con ningún dato personal.

3. *Arquitectura del sistema*

Los expertos estonios de seguridad en tecnologías de la información (TI), en su análisis de la seguridad,[17] publicado en 2003, declararon que en *sentido práctico* el sistema de *I-voting* estonio era lo suficientemente seguro como para su implementación. En sistemas absolutamente seguros, no son posibles eventos inesperados. Uno puede soñar con este tipo de sistemas, pero nunca se pueden obtener en la práctica. Esto se aplica en particular a los sistemas de voto por Internet. Considerando el nivel de seguridad de las computadoras personales, es imposible diseñar sistemas de *I-voting* que sean absolutamente seguros para todos los usuarios. El objetivo de seguridad más importante de la votación es no afectar los resultados finales y no abusar de los principios de la democracia. Los incidentes individuales con los usuarios siguen siendo importantes, pero no tienen influencia en el resultado final. Además, incluso en los sistemas de votación tradicionales, incidentes en pequeña escala son aceptables.[18]

[17] Disponible en *www.vvk.ee*

[18] Mägi, Triinu, *Practical Security Analysis of E-Voting Systems*, Universidad Tecnológica de Tallinn, tesis de maestría, 2007, *http://triinu.net/e-voting/* (consultado el 20 de diciembre de 2013).

La parte del voto por Internet en todo el proceso de organización de las elecciones es relativamente pequeña. El sistema utiliza los sistemas de información existentes: el Registro de Población como lista de votantes, el sistema de información sobre las elecciones del CEN, para la recopilación y publicación de información sobre los candidatos y los resultados de la votación, y de la infraestructura de Certification Centre Ltd. para comprobar la validez de los certificados de la tarjeta de identificación.

Los principales componentes de los sistemas de voto por Internet de Estonia son los siguientes: una Aplicación Independiente para Votantes a fin de que puedan emitir su voto, el Servidor de Expedición del Voto, el Servidor de Almacenamiento del Voto, el Servidor de Conteo del Voto y el Servidor de Monitoreo (*log-file*).

La criptografía asimétrica se utiliza para garantizar la secrecía del voto. Un par de claves se generan para el sistema en un módulo de seguridad de *hardware* especial para que su componente privado nunca abandone el voto. El componente público del par de claves está integrado en la aplicación de los electores y se utiliza para encriptar los votos. El componente privado del par de claves es utilizado en la Aplicación del Conteo de Votos para abrir los sufragios en la noche de la Jornada Electoral. El CEN puede abrir los votos, es decir, utilizar el componente privado, solo de forma colegiada. Después del final del periodo donde se atienden las posibles quejas, la clave privada se destruye.

4. *Perspectiva de los usuarios*

El sistema de voto por Internet se aprovecha de la infraestructura existente y de las bases de datos gubernamentales. Para votar electrónicamente, un votante no necesita registrarse de forma adicional. El votante necesita una tarjeta de identificación y una computadora conectada a Internet y con un lector de tarjetas instalado (no es necesario si se utiliza la identificación móvil). El votante también necesita códigos PIN para la autentificación y la firma. Puede usar las mismas herramientas para otras transacciones, incluidos los servicios electrónicos gubernamentales y la banca por Internet.

Desde la perspectiva del usuario, el procedimiento de votación es el siguiente:

1) El votante abre la página de votación *www.valimised.ee*.

2) El votante debe elegir la forma de identificarse a sí mismo (mediante una credencial de identificación o la identificación móvil).

3) Después de esto, el votante inserta la tarjeta de identificación en el lector universal de tarjetas e introduce el PIN 1 de la tarjeta de identificación 1 o teclea el PIN 1 en el teléfono móvil, en caso de contar con la identificación móvil.

4) El servidor comprueba si el votante es o no elegible (usando los datos del registro de población).

5) Se muestra la lista de candidatos del distrito electoral correspondiente.

6) El votante toma su decisión de voto, el sistema lo encripta.

7) El votante confirma su elección con una firma digital mediante la introducción del PIN 2 de la tarjeta de identificación o de la identificación móvil. El sistema verifica si la misma persona que se autentificó al inicio de la sesión dio la firma digital correspondiente. Además, la validez de la firma digital es verificada por el Servidor de Confirmación de Validez.

8) El sistema confirma que el voto se ha almacenado en el Servidor de Almacenamiento del Voto.

Como se ha señalado con anterioridad, las elecciones locales de 2013 ofrecieron la posibilidad para que el CEN realizara un proyecto piloto sobre la verificación: por primera vez los votantes tuvieron la posibilidad de verificar si su voto por Internet llegó al servidor central como se pretendía. Con el fin de comprobar el voto, los electores deben contar con un dispositivo inteligente (teléfono móvil o tableta) que tenga una cámara, conexión a Internet y una aplicación especial descargada de Internet. Inmediatamente después del procedimiento de votación se mostrará un código QR en la pantalla de la computadora donde se vota. El elector debe ahora de abrir la aplicación especial en el dispositivo inteligente y apuntar la cámara hacia el código QR en la pantalla. Después de leer el código, la aplicación contacta al servidor central de elecciones y descarga el voto electrónico encriptado (secreto) del elector. En pocos segundos la elección del votante aparece en la pantalla de su dispositivo inteligente y el elector puede comprobar si su voto ha llegado al servidor central de las elecciones y refleja su elección correctamente.[19]

V. Análisis del impacto

No se puede evitar el tema de la brecha digital, la cuestión de si la votación a través del Internet exacerba la diferencia de posibilidad de representación dentro de los grupos sociales. Lo que está claro es que el voto a través de Internet elimina las barreras físicas que dificultan la participación en las elecciones de los ancianos, discapacitados u otros grupos con movili-

[19] Véase más en *www.valimised.ee*.

dad reducida o que tienen dificultades para asistir a las casillas de votación (por ejemplo, personas que tienen horarios de trabajo muy apretados o que trabajan en el extranjero, padres de niños pequeños y personas que viven en regiones con escasa infraestructura), asumiendo, por supuesto, que estas personas tengan acceso a Internet.

Trechsel *et al.* concluyeron en sus informes preparados para el Consejo de Europa a raíz de la experiencia del voto por Internet de 2005 a 2011, que la educación y el ingreso monetario, así como el tipo de vivienda han sido factores insignificantes al momento de elegir Internet sobre otros medios de votación. Uno de los hallazgos más importantes de los estudios, hasta las elecciones de 2009, ha sido que no es tanta la división entre quienes tienen acceso a Internet y quienes no lo tienen, sino que claramente las habilidades de computación y la frecuencia de uso del Internet han sido importantes vaticinadores al momento de elegir el *I-voting*. Sin embargo, a partir de las elecciones locales de 2009, donde más de 100,000 votantes utilizaron el voto por Internet, estos factores se han desvanecido. La confianza en el procedimiento del voto por Internet ha sido a lo largo de los años el factor más significativo que dirige las decisiones de los votantes de utilizar o no el *I-voting*.[20]

El verdadero impacto del voto por Internet en el cambio en la participación de los votantes no se presta a un análisis objetivo. Se pueden determinar las variaciones de la participación de los votantes en los diferentes años de elecciones (comparando los tipos equivalentes de elecciones) y tratar de esclarecer las causas que sustentan las variaciones con la ayuda de estudios sociológicos. Tal vez la pregunta más importante es qué parte del electorado no hubiera participado en la votación, de no habérseles dado la oportunidad de votar por Internet. No existe forma de obtener evidencia empírica. Debemos, por tanto, atenernos a los dichos no verificables dados por los propios electores. La única excepción es el caso en el que el voto por Internet es la única posibilidad de votar para el elector, y él o ella utiliza esta posibilidad. Por ejemplo, las elecciones de los consejos locales de gobierno en Estonia no permiten votar en el extranjero mediante una papeleta postal o en una representación diplomática. No obstante, se prevé la posibilidad de votar a través del Internet.[21]

[20] Trechsel, Alexander H. y Vassil, Kristjan, *Internet Voting in Estonia: A Comparative Analysis of Five Elections Since 2005*, European University Institute, Report for the Estonian National Electoral Committee, 2011, *http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf* (consultado el 20 de diciembre de 2013).

[21] Madise, Ülle y y Vinkel, Priit, "Constitutionality of Remote Internet Voting: The Estonian Perspective", *Juridica International*, núm. XVIII, enero de 2011, pp. 4-16.

Tabla. Estadísticas del voto por Internet de seis elecciones

	2005 EL*	2007 EP**	2009 EPE***	2009 EL	2011 EP	2013 EL
Votos por Internet	9,681	31,064	59,579	106,786	145,230	136,863
Votos por Internet repetidos	364	789	910	2,373	4,384	3,045
Votantes por Internet	9,317	30,275	58,669	104,413	140,846	133,808
Votos por Internet cancelados por boletas de papel	30	32	55	100	82	146
Votos por Internet contabilizados	9,287	30,243	58,614	104,313	140,764	133,662
Votos válidos emitidos	496,336	550,213	396,982	658,213	575,133	625,336
Porcentaje de votos por Internet	1.9%	5.5%	14.8%	15.8%	24.5%	21.4%
Porcentaje de votos por Internet entre los votos anticipados	7.2%	17.6%	45.4%	44%	56.4%	50.5%
Votos por Internet emitidos desde el extranjero	n. a	2 %	3 %	2.8%	3.9%	4.2%

* EL: Elecciones Locales (municipales).
** EP: Elecciones Parlamentarias.
*** EPE: Elecciones al Parlamento Europeo.

La pregunta más intrigante para los partidos políticos es probablemente el impacto de la utilización del *I-voting* en los resultados. Aunque los partidos que favorecen la votación por Internet han acaparado a través de los años la mayoría de los votos electrónicos,[22] los estudios muestran que el auto posicionamiento izquierda-derecha no juega ningún papel importante al momento de elegir el medio de votación.[23] En 2005, el *I-voting* parece haber tenido un ligero efecto en el incremento de la participación de los electores que a veces votan y a veces no.[24] En 2007, ya aproximadamente un 10% de los votantes por Internet encuestados dijo que cierta o probablemente no habrían votado si no hubieran tenido la posibilidad de hacerlo a través del Internet. Trechsel y Vassil[25] mostraron que el porcentaje de los votantes por Internet encuestados que dijeron que ciertamente o probablemente no habrían votado de no haber tenido la posibilidad de hacerlo a través del Internet se había elevado al 16.3%, lo que permite concluir que la participación general pudo haber sido hasta un 2.6% menor en ausencia de este método de votación. Este ya es un marcador significativo cuando se considera el impacto del voto por Internet en la participación total.[26] Tres casos de *I-voting* en Estonia, en 2013, 2014 y 2015, también serán analizados por expertos de la Universidad de Tartu. Esta investigación ofrece una visión prolongada única acerca del desarrollo de este método de votación a lo largo de los años.

Aproximadamente una quinta parte de los encuestados que no votaron por Internet señaló que una razón para no votar por este método era la suficiencia del sistema de boletas de papel. La falta de confianza, con el 3.2%, y lo absurdo del *I-voting*, con un 1.9%, no fueron razones dominantes. Previo a la verdadera votación electrónica existía la preocupación de que la posibilidad de cambiar el voto por Internet iba a ser mal utilizada. No fue el caso. Las estadísticas generales muestran que el número de votos por Internet modificados fue insignificante. Como se señaló anteriormente, la influencia indebida de otros sobre los votantes por Internet es un problema teórico, pero potencialmente significativo, a pesar de que este tipo de amenazas son toleradas en el voto por correo en numerosas jurisdicciones. Si consideramos la experiencia de los electores durante las votaciones por

[22] *Idem*.

[23] Trechsel, Alexander H. y Vassil, Kristjan, *op. cit.*, nota 20, pp. 1-29.

[24] Breuer, Fabian y Trechsel, Alexander H., *E-voting in the 2005 Local Elections in Estonia: Report for the Council of Europe*, 2006, pp. 1-59. Disponible en la página web del Consejo de Europa.

[25] Trechsel, Alexander H. y Vassil, Kristjan, *op. cit.*, nota 20, pp. 1-29.

[26] Madise, Ülle y Vinkel, Priit, *op. cit.*, nota 21, pp. 4-16.

Internet, vemos que hay poca evidencia de coerción o preocupación acerca de la privacidad, basados en el comportamiento de los votantes. Los pequeños porcentajes de votos repetidos, así como el aumento significativo en el número total de votantes por Internet, a lo largo de los años, indican que la confianza en el sistema existente de *I-voting* ha crecido.

La hipótesis de que el *I-voting* premia las ventajas del electorado urbano no encontró pruebas que la respaldaran. El género no es un factor importante al elegir el voto por Internet de entre los posibles medios de votación. La edad, por el contrario, si es un factor bastante importante: la mayoría de los votantes por Internet en todas las elecciones pertenecen al grupo de edad de entre 18 y 39 años. Además, un interesante análisis del impacto del *I-voting* sobre la participación y el papel de los votantes, que de otro modo no se involucran en los asuntos públicos, ha sido realizado por Vassil y Weber en 2011.[27]

Sin embargo, la legitimidad del voto por Internet no puede juzgarse únicamente en función de su impacto sobre la alienación política. La legitimidad y constitucionalidad del voto por Internet, así como su impacto en la democracia, solo se discuten brevemente. Es demasiado pronto para hacer declaraciones contundentes sobre ese tema: por un lado, la experiencia del voto remoto por Internet tiene una base demasiado débil para ello, y por otro, el entorno sociopolítico está cambiando constantemente.

VI. Retos

1. *Administración electoral transparente*

¿Cómo crear confianza y garantizar la transparencia del voto electrónico? El voto por Internet representa nuevas oportunidades para mejorar el proceso electoral pero también presenta nuevos retos.

Los métodos simples han sido utilizados en Estonia para incrementar la comprensión y la confianza de los votantes en el sistema de *I-voting* en un intento de superar cualquier preocupación sobre la falta de transparencia y la complejidad. En todas las elecciones en las que se utilizó el voto por Internet, previo al periodo de votación, el gobierno permitió que todos los individuos elegibles para votar tuvieran la oportunidad de poner a prueba el sistema de *I-voting* con el fin de alentar a las personas para que vieran cómo funcionaba el sistema. Esto ayudó a los votantes a detectar cualquier proble-

[27] Vassil, Kristjan y Weber, Till, "A Bottleneck Model of E-Voting: Why Technology Fails to Boost Turnout", *New Media & Society*, Sage Journals, 2011, pp. 1-19.

ma que pudieran encontrar antes de que el verdadero periodo de votación por Internet comenzara. En Estonia, las principales preocupaciones entre los funcionarios electorales del país, los observadores externos, los partidos políticos y los ciudadanos, se relacionan con la adquisición del *hardware* y *software* necesarios para utilizar una tarjeta de identificación en una computadora personal, con la actualización de los certificados vencidos de las tarjetas de identificación o de identificación móvil, y con la renovación de los códigos PIN necesarios para el uso electrónico de la tarjeta de identidad o de identificación móvil.

Como elemento adicional de transparencia, el número de electores por Internet que habían votado con boletas de papel se actualizaba regularmente en la página web del *I-voting*. Este sencillo proceso permitía al público nacional más amplio, así como a los partidos políticos y a los medios de comunicación, saber cuántos votantes por Internet habían votado y determinar si la tendencia en el número de votantes por Internet emitiendo votos mediante boletas de papel parecía razonable. Al final, las personas fueron también capaces de comparar el número de votantes por internet con el número de votos electrónicos escrutados.

Con el fin de convencer a los votantes de que sus votos habían sido registrados correctamente, estos tenían la opción para comprobar si su voto válido por Internet se reflejaba en las listas de votación el día de la elección a fin de evitar que se votara más de una vez. Una segunda opción para verificar la exactitud de un voto por Internet válido era posible durante el periodo de votación anticipada. Si el votante decidía reemplazar su voto por Internet por uno nuevo, recibía una notificación del voto por Internet registrado anteriormente.

2. *Observación en la práctica*

De acuerdo con la legislación electoral de Estonia, todas las actividades relacionadas con las elecciones son públicas. Los observadores tienen acceso a las reuniones de todos los comités electorales y pueden seguir todas las actividades electorales, incluyendo el proceso de votación, el conteo y la tabulación de los resultados. Con el voto por Internet no ha sido diferente. Todos los documentos importantes describiendo el sistema de *I-voting* se pusieron a disposición de todos, incluidos los observadores. A fin de aumentar el conocimiento de los observadores sobre el sistema, se invitó a los partidos políticos a participar en un curso de capacitación antes de cada elección. Además de los partidos políticos, los auditores y otras personas interesadas

en el sistema de votación por Internet también tomaron parte en el entrenamiento, el cual fue seguido por encuestas de los procedimientos concretos que eran necesarios para instalar el sistema de *I-voting*. Los observadores fueron invitados también a una prueba del proceso de escrutinio.

A lo largo del periodo de observación de un mes del voto por Internet, el principal instrumento de observación fue la comprobación de las actividades del comité de votación electrónica comparando la documentación escrita describiendo los procedimientos necesarios. La función principal de gestión requirió de una atención especial, ya que la seguridad y el anonimato de los votos por Internet se basan en el encriptado y descifrado de los votos. Durante el evento de conteo —el punto culminante del periodo electoral— la gestión de la clave privada de los sistemas, que es la garantía de la secrecía electoral, se demostró a los observadores. Esta clave, dividida en siete piezas, estaba resguardada por el CEN, y sus miembros abrieron colegiadamente los votos encriptados anónimos. El proceso del conteo de las boletas se llevó a cabo con observadores que podían ver todas las actividades de escrutinio de las boletas en grandes pantallas en el área de observación. El proceso fue narrado completamente y los observadores fueron capaces de seguir cada paso.

Es importante que los observadores se desplieguen durante el tiempo necesario para permitir una observación significativa. Si algunas etapas importantes que influyen en la exactitud de los resultados finales no han sido observadas, las conclusiones acerca de la integridad del sistema no se pueden hacer. Especialmente para los observadores extranjeros, la longitud del periodo de observación parece ser un desafío. La OSCE hizo auditorías en las elecciones de 2007 y 2011, y en su último informe señala: "La OSCE, en términos generales, encontró una confianza generalizada en la conducción de la votación por Internet por parte del CEN. Sin embargo […] un control más detallado y formal de la instalación del *software* e información sobre las pruebas del sistema de voto por Internet podrían aumentar aún más la transparencia y la verificabilidad del proceso".[28]

3. *Validación de los sistemas y procedimientos de votación*

A fin de validar el sistema de votación electrónica, los procedimientos de certificación, pruebas y auditorías deben de ser considerados. Actualmente no existe un organismo nacional o internacional que sea capaz para

[28] *OSCE/ODIHR Election Assessment Mission Report*, Estonia, Parliamentary Elections, 6 de marzo de 2011, *http://www.osce.org/odihr/77557* (consultado el 20 de diciembre de 2013).

certificar el sistema de votación por Internet estonio. En su lugar, Estonia utiliza un sistema similar al usado en otros países (y en casos similares), donde el código fuente del sistema es auditable y los procedimientos operativos han estado bajo una fuerte supervisión de los auditores. Las pruebas del sistema, previas a las elecciones, son también una parte importante a fin de controlar la funcionalidad y la precisión por parte de analistas contratados, observadores y el público.

El sistema de votación por Internet de Estonia fue desarrollado con el principio subyacente de que todos los componentes del sistema deben de ser transparentes para fines de auditoría: los procedimientos están plenamente documentados y los procedimientos críticos se registran, auditan, observan y videograban (desde 2013 también se publican en *Youtube*), mientras se llevan a cabo. El procedimiento de auditoría, realizado en cada elección, revisa y monitorea los aspectos de seguridad sensibles del proceso, tales como la actualización de la lista de electores, la preparación del *hardware* y su instalación, la carga de los datos de la elección, el mantenimiento y la renovación de los datos electorales y el proceso de conteo de los votos.[29]

Un requisito común es que el código fuente del sistema de votación debe de estar disponible para auditarse públicamente. En Estonia, sin embargo, hasta 2013 el código no estaba universalmente disponible, pero uno podía acceder a este si se firmaba una NDA con el CEN. Sin embargo, después de los segundos debates legales mencionados anteriormente, en 2013, el código fuente de todos los servidores centrales del sistema de votación, así como el *software* de la aplicación de la verificación de la votación se puso de forma disponible en Internet. Este es un paso importante para crear una mayor transparencia, y por lo tanto, una mayor confianza hacia el propio concepto de votación por Internet.

VII. Conclusiones

Estonia es el primer país del mundo en el que el voto por Internet con resultados vinculantes fue utilizado con éxito en todo el país. El electorado estonio completo ha tenido seis veces la posibilidad de emitir el voto a través de Internet en elecciones locales (2005, 2009 y 2013), parlamentarias (2007 y 2011) y para el Parlamento Europeo (2009). El lanzamiento del

[29] Vinkel, Priit, "Internet Voting in Estonia", en Laud, Peeter (ed.), *Information Security Technology for Applications*, 16th Nordic Conference on Security IT Systems, NordSec 2011, Talinn, Estonia, 26-28 de octubre de 2011, Lecture Notes in Computer Science, vol. 7161, Springer Verlag, Berlin, 2012, pp. 4-12.

I-voting constituye un genuino cambio cualitativo en el desarrollo del sistema y la administración electorales. La experiencia del voto por Internet estonio demuestra que es posible garantizar la conformidad del *I-voting* remoto con todos los principios constitucionales electorales, incluyendo el principio de secrecía.

La tarjeta de identificación como un documento de identificación principal en Estonia con dos funciones obligatorias —autentificación remota y firma digital— ha sido la piedra angular del sistema del doble sobre virtual. Así, tanto la identificación confiable del votante como el anonimato del voto y el correcto conteo de los sufragios están garantizados.

Un factor importante que explica la posibilidad de poner en marcha soluciones completamente nuevas como la votación por Internet en Estonia es el tamaño pequeño del país. Lennart Meri, el fallecido presidente de la República de Estonia, comparó en su discurso en el colegio St. Olaf de Minnesota el 6 de abril de 2000 a Estonia con un bote pequeño: "Un súper petrolero necesita dieciséis millas náuticas para cambiar de curso. Estonia, por el contrario, es como un kayak esquimal, capaz de cambiar su rumbo en el acto".

Mientras no se garantice el acceso universal a Internet y la autentificación segura de los votantes, las dudas relacionadas con la neutralidad política de esta técnica probablemente permanecerán. Sin embargo, el *I-voting* debe de ser considerado como un servicio público esencial en una sociedad de la información. Los problemas con las máquinas de votación que afrontan muchos países, como Estados Unidos, Alemania o los Países Bajos, no deben de hacerse extensivos a la votación remota por Internet, aunque eso no quiere decir que el *I-voting* esté libre de riesgos.

La pregunta básica en la administración electoral ya no se centra en si los nuevos desarrollos tecnológicos son aceptables en los procesos electorales, sino en qué tipo de tecnología es la adecuada para cada país, teniendo en cuenta su tradición política y su cultura social, el nivel de su infraestructura tecnológica, y su sistema electoral. En el caso de Estonia, las condiciones previas fueron favorables para la introducción del cambio más ambicioso en la naturaleza de las votaciones: votar a través de Internet.

VIII. Bibliografía

Breuer, Fabian y Trechsel, Alexander H., *E-voting in the 2005 Local Elections in Estonia: Report for the Council of Europe*, 2006. Disponible en la página web del Consejo de Europa.

BUCHSTEIN, Hubertus, "Online Democracy. Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory", en Kersting, Norbert y Baldersheim, Harald (comp.), *Electronic Voting and Democracy. A Comparative Analysis*, Basingstoke, Palgrave Macmillan, 2004.

DRECHSLER, Wolfgang, "Dispatch from the Future", *The Washington Post*, The Washington Post Company, 5 de noviembre de 2006.

_____ y Annus, Taavi, "Die Verfassungsentwicklung in Estland von 1992 bis 2001", en Häberle, Peter (ed.), *Jahrbuch des öffentlichen Rechts der Gegenwart*, Tübingen, Mohr Siebeck, 2002.

_____ y Madise, Ülle, "Electronic Voting in Estonia", en Kersting, Norbert y Baldersheim, Harald (comp.), *Electronic Voting and Democracy. A Comparative Analysis*, Basingstoke, Palgrave Macmillan, 2004.

EUROSTAT 2013, *Survey on Individuals regularly using the Internet and on Households - Level of Internet Access. General Description of e-Voting*, 2004, NEC.

FORO ECONÓMICO MUNDIAL, *The Global Information Technology Report 2013*.

HEIBERG, Sven *et al.*, "On E-Vote Integrity in the Case of Malicious Voter Computers", en Gritzalis, Dimitris *et al.* (eds.), *Computer Security – ESORICS 2010*, *15th European Symposium on Research in Computer Security*, 20-22 de septiembre de 2010, Atenas, Springer-Verlag Berlin Heidelberg, Lecture Notes in Computer Science, 2010.

MADISE, Ülle, "Legal and Political Aspects of the Internet Voting: Estonian Case", en Reniu, Joseph M. (ed.), *E-voting: The Last Electoral Revolution*, Barcelona, Institut de Ciències Politiques i Socials, 2008.

_____ y Maaten, Epp, "Internet Voting in Estonia", en Ríos Insua, David y French, Simon (comp.), *E-Democracy: A Group Decision and Negotiation Perspective*, Nueva York, Springer Science+Business Media, 2010.

_____ y Martens, Tarvi, "E-Voting in Estonia 2005. The First Practice of Country-wide binding Internet Voting in the World", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006.

_____ y Vinkel, Priit, "Constitutionality of Remote Internet Voting: The Estonian Perspective", *Juridica International*, núm. XVIII, enero de 2011.

MÄGI, Triinu, *Practical Security Analysis of E-Voting Systems*, Universidad Tecnológica de Tallinn, tesis de maestría, 2007, *http://triinu.net/e-voting/* (consultado el 20 de diciembre de 2013).

MÄLKSOO, Lauri, "Von der Demokratie bis zur Diktatur: ein verborgener Dialog zwischen Artur-Tõeleid Kliimann und Carl Schmitt", *Der Staat*, vol. 43, núm. 1, 2004.

MONNOYER-SMITH, Laurence, "How e-Voting Technology Challenges Traditional Concepts of Citizenship: An Analysis of French Voting Rituals", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006.

NARITS, Raul, "Rechtssprache und juristische Semantik im sozialen Kontext der estnischen Rechts - und Lebensordnung", en Krawietz, Werner y Narits, Raul (eds.), *Rechtstheorie. Internationales Symposium der Estnischen Juristischen Fakultät in Tartu. Sonderheft Estland*, vol. 31, núm. 3-4, 2001.

OSCE/ODIHR Election Assessment Mission Report, Estonia, Parliamentary Elections, 6 de marzo de 2011, *http://www.osce.org/odihr/77557* (consultado el 20 de diciembre de 2013).

SKAGESTEIN, Gerhard *et al.*, "How to Create Trust in Electronic Voting over an Untrusted Platform", en Krimmer, Robert (ed.), *Electronic Voting 2006*, Bonn, Gesellschaft für Informatik, 2006.

TRECHSEL, Alexander H. y Vassil, Kristjan, *Internet Voting in Estonia: A Comparative Analysis of Five Elections Since 2005*, European University Institute, Report for the Estonian National Electoral Committee, 2011, *http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf* (consultado el 20 de diciembre de 2013).

VASSIL, Kristjan y Weber, Till, "A Bottleneck Model of E-Voting: Why Technology Fails to Boost Turnout", *New Media & Society*, Sage Journals, 2011.

VINKEL, Priit, "Internet Voting in Estonia", en Laud, Peeter (ed.), *Information Security Technology for Applications*, 16th Nordic Conference on Security IT Systems, NordSec 2011, Talinn, Estonia, 26-28 de octubre de 2011, Lecture Notes in Computer Science, vol. 7161, Springer Verlag, Berlin, 2012.

VIII Ülle Madise, **Priit Vinkel** and Epp Maaten. 2006. *Internet Voting at the Elections of Local Government Councils on October 2005*. Report. Tallinn: Estonian National Electoral Committee. (6.7)

Internet Voting
at the Elections of Local Government Councils
on October 2005

Report[1]

The purpose of the report is to give an overview of the preparations of Estonia's e-voting project and find answers to possible social-scientific questions connected with Estonia's e-voting project.

Contents

[1] Report is written by Ülle Madise, Priit Vinkel and Epp Maaten. The authors wish to thank Liia Hänni, Mihkel Pilving, Heiki Sibul, Tarvi Martens, Wolfgang Drechsler, Alexander Trechsel, Silver Meikar, Marika Kirch, Arne Koitmäe and Peeter Marvet.

Appendix:

Tables:

Figures:

1. Background Information

1.1 Use of Terms

Throughout the Report, the term 'e-voting' is used to denote voting on the Internet; the term is used in the same meaning also by the Estonian public.

Besides voting on the Internet, the concept of electronic voting or e-voting also embraces other electronic voting methods, including methods of casting, forwarding and counting the votes. Thus the concept of e-voting is wider than voting on the Internet, and Estonia's e-voting includes casting the vote as well as forwarding and counting the votes.

The purpose of implementation of voting on the Internet in Estonia is not to replace the existing ways of voting in the nearest future.

1.2. Eligible residents

People who have gotten used to fundamental reforms in recent years are comparatively open to innovative solutions. Estonia, whose number of population is relatively small, sees itself as a successful e-state: Internet access is easy and genuinely available to the majority of the population, also the number and availability of e-services is increasing year by year.

In terms of e-voting the most important factor is the mandatory ID card that has the functions of remote authentication of persons and digital signature. The small number of population enabled to implement the ID card project very quickly: since 2002 it is compulsory to hold an ID card[2]. By February 2006 over 900.000 cards are issued, thus, 65% of Estonian residents hold the ID-card (source: AS Sertifitseerimiskeskus, *http://www.sk.ee/cgi-bin/cards.py*).

Table 1 Number of Population in the Local Government Council Election Years
Source: Statistical Office of Estonia (http://pub.stat.ee)

YEAR OF ELECTIONS	1993	1996	1999	2002	2005
Number of population	**1 511 303**	**1 425 192**	**1 379 237**	**1 361 242**	**1 347 510**

The number of eligible voters at the local government council elections has been increasing year by year. Besides the citizens of Estonia and other EU member states, aliens residing in Estonia who are not citizens of the EU but have lived in one and the same town or municipality of Estonia at least five consecutive years are also eligible to vote at the local government council elections.

[2] Identity Documents Act § 39 (http://www.legaltext.ee/text/en/X30039K10.htm)

Table 2 Number of Population with the Right to Vote in the Local Government Council Election Years
Source: web page of National Electoral Committee (http://www.vvk.ee)

ELECTIONS	LGC 1993	LGC 1996	LGC 1999	LGC 2002	LGC 2005
Number of eligible voters	**880 296**	**879 034**	**1 062 028**	**1 021 439**	**1 059 292**

Large part of the people of Estonia live in urban areas, this facilitates Internet access and also creates possibilities for using ID card for e-voting. Projects like "Village road" for spreading Internet using skills and access to the Internet also reach also rural regions. More than 1,000 free Internet access points have been opened all over Estonia, possibility to use the Internet is also offered at public libraries. Since 1 January 2006 all legal acts are available only through the Internet, in the electronic *Riigi Teataja*, which in its turn requires facilitating Internet access.

Table 3 Urbanisation indicators in 2005
Source: Statistical Office of Estonia (http://pub.stat.ee)

	Number	%
Population in towns	898 136	66,7
Population of rural municipalities	449 374	33,3

Table 4 Number of Population in Tallinn and Tartu in 2005
Source: Statistical Office of Estonia (http://pub.stat.ee)

	Number	%
Tallinn	396 010	**29,4**
Tartu	101 483	7,5
Total population of Estonia	1 347 510	100,0

1.3. Economic Welfare in Election Years

As economic welfare is one of the factors that influence voter turnout in voting and trust in the state, it has been described below through average gross salary, gross domestic product and state budget volume in election years. The possible influence of economic welfare on voter turnout and attitude towards e-voting is not dealt with in this report.

Table 5 Average Gross Salary in the Election Years
Source: Statistical Office of Estonia (http://pub.stat.ee)

YEAR OF ELECTIONS	1993	1996	1999	2002	2005
Average gross salary	**1069 EEK 69 •**	**2986 EEK 191 •**	**4418 EEK 283 •**	**6110 EEK 392 •**	**7835 EEK 502 •**

The growth rate of average gross salary in 2005 in comparison to the previous year was 11.8%.

Table 6 Volume of State Budget in Election Years
Source: Statistical Office of Estonia (http://pub.stat.ee)

YEAR OF ELECTIONS	1993	1996	1999	2002	2005
State budget million EEK •	**4 151** **266**	**13 368** **857**	**17 571** **1 126**	**33 639** **2 156**	**53 072** **3 402**

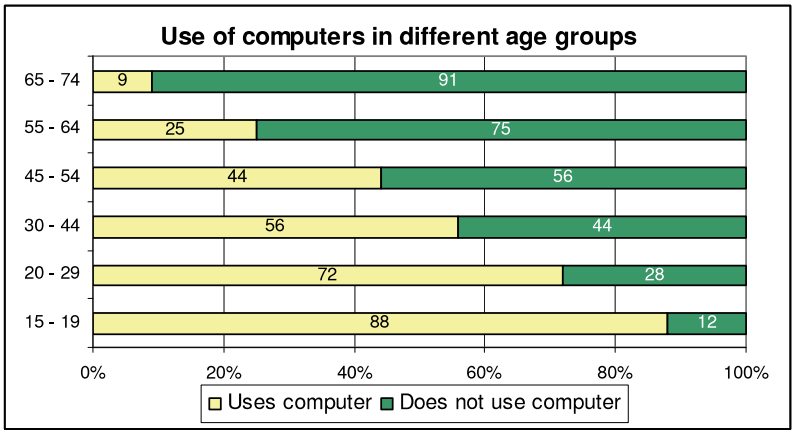
Table 7 GDP in Election Years
Source: Statistical Office of Estonia (http://pub.stat.ee)

YEAR OF ELECTIONS	1993	1996	1999	2002	2005
GDP million EEK •	**22 820** **1 462**	**55 895** **3 583**	**81 775** **5 241**	**116 915** **7 494**	**141 493** **9 070**

1.4. Internet Access

In Estonia the use of digital channels is steadily widening. Over 50 % of residents of Estonia use Internet, 40% of households have a computer at home and 81% of home computers are connected to the Internet[3]. Nowadays all schools and public libraries have Internet connection. Many national projects like "Vaata Maailma, "Tiigrihüpe" and "Külatee" have been successfully carried out to ensure for all Estonian citizens benefits related to the use of computers and the internet and to increase the supply and availability of fast internet connections.

Table 8 Use of Computers in Different Age Groups in 2004
Source: Eesti elavik 21. sajandi algul (Life-World of Estonia at the Beginning of the 21 Century), Tartu 2004



The results of the study of 2004 that were the source material for *Eesti elavik* and according to which **48%** of the population of Estonia used the computer (**57% of them** every day), can be compared with the data of TNS Emor study on 2004 and 2005.[4]

[3] Survey „E-Seire", TNS Emor Sept-Nov 2005
[4] The book "Eesti elavik 21. sajandi algul" (*Life-World of Estonia in the Beginning of the 21 Century*; editors Veronika Kalmus, Marju Lauristin and Pille Pruulmann-Vengerfeldt, TÜ kirjastus 2004) is a survey of the results of broad research "Mina. Maailm. Meedia." (*I. World. Media*).

Table 9 Use of Computers in Different Age Groups in 2004 and 2005
Source: TNS Emor 2005

AGE IN YEARS	MARCH–MAY 2004, % OF THE STUDIED GROUP	MARCH–MAY 2005, % OF THE STUDIED GROUP
6 - 9	47	57
10 - 14	86	91
15 - 24	88	91
25 - 34	71	71
35 - 49	49	50
50 - 74	17	19

1.5. E-Services

Electronic X-road environment (http://x-tee.riik.ee) embraces the e-services offered by the state. 355 institutions and 50 national data bases are already connected through it. 106,346 citizens, 30,000 more than the year before, used the X-road environment in 2005.

E-services in use are follows:
* X-road – data exchange layer and citizen portal through which enquiries can be made from following registers:
    - Estonian Health Insurance Fund
    - Estonian Motor Vehicle Registration Centre
    - Register of Construction Works
    - Databases of Citizenship and Migration Board
    - Land cadastre
    - Register of mandatory funded pension
    - Register of professional certificates
    - Land Information system
    - Register of Economic Activities
    - State Pension Insurance Register
    - Population Register
    - Databases of National Examination and Qualification Centre
    - SAIS - Admissions Information System to higher education institutions
    - Register of weapons
    - Database of individuals and cases pending in execution procedure
    - Commercial Register
    - The Register of Students of Higher and Vocational Education Institutions
* E-services of Estonian banks
* Electronic catalogue of Estonian libraries
* Electronic state gazette “Riigi Teataja”
* Electronic management systems of draft legislation
* E-Kool – system enabling to monitor over Internet grades given at school.
* Citizen’s portal www.eesti.ee
* TOM-portal
* Database of Court Decisions
* E-billing portal

* eTaxBoard for forwarding tax declarations online
* Electronic services of the Estonian Agricultural Registers and Information Board

For using e-services whether the identification systems of private banks or ID card can be used. Besides electronic identity and digital signature the ID card is also used as library card, travel card on public transport, Health Insurance Fund membership card etc.

The most widespread and used e-service is the Internet bank: 72% of adult Internet users use online banking services.[5] Electronic submission of income declarations has become very popular. According to Tax and Customs Board, 76% of declarations were submitted electronically in 2005. This tendency has been increasing year by year.

It is planned to develop new e-services, including an electronic childcare service environment, paper-free car register and e-health project etc. Transition to digital correspondence between state agencies and between citizens and state agencies is intended. More information about e-services can be found on website www.riso.ee/en.

1.6. ID-Card[6]

Estonian e-voting system is based on ID card. As far as it is known, Estonia is the only state in the world where an ID card enabling remote identification of persons and digital signing is compulsory and issued to more than half of the population. As of February 2006, more than 900,000 had been issued, thus about 65% of the population holds an ID card.

According to the Identity Documents Act, citizens of Estonia and aliens staying permanently in Estonia must hold an ID card. A certificate which enables digital identification and a certificate which enables digital signing shall be entered on each identity card.

Extract from the Identity Documents Act:

§19.

Basis for issue of identity cards*(1) An identity card is an internal document held by an Estonian citizen or an alien staying permanently in Estonia. Identity cards shall be issued to the following:*
1) Estonian citizens;
2) aliens staying (residing) permanently in Estonia who have valid residence permits.

1[1]) An Estonian citizen may cross the Estonian state border which also is a border between Member States of the European Union with a valid identity card.

2) Other documents established by this Act shall be issued on the basis of data entered on the identity card of the person concerned. This subsection does not apply to persons who, pursuant to this Act, need not hold an identity card.

[RT I 2004, 28, 189 – entered into force 1. 05. 2004]

§19[1]. Digital data to be entered on identity card

[5] TNS Emor e-monitoring 2nd period 2005
[6] *source www.id.ee, www.pass.ee*

(1) A certificate which enables digital identification and a certificate which enables digital signing shall be entered on an identity card. The list of other digital data entered on an identity card shall be approved by the Government of the Republic, having regard to the provisions of subsection 9 (3) of this Act.

(2) If a certificate is entered in a document within the meaning of the Digital Signatures Act (RT I 2000, 26, 150; 92, 597), a description of the limitations on the scope of use shall not be entered in the certificate.

(3) Certification service providers specified in subsection 18 (1) of the Digital Signatures Act shall issue certificates specified in subsection (1) of this section.

[RT I 2001, 56, 338 – entered into force 7. 07. 2001]

The project of an ID card enabling remote identification and digital signing was initiated in 1997. The obligation to hold an ID card was established by the Identity Documents Act which was adopted in 1999 and entered into force on 1 January 2000, and according to which the holding of ID card is obligatory since 1 January 2002. In 2000 the provision on the possibilities of digital using of ID card was added to the Act. In addition to that, the Digital Signature Act was adopted in March 2000. .

Subsection 3 (1) of Digital Signature Act stipulates: "A digital signature has the same legal consequences as a hand-written signature if these consequences are not restricted by law and if the compliance of the signature with the requirements of subsection 2 (3) of this Act is proved." and subsection 4 (3): "State and local government agencies, legal persons in public law, and persons in private law performing public law functions are required to provide access through the public data communication network to information concerning the possibilities and procedure for using digital signatures in communication with such agencies and persons."

Subsection 5 (6) of Administrative Procedure Act stipulates: "In administrative procedure, electronic operations shall be equal to written operations. Digital signatures shall be used in administrative procedure pursuant to the procedure provided for in the Digital Signatures Act and other legislation."

Similarly to administrative procedure, in court proceedings it is also possible to present all procedural documents digitally signed.

Upon the issue of ID card a person is given two PIN codes. PIN 1 is meant for digital identification of a person and PIN 2 for digital signing. Besides that, an e-mail address (in the format firstname.lastname@eesti.ee) is given with the ID card. The PIN codes and PUK code necessary for the electronic use of the ID card are known only to the owner of the card, the codes are issued in a safety envelope together with the ID card. Digital signature is verified and authenticated to another party by Sertifitseerimiskeskus AS who provides certification service and also administers the list of suspended and revoked certificates.

The problem that had to be solved before the implementation of e-voting was the updating of ID card certificates and restoring PIN codes. The period of validity of ID card is ten years, but the period of validity of ID card's security certificates is three years. Thus part of the certificates had expired immediately before the elections in 2005. On the other hand, most of the ID card holders do not use the card electronically and they have no need for PIN codes, so they have been lost or destroyed in the course of time. E-services which require ID card with codes have been created but in most cases it is possible to use these services also with the help of identification systems offered by banks that do not require the procurement and adjustment of a card reader.

A campaign was organised before the elections to inform the cardholders of the need to update the certificates and a possibility to get new PIN codes free was created. The purpose was to establish conditions for the use of ID card at e-elections for as many people as possible.

ID card holders whose certificates expire in less than 105 days and whose certificates have not been suspended or revoked can update their certificates free of charge. Certificates can be updated on ID card web page (www.sk.ee/id-kontroll) and on Citizenship and Migration Board web page (http://www.mig.ee/est/paringud/isikuparing). The certificates can also be updated at the Citizenship and Migration Board offices and the information desk of certification centre at Tallinn City Government Service Bureau. As the e-services for which codes are needed are relatively few and little used, many ID card holders had lost or forgotten their codes. Lost or forgotten PIN codes could be renewed at Citizenship and Migration Board offices, Tallinn City Government Service Bureau and *SEB Eesti Ühispank* and Hansapank offices. At the banks the envelope with new PIN codes had to be redeemed for EEK 90.

The card looks as follows.

Figure 1. Description of the identity card (ID-card) of the Republic of Estonia
Source: www.id.ee

The front side of the card contains the card holder's signature and photo, and also the following data:

- name of card holder
- personal code (national ID code) of card holder
- card holder birth time
- card holder sex
- card holder citizenship
- card number
- card validity end

The back side contains the following data:

- card holder birth place
- card issuing date
- residence permit details and other information (if applicable)
- card and holder data in machine-readable (ICAO) format

1.7. Electronic Data Transmission and Processing at Earlier Elections

Already for years the registration of electors has been electronic in Estonia, and on the basis of it the lists of voters are printed out. This has been one of the preconditions for the implementation of electronic voting.

The public's peaceful reaction to the e-voting project may be explained with the fact that according to wider definitions e-voting has taken place in Estonia for years (according to the definition in the recommendation of Council of Europe[7], e-voting is using electronic means in one or several stages of election procedures).

In the 1990s the main means of data transmission were telephone, fax and electronic mail, but in 1999 the National Electoral Committee started using Internet-based electoral information system (EIS).

The system is used by all electoral committees of different levels (electoral committees of divisions, rural municipalities, cities and counties). HTML screen formats are used for collecting and updating the data in the infosystem user interface. Electoral committees who have username and password have access to user interface. Each committee can transmit and change only their own data and the data of their subcommittees. National Electoral Committee coordinates the use of the system.

Central database and web servers that serve all data entry points are the focal part of electoral information system. Only Internet connection and web browser are needed in the user's workplace computer. In the centre, all users are served and the received data is collected into the database. The database can be used for generating in real time suitable outlets to the National Electoral Committee web page which is the main channel for publication of data.

Data base of the electoral information system contains data of electoral districts, electoral committees, polling divisions, candidates, political parties and election coalitions (determined when the elections are prepared), and voting and election results (received when the elections are carried out). On the average three months before the election day the establishing of data base for these elections begins and the active use period of EIS ends about a week after the elections.

In connection with the implementation of e-voting in 2005 EIS was the channel through which the information exchange guaranteeing that each voter could vote only once took place. Also the results of e-voting from vote counters, i.e. from the National Electoral Committee reached the electoral committees of rural municipalities and cities in electronic form through EIS.

EIS is constantly developing, proceeding from experience and growing needs. In 2007 it is planned to establish a direct connection between EIS and population register in order to control the right to vote, information on the residence etc. of the candidates and members of committees entered into EIS database.

Although a large amount of data is collected electronically via EIS, alternative ways of data transmission can also be used by those electoral committees who have no access to the Internet and computer in the polling place or its immediate vicinity.

[7] Recommendation Rec(2004)11 "Legal, operational and technical standards for e-voting"

It must be noted that as all polling divisions are not yet equipped with computers and Internet connection, the lists of voters are still printed out on paper, and when the printed lists and electronic data are compared, it is checked that only one vote is counted for each voter.

1.8. Electoral System

In Estonia local government councils are elected for four years on the basis of proportional electoral system.[8] Each voter has one vote.

Not later than on the 90th day before the election day the local government council forms electoral districts, as a rule there is one electoral district on the territory of one rural municipality or city. In Tallinn the electoral districts are formed on the basis of city districts.[9]

2005. At the time of the local government council elections in 2005 there were 227 cities and rural municipalities, but 240 electoral districts in Estonia.

A simple quota shall be calculated for each electoral district, which shall be obtained by dividing the number of valid votes cast in the electoral district by the number of mandates. A candidate in favour of whom the number of votes cast exceeds or equals the simple quota shall be elected. Mandates which are not distributed in electoral districts on the basis of a simple quota shall be distributed as compensation mandates between the political parties and election coalitions whose candidates receive at least 5 per cent of the votes nationally. To be elected, an independent candidate must collect the number of votes that equals or exceeds the simple quota.

For the distribution of mandates the candidates shall be re-ranked according to the number of votes received by each candidate. If at least two candidates receive an equal number of votes, the candidate who is further towards the bottom of the list shall be ranked ahead. The votes cast for candidates standing in the list of candidates of the same political party or an election coalition shall be totalled. Mandates are divided according to the d'Hondt distribution method (with the distribution series of 1, $2^{0.9}$, $3^{0.9}$, 4, etc). If the comparative figures of at least two political parties or election coalitions are equal, the political party or election coalition whose candidates are further towards the bottom of the general list of candidates in the electoral district shall be given the mandate.

[8] Due to relative smallness of electoral districts and the use of modified d'Hondt method that prefers larger vote collectors, the level of unproportionality has increased in converting the votes to mandates.

[9] Local Government Council Election Act (RT I 2002, 36, 220) § 8

1.9. Voter Turnout

Table 10 Voter Turnout at Local Government Council Elections
Source: National Electoral Committee web page

ELECTIONS	LGC 1993	LGC 1996	LGC 1999	LGC 2002	LGC 2005
Number of voters	**464030**	**462439**	**530723**	**536044**	**502504**
Voter Turnout (%)	**52,71**	**52,61**	**49,97**	**52,48**	**47,44**

Voter turnout in municipal elections is generally smaller than in parliamentary elections. At the Riigikogu elections turnout has been somewhat bigger (58% in 2003) but the participation rates did not exceed 70 per cent even at the referendum of 1992 when the Constitution was adopted (it was 67% then) nor at the first round of voting at presidential elections (68%).

1.10. E-Voting Debate at the Riigikogu

E-voting was legalised in all election acts in 2002, when there were the following political parties in the parliament:

- Estonian Centre Party with 28 mandates
- Estonian Coalition Party with 7 mandates
- Estonian People's Union with 7 mandates
- Isamaaliit with 18 mandates
- Reform Party with 18 mandates
- United People's Party of Estonia with 6 mandates
- People's Party Mõõdukad with 17 mandates

Due to proportional election system all political parties with wider support are represented in the Riigikogu. Estonian Centre Party, Estonian Coalition Party, Estonian People's Union, Reform Party and United People's Party of Estonia supported e-voting, Isamaaliit and Mõõdukad were against.

The chronology of the act on e-voting was the following:

1. Initiation of the draft of Local Government Councils Election Act 30 April 2001

2. First reading of the bill at the Riigikogu 13 June 2001
(http://web.riigikogu.ee/ems/stenograms/2001/06/t01061318-28.html#P2693_612185)

3. Second reading of the bill at the Riigikogu 23 January 2002
(http://web.riigikogu.ee/ems/stenograms/2002/01/t02012302-07.html#P258_62979)

4. Resumption of the second reading of the bill at the Riigikogu 27 February 2002
(http://web.riigikogu.ee/ems/stenograms/2002/02/t02022706-12.html#P497_105059)

5. Resumption of the second reading of the bill and adoption of the Act at the Riigikogu 27 March 2002 Result of voting (55 in favour, 31 against, 0 abstentions)
(http://web.riigikogu.ee/ems/stenograms/2002/03/t02032709-07.html#P385_68538)

(The Act entered into force on 6 May 2002)

In 2003 the following political parties were elected to the Riigikogu (number of mandates after the elections):

- Estonian Centre Party with 28 mandates (www.keskerakond.ee)
- Estonian People's Union with 13 mandates (www.erl.ee)
- *Isamaaliit* with 7 mandates (www.isamaaliit.ee)
- Reform Party with 19 mandates (www.reform.ee)
- Res Publica with 28 mandates (www.respublica.ee)
- Social-Democratic Party 6 mandates (www.sotsdem.ee)

In 2005, at the debates on making amendments to e-voting provisions, the division of mandates was the following:

- Estonian Centre Party with 20 mandates
- Estonian People's Union with 16 mandates
- *Isamaaliit* with 7 mandates
- Reform Party with 22 mandates
- Res Publica with 26 mandates
- Social-Democratic Party with 10 mandates

The results of voting at the final voting on 26 June 2005 (52 in favour, 0 against, 0 abstentions):

- Estonian Centre Party did not vote (against)
- Estonian People's Union did not vote (against)
- *Isamaaliit* in favour
- Reform Party in favour
- Res Publica in favour
- Social-Democratic Party in favour

The following are references to verbatim records of the debates on the issue:

1. First reading of the bill at the Riigikogu 12 April 2005 (http://web.riigikogu.ee/ems/stenograms/2005/04/t05041211-09.html#P576_110846)

2. Second reading of the bill at the Riigikogu 3 May 2005 (http://web.riigikogu.ee/ems/stenograms/2005/05/t05050313-01.html#P26_1021)

3. Resumption of the second reading of the bill at the Riigikogu 11 May 2005 (http://web.riigikogu.ee/ems/stenograms/2005/05/t05051114-06.html#P326_55674)

4. Third reading and adoption at the Riigikogu 12 May 2005 (http://web.riigikogu.ee/ems/stenograms/2005/05/t05051214-04.html#P108_18987)

5. 25 May 2005 resolution of the President of the Republic on the refusal to proclaim the Act RTL 2005, 58, 829

6. Renewed deliberation of the Act, refused to be proclaimed by the President, at the Riigikogu on 1 June 2005 (http://web.riigikogu.ee/ems/stenograms/2005/06/t05060116-05.html#P280_52355)

7. Second reading of the draft Act, refused to be proclaimed by the President, at the Riigikogu on 09 June 2005 (http://web.riigikogu.ee/ems/stenograms/2005/06/t05060917-08.html#P359_85217)

8. Third reading of the second proceeding of the draft Act refused to be proclaimed by the President and adoption of the amended Act at the Riigikogu on 15 June 2005 (http://www.president.ee/et/ametitegevus/otsused.php?gid=64640)

9. Resolution of the President of the Republic of 22 June 2005 on the refusal to proclaim the Act RTL 2005, 74, 1059 (http://www.president.ee/et/ametitegevus/otsused.php?gid=64640)

10. Renewed deliberation of the Act, refused to be proclaimed by the President, and adoption, unamended, at the Riigikogu on 28 June 2005 (http://web.riigikogu.ee/ems/stenograms/2005/06/t05062801-03.html#P39_2700)

11 Proposal of 12 July 2005 of the President of the Republic to the Supreme Court to declare the Act unconstitutional.

12. Decision of the Supreme Court of 1 September 2005 to deny the request of the President, Decision No. 3-4-1-13-05 (http://www.nc.ee/klr/lahendid/tekst/RK/3-4-1-13-05.html)

13. Resolution No. 888 of 5 September 2005 of the President of the Republic on proclamation of the Act (http://www.president.ee/et/ametitegevus/otsused.php?gid=64640)

14. Entry into force of the Act on 18 September 2005, RT I 2005, 47, 387.

2. E-Voting Project: Legislation, Budget, Management

2.1. Legal Debate over the Conformity of E-Voting with Election Principles

2.1.1. E-Voting Provisions Adopted in 2002

On 27 March 2002 the Riigikogu adopted the Local Government Councils Election Act which gave the right to vote electronically on the web page of the National Electoral Committee on the days of advance polling. Subsection 74 (5) of the Act stipulated that electronic voting would not be applied before 2005. Such norm of enactment lost its regulatory action on 1 January 2005. Thus the Act granted the voters the right of e-voting beginning from the local government council elections of 2005.

The provisions on e-voting adopted in 2002 are the following:

§ 44. Time of voting

(1) Voting on election day shall open at 9 a.m. and close at 8 p.m.

(2) Advance polls shall begin on the sixth day before election day and close on the fourth day before election day. Voting on advance polling days shall open at 12 p.m. and close at 8 p.m. Votes can be submitted using electronic means on a twenty-four hour basis.

(3) Home voting shall be held on election day in the cases prescribed in this Act.

(4) Voting in custodial institutions shall be held on advance polling days in the cases prescribed in this Act.

§ 47. Specifications for advance polls held outside polling division of residence

(1) On advance polling days (subsection 44 (2)), voters may vote outside the polling division of their residence in a polling division designated by the rural municipality or city government or electronically on the webpage of the National Electoral Committee.

(2) A division committee designated by the rural municipality or city government shall organise voting outside the polling division of residence. The rural municipality or city government may designate a division committee which, in addition to advance polls, organises voting only at the location of a voter (§ 49) or only in custodial institutions (§ 51).

§ 50. Electronic voting

(1) On advance polling days, voters holding a certificate for giving a digital signature may vote electronically on the webpage of the National Electoral Committee. A voter shall vote himself or herself.

(2) A voter shall identify himself or herself by giving a digital signature.

(3) After identification of the voter, the general list of candidates in the electoral district of his or her residence shall be displayed on the webpage.

(4) The voter shall indicate on the webpage the candidate in the electoral district of his or her residence for whom he or she wishes to vote and shall confirm the vote.

(5) A notice that the vote has been accepted shall be displayed to the voter on the webpage.

§ 53. Calculation of votes cast during advance polls outside polling division of residence

(1) A division committee shall pack the envelopes with the ballot papers of electors who voted outside the polling division of their residence by the counties, and by the cities of Tallinn and Tartu, and shall forward such envelopes to the county electoral committee of their location.

(2) A county electoral committee shall forward the envelopes with ballot papers specified in subsection (1) of this section to the corresponding county electoral committees through the National Electoral Committee not later than on the second day before election day.

(3) After the close of electronic voting, the National Electoral Committee shall prepare a list of persons who voted electronically by polling divisions and shall forward the list to the county electoral committees not later than on the second day before the day of the referendum.

(4) A county electoral committee shall forward the envelopes with ballot papers received pursuant to the procedure provided for in subsections (2) and (3) of this section from other county electoral committees and the lists of voters who voted electronically to the appropriate division committees not later than on the day before election day.

(5) After receipt of the envelopes with ballot papers and the list of voters who voted electronically pursuant to the procedure prescribed in subsection (4) of this section, the division committee shall check that each voter is entered in the polling list of the polling division and that he or she has not voted more than once. At least three members of the division committee shall be present during the verification.

(6) If a voter has not been entered in the polling list of a polling division or has voted several times, the division committee shall not take into account any of the ballot papers of the voter received pursuant to the procedure prescribed in subsection (4) of this section. If a voter has voted several times, including electronically, the division committee shall promptly send a corresponding notice to the National Electoral Committee. On the basis of the notice, the National Electoral Committee shall not take into account a vote cast electronically by the

voter. If the voter has not voted in the polling division of his or her residence, a member of the division committee shall make a notation in the polling list concerning voting at the advance polls.

(7) After performing the acts prescribed in subsections (5) and (6) of this Article, the division committee shall open the outer envelopes, deposit the inner envelopes with ballot papers in the ballot box used at the advance polls and seal the opening of the ballot box again.

§ 55. Verification of voting results in rural municipality or city electoral committees

(1) On the basis of the records received from the division committees and the voting results of voters who voted electronically, the rural municipality or city electoral committee shall verify the number of voters entered in the polling lists, the number of voters who were given a ballot paper, the number of voters who participated in voting, the number of invalid ballot papers and the number of votes cast for candidates, political parties and election coalitions in each electoral district. The result obtained shall be checked by recounting the ballot papers.

(2) If the numbers obtained by recounting the ballot papers are different from the numbers in the records of a division committee, the rural municipality or city electoral committee shall set out the differences and the circumstances which caused such differences in the appendix to the record. The records of the division committee shall not be amended. The rural municipality or city electoral committee shall adopt a decision concerning the final voting results.

(3) A rural municipality or city electoral committee shall prepare a standard format record concerning verification of the voting results in the rural municipality or city which shall be signed by the chairman of the committee. The date and time of preparation shall be indicated in the record.

(4) The results of electronic voting shall not be disclosed before the close of voting on election day.

(5) Voting results shall be verified in rural municipality or city electoral committee in public.

§ 74. Entry into force of Act

This Act enters into force on the tenth day after publication in the Riigi Teataja.

(2) Section 71 and clause 72 2) enter into force on 17 October 2005.

(3) Clause 72 1) enters into force on 21 October 2002.

(4) The provisions of subsections 5 (1) and (5), subsections 14 (1) and (2), clause 17 (4) 3), § 25, subsection 31^1 (1) and clause 31^1 (3) 4) concerning citizens of the European Union enter into force upon Estonia's accession to the European Union.

(5) Electronic voting is not applied before 2005.

2.1.2. Amendments of 2005

Description of the e-voting procedure in the Act adopted in 2002, among other things, left it open whether it is allowed to change the e-vote or not, also there was no description of how the e-votes are to be calculated. Upon completion of the technical solution the National Electoral Committee presented the detailed description of e-voting procedure to the Riigikogu Constitutional Committee and the Constitutional Committee initiated a relevant amendment to the Act.

On 12 May 2005 the Riigikogu adopted the Local Government Councils Election Act Amendment Act which specified the provisions on e-voting. On the local government councils elections of 2005, e-voting was applied on the basis of the following provisions that entered into force on 18 September 2005:

§50. Electronic voting

(1) A voter may vote electronically on the webpage of the National Electoral Committee on days prescribed in clause 44(2)3). A voter shall vote himself or herself.

(2) A voter shall identify himself or herself on the basis of a certificate on identity documents permitting digital authentication.

(3) After identification of the voter, the general list of candidates in the electoral district of his or her residence shall be displayed on the webpage.

(4) The voter shall mark the name of the candidate in favour of whom he or she wishes to vote in the electoral district of his or her residence, and shall confirm the vote by giving a digital signature with the aid of a certificate permitting digital signing on the identity document.

(5) A notice that the vote has been accepted shall be displayed to the voter on the webpage.

(6) The voter may change his or her electronically given vote:
1) by voting again electronically at the time prescribed in clause 44(2)3) of this Act;
2) by voting with a ballot paper from the sixth day to the fourth day before election day pursuant to the procedure provided for in Articles 46-49 and Article 51 of this Act.

§53[1]. Counting of electronically given votes

(1) In case of several electronically given vote (subsection 50(6)), the last vote shall be taken into account.

(2) After the close of electronic voting, the National Electoral Committee shall prepare a list of persons who voted electronically by polling divisions and shall forward the list to the county electoral committees not later than on the second day before the day of the referendum. A county electoral committee shall forward the list to division committees not later than on the day preceding the election day.

(3) If a voter has voted electronically, a member of the division committee shall make a notation in the polling list concerning voting electronically.

(4) If a voter has voted electronically as well as with a ballot paper, the ballot paper of the voter shall be taken into account. The division committee shall send an appropriate communication to the National Electoral Committee, whereby the National Electoral Committee shall annul the electronically given vote of the voter.

(5) If a voter has voted several times outside the polling division of his or her residence, and electronically, all envelopes with ballot papers of the voter as well as the electronically given vote shall be rejected. The division committee shall send an appropriate communication to the National Electoral Committee, whereby the National Electoral Committee shall annul the electronically given vote of the voter.

§54[2]. Counting of electronically given votes

(1) National Electoral Committee shall verify the results of electronic voting on election day not before 7 p. m.

(2) At least one-half of the members of the National Electoral Committee, including the Chairman or Deputy Chairman of the Committee shall be present at the counting of votes.

(3) Voting results shall be verified in the National Electoral Committee in public, taking into account the restrictions provided for in subsection 54[1] (6) of this Act.

(4) The results of voting shall not be disclosed before 8 p.m.

(5) The National Electoral Committee shall immediately forward the results to the rural municipality or city electoral committee.

[RT I 2005, 47, 387 – entered into force 18.09.2005]

Art. 50 of the Local Government Councils Election Act was amended with subsection6 which explicitly gave the voter the right to change his or her e-vote in three ways: voting again electronically during the advance polling, voting with ballot paper during the advance polling and voting with ballot paper on the election day. In the initial variant of the bill it was allowed to change the e-vote also on the election day up to 4 p.m. (the reason for such time limitation was to give the electoral committees time to exchange information and cancel repeated votes). The right to change one's e-vote creates a so-called virtual voting booth: e-vote who has e-voted under undesirable influence, can choose a moment when he or she is free to vote without outside influence. In order to guarantee freedom of voting, it is advisable to have the right to change one's vote on election day.

With the same amendment, the Penal Code was also changed to exclude changing electronically given votes from punishable offences.

§ 165. Election fraud

Voting more than once, except in the cases a voter changes his/her electronically given vote, or participating in an election or referendum without the right to vote or in the name of another person shall be punished by a fine of up to 300 fine units or by detention.

2.1.3. Constitutional Review of the Amendments of 2005

President of the Republic refused to proclaim the Local Government Councils Election Act on 25 May 2005, referring in the reasons for his decision to contradiction with the principle of uniformity of local government councils elections stipulated in subsection 156 (1) of the Constitution. According to the judgement of the President of the Republic, the violation of the principle of uniformity lied in the fact that not all voters were guaranteed equal opportunities for voting: the voter who can vote electronically has the right to change his or her electronically given vote by voting again electronically or with ballot paper, whereas the voters using other means of voting do not have such possibility to vote again.

After analysing the reasons given by the President of the Republic the Riigikogu decided to make amendments to the Act. The Riigikogu found that the possibility to change one's e-vote on election day can indeed be regarded as an advantage, it is possible that guaranteeing freedom of vote does not outweigh infringement of uniformity. All who vote during advance polls outside the polling division of their residence should formally be in uniform circumstances. If it were possible to change e-vote on election day, it could influence to change the vote on the basis of information received during the time between the end of advance poll (Wednesday evening) and election day. In practice the information having strong influence on election results has been disclosed just before election day.

2005. On 15 June 2005 the Riigikogu adopted the abovementioned amendment. A week later the President of the Republic again refused to proclaim the Act.

The Riigikogu again adopted the Act the President of the Republic refused to proclaim unamended on 28 June 2005. President of the Republic refused to proclaim the Act on 12 July and turned to the Supreme Court to declare the Act unconstitutional.

During the constitutional review proceedings all the arguments voiced during the legal debate over e-voting were presented again and deliberated. Therefore the Supreme Court resolution on e-voting as a whole is a good summary. In Appendix 2 of the Report the positions of the parties and the reasoning of the Court are set forth.

The Constitutional Review Chamber of the Supreme Court refused to satisfy the application of the President of the Republic. Pursuant to the Constitution, the President of the Republic was obliged to proclaim the Local Government Councils Election Act and the Act could enter into force.

2.2 Project Management

2.2.1. General Management

The electronic voting project was started in 2003. The term for the implementation of e-voting stipulated in the election acts was 2005.

Preconditions for the implementation of e-voting were:

1. the existence of legal basis;
2. widespread use of ID card that guaranteed all necessary means for e-voting – electronic identification of persons and digital signature;
3. the existence of electronic polling lists.

With the National Electoral Committee Resolution No. 75 of 25 July 2003, the e-voting project executive group was formed and the project leader elected, also the roles were distributed between the National Electoral Committee, executive group and project leader.

In accordance with the project organisation, the National Electoral Committee passed the more relevant decisions, the task of the executive group was making proposals and recommendations to the Committee and control the achieving of set objectives. Project leader was in charge of implementation of the project, summoned project groups formed of experts upon necessity, directed their work and checked the results.

As the first stage, the e-voting concept was completed. After that the safety analysis of the e-voting concept was carried out by working group formed of specialists. Proceeding from the recommendations of the safety analysis, changes were made to the concept and presented as a new document titled General Description of E-Voting.

In the beginning of 2004, the technical project of e-voting software was compiled. Together with the safety analysis, it was an essential preliminary document for proclaiming the public procurement for e-voting software. At the same time preparatory work for the acquisition of hardware-based safety module was going on. Module is an international standard product and it is necessary for carrying out the key management procedures of e-voting.

In March, three tenders were submitted to the public procurement of e-voting software. The Government of the Republic declared the offer of AS Cybernetica winner.

In autumn 2004 the software was ready and preparations were made for the first public pilot project, which was offering the possibility of e-voting in the polling of the residents of Tallinn. The polling took place on 24–30 January 2005; 703 voters participated and 697 votes were counted. The system worked without failures.

The final objective of the e-voting project was implementation of e-voting at the local government elections in autumn 2005. Preparatory work was completed – the e-voting system existed and had been tested, only the debated of constitutional issues had to be solved, which took place in September 2005.

2.2.2. Informing the Public

The National Electoral Committee organised a publicity campaign to give information about the elections, including e-voting. One of the aims of the campaign was to inform the public through different media channels that the elections are coming. TV, radio, printed materials (posters, flyers) and web portals were used.

The second aim of the campaign was to draw attention to e-voting as a new way of voting. Advertising channels where it was possible to discuss a subject in greater detail or arrive at instructions in an easier way were used for promoting e-voting. Therefore the advertisement was published in main web portals and besides that flyers with longer instructions on how to e-vote were printed.

Informing about the updating of ID card certificates and the possibility of restoring PIN codes was carried out in cooperation with Citizenship and Migration Board and AS Sertifitseerimiskeskus.

On 16 September the conference E-Voting – Possibilities and Challenges was held in cooperation with the E-State Academy and the National Electoral Committee. The purpose of the conference was to introduce in detail the e-voting system, its legitimacy and reliability. During the conference it was possible to try e-voting in practice in a class opened for that purpose.

As the debates that took place at the Riigikogu highlighted several risks that could accompany the new way of voting, it was planned to hold a panel discussion on the principles of Good E-Voting Practice (see Appendix 1) at the conference.

Before elections from September 26 until October 2 all persons eligible to vote were given the possibility to test e-voting (see chapter 3.3.2).

2.2.3. Training of Representatives of Political Parties as Observers

In August 2005 all larger political parties were called to take part in training course on observing e-voting. As e-voting was new way of voting that could not be observed according to the same principles as traditional voting, special approach to the observing of e-voting was necessary.

Training was started with introducing the e-voting system documentation and after that proceeded with a survey of concrete actions that were necessary for putting the e-voting system in working order (see the time schedule in section 3.3.31).

Besides representatives of political parties, other persons interested in e-voting system and auditors took part in the training.

It should be noted that in the beginning the interest of observers of electronic voting was relatively great but at the last activities only a few representatives of political parties were present.

2.2.4. Observation

51 interested persons from 16 different states wished to come to observe the implementation of unique in the world project of e-voting in local government elections in autumn 2005. The observers were officials from different states dealing with elections, members of third sector organisations and specialists of their field of science.

Official foreign observers were offered a two-day programme with introductory and explanatory reports and the possibility to observe elections in reality both in Tallinn and in Ida-Virumaa.

2.3 Budget

E-voting project was financed from the state project. In 2004 the National Electoral Committee was allocated 172 550 € and in 2005 223 700 € for the organisation of e-voting.

All means allocated from the state budget have not been spent. From August 2003 to the end of 2005, the e-voting project has cost a little more than 320 000 €. The largest expense categories have been:

- creating new software and adapting the existing one 166 175 €;
- acquisition of hardware 19 800 €;
- organisation of pilot project in Tallinn 20 450 €;
- information campaigns for Tallinn pilot project and local elections 26 850 €;
- salaries 31 960 €;
- documentation of procedures, compiling the handbook 17 900 €;
- system audit 12 150 €;
- organisation of conference 10 870 €.

The above figures on the expenses of e-voting are approximate as it is not possible to differentiate which are e-voting expenses and which are the expenses for ordinary voting.

3. Technical Solution

3.1. Envelope Method

8 different possibilities of voting have been in use at the local government councils elections. For years voting outside the polling division of residence has been practiced; it means that during the voting, the voter puts his or her vote into double envelope and the envelope is delivered to the voter's polling division of residence.

The general pattern of e-voting has been derived from the above mentioned voting outside the polling division of residence in Estonia. In these two voting methods, both the ways of checking that the vote has been cast only once and guaranteeing the anonymity of vote are similar.

In order to understand the e-voting system for guaranteeing the secrecy and singleness of vote, the envelope voting method used in Estonia should be described shortly. The latter gives the voter possibility to vote outside the polling division of the voter's residence in any rural municipality or city. A voter presents a document to be entered in the list of voters, and then receives the ballot and two envelopes. The inner envelope has no information about the identity of the voter and the ballot paper is put in it. The inner envelope id put into an outer envelope and the voter's details are written on it so that after the end of advance poll the envelope could be delivered to the voter's polling division of residence. There it is verified whether the voter has the right to vote, then the inner envelope is taken out and put unopened into the ballot box. The system guarantees that the voter's choice shall remain secret and recording the postal voting in the list of voters in the polling division of residence prevents voting more than once.

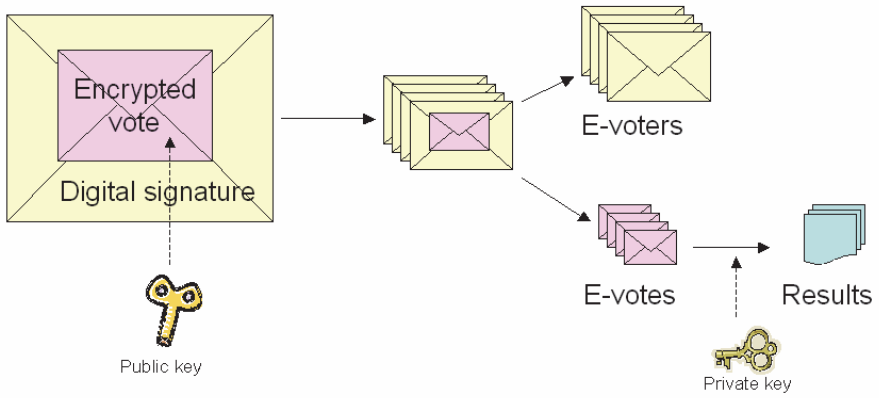


Figure 2 Envelope method at e-voting
Source: General Description of E-Voting, NEC 2004

The application downloaded in the voter's computer during e-voting encrypts the vote before it is sent to the voting server through web connection. The encrypted vote can be regarded as the inner, anonymous envelope. After that the voter gives a digital signature to confirm his or her choice. By digital signing, the voter's personal data or outer envelope are added to the encrypted vote.

E-voting, like voting outside the polling division of residence, is possible only during advance polls. This is necessary in order to guarantee that in the end only one vote is counted for each voter. During the e-voting process, the voter's right to vote is checked but if the voter uses the possibility to cancel his or her vote by going to vote at the polling division during the advance poll, then it has to be guaranteed that finally only one vote is counted for each voter. For that, all polling stations are informed of the e-voters on their list of voters after the end of advance poll and before the election day on Sunday. If it is found at the polling division that the voter has voted both electronically and with paper ballot, the information is sent to the National Electoral Committee who cancels that voters e-vote. Before the verification of voting results in the evening of the election day, the encrypted votes and the digital signatures with personal data or inner and outer envelopes are separated. Then the e-votes are opened and counted. The system opens the votes only if they are not connected to personal data.

3.2. System Architecture

If you want to describe only the part of e-voting of the whole process of organising the elections, it would be relatively small. The system uses existing information systems – Population Register as polling list, National Electoral Committee information system for the collection and publication of information on candidates and voting results and the infrastructure of AS Sertifitseerimiskeskus for checking ID card certificates. From the outside, the e-voting system gets polling lists (from the Population Register) and lists of candidates (from the elections information system), it itself issues lists of e-voters and e-voting results.

Voting has two parties – the giver of the vote and the receiver of the vote. In the case of e-voting, they are the voter's computer into which the voter's application is downloaded and the server pool administered by the national electoral committee.

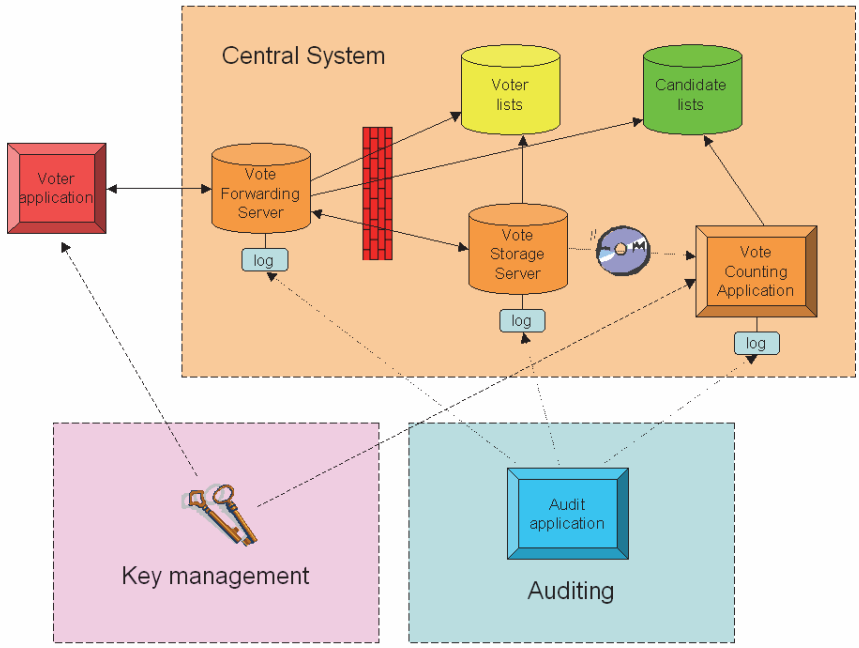


Figure 3 General architecture of e-voting system
Source: General Description of E-Voting, NEC 2004

Components of the Central System are depicted in the orange field of the figure:
1. Vote Forwarding Server (VFS) – authenticates the voter with the help of ID card, verifies his or her right to vote, displays the voter the candidates of his or her electoral district and accepts the voter's encrypted and digitally signed vote. It forwards this vote immediately to Vote Storage Server and forwards the voter the confirmation of the receiving of vote. Finishes work after the end of e-voting.
2. Vote Storage Server (VSS) – receives e-votes from VFS and stores them. When the e-voting has ended, removes repeated votes, cancels the votes of persons with no right to vote and receives and performs cancellations of e-votes. Finally it separates encrypted votes from digital signatures with personal data and prepares them for Vote Counting Application.
3. Vote Counting Application (VCA) – movable regime component where the encrypted votes from which digital signature has been removed are transferred on CD. VCA uses private key of the system, sums up the votes and issues e-voting results.

VFS is the only component of the Central System that is directly accessible through the Internet. All other components are protected by firewall and the access to them is possible only via VFS.

Asymmetric cryptography is used to guarantee the secrecy of votes. A pair of keys is generated for the system in a special safety module so that its private component never leaves it. Public component of the pair of keys is integrated into the voter application and it is used for encrypting the votes. Private component of the pair of keys is used in the Vote Counting Application for opening the votes on election day evening. The National Electoral Committee can open the votes, i.e. use the private component, only collegially. After the end of the period of dealing with the complaints the private key is destroyed.

During auditing of the system possible complaints connected with e-voting are solved, using the information from the Central System log. In its different stages the e-voting system

produces different logs on received, cancelled, counted, invalid and valid votes. Audit Application enables to establish what happened to an e-vote given by a concrete person without revealing the voter's choice.

General description of the e-voting system is available at the National Electoral Committee web page at the address: http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf.

3.3. Implementation of E-Voting System

3.3.1. Pilot Project in January 2005[10]

In cooperation with the town of Tallinn the completed e-voting system was used in January 2005 at the polling of the inhabitants of Tallinn about the location of the Freedom Monument to be erected in Tallinn. The system was implemented as a whole, including the possibility to change one's vote, giving priority to ballot paper and public opening of votes with the e-voting system keys divided between the members of the committee.

It was possible to vote at public polling divisions with ballot paper or electronically via the web page www.valimised.ee. Within the framework of the pilot project, 703 inhabitants of Tallinn, i.e. 13.7% of all those who participated in the poll, used the possibility of e-voting. There were no technical failures.

The inhabitants of Tallinn were posed the following question: "Where in your opinion should the Freedom Monument be located?" and the answers were "In the region of the Freedom Square" and "In some other place".

The wording of the question caused public criticism and the problem itself probably was not important enough to motivate more inhabitants of the town to vote. This also explains the low turnout (1.5% of the inhabitants of Tallinn).

The result of e-voting did not differ significantly from the result of votes on ballot paper.

3.3.2. Public Testing of E-Voting Immediately Before the Local Government Council Elections

Between 26 September and 2 October 2005 all persons eligible to vote were given the possibility to test e-voting in order to encourage people to solve the problems that might emerge (acquisition of necessary software, updating expired ID card certificates, renewal of PIN codes etc.) before the days of real e-voting.

The system used for public testing was as similar as possible to the system used on the days of actual e-voting: a person had to identify himself or herself with ID card, the list of candidates was displayed and the choice had to be confirmed with digital signature. The candidates had been invented for public testing, the names of political parties and election coalitions that actually participated in the elections were not used.

3.3.3. Local Government Council Elections in October 2005

[10] Information about the pilot project can be found at the following web addresses: http://port.andmevara.ee/vabadussammas/statistika.html, http://www.tallinn.ee/est/g2248s20160.

3.3.3.1. Calendar of Events Connected with E-Voting

Aug 18 – training of auditors and observers started
Sept 8 – generating of web server and pairs of keys for coded signature (*)
Sept 9 to 12 – loading of list of candidates and participants for test voting and the list of actual polling divisions, adjustment of servers for test voting
Sept 13 – generating of the pair of keys of the e-voting system, distribution of keys between the members of NEC (*)
Sept 16 – participants of e-voting conference could try e-voting
Sept 22 – loading of lists of e-voters for public test voting, tuning of system for e-voting
Sept 26 – start of public test voting
Oct 2 – end of test voting
Oct 3 – counting of test votes
Oct 5 – audited installing of operation systems (*)
Oct 6 – loading of lists of voters, tuning of servers and voter application (*)
Oct 7 – transport of servers to server rooms (*)
Oct 10 at 9 am – loading of updates to lists of voters, beginning of e-voting (*)
Oct 10 and 11 at 5 pm – making changes to the lists of voters (*)
Oct 12 at 8 pm – end of e-voting, transport of servers (*)
Oct 13 – printout of the list of e-voters (*)
Oct 16 at 5.30 pm – compilation of annulment list, annulment of e-votes (*)
Oct 16 at 7 pm – counting of e-votes and signing the results (*)

(*) activity where auditing/observation was mandatory

E-voting at local government councils elections started on 10 October at 9 am and ended on 12 October at 8 pm on the web page www.valimised.ee.

3.3.3.2. Evaluation from the Technical Perspective

From the point of view of the central system of voting, e-voting took place without greater disruptions. In the morning of the first day of voting the publication of the references to the right web page in info servers was delayed for some minutes which gave an erroneous impression that the beginning of voting was delayed. On the third voting day voting was disturbed for half an hour because of the malfunction of the validity confirmation service of AS Sertifitseerimiskeskus.

System monitoring was launched for the period of e-voting in order to discover possible security problems. There were no attacks that would have endangered the operation of the system.

Server room with very strict security and guarding requirements concerning the access to e-voting hardware was used for secure accommodating of the central system servers.

Overwhelming majority of e-voters (99.1%) used the Windows platform, Linux was used by 0. 72% and Macintosh 0.18 % of e-voters *(Source: Tarvi Martens. E-Voting Report).*

4. Analysis of E-Voting Results

As this was the first experience of e-voting and there were relatively few e-voters, all conclusions drawn of the basis of this experience should be treated with certain reservations. General conclusion is that the implementation of e-voting at the local government councils elections of 2005 was successful. The auditors confirmed that the e-voting system worked correctly, also there were no failures or problems that could have shattered people's trust in the honesty of e-voting and the reliability of the system. No complaints connected with e-voting were submitted to the National Electoral Committee or the Supreme Court.

The analysis of e-voting results is based on existing facts (source: National Electoral Committee) and the following polls conducted before and after the local government councils elections of 2005:

- research centre Faktum "E-voting and the reduction of alienation"; the polling ordered by the Department of Economic and Social Information of the Chancellery of the Riigikogu (DESICR) took place on 5–22 December 2003, the sample was formed on the basis of actual voting behaviour, i.e. persons who had taken part in all elections and in some elections and persons who had never taken part in elections were included in the sample. Reasons for the respondents' voting behaviour and the possibilities and readiness for e-voting were studied;
- research centre Faktum "Attitude of the population towards e-voting". The polling ordered by DESICR was conducted on 4–14 February 2004;
- research centre Faktum "Attitude of the population towards e-voting". The polling ordered by DESICR was conducted from 26 January to 23 February 2005. Omnibus polling where 1700 persons of voting age proportionally from all over Estonia were polled;
- "E-voting poll" of research centre ES Turu-uuringute AS. Ordered by DESICR. Polling was conducted from 27 May to 3 June 2005. Omnibus poll where 966 persons of voting age from all over Estonia were polled[11];
- Faktum's polling within the framework of the project "Democracy and National Interests. Polling was ordered by Estonian Open Society Institute. Project was supported by Open Estonia Foundation. It was an omnibus polling which was conducted from 19 October to 2 November 2005. Sample size was 936;
- Report to the Council of Europe "E-Voting in Estonia at the Local Government Councils Elections of 2005". Authors Fabian Breuer ja Alexander H. Trechsel, European University Institute.[12] The report is based on a sociological polling conducted after e-voting. The sample consisted of 939 persons with the right to vote, it was put together according to actual voting behaviour, 315 e-voters, 319 voters at the polling division and 305 persons who did not take part n voting were included on the sample. The main purpose of the polling was to was to find out the reasons for participating or not participating in e-voting, and also the effect of e-voting on political turnout and election results. The following reference in the report: *Source: CoE +eGA.*

Certainly the conclusions drawn are not exclusive or extensive, but the collected facts and the results of polls with preliminary interpretation form a basis for future scientific research.

4.1. Results of E-Voting

[11] Polling results are available on DESICR home page: http://www.riigikogu.ee/?id=36584

[12] Report for the Council of Europe. E-voting in the 2005 local elections in Estonia. Authors Fabian Breuer and Alexander H. Trechsel, European University Institute. Project leaders Prof.Dr. Alexander H. Trechsel, European University Institute, Florence, Italy & Director of the e-Democracy Centre (e-DC), University of Geneva, Switzerland; Ivar Tallo, Director of the e-Governance Academy, Tallinn, Estonia. Florence, March 6 2006

About 2% of all votes through the Internet. Keeping in mind that it was the first time it was possible to e-vote, that ID card readers most probably are not very widespread, that in the beginning of 2005 a large portion of ID card certificates expired and needed updating and that there are not many of those who use e-services with the help of ID card, it is a good result.

Table 11 Main Statistics of E-Voting
Source: National Electoral Committee

Number of persons with the right to vote	*1059292*
Votes:	502504
valid (with e-votes)	496336
invalid	6168
Voter turnout	47%
E-votes given	9681
incl. repeated e-votes	364
Number of e-voters	9317
E-votes counted	9287
E-votes cancelled	30
Percentage of e-votes among all votes	1.85%
Advance voter turnout (% of all voters)	24%
Percentage of e-votes among votes of advance polls	8%
Number of e-voters who used ID card electronically for the first time	5774
Percentage of e-voters who used ID card electronically for the first time	61%

In order to take part in e-voting, it was necessary to have access to a computer with Internet connection, ID card with valid certificates and PIN codes and a card reader. There is information about the possibilities to use the Internet and the spread of ID cards but no reliable data on the distribution of card readers in Estonia.

At the local government councils elections of 2005 about 2% of the voters, i.e. 9317 persons with the right to vote used the possibility of Internet voting, giving a total number of 9681 e-votes. 9287 e-votes were taken into account in the verification of election results: during the changing of e-votes, 364 e-votes were given and the e-voters also voted with 30 ballot papers. When the repeated votes were counted, the vote given last was taken into account. When the vote was also cast on ballot paper, this was taken into account in verifying the election results and the e-vote was cancelled.

To guarantee the freedom of voting, it was allowed to change one's e-vote with an e-vote or ballot paper. Changing of e-votes was allowed only on sixth to fourth day before the election day so that no advantages would be given to e-voters in comparison to other advance poll voters outside the polling division of their residence. The possibility to change one's e-vote on election day would have created a situation where e-voters in comparison to other voters would have had a substantial and insufficiently justified advantage in expressing their electoral decision: they could have changed their vote on the basis of information received between Thursday and Saturday.

4.2. Digital Gap Issue

The main problem is whether Estonia's experience supports the presumption that the possibility of e-voting would increase the so-called digital gap, i.e. the social inequality proceeding from access to the Internet and the possibility to use the services offered on the Internet.

Attitude towards e-voting has been mostly favourable since the beginning of the e-voting project.[13] Positive attitude did not change also after the implementation of actual e-voting.

In November 2005 (after the implementation of e-voting at the local government councils elections) research centre Faktum conducted a polling of the population which included questions about last local government elections. Faktum has investigated the general attitude of the public towards e-voting also in February 2004 and February 2005. The number of persons with the right to vote who are ready to vote through the Internet has steadily increased; at the same time the number of those who in any case would like to vote at the polling division is diminishing.

Table 12 Attitude Towards E-Voting in 2004-2005
Source: Faktum polling

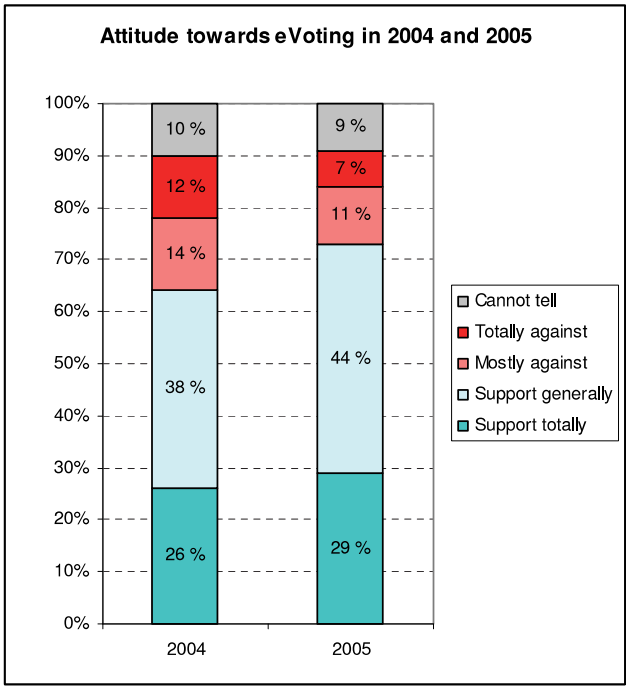
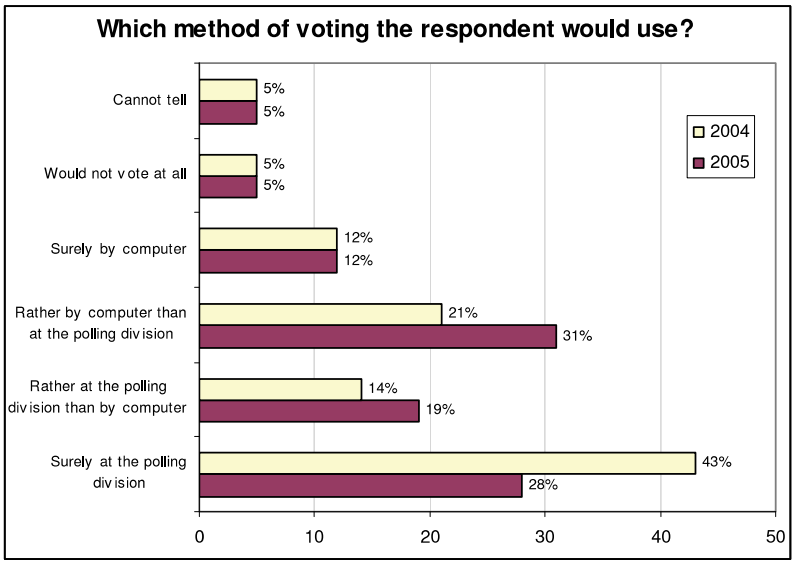


Table 13 Preferences in the Way of Voting in 2004–2005
Source: Faktum polling

[13] Estonian public defines e-voting as voting through the Internet, the media has operated with this meaning and public polls, too, have proceeded from this definition. Among other things it was claimed in the debates at the Riigikogu that as in the polls there was no question about voting via the Internet, but about e-voting, it should be presumed that the respondents expressed their support to machine voting and other forms of electronic voting and not to voting through the Internet. Most likely this is not the case here.



Implementation of e-voting increases social inequality in the case the representation of the people who do not have the possibility to e-vote in representative bodies decreases because of that. The equality of the possibility of being represented would clearly decrease if in connection with e-voting the density of polling divisions and the number of voting days were considerably reduced. The density of polling divisions remained the same at the local government councils elections of 2005, the number of days for voting was also not reduced. The number of days when it is possible to vote has actually been increased at two last elections because since the elections of the European Parliament in 2004 it possible to vote at the polling division since the thirteenth day before the election day.

People with higher level of education have more favourable attitude towards e-voting than people with lower level of education; there were more people with higher education also among actual e-voters. On the basis of existing studies it may be said that the difference in attitude and actual participation is relatively small, around 10% (see tables 14 and 15).

Table 14 Relationship between the Level of Education and Attitude Towards E-Voting
Source: Faktum polling in February 2005

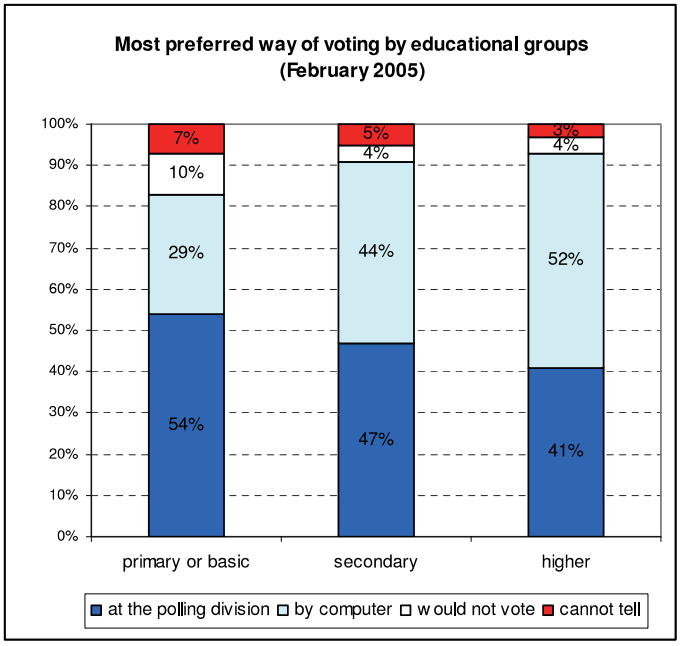
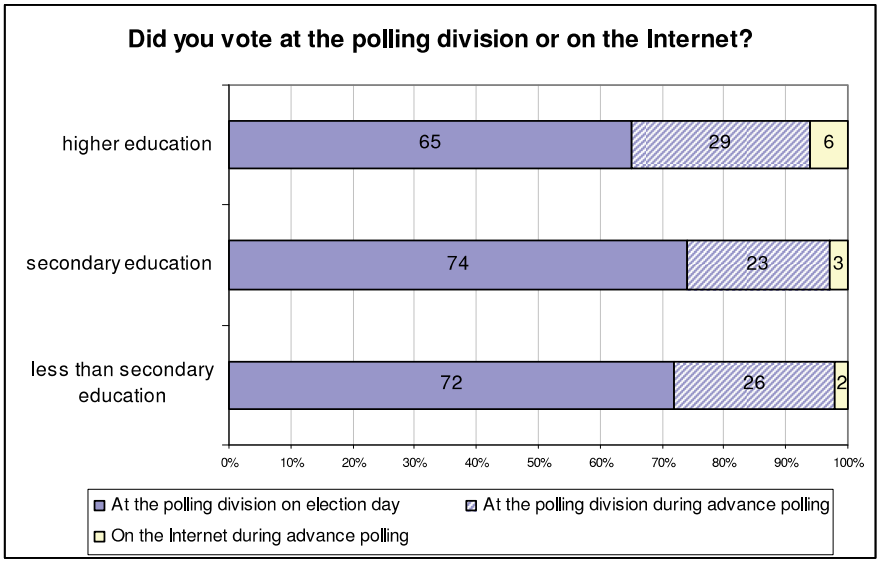


Table 15 Relationship between the Level of Education and Actual E-Voting
Source: Faktum polling in October and November 2005



The comparison of the attitude and actual voting behaviour of different age groups shows that among younger people there are more those who support the possibility of e-voting and here the differences between different age groups are great. There are more than two times more supporters of e-voting among the 15–34 year olds than among over 50 year olds (see Table 16). The polling on actual voting behaviour does not show such large differences but the result of polling must be regarded cautiously because of the small sample group (see Table

17). Unfortunately there is no data on the percentage of all voters in the same age groups who used the possibility of e-voting, the percentage of those who used other possibilities of advance polls and the percentage of those who voted at polling division on election day.

There are data on how the e-votes were distributed between different age groups. 62% of all e-voters were in the age group 30–59 years; 18–29 years old voters formed 27.5% of e-voters and over 60 year olds around 10%. It must be noted that in the age group 30–59 there are considerably more 30rs old e-voters than 50–59 years old e-voters (see Table 18).

Table 16 Relationship between Age and Attitude Towards E-Voting
Source: Faktum polling in February 2005

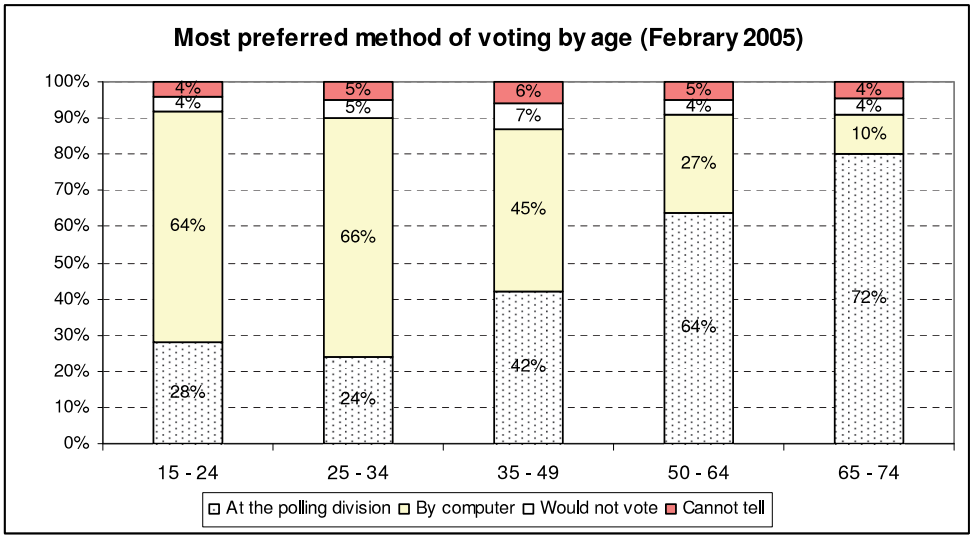


Table 17 Relationship between Age and Actual E-Voting
Source: Faktum polling in October and November 2005

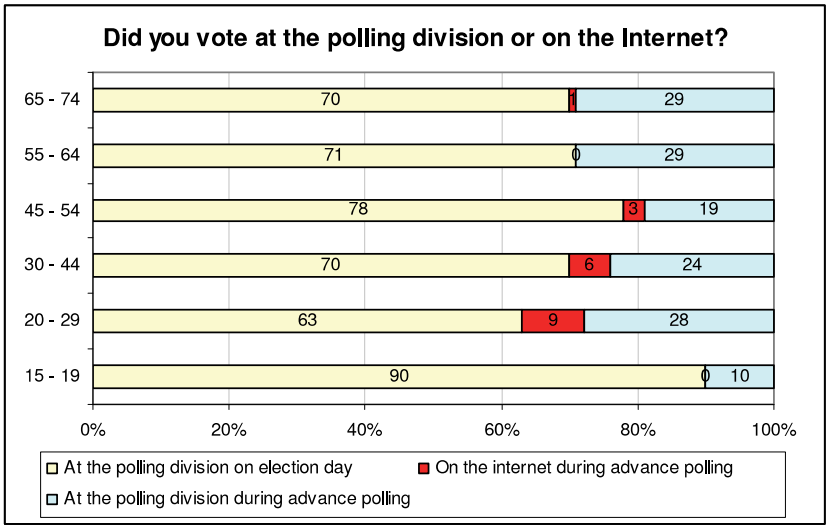


Table 18 E-Voters by Narrower Age Groups
Source: National Electoral Committee

	women	%	men	%
up to 29	1062	25,0	1512	30,0
30 - 34	542	12,8	908	18,0
35 - 39	506	11,9	688	13,6
40 - 44	497	11,7	553	11,0
45 - 49	451	10,6	433	8,6
50 - 54	362	8,5	345	6,8
55 - 59	278	6,5	228	4,5
over 60	547	12,9	375	7,4
TOTAL	4245	100,0	5042	100,0

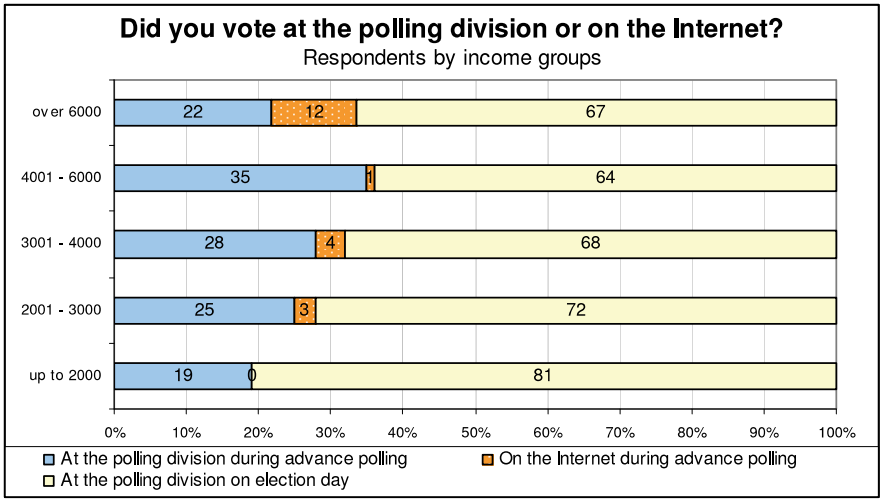
Data about the sex of e-voters shows that in general there are more e-voters among men (see Table 19), but comparison of narrower age groups shows that when the age increases the difference between sexes diminishes and among more than 40 years old e-voters there are more women than men (see Table 18).

Table 19 E-Voters by Sex
Source: National Electoral Committee

gender	votes	%
Women	4245	45,7
Men	5042	54,3
TOTAL	9287	100

Faktum's polling also included questions necessary for linking the use of the possibility of e-voting and the income of the respondent. The result received (although again on the basis of relatively small sample) confirms the hypothesis that wealthier people use the possibility of e-voting and generally the possibility of advance poll more. The percentage of people with the smallest income is greatest among the voters at the polling division on election day (see Table 20).

Table 20 Relationship between the Level of Income and Actual E-Voting (income in crowns)
Source: Factum polling in October and November 2005



As a rule, linking the possible e-voting turnout with place of residence proceeds from the hypothesis that the e-voting possibility is most used in large cities and less in rural regions. The survey made on behalf of Council of Europe showed that percentages of e-voters in rural areas and in cities are similar and place of residence is not decisive factor (see Table 21).

Table 21 Frequency of Political Participation and Mode of Vote in 2005
Source: CoE +eGA

Type of settlement	Type of political participation			
	vo vote	vote at polling place	e-vote	total
Urban	67,9%	67,6%	70,2%	68,6%
Rural	32,1%	32,4%	29,8%	31,4%
Total № of respondents	100,0% (305)	100,0% (318)	100,0% (315)	100,0% (938)

When we look at the absolute number of e-voters by towns and rural municipalities, we can see that the largest number of e-votes was given in Tallinn, Tartu and Pärnu. Viimsi rural municipality ranked fourth by the absolute number of e-votes (see Table 23). When we compare the percentage of e-votes in all votes cast in a municipality or town, it can be seen that at the top there is not Tallinn or Tartu but the tiny municipality of Ruhnu with 11.1% Neighbouring municipalities of the capital follow: Harku municipality with 3.97% and Saku municipality with 3.72%. Of towns, Kärdla has the highest, 10th place with 3%. Tallinn ranks 15th and Tartu 29th, respectively with 2.75% and 2.42% of all votes. If we compare the percentage of towns and municipalities, the differences are not really great (see Table 25). Among 240 districts, there were only 18 with no e-voters.

Table 22. The Percentage of E-Voters among the Eligible Voters by Counties and in Tallinn and in Tartu
Source: National Electoral Committee

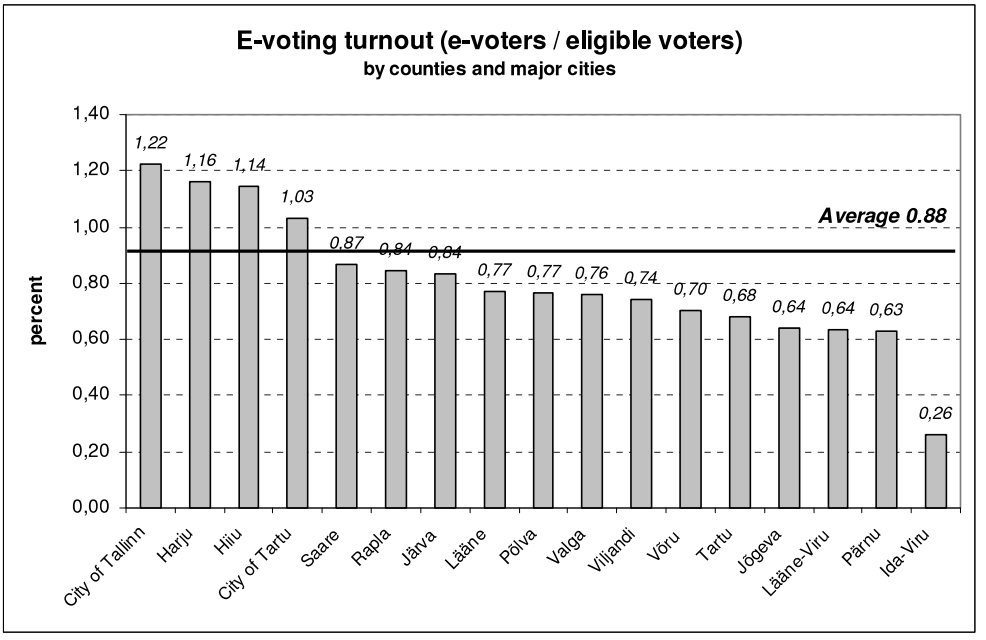


Table 23. The Percentage of E-Voters among the Persons Who Participated in Voting by Counties and in Tallinn and in Tartu
Source: National Electoral Committee

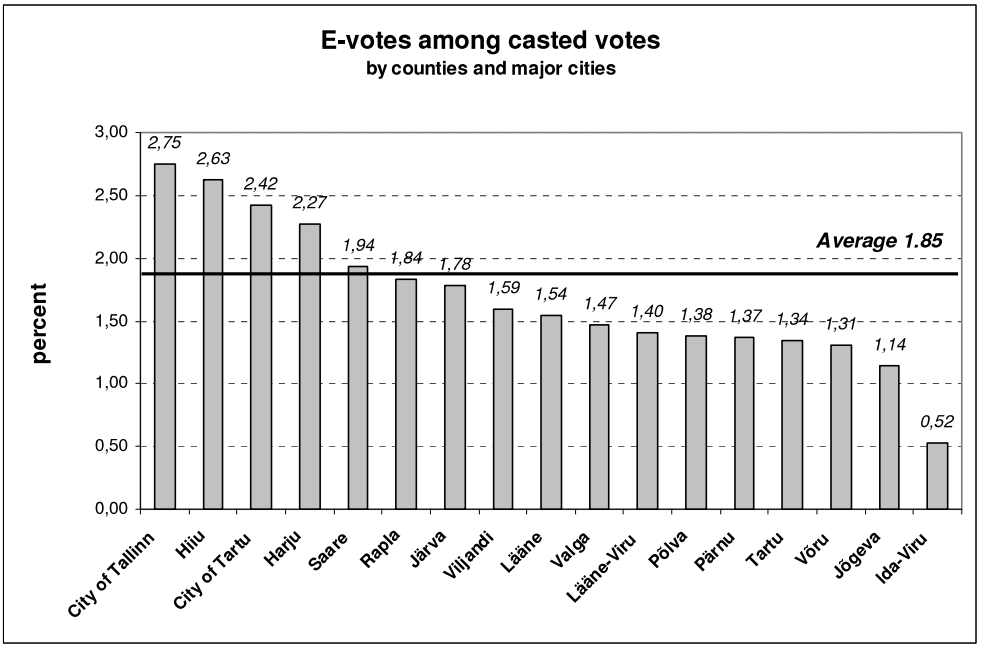


Table 24 Number of E-Votes in Towns and Rural Municipalities (? 40 e-votes)
Source: National Electoral Committee

1. City of Tallinn: 3833
2. City of Tartu: 786
3. Town of Pärnu: 250
4. Viimsi municipality 179
5. Town of Kuressaare: 135
6. Town of Viljandi: 129
7. Harku municipality: 124
8. Saku municipality: 107
9. Town of Narva: 103
10. Saue municipality: 97
11. Town of Rakvere: 95
12. Town of Võru: 93
13. Town of Keila: 88
14. Town of Haapsalu: 79
15. Rapla municipality: 78
16. Türi municipality: 74
17. Town of Saue: 70
18. Rae municipality: 68
19. Town of Valga: 67
20. Town of Paide: 64
21. Kuusalu municipality: 62
22. Town of Kohtla-Järve: 59
23. Town of Põlva: 57
24. Jõelähtme municipality: 52
25. Märjamaa municipality: 47
26. Anija municipality: 45
27. Suure-Jaani municipality: 42
28. Otepää municipality: 42
29. Town of Põltsamaa: 42

Table 25 Number of E-Votes in Polling Divisions (≥ 40 e-votes)
Source: National Electoral Committee

1. Viimsi mun., Dvn. No. 2: 100
2. City of Tallinn, Dvn. No. 9: 98
3. Harku mun.,, Dvn. No. 1: 82
4. Viimsi mun., Dvn. No. 1: 78

5. Town of Saue, Dvn. No. 1: 70
6. City of Tallinn, Dvn. No. 24: 69
7. City of Tallinn, Dvn. No. 31: 68
8. Saue mun, Dvn. No. 2: 65
9. City of Tallinn, Dvn. No. 102: 56
10. City of Tallinn, Dvn. No. 34: 55
11. City of Tallinn, Dvn. No. 20: 55
12. City of Tallinn, Dvn. No. 15: 55
13. City of Tallinn, Dvn. No. 127: 55
14. City of Tallinn, Dvn. No. 104: 52
15. City of Tartu, Dvn. No. 8: 51
16. City of Tartu, Dvn. No. 20: 51
17. City of Tallinn, Dvn. No. 103: 51
18. City of Tartu, Dvn. No. 19: 50
19. City of Tallinn, Dvn. No. 101: 50
20. Saku mun, Dvn. No. 2: 50
21. City of Tartu, Dvn. No. 13: 49
22. City of Tallinn, Dvn. No. 38: 49
23. City of Tartu, Dvn. No. 17: 48
24. City of Tartu, Dvn. No. 15: 48
25. City of Tallinn, Dvn. No. 108: 48
26. Town of Keila, Dvn. No. 2: 48
27. City of Tartu, Dvn. No. 18: 47
28. City of Tallinn, Dvn. No. 18: 47
29. City of Tartu, Dvn. No. 3: 46
30. City of Tallinn, Dvn. No. 23: 46
31. City of Tallinn, Dvn. No. 100: 46
32. City of Tallinn, Dvn. No. 27: 45
33. City of Tallinn, Dvn. No. 114: 45
34. City of Tallinn, Dvn. No. 111: 45
35. City of Tallinn, Dvn. No. 83: 44
36. City of Tallinn, Dvn. No. 32: 44
37. City of Tallinn, Dvn. No. 116: 43
38. City of Tallinn, Dvn. No. 107: 43
39. City of Tallinn, Dvn. No. 86: 42
40. City of Tallinn, Dvn. No. 84: 42
41. Town of Põltsamaa, Dvn. No. 1: 42
42. Karksi mun., Dvn. No. 1: 40
43. Town of Keila, Dvn. No. 1: 40

Table 26 The Percentage of E-Votes of Total Votes Cast in Rural Municipalities and Towns
Source: National Electoral Committee

1. Ruhnu municipalitu 11.11
2. Harku municipality 3.97
3. Saku municipality 3.72
4. Vastse-Kuuste municipality 3.64
5. Käina municipality 3.53
6. Suure-Jaani municipality 3.38
7. Viimsi municipality 3.30
8. Saue municipality 3.17
9. Meeksi municipality 3.11
10. Town of Kärdla 3.00
11. Town of Saue 2.87
12. Nõo municipality 2.85
13. Emmaste municipality 2.85
14. Maidla municipality 2.80
15. City of Tallinn 2.75
16. Town of Kuressaare 2.72
17. Lümanda municipality 2.68
18. Jõelähtme municipality 2.67
19. Puka municipality 2.62
20. Kiili municipality 2.58
21. Juuru municipality 2.54
22. Kõlleste municipality 2.54
23. Kaisma municipality 2.54
24. Town of Põlva 2.53
25. Kernu municipality 2.45
26. Karksi municipality 2.44
27. Town of Keila 2.44
28. Paide municipality 2.43
29. City of Tartu 2.42
30. Leisi municipality 2.38
31. Kuusalu municipality 2.38
32. Saarepeedi municipality 2.33
33. Tootsi municipality 2.33
34. Raikküla municipality 2.27
35. Rapla municipality 2.26
36. Alatskivi municipality 2.26
37. Paikuse municipality 2.25
38. Tõlliste municipality 2.21
39. Keila municipality 2.21
40. Taebla municipality 2.20
41. Rae municipality 2.20
42. Oru municipality 2.17
43. Ülenurme municipality 2.16
44. Kärla municipality 2.15
45. Kolga-Jaani municipality 2.14
46. Hummuli municipality 2.10
47. Anija municipality 2.09
48. Padise municipality 2.03
49. Iisaku municipality 1.98
50. Mõniste municipality 1.96
51. Otepää municipality 1.93
52. Town of Põltsamaa 1.93
53. Pühalepa municipality 1.92
54. Kohila municipality 1.91
55. Town of Viljandi 1.90
56. Toila municipality 1.89
57. Võru municipality 1.87

58. Rakvere municipality	1.86		
59. Türi municipality	1.85	**Average in Estonia:**	**1.85 %**
60. Palamuse municipality	1.85		

When researching the issue of digital gap, it should be also studied where exactly the e-votes were given: at workplace, at home, in public voting place or abroad. On the basis of the results of research ordered by the Council of Europe it is known that most votes were given at home and workplace was the second voting place by popularity (table 27).

Table 27 E-voting places:
Source: CoE+eGA

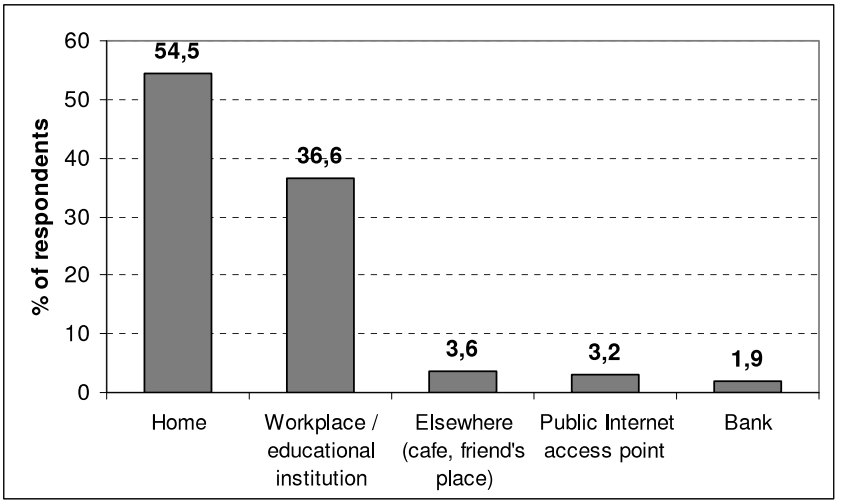


Table 28 shows from which IP-addresses the largest number of e-votes came. These were Ühispank offices, Citizenship and Migration Board and Tallinn City Government, and also the offices of Elion, EMT and Hansapank. The voters at workplace and the users of public voting places are not brought out separately. A number of state agencies and large enterprise Eesti Energia follow, i.e. the places where the workers have the possibility to use computers with Internet access and ID card reader.

Table 28 Places Where More than 20 E-Votes Were Cast:
Source: National Electoral Committee

No. of votes	*Voting place*	*No. of votes*	*Voting place*
210	Ühispank offices	44	Ministry of Economic Affairs and Communications
165	Citizenship and Migration Board	43	Eesti Energia
80	Tallinn City Government	32	Tartu City Government
70	Riigikogu	28	Clients of AS Kernel (radio links) www.kodu.ee
61	different state agencies	27	Ministry of Finance

58	Ministry of Justice	26	Transservice-N http://www.narvatransiit.ee/
58	Tax and Customs Board	26	Social Insurance Board
58	Elion	25	Ministry of Foreign Affairs
55	Police Board	24	AS If Kinnisvarahaldus
54	EMT	23	State Audit Office
50	Hansapank	22	University of Tartu
49	State Chancellery	21	Clients of Elisa

When we look at voter turnout by days (see Table 29), we can see that number of voters was the greatest on the first day of voting. The periods of the most active voting were at 9 a.m. and at 7 p.m. (see Table 30). During the whole e-voting period, the number of e-voters was the largest at the beginning of the voting period and even larger during the last hour of e-voting (see Table 31).

Table 29 E-Voting Activity By Days
Source: National Electoral Committee

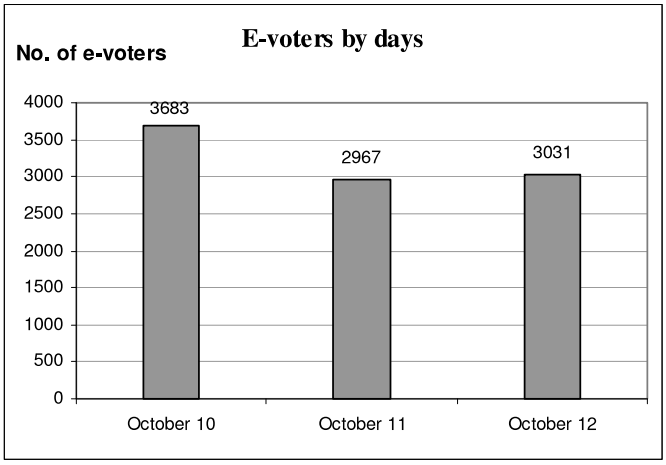


Table 30 E-Voting Activity By Hours
Source: National Electoral Committee

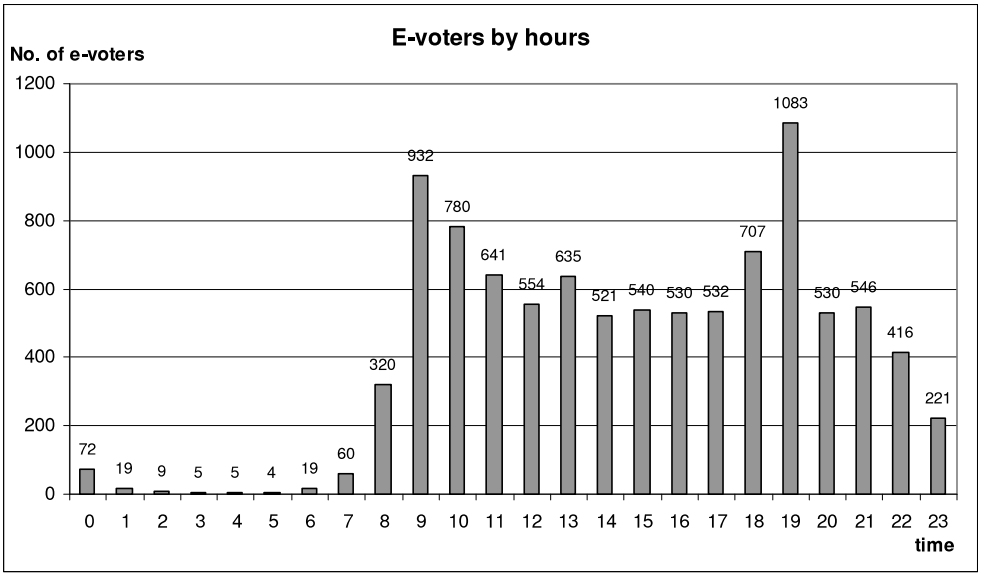
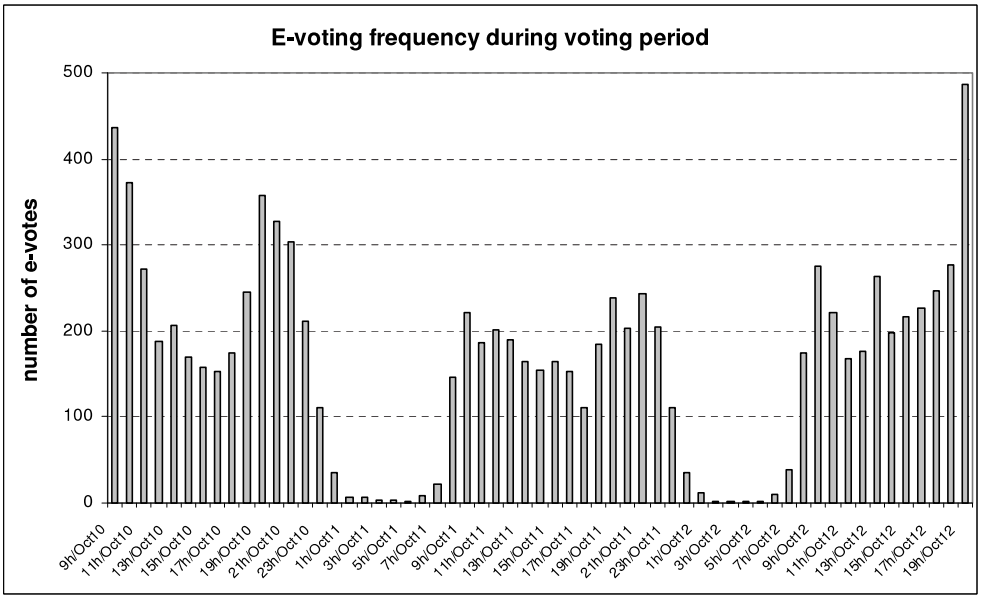


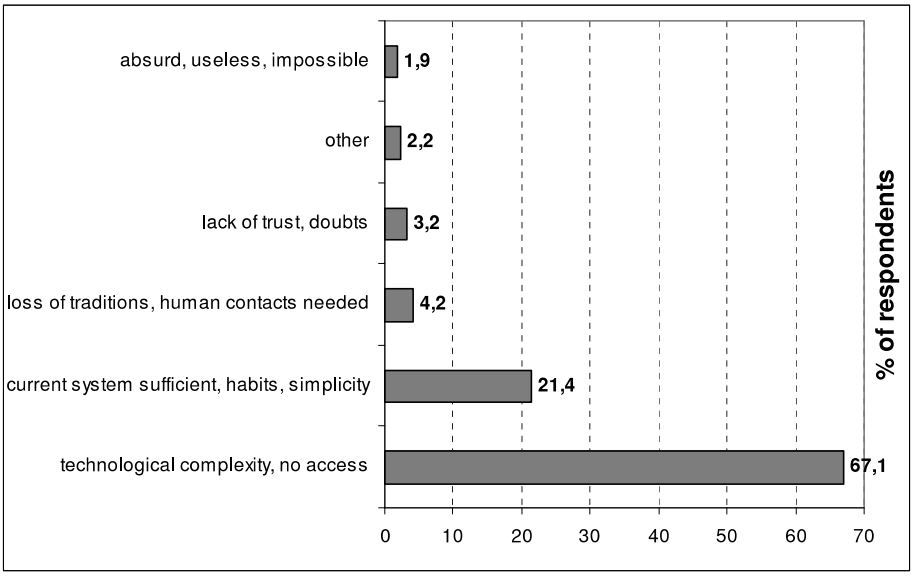
Table 31 E-Voting Frequency During Voting Period
Source: National Electoral Committee



The research ordered by the Council of Europe and carried out by Faktum came to conclusion that living place, gender, income and education are not decisive factors for e-voting. Also the data about real e-voters do not support the presumption that e-voting widens the digital gap. The research mentioned above notices that voters' language influences the participation in e-

voting – Russian speaking voters did not participate at the level as the other voters. However, the general attitude towards e-voting was positive. Voters who did not use e-voting were mostly afraid of technical complexity or they did not have access to Internet. The amount of people who did not trust the whole system or considered it useless was not significant (Table 32).

Table 32 Subjective reasons for not using e-voting
Source: CoE+eGA



4.3. Influence of E-Voting on Election Results

4.3.1. Change of Voter Turnout

Estonian e-voting experience in 2005 reassures the hypothesis that e-voting does not raise the voting activity of people who never take part in elections, but it encourages the participation of voters who vote sometimes. Thus, e-voting slows down the trend of falling participation.

Table 33. Frequency of usual political participation and mode of vote in 2005
Source: CoE+eGA

Vote in 2005	Frequency of usual political participation				
	in all elections	in some elections	from time to time	never	total
At the polling place	77,6%	18,0%	3,5%	0,9%	100%
By Internet	70,2%	24,4%	4,8%	0,6%	100%
Total					100%
No. of respondents	(467)	(234)	(26)	(5)	(632)

In specialist literature, increasing of voter turnout is regarded as the main purpose of the implementation of e-voting. In Estonia increasing voter turnout has not been so clearly set as

objective. It is clear that at the local government councils elections the voter turnout increased at least by the votes given abroad: voting by mail from abroad is not possible at the local government councils elections. The introduction of e-voting serves the goal to bring people to vote by enlarging the accessibility.

4.3.2. Comparison of E-Voting Results of Political Parties with the General Voting Results

The largest number of votes were given to the Reform Party who was the initiator of the e-voting project and promoted e-voting during the whole e-voting project. Among other things the Reform Party organised ID card user training and handed out ID card readers during their election campaign. The Centre Party who on the background of their general success could have received many e-votes ranked 5th among the political parties by the number of e-votes. The reason for such result may among other things be the opposition towards e-voting among their supporters.

Table 34 Division of E-Votes by Political Parties in Comparison with the Total Results
Source: National Electoral Committee

Party	*e-votes*	*%*	*total number of votes*	*%*	*percentage of e-votes in all votes* [14]
Estonian Reform Party	3039	32,7	83 953	16,9	3,61
Isamaaliit	1629	17,5	42 566	8,6	3,82
Res Publica	965	10,4	42 004	8,5	2,29
Social Democratic Party	916	9,9	31 921	6,4	2,86
Estonian Centre Party	806	8,7	126 449	25,5	0,63
Estonian People's Union	640	6,9	61 871	12,5	1,03
Estonian Christian People's Party	24	0,3	1799	0,4	1,33
United People's Party of Estonia	12	0,1	3407	0,7	0,02
Estonian Independence Party	8	0,1	687	0,1	1,16
Estonian Left Party	6	0,1	317	0,1	1,89
Russian Party in Estonia	0	0,0	406	0,1	0,00
Total number of e-votes	9287	100,0	496 336	100,0	

The research ordered by the Council of Europe studied the impact of political variables on choosing e-voting over the voting in polling place. On the political left-right scale voters in right side tend to be more likely to vote by Internet. The real decision whether to vote electronically or by paper ballot is influenced by other factors and considering all other factors in general the political variables lose their importance and apparently e-voting is politically neutral.

According to research important factors in choosing e-voting over voting in polling place are voters' age, language, computing knowledge and trust in e-voting procedures. The non-decisive factors are gender, living place, education, income, trust in parliament and government, trust in politicians, frequency of Internet use and its accessibility and trust in transactions over the Internet.

[14] Percentage of e-votes given to a political party among all votes given to a political party

4.4. Influence of E-Voting on the Legitimacy of Election Results

In the media the fact that elderly people e-voted by themselves has been put under dispute. However there is no evidence to prove this statement. It should be mentioned that according to law it is allowed to assist voters if he or she is unable to complete the ballot himself or herself.

In single cases voters who have e-voted during advance voting period were allowed to vote additionally in election day. Originally the election law legislated that e-voter may change his or her e-vote also in election day but this principle was changed closely before elections. However, polling station committees reported the cases named above and the National Electoral Committee cancelled the e-votes and consequently the principle that every voter has one vote was followed.

No failures were found in the technical system of e-voting. No cases of buying e-votes have become public and no legal proceedings were initiated. The legitimacy of election results has not been contested by referring to e-voting.

APPENDIX 1

Good Practice of E-Voting

Acknowledging Estonia's progress in the use of information technology in different spheres of life and people's readiness to use new means of communication;

keeping in mind the importance of the legalisation of e-voting by increasing the citizens' freedom of choice in choosing the way of voting;

declaring that e-voting does not mean giving up traditional ways of voting;

aware of the responsibility of all of us for the lawful and successful running of e-voting;

we adopt both in word and deed the following Principles of Honest E-Voting:

1. the procedure of e-voting, and also the fact that guaranteeing privacy during the act of voting is a requirement proceeding from the Constitution, is explained to electors neutrally and impartially; people are informed of the dangers that accompany the transfer of ID card and its codes to other persons;

2. no collective e-voting events (opening of e-voting offices or service desks etc.) are organised on e-voting days, and such events are considered violations of the freedom of voting;

3. people are not urged to vote on e-voting days by offering a computer for that purpose or influencing the electors in any other way with the aim of collecting their votes;

4. electronic advertising containing the hyperlink https://www.valimised.ee to the e-voting web page is avoided in order to prevent the danger of entering a false web page that might have been set up for collecting people's personal data;

5. no election campaigning is carried out at public Internet access points with e-voting possibility;

6. when and if possible, take actively part in observing the procedure of e-voting, recording the results of observation honestly and impartially and informing the National Electoral Committee and general public of them;

7. during the election campaign and after the elections, if the lawful procedures of e-voting are observed, e-voting and thus the legality of the whole election is not questioned for political reasons.

Good E-Voting Practice has been prepared on the initiative of e-Government Academy in cooperation with the representatives of political parties and the public.

APPENDIX 2

Decision of the Supreme Court of Estonia of Electronic Voting

(see http://www.nc.ee/klr/lahendid/tekst/RK/3-4-1-13-05.html)

In the Decision of the Supreme Court, the positions of the parties of the dispute are reviewed as follows.

The President of the Republic is of the opinion that the amendment to the Local Government Council Election Act, establishing the right of a voter to change his or her vote given by electronic means for unlimited number of times during the time allocated for advance polls, is in conflict with the principle of uniformity of local government council elections, established in § 156(1) of the Constitution, which requires that each person with the right to vote has one vote and that all persons have been given the possibility to vote in similar manner. The principle of uniformity means that a voter can vote but once, that his or her vote is taken into account but once when counting votes, and that the vote does not become distorted in the course of voting. Through the possibility to change the vote given for unlimited number of times the contested Act accords advantages to voters voting by electronic means in comparison to the voters using other voting channels, as the latter lack the possibility to vote again or vote differently.
The justification that the possibility to change the vote given by electronic means for unlimited number of times helps to prevent purchasing of votes when voting via the uncontrolled medium of Internet and guarantees the freedom of voting, is not appropriate. The possibility to change, during advance polls, for unlimited number of times the vote given by electronic means, established for the protection of the freedom to vote and secrecy of voting, must not infringe upon other electoral principles protected by the Constitution.

The Constitutional Committee of the Riigikogu pointed out that the possibility to change electronic votes serves the aim of guaranteeing the freedom to vote and of guaranteeing the uniformity of voting through preventing the purchasing of votes.
The principle of uniformity means that all voters have equal possibilities to affect the voting results, i.e. an equal number of votes will be taken into account per voter. The principles of uniformity and generality in their conjunction require that the participation in voting, guaranteed to voters, be as convenient as possible. New voting channels serve the aim of increasing the participation in voting and thus protecting the representative nature of representative bodies.
The principle of uniformity does not mean that all votes should vote using exactly the same channel. All those who use different channels of voting are, in fact, in a somewhat different situation, and so far this has not been deemed to be in conflict with the principles of democratic elections. From the point of view of democracy it is important that only one vote per voter be taken into account. In regard to voting by electronic means the taking into account of one vote per voter shall be guaranteed by the same methods, which are used when counting the votes given outside the polling divisions of one's residence.
Proceeding from the principle of uniformity the state shall take measures to prevent the purchasing of votes, otherwise it would be possible to obtain more than one vote either in consideration for benefits or under the influence of a threat. Purchasing of an electronic vote becomes less reasonable only when an electronic vote can be changed by another electronic vote or by a ballot paper.

The Chancellor of Justice is of the opinion that the Act contested by the President of the Republic is constitutional.
Proceeding from the principle of uniform elections the state shall enact regulations enabling all voters to vote in equal manner. By the contested Act the state has guaranteed all voters a legal possibility to vote in similar manner, including the right to vote by electronic means and to change the vote given by electronic means. According to the valid law it is possible to change a vote given by a ballot paper outside the polling division of one's residence during advance polls. The principle of uniformity can not be interpreted as a requirement that all voters must in fact vote in a similar manner. Uniformity means, first and foremost, the requirement that all voters have equal possibilities to influence the voting result.
If uniformity were interpreted as the prohibition to change one's vote during voting, the restriction of the principle of uniformity would be justified with the principles of freedom to vote and secret voting. The possibility to change the vote given by electronic means renders the influencing of the will of a voter by illegal means useless and pointless, and is thus an additional guarantee, supplementing the measures of penal law, for guaranteeing the principle of free voting when voting by electronic means. To those persons who did not vote secretly the possibility to change one's vote gives an essential remedy for restoring the secrecy of voting.
Bearing in mind the values underlying different electoral principles and the weight thereof, the apparent infringement of the principle of uniformity is justified by the need to protect the principles of freedom to vote and secrecy of voting.

The Minister of Justice also did not concur with the position of the President of the Republic and was of the opinion that the contested Act was not unconstitutional.
The principle of uniformity means that all voters have an equal number of votes and that the votes of voters of different electoral districts have more or less the same weight. The principle of uniformity does not require absolute equalisation of voting conditions and procedures. Estonian electoral law recognises different methods of voting, which are all deemed to be in conformity with the principle of uniformity. Uniformity is meant to protect a voter against unequal treatment upon considering the influence of his or her vote on voting results. The possibility to change one's vote does not increase the influence of the vote in comparison to the vote of a person voting through any other channel. At local government council elections there is the possibility to change one's vote both upon voting by electronic means as well as upon voting by a ballot paper at a polling division.
Even if we considered the possibility to change votes as a restriction to the principle of uniformity, the restriction still serves a reasonable aim and is a proportional one. The aim of the contested Act is to sufficiently guarantee the secrecy of voting, and through this, the freedom to vote. When there is a possibility to change one's vote, the influencing of voters in an uncontrolled voting medium becomes pointless. In the present case the highest possible degree of equal treatment of voters using different voting channels is guaranteed, a degree that can be considered compatible with the requirements to voting via uncontrolled medium, proceeding from the principle of freedom of voting.

The National Electoral Committee points out that the preclusion of several votes by one voter, i.e. the uniformity in the context of voting by electronic means, is guaranteed by a system similar to the system of two envelopes, employed upon voting outside the polling division of one's residence at advance polls. Upon voting by electronic means a voter makes his or her choice, which shall be encoded. At the end of the voting procedure the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote. The personal data and the encoded vote shall be stored together until the counting of

votes on the election day, with the aim of ascertaining that the person has given only one vote. The personal data of a voter and the e-vote given by the voter shall be separated before the counting of votes, after the fact that the voter has given only one vote has been checked. As it is not possible to transfer the votes together with personal data into the computer counting the votes, the secrecy of voting is also guaranteed.

The system of electronic voting is completed, it has undergone repeated laboratory trials and was publicly tested during a poll of inhabitants of Tallinn in January 2005.

The Supreme Court justified the confirming of e-voting to the Constitution of Estonia with the following:

The principle of uniformity of local government council elections is established in the second sentence of § 156(1) of the Constitution, pursuant to which the elections of a local government council shall be general, uniform and direct. The principle of uniform elections, being one of the pillars of democratic statehood, means that all voters must have equal possibilities to influence the voting results. In the context of active right to vote the principle of uniformity primarily means that all persons with the right to vote must have equal number of votes and that all votes must have equal weight upon deciding the division of seats in a representative body.

Pursuant to Recommendation Rec(2004)11 of the Council of Europe of 30 September 2004 to member states on legal, operational and technical standards of e-voting (hereinafter 'Standards of e-voting') the principle of uniform suffrage in the context of e-voting means four requirements. Firstly, it should be guaranteed that a voter shall be prevented from inserting more than one ballot into the electronic ballot box, and that a voter shall be authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box (§ 5). Secondly, the e-voting system shall prevent any voter from casting a final vote by more than one voting channel (§ 6). Thirdly, every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once (§ 7). Fourthly, where electronic and non-electronic voting channels are used at the same time, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result (§ 8). All the requirements are aimed at guaranteeing that only one vote per voter is taken into account upon electronic voting. Although the Recommendation of the Council of Europe is not a legally binding document, it summarises the understanding of the democratic states of Europe of the conformity of electronic voting with the election principles inherent to democratic states, and it is thus an appropriate tool for interpreting the Constitution.

Pursuant to § 1(2) of the Local Government Council Election Act each voter shall have one vote. Pursuant to § 17 of the Contested Act the LGCEA shall be supplemented with § 53^1, subsection (1) of which of establishes that when a voter has given several votes electronically, the last vote shall be taken into account. Pursuant to subsection (4) of the same section, if a voter has voted both electronically and by a ballot paper, the ballot paper shall be taken into account (the principle of supremacy of ordinary voting).

Within the system of electronic voting the taking into account of only one vote per voter is guaranteed by a system similar to the so called system of two envelopes, used upon voting outside the polling division of one's residence during advance polls. Upon voting by

electronic means a voter makes his or her choice, which shall be encoded (placed in a so-called inner envelope). Thereafter the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote (so-called outer envelope). The personal data and the encoded vote shall be stored together until the counting of votes on the election day, with the aim of ascertaining that the person has given only one vote. The personal data of a voter and the vote given by the voter shall be separated after the fact that the voter has given only one vote has been checked and repeated votes have been eliminated. It is possible to open the so-called inner envelope only after the personal data added to encoded vote have been separated with the help of a key given only to the members of the National Electoral Committee, after the polling divisions have been closed. Thus, the system of electronic voting guarantees that only one vote per voter shall be taken into account, ensuring, at the same time, that the voting remains secret.

Upon weighing the effect of the possibility to change an electronic vote on the weight of the vote given by a voter, the Chamber points out that in the case of repeated voting the votes given earlier shall be annulled. Despite the repeated electronic voting a voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. A vote given by electronic means shall be counted as one vote and from the point of view of voting results this vote is in no manner more influential than the votes given by voters using other voting channels.

Pursuant to the petition of the President the violation of uniformity of voting also consists in the fact that through the possibility to change the vote given for unlimited number of times advantages are accorded to voters voting by electronic means in comparison to the voters using other voting channels, as the latter lack the possibility to vote again or vote differently. This interpretations renders the principle of uniform elections a special case of general right to equality, established in § 12 of the Constitution.

Through legislation concerning suffrage the legislator has guaranteed all voters the legal possibility to vote in a similar manner. In the legal sense the system of electronic voting is equally accessible to all voters at local government council elections. Pursuant to § 5(1) and § 6(1) of Identity Documents Act, the identity card (ID card) necessary for electronic voting is mandatory both for an Estonian citizen staying permanently in Estonia and an alien staying permanently in Estonia on the basis of a valid residence permit. Thus, the state has created no legal obstacles to anyone to electronic voting, including to changing ones vote during the time prescribed for advance polls.

The Minister of Justice and the Chancellor of Justice refer to the possibility that the fact that due to factual inequality the possibility to change one's vote through electronic voting is not equally accessible to all voters can be regarded as an infringement of the general right to equality and the principle of uniformity. The Chamber also examines this allegation and points out that the existence of such infringement of the general right to equality and the principle of uniformity does not amount to an unconstitutional violation of the referred electoral principles. In order to answer the question of whether the possibility to change the vote given by electronic means amounts to an unconstitutional infringement of the right to equality and the principle of uniform voting, it shall be necessary to weigh whether the intensity of the infringement, consisting in the different treatment of the voters using electronic voting channels upon electing the local government councils, is proportionally related to the weight of the aims pursued.

The principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons with the right to vote. In fact, those who use the different voting methods provided by law (advance polls, voting outside the polling division of residence, voting in custodial institutions, home voting, voting in a foreign state, etc) are in different situations. For example, the voters who have to use the possibility of advance polls, are in a situation different from that of the voters who can exercise their right to vote on the election day. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the Constitution.

The decision to allow electronic voting at the elections of local government councils was taken by the Riigikogu upon passing the Local Government Council Election Act on 27 March 2002, with the aim of increasing the participation in elections, that is the democratic participation of people in making decisions pertaining to communal life. Bearing in mind the principle that elections shall be general, the aim is a legitimate one. Pursuant to the principle that elections shall be general all persons with the right to vote must be guaranteed a possibility to participate in voting. The measures the state takes for guaranteeing the possibility to vote to as many voters as possible are justified and advisable.

Another aim of allowing electronic voting is the modernising of voting practices, that is the introduction of new technological solutions. The ever growing number of Internet users among Estonia's inhabitants and the spread of services offered through electronic means (see TNS EMOR monitoring survey of 2005 - http://www.riso.ee/et/?q=node/136), as well as the introduction of mandatory ID card, have created favourable conditions for the introduction of electronic voting. Also, the preamble of "Standards of e-voting", enumerating the aims of allowing e-voting, refers, inter alia, to facilitating the casting of the vote by the voter, increasing voter turnout by providing additional voting channels, bringing voting in line with new technologies and reducing, over time, the overall cost of conducting an election. Pursuant to this document the members states (of the Council of Europe) need to take account of the new information and communication technologies, which are increasingly being used in day-to-day life, also in their democratic practice. The Constitution does not prohibit the modernisation of electoral practices, and thus it is a legitimate justification of the infringement of the right to equality and principle of uniformity.

The introduction of electronic voting without allowing to change the vote given by electronic means may endanger the principles of free voting and secret voting. The principle of free elections is established in the first sentence of § 156(1) of the Constitution, pursuant to which a local government council is elected in free elections. The secrecy of voting as a sub-principle of freedom of elections is a prerequisite of free elections. Pursuant to the principle of free elections both the participation in elections as well as the choice to be made are voluntary. In addition to the obligation that the state refrain from interfering with the freedom of choice of persons, the principle gives also rise to the obligation of the state to guarantee the protection of voters against the persons who try to influence the voter's choices. Pursuant to this principle the state must create necessary conditions for conducting free voting and protect voters from such influences that prevent the voter to give or not to give his or her vote in the manner he or she wishes.

The most effective way to guarantee the freedom of the voters from any external influences is to allow voting only in polling divisions and in voting booths, where a voter enters alone. It is clear that in the case of electronic voting in an uncontrolled medium, that is via Internet

outside a polling division, it is more difficult for the state to guarantee that voting is free of external influence and secret.

In accordance with § 162 of Penal Code (violation of freedom of election or voting), preventing a person to freely exercise his or her right to elect or be elected at an election or to vote at a referendum, if such prevention involves violence, deceit or threat or takes advantage of a service, economic or other dependent relationship of the person with the offender is punishable by a pecuniary punishment or up to one year of imprisonment.

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 watched 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, unlike 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 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 overweigh the aim of increasing the participation in elections and introducing new technological solutions. The Chamber is of the opinion that the possibility to change one's electronic vote is necessary for guaranteeing the freedom of elections and secrecy of voting upon electronic voting.

The Constitutional Review Chamber of the Supreme Court remarks that upon passing the contested regulation the legislator, having weighed different principles and the values underlying these, has appropriately balanced all electoral principles arising from the Constitution. Thus the e-voting provisions were considered constitutional and the President of the Republic proclaimed the Local Government Councils Election Act.

CURRICULUM VITAE
Priit Vinkel

1. Personal data

Date and place of birth	23 May 1983, Tartu
Citizenship	Estonian

2. Contact information

Address	Uus-Kalamaja 19-5, Tallinn 10415
Phone	+372 52 96 836
E-mail	pvinkel@gmail.com

3. Education

2006-2008	Tallinn University of Technology, *public administration, master's degree in social science, cum laude*
2001-2005	University of Tartu, *political science, BA degree (4 years)*

4. Defended theses

2008	*Master's degree in social science, cum laude*, supervisor Ülle Madise, *Organizational Culture in Estonian Municipalities in the Light of a Multi-dimensional Approach on Administrative Culture*, Tallinn University of Technology
2005	*Baccalaureus artium degree*, supervisor Rein Taagepera, *Compiling and Analysis of Proportional Profiles in Eastern Europe*, University of Tartu

5. Language skills

Estonian	native language
English	proficient
German	proficient
Russian	intermediate

6. Employment

2013-	Chancellery of *Riigikogu*, Head of Elections Department
2005-	National Electoral Committee, Member of Secretariat (since 2013 chief executive)
2011-2013	University of Tartu, Institute of Constitutional and International Law, assistant
2010-2011	Tallinn University of Technology, Tallinn Law School, extraordinary researcher
2008-2013	Tallinn University of Technology, Ragnar Nurkse School of Innovation and Governance, part-time lecturer
2007-2013	Chancellery of *Riigikogu*, Advisor of Elections Department
2006-2007	Chancellery of *Riigikogu*, Consultant of Constitutional Committee
2005-2006	Chancellery of *Riigikogu*, Consultant of Legal Affairs Committee

7. Supervised theses

2013	Aleksandr Toots, master's thesis *Erakondade rahastamise piirangud ja nendest kinnipidamise tagamine (TUT TLS)*
2012	Liina Osila, master's thesis *Turvalise paindlikkuse kontseptsioon Eestis vanemaealistele suunatud tööpoliitika näitel (TUT RNS)*
2012	Sten Šults, bachelor's thesis *Negatiivse valimisreklaami ulatus ja mõju Eestis 2011. aasta Riigikogu valimiste näitel (TUT RNS)*
2011	Siim Tolsting, bachelor's thesis *Kategooriakaitse gruppide roll Eesti poliitikas (TUT RNS)*
2010	Ain Ellam, bachelor's thesis *Noorte poliitiline aktiivsus ja võimalused poliitikasse sisenemiseks (TUT RNS)*

2009	Jelizaveta Krenjova, bachelor's thesis *European Parliament Elections in the Light of the Democratic Deficit: The Case of Estonia (TUT RNS)*

ELULOOKIRJELDUS
Priit Vinkel

1. Isikuandmed

Sünniaeg ja -koht	23. mai 1983, Tartu
Kodakondsus	Eesti

2. Kontaktandmed

Aadress	Uus-Kalamaja 19-5, Tallinn 10415
Telefon	+372 52 96 836
E-mail	pvinkel@gmail.com

3. Hariduskäik

2006-2008	Tallinna Tehnikaülikool, *avaliku halduse magistriõpe, sotsiaalteaduse magistrikraad, cum laude*
2001-2005	Tartu Ülikool, *politoloogia bakalaureuseõpe, BA kraad (4a)*

4. Kaitstud lõputööd

2008	Sotsiaalteaduse magister *cum laude*, juhendaja Ülle Madise, *Eesti linna- ja vallavalitsuste organisatsioonikultuur halduskultuuri mitmemõõtmelise hindamise taustal*, Tallinna Tehnikaülikool
2005	*Baccalaureus artium*, juhendaja Rein Taagepera, *Ida-Euroopa proportsionaalsusprofiilide koostamine ja analüüs*, Tartu Ülikool

5. Keelteoskus

eesti keel	emakeel
inglise keel	kõrgtase
saksa keel	kõrgtase
vene keel	kesktase

6. Teenistuskäik

2013-	Riigikogu Kantselei valimiste osakonna juhataja
2005-	Vabariigi Valimiskomisjoni sekretariaadi liige (alates 2013 juhataja)
2011-2013	Tartu Ülikooli riigi- ja rahvusvahelise õiguse instituudi assistent
2010-2011	Tallinna Tehnikaülikooli õiguse instituudi erakorraline teadur
2008-2013	Tallinna Tehnikaülikooli Ragnar Nurkse innovatsiooni ja valitsemise instituudi õppeülesande täitja
2007-2013	Riigikogu Kantselei valimiste osakonna (politoloogia)nõunik
2006-2007	Riigikogu põhiseaduskomisjoni konsultant
2005-2006	Riigikogu õiguskomisjoni konsultant

7. Juhendatud lõputööd

2013	Aleksandr Toots, magistritöö *Erakondade rahastamise piirangud ja nendest kinnipidamise tagamine (TTÜ ÕI)*
2012	Liina Osila, magistritöö *Turvalise paindlikkuse kontseptsioon Eestis vanemaealistele suunatud tööpoliitika näitel (TTÜ RNI)*
2012	Sten Šults, bakalaureusetöö *Negatiivse valimisreklaami ulatus ja mõju Eestis 2011. aasta Riigikogu valimiste näitel (TTÜ RNI)*
2011	Siim Tolsting, bakalaureusetöö *Kategooriakaitse gruppide roll Eesti poliitikas (TTÜ RNI)*
2010	Ain Ellam, bakalaureusetöö *Noorte poliitiline aktiivsus ja võimalused poliitikasse sisenemiseks (TTÜ RNI)*
2009	Jelizaveta Krenjova, bakalaureusetöö *European Parliament Elections in the Light of the Democratic Deficit: The Case of Estonia (TTÜ RNI)*

LIST OF AUTHOR'S PUBLICATIONS

Madise, Ü and P. Vinkel. 2015. "Judicial Approach to Internet Voting." In Jordi Barrat and Ardita Driza Maurer (eds.). *E-Voting Case Law: A Comparative Analysis*. Farnham: Ashgate Publishing, 1-35 *(forthcoming)*.

Vassil, K., M. Solvak and P. Vinkel. 2014. "E-valimiste levik Eesti valijate hulgas." *Riigikogu Toimetised* 30, 116-128.

Madise, Ü and P. Vinkel. 2014. "Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections." In Tanel Kerikmäe (ed.). *Regulating eTechnologies in the European Union*. Cham: Springer International, 53-72.

Madise, Ü., E. Maaten and P. Vinkel. 2014. "Voto por Internet en Estonia." In A. Ayala Sanchez (ed.). *Nuevas Avenidas de la Democracia Contemporanea*. Mexico: Institutio de Investigaciones Juridicas, Universidad Nacional Autonoma de Mexico, 575-601.

Ehin, P., Ü. Madise, M. Solvak, R. Taagepera, K. Vassil and P. Vinkel. 2013. *Independent Candidates in National and European Elections: Study*. Brussels: European Union.

Vinkel, P. 2012. "Internet Voting in Estonia." In P. Laud (ed.). *Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011, Tallinn, Estonia, October 26-28, 2011, Revised Selected Papers.* Berlin: Springer, 4-12.

Vinkel, P. 2012. "Internet Voting: Experiences from Five Elections in Estonia." In: T. Jundzis (ed.). *Proceedings of the International Conference: Democracy and Development – Taiwan and Baltic Countries in Comparative Perspective, 27-28 April 2012.* Riga: Latvian Academy of Sciences, 176-188.

Koitmäe, A., M. Pilving, P. Vinkel, M. Ets, H. Trumann and M. Vihuri. 2012. *Elections in Estonia 1992-2011*. Tallinn: National Library of Estonia.

Madise, Ü. and P. Vinkel. 2011. "Constitutionality of Remote Internet Voting: The Estonian Perspective." *Juridica International* 18, 4-16.

Stepanov, H. and P. Vinkel. 2011. *Riigikogu valimine 6. märts 2011*. Tallinn: Riigikogu Kantselei.

Heinsalu, A., A. Koitmäe, M. Pilving, P. Vinkel, H. Sibul, M. Plink and A. Igalaan. 2011. *Valimised Eestis 1992-2011: Statistikat ja selgitusi*. Tallinn: Vabariigi Valimiskomisjon

Madise, Ü. and P. Vinkel. 2010. "TIC, votacions per Internet i altres serveis electronics a Estonia." In J. Vall (ed.). *EINES 12, Politica 2.0*. Barcelona: Fundacio Josep Irla, 59-67.

Vinkel, P. and H. Stepanov. 2010. *Kohaliku omavalitsuse volikogu valimised: 18. oktoober 2009*. Tallinn: Vabariigi Valimiskomisjon.

Vinkel, P. 2010. *Euroopa Parlamendi valimine: 7. juuni 2009*. Tallinn: Vabariigi Valimiskomisjon.

Madise, Ü., P. Vinkel and A. Heinsalu. 2009. "Hinnang Tallinna volikogu valimise süsteemi muudatuste mõjule." *Juridica 9*, 636-646.

Mäeltsemees, S., Ü. Madise and P. Vinkel. 2008. "Dimension of Administrative Culture in Estonia." In J. Beck and F. Thedieck (eds). *The European Dimension of Administrative Culture: Conference on The European Dimension of Administrative Culture. Strasbourg, 15-16 May 2007*. Schriften der Deutschen Sektion des internationalen Instituts für Verwaltungswissenschaften 33, Baden-Baden: Nomos Verlagsgesellschaft, 144-160.

Madise, Ü., S. Mäeltsemees, K. Aas and P. Vinkel. 2007. "Administrative Culture in Estonia." In F. Thedieck (ed.). *Foundations of Administrative Culture in Europe*. Baden-Baden: Nomos Verlagsgesellschaft, 135-145.

Jõeorg, M., L. Kirsipuu, M. Kõrgmaa, S. Hansson, M.-M. Vanatalu, E. Vanatalu, A.-M. Veidemann, P. Vinkel, R. Kaarma, M. Räis, K. Vaksmaa, R. Taagepera, A. Jarne, K. Piiskop and K. Klettenberg-Paas. 2007. *Kodaniku käsiraamat*. Tallinn: Mitte-eestlaste Integratsiooni Sihtasutus

Orav, M., E. Maaten and P. Vinkel. 2007. *Riigikogu valimine: 4. märts 2007*. Tallinn: Vabariigi Valimiskomisjon.

Madise, Ü., P. Vinkel and E. Maaten. 2006. *Internet Voting at the Elections of Local Government Councils on October 2005: Report for the National Electoral Committee*. Tallinn: Estonian National Electoral Committee.

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESES
SERIES I: SOCIAL SCIENCES

6. **Ülle Madise**. Elections, Political Parties, and Legislative Performance in Estonia: Institutional Choices from the Return to Independence to the Rise of E-Democracy. 2007.
7. **Tarvo Kungla**. Patterns of Multi-Level Governance in Europe: The Challenge of the EU's Enlargement. 2007.
8. **Mikk Lõhmus**. Avaliku halduse detsentraliseerimine Eestis. 2008.
9. **Tarmo Kalvet**. Innovation Policy and Development in the ICT Paradigm: Regional and Theoretical Perspectives. 2009.
10. **Thomas Duve**. Die Verschuldung deutscher Gemeinden: Präventionsansätze im Spannungsverhältnis von kommunaler Selbstverwaltung und staatlicher Gesamtverantwortung. 2009.
11. **Veiko Lember**. Contracting-Out Public Services and Public Procurement for Innovation: Revisiting Contracting Limits in Estonia and Beyond. 2009.
12. **Raivo Linnas**. An Integrated Model of Audit, Control and Supervision of the Local Government Sector: The Case of Estonia. 2010.
13. **Simon Lang**. Transformations in European R&D and Regional Policies within the Multi-Level Governance Framework: The Changing Nature of the European Union Ten Years after the Launch of the Lisbon Strategy. 2010.
14. **Erkki Karo**. Governance of Innovation Policy in Catching-up Context: Theoretical Considerations and Case Studies of Central and Eastern European Economies. 2011.
15. **Margit Suurna**. Innovation and High-Technology Policy, Policy-Making and Implementation in Central and Eastern European Countries: The Case of Estonia. 2011.
16. **Marek Tiits**. Technology Foresight and the Catching-up Strategy in Small Countries: The Case of Estonia. 2011.
17. **Vasileios Kostakis**. The Political Economy of Information Production in the Social Web: Towards a "Partner State Approach". 2011.
18. **Jane Järvalt**. Strategic Human Resource Management in the Public Service: Evidence from Estonia and Other Central and Eastern European Countries. 2012.
19. **Robert Krimmer**. The Evolution of E-voting: Why Voting Technology is Used and How It Affects Democracy. 2012.

20. **Külli Sarapuu**. Mapping and Explaining Post-Communist Development of Administrative Structure: The Case of Estonian Public Administration 1990–2010. 2013.
21. **Kristi Joamets**. Gender as an Element of Marriage Capacity in the Context of National and Supranational Law in the European Union. 2014.
22. **Aleksandr Aidarov**. Estonian National Minorities' Cultures: Successes and Failures Policy Goals, Instruments and Organization. 2015.
23. **Riin Savi**. The Impact of Fiscal Crisis on Public Administration: Cutback Management and Changes in Decision-Making. 2015.
24. **Priit Vinkel**. Remote Electronic Voting in Estonia: Legality, Impact and Confidence. 2015.