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

© Springer International Publishing Switzerland 2014

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).

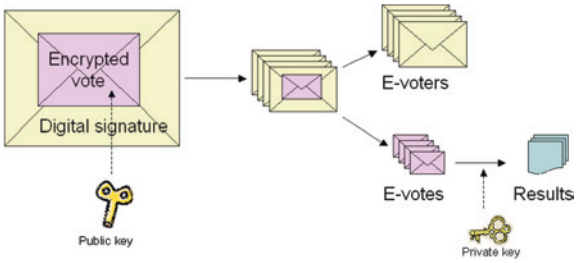

Fig. 1 Double-virtual envelope PKI-based method for I-voting

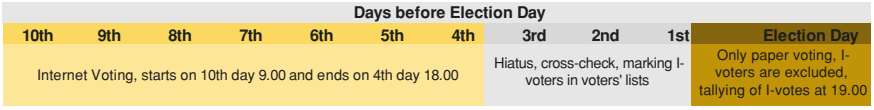

Fig. 2 I-voting event cycle

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.