

# **Towards remote e-voting: Estonian case**

Epp Maaten

Elections Department  
Chancellery of the Riigikogu (Parliament)  
Lossi pl. 1A  
15181 Tallinn, ESTONIA  
epp.maaten@riigikogu.ee

**Abstract:** This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

## **1 Introduction**

The possibilities of implementing e-voting have been actively discussed in Estonia already since 2001. In 2002 the legislative basis to conduct e-voting was created. In summer 2003 by the National Electoral Committee the e-voting project was initiated.

The e-voting project serves the Estonian government's goal of using digital technology to help making the public sector more efficient, effective, and customer-friendly. The coalition agreement of the current government states that e-voting should be available starting from local government council elections of 2005 and for the following elections.

A number of countries use electronic voting machines within polling stations to e-enable elections, but this has not been an option for Estonia. E-voting in the context of Estonia means remote voting via Internet. The main goal is to provide voters an extra opportunity to cast their vote and thereby increasing voter participation.

## **2 Legislative basis**

According to Estonian election legislation<sup>1</sup> e-voting takes place during the advance voting period from 6<sup>th</sup> to 4<sup>th</sup> day before Election Day. The following requirements of e-voting are laid out:

“(1) On advance polling days, voters holding a certificate for giving a digital signature may vote electronically on the web page 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 consolidated list of candidates in the electoral district of the residence of the voter shall be displayed to the voter on the web page. The opportunity for the voter to examine the national lists of candidates shall be provided.

(4) The voter shall indicate on the web page 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 taken into account shall be displayed to the voter on the web page.”

E-voting shall be an additional voting option. The other options existing today, which are voting at the polling place or by embassies, advance voting outside of polling place of voter’s residence and voting by mail in foreign states, remain.

## **3 Basic principles of e-voting**

The main principle of e-voting is, that it must be as similar to regular voting as possible and compliant with election legislation and principles. E-voting should offer the same level of security and confidence as traditional voting. Therefore according to the electoral laws e-voting must be uniform and secret, only eligible persons must be allowed to vote, every voter should be able to cast only one vote, a voter must not be able to prove in favour of whom he/she voted. At last, the collecting of votes must be secure, reliable and accountable.

From a technical point of view the e-voting system must be as simple as possible as well as transparent so that a wide range of specialists would be able to audit it. The e-voting system must be reusable in a way that developing a new system for the next voting is not needed.

---

<sup>1</sup> Riigikogu Election Act, Local Government Council Election Act, Referendum Act and European Parliament Election Act – all 4 election acts contain similar terms for e-voting.

The following principles are specific to Estonian e-voting concept:

- \* ID-cards are used for voter identification;
- \* Possibility of electronic re-vote – e-voter can cast his/her vote again and the previous vote will be deleted;
- \* The priority of traditional voting – should the voter go to polling station on voting day and cast a vote, his or her e-vote shall be deleted.

### **3.1 Voters authentication with ID-card**

Estonia has implemented ID card as the compulsory document for identifying citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and legally binding digital signature, in connection with nationwide online services. ID-cards are equipped with a chip containing electronic data, certificates and their associated private keys protected with PIN-codes. The ID card functions as an electronic identity, enabling to use services online conveniently and securely.

According to law a voter identifies himself or herself by giving a digital signature. This is a crucial point laid down by law to avoid security risks related to voter identification during remote e-voting. The introduction and rapid spread of ID-cards provides the necessary tools for e-voting – electronic voter authentication and possibility to give digital signatures.

The use of ID-card is a different approach to solve the problem of voters identification. In some countries, which are piloting the e-voting, identification codes are sent to the voters often by post. It would be quite insecure method for Estonia. For different reasons many citizens have not been interested to disclose their real home address to the national population register. Because of incorrect information of the register many envelopes with codes necessary for identification would be lost or would reach a wrong addressee.

Widespread use of ID-card is vital – in regards to Estonian e-voting, systems that require previous on-the-spot registration are not considered. Recently a number of mass-market projects using the ID-card were started. For instance in the public transportation system of the capital city of Tallinn a new virtual ID-card-based payment and control system is employed. Residents, willing to use the Tallinn public transport!and other services for city residents at discounted prices, have to obtain an ID-card.

The number of ID-card holders has increased very rapidly during the last year. By now about 500 000 ID-card have been issued<sup>2</sup>. By the 2005 elections this number should approach 800, 000, meaning that most of the eligible voters (about 1 Million for local elections) should be covered [GD04; P 4].

### **3.2 Electronic re-vote and the priority of traditional voting**

In the concept of e-voting two principles are important:

---

<sup>2</sup> Statistics of issuing the ID-cards: : <http://www.id.ee/pages.php/03020504>

\* *The possibility of re-vote* – voter has a chance to cast his/her vote again; Voter is allowed to vote electronically more than once. In this case the previous e-vote will be deleted. Multiple voting is mostly considered as a crime, but according to General Description of the E-Voting System only one e-vote per voter, the last one will be entered into the electronic ballot box [GD04; P 7]. Electronic re-vote cannot thus be considered as multiple voting, as the system will take into account only one vote. Allowing to re-vote is considered as a measure against vote-buying and against voting under coercion. Remote voting in an uncontrolled area can be easily manipulated. A voter could be coerced into voting for a particular candidate or voters have the opportunity to sell their vote. By re-voting the voter who was illegitimately influenced can cast a new vote once the influence is gone.

\* *The priority of traditional voting* – if the voter goes to polling station on Election Day before 16.00 and casts the vote using a paper ballot, then his or her e-vote cast during advance voting period, will be deleted.

The justification of this principle is similar to the previous one. The principle makes also possible to declare the e-voting invalid in the case the e-voting system used during advance polls has been seriously compromised or rendered. Then the voters still have the possibility to participate on elections and vote traditionally on Election Day.

#### **4 General concept of e-voting - the envelope method**

It is highly important that public confidence in the election process remains strong. The right of individuals to vote is one of the main principles of democracy. Great effort and care should be taken to ensure that elections as well as e-voting, which is a part of whole election process, are conducted in a fair manner. A research about public opinion concerning e-voting shows that people mostly trust electronic services available through Internet (banking, for instance) and thus they also tend to trust e-voting. On the other hand there is a lack of information what e-voting actually means and many people could not answer the question about trusting the system [RCF04; P 22, 23]. As the detailed e-voting concept has been published only in January 2004, it has not been widely discussed by media.

It is important that e-voting could be explained as simply as possible to be understandable for voters. One way to simplify the complexity of e-voting is to draw parallels to ordinary voting. The e-voting scheme is similar to the envelope method used during advance polls today:

- \* the voter identifies himself/herself to polling commission,
- \* the voter fills the ballot and puts it in an inner envelope,
- \* that envelope is put into another envelope on which the voter's data is then written,
- \* the envelope is transported to the voter's polling station, the voter's eligibility is verified, and if the voter is eligible, the outer envelope is opened and the anonymous inner envelope is put into the ballot box.

The e-voting follows the same scheme:

- \* The voter inserts the ID-card into a card reader and opens the homepage of the National Electoral Committee,
- \* a relevant candidate list of voter's constituency is displayed according to the voters personal identification number,
- \* the voter makes his/her voting decision, which is encrypted and can be defined as inner envelope,
- \* the voter confirms his/her choice with a digital signature and the outer envelope comes up, voter gets a confirmation, that his/her vote has been recorded,
- \* at the vote count the voter's digital signature (outer envelope) is removed and at the final stage the members of the National Electoral Committee can only collegially open the anonymous e-votes and count them.

The following figure illustrates the envelope method:

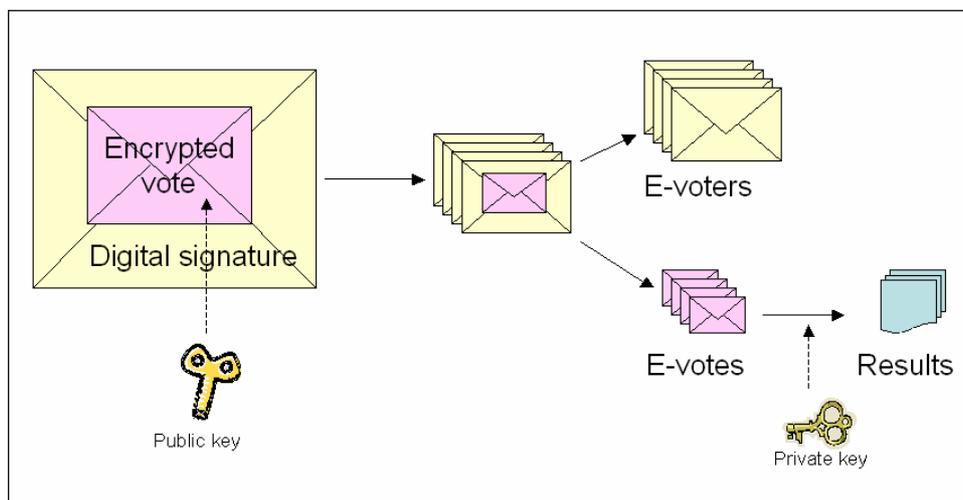


Fig 1: The envelope method [GD04; P 9]

Public-key cryptography is used here. Application encrypts voter's choice with the system's public key and voter confirms the choice by signing it digitally. The votes are collected, sorted, voter's eligibility is verified and double votes are removed. Then the outer envelopes (digital signatures) are separated from inner envelopes (encrypted votes).

Inner envelopes are forwarded to the National Electoral Committee who has the private key of the system. Voter's choice encrypted with the system's public key can be decrypted only with private key. To ensure the voter's privacy the requirement is, that at no point should any part of the system be in possession of both the digitally signed e-vote and the private key of the system. In order to count e-votes, the system's private key is activated by key-managers according to the established key management procedures. The counting of votes takes place in the vote counting application, separated from the network.

The lists of voters who voted electronically are compiled from outer envelopes - from voter's ID-numbers. These lists are sent to local polling stations and on Election Day it is easily detectable if a voter who has already voted electronically, comes to polling station to vote by paper ballot. In that case the polling station committee informs the National Electoral Committee and voter's e-vote shall be deleted.

There are always two participating parties in voting – the voter and the vote receiver. The weakest link of the e-voting procedure is probably the voter's personal computer as no control can be exerted over it. The central servers which are under National Electoral Committee's responsibility can be controlled, however the errors and attacks, which may occur there influence a large amount of votes simultaneously. The e-voting system should take these issues very seriously.

The following considerations speak in favour of the envelope method:

- \* simplicity and clearness of the scheme, possibility to draw a parallel with traditional elections;
- \* simplicity of the system architecture – the number of components and parties is minimal;
- \* full use of digital signature.

The e-voting system shortly described here enables a basis for conducting e-voting at least as securely as traditional voting upon condition that that sufficient organisational, physical and technical security measures are implemented.

These were the main principles of the selected envelope system. Obviously the scheme is more complex in reality, offering additionally a possibility to securely cancel e-votes, covering detailed architectural components of the system, different organisational parties etc.

## **5 Problems decelerating the implementation of e-voting**

There are many aspects of elections besides technical security problems that may bring e-voting into question.

E-voting brings along many concerns of fraud and privacy associated with remote balloting, including the risk that voters who do not cast their votes in the privacy of a voting booth, may be subject to coercion, or that voters have the opportunity to easily sell their vote. During the last elections in Estonia some vote-buying incidents became public and the problem has been blown up in mass media. This is partly the reason why the e-voting concept suggests that the re-voting should be allowed. The fact that voter has always a possibility to re-vote, even in the controlled area on elections day, can minimise the number of manipulative attempts.

**The legislative basis** to conduct e-voting has been created but according to e-voting concept evolved during the last year, the election laws should be amended in some crucial points like allowing to re-vote electronically. Also the priority of traditional voting should be enacted. It is indispensable to convince politicians that the e-voting system can still guarantee that there is only one vote per voter in the ballot box.

The number of people holding **ID-cards** has increased very rapidly but possessing the card is not enough for e-voting. Giving a digital signature implies that voter had a computer with the proper software installed and a card reader. The software enabling the use of the ID-card and digital signature is freeware, the card reader costs about 20 €. Thus, insufficient number of card readers, the complexity of software installation and the lack of knowledge how to give a digital signature may endure as obstacles of widespread e-voting.

**Privacy** is a key issue in e-voting. Like in most European countries, also in Estonia voting privacy in ordinary voting is guaranteed by forcing voters to vote alone in a voting booth. Voting in an uncontrolled area means, that there is no guarantee for privacy any more. However, it is not solely a problem of e-voting. Similar concerns arise if voting by mail is allowed. This aspect cannot be ignored, but as the possibility of traditional voting remains, voters who are worried about the privacy can choose the paper balloting.

A mention must be made of the **sociological problems**. Remote voting also requires technology and the knowledge to use it. If remote voting were to become the dominant form of voting, it could result in an increased digital divide caused by Internet access and computer skill barriers. Even if e-voting is an additional voting option, the proportions between voter's age groups may change. In 2002 the share of Internet users was 39% in the 15-74 age bracket, but the percentage is much higher among the young people [DD02]. It is reasonable to assume that e-voting will activate people, who would not participate in voting at polling stations.

Some steps towards overcoming the **digital divide** are already made. Since 2001 a national training project during which about 10% of the adult population of Estonia received free elementary computer and Internet training, has been carried out [LW04, P 2]. To improve the Internet access another project named "Village Road" was launched. The aim of that project is to establish Internet connection in Estonian public libraries, to establish of Public Internet access points in them, and provide with workplace computers and software. In 2003 all access points have been supplied with smart card readers so that people would be able to use e-services with their ID-card. In April 2004 about 550 access points existed [LW04, P 12].

There are still many concerns about the **confidentiality** of electronic voting and fears that a vote can be related to voter. An information campaign could be one of the measures to make the details of e-voting security, including the role of cryptology in it, publicly acquainted. Building public trust is one of the most difficult aspects of introducing the e-voting. The proposed e-voting methods need public acceptance otherwise legitimacy of e-voting can be placed in doubt.

## **6 Current state of e-voting project and future plans**

During the last year a technical and organisational concept of e-voting has been prepared, which in turn has been subjected to a thorough security analysis. Afterwards the technical planning of the system has been made. A public procurement procedure was carried out and the contract to develop the e-voting software was given to the Estonian company named Cybernetica Ltd. The software should be ready by autumn 2004 and further it will be a subject to audit. The key management and audit regulations are under work.

In late 2004 the first pilot project is planned, where the whole e-voting system will be put to test. This pilot will, according to current plans, take place in the capital city of Tallinn in a form of consultative referendum. After the test and the audit further plans can be made. As mentioned before, the next pilot is planned for the local government council elections in October 2005.

It is not clear if e-voting could raise the level of voter turn-out. However, it is a measure, which may hinder the steady decrease of turn-out percentage. Remote e-voting is regarded as an added value to the voter and a measure of widening of the democracy. Growth of online interaction and presence can be witnessed by the exponential increase in the number of people with home computers and Internet access. Since the idea of e-voting became public in 2001, many people in Estonia expect that e-voting becomes an integral part of today's information society as soon as possible. There are strong views that rapid developments of information society should be taken into account in state's democratic practice.

A step-by-step approach when introducing e-voting is regarded as absolutely necessary: from testing to piloting, from small to bigger numbers of potential voters, from restricted to general elections. For Estonia there is a long way to go towards the successful implementation of remote e-voting, but at least we have started off and took the first steps on this way. We try to make our best that this way will bring success.

### **Literature used**

- [GD04] The Estonian National Electoral Committee: General Description of the E-Voting System, Tallinn 2004. <http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf>
- [RCF04] Research Centre Faktum: E-voting and decrease of alienation. Tallinn, January 2004. P 23-27. <http://www.parlament.ee/?id=846>
- [DD02] M.Kalkun, T.Kalvet , Emor and Praxis Centre of Policy Studies: Digital Divide in Estonia and How to bridge it, Tallinn 2002, P 49.
- [LW04] Look@World Foundation: Internet Training Project Report, Tallinn 2002, P 2. [http://www.vaatamaailma.ee/pls/VM/docs/FOLDER/VAATA\\_MAAILMA2/DOKUME\\_NDID/PROJEKTID/LW\\_TRAINING\\_PROJECT\\_REPORT.PDF](http://www.vaatamaailma.ee/pls/VM/docs/FOLDER/VAATA_MAAILMA2/DOKUME_NDID/PROJEKTID/LW_TRAINING_PROJECT_REPORT.PDF)