The National Election Committee

E-Voting System

Overview

- Tallinn 2005 -

Annotation

This paper gives an overview of the technical and organisational aspects of the proposed Estonian e-voting system. The present paper is aimed at the general public.

Contents

Introduction

The subject of e-voting has been actively discussed in Estonia on different levels since the beginning of this century. There exists an opportunity and motivation to implement such a project with the purpose of offering voters a possibility of e-voting at local government council elections of 2005, for:

- There exists a legal basis for carrying out e-voting which is laid out in the following legal acts:
  - Local Government Council Election Act, § 50;
  - Riigikogu Election Act, § 44;
  - European Parliament Election Act, § 43;
  - Referendum Act, § 37.
- A public key infrastructure enabling secure electronic personal authentication using digital signatures and ID-cards has been created – currently (August 2005) over 800,000 ID-cards have been issued, meaning that most of the eligible voters is covered.

This overview gives a general description of the technical and organisational system of the planned e-voting system. This document:

- defines the scope of e-voting, in other words, defines the subject in the context of the election process as a whole,
- specifies the system requirements,
- specifies the participating parties of the system and describes their roles,
- specifies the architecture of the e-voting system, the general description of functionality, protocols and algorithms,
- analyses and describes possible security hazards and examines the compliance of the system to security requirements.

This document discusses to some extent but does not concentrate on:

- exact specification of the security level of system components,
- specification of data structures,
- choice of software and hardware platforms,
- technical structure of the system's network – server redundancy, network security measures to be used (firewalls, intrusion detection systems), architecture of network connections.

1. Scope of E-voting System

The e-voting system to be discussed makes up a relatively small part of the whole election process. From a technical viewpoint the elections are made up of the following components:
* calling of elections,
* registration of candidates,
* preparation of polling list,
* voting (a subset of which is e-voting),
* counting of votes.

Other components such as auditing, reviewing of complaints and other supporting activities could be mentioned.

The e-voting system discussed in this paper assumes that:
a) voter lists have been prepared and are available in a suitable format,
b) the candidate lists have been prepared and are available in a suitable format,
c) e-votes are counted separately and are later added to the rest of the votes.

In other words the input of the e-voting system is made up from:
a) voter lists (including the polling division and constituency assigned to the voter),
b) candidate lists (by constituencies),
c) expressed will of the voters,
and the output is made up from:
a) summarized voting result of e-voters,
b) list of voters who used e-voting.

The following figure illustrates the scope of an e-voting system and its input and output parameters:

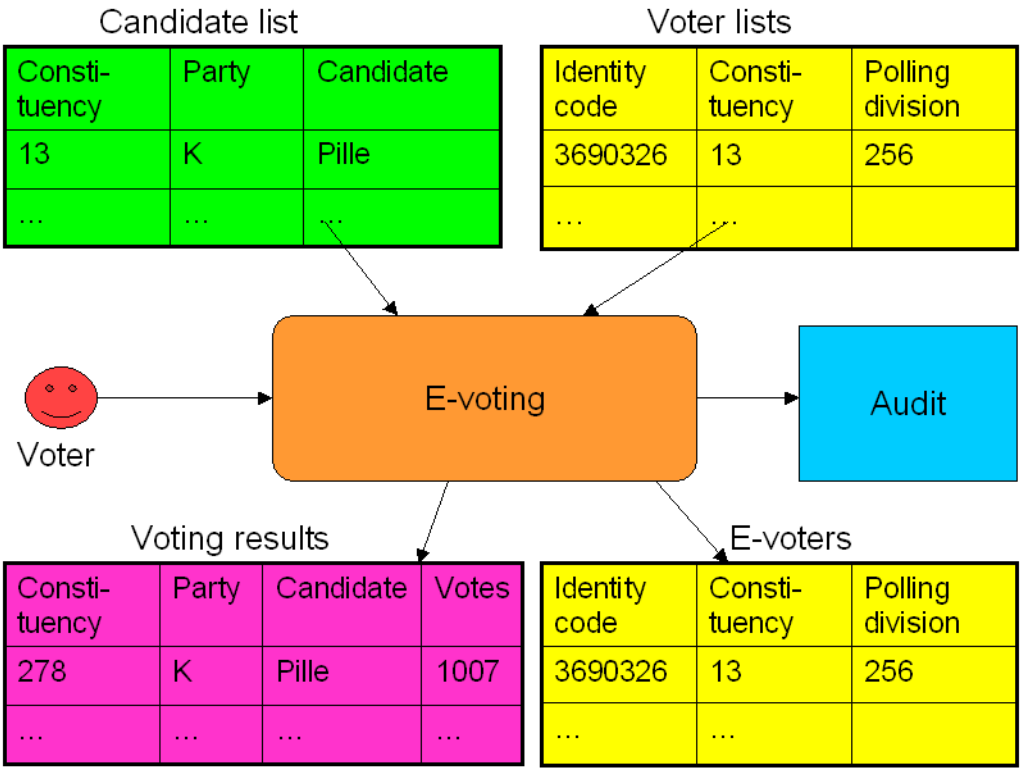

Fig. 1 The scope of e-voting: input and output

2. Basic Principles of E-voting

The main principle of e-voting is that it must be as similar to regular voting as possible, compliant with election legislation and principles and be at least as secure as regular voting.

Therefore e-voting must be uniform and secret, only eligible persons must be allowed to (e-)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. In addition to this the collecting of votes must be secure, reliable and accountable.

According to Estonian election legislation e-voting takes place from 6th to 4th day before Election Day and the following requirements are laid out:

"(1) On advance polling days, voters 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 using the certificate entered on his or her identity card which enables digital identification.

(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.

(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 by signing it digitally using the certificate entered on his or her identity card which enables digital signing.

(5) A notice that the vote has been taken into account shall be displayed to the voter on the web page.

(6) Voter may change his or her electronic vote during the advance voting period from 6th to 4th day before Election Day:

1) by voting electronically;
2) by voting in polling station.

The following principles are specific to e-voting:

* For voter identification ID-cards are used

At the moment ID-card is the only independent means of electronic communication that enables to authenticate voters at a maximum security level, enables to give digital signatures and that most of voters already possess. The last aspect is vital – in regards to Estonian e-voting, systems that require previous on-the-spot registration are not considered.

* Possibility of electronic re-vote – e-voter can cast his/her vote again and the previous vote will be deleted

Even though usually multiple voting is considered a crime (Penal Code, § 165), in this case it is a measure against vote-buying – the voter who was illegitimately influenced can cast the vote anew once the influence is gone. Electronic "re-vote" cannot thus be considered "multiple voting" as the system will only take into account one vote (the one given last).

* The priority of traditional voting – should the voter go to polling station on advance voting day and cast a vote, his or her electronically cast vote shall be deleted.

The justification to this principle is similar to the previous one. It might be also necessary in a more general case – for example, should it be determined that the e-voting system used during advance polls is seriously compromised or rendered unusable and all or some of the e-votes have to be declared invalid, the voters can cast their vote in a traditional way.

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 are 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.

There are always two participating parties in voting – the voter and the receiver of the vote. For e-voting these are the voter's PC and the servers maintained by and under the responsibility of the National Election Committee (NEC). The weakest link of the e-voting procedure is probably the voter's PC as no control can be exerted over it. The NEC's servers can be controlled, however the errors and attacks, which may occur there, influence a large amount of votes simultaneously. The e-voting system takes these issues very seriously.

3. Stages of E-voting Process

The electoral acts stipulate that e-voting takes place from 6th to 4th day before Election Day. This gives time to prepare voter lists for Election Day in such a way that they would show the persons who have already voted electronically, thus avoiding double voting.

As the requirements also state the priority of traditional voting over e-voting, a procedure is foreseen that enables to inform of the cancellation of e-votes of those persons who have re-cast their votes at the polling station.

Considering these limitations we can come up with the following schedule:

* The electronic lists of candidates as well as voters lists must be finalized at least by Sunday, one week before election day. The voters list will be updated during advance voting days.
* E-voting is made available simultaneously with advance polls, it starts from Monday of the election week at 9 a.m and ends on Wednesday at 8 p.m.
* After the close of e-voting the list of e-voters is finalized.
* E-votes are sorted, multiple votes and votes of ineligible voters are declared invalid.
* The lists of e-voters are sent to polling divisions after which the division committees make the relevant notations to the polling division voter lists.
* On election day a list of the voters whose e-vote is declared invalid (as they have cast their votes at a polling division during advance polls) is prepared by polling division committees and it will be sent to the NEC which will cancel the corresponding e-votes. By 12.00 on Elections Day these lists must reach the NEC.
* At 19.00 the "e-ballot box" is opened and e-votes are counted. The results shall not be published before 20.00 on Election Day.

4. General Concept of E-voting

The e-voting concept is similar to the envelope method used during advance polls today to allow voting outside of polling place of voter's residence:
* 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. E-voter creates during the voter procedures an inner envelope (which is essentially an encrypted vote) and an outer envelope (which is essentially a digital signature).

The following considerations speak in favour of the envelope method:
* simplicity and understandability of the scheme, possibility to draw a parallel with traditional elections;
* simplicity of system architecture – the number of components and parties is minimal;
* full use of digital signature.

The following figure illustrates the envelope method:

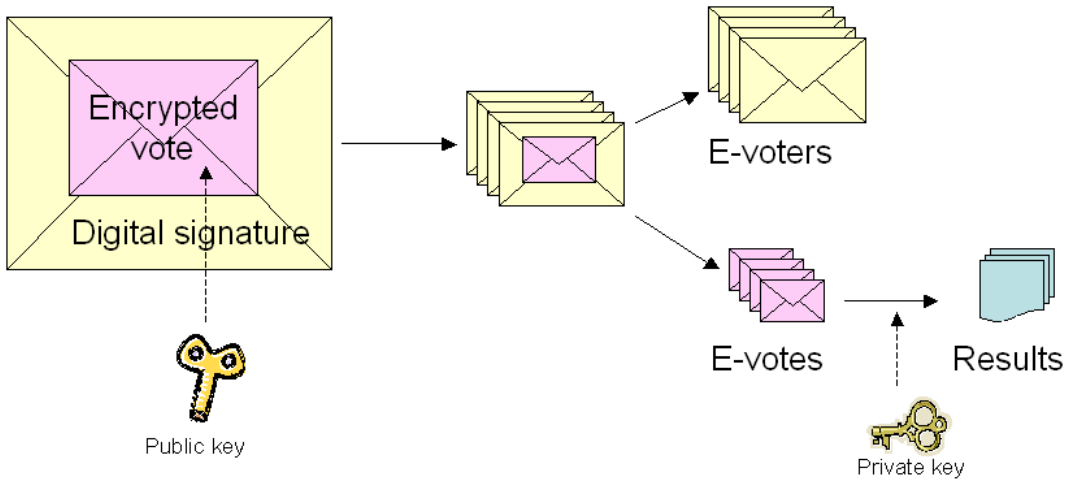

Fig. 2. The envelope method

Public key cryptography is used here.[1] E-voter (application) encrypts his/her choice (number of candidate) with the system's public key and signs the result digitally. The votes are collected, sorted, voter's eligibility is verified and invalid votes are removed (double votes, votes of ineligible voters). Next the outer envelopes (digital signatures)

[1] Public key cryptography uses a key pair – private key and public key. When a source text is encrypted with a private key the resulting cryptogram can only be decrypted with the corresponding public key. And vice versa – once the source text is encrypted with a public key then the resulting cryptogram can only be decrypted with the corresponding private key.

are separated from inner envelopes (encrypted votes). Voter lists are compiled from outer envelopes. Inner envelopes (which are not associated with the identity of the voter any more) are forwarded to the vote-counter who has the private key of the system. The vote-counter (application) outputs the summed results of e-voting.

The following requirement ensures that the privacy of e-voters is maintained: **at no point should any party of the system be in possession of both the digitally signed e-vote and the private key of the system.**

This is the basic scheme of the selected envelope system. Obviously the scheme is more complex in reality, additionally offering a possibility to securely cancel e-votes, covering detailed architectural components of the system, different organisational parties etc. This will be discussed in the following sections.

5. System Architecture and Participating Parties

In this section we will specify the system components and describe their functionality and interfaces. We will determine the participating parties in the system and describe the possible breakdown of components between different parties.

The following figure describes the system architecture:

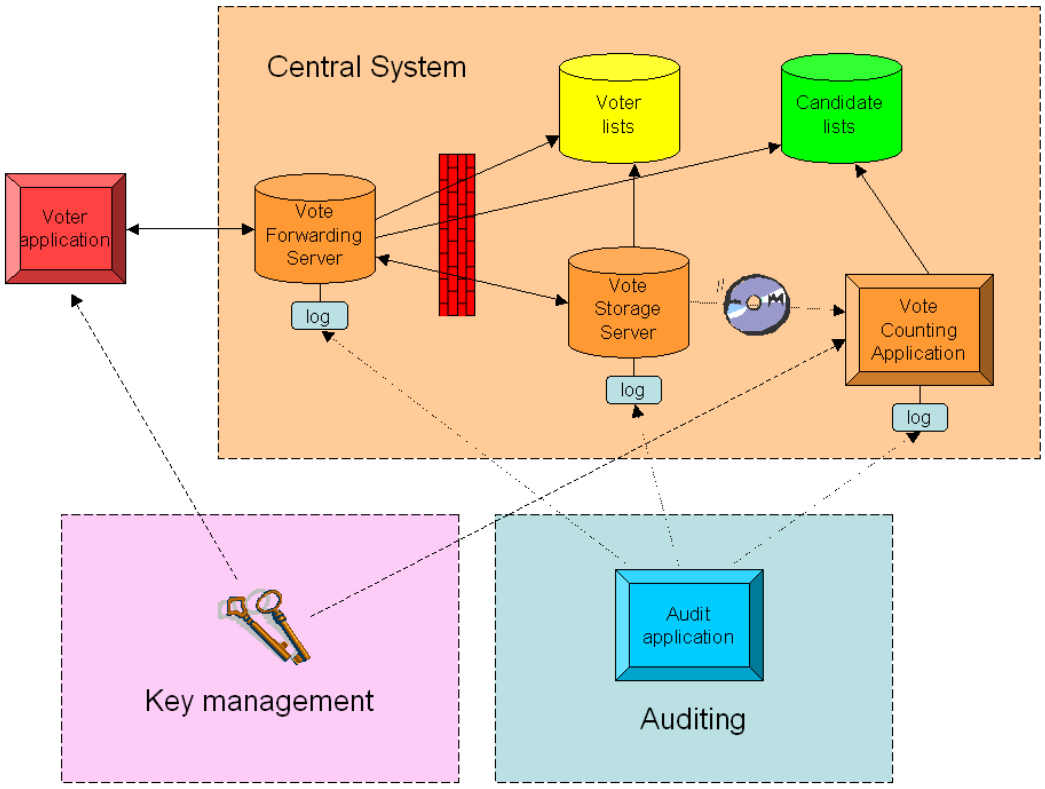

Fig. 3. Election System's general architecture

We will start by describing the parties which in the figure are represented by differently coloured squares:

* **Voter** – e-voter with his/her PC. Creates an encrypted and digitally signed vote and sends it to the Central System.

* **Central System** – System component that is under the responsibility of the National Election Committee. Receives and processes the votes until the composite results of e-voting are output.
* **Key Management** – Generates and manages the key pair(s) of the system. The public key (keys) are integrated into Voter's applications, private key(s) are delivered to Vote Counting Application.
* **Auditing** – solves disputes and complaints, using logged information from the Central System.

The Central System is also dependent of two other parties:
* Compiler of voter lists (The Population Register),
* Compiler of candidate lists (NEC itself).

Now we will examine the components of the Central System:
* **Vote Forwarding Server (VFS)** – authenticates the voter with the means of ID-card, displays the candidates of voter's constituency to the voter and receives the encrypted and digitally signed e-vote. The e-vote is immediately sent to the Vote Storage Server and the confirmation received from there is then forwarded to the voter. Ends its work after the close of advance polls.
* **Vote Storage Server (VSS)** – receives e-votes from the VFS and stores them. After the close of advance polls removes double votes, cancels the votes by ineligible voters and receives and processes e-vote cancellations. Finally it separates inner envelopes from outer envelopes and readies them for the Vote Counting Application.
* **Vote Counting Application (VCA)** – offline component to which crypted votes are transmitted with the digital signatures removed. The Vote Counting Server uses the private key of the system, tabulates the votes and outputs the results of e-voting.

6. E-Voting Procedures

In this section we will describe in greater detail the behaviour of the components present in the general architecture of the system during different stages of e-voting.

6.1. Key Management

The key management procedures and the security scheme used are one of the most critical points of the system on which the fulfilment of the main requirements of the system (privacy and secrecy of voting) depends. What follows is not a final description of the measures and procedures, but we will outline the main concept, main risks and possible solutions.

The main tool to guarantee the secrecy of voting in the system is asymmetric cryptography. A **system key pair** is generated, the public component of which is integrated into client software and is used to encrypt the vote. The private component of the key pair is used in the Vote Counting Application to decrypt the vote. It is of utmost importance that the use of private key is possible only for counting the votes in the VCA (at 19.00 on election day and, if necessary, during recount). When the period for filing complaints has expired, the private key will be destroyed.

The privacy and secrecy of an e-voter can be compromised by a simultaneous occurrence of two security hazards: a party appears in the system (or outside the system) who has access to both the private key of the system as well as the digitally signed votes. Even though this data is separated in the system, the risk remains. A one and only private key is probably a lot easier to protect than the digitally signed e-votes – the latter pass through several system components (Voter, VFS, VSS) and data transfer channels, consequently, the danger of leaked e-votes is higher. Thus for ensuring the security the main focus should be on key management.

The private key is subject to two dangers:
* **Compromise or becoming publicly available**. The occurrence of this would enable the parties in possession of digitally signed e-votes to determine who cast a vote in favour of whom, thus compromising the privacy of the voter.
* **Corruption.** The private key carrier may be destroyed, lost or be corrupted because of a technical error. When this occurs it becomes impossible to decrypt the e-votes and all the electronically cast e-votes are lost. This is a critical danger and **therefore two key pairs should be used simultaneously in the system**.

The key pair is generated in a Hardware Security Module (HSM) in such a way that the private component never leaves the module. The generation of the key pair and use of private key is maintained by **key managers,** there should be several of them. A scheme "N out of M" is recommended, for National Electoral Committee four members out of seven should be present in order to perform security critical operations. Key managers have physical (for example a keycard) as well as knowledge-based (PIN-code) authentication devices for communicating with the HSM.

The procedures of key management, meaning the generation of the key pair and PINs, delivery of the public component to the vendor of client application, preservation of the private component, its backup and delivery to the VCA must be subject to audit supervision and should be described in a separate document.

6.2. Voting and Vote Storing

Voting takes place during advance polls from Monday to Wednesday of the election week. When the advance polls close, the Central System ends communication with the outside world.

Voting is conducted as a transaction between voter and the VFS. The VFS performs queries from local databases of voter and candidate lists and finally sends the vote to the VSS. The architecture of this stage is depicted in the following figure:

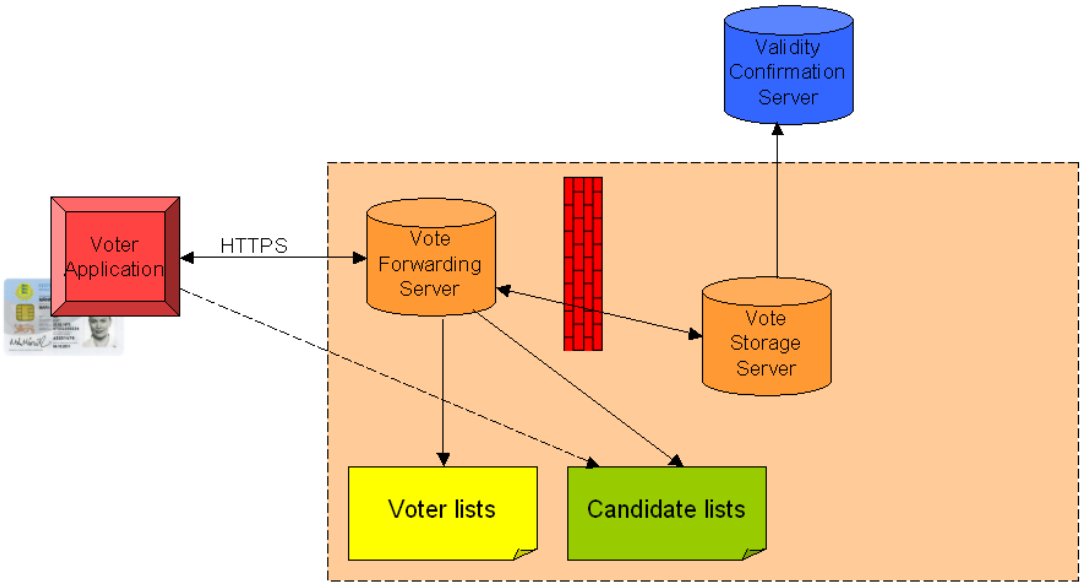

Fig.4 Components participating in the voting process

The voter application functions in the WWW-environment. In addition to HTML-pages, a signed ActiveX applet is loaded into voter's browser that allows to encrypt the vote and digitally sign the resulting cryptogram. In addition to this the voter application possesses information about the candidate list and before encrypting the voter's choice and digital signing asks voter to confirm his/her choice.

The VFS is essentially a web server with its application. The VFS is the only component of the Central System that is directly accessible from the Internet – all the other Central System components are behind an inner firewall and access to them is provided only from the VFS.

During the e-voting period the voter list database is dynamic. During the e-voting period the voter list maintainer (The Population Register) sends operative updates to the database using a specified protocol, after the e-voting is closed status of e-voters list is finalized.

In comparison with the general architecture we now also have a validity confirmation server which is not part of the Central System. It is operated by *AS Sertifitseerimiskeskus* as a standard service and is available via OCSP (*Online Certificate Status Protocol*). A validity confirmation is needed to prove the validity of ID-card certificates without which the digital signature is invalid.

The voting process takes place as follows:

1. The voter accesses via HTTPS-protocol the VFS and identifies him/herself with the ID-card.
2. The VFS performs a query using voter's personal identification code (PIC) from the voter list database, verifies the eligibility of the voter and identifies his or her constituency. If the voter is not eligible, a corresponding message is delivered and he/she is directed to the X-tee service provided by the Population Register where he/she can check his/her eligibility status.

3. The VFS performs a query from the VSS whether such voter has already voted. If this is the case, the voter is informed about it.
4. The VFS makes a query using the constituency data from the candidate list database and as a result receives the list of candidates in that constituency. The list is displayed to the voter.
5. The voter selects a candidate.
6. The voter application, having the candidate list, asks the user to confirm his/her choice.
7. The application encrypts the choice and a random number with the public key of the VCA. The voter signs the cryptogram (hereinafter: *vote*) with his or her digital signature.
8. The voter application transmits its digitally signed envelope to the Vote Forwarding Server which verifies the formal correctness of the received material and whether the same person who authenticated him/herself during the start of the session gave the digital signature.
9. The VFS forwards the received vote to the Vote Storage Server (VSS). The VSS accesses the validity confirmation server and acquires a certificate confirming the validity of the digital signature which is then added to the signed vote.
10. In case of successful vote the VSS sends the VFS a confirmation that the vote has been received. A corresponding message is delivered to the voter as well. An entry about receiving of the vote is recorded in the log-file (LOG1), using the format [*PIC, hash(vote)*].
11. The voter may vote several times. All the votes are transmitted through the VFS to the VSS.
12. After the end of e-voting the VFS ends all communication.
If the validity confirmation server is unavailable at the moment of voting, the time of receiving the vote is stored. The validity confirmation service allows to verify the validity of certificate at a later stage. The time on system servers and validity confirmation server must be synchronized. All validity confirmations must be received before the beginning of the next stage.

6.3. Vote Cancellation and Sorting

The Vote Storage Server (VSS) application is a central component in the vote cancellation and storing stage. The result of this process are *votes* (encrypted candidate numbers, from which the digital signature is removed) and a list of voters who voted electronically. The procedure is illustrated by the following figure:

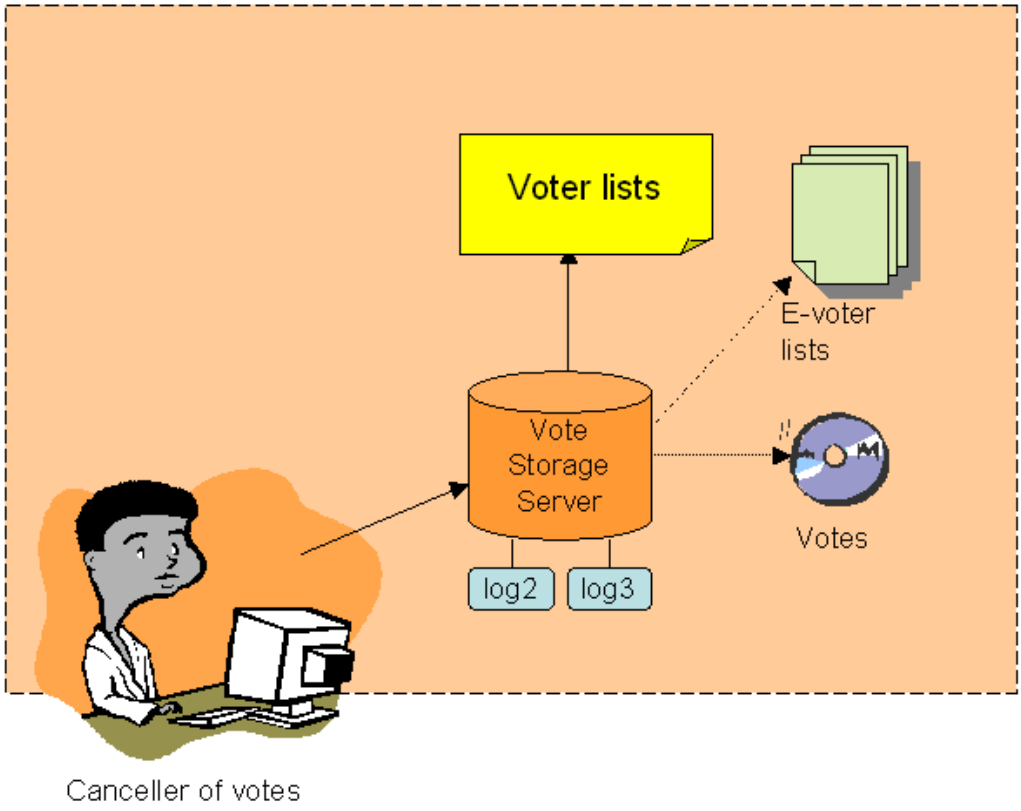

Fig. 5. Sorting and cancellation

After the end of advance polls double votes are cancelled immediately. Only the last vote cast by the voter is taken into account. The time the vote is cast is checked against the time of the validity confirmation of the digital signature.

Every cancelled vote is recorded in the log LOG2, using the following format:
PIC, hash(vote), reason
Where the reason could be:
a) multiple vote, reference to the vote counted,
b) participation in advance polls, reference to the cancellation appeal,
c) re-vote on election day, reference to the cancellation appeal.

After cancelling double votes the lists of e-voters (name, personal identification number, number of the line in the polling division's voter list) by polling divisions are compiled and sent to polling stations simultaneously with the advance polls envelopes. The integrity, authenticity and proof of delivery of this information is critical – or else it is possible for a person to cast two votes (e-vote and a traditional vote). While we cannot rely on the existence of computers at all polling divisions, we shall consider here the processing of paper documents.
The next stage that ends on Election Day at 20.00 is the e-vote cancellation stage.

The polling divisions begin preparing the appeals for cancelling of e-votes. First, the people who have cast an e-vote and voted in advance as well are marked in the appeals. This should be finished by the election day at the latest.

The next set of cancellations takes place on election day. E-voters may, should they choose to, re-vote at polling stations until 17.00. After that the polling stations will end submitting entries into the cancellation appeals, sign it as a document and send it to the county election committee (the information may move through other channels, however, it is important that a signed document be created that would serve a basis for cancellation of e-votes).

All the cancellation appeals from the polling divisions should arrive at the county election committee by 18.00 at the latest (even when there are no cancellations, relevant information and document must be created!). Next the county election committee compiles an electronic list from the data of all its polling divisions, signs it digitally (there should be at least two persons in the committee who are able to sign digitally) and sends it to the NEC by 19.00 at the latest.

The NEC again prepares a consolidated list of the lists received, signs it digitally (again, at least two persons are required) and feeds it to the VSS. The latter checks the digital signature, saves the cancellation appeal and executes the cancellations (while recording them into log LOG2). The persons authorized by the NEC to cancel votes are entitled to submit digitally signed cancellation appeals to the VSS as well as appeals to recall cancellations of a single or multiple votes.

When the cancellation period has ended, the outer envelopes are separated from the inner ones, i.e. digital signatures from the signed content (*votes*). The algorithm itself is as follows:

1. The envelopes are sorted by constituencies. The voters' personal identification codes are taken from the digital signatures and by using these to perform queries from the voter list database the corresponding constituency can be determined.
2. The outer envelopes are opened, i.e. the digital signatures are removed and the cryptograms encrypted with the public key of the VCA (meaning *votes*) remain.
3. Digital signatures are stored separately without the content. We call it the e-voter list (in case it is necessary to save it) – it is in fact sufficient to store a list of personal identification codes and constituencies/polling divisions.
4. *Votes* are prepared for transfer to the VCA on an external storage medium (CD for example). During the transfer process the integrity of the bulk of *votes* must be preserved in an accountable manner.

All the entries sent to the VCA are recorded in logfile LOG3 using the format *PIC, hash(vote)*.

6.4. Counting of votes

The counting of votes takes place in the Vote Counting Application (VCA), separated from the network. At the same time the VCA must be able to use a local database with candidate lists.

It is required that the vote count procedure be repeatable. This provides insurance in case of hardware failures of the VCA computer, makes it possible to verify the count in another computer, etc.

In order to count votes the system's private key (private keys when several key pairs are used) is activated by key managers according to the established key management procedures.

The vote counting input are the votes brought from the VSS on an external storage medium and sorted according to the constituencies.

The vote counting environment can be visualized by the following figure:

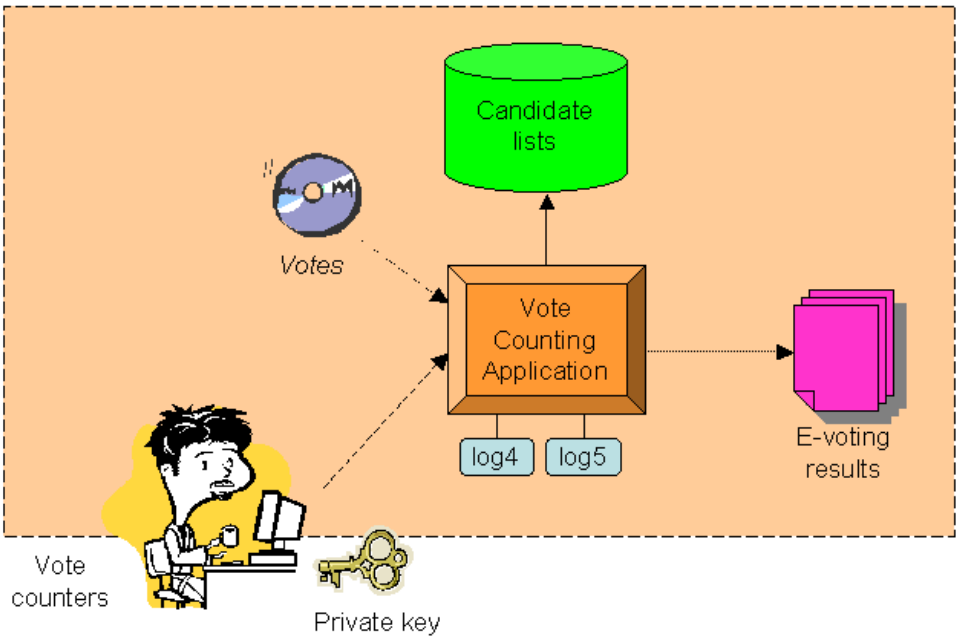

Fig. 6. Counting of votes

The votes are decrypted by constituencies using the private key (keys). The original *vote* is preserved for the time being. The decrypted vote is checked against the candidate list to determine if it is possible to vote for the candidate in that constituency. If the candidate number is incorrect, the vote is declared invalid. A corresponding notice is recorded in log LOG4 in the format *hash(vote)*.

The votes to be taken into account are summed by candidates and constituencies, and recorded in log LOG5 in the format *hash(vote)*.

The results of the e-vote are added to the results of the ordinary voting.

6.5. Audit Application Possibilities

The e-voting system creates several logs during different stages, namely:

LOG1: received votes	*PIC, hash(vote)*
LOG2: cancelled votes	*PIC, hash(vote), reason*
LOG3: votes to be counted	*PIC, hash(vote)*
LOG4: invalid votes (invalid candidate number)	*hash(vote)*

LOG5: accounted votes *hash(vote)*

The reason for producing a hash from the encrypted candidate number and a random number (*vote*) is simple – one cannot deduce the original vote from the hash while the collision-free property of the hash algorithm ensures its uniqueness. To sum it up, for the auditor *hash(vote)* is a unique value so that the votes can be separated from one another but the auditor lacks any means to reconstruct the real value of this vote (even with the help of the system's private key).

The audit application makes it possible to determine what happened with the vote cast with a specific PIC. The possibilities are:
* accepted, recorded in LOG1,
* cancelled because the person attended advance polls – recorded in LOG2,
* cancelled because the person voted on Election Day – recorded in LOG2,
*cancelled because the candidate whose number was on the ballot did not stand as a candidate in the constituency – recorded in LOG3 and additionally the corresponding *hash(vote)* is recorded in LOG4,
* the vote was counted: recorded in LOG3 and a corresponding *hash(vote)* in LOG5.

The audit application is mostly used in reviewing complaints. In principle, however, it is also possible to offer the e-voter a web application where after authenticating him/herself with the ID-card he/she can be notified of the status of his/her vote (votes) cast.

In addition to this, the audit application possesses the ability to check the integrity of logs – LOG2 and LOG3 combined must equal to the content of LOG1; LOG4 and LOG5 combined must equal to the content of LOG3.

All the log entries must carry creation time information and should be linked to each other cryptographically in order to ensure the integrity and fraud-proofness of logs .

7. On Software Development, Environments and Integration

As a general rule – all the "white boxes" are created as a domestic production. The utilization of software of foreign origin to be used as "black boxes" (operation systems, components, libraries etc) must be designed in a way that the impact of the possible compromise of these components upon the e-voting system's security logic would be minimized.

Specific data exchange protocols and data structures are described in the technical project.

The components' source code is audited, compiled in an independent environment and its functionality is tested. The executable code which has passed audit is signed, the signature is published.

The election application and the corresponding web-environment are only in the Estonian language. It would be very beneficial to provide supporting help information in other languages as well.

In selecting, installing and configuring system components (operation system, web server, supporting libraries), meaning “black boxes”, it is kept in mind that:
* Components that are as stable as possible are chosen (having been used and tested for a considerable time). The components’ identifying information (sources, checksums, etc) are documented.
* The components are to be taken from the original source, **all** changes (deletion of system parts, configuration) are documented.
* A later audit must be able to rebuild a similar system state by relying on downloadable software from the original source and following the changes specified in the documentation.

In choosing and developing environments, the following guidelines are followed:
* It must be presumed that the voter’s environment is a home or office PC the operation system and setup of which the voter will not change. Supporting all user platforms is technologically extremely complicated and thus costly.
* When choosing the Central System’s environment one must concentrate on the integrity and security of the base system – influence of any auxiliary programmes that interfere or halve the process must be negated.
* The audit application is relatively Spartan, a set of UNIX command line utilities.

8. Conclusion

The e-voting system described in the document enables, provided that sufficient organisational, physical and technical security measures are implemented, a basis for conducting e-voting at least as securely as traditional voting.

More detailed information can be obtained from the e-voting concept and its security analysis documents.