Electronic Voting Committee

General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia

Document: IVXV-ÜK-0.98
Date: 23 May 2016

Tallinn 2016

Annotation

This paper gives an integrated overview of the technical and organisational aspects of the framework of electronic voting („IVXV“), and the implementation of the framework at the national elections in Estonia. It is meant for the general public and does not require any detailed technical preliminary knowledge from the reader. For more detailed requirements and descriptions, see the technical source documents. This paper gives a general description of the system; implementation of the system in Estonia is discussed in the appropriately marked sections.

Contents

1. Introduction

In this paper, electronic voting (e-voting) denotes the method of voting where the voter gives their vote **from a computer via the Internet**. This method of voting may also be called 'i-voting' in order to make a distinction from other methods of voting using information technology, like the use of electronic voting machines, in the international context.

The i-voting framework described here is universal and can be applied in different types of elections. This paper focuses on the national elections (the Riigikogu elections, the local government councils' elections and the European Parliament elections) and referendums held in Estonia. Therefore, besides the description of the general framework, the circumstances arising from the Acts of Estonia and their implementation acts are explained in the text below.

This paper:

- defines the scope of the i-voting system, that is, delimits the role of i-voting in the whole voting process;
- summarises the requirements for the i-voting system;
- defines the parties of the system and describes their activities;
- describes the principal processes of i-voting;
- gives an overview of the possibilities of checking the correctness of the system and its compliance with the basic requirements.

This paper does not aim to define the specific security level of the system components, data structures, software and hardware platforms used, or the detailed technological structure.

When reading the paper, it should be taken into account that the amount of detail increases gradually so that the issues described generally at the beginning may be explained in more detail further on.

In Estonia
I-voting has been used in Estonia since 2005. Each person who has the right to vote in Estonia can cast their vote in a secure way via the Internet at the elections and referendums, because:

- there is a legal basis for the use of digital signature, and all Acts concerning elections provide for a legal basis for the conducting of i-voting;
- most of the persons who have the right to vote possess an ID card that enables secure electronic identification and giving digital signature; many people also have an additional legally backed electronic ID document, like Digi-ID or Mobile-ID.

2. Scope of the i-voting system

I-voting is a part of the voting process. Elections consist of the following principal stages:

- declaration of elections;
- registration of candidates;
- preparation of lists of voters;
- voting;
- counting of votes;
- announcement of election results.

The i-voting system partially covers only the three last stages, i.e. the voting via the Internet, the counting of votes and, after the announcement of election results, the destruction of the key necessary for counting the i-votes.

Prerequisites for the i-voting system are that:

1) the lists of voters (with the polling division and electoral district linked to the voter) have been prepared and are available in a suitable format;
2) the lists of candidates (by electoral districts) have been prepared and are available in a suitable format;
3) i-votes are counted separately, and the results are later added to the results of the counting of paper votes, keeping in mind that the votes of one person (the electronic vote and the paper vote) are not counted twice.

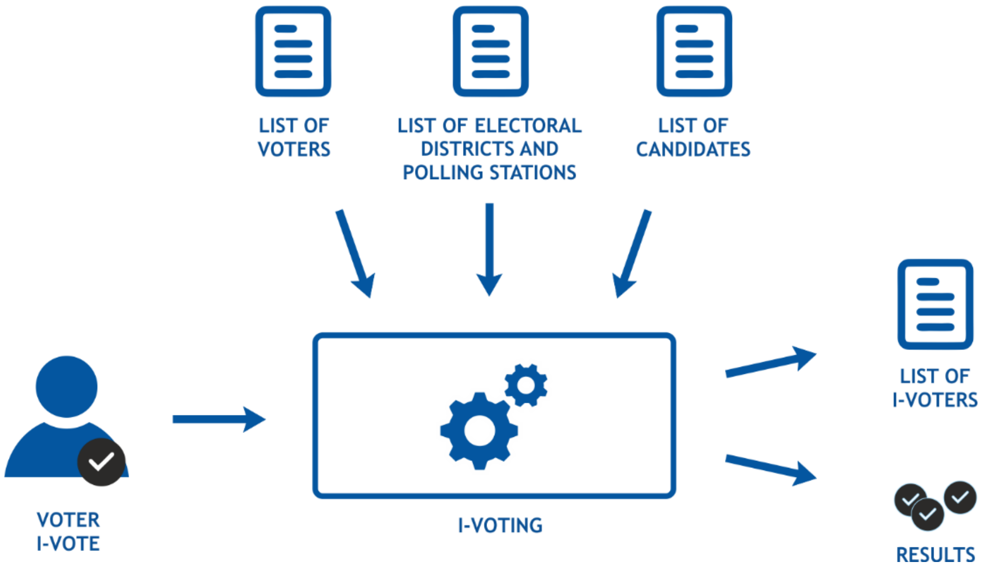

Figure 1. Scope of i-voting

3. Principal requirements for i-voting

I-voting must adhere to all Acts concerning elections and must follow all election principles, and be at least as secure as regular voting. Thus, i-voting has to be uniform and secret, only the persons who have the right to vote may (i-)vote, every person has one vote, and it must be impossible for voters to prove for whom they cast their vote.

The main difference between i-voting and voting with paper ballot is that the voter can vote repeatedly electronically; only the last vote cast is counted. This principle enables to protect i-voters against coercion. A coerced voter can vote again after becoming free from coercer, invalidating the vote cast under pressure.

I-voting takes place before the election day, during the period specified by law. If something unexpected happens to the i-voting system (large-scale attack, serious software error, etc.), the organiser of the election may annul a part or all of the i-votes in extreme cases. In such a case those who i-voted can vote again at the polling station.

If advance voting at polling stations takes place at the same time as i-voting (**parallel voting**), then it may happen that a voter votes in two ways. In that case, only the paper vote is counted, and all i-votes of the voter are annulled. This principle also protects the voters against coercion.

Another important requirement of i-voting is the use of digital signature. The voter has to confirm their choice with a legally accepted **digital signature**. Compliance with the provisions of the Digital Signatures Act ensures the fulfilment of the main security requirement of i-voting – secure personal identification of voters.

The voter must have the possibility to **verify** whether their i-vote has arrived safely. This can be done with the help of a separate smart device (mobile phone, tablet). A device different from the computer used for i-voting should be used for checking the arrival of i-vote. In this way it is possible to increase the probability of detection of attacks (primarily against the voter’s computer) directed against the i-voting system.

When building up an i-voting system, its *auditability* must additionally be taken into account – the system must be technically sufficiently simple so that a widest possible range of specialists could audit it.

In Estonia

In Estonia, i-voting takes place during seven days, and it starts ten days before the election day. Parallel voting is used. Identity document (ID card), Mobile-ID, and digital identity document (Digi-ID) can be used as tools for giving digital signature. Starting from 2015, the organiser of the election is required to provide the voter with the possibility to check the integrity of the recorded vote.

4. Envelope Scheme

I-voting system is based on so-called “envelope scheme”, which is known from voting by paper mail, where an anonymous closed envelope with the vote is placed into an outer envelope with the voter’s name and signature. With the help of the programme used for i-voting (so-called *Voter Application*), the i-voter:

1) encrypts the vote and the random number generated by the computer with the elections-specific public key, forming the “inner envelope”;

2) signs the encrypted vote by using a digital signature tool, forming the “outer envelope”.

A vote encrypted with the public key can be decrypted only with the private key.

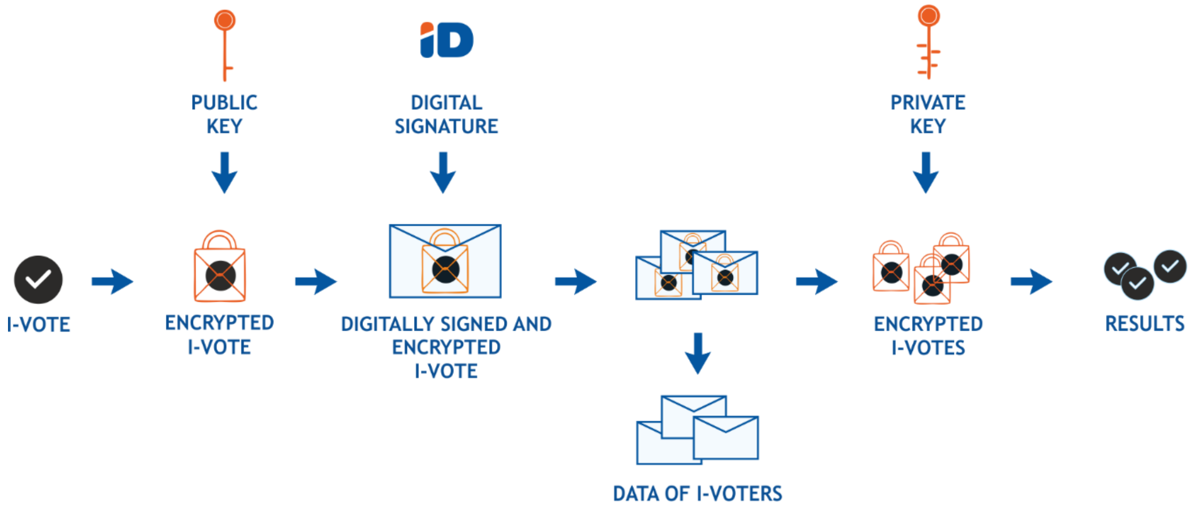

Figure 2. Envelope Scheme

Encrypted and signed votes are collected and sorted, the eligibility of voters is checked, and repeated i-votes and the i-votes of the persons who also voted at a polling station during advance voting are removed.

Before the counting of i-votes they are sorted by electoral districts, the list of i-voters is compiled, and then the digital signatures are removed.

During the counting of votes, anonymous and mixed votes are decrypted with the elections-specific private key, and the summarised results of i-voting are issued.

5. Stages of i-voting

Organisationally, i-voting can be divided into four stages.

1. During the **pre-voting stage**, the system is set ready for use, which includes the following:

    - lists of electoral districts, polling stations, candidates and voters are prepared;
    - public and private keys for votes are created for each voting;
    - the voter application, the individual verification application, and relevant instruction materials are published. Data necessary for verifying their authenticity and integrity are published in a separate information channel.

2. During the **voting stage**, i-voting takes place. In case of parallel voting, it is also possible to vote at polling stations.

3. During the **processing stage**:

    - the integrity and authenticity (digital signature) of i-votes is checked, and whether all i-votes that have been cast still exist is checked;
    - the votes are sorted, and the repeated i-votes of one and the same person are annulled;
    - in case of parallel voting, the lists of i-voters are drawn up for each polling station. Polling station committees identify the voters who have voted both electronically and at the polling station, and prepare lists of them for annulling their i-votes;
    - the i-votes of persons who cast double votes are annulled, and the votes that go to counting are anonymised.

4. In the counting stage, the anonymised votes are opened with the private key and added up to ascertain the voting result.

In Estonia

In Estonia, i-voting is opened ten days before the election day, on Thursday at 9 a.m., and closed four days before the election day, that is, on Wednesday of the election day week at 6 p.m. It is possible to vote round the clock via the website www.valimised.ee. Possible changes in the list of voters are entered in the i-voting system at least once every twenty four hours according to the data received from the Population Register.

Parallel voting takes place, the list of i-voters is sent to the polling station committees via the county electoral committees; the i-votes of the persons who cast double votes are annulled just before the counting of i-votes.

The results of i-voting must not be published before the time provided for by law.

6. Parties and components of the system

The most important role in i-voting belongs to the **Organiser** who appoints the persons for all other roles. Generally, the Organiser also holds the fundamental secret of the i-voting system, i.e. the private key, and thus performs also the role of the opener and adder-up of the votes, that is, the role of the **Tallier**.

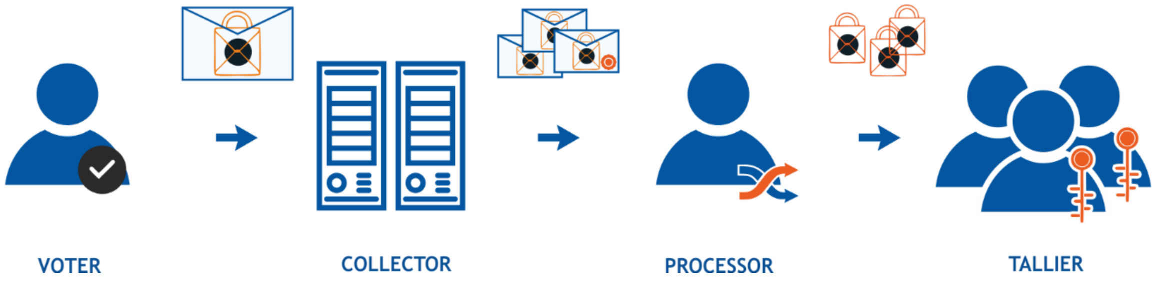

Figure 3. The principal parties of the i-voting system

The principal parties of the system and their actions are the following.

- The **Voter** makes their choice with the help of the Voter Application in the computer, encrypts it, signs it digitally and sends their choice to the Collector. The Voter can check if his choice arrived intact with the help of a separate smart device.
- The **Collector** is a server system that helps the Voter to form the i-vote (issues the list of candidates to the Voter, helps with digital signature) and accepts i-votes. The Collector also answers verification queries on the integrity of the vote, made by the Voter. The provider of collection service digitally signs the data (i-votes and logs) handed over to the Processor at the end of the voting period.
- The **Processor** processes the i-votes collected during the voting period, and among other things:
    - verifies the digital signatures and the integrity of the data received from the Collector;
    - annuls repeated i-votes and, in the case of parallel voting, also the i-votes of those who voted at a polling station during advance voting;
    - sorts the i-votes by electoral districts and anonymises them by removing personal digital signatures from them;
    - mixes anonymised votes in an appropriate way and sends them to counting. This can also be regarded as a sub-role; in such a case, the performer of the role is called the **Mixer**.
- The role of the **Tallier** is performed by the Organiser, who holds the private key. The Tallier opens the anonymised and mixed votes and adds them up as the results of i-voting.

In addition to the principal parties, the system has the following parties.

- The **Auditor** checks the integrity and completeness of the data published by the Organiser of the system, as well as the data moving between the principal parties.
- The **Client Desk** is the party whom the Voter contacts in case of problems. The Client Desk helps the Voter with the information received from the Collection Service, and registers all the received questions and their solutions in its database.

- The **compiler and updater of the list of voters** compiles the lists of persons with the right to vote depending on how the elections are organised. The list may change during the voting period.

Important external services are the following.

- The **Identification Service** is used to identify the Voter, if necessary.
- The **Signature Service** depends on the signature tool. It helps the Voter in the signing and the obtaining of the validity confirmation for a digital signature.
- With the help of the **Registration Service**, the Collector registers all the votes received from the Voters. After the end of the voting period, the service provider forwards all the registrations to the Processor.

To fulfil these roles, tools are needed that the performers of the roles use in their procedures. The software components of the system are defined in what follows.

- The **Voter Application** runs in the computer of the Voter, communicates with the Collector, and allows the Voter to make their choice, to encrypt it, and to sign it digitally. The Voter Application displays a QR code on the basis of which the Voter can check with the Verification Application whether his i-vote has reached the Collector correctly.
- The **Verification Application** allows the Voter to check on a smart device platform that his i-vote has reached the Collector and has expressed his wish correctly. The device used for checking is different from the device used for voting.
- The **Key Application** is the main tool of the Organiser. It is used to generate a public and a private key for every voting. The Key Application is also used to count the votes and issue the results.
- The **Collection Service** is the central component of the system, operated by the Collector. The Service assists the Voter in composing an i-vote, and registers it before saving it into the i-ballot box. The Collection Service uses external services (identification, signing, registration). The Collection Service has other administrators besides the Collector itself (Organiser, Client Desk), and the Collection Service has separate administration interfaces for them.
- The **Processing Application** is the main tool of the Processor. It is used to check the individual integrity of votes and the integrity of the i-ballot box, to annul votes, to compile lists of persons who voted and lists of anonymised votes grouped by electoral districts. The Collector, the Registration Service and the Organiser provide the input for the Processing Application. The Processing Application can also be operated by the Auditor to check the results of the work of the Processor.
- The **Mixing Application** is a tool for the Processor or the Mixer. Its input consists in the anonymised encrypted votes grouped by electoral districts, and it issues the mixed votes in such a way that they cannot be linked back to the input. Mixing must be carried out in such a manner that the decrypting and tallying of both input and output votes give the same result. In addition, the Mixing Application issues a *mix-proof*.
- The **Audit Application** is a tool for the Auditor. It allows to check the correctness of the work of the Counter and the Mixer. The correctness of the work of the Counter can also be checked publicly.

7. Main Processes

This chapter describes the actions of the parties of the system, explaining the general functionality of the system components and the general requirements for the external parties of the system.

7.1. Key management

The key management procedures and the security scheme used are among the most crucial parts of the i-voting system. They are instrumental for the fulfilment of the main requirements of the elections – the secrecy and correctness of voting, and the independence of the Voter.

Secrecy is guaranteed by encrypting the votes with asymmetric cryptography tools. For every voting, the key pair of the system – a public key (encryption key) and a private key (decryption key) is created with the help of the Key Application.

The Voter Application uses the public key of the votes to encrypt votes. The private key is used in the Key Application to decrypt votes. After the voting results have been announced, the private key is exterminated.

The generation of the key pair and the use of the private key are organised by several *keyholders* together. The number and list of keyholders is determined under the established rules. The private key can only be activated if the previously agreed number of keyholders are present. Keyholders receive physical and knowledge-based **keyshares** (e.g. chip card and password) to activate the private key.

Actions of key management, including the generation of the key pair and the passwords, the keeping and duplicating of the private key, and its use in the Key Application are audited by the Auditor.

7.2. Voter identification

Identification of the Voter by the Collector is necessary for the preliminary check of the right to vote, as well as for obtaining the list of the candidates of the electoral district. A Voter can be identified by asking them to submit their personal identification code; however, it is more expedient[1] to request identification by an authentication tool.

The Collector supports a variety of authentication methods that the Voter can choose from depending on the authentication credentials at his disposal. These credentials can be simply knowledge-based (user name/password, PIN); however, stronger identification security is ensured by a physical authentication token (e.g. chip card, SIM-card, etc.) combined with a knowledge-based PIN.

Depending on the authentication method used at the elections, it might be pertinent to involve the external Identification Service which either confirms the validity of the authentication tool used (Validity Service) or asks the Voter for an authentication credentials. The Voter Application and the Collection Service serve as mediators between the Voter and the Identification Service in a suitable manner. As a result of the process, the Collection Service learns the identity of the Voter.

Admissible authentication credentials and the corresponding Identification Services are determined by the Organiser.

[1] An electronic authentication tool is usually linked to a signature tool in the same data carrier (ID card). In such a case, it is expedient to use the same data carrier for both purposes.

7.3. Signing of votes

The Voter signs the encrypted vote to ensure its authenticity and integrity. The personal identity proven by the digital signature is the basis for taking the i-vote into account. This means that the identity determined in the identification of the Voter is not taken into account during the further handling of the digitally signed vote.

To give a digital signature, the Voter uses a signature tool which is a combination of the physical (e.g. chip card, SIM card) and the knowledge-based (PIN) parts.

The creation of a digital signature consists of the following:

- creating of a cryptographic signature with the private key contained in the signature tool of the Voter – the Voter uses a relevant PIN-code for that. The Voter Application checks the integrity of the signature created;
- obtaining a validity confirmation that proves the validity of the certificate corresponding to the private key used in creating the signature. The query for and reply to validity confirmation can also include the message digest of the signature created.

The manner in which the Voter Application and the Collection Service use the Signature Service depends on the signature tool used. One part of the Signature Service – validity confirmation service – must always be used.

As a result of the process, the Collection Service forms a digital signature containing the Voter's signature, his certificate, and the validity confirmation of the signature.

The signature tools used and the corresponding Signature Services are determined by the Organiser on the basis of the legislation concerning digital signature.

7.4. Registration of votes

All the i-votes sent to the Collector must be registered. The Registration Service is an independent party that registers and confirms every encrypted vote (message digest of thereof) forwarded by the Collection Service, and produces a *time-mark* by adding time value to it.

The Registration Service securely identifies all the queries by the Collector. After the end of the voting, the Registration Service hands all the time-marks over to the Processor.

The Registration Service can be combined with a validity confirmation service used to create a digital signature.

The Organiser chooses the provider of the Registration Service, keeping in mind that the Service must meet the requirements for the provision of trust services within the meaning of Chapter 3 of eIDAS[2].

7.5. Voting and vote verification

A Voter uses the Voter Application installed on their computer for voting. The Application communicates with the Collection Service. The Collection Service makes use of the list of voters, the list of candidates, and the list of electoral districts and polling stations. The Collection Service

[2] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014R0910

may use the Identification Service to identify the Voter; the Collection Service assists the Voter in digitally signing the encrypted vote by using an external Signature Service. The Collection Service registers the digitally signed vote at the Registration Service. The Voter Application notifies the Voter of the successful recording of the vote by issuing a relevant QR code.

To check the vote, the Voter uses the Verification Application downloaded to his smart device. This application also communicates with the Collection Service. The Verification Application receives data necessary for its work from the Voter Application by reading the QR code with the help of the camera of the smart device. The Verification Application notifies the Voter of his choice recorded in the Collection Service.

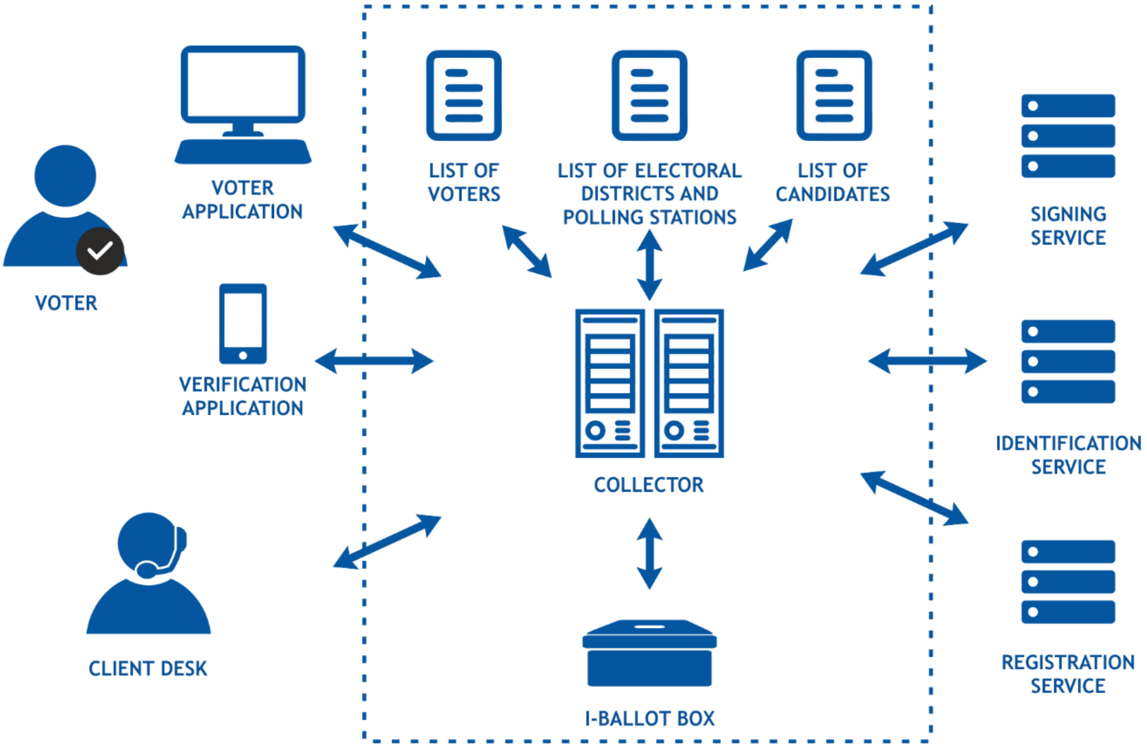

Figure 4. Voting services and components

The Voter downloads the Voter Application from the web page managed by the Organiser. The Verification Application can be installed on a smart device via the relevant application store, and the installation instructions are also available on the web page. The authenticity and integrity of the web page as well as the Voter Application and the Individual Verification Application can be checked with the help of the data that the Organiser has securely published.

Voting takes place in two stages: the identification and the voting stage.

In the **identification stage**, the Voter is identified, and voting options are sent to the Voter. The following actions take place in this stage.

1. The Voter chooses a convenient authentication tool.
2. The Voter Application contacts the Collection Service using a secure data communication protocol. The Voter is identified with the help of the authentication tool chosen. The Collection Service uses the Identification Service if needed.
3. The Collection Service checks whether the Voter has already i-voted. If the answer is positive, the Voter is notified, and he may nevertheless continue and cast a new vote replacing the prior one.

4. The Collection Service identifies eligibility of the Voter as well as his electoral district. If the Voter does not have the right to vote, an error message is displayed.
5. List of candidates standing in the electoral district of the Voter (or choices for the referendum question) is sent by the Collection Service to the Voter Application.

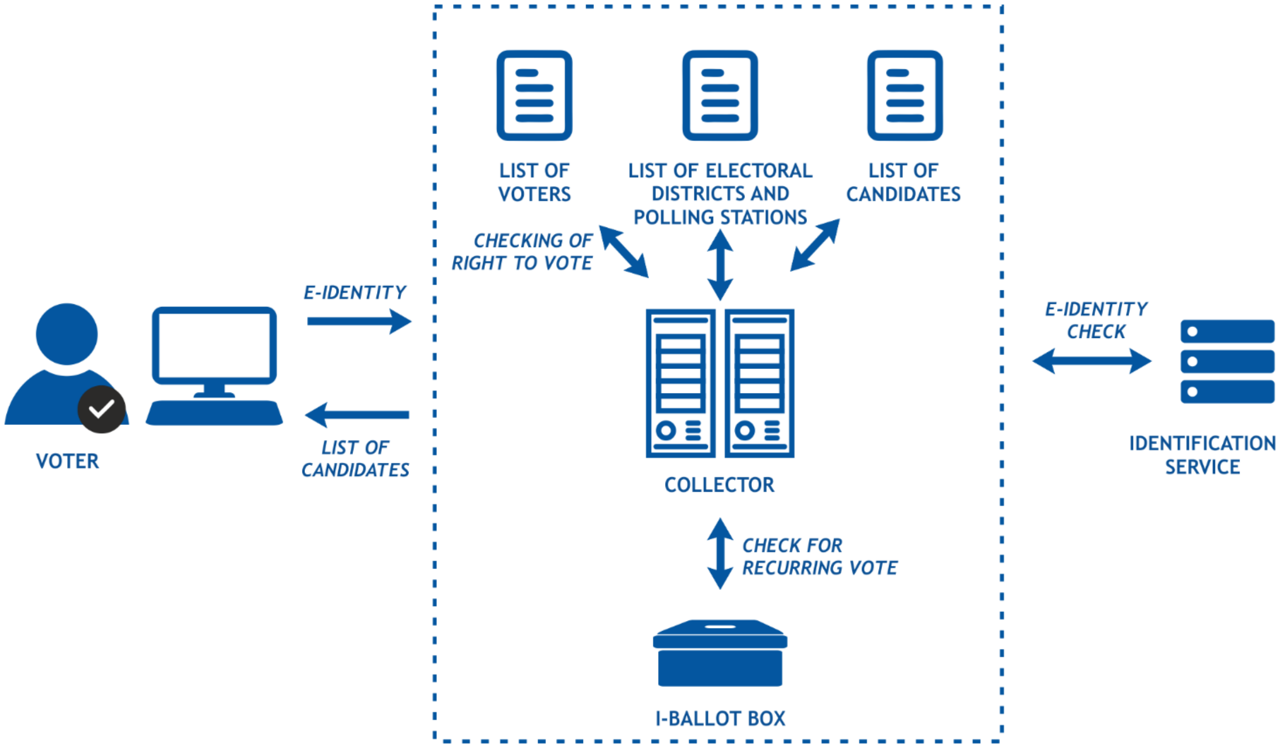

Figure 5. Identification of the Voter

The identification stage is followed by the voting stage, unless the Voter interrupts the voting. The voting stage proceeds as follows.

1. The Voter makes their choice among the candidates displayed. The Voter Application encrypts voter's choice along with a *random number* with the help of the public key.
2. The Voter signs his encrypted vote according to section 7.3 and sends it to the Collection Service along with his certificate. The Collection Service checks for existence of the Voter in the list of voters, and appends the vote with a validity confirmation.
3. The encrypted and signed vote must be registered. For that, the Collection Service uses a separate Registration Service or reuses the time-mark within the validity confirmation if applicable.
4. The Collection Service notifies the Voter via the Voter Application that his vote has been successfully received and recorded. A QR code is issued to the Voter, that includes the *random number* used in the encryption, as well as the one-off *vote identifier* generated by the Collection Service in the registration of the vote.

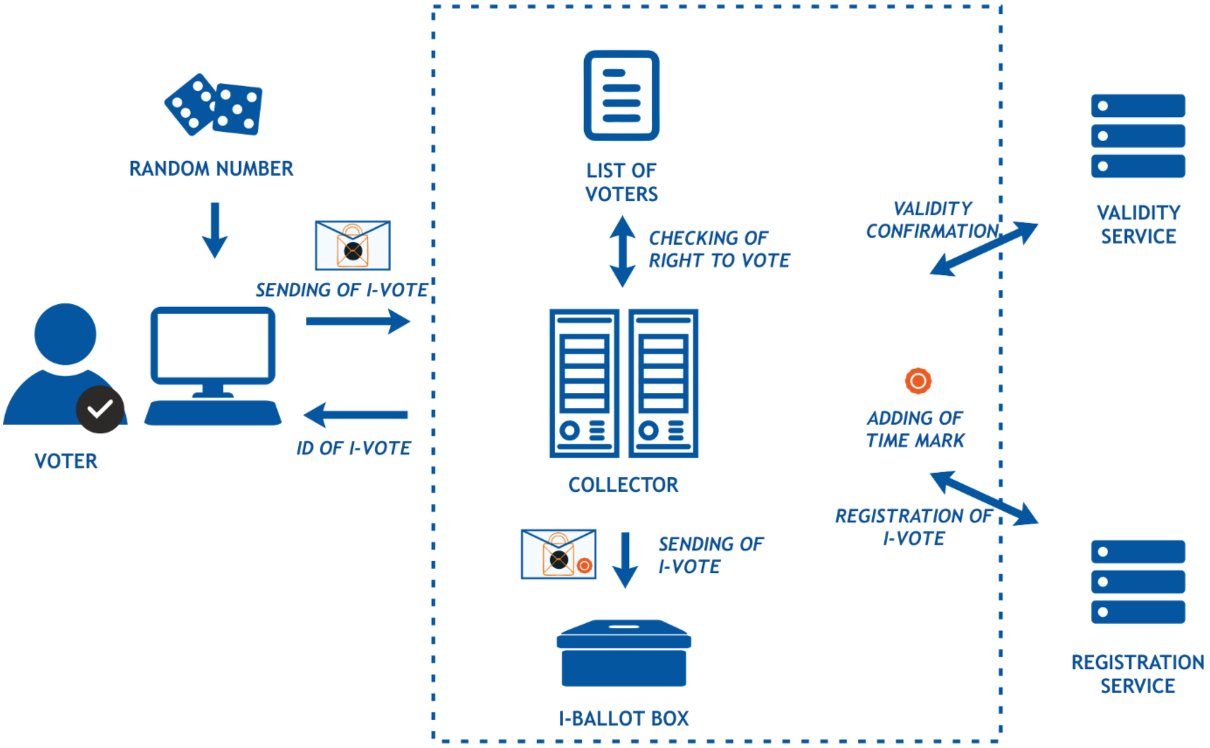

Figure 6. Voting stage: dispatching the vote

In the **verification phase**, the Voter can make sure that his vote has integrally arrived the i-ballot box of the Collector, by using a separate smart device. The smart device must have a camera and Internet connection, and the Verification Application must be installed into it configured with parameters and trust anchors necessary to carry out the verification.

The arrival of the vote is checked as follows.

1. The Voter starts the Verification Application and scans the QR-code displayed by the Voter Application.
2. The Individual Verification Application makes a query concerning the i-vote from the Collecting Service by using the *vote identifier* contained in the QR-code to identify the vote. The Collection Service returns the i-vote Together with the i-vote, the Collecting Service sends the list of candidates options to the Voter.
3. The Verification Application checks the authenticity of the Collection Service, the digital signature of the vote, and the time-mark therein received upon registration.
4. Knowing the *random number* used in the encryption of the vote, and the public key, the Verification Application calculates a cryptogram for every candidate.
5. The Verification Application displays the number and/or the name of the candidate whose calculated cryptogram corresponds to the cryptogram contained in the i-vote.

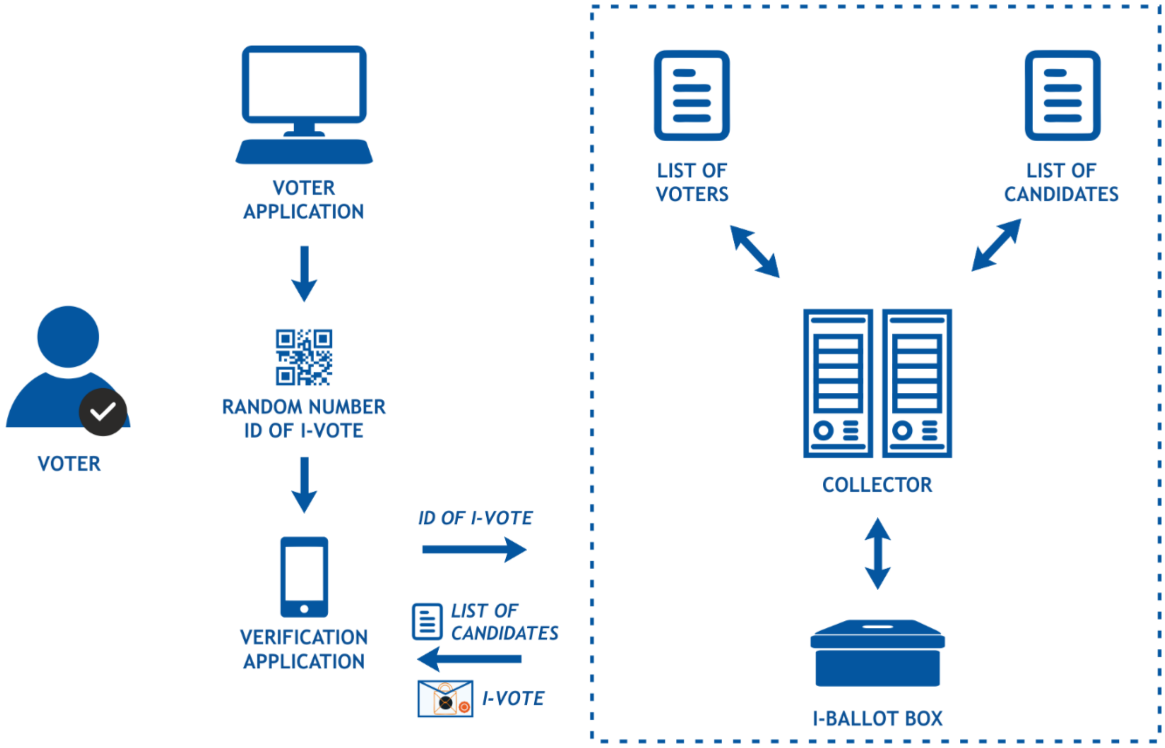

Figure 7. Vote verification

The arrival of the vote can be checked for a certain number of times for a limited period. Limits are established by the Organiser.

After the end of the voting period, the Collector gathers the votes collected in the i-ballot box into a set, and signs them digitally. The signed set of votes is forwarded to the Processor. The technical logs created in the voting process are given to the Organiser who may use the help of the Auditor to check them.

The provider of the Registration Service gives to the Processor all time-marks, attaching a digital signature to them.

7.6. Processing of votes

The processing of votes takes place after the end of the voting period and before the counting of votes. Stages of processing are performed by the Processor. Final stage – mixing – may also be performed by a separate party: the Mixer. The Processor signs the results of all stages. The processing of votes is carried out in an off-line environment.

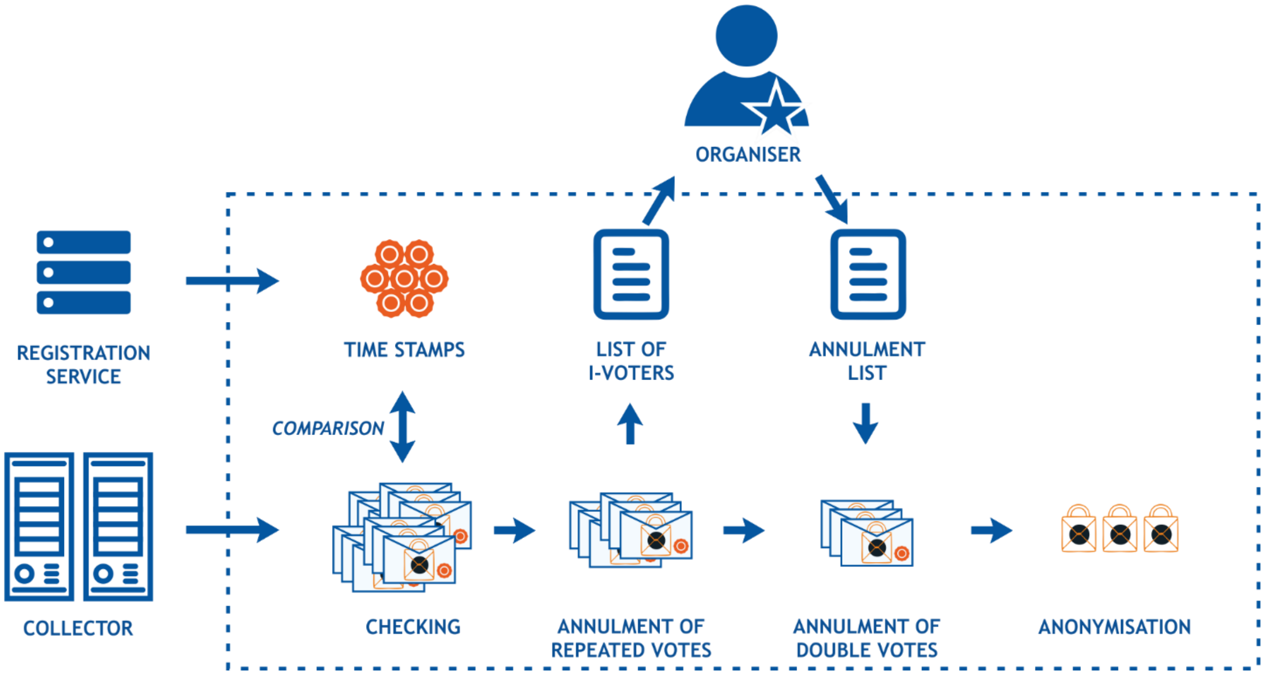

Figure 8. Stages of vote processing

The stages of processing are the following.

I stage: checking of the integrity of the i-ballot box

1. The Processor checks the digital signature of every individual vote, and the existence of the time-mark therein in the information received from the Registration Service.
2. The Processor checks the existence of all time-marks received from the Registration Service in the set of votes.

The result of the stage is the votes of the i-ballot box for which matches are found in the data set received from the Registration Service. At the end of this stage, digital signatures may be removed from the votes, integrally preserving the connection between the encrypted vote, the person who cast it, and the time of casting the vote.

II stage: annulment of recurring i-votes

Recurring votes cast by the voter are removed, preserving only one, the last i-vote. At the end of the stage, the time of giving the vote may be removed, preserving the connection between the encrypted vote and the person who cast it.

In the event of parallel voting, a list of persons who have i-voted, sorted by polling stations, is drawn up by the end of the stage, and it is sent to polling stations for identification of double voting (i-vote and paper vote). On the basis of the double votes identified, an *annulment list* is drawn up of persons whose i-vote is to be annulled. The Organiser signs the list.

III stage: annulment of the i-votes of persons who cast double votes (only in the event of parallel voting)

I-votes are removed from Voters whose name appears on the *annulment list*.

Unique personalised i-votes remain. Before they are counted, they must be anonymised, preserving the connection between the vote and the electoral district.

IV stage: anonymisation of i-votes

1. The Processor groups i-votes by electoral districts.

2. The Processor removes personal data from i-votes.

The result of the stage is anonymous i-votes grouped by electoral districts (encrypted votes).

In order for the counting of votes to be publicly verifiable, cryptographic mixing can be used.

V stage (optional): mixing

The Processor (or the Mixer authorised therefor) mixes anonymous i-votes grouped by electoral districts, using the Mixing Application. Mixing consists of random shuffling and cryptographic re-encryption of votes. A precondition for using the latter technique is the use of a homomorphic cryptosystem in the encrypting of votes. Mixing must be carried out so that the decryption of both the input and the output would give the same result. As a side-result of the process, a mix-proof is issued which can be used, with the help of the Audit Application, to prove the correctness of the process.

Both mixed and unmixed votes may be sent to counting. If the Organiser wishes to prove the correctness of the use of the private key in his or her possession in the counting process, it is necessary to also go through the mixing stage.

7.7. Counting of votes

Votes are opened and counted with the help of the Key Application in an off-line environment. Counting is organised by the Tallier together with the keyholders between whom the private key has been distributed.

1. Both the list of candidates and the list of electoral districts are loaded into the Key Application.
2. Anonymised (and mixed) votes are loaded into the Key Application.
3. To activate the private key, the keyholders use the keyshares distributed to them in the course of the generation of the key pair.
4. Votes are decrypted. If, as a result of the decryption of the votes, it appears that the candidate is not listed among the candidates standing as candidates in the relevant electoral district, the vote is deemed invalid.
5. Eligible votes are summed by candidates and electoral districts. The counting process also issues a zero-knowledge *tally-proof*[3], which can be used to prove the correctness of the opening of votes.
6. At the end of the process, the private key is deactivated.

The Auditor monitors the process. The tally-proof allows to verify the mathematical correctness of the process with the help of the Audit Application. If the votes that went to counting were mixed, the correctness of the counting can also be verified publicly.

The Tallier signs the results of the counting digitally.

[3] To produce a proof, a specific homomorphic cryptosystem shall be used in the encrypting of votes.

8. Security and auditing

The i-voting system described in this document ensures full compliance with the basic requirements for elections and, in addition, is **end-to end verifiable**: the input and output of all processes can be verified mathematically.

Upon application, the security of the system depends on the usage environment, the quality of the information technology system, the correctness of following procedures, etc.

8.1. Cryptographic security

In terms of cryptography, the i-voting system is exceptional as the majority of the security characteristics of the votes collected in a voting must be preserved only until final election results are announced, which generally is 30 days after the election day. Thereafter the private key is exterminated, and the personalised and encrypted votes become unusable.

At the same time, a theoretical risk remains that someone is able to copy personalised i-votes from the system and attempts to guess the private key over time, by using remarkable computer resources over a long period of time.

When choosing the crypto algorithm for encryption of votes and the length of the key, the Organiser must take account of the abovementioned risk, and must rely on up-to-date studies on the security of crypto algorithms.

When choosing the digital signature methods and tools, reliance on everyday practice is sufficient, keeping in mind that the signature tools should be in use also in other important spheres of life.

8.2. Compliance with basic requirements

The **secrecy of voting** is ensured with encryption of the vote by the Voter. An asymmetric crypto algorithm is used, so that votes encrypted with the public key cannot be decrypted with the same key. Adding a random number to the vote is directly necessary to ensure the secrecy of the votes, in order that the cryptograms of the votes cast for the same candidate were different.

For decryption, the private key is needed, but it cannot be used before the process of counting of votes. The Tallier decrypts only anonymous votes, from which personal data have been removed. To activate the private key, cooperation of several keyholders is needed.

The system described supports repeated voting, i.e. the Voter can vote repeatedly, and only the last cast vote is taken into account. Thus the time of the last cast vote represents certain voting secret. For example, in the event of malevolent influencing of a voter or an attempt to buy a vote, the persons who know the time of the last voting of the Voter would have the possibility to check if such vote was taken into account in the counting. Therefore, the circle of persons who have contact with the personalised votes (Collector, Processor, Auditor, Registration Service, Signature Service) must be contained.

The **correctness of voting** (taking into account the right to vote, “one person – one vote” principle) is ensured by personal identification of the Voter with the help of a secure and widely used signing tool.

The **independence of the Voter** (safeguarding the free will) is ensured with the possibility of repeated voting, i.e., a person who has voted under pressure can vote again after becoming free of the pressure, by invalidating the earlier votes cast under pressure. In addition, the Voter can vote at a polling station during advance voting, as a result of which all i-votes cast by the Voter are annulled.

8.3. Verifiability

I-voting consists of several basic processes which are described in Chapter 7. The processes can be verified by mathematically checking the concordance between the input and output of the process. Depending on the party who carries out verification, verification is:

a) individual – checking is carried out by the Voter,

b) delegated – checking is carried out by the Auditor,

c) public/universal – checking can be carried out by all who are interested.

The Voter can individually verify the arrival of his or her personal vote in the i-ballot box of the Collector, and the registration of the vote at the Registration Service.

The Auditor can, by repeating the processes, verify all the processes of the Processor and the Counter, with the exception of mixing and counting. For the latter, the Auditor uses the special proof issued by these processes, and the Audit Application.

If the anonymised votes were additionally mixed before counting, it is possible to also disclose the cryptograms that went to counting, and it is possible to verify the work of the Tallier in a public manner by using the relevant auxiliary tools and data.

8.4. Auditing and observation

The Auditor is the party appointed by the Organiser who carries out process and data audits to check the integrity of the system. On the same bases with the Auditor, observers can also carry out similar checking procedures on a voluntary basis.

The Auditor and observers handle personalised encrypted votes, one component of which is the time of casting the vote. It is possible for them to track the fact and time of voting by the Voter. These data may not be copied or used for other purposes than audit in an environment controlled by the Organiser.

Process audits are applied to acts that are connected with the private key. These acts are carried out with the Key Application, with the exception of extermination of the private key (rendering it unusable).

Data audits are used to check the mutual concordance between the input and the output of processes, and the integrity and authenticity of the data signed digitally in the course of the processes. The main inputs and outputs of processes are the following:

- The input of the Collector: lists of voters, electoral districts and polling stations, the authentication and signature tools used, public key, and the parameters of the crypto algorithm used;
- The output of the Collector: votes collected into the i-ballot box;
- The output of the Registration Service: time-marks issued to the Collector;
- The outputs from the work stages of the Processor: checking of the integrity of the i-ballot box, annulment of repeated votes, anonymisation of votes, mixing;
- The output of the counting process: voting results.

In the course of data audit, the Auditor checks the integrity of the i-ballot box, and the correctness of the annulment of repeated votes and of the anonymisation of votes, by repeating the process with their tool that behaves in the same way as the Processing Application.

To verify the mixing and counting, the Auditor uses the mixing or tallying proof, in addition to the input and output. Mutual concordance between these data sets is checked with the help of the Audit Application; the Auditor is responsible for ensuring the reliability thereof.