Electronic Voting Pilot 2008

Technical Implementation and Security

Electronic Voting Pilot 2008 – Technical Implementation and Security

1 Introduction

Electronic voting will be used in the municipal elections held on October 2008. This is stated in the Election law (880/2006) accepted by the Parliament of Finland. Voters of the three municipalities (Karkkila, Kauniainen and Vihti) may choose to vote electronically or by using a traditional paper ballot. Electronic voting will not affect the well-established ways of casting ballots manually.

This document describes the technical solution used for electronic voting (e-voting). The intended audience of this document includes information technology experts, data security experts and other professionals familiar with e-voting technologies.

The system overview is in section 2. The main phases of e-voting process from preparations to tallying the election result are described in sections 3 – 7. Section 8 concentrates on the ballot encryption technology. Section 9 discusses briefly about the arrangements during the elections and section 10 is for those looking for more information about the e-voting pilot.

The emphasis in this document is on the technical implementation of the software and especially on the solutions for data security. Additional arrangements required during the elections at the polling stations and data centres are mentioned only briefly.

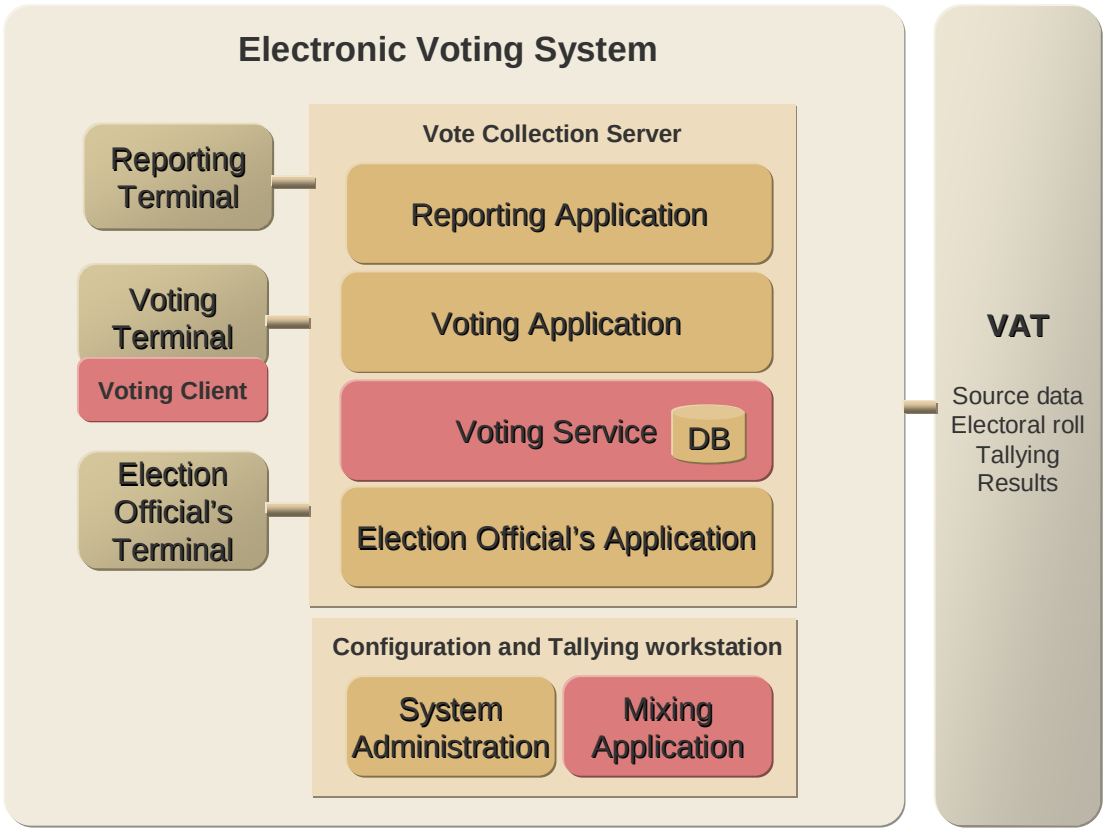
2 System Overview

Electronic voting takes place at the polling stations under the election authorities' supervision. The Electronic Voting System (picture 1) is based on integrating Pnyx.core software with the current Election Information System (VAT) that has been used for several years in general elections in Finland. Pnyx.core is a product that concentrates on e-voting data security.

Election authorities use the *Election Official's Application* to check the person's right to vote and to register when the voter has used this right.

The voter chooses a candidate in the *Voting Application* and confirms his/her choice. After that the Voting Application encrypts the ballot, digitally signs it and sends it to the Voting Service using a secure connection.

The Voting Service saves the cast ballot in encrypted form and confirms that the right to vote has been used.



Picture 1: The Electronic Voting System

Election authorities use the *Reporting Application* to monitor the Electronic Voting System. They can monitor the number of voters that have participated during the elections and the counting of electronic ballots after the election has ended.

Electronic voting is configured using the *System Administration*.

The Mixing Application is used at the end of the voting process to decrypt the cast ballots and to break the correlation between the vote and the voter ensuring voter's privacy. This process is executed under authorities' supervision in an isolated environment (air-gapped).

The Election Information System (VAT) is a mainframe system used to manage the basic election information, tally the votes and report the election results.

3 Election Preparation

The preparations for e-voting before the election includes, among other things, checking software versions, uploading the basic election information from VAT (eligible voters, candidates, parties etc.) using secure file transfer and configuring the electronic voting system.

The configuration will be done under the surveillance of election authorities and in a standalone computer (configuration server) without any network connections (air gapped).

During the configuration a cryptographic key pair is created (PKI). The private key is split into shares according to a cryptographic secret sharing scheme. The representatives of the Helsinki City electoral district committee and the Ministry of Justice will each receive a share of the key, stored on a smart card that is password protected. The password is only known by the representative himself. During this splitting process the private key is destroyed and therefore does not exist during the election.

The public key will be later used by the voters to encrypt the votes. The cast votes can only be decrypted collectively by the Helsinki City electoral district committee and the Ministry of Justice representatives by contributing with their shares to recreate the private key. This process (The Mixing Protocol) is described in further detail in chapters 6 and 8.

4 Verifying the Right to Vote and Registering the Use of it

Election official identifies the voter using his/her voter's identity card. This is the same procedure used when voting traditionally with a paper ballot. After the identification the official registers that voting has started and gives a smart card to the voter that allows him/her to cast one vote.

Using the Election official's application an official

- verifies against VAT-system that this person is entitled to vote,
- registers in VAT-system that the voting has been started and
- configures electronic voting card (smart card) for the voter.

Election official's application configures the voting card (manufactured by Giesecke & Devrient) by writing voter's credentials on it. The card ensures that the voter casts the ballot according to the entry made by official to the Electoral roll in VAT.

Election official's terminal is a standard PC that has been booted from a safe and secured read-only media (CD/DVD). This is to prevent malware and to limit the usage of the terminal only for the electronic voting. The terminal includes a card reader (manufactured by OmniKey) to manage the e-voting smart cards.

Election official's application is a combination of browser interface (Firefox) and server application. Firefox-browser interface is implemented using JSP generated HTML-pages. JavaScript- and Applet-technologies are used to manage the electronic voting cards. Server application is implemented with J2EE, and it has a real-time JDBC-connection to the vote collection server and VAT.

5 Casting a Ballot

Ballots are cast on a voting terminal that is placed in a voting booth. To be able to use the voting terminal the voter must receive an electronic voting card (smart card) from an election official. The system ensures that the voter can cast one and just only one vote.

Once the voter receives the electronic voting card he/she:

- enables the system by inserting the voting card in the card reader,
- chooses a candidate by entering a candidate number,
- confirms and casts the ballot, and
- returns the electronic voting card back to the election official.

During the ballot casting the voter's application

- verifies the data stored on the voting card (voter credentials),
- verifies the voter's right to vote against the electoral roll (VAT),
- verifies if the election official has marked the voting process as started,
- encrypts and digitally signs the ballot cast by the voter ,
- marks that the voter has used his/her right to vote, and
- saves the encrypted ballot on the vote collection server.

Voting terminal is a standard PC equipped with a touch screen and a card reader. The terminal is booted using a non-rewriteable media similarly to the official's terminal. Touch screen interface limits the usage to the voting functions.

Voter's application is a Java application based on Swing technology. Encrypted requests about voter identification and ballot casting are transmitted by the interface to a Voting Service located at the Vote Collection Server.

The Vote Collection Server has a Voting Service (Pnyx.Core) and a database (Oracle DB). Voting service receives the ballot that was encrypted by the voting application (Ballot Casting Protocol), verifies the voter's right to vote, confirms the right as used in VAT-system's electoral roll and saves the encrypted ballot in the database. The cryptographic solution ensures the privacy of voters and secrecy of intermediate results. The database integrity is assured by a cryptographically chained log file.

6 Mixing Service and Tallying

The electronic votes will be decrypted after the election has ended. The votes will be transferred to the air gapped tallying server using offline media (i.e. CD-ROM). The decryption is done by Helsinki electoral district committee and the Ministry of Justice representatives. Each representative contributes with their key shares to the Mixing Service using the smart card in their possession and introducing the password that protects it. The representatives' shares are used to reconstruct the election private key needed to decrypt the votes.

The Mixing Service implements a cryptographic process that shuffles and decrypts the votes, breaking any correlation between the encrypted digitally signed votes and the decrypted votes. Therefore it is not possible to correlate votes with voters based on the order the votes are decrypted. This process (The Mixing Protocol) is described in further detail in chapter 8 (Encryption of ballots).

The ballots are combined according to the law (Election law 86a§) after the mixing process has ended.

7 Combining Electronic Ballots with Paper Ballots and Tallying the Election Results

The Election information system (VAT) operates in the IBM-mainframe environment (DB2 and IDMS). It has been used for several years for general elections in Finland. The system is used to manage the basic data (parties, candidates, the electoral roll etc.), to register ballots, to tally (including electronic and paper ballots) and to manage the election results service.

The electronic votes are counted by the Electronic Voting System and the result is transferred to VAT. The VAT-system combines the results from the electronic ballots with the results from the paper ballots. After this the actual tallying takes place. The result of the elections will be transmitted from VAT to the election authorities, the media and other interest groups.

8 Encryption of Ballots

Electronic voting makes the use of encryption at the data communication level and at the application level. *Data communication* is encrypted with the commonly used SSL security protocol.

At the *application level* the encryption of the ballots is based on Pnyx.core's security solutions. Pnyx.core is a product developed by a company that is specialized in highly secure electronic voting (Scytl Secure Electronic Voting, S.A.). Pnyx.core's main components are: Voting Client (voting terminal's encryption component), Voting Proxy, Voting Service and Mixing Service (decryption application). Pnyx.core uses several internal protocols. The most important protocols are Ballot Casting Protocol and Mixing Protocol.

The Ballot Casting Protocol contains functions relating to the ballot casting process. The voter enters the candidate number of her choice on a touch screen. Then the system shows the personal particulars of the corresponding candidate and prompts the voter to confirm her choice. After the confirmation, the cast ballot (with the information on electoral district and polling station involved) is encrypted with the election public key, signed digitally and sent to the central vote collection server. The information can only be decrypted with the private key that is split in shares distributed among the electoral board members. These shares are stored on smart cards protected by passwords only known by each individual member.

The application level encryption is based on a commonly used Public Key Infrastructure (PKI). The ballot encryption is based on an asymmetric key pair, consisting of a public and a private key with mathematical interdependence. The information encrypted with a public key can only be cleared with the corresponding private key. In the case of electronic voting the private key is not available by an individual person or interest group. The private key is split with a cryptographic algorithm (secret sharing scheme) into shares and distributed among the members of the electoral board. Since the private key is destroyed during the splitting process, the actual private key only can be reconstructed combining these shares.

The decryption (Mixing Protocol) is performed after the voting is over but before the actual tallying. Decryption is processed in a computer without any network connections (air gapped). The members of the electoral board reconstruct the election private key using their personal smart cards and passwords. The Mixing Protocol uses this private key, corresponding to the public key that was used in the ballot encryption, during the shuffling and decrypting process of the ballots after validating them. Since the ballots are randomly shuffled, it is impossible to find out who cast the ballot for example through the ballots timestamp.

The most important PKI-standards used in this system are x.509v3 (certificates), PKCS (Public Key Cryptography Standards) and CRL (Certificate Revocation List).

9 Quality Assurance and Arrangements during Elections

The Pilot's *quality assurance* consists of system testing, external auditing and other quality measures. The system will be verified to be unaltered during the elections by using electronic signatures for the system components and using code signing certificates for the user interface.

Arrangements during the elections have a key role in securing the reliability of voting. Some of the most important factors are the actions by the election officials (e.g. supervision of polling stations), physical data security (e.g. physical protection of terminals), user rights and access control, and protection of data communication.

The backup plan is used to recover from exceptional situations. For example a power failure can be handled in several ways including the possibility to replace electronic voting to manual voting using paper ballots in certain restricted area.

10 Additional Information

Law about altering the Election Law (880/2006) www.finlex.fi.

The e-voting pilot system is provided by TietoEnator www.tietoenator.com. TietoEnator has successfully delivered information systems and services for Finnish National Elections since the mid 1980's.

The e-voting pilot system uses Pnyx.core -product functionality as described in this document. More information about the manufacturer can be found at www.scytl.com and detailed description about Pnyx.core at www.scytl.com/eng/pnyx_core_pdf.htm.

The Ministry of Justice will provide more information about e-voting Pilot project: http://www.vaalit.fi/14173.htm