Internet voting solution

CYBERNETICA
Internet voting – i-voting – allows voters to participate in an election over the Internet using their PC or notebook. i-voting is used as an additional voting method to better support the generality of elections.

- First i-voting solution in the world that is used for Parliamentary elections
- Used in Estonia five times for Parliament and Local Government elections since 2005
- Widely used and trusted – 24.3% of votes were cast over the Internet at Estonian Parliamentary elections in 2011
- Can be used from anywhere in the world – traveling citizens could easily participate in home elections
- Facilitates the timely publication of accurate election results
- Since the introduction of i-voting, overall voter turnout has risen
I-VOTING SOLUTION HIGHLIGHTS

I-VOTING MAKES LIFE EASIER FOR BOTH VOTERS AND ELECTION ORGANIZERS:

- Voter can vote when and where is most suitable, practically anywhere in the world
- Election organizers can publish accurate election results on the evening of election day

I-VOTING FULLY SUPPORTS PRINCIPLES OF DEMOCRATIC ELECTIONS

- **Freedom of elections**
  votes are not unduly influenced from the outside. To reduce a risks of negative influences, a voter can i-vote multiple times during election period.

- **Generality of elections**
  i-voting increases availability being a universal alternative to the physical appearance at the polling stations. i-voting uniquely provides unassisted private voting for visually impaired.

- **Uniformity of elections**
  i-voting is organized in a way that guarantees that all votes of eligible voters are equal.

- **Secrecy of the ballot**
  is rigorously protected by modern cryptography; no one other than the voter will know his/her vote.

### VOTERS AMONG PARTICIPATING VOTERS

- % of i-votes among advance votes
- Voter turnout

### VOTER TURNOVER 1992-2011

- Parliament elections
- Parliament elections without i-votes
- Local municipalities elections
- Local municipalities elections without i-votes
The success of i-voting solution depends on the availability of Internet and electronic identity (e-ID) to electorate. In Estonia, smart-card based e-ID is the primary identity document available to all residents. With an e-ID, people can give legally binding digital signatures and authenticate themselves in electronic environments.

The software, protocols and organization of i-voting are carefully designed to meet the requirements of democratic elections. e-ID is used to identify eligible voters, uniformity of elections and ballot secrecy are achieved through the application of double-envelope scheme:

- **Anonymous envelope** contains only the encrypted ballot expressing the choice of a voter
- **Signed envelope** confirms the choice of the voter by adding digital signature to the anonymous envelope
- **Anonymous envelope and signed envelope together form an i-vote**

Voter casts an i-vote with **i-voting client application**. The i-vote is sent to **i-voting system** for storage and later tabulation.

To ensure the ballot secrecy, the anonymous envelopes with encrypted ballots and the signed envelopes with personal data are separated after the i-voting period. After this **anonymization** of the digital ballot-box the **tabulation** follows: the encrypted ballots are decrypted and counted. The system opens the i-votes only if they are not connected to personal data.

To ensure that the voters can express their true will freely, without coercion, they are allowed to change their i-votes by voting again over the Internet or at the polling station. Only the last vote cast by a voter is taken into account.
**MAIN PRINCIPLES OF I-VOTING IN ESTONIA**

- All major principles of paper voting are followed
- Paper votes have supremacy over i-votes for the same person
- i-voting is allowed during a 7-day period before the voting day
- The voter uses e-ID to authenticate to i-voting system and to confirm the choice with a digital signature
- Repeated i-voting is allowed – only the last i-vote is taken into account
- Manual re-voting is allowed – if vote is cast in paper, i-vote will be revoked

**THE I-VOTING SOLUTION HAS THREE MAIN SOFTWARE COMPONENTS:**

- i-voting client application is a multi-platform user friendly voting-application for the voter. The i-voting client application is customizable for numerous types of elections.
- i-voting system is a group of servers under the control of the electoral committee. The i-voting system collects, stores, tabulates votes and creates reports for election management.
- i-voting verification application is a mobile app for the voter. The i-voting verification application assists voter in verifying that his ballot was cast as intended and accepted as cast.

The i-voting client application communicates with the i-voting system through the i-voting protocol. This protocol is used to securely authenticate and authorize voters, distribute lists of candidates, and collect i-votes.

The i-voting client application is an online client-side component that interacts with the Vote Forwarding Server. It is responsible of the actual voting act of the voter. All major platforms (Windows, Linux, MacOS X) are supported.

Functions of i-voting client application:

- **Voter authentication and authorization** – e-ID is used to identify eligible voters.
- **Candidate selection** – The list of available candidates is downloaded from the server and displayed to the voter who makes a selection with point-and-click UI.
- **Voting** – The anonymous envelope is composed by encrypting the ballot.
- **Digital signing** – For the protection of ballot integrity and identification of the voter, the encrypted ballot is put into digitally signed envelope.

The i-voting client application supports accessibility for people with disabilities, including possibility for visually impaired people to vote. Multi-language setups are also possible.

The i-voting verification application is a mobile app that interacts with the client application and the Vote Forwarding Server. It provides voter with an independent channel to verify that there has been no tampering with the vote on the client side.

The i-voting system consists of Vote Forwarding Server, Vote Storing Server and Counting Server. They are responsible for respectively collecting, storing and tabulating i-votes.

The Vote Forwarding Server and Vote Storing Server are online components of the i-voting system. Counting Server is offline at all times due to high security requirements. All servers interface with the election management for retrieving the configuration and sending the reports and results.
1. i-voting client software is downloaded
2. Integrity of software is validated
3. List of candidates is requested
6. Voter votes
7. Signed and encrypted i-vote is sent

1. i-voting client application is updated for current elections

4. Authenticates, verifies and authorizes voters
5. Distributes candidates lists
8. Accepts votes from i-voting clients
9. Forwards votes to Votes Storing Server
10. Stores i-votes

2. Integrity of software is validated

7. Signed and encrypted i-vote is sent

12. Vote is verified

3. i-votes are anonymized
4. i-votes are decrypted

5. i-votes are decrypted
6. Ballot tabulation

11. Stores i-votes

8. Accepts votes from i-voting clients

9. Forwards votes to Votes Storing Server

10. Verifies votes using OCSP

11. Stores i-votes

12. Vote is verified
THE VOTE FORWARDING SERVER accepts i-votes sent by i-voting client applications over the public Internet.
Functions of the Vote Forwarding Server:
Voter authentication – verify voter’s identity according to the rules of applied PKI.
Voter authorization – check that the authenticated person is an eligible voter indeed.
Candidates lists’ distribution – provide voter with the candidate list according to the electoral district he/she is registered in.
Vote collecting – accept correctly signed i-votes from the i-voting client applications.
Vote forwarding – send votes to the Vote Storing Server for secure storage.

THE VOTE STORING SERVER stores signed and encrypted i-votes in a secure location behind a firewall.
Functions of the Vote Storing Server:
Vote verification – verify the digital signature of the i-vote.
Voter verification – check the validity of the signing certificate used for voting.
Vote storage – store i-votes securely in digital ballot-box.
Vote anonymization – separate signed envelopes from anonymous envelopes before the tabulation.
Report generation – report list of i-voters to election officials.

THE COUNTING SERVER tabulates the i-votes to produce election results. The Counting Server is never connected to any network.
Functions of the Counting Server:
Tabulation – calculate election results by opening and counting the anonymous envelopes with securely stored decryption key.

ORGANIZATIONAL SECURITY REQUIREMENTS
Security of i-voting conception needs also organizational security measures.
• The i-voting organizational procedures must guarantee that i-vote anonymization and tabulation occur according to the election rules.
• The i-voting organizational procedures must be documented; the following of the procedures must be audited.
• The i-voting server administration tasks must be done only in the presence of several administrators.

I-VOTING RESEARCH AND DEVELOPMENT IN CYBERNETICA
i-voting system research and development activities are focused to two main objectives:
• ensuring security
• increasing usability and availability

Security related research and development:
• Fundamental research about i-voting, generation and study of attack-trees, improvement of defense mechanisms, cryptographic research
• Development of new i-voting protocols
• Increasing security in client platforms

Increase of usability and availability:
• Implementation of new authentication methods
• Researching i-voting client application implementation methods for new platforms (smartphones, tablet PC’s)
I-VOTING SYSTEM IMPLEMENTATION SERVICES BY CYBERNETICA

Cybernetica offers i-voting consulting and system development services to governmental institutions which are interested in implementing i-voting solutions in their region. We are willing to work together with local system integrators, in order to provide solutions that comply with local laws, regulations and cultural habits.

Internet voting can provide most of the value for local and governmental elections. i-voting can be used also in private sector activities.

SYSTEM DEVELOPMENT SERVICES:

- training and education
- technology provision, customization, installation, configuration
- technical online support for administrators
- software support
- implementation of security measures
- research and development of i-voting solutions

I-VOTING MANAGEMENT CONSULTING

- election procedures and requirement analysis
- planning
- legal framework consulting
- development of organizational processes
- authentication mechanisms consulting
- security requirements analysis and specification

CONTACTS

CYBERNETICA AS
Mäealuse 2/1, 12618 Tallinn, Estonia
Phone: +372 6397991
E-mail: info@cyber.ee