scytl
Secure Electronic Voting

scytl
Secure Electronic Voting

Voter-Verifiability through Independent Electronic Verification Modules

Jordi Puiggalí
R&D Director

Frontiers in Electronic Elections (FEE 2005)
September 15-16, 2005
Milan, Italy

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DRE Voting Terminals
- Our proposal: Pnyx.DRE
- Conclusions

Contents

scytl
Secure Electronic Voting

- **Presenting Scytl**
- DRE Voting Terminals
- Our proposal: Pnyx.DRE
- Conclusions

About Scytl

- Scytl is a European software company specializing in development of secure electronic voting solutions
- Scytl was formed as a spin-off from a University research group that holds two PhD thesis on e-voting security (with over 25 scientific papers) and that participated in the first Internet binding elections in Europe in 1997
- Scytl commercializes Pnyx, a unique family of products that derives from its more than 10 years of research and development and is protected by international patents
- The objective of Pnyx is to provide electronic voting platforms with the same levels of trust, privacy and security as the conventional paper-based electoral systems
- Pnyx has been successfully used in numerous projects, including one of the only two permanent Internet voting platforms in the world (Switzerland)
- Scytl focuses its efforts on developing and maintaining unique e-voting technology and distributes its solutions through partners such as Hewlett-Packard, Accenture, Oracle and Telefonica
- Scytl has received numerous international awards including the 2005 IST Prize granted by the European Commission to the best technology companies in Europe

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- **DRE Voting Terminals**
- Our proposal: Pnyx.DRE
- Conclusions

DRE Voting Terminals - Benefits

scytl
Secure Electronic Voting

- **User-friendly** – Easy-to-use voter interface that facilitates the voting process
- **Speed and accuracy** in the vote counting process – Votes are counted electronically in digital format
- **Accessibility** – People with disabilities (e.g., visually impaired) can vote without the assistance from a third party
- **Flexibility** – Allows last-minute changes in the ballots, supports multiple languages, etc.
- **Prevention of unintentional errors** – Reduces “under-voting” and prevents “over-voting” errors

DRE Voting Terminals - Drawbacks

scytl
Secure Electronic Voting

- DREs may be perceived as **“black boxes”**
  - DREs are generally based on proprietary and complex software
  - Difficult to audit and certify by election authorities
  - Need to re-audit the software after any change
- DREs **do not provide voters with verification mechanisms** to check that their votes have been correctly cast and recorded
  - Votes cannot be checked independently from the DRE before being stored
  - DREs do not provide a secure and reliable independent register of the votes that could be used in case of problems
- DREs **do not provide election authorities and third-parties with sufficient independent audit mechanisms** (e.g., DREs do not allow a meaningful parallel recount of the votes independent from the results from the DRE)

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DRE Voting Terminals
- **Our proposal: Pnyx.DRE**
- Conclusions

Objectives of the proposal

scytl
Secure Electronic Voting

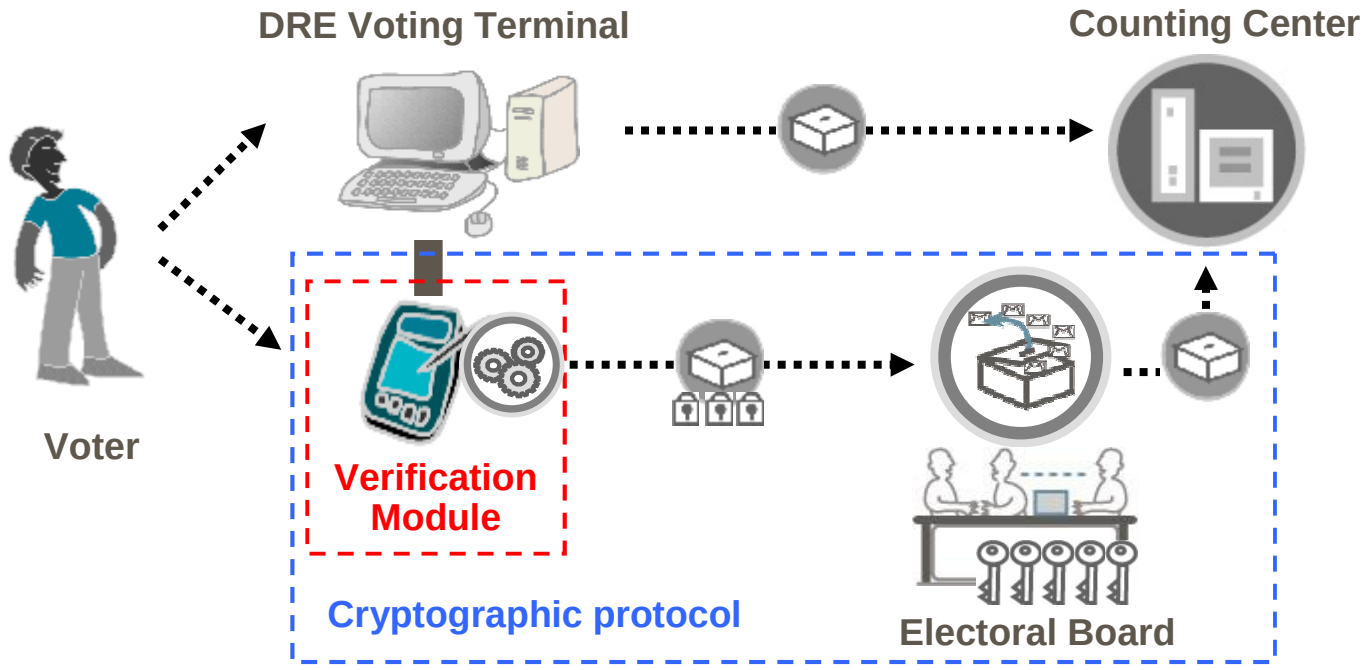
1. **Allow the voter to individually verify the correct treatment of his/her vote**
   - Verification that his/her vote is cast and recorded as he/she intended
   - Assurance that the recorded vote will be counted as cast
   - Make this verification process accessible to everyone
2. **Provide redundancy through a double-register of the votes**
   - Reduction in the risk of loss of votes
   - Facilitates the resolution of disputes
   - Facilitates a secure, private and independent parallel recount of the votes
3. **Facilitate the audit and certification process by the election authorities**
   - Simplification of the audit and certification of the voting system by concentrating the critical security features in a simple and easy-to-audit device
   - Enhancement of the auditability of the election through the use of cryptographic tools

Proposal Components

scytl
Secure Electronic Voting

The proposal is based on the combination of two main components:

- An independent hardware component (called **Verification Module**) connected to the DRE, that is used as a secure environment to verify and protect the vote
- A cryptographic protocol, that is used to protect the voter-verified vote and to facilitate the election auditability



Verification Module

scytl
Secure Electronic Voting

- The Verification Module represents a secure and reliable environment easy to audit because:
  - It is independent from the manufacturer of the DRE
  - It is based on software that is open to audits (open-source)
  - It is very simple since it only performs a limited number of functions
- The Verification Module provides an environment independent from the DRE where voters can verify theirs votes
- It also provides a secure and reliable environment to:
  - Store a backup register of the cast votes, independent from the DRE
  - Execute the critical steps of the cryptographic protocol

Cryptographic Protocol

scytl
Secure Electronic Voting

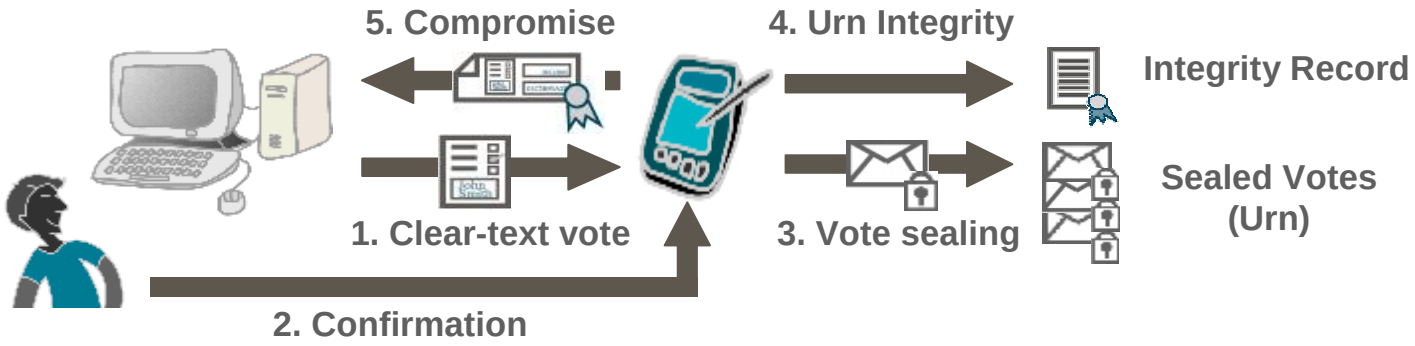
- The Cryptographic Protocol protects the votes verified and cast by the voters in the Verification Module by providing:
  - **Vote integrity**: Each verified and accepted vote is digitally signed by the Verification Module before being stored
  - **Vote privacy**: The votes are protected (encrypted) before being stored in the Verification Module. They can only be decrypted by the Electoral Board
  - **Vote authenticity**: Only votes digitally signed by a valid Verification Module can be accepted
  - **Digital urn integrity**: The protocol generates an integrity register of the urn stored in the Verification Module. This register can be used to check the integrity of the DRE digital urn during the counting process
  - **Voter verifiability**: The protocol allows the voter to verify his/her vote in an environment independent from the DRE. The protocol ensures that the vote is stored as it has been verified by the voter
  - **Dispute resolution**: The protocol allows to detect inconsistencies between the DRE and the Verification Module and facilitates its resolution.

Protocol Components

- **Election key pair**
  - The election public key will be used to encrypt the votes in the Verifications in order to protect voters' privacy
  - The Electoral Board is in charge to protect the election private key used to decrypt the votes
  - The private key is split in shares among the Electoral Board members during the election configuration by means of a secret sharing scheme
- **Verification Module key pair**
  - Each verification module has its own key pair used to protect the integrity of the election generated data (votes and internal registers)
- **Verification Module integrity record**
  - The Verification Module maintains an integrity record of the digital urn stored in the module. This record is generated using a One-Way Accumulator function to provide independency of the storage order of the votes

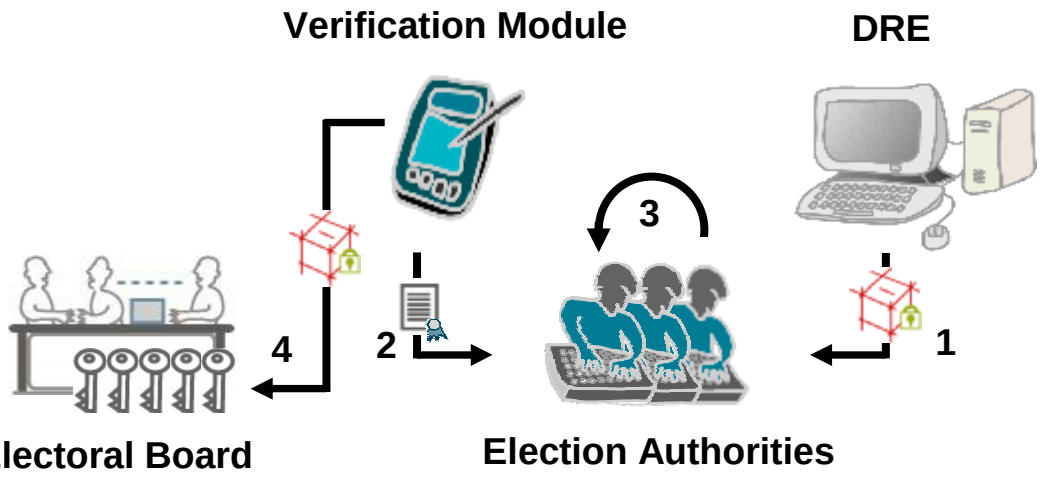
Voting Process

scytl
Secure Electronic Voting



1. A clear-text vote (i.e., the voting options selected by the voter in the DRE) is sent from the DRE to the Verification Module through an authenticated channel
2. The vote contents is presented to the voter (visually or via audio) who confirms it in the same Verification Module
3. The Verification Module encrypts the clear-text vote using the election public key (e.g. using a digital envelope) and digitally signs the encrypted vote using its own private key. The sealed vote is stored in the Verification Module
4. The Verification Module generates an integrity record of the votes stored in it by means of a commutative hash function (One-Way Accumulator). This function uses the contents of the clear-text vote and the last value of the Integrity Record. This Integrity Record is digitally signed by the Verification Module to avoid tampering
5. The Verification Module generates a compromise of the confirmation using the received vote (digitally signs the clear-text vote and confirmation) and sends it to the DRE. The DRE verifies the compromise and stores it with the verified vote

Audit Process



1. The election authorities retrieve the votes from the DRE
2. The election authorities retrieve the Integrity Record from the Verification Module. This Integrity Record was generated in a secure environment based on every single voter-verified vote
3. The Election Authorities calculate the Integrity Record of the votes retrieved from the DRE (using the same hash commutative function used by the Verification Module) in order to check that the Integrity Record of the DRE votes matches the value of the Integrity Record from the Verification Module
4. If the check fails, the Electoral Board can retrieve the back-up votes from the Verification Module using the election private key. To this end, the Electoral Board members must provide their shares of the private key to decrypt the votes. A Mixing protocol is used to break the correlation between the encrypted votes and the retrieved clear-text votes. The retrieved votes can be used to solve any dispute or to implement a parallel recount of the results.

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DRE Voting Terminals
- Our proposal: Pnyx.DRE
- **Conclusions**

Conclusions

scytl
Secure Electronic Voting

- The described proposal can **enhance the security and auditability** of existing voting equipment by:
  - Allowing voters to verify that their votes were cast and recorded as they intended
  - Simplifying the audit and certification processes since the auditing efforts need to focus only on the simple and easy-to-audit Verification Module
  - Protecting the integrity and anonymity of every single vote
  - Reducing the risk of losing votes by providing the voting system with redundancy
  - Allowing an independent parallel vote recount
  - Allowing dispute resolution in case a problem arises with the votes recorded in the DRE

scytl
Secure Electronic Voting

Secured by scytl