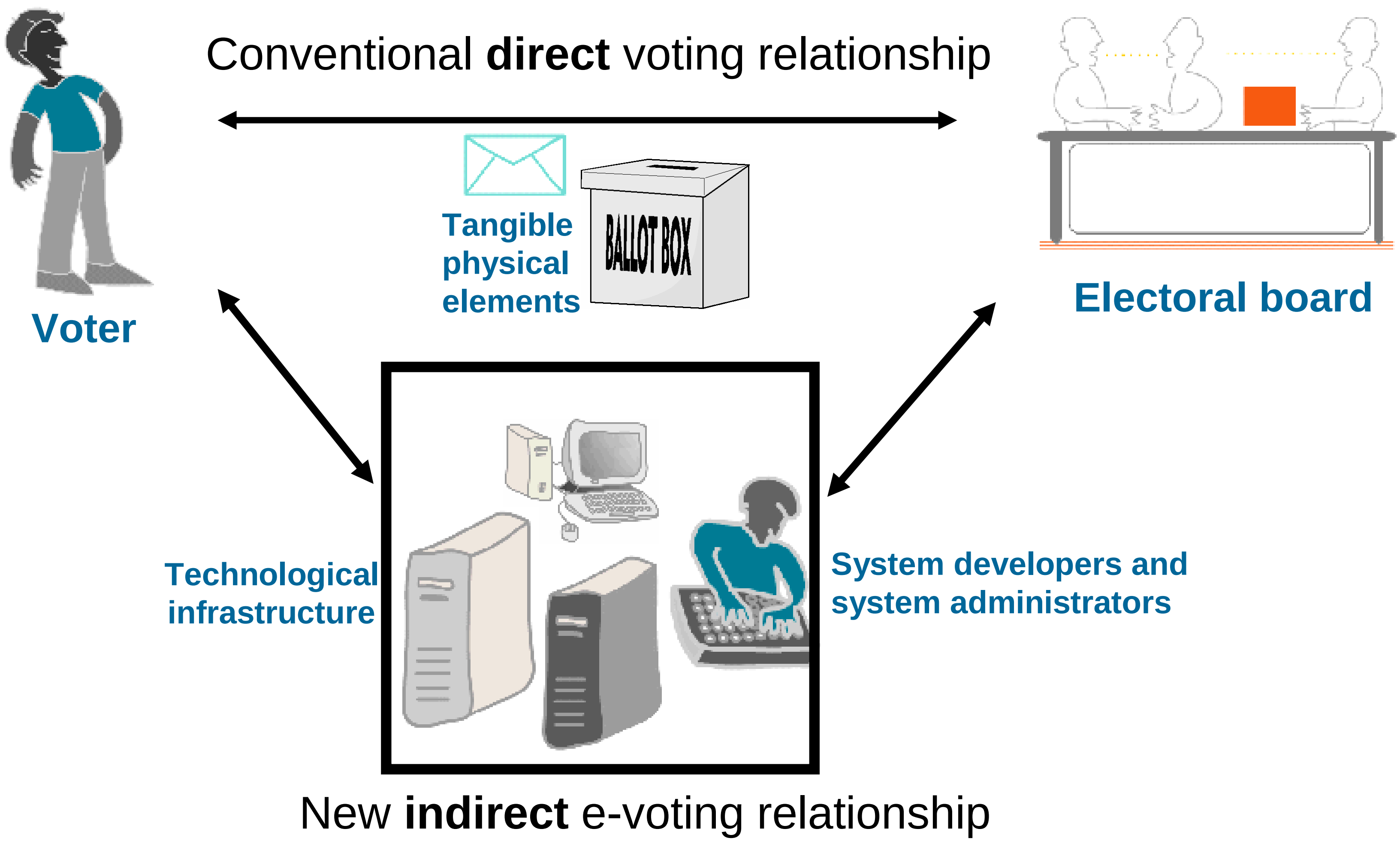
Applied Cryptography Enabling Trustworthy Electronic Voting

Scytl Online World Security, S.A.

Disclosure Note

The property of the cryptographic mechanisms and protocols described in this document is protected by Patent Applications PCT / ES02 / 00423 and PCT / IB03 / 01884

Change of Voting Paradigm



Electronic voting creates a new indirect voting relationship that brings **new security risks** that reduce the trustworthiness of the electoral process.

Sources of New Security Risks

Four main **sources of security risks** emerge due to the technical infrastructure interposed between the voter and the electoral board:

- The **digital (virtual) nature** of the ballots
  - Ballots may be added, deleted or otherwise manipulated
  - Voters' privacy may be compromised on a large scale
- The **complexity** of the systems used
  - Electronic equipment may malfunction
  - Software may contain programming errors
- The **lack of transparency** of the systems used
  - The technical infrastructure is not easily audited
- The introduction of **people with privileges** on the systems used
  - New players enter the scene

These risks all serve to undermine the trust in the e-voting system caused by an indirect e-voting relationship

How to Manage These New Risks

?

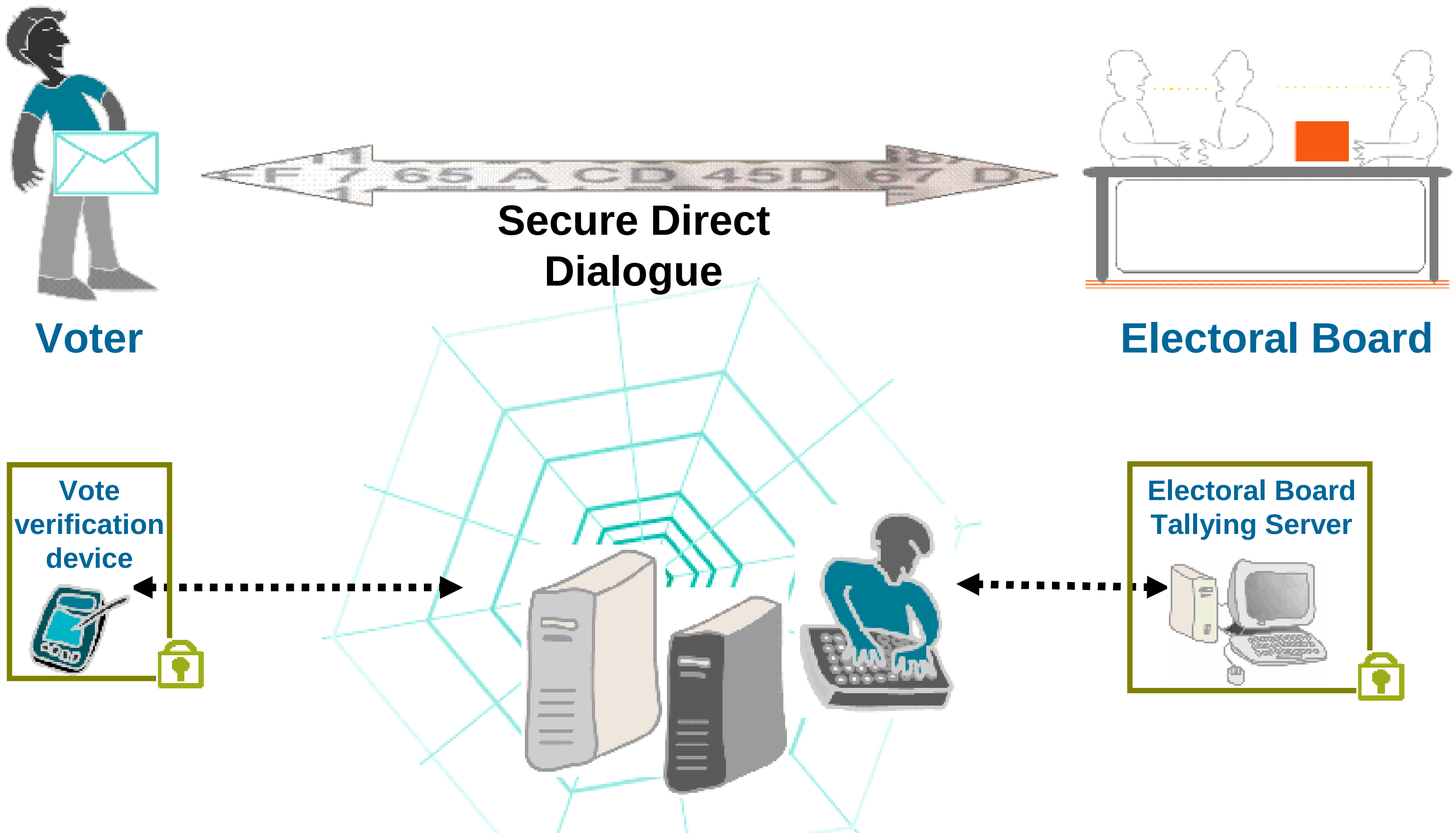
Ignore the risks → Expect **catastrophic** results

Manage the risks by deploying an adequate security architecture → Use a combination of **technological, physical and procedural security measures** to re-establish the direct dialogue between voter and electoral board

Avoid the risks by returning to the tangible election → Create a **physical audit trail** to bring trust to the voting process

We believe that adequate solutions can be devised to **bring trust to electronic voting** systems

Security Architecture Overview



A **secure direct dialogue** between the voter and the electoral board is created by tunnelling through the complex technological infrastructure

Security Architecture Principles

- Critical functions should be isolated on **simple modules** that are **physically protected**
  - Avoid complexity on these key modules so that they are easier to secure
- **Source code** on the simple modules should be **made available for inspection and certification**
  - Closed voting systems located between these modules do not need to be trusted for the whole system to be trustworthy
    - e.g. SSL connection tunnelling through insecure internet
- **Extensive auditing** must be done of the system design, the modules and the software
  - To trust an open security system that surrounds a closed voting system, the security system must be beyond reproach
- **Voter-verification** is key
  - For security, and more importantly for trust in the system
  - Run independently of the voting system

Security Architecture Modules

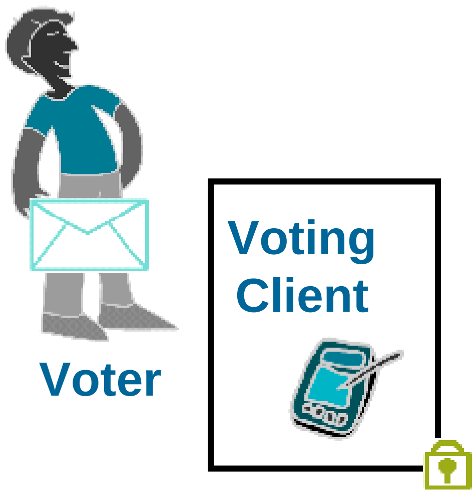
- **Voter verification device**
  - A simple *hardware security module* connected to the DRE
  - Includes either a printer or a visual display for verification purposes
  - Contains buttons to either confirm or reject the vote as presented
  - Runs digitally signed certified software that performs the voter-side of the cryptographic protocol

- **Electoral board tallying server**
  - A special-purpose stand-alone server that is physically monitored
  - Runs digitally signed certified software that performs the electoral board-side of the cryptographic protocol

The security modules are simple, comprehensively audited, and physically protected

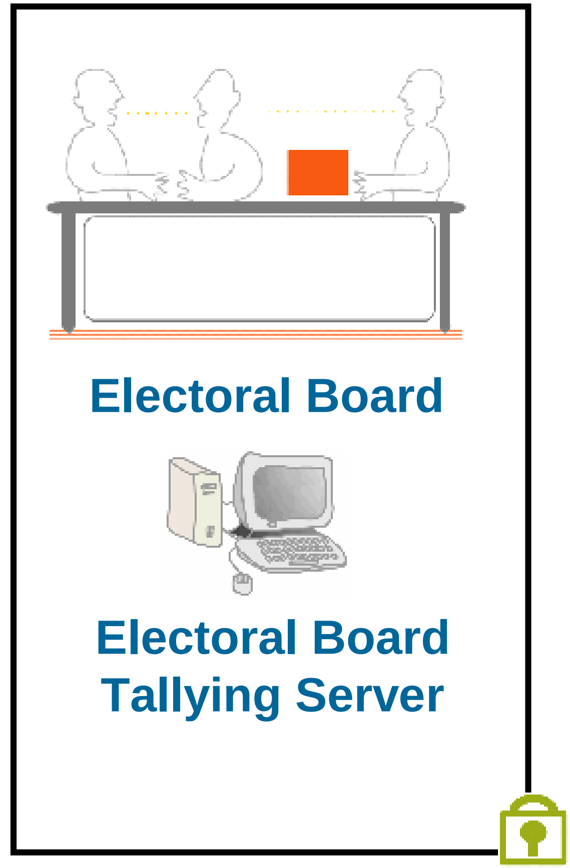
Voter Verification Device Tasks

- Asks the voter for confirmation of their vote
  - The voter-verification takes place outside of the DRE
- Protects the ballot's integrity & confidentiality with a digital envelope
  - The private key needed to open the envelope does not exist during the election
- Attaches a proof of authenticity to the ballot envelope
- Keeps a fingerprint/copy of the ballot box
- Can provide cryptographic security for paper ballots that are printed



Electoral Board Tallying Server Tasks

- Generates the unique cryptographic key pair
  - This key pair is used to lock (with the public key) and unlock (with the private key) ballots into digital envelopes
- Distributes trust among the members of the electoral board
  - A secret sharing scheme allows the electoral board to act collectively
- Uses a mixing protocol to break any correlation between clear ballots and enveloped ballots
  - This allows the system to ensure the anonymity of the vote



Security Architecture Benefits

- The **critical security requirements** for e-voting systems are resolved by transferring the control of all critical functions to the electoral authorities:
  - **Voter self-verification** during the voting process
  - Preserves **anonymity**
  - The **protection** of the digital urn:
    - Partial results stay secret during the election
    - Integrity of votes is guaranteed
    - Addition of bogus votes is not possible
- Using **simple secure modules** for critical functions avoids the need to place trust in complex technology that may be harder to secure
- The **replication of conventional protection mechanisms** online will foster a greater acceptation of e-voting by all parties involved
  - e.g. the use of an electoral board
- The architecture is **voting-channel neutral**
  - This can be used on DREs in polling stations or via internet remotely

Scytl

http://www.scytl.com

products@scytl.com

Phone +34 934 230 324