

Dear Mr. Eustis,

My name is Pere Valles and I am the Managing Director of Scytl, a European software company specialized in developing secure electronic voting solutions. I am contacting you regarding your public invitation to send you information on electronic voting technologies.

Scytl's R&D efforts over the last ten years have focused on Internet voting where we have developed a wide-range of products (e.g., Pnyx.core, Pnyx.government, Pnyx.corporate and Pnyx.labour). Each of these products addresses a specific market segment within the Internet voting industry, ranging from elections and consultations for the public sector to shareholders' meeting and labour union elections for the private sector. Pnyx.core, which is the e-voting security engine for all the other products, has been awarded the prestigious 2005 IST Prize by the European Commission and it has been successfully integrated into numerous Internet voting platforms throughout Europe, including one of the only two permanent Internet voting platforms for binding elections and consultations in the world.

We have recently launched Pnyx.DRE, a security solution for poll-site electronic voting that provides redundancy, enhanced auditability and voter-verifiability to DREs. Pnyx.DRE is based on (i) a simple easy-to-audit hardware device (called the "verification module") which represents a secure and reliable environment in which voters can verify their votes before casting them, and (ii) a cryptographic protocol (implemented in this secure hardware device) that protects the votes before they are cast and returned to the DRE.

We were recently invited by the Maryland House of Delegates to present Pnyx.DRE. Enclosed please find a copy of the presentation (slides 9 through 13 explain the main objectives of our solution and how it works). You can also find a complete white paper on Pnyx.DRE at the following link: <http://www.scytl.com/docs/pub/a/PNYX.DRE-WP.pdf>

Best regards,

Pere Valles

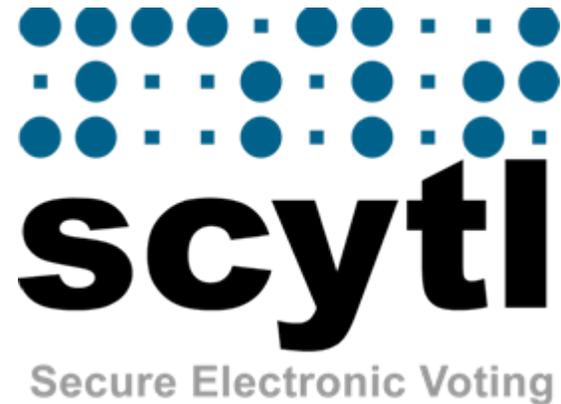
Managing Director

email: pere.valles@scytl.com

phone: +34 934 230 324

fax: +34 933 251 028

mobile: +34 619 761 349



PNYX.DRE

Presentation to the Maryland House of Delegates

Annapolis (Maryland), March 18 2005

- Presenting ScytI
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- Conclusions

- **Presenting ScytI**
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- Conclusions

About ScytI



- ScytI is a European software company specialized in application-level cryptography and in the development of secure electronic voting solutions
- ScytI was formed as a spin-off from a University research group that holds the first two European PhD thesis on e-voting security (with over 25 scientific papers) and that participated in the first Internet binding elections in Europe in 1997
- ScytI commercializes a unique software product, Pnyx, 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)
- ScytI focuses its efforts on developing and maintaining unique security technology and distributes its solutions through partners such as Hewlett-Packard, Accenture, Oracle and Telefonica
- ScytI has received numerous international awards including the 2005 IST Prize granted by the European Commission to the best technology companies in Europe

- Presenting ScytI
- **DREs: Benefits and Drawbacks**
- Our solution: Pnyx.DRE
- Conclusions

- **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 “over-voting” errors

DREs - Drawbacks

- DREs are perceived by many voters as “**black boxes**”
 - DREs are generally based on proprietary software
 - High-level of complexity in the software
 - Difficult to audit and certify by election authorities
 - Need to re-audit the software after any change in the election
- DREs **do not provide voters with verification mechanisms** to check that their votes have been correctly cast and recorded
- DREs **do not provide election authorities and independent third-parties with sufficient audit mechanisms** (e.g., DREs do not allow a meaningful parallel recount of the votes independent from the results from the DRE)

- Presenting ScytI
- DREs: Benefits and Drawbacks
- **Our solution: Pnyx.DRE**
- Conclusions

Objectives of Pnyx.DRE



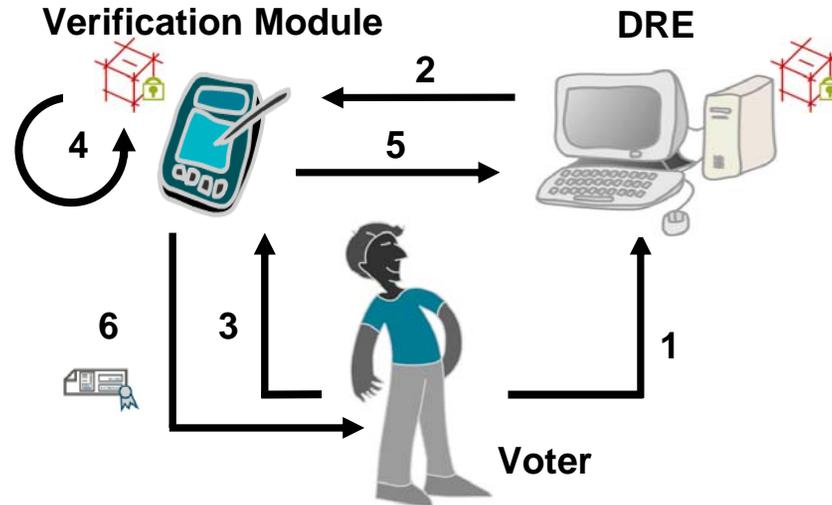
1. **Allow the voter to individually verify the correct treatment of his/her vote**
 - Verification that his/her vote is cast and recorded as he/she intended
 - Assurance that the recorded vote will be counted as cast
2. **Provide redundancy through a double-register of the votes**
 - Prevention of the loss of votes
 - Possibility of an independent parallel recount of the votes
3. **Facilitate the audit and certification process by the election authorities** by concentrating the critical security features in a simple and easy-to-audit device

Pnyx.DRE Components



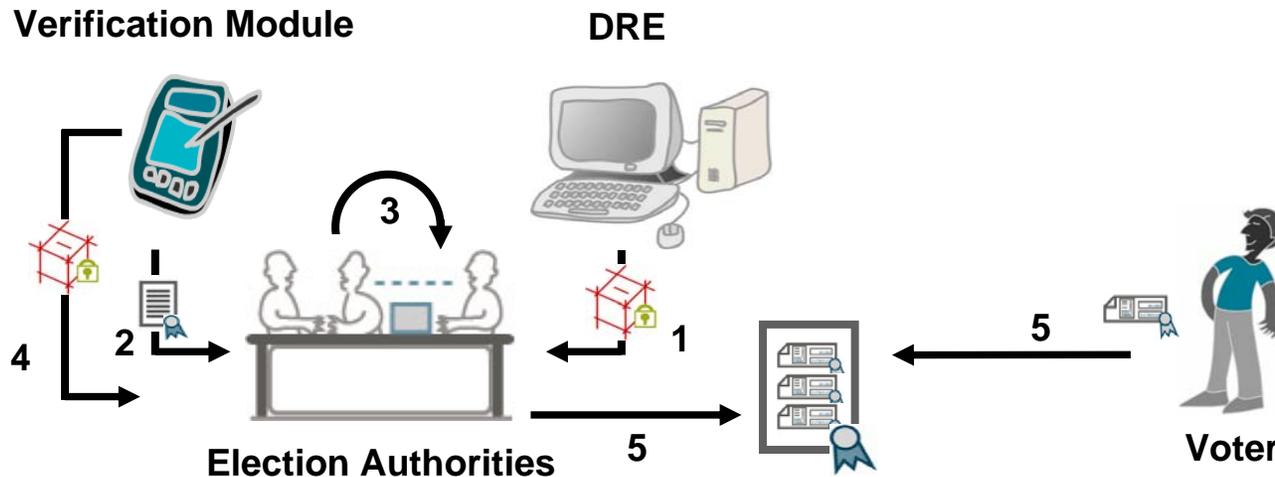
- Pnyx.DRE is based on an independent module (called **Verification Module**) connected to the DRE
- The Verification Module has **two components**:
 - A **hardware device** with a screen, an audio output and two buttons
 - **Software** running in this hardware device to cryptographically protect the votes
- The Verification Module represents a **secure and reliable environment** because:
 - It is independent from the manufacturer of the DRE
 - It is based on open-source software and on software that is open to audits
 - It is very simple since it only performs a limited number of functions
 - It is very easy to audit and certify by election authorities
- Additionally, our solution provides **election authorities with cryptographic tools** (e.g., one-way accumulators) **to check the integrity of the votes**

How is the voting process?



1. The voter makes his selection in the DRE
2. The selected options are transferred to the Verification Module
3. The voter verifies (via screen and/or audio) and confirms the selected options
4. The selected options are encrypted and digitally signed in the Verification Module in order to protect the ballot from internal and external attackers
5. The protected ballot is stored in the Verification Module and transferred to the DRE where it is also stored until the end of the election
6. Optional: The Verification Module generates a paper receipt (i.e., a randomly-generated unique identifier) that will allow the voter to check this identifier against a list of all the identifiers that correspond to the votes managed by the Electoral Board during the counting process

How is the audit process?



1. The election authorities retrieve the Ballot Box from the DRE
2. The election authorities retrieve the Ballot Box 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 verify that the contents of the Ballot Box retrieved from the DRE correspond to the integrity record from the Verification Module
4. If the check fails, the election authorities can retrieve the back-up Ballot Box (containing the cryptographically-protected voter-verified votes) from the Verification Module and implement a parallel recount of the votes
5. Optional: The election authorities can publish the unique identifiers (i.e., voter receipts) corresponding to the votes retrieved from the Verification Module. Voters can check at the end of the election that their votes were present during the counting process

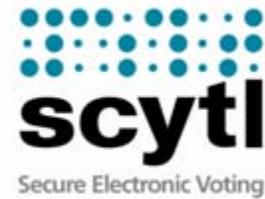
Cost of Pnyx.DRE



- The **cost** of Pnyx.DRE is **approximately \$500** per DRE and includes the following:
 - The **hardware** device with a color screen, audio output, computing and cryptographic capabilities and two buttons
 - The **software** implemented in this hardware device to cryptographically protect every single vote
 - The **software** used by electoral authorities or independent auditors to check the election accuracy and integrity
- There is an additional charge of **approximately \$300** per DRE for the **optional feature of providing voters with a paper receipt**. This additional cost includes:
 - The **printer**
 - The **software** to generate the cryptographic receipt

- Presenting ScytI
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- **Conclusions**

Conclusions



- Pnyx.DRE can **enhance the security** of your existing voting equipment and contribute to **increase public confidence** in this 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
 - Preventing the loss of votes by providing redundancy to the voting system
 - Allowing an independent parallel vote recount
- Pnyx.DRE can be **easily integrated with your current Diebold equipment**
- Pnyx.DRE is a **cost effective** solution to provide electronic voter verification to your current voting equipment



Secured by
scytel 