Pnyx.core: The Key to Enabling Reliable Electronic Elections

A Description of Scytl's Cryptographic e-Voting Security Software

scytl
Secure Electronic Voting

Pnyx.core: The Key to Enabling Reliable Electronic Elections

A Description of Scytl's Cryptographic e-Voting Security Software

White Paper

Scytl Secure Electronic Voting

May 2009

STRICTLY CONFIDENTIAL

Use only for evaluation purposes

The property of the cryptographic mechanisms and protocols described in this document are protected by means of International Patent Applications

Abstract

Adequate cryptographic solutions are needed whenever an election is conducted by electronic means (poll-site electronic voting systems using digital ballots or networked voting systems with remote ballot casting). Scytl has developed a cryptographic e-voting framework to enable reliable and trustful electronic elections. Scytl's e-voting framework ensures the authenticity of ballots, privacy of voters, accuracy of election results, secrecy of intermediate results, verifiability of election results by voters, and uncoercibility (the prevention of vote-selling and coercion of voters).

This document describes Pnyx.core, the software product developed by Scytl to implement the patented cryptographic protocols comprising Scytl's e-voting framework. The most important among these protocols are: the ballot casting protocol, performed by voters in collaboration with a ballot box server; the mixing protocol, performed by electoral authorities to open up the digital ballot boxes; and the verification protocol, that allows voters to verify their ballots against the published results ensuring that their votes have been correctly accounted for. Scytl's e-voting product Pnyx.core, named after the hill in ancient Athens where elections were performed, conforms the core of all Scytl's e-voting solutions, and can be easily integrated into other electronic voting systems.

Intended Audience

The intended audience of this document includes IT officers, security officers, managers, and other parties and individuals involved in the security of electronic electoral processes. This document is also interesting to parties evaluating and/or developing a transition process from traditional voting to any kind of electronic voting system (poll-site voting or remote voting), and who need to understand the benefits of using cryptographic e-voting frameworks.

1 Introduction

Conducting an electronic election that involves ballots in digital form is a complex issue that raises a number of security concerns. The confidence relationships found in traditional elections must be replicated in electronic systems, without losing reliability. Electronic voting must therefore reproduce the practices of traditional voting methods (e.g. secure identification of voters, as well as distribution of trust among the members of an Electoral Board). Additionally, electronic voting faces new requirements (e.g. new privileged actors such as system administrators) and new technical risks (e.g. digital ballot formats that are more easily manipulated than physical ones).

Digital security measures are therefore paramount for electronic voting success. However, conventional computer and network security measures (e.g. firewalls, intrusion detection systems, antivirus software...) fall short of providing a complete solution to electronic voting. These generic security measures, although regularly used to secure e-commerce and e-business transactions, are not enough for e-voting.

Indeed, casting ballots is not an ordinary transaction. When performed electronically, it must address the following requirements and security concerns:

- **Authenticity of ballots** Reliable means to verify the origin of a ballot (i.e. the identity of the voter who casts it) must be used, to ensure the “one voter, one vote” premise.
- **Privacy of voters** Despite the previous requirement, it must impossible to correlate the votes to the identities of their respective voters, unless required by law (as it is in some countries).

- **Accuracy of election results** It must not be possible for anyone to remove or alter the ballots that have been cast by eligible voters or to add invalid ballots (e.g. on behalf of abstaining voters).
- **Secrecy of intermediate results** To ensure that voters' choices are unbiased, intermediate results must be secret until the election is completed.
- **Ballot verifiability** Voters must be able to independently verify that their ballots have been correctly accounted for.
- **Uncoercibility** The fact that voters can verify their votes must prevent fraudulent practices such as coercion or vote-selling possible

The digital security measures for e-voting must meet the requirements above, detecting and preventing fraudulent practices even when they are performed by privileged actors in electronic voting environments (e.g. electoral authorities or systems administrators). There is only one way to ensure the fulfillment of these security requirements that are specific to e-voting applications, and therefore to ensure reliability of electronic voting systems: to construct digital security measures around an application-level cryptographic e-voting framework.

Figure 1 depicts the general security architecture of an electronic voting system involving a sound cryptographic e-voting framework. This kind of e-voting framework raises the level of the security solution to the highest layer (the application level). Additionally, it is complemented with generic digital security measures to obtain in-depth security.

Scytl leveraged the groundbreaking research on cryptographic e-voting frameworks carried on by a renowned academic research group to develop Pnyx.core, a software product that meets the requirements and security concerns posed by electronic voting environments. Pnyx.core has been designed to be highly configurable and easy to integrate into existing as well as newly developed electronic voting systems.

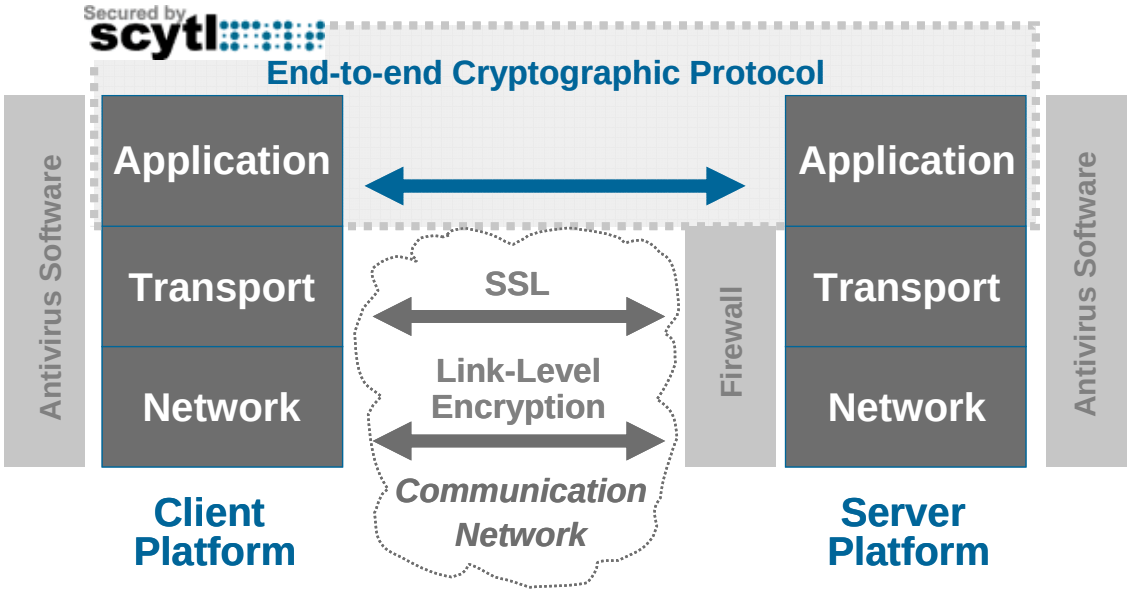

Figure 1: Overview of security measures for e-voting systems

The following sections provide additional details about Pnyx.core: how the product increases security and grants reliability to electronic elections, and how the product is integrated into Scytl's electronic voting systems.

2 E-Voting Architecture Overview

Pnyx.core consists of a set of software components that may be integrated into an e-voting system (either poll-site-based or remote). These software components may be distributed across several server systems and computerized client devices with different architectural requirements. To ensure a painless integration, only a minimum number of platform elements are affected by Pnyx.core.

The design of Pnyx.core has been based upon e-voting system architectures comprising of at least the following elements (see Figure 2):

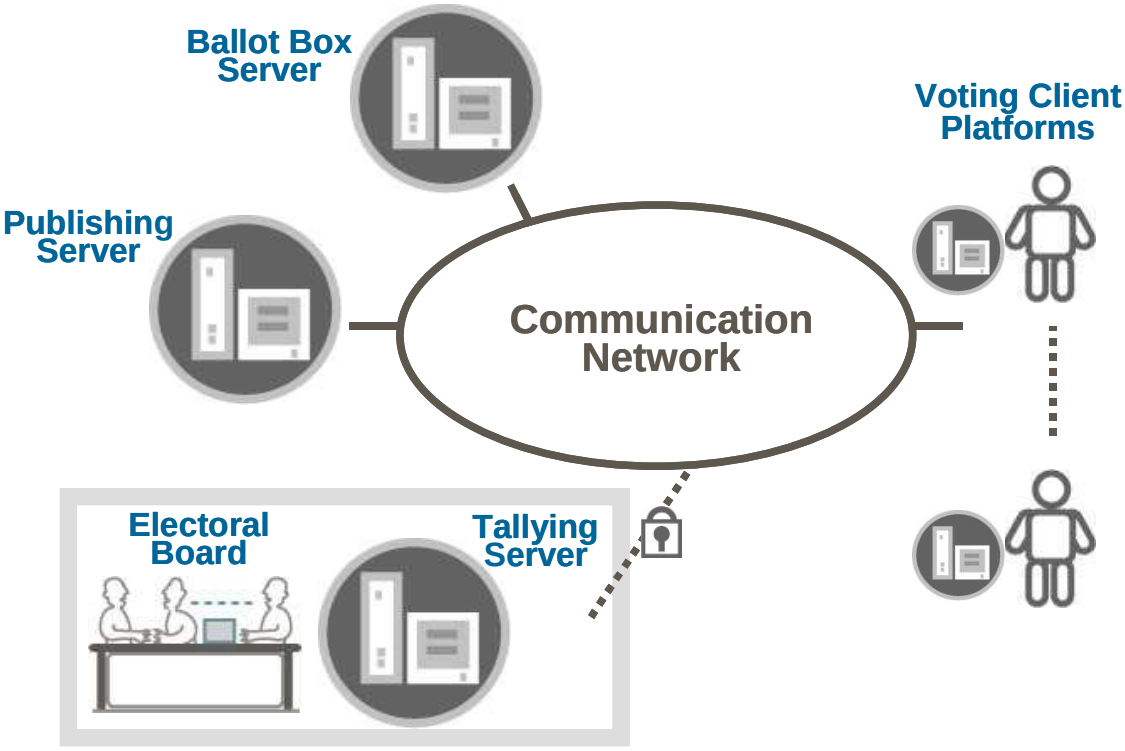

Figure 2: Main elements of an e-voting system upgraded by Pnyx.core

- **Voting client platforms -** Computerized devices and systems used by voters to interact with the voting services. Pnyx.core components allow voters to securely cast their ballots and to verify that the ballots have been properly accounted for. Special care has been taken in allowing integration of Pnyx.core software on thin-client devices. Therefore, Personal Computers, voting kiosks, poll-site voting terminals and handheld devices (such as PDAs or Java-enabled mobile phones) are supported.
- **Voting server platforms -** The server systems that handle the electronic election. According to the specific functionality they provide, three basic server system types can be distinguished:

- **Ballot box server:** The server system responsible for collecting and storing the ballots cast by voters. Pnyx.core provides the proper framework to securely collect and store these ballots.
- **Tallying server:** The server system where the digital ballot box is opened and the ballots are decrypted and tallied. Pnyx.core provides the cryptographic framework to access the contents of ballots without compromising voter privacy, and to issue the data needed for vote verification.
- **Publishing server:** The server system that publishes the election results. Pnyx.core enables a new function on this server: the verification process by the electorate.

Depending on the specific characteristics of the architecture of the election platform, these servers can be totally distributed or partially grouped.

- **Communication network -** A suitable communication network (or a group of them) that links all the elements of the voting system. In poll-site voting systems, such a network could take the form of a Local Area Network, while in remote voting systems the network will probably be the Internet or a corporate Intranet.

The purpose of Pnyx.core is not to provide full-blown server implementations, but to augment the functionality of electronic voting platforms (such as Scytl's Pnyx.government or Pnyx.labour) with the integration of its application-level security components. Pnyx.core implements a set of cryptographic protocols and mechanisms which jointly ensure the electoral security requirements listed above.

The main cryptographic protocols included in Pnyx.core are devoted to securing the process of ballot casting by voters, and the process of opening the ballot box by the electoral authorities in charge of the election. A third protocol, the verification

protocol, provides voters with the capability of verifying that their ballots were properly accounted for (allowing them to make public complaints in case of the detection of any problems). Other administration protocols offer secure mechanisms to open and close the voting period and to detect fraudulent practices. All these cryptographic protocols take place at different times, during the several phases that constitute an election. Still, they are intertwined by shared data structures and they work cooperatively to address the goals of a secure e-voting process. Figure 3 shows an overview of the cryptographic protocols implemented by Pnyx.core's components.

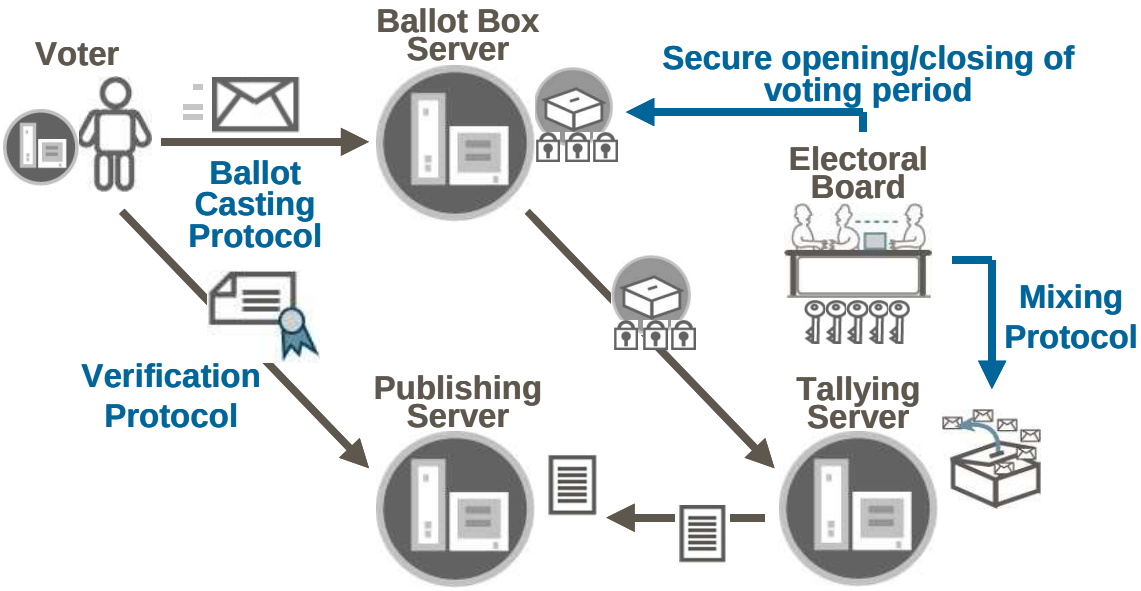

Figure 3: Pnyx.core main cryptographic protocols

Pnyx.core addresses not only security concerns, but also practical ones which facilitate a seamless integration into existing or new electronic voting platforms:

- **Independence of ballot layout -** The framework's implementation and configuration is completely independent of the ballot's format. Therefore, Pnyx.core can deal with any kind of ballot option input format, such as write-in

candidates.

- **Low client resource requirements -** The low computing resources needed to implement the client side of this protocol make it suitable for integration in thin clients like PDAs, Java Cards and J2ME-enabled phones (i.e. devices with limited execution capabilities).

3 Secure open/closing of voting period

Before starting the voting process, the election is configured using the information provided by the Election Officers (e.g., races, ballot templates, electoral roll, etc.). This configuration process is carried out through a Pnyx Election Configuration component that is executed in an isolated machine (i.e., disconnected from any network). Therefore, the information is transferred to this machine using removable storage media (e.g., CDROM or DVDROM). Once the election data is introduced, the information is reviewed by the Electoral Board: a set of election authorities with divergent interests (e.g., representatives of the political parties).

If the information is correct, the Election private key (RSA) is created and protected by means of a cryptographic secret sharing scheme (Shamir). The secret sharing scheme is used to split the key in shares that are distributed among the members of an Electoral Board. Since the private key is destroyed after split, it does not exists anymore during the voting process and until the Electoral Board members join again to provide their shares and reconstruct the key. Shares are usually stored in cryptographic smartcards protected by PINs provided by each individual member. The secret sharing scheme allows to define a threshold of members (e.g., 5 of 7) to reconstruct the private key to prevent that the loose of an individual share could prevent the reconstruction of this key. The objective of this key is to preserve the privacy of the voters: it allows the decryption of the votes encrypted by the voters. One of the main advantages of cryptographic secret sharing schemes is that having access to a number of shares under the threshold limit does no provide any

information that could allow to discern the value of the private key. In other words, the number of possible private keys that can be inferred from any combination of shares that are the pre-defined threshold is infinite. For instance, having 3 shares of the 4 required to reconstruct a key does not provide a 75% of the information required to reconstruct the key but 0. Another advantage of secret sharing schemes is that the key does not exist in a whole during the election, preventing to have a single point of attack that could be exploited to break the voter privacy or make a DoS attack (e.g., an attacker cannot target the attack to a single HSM module to steal the private key or destroy it to prevent the decryption of the votes).

Finally, the Electoral Board digitally signs the election configuration information (election identifier, election opening and closing time, electoral roll, etc.) and this digitally signed information is uploaded to the voting platform (using the removable media). As part of the election configuration information, there are an opening and closing tokens that specify the start and end of the voting period. This information is also digitally signed by the Electoral Board.

4 Ballot Casting Protocol

In the context of an electronic election, the action of casting a ballot is one of the most critical activities. Pnyx.core assembles a set of cryptographic techniques, specifically designed to meet the strong security requirements posed by electronic elections (see Section 1). The start and end of the acceptance of votes by the ballot casting protocol is setup through the Election opening and closing tokens. These tokens are digitally signed by the Electoral Board and the digital signature is validated to prevent any manipulation of these dates.

The main features of the Pnyx.core ballot casting protocol are:

- Secure authentication of server platforms and establishment of an authenticated and confidential connection between client and server. A secure data transport protocol, like SSL, is proposed.
- Casting of ballots to the ballot boxes ensuring integrity of votes and voters' privacy, even against malicious actions by system administrators in charge of the ballot box servers. To meet these requirements, cryptographic mechanisms such as voting receipts and digital envelopes are implemented.
- Generation of the information needed to verify the results of the election by the voter. Voter verifiability allows voters to verify the presence of their ballots in the final tally, but not their contents. The verifiability process is further described in Section 5.

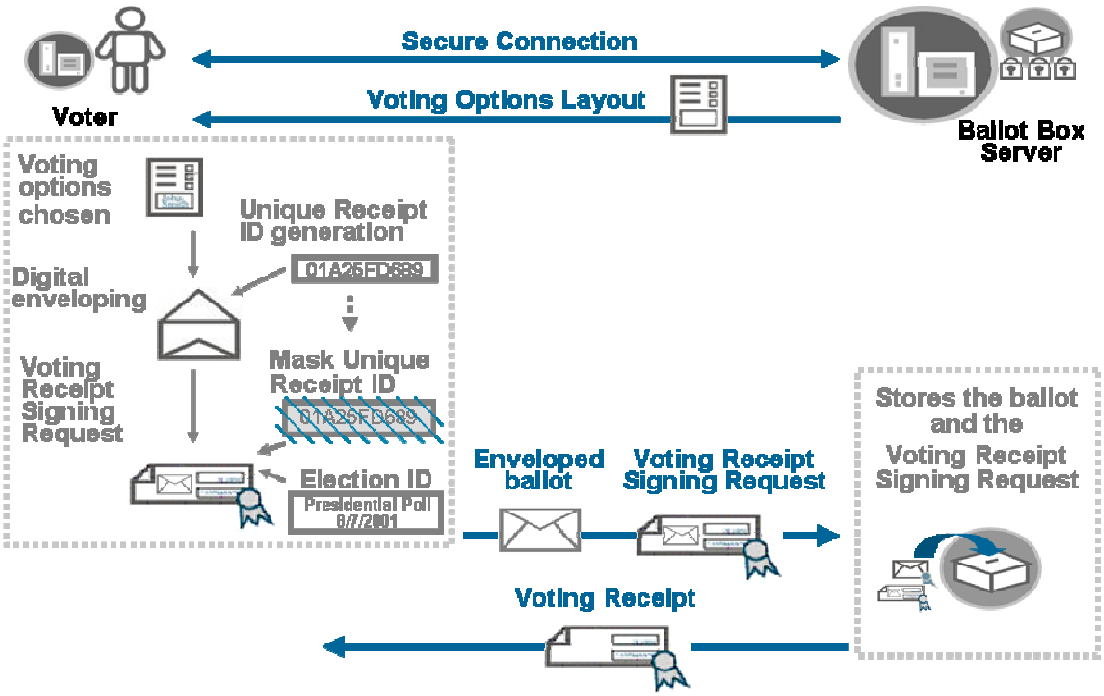

Figure 4: Ballot casting protocol

Figure 4 depicts the main steps of the Pnyx.core ballot casting protocol (i.e. the cryptographic operations involved in casting a ballot, performed both by the voting

client platform and by the corresponding ballot box server). A brief description of the processes and elements involved in each step of the protocol follows:

- **Secure connection -** To achieve communications security, the ballot casting protocol is tunneled through a secure connection (most probably at transport level, such as SSL). This initial step allows authentication between voters and the voting front-end, and establishes an authenticated and confidential channel between them.
- **Voting options layout -** The ballot layout is received from the server platform, jointly with an election ID and opening token, and it is displayed on the client platform. After the voter has filled the ballot (which could include open-ended questions or write-in candidates), the protocol proceeds.
- **Verification of the voting options -** Before cast the vote, the voter is required to verify the options selected. This process is done in a client module independent from the vote selection platform. For instance, the selection can be implemented through an Internet browser and the verification and subsequent steps are implemented in a digitally signed applet. The client module shows a summary of the selected options to allow the voter to verify that they represent the voter intent. If the voter rejects the voting options (possibly because she wants to correct any of the voting options), the voting process returns to the previous step (i.e., selection platform) to allow the voter to make changes. If the voter accepts, the voting process continues in the client module.
- **Enveloping the ballot -** A unique receipt identifier is generated by Pnyx.core client module. This unique identifier is generated using a random number (possibly generated with the voter's collaboration) and the election identifier. After generating the unique receipt identifier the client module protects this identifier and the selected voting options by means of a digital envelope. This digital envelope is created using a symmetric random key (3DES) to encrypt the information and the asymmetric public key of the Electoral Board (RSA) to

encrypt the symmetric random key. As the private key was split among the members of the Electoral Board through a secret sharing scheme (see Section 3), this digital envelope cannot be opened (i.e., the symmetric random key decrypted), since the requisite key does not exist. The use of a digital envelope using a random asymmetric key provides semantic security to the vote encryption, preventing that votes with the same selected voting options could generate the same cipher-text. Therefore, it is not possible to verify if two voters vote for the same options or to discern the vote of a voter, based on the value of the cipher-text (i.e., comparing vote cipher-texts among them).

- **Attaching a proof of authenticity to the enveloped ballot -** The client module masks the unique receipt identifier and concatenates the masked information with the digital envelope and voting data (such as an election ID, opening token, or other administrative data). A receipt signing request is generated by digitally signing the concatenated data using the voter private key. This digital signature protects the integrity and authenticity of the whole vote and receipt information. Finally this receipt signing request and the digital envelope are sent to the ballot box server.
- **Validated voting receipt -** The ballot box server checks if the digital signature of the receipt signing request corresponds to the digital envelope, and verifies if the voter has the right to vote. If these checks are successful, the vote and receipt signing request (i.e., its digital signature) are stored at the digital ballot box, and a validated receipt is issued to the voter by the ballot box server. This validated receipt is generated by means of digitally signing the masked unique receipt identifier included in the receipt signing request. Since the ballot box server is signing the masked information, it is not able to discern the real value of the receipt identifier. The validated receipt is returned to the voter. The digital signature from the ballot box is verified. If this signature is correct (i.e., correlated to the receipt identifier) the receipt identifier and digital signature from ballot box server is shown to the voter, who can print them as a voting receipt. This receipt is useful to prove that the vote has been effectively

cast by the voter (see Section 6). Ballots are stored by means that prevent their loss by power failures, or similar incidents.

5 Mixing Protocol

At the end of the voting process, the ballot box servers close the acceptance of new votes and digitally sign their ballot boxes. Ballot boxes are transferred using an air-gapping approach (i.e., using a removable storage media) to the host where votes will be decrypted using the Mixing protocol.

The main goal of the mixing protocol is to ensure that the ballots are properly decrypted and taken into account, without compromising the privacy of voters (i.e. to ensure that the correlation between each voter and her vote is properly prevented). Two processes are implemented to accomplish this goal:

- **Ballot box integrity control –** The first step before start the decryption of the votes (ballot Mixing) is to check the authenticity and integrity of the ballot boxes and its contents. The digital signature of the ballot box is then validated to verify that has been issued by a valid ballot box server and remain intact. After this, digital signatures of the votes (receipt signing requests) are checked against the digital certificates of eligible voters and the signed contents. Incorrect votes (i.e., votes that do not pass the digital signature check) are reported and separated from the valid ones.
- **Reconstruction of Election key –** The second step is to reconstruct the election private key using the shares of the Electoral Board. As described in Section 3, this key was split into several secret shares and distributed among the Electoral Board members. The key is destroyed during the splitting process. To proceed with the key reconstruction, a minimum threshold of Electoral Board members must be present and contribute with their shares.

- **Ballot mixing –** Once the private key is reconstructed, valid ballots are uploaded into memory and their digital signatures detached. After this, a random number permutation is generated and applied to the memory stored votes, randomly shuffling their positions. The private key is used then to decrypt the votes. Vote decrypted contents (excluding the receipt identifier) are then stored in disc (e.g., database or XML file) and eliminated from memory. A second random permutation is calculated and applied to the information remaining in memory: receipt identifiers. Finally the receipt identifiers are stored in the disc in a different file o database. This second shuffling is done to prevent the correlation between the decrypted votes and the voting receipts.
- **Results sealing –** Finally, the Electoral Board digitally signs the list of decrypted votes and the list of receipts identifiers. Therefore, the integrity and authenticity of both lists can be validated at any time before tallying the results of implementing parallel recounts. The private key is destroyed again. Both lists are transported to the tallying application using again an air-gapping approach.

The mixing protocol does not need any information about the ballot format, and therefore, it is independent of the ballot layout and contents, greatly improving its ease of integration into pre-existing e-voting environments (i.e., supports any complex election selection rule such as preferential voting or write-in options). The tallying and publishing of the election results are not part of Pnyx.core's functionalities, and must be implemented by the election platform, such as Scytl's Pnyx.government or Pnyx.labour.

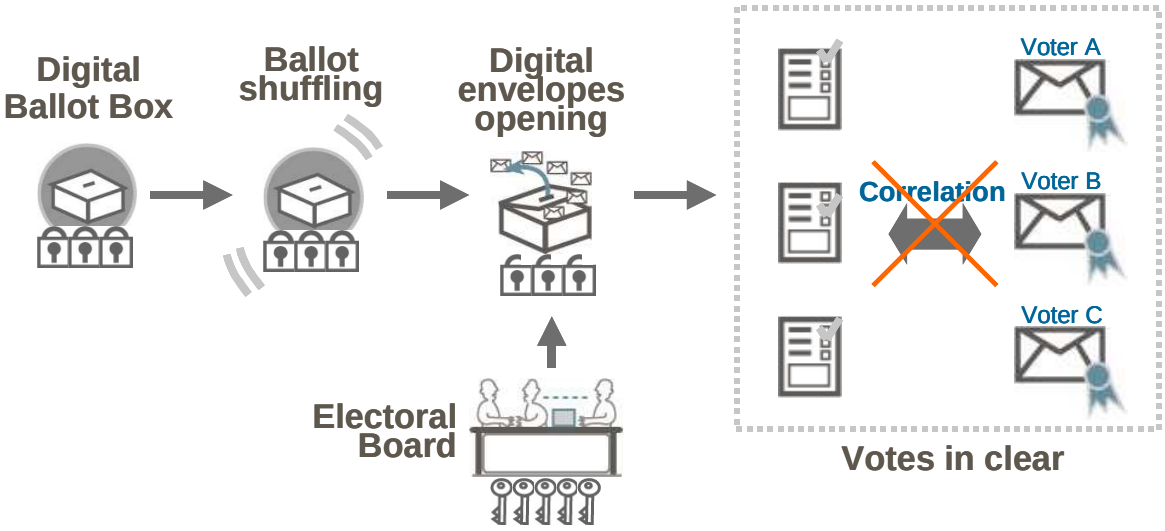

Figure 5: Mixing protocol

Figure 5 depicts how the Electoral Board private key, reconstructed from the shares kept by its members, allows the mixing server to open the inner digital envelopes that protect ballots. An additional shuffling process is performed on the ballots, to prevent correlation between enveloped ballots and the resulting disclosed contents.

6 Verification Protocol

The Pnyx.core e-voting framework ensures that digital ballots cannot be manipulated. Because political parties and authorities generally have divergent interests, the collusion of the members of the Electoral Board is very unlikely (such boards are used in traditional voting environments). Pnyx.core provides the further means to verify the published election results by the voters themselves. In this way, the electorate's trust in the fairness of the electronic electoral system is greatly improved since each voter is able to independently verify her particular ballot.

Furthermore, individual verifiability can also identify (even small) manipulations of the tally, even if only a tiny percentage of voters actually verify their own ballots. A few examples may serve to illustrate the effectiveness of individual verifiability to detect general manipulations of the election results: In an election with 2,000 ballots cast, only 30 voters are required to verify the presence of their own ballots on the tabulated results in order to achieve a more than 90% probability to detect a manipulation of just 150 ballots. If the number of voters that verify doubles (that is, just 60 voters), the probability of detection rises to more than 99%. In an election with 40,000 ballots cast and a manipulation of just 1% of them, the chances of detecting the manipulation are more than 90% if just 230 voters verify. If 2% of the voters verify their ballots, the same manipulation is detected with a probability of more than 99.9%.

The verification protocol implemented by Pnyx.core allows voters to verify that their ballots indeed reached the proper electoral authorities (this is the verifiability level found in conventional elections). This voter verifiability needs the unique ballot ID, generated during the ballot casting protocol, and the ballot verifiability list, generated during the mixing protocol, to perform the verification process.

With this kind of verification, the voter can check that her particular ballot has been an input to the tallying process. The voter looks for her ballot ID on the verifiability list, which includes the entire ballot IDs belonging to correct ballots.

To avoid compromising the voters' privacy during the verification process, this is performed on the client side. To this end, the voting agent downloads a subset of the verification data list and the voter locally checks it. In this way, the receipt identifier is never disclosed to the publishing server.

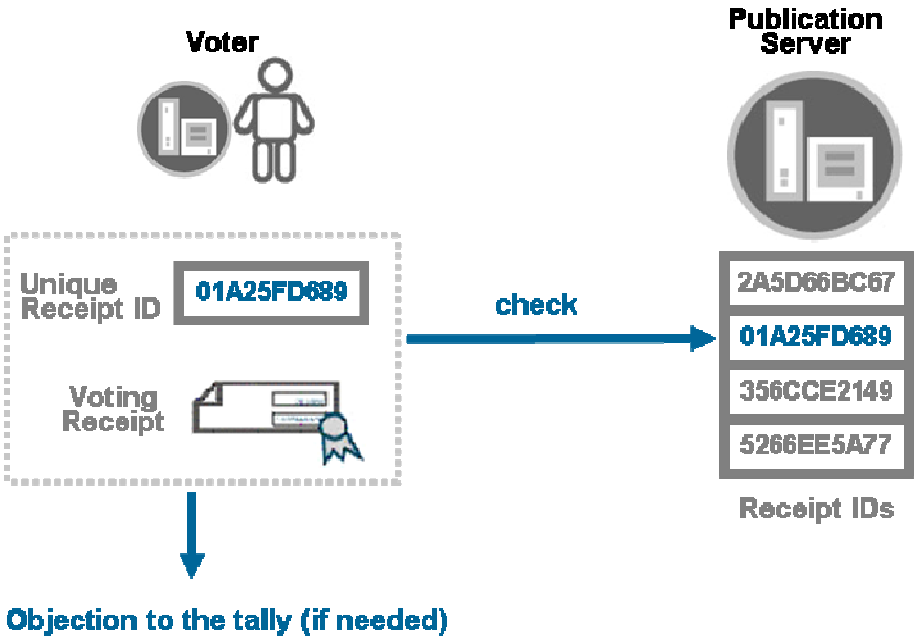

Figure 6: Verification protocol

In case a voter detects any problem, she can issue a public objection using the voting receipt. Such objection does not compromise the voter's privacy since the ballot contents are not needed to verify its validity.

The main steps of the verification protocol are depicted in Figure 6. The voter looks for her ballot ID in the published results (downloading the verification list from the server), verifying in this way that the Electoral Board has effectively processed her ballot.

7 Immutable Logs

In addition to the cryptographic protocol used to preserve the voter privacy and election accuracy, Pnyx.core also implements cryptographic measures to preserve the integrity and authenticity of election logs. During the voting period, all the election

transactions are registered and cryptographically chained to preserve the log integrity at log entry level. Periodical checkpoint signatures are also generated to preserve the log authenticity and non-repudiation.

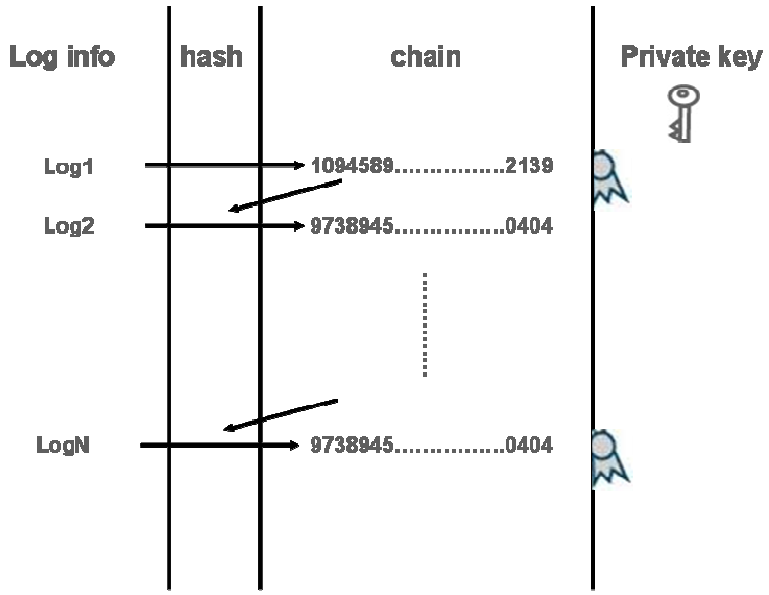

Figure 7: Log chaining

Figure 7 shows how this process is implemented:

- **Log entry chaining –** Each log entry is chained with the previous one using a hash function. Therefore, if any log entry is manipulated or deleted the chain verification will file in the place were the manipulation is done.
- **Log checkpoint –** Every configured number of lines or time, a digital signature of the last chain is generated. Therefore, any log entry manipulation attempt will invalidate the digitally signed section where this entry was located. Isolating the suspicious log entries from the valid ones.

The main advantage of immutable logs, compared with digitally signed logs, is that allow locating the situation of any manipulation attempt and isolating this from the rest of the log entries that remain intact. A manipulation in a digitally signed log invalidated the whole log.

8 Pnyx.core

Pnyx.core is a component framework that powers e-voting application platforms with the functionalities needed to address the security requirements and concerns of an electronic voting process. These components are deployed on the different elements of the platform (ballot box server, tallying server, publishing server and voting client platform) providing them with the adequate cryptographic functionality. Pnyx.core does not interfere with the entire process of the e-voting platform (e.g. the mixing protocol does not tally the results) and it is designed to be highly independent of the platform implementation technology. This eases the integration on existing platforms and facilitates the implementation of new ones. Scytl has developed several e-voting platforms on top of Pnyx.core, each one specialized on solving the issues related to different kind of electoral processes (public elections, referenda, e-consultations, union elections…), that implement the functionalities not covered by Pnyx.core, like the tallying process or the voting front-end.

Once Pnyx.core is integrated on an electronic voting platform, the implemented protocols breakdown the electoral voting process into the following phases:

- **Configuration** Before starting the election process, some configuration of Pnyx.core must be carried out: definition of the Electoral Board (creation of members' secret shares), generation of an unique election identifier, election schedule definition, creation of the electoral roll PKI information, definition of the verification type, etc. After the Electoral Board is registered, the

configuration processes are reviewed and certified by its members before proceeding with the election.

- **Opening the election -** The Electoral Board certifies the opening token that must be installed in the ballot box servers in order to start the voting period.
- **Ballot casting supervision -** During the voting period, the platform administrators must handle any incident detected by them or reported by voters. A number of logs, with security controls, are generated to facilitate problem detection and solving.
- **Closing the election -** The Electoral Board certifies the closing token that must be installed in the ballot box servers to stop accepting new ballots. New voters are rejected, whereas voters that have not completed the voting process can proceed until a predetermined timeout expires.
- **Collecting digital ballot boxes -** Ballot boxes are collected by the Electoral Board for mixing their contents.
- **Mixing the ballots -** The ballots are extracted from the ballot boxes and their consistence is checked to detect invalid ones. Afterwards, correct ballots are securely mixed and the list of the valid votes with the corresponding verification data is issued.
- **External auditing -** Pnyx.core provides enough log information and security controls (due to its cryptographic features) to allow exhaustive external auditing of the election process. Digitally signed voting receipts can be printed and used as a paper-based trail that, in conjunction with the physical security implemented on the mixing server, may serve as the basis of recounts and audits without losing information integrity, privacy or reliability.

The Electoral Board supervises the main security functions of the voting environment and controls the whole process. Any configuration parameter or critical operation of the Pnyx.core components (e.g. opening the election) must be reviewed and certified by the full coalition of the members or a qualified majority of them. Technical administrators can monitor the performance of Pnyx.core to detect and respond to

any incident. To this end, a number of reliable logs are generated by Pnyx.core components, easing the system's monitoring and auditing. Technical administrators have limited privileges and cannot modify Pnyx.core's configuration without the Electoral Board's intervention.

During the configuration phase, the concrete electoral requirements of current election are defined. In this stage, important information (e.g. secret cryptographic shares) is generated and distributed among the election authorities. The configuration of Pnyx.core basically deals with the following items:

- **Electoral Board -** Definition of the digital identities of the members of the Electoral Board, and distribution of cryptographic data among them.
- **Election information -** Definition of the unique election identifier and of the election scheduling.
- **Electoral roll -** Identification data and PKI data of the set of voters that will participate on the electoral process. Depending on the election requirements, other specific Pnyx.core information for the voters (e.g. coercion codes) could be included.

Due to the cryptographic nature of the protocols, Pnyx.core implementation requires that voters and electoral authorities are provided with digital certificates. Pnyx.core therefore assumes the existence of an electoral roll and also of a PKI to issue these inputs. These components are not part of Pnyx.core and must be externally provided (for instance, Pnyx.government includes its own PKI). From them, Pnyx.core can extract the internal electoral roll PKI information (basically, every voter's certificate) and can request the certificates needed from the election authorities. All the cryptographic functions implemented by Pnyx.core need of such certificates to proceed. Nevertheless voters do not need to manage their private key; every private key can be protected by means symmetric cipher with a strong password and stored in the Ballot Box Server. This password only must be owned by the voter. When the

voter starts the voting process then the protected private key is downloaded from the Ballot Box Server. The voter introduces his password and the downloaded private key can be used to cast the ballot. This method makes it impossible to use the voters' private keys without their passwords. All this process is transparent to the voter, and avoids the drawbacks related to installing the private keys and digital certificates on the voting client platforms.

Figure 8 depicts these external data sources, and the Pnyx.core components integrated into the electronic voting platform providing a suitable cryptographic framework. They must be integrated on client and server sides to allow the fulfillment of the electoral security requirements. External components such as the Electoral Roll and a PKI are needed to provide the suitable digital certificate data for voters and electoral authorities.

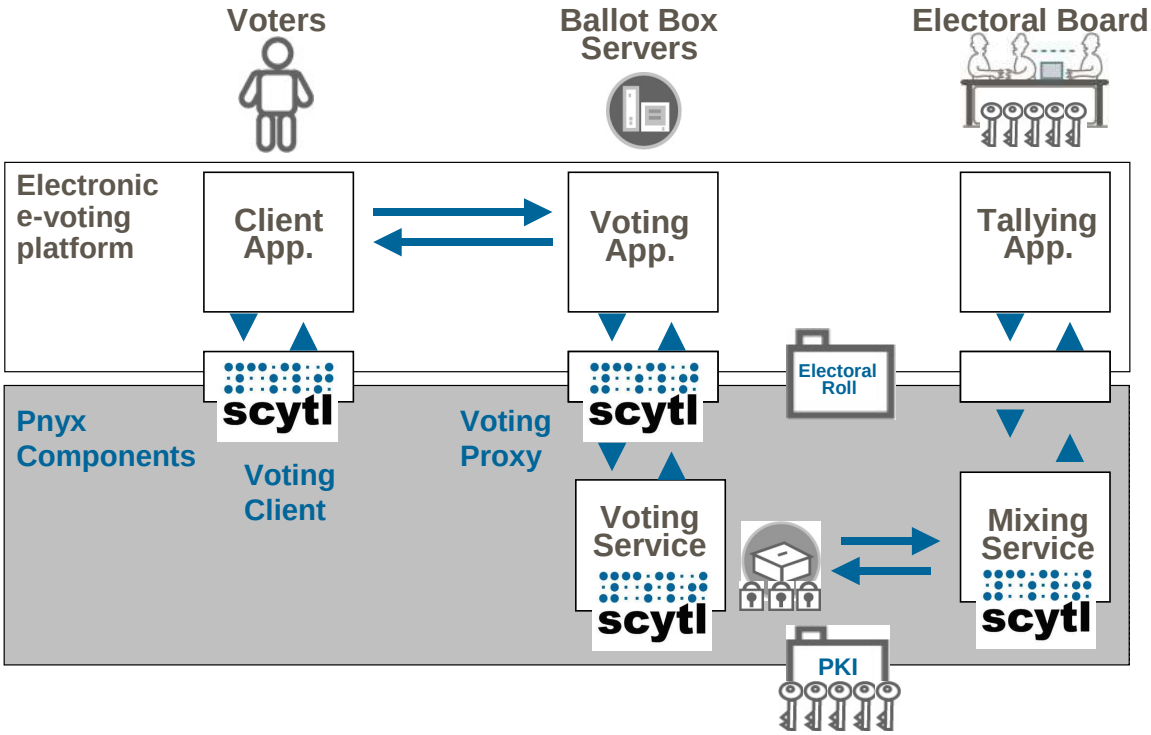

Figure 8: Integration of Pnyx.core

7 Security Analysis

Pnyx.core empowers electronic voting systems with the technical means needed to fulfill the requirements posed by electoral processes. This section discusses the suitability of the cryptographic components to achieve this task.

Strong authentication of voters and authenticity of ballots - Scytl technology uses the most advanced digital identity techniques in order to authenticate voters. Digital certificates and strong authentication protocols are currently the most adequate authentication technology for remote voting. Biometrics will be incorporated in the future. In the case of poll-site voting systems, the conventional identification mechanisms already in place are the proper way to authenticate voters. Ballot authenticity is ensured through digital signatures. As mentioned, the use of digital certificates and private keys can be transparent to the voter; she only needs to manage her own password.

Privacy of voters - The privacy of voters is paramount in any election. Pnyx.core ensures the privacy of voters by means of digital envelopes and cryptographic techniques to mask voting receipts before the ballot box server validates them. Only the full collusion of members of the Electoral Board (or a qualified majority of them) is able to open the digital envelopes that protect the ballots. This action is done in the context of a secure mixing process that ensures that no correlation is possible between the voters and their votes in clear. Physical security is used to maximize the protection of the mixing process.

Accuracy of election results - Every outer digital envelope contains a proof of authenticity that may be linked to the corresponding voter. This proof of authenticity prevents the modification of ballots and the addition of invalid ballots (e.g. on behalf of abstaining voters). The mixing process, performed on a secured and audited site operated by the Electoral Board, leaves no further opportunity to manipulate the ballots.

Secrecy of intermediate results - The digital envelopes that protect voters' privacy offer also adequate protection to ensure secrecy of intermediate results, if needed.

Verifiability of ballots - The publication of election results including ballot IDs partly chosen by the voters themselves, gives them complete confidence that the Electoral Board has processed their ballots during the mixing protocol. In case of the detection of any problem, voters are able to complain by publicly showing the corresponding voting receipt. The design of the voting receipts ensures that such complaints do not reveal the actual voting options chosen.

Uncoercibility - Pnyx.core is prepared for handling coercion codes in order to remove the possibility of individual coercion in case of remote voting systems in which voters cast their ballots from environments without direct supervision of electoral authorities. In addition, the use of voting receipts for verifiability purposes does not facilitate massive coercion or vote-selling since the receipts do not give proof of the chosen voting options.

8 Conclusions

Scytl's cryptographic e-voting framework has been designed to ensure a smooth transition from conventional electoral systems to electronic (possibly networked)

ones. The use of the framework described in this document by computerized voting platforms makes them trustworthy, auditable and verifiable.

Pnyx.core, the software product that implements Scytl's patented e-voting framework, has been implemented as a set of highly flexible software components to enable a painless integration into any electronic voting system. These software components are integrated with the different elements that constitute the voting system, to implement election preparation, ballot casting sessions, ballot mixing and the verification of results. Scytl has developed several complete e-voting systems on top of Pnyx.core.

9 About Scytl

Scytl Secure Electronic Voting S.A. (Scytl) is a highly specialized software company that commercializes the most secure e-voting voting solutions currently available. These solutions incorporate unique cryptographic protocols that enable to carry out all types of electronic voting processes or elections in a completely secure and auditable manner. Scytl's advanced e-voting security technology positions the company as a leader in the e-voting industry.

Scytl was formed as a spin-off from a leading research group at the Universitat Autònoma de Barcelona. This group, funded by the Spanish Government's Ministry of Science and Technology, has pioneered the research on e-voting security in Europe since 1994 and has produced significant scientific results, including 25 scientific papers published in international journals and the first two European Ph.D. theses on electronic voting security, by Prof. Joan Borrell and Scytl's founder Dr. Andreu Riera (in 1996 and 1999, respectively). This research group also participated in the first Internet binding election in Europe (i.e., the 1997 election to the Presidency of the IEEE IT Spanish chapter).

One of Scytl's main strengths is its unique technology, which derives from over ten years of pioneering R&D and is protected by a portfolio of international patents. The groundbreaking e-voting cryptographic protocols developed by Scytl provide e-voting with the highest levels of security, in terms of anonymity, urn integrity, and voter-verifiability. This innovative technology has received numerous international awards, including the prestigious IST Prize granted by the European Commission in 2005.

Scytl has customers both in the private and public sectors. The former are local, state (regional), and federal governments which license Scytl's e-voting products to carry out their elections, referenda, or citizen consultations by electronic means. The latter are large corporations and organizations that choose Scytl's technology to carry out by electronic means electoral/consultation processes such as labor union elections or shareholders' meetings. Some of these customers represent leading references in the electronic voting industry (e.g., governments in Spain, Switzerland, Argentina, Finland and Australia that are pioneering new electronic voting applications). Scytl's products have already been successfully used in multiple projects worldwide, some of which represent breakthrough projects for the electronic voting industry.

Tuset 20, 1-7
08006 Barcelona
SPAIN

tel:. +34 934 230 324
fax: +34 933 251 028

http://www.scytl.com