scytl

Secure Electronic Voting

Pnyx.VM

Auditability and Voter-Verifiability for Electronic Voting Terminals

scytl
Secure Electronic Voting

Pnyx.VM

Auditability and Voter-Verifiability for Electronic Voting Terminals

White Paper

The electronic voting security system described in this document is protected by international patent applications

http://www.scytl.com

TABLE OF CONTENTS

Executive Summary

Direct Recording Electronic voting terminals, also known as DRE voting terminals or DREs, are designed to record and store votes entirely in electronic form, so there is no physical record of each vote. The main advantages of these terminals are the prevention of unintentional voting errors and the increased accessibility for people with disabilities. These and other advantages have favored their progressive introduction into polling places. However, recent incidents that have arisen have called their security and reliability into question. Criticisms concerning the lack of voter verification mechanisms or the auditing and certification difficulties arising from the complexity of the DRE voting terminals require solutions to increase confidence in such terminals.

This document describes a solution to the fundamental problems that may lead to misgivings concerning the use of DRE voting terminals. This solution enables voters to verify that their votes have been cast and recorded correctly and provides the necessary means to guarantee a safe democratic process. The proposed solution is based on the combination of a simple and secure hardware component, which we call the verification module, and a cryptographic protocol.

The verification module provides voters with a secure and reliable environment in which they can verify that their votes are cast correctly. This module is a simple hardware device connected to the DRE voting terminal. This device is composed of a screen, an audio output and two buttons to facilitate interaction with the voter. Once the voter has selected the voting options in the DRE voting terminal, these choices are sent to the verification module where the voter can verify them. Such verification is carried out visually, or with a headset connected to the audio output of the module. The module buttons enable voters to decide whether they wish to cast their vote or to return to the DRE voting terminal to make changes.

The cryptographic protocol implemented by the verification module protects the privacy and integrity of every single verified vote. The operations for the protection of the votes are carried out in the verification module once the voter confirms the casting of his/her vote. These operations consist in the sealing of each vote by means of a digital envelope that is digitally signed with the private keys installed in the verification module. These private keys are managed by the members of the Electoral Board who may belong to the different political parties involved in the electoral process. Additionally, the decryption key needed to open the digital envelopes is distributed in shares among the members of the Electoral Board. The digitally signed envelope containing the vote is sent from the verification module to the DRE voting terminal and a copy is kept in the verification module itself. The tabulation of the votes consists in the reconstruction of the decryption key with the shares in possession of the members of the Electoral Board, and the opening of the digital envelopes by a mixing process. The use of mixing techniques guarantees the privacy of the votes retrieved, thus preventing any correlation between the clear-text votes and the order of arrival of the voters. The authenticity and integrity of every single vote included in the tabulation process can be verified by checking the digital signatures on the digital envelopes. These signatures ensure that every counted vote has been previously verified by the corresponding voter.

The solution proposed in this document facilitates the audit of the election, since it allows to focus the auditing efforts on the verification module which is a much simpler device than the DRE voting terminal. This reduces the difficulty, time and overall costs of auditing the election. Furthermore, the individual voter verification and the cryptographic protection measures ensure the detection of any eventual irregularities in the DRE voting terminals during the election.

Finally, should any doubt about the validity of votes recorded in the DRE voting terminals arise, the solution proposed herein enables the electoral authorities to carry out a parallel vote recount, independent of the results of the DRE voting terminals, from the votes encrypted and stored in the verification modules as a backup.

A Brief History of Poll-site Voting Systems

The first instance of mechanization of electoral processes was with the appearance of the voting lever machines, invented by Thomas Edison. Voters cast their votes with these machines by operating the lever corresponding to the candidate for whom they wish to vote. After drawing the curtain behind which voters vote in secret, the levers return automatically to their original position so that no trace of the votes previously cast remains when subsequent voters enter the booth.

The first systems of electronic vote counting based on punch cards appeared in the state of Georgia (USA) in 1964. With these systems, voters select their voting options by punching in the appropriate place on the ballot card. Voters then deposit their punch cards in a ballot box, and when the election is over the cards are introduced into a computerized counting device.

With the introduction of technology such as mark sense devices, and particularly of optical scanners, new methods of electronic vote counting appeared. This technology enables voters to select their voting options by filling out circles or other shapes on a special ballot paper. As in the case of punch cards, the ballot papers are deposited in a ballot box and when the polling station closes the votes are counted by a computerized device.

However, it was not until the appearance of Direct Recording Electronic voting terminals (also known as DRE voting terminals or DREs), that one could properly speak of a totally electronic voting system. These DRE voting terminals are capable of directly recording and storing votes electronically, so there is never a physical record of each vote. One could say that this system constitutes a replacement by electronic means of former methods of voting by lever machines. With the DRE voting terminals, voters cast their votes by means of a touch screen or push-buttons. Once the voter has made his/her selection, the votes are stored in the electronic memory of the terminal. The votes can later be counted in the terminal itself or sent to a counting center by means of a removable memory device or a communication channel.

A More Detailed Analysis of DRE Voting Terminals

The introduction of DRE voting terminals was welcomed with enthusiasm in countries such as the United States, the Netherlands or Brazil. Situations such as those arising in the 2000 U.S. Presidential election, where errors generated by punch card and optical scanning systems gave rise to much controversy about the final outcome of the election, have since then favored the use of this type of voting terminals. At present, almost a third of the U.S. population uses DRE voting terminals, while in the Netherlands and Brazil the percentage is already 95% and 100%, respectively.

DRE voting terminals solve many of the problems caused by previous voting systems. Firstly, DRE voting terminals prevent the loss of votes caused by unintentional errors when votes are cast (i.e., undervoting and overvoting). A further important advantage of DRE voting terminals is the increased accessibility for people with disabilities, such as the visually impaired. Such voters can use a headset connected to the DRE voting terminal to cast their votes without the assistance from a third party, thus ensuring voting privacy. Finally, the vote counting process with DRE voting terminals is faster and more accurate since ballots are processed directly in electronic format and no physical reading of votes (for example, by scanner) is necessary.

Despite the significant advantages of DRE voting terminals, recent studies on their potential security deficiencies have given rise to misgivings about their reliability. Additionally, the lack of transparency regarding the internal functioning of these terminals has considerably increased the doubts about the security and integrity of this voting system.

In what follows, we describe the main criticisms leveled at DRE voting terminals in greater detail.

One of the criticisms most commonly heard is the lack of transparency of the electoral process for the voters. In a system based on physical voting (e.g., paper ballots), voters can be sure that their votes have been correctly cast because they themselves introduce the paper ballots into the ballot box (however, it is important to note that voters do not have any direct assurances that their votes will be correctly counted and, therefore, they have to place trust on third parties). On the other hand, in a process based on DRE voting terminals, voters do not have the visual means of assuring that their votes have been properly cast and recorded since voting is carried out electronically. For this reason, it is important to provide voters with a mechanism that enables them to verify that their electronic votes have been correctly cast and stored.

Another criticism concerns the auditing restrictions of these terminals. In many occasions, it is not possible to openly audit the code that is being executed in the voting terminals, since the code is protected as a trade secret. Furthermore, should suspicion of irregularity arise in the election results, this type of system provides no possibility of a parallel recount of votes independent of the results of the DRE voting terminals. Such drawbacks often require a blind faith in the correct functioning of the DRE voting terminals.

Other criticisms refer to the complexity of the certification process for these terminals by the electoral authorities. DRE voting terminals are complex devices that carry out all the functions in the voting process: configuration and display of the voting options, selection and confirmation of the desired options, and casting and counting of the votes. This complexity makes hidden irregularities (unintentional or otherwise) in the DRE voting terminal code difficult to detect. Furthermore, it is necessary to guarantee that the integrity of the system remains intact even after being audited, without coming into conflict with the manufacturers' intellectual property rights. Last minute changes in the configuration (one of the advantages of this system) make the certification process even more difficult since these changes must be tested and certified quickly so that they can be reliably applied in the voting terminals.

Finally, the measures of internal security implemented by these terminals have also come in for criticism. In occasions, these security measures have been proven to be insufficient and unsatisfactory to guarantee the security of the electoral process.

Later in this document, we present a new proposal to solve all these problems.

Previous Security Solutions and their Deficiencies

With the objective of addressing the criticisms described in the section above, experts and researchers in security have developed methods for guaranteeing the necessary security for DRE voting terminals.

A first set of solutions proposes to keep a parallel printed record of the electronic votes. The main objective of this solution is to enable voters to verify that their votes have been correctly cast while keeping a physical record of those votes after they have been verified. With this type of solution, voting options are displayed on the DRE voting terminal screen and, after the voter makes his/her selection, the selected options are printed out on paper. Voters may then check that the options on the print-out correspond to the choices they selected on the DRE voting terminal. If this is the case, the vote is recorded electronically and the print-out is also stored in a physically protected ballot box. When the period for casting votes is over, the accuracy of the results based on the electronic votes stored in the DRE voting terminals can be checked by carrying out a manual recount of the paper ballots stored in the physically protected ballot boxes.

Although the solution described above allows voters to verify the correct casting of their votes, it presents several problems. This solution does not allow visually impaired voters to verify their votes. Moreover, with this system it is not possible to identify the sources of discrepancy in those cases where the count of paper ballots does not agree with the count of electronic votes. In other words, it is not possible to determine whether the correct result is given by the paper ballots, the electronic votes or neither of the two. It would not be prudent to always assume by default that the paper ballot count is the correct one since paper ballots can be physically manipulated (e.g., addition of non-authorized votes, subtraction of valid ones, etc.).

A second set of solutions consists in emulating paper ballots by using removable memory devices (e.g., smart cards) in which copies of the electronic votes are stored. These cards are also stored in a physical ballot box to enable a parallel recount of the votes. This solution is implemented through a modular architecture that separates in two different systems the voting option selection process from the vote casting process. The selection process is carried out in the DRE voting terminal, which records the options selected by the voter in the removable memory device. The vote casting process is carried out in the vote casting terminal, which has a physical ballot box where the memory devices with the votes cast are deposited and stored. In this second terminal, voters can verify the contents of the memory device (i.e., their votes) before casting them. This proposal, in contrast with the former one, enables visually impaired voters to verify their votes. In addition, the modular architecture of this proposal also offers the important advantage of simplifying the audit of the overall system since the audit of the vote casting terminals is sufficient to detect any tampering with the DRE voting terminals. Nevertheless, this system is not entirely free of drawbacks. For example, the use of removable devices may facilitate vote selling or coercion, since voters could reveal the contents to third parties before casting their votes. Furthermore, the system shares some of the problems of systems based on paper ballots, such as manipulation of physical votes (cards) in the ballot box or the inability to detect the sources of discrepancies in a parallel vote recount.

A final set of solutions is based on the use of cryptographic tools to generate voting receipts that enable voters to verify that their votes have been cast in accordance with their choice. The main advantage of the use of cryptographic protocols resides in the fact that they allow voters to verify not only that their votes have been recorded correctly in the voting terminal but also that these votes are present (and unaltered) when votes are finally tabulated. Although these methods in theory provide efficient protection for the integrity and privacy of the electoral process, in practice their security depends to a large extent on the security of the system (usually, the DRE voting terminal) in which they are executed. In addition, in some of their implementations, they offer an excessively complex and sophisticated solution for both voters and election authorities, since the structure of the voting receipts and the cryptographic mechanisms that ensure their authenticity are not easy to interpret. In some other implementations, they are difficult to put into practice because of the necessity of using sophisticated equipment for the generation and verification of these receipts. Finally, there are certain implementations which can cause problems regarding voting privacy and vote selling if the security measures of the systems protecting the codes used for generating receipts are not sufficiently robust. Such drawbacks make it difficult for these methods to be widely adopted in elections. In summary, although from a theoretical standpoint they represent sound solutions, from a practical point of view, the usability of the system or its dependency on the security of the environment in which it operates render viability difficult.

The following section describes a new solution that significantly reduces the complexity in the audit of the DRE voting terminals and that enables voters to verify the correct casting of their votes. The proposed solution also implements the security measures necessary for guaranteeing the integrity and privacy of every single vote.

Pnyx.VM: A Cryptographic Solution Based on Verification Modules

General Description

As described in previous sections, in an election based on DRE voting terminals voters select their voting options, confirm these options and cast their votes in the same voting terminals. The votes cast are stored in the terminal itself until the vote counting process is over, there being no second record of votes. Consequently, much of voter confidence in the integrity of the election depends on the integrity of these terminals. Likewise, candidates and election authorities are forced to trust to some extent the inner workings of those complex systems.

The main objective of the solution proposed in this section is to generate this confidence without having to depend on the integrity of the DRE voting terminals, providing voters with a verification mechanism of the correct casting of their votes and facilitating the task of the election auditors. To this end, the proposed solution combines the use of a secure physical module, which we will call the verification module, and a cryptographic protocol that protects the digital images of the votes cast.

The verification module consists of a simple hardware device composed mainly of a screen, an audio output and two push-buttons (a “CONFIRM” button and a “CANCEL” button). The verification module enables voters to verify and confirm their votes before casting them. The device is also equipped with an internal memory for safely storing votes confirmed by voters, together with an integrity register of all these votes. Finally, the device has sufficient computing capability for the execution of the cryptographic protocol that protects the confirmed votes and fulfils the basic security requirements for electoral processes; that is, integrity of the results and voter privacy.

The verification module is connected to the DRE voting terminal to allow voters to verify that their desired votes will be accurately cast and recorded (see Figure 1). The cryptographic protocol implemented in this verification module protects every single vote against any potential manipulation afterwards (e.g., in the DRE voting terminal).

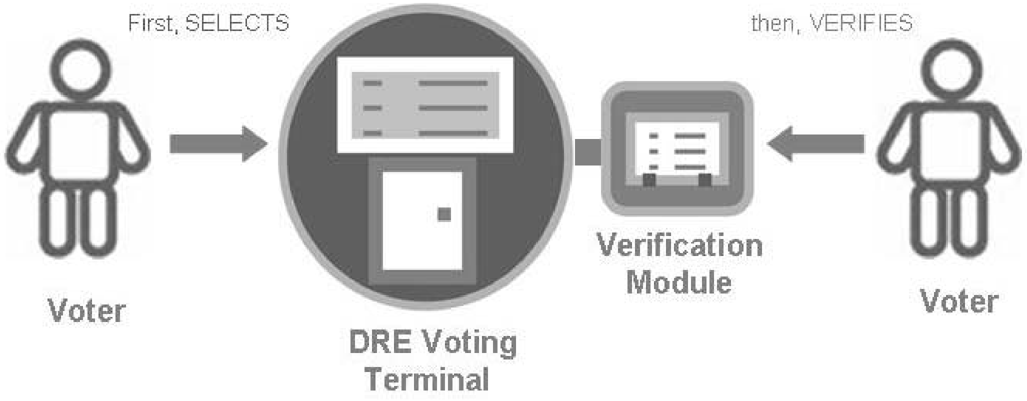

Figure 1. Voting Verification Process

Essentially, the voting process is as follows. First, the voter interacts with the DRE voting terminal, and after viewing the different options on the terminal screen he or she selects the desired voting options. Then the voter verifies visually, or with a headset connected to the audio output of the verification module, whether the options previously selected in the DRE voting terminal match those transferred to the verification module. If this is indeed the case, the voter confirms (with the “CONFIRM” button) the casting of the vote and this is protected by cryptographic techniques which will be described below. Otherwise, the selection process is restarted (with the “CANCEL” button) in the DRE voting terminal. Once the voting process is over, the votes contained in the DRE voting terminal are managed as usual, i.e., they are transferred to the place where counting is to be carried out (sometimes in the terminal itself).

The use of the verification module guarantees the integrity of the results without having to place any trust on the integrity and adequate operation of the DRE voting terminal. As a result, it is not necessary to extensively audit all the systems involved in the election. The audit of the verification module, which is a simple device, fulfils the same objectives as an overall audit. Since the operations carried out by the verification module are simpler than those carried out by the DRE voting terminal, the former is much easier to audit and certify than the latter. Furthermore, voters themselves play an important part in auditing, since while casting their vote they can verify whether or not the DRE voting terminal is behaving correctly. This feature contributes to increase voter confidence in the election process.

The cryptographic protocol implemented in the verification module protects the privacy and integrity of every single vote. The operations for the protection of the votes are carried out in the verification module once the voter confirms the casting of his/her vote. These operations consist in the sealing of each vote by means of a digital envelope, digitally signed with the private keys installed in the verification module. These private keys are managed by the members of an Electoral Board, the different political parties or by third-party auditors. Additionally, the decryption key needed to open the digital envelopes is distributed in shares among the members of the Electoral Board. The digitally signed envelope is sent from the verification module to the DRE voting terminal and a copy is also stored in the verification module itself. The tabulation of the votes consists in the reconstruction of the decryption key, using the shares in possession of the members of the Electoral Board, and the opening of the digital envelopes by means of a mixing process. The use of mixing techniques ensures privacy of the retrieved votes, avoiding any correlation between the clear-text votes and the order of arrival of voters. The authenticity and integrity of every single vote included in the tabulation process can be verified by checking the digital signatures on the digital envelopes. These signatures ensure that every counted vote has been previously verified by the corresponding voter.

Additionally, the verification module keeps a cryptographic integrity record of all the votes cast (the entire electronic urn). The existence of this record allows the verification of the accuracy of the results obtained in the DRE voting terminal count. The copies of the votes stored in the verification module also allow a parallel recount, should there be any anomalies in the voting process.

Below is described in greater detail each one of the components of the proposed solution and the functions carried out at each phase of the election.

Detailed Description

Architecture

As described in the previous section, the solution that we propose is mainly based on the addition to every DRE voting terminal of a simple and secure hardware device that enables voters to verify that their votes are cast correctly and that facilitates the audit of the election. This hardware device, which is called verification module, encrypts and digitally signs the confirmed votes and keeps a backup record of each one of them.

In addition to the verification module, two other modules are required to configure the verification modules and to recover the votes cast. These modules are known as the configuration module and opening module, respectively. A single configuration module and a single opening module can be used for a polling site or group of polling sites (or even an entire election) with several DRE voting terminals and their respective verification modules.

The parameters necessary for the correct configuration of the systems involved in the election are generated in the configuration module. The opening module is used to retrieve the contents of the encrypted votes and to carry out the necessary operations to ensure the accuracy of the results. These two modules are independent of each other, although it is advisable to integrate them into the same system in order to simplify the architecture of the solution. It is also necessary for both modules to be physically protected and easy to audit so that a satisfactory implementation of the protocol can be ensured. Figure 2 shows the different modules that integrate the proposed solution and their interaction.

The configuration module is used to generate the parameters required for executing the cryptographic protocols. One of the fundamentally important parameters for the security of the electoral process is the election private key, which is necessary to open the cryptographic seal (i.e., digital envelope) that protects every single vote and to carry out other critical tasks by the Electoral Board. This private key is distributed in shares among the members of the Electoral Board by means of a cryptographic secret sharing scheme. In this way, the election private key does not remain in the hands of one person only, but rather a predetermined threshold of Electoral Board members is required to obtain it. The configuration module requires no specific hardware, only a standard PC. As a security requirement, it must be a system entirely devoted to the execution of the cryptographic tasks, under the strict control and supervision of the Electoral Board and disconnected from any communication network.

The opening module is that in which the Electoral Board, at the end of the election, opens the votes that have been sealed by the verification modules. The need of a private key that has been distributed in shares among the members of the Electoral Board and the use of a mixing protocol in the tabulation process protect voter privacy by preventing the correlation between the clear-text votes and the order of arrival of the voters (i.e., their identities). As with the configuration module, the opening module does not require a specific hardware and the security requirements are the same as those for the configuration module, so both modules can exist side by side in a single system, thus maximizing the security and usability of the solution.

As stated before, the verification module is the easy-to-audit, secure environment where voters can verify their votes. Additionally, the operations to cryptographically protect the votes that will be subsequently checked and counted by the members of the Electoral Board and third-party auditors are carried out in the verification module. The verification module interacts with the DRE voting terminals through a simple connection via USB port or serial port. It is through this connection that the verification module receives the voting options selected in the DRE voting terminal by the voters and returns the confirmed and protected votes. The verification module has its own screen on which voters can verify the voting options received by the module. It is also equipped with an audio output to allow audible vote verification for visually impaired voters. The device has two buttons for voters to confirm if their voting options are correct; one to cast the vote (the "CONFIRM" button), and the other to abort the casting process and restart the selection process in the DRE voting terminal (the "CANCEL" button). It is also composed of a non-volatile memory for storing the votes cast, plus a register about ballot box integrity. This memory allows to keep a parallel record, independent of the electronic ballot box of the DRE voting terminal, which can be very useful during later stages of the election process. Lastly, the verification module also has a printer port that could be used to print receipts of votes (if required) as it will be explained later in this document.

Having described the system architecture, we can now consider the functions of each of the modules making up it.

Configuration

During the election configuration process, all the necessary cryptographic keys and digital certificates are generated. This process basically consists of the constitution of the Electoral Board and the configuration of the verification modules. Both processes take place in the configuration module previously described.

When the people forming the Electoral Board have been chosen, the election public and private keys are generated. One of the main duties of the Electoral Board is to jointly protect the secrecy of the private key. In view of the risk entailed by only one person taking charge of the private key, this is divided in shares immediately after its creation and destroyed, and the shares are distributed among the members of the Electoral Board. The division in shares is done by a cryptographic secret sharing scheme; that is, the private key cannot be known unless a number equal to or greater than a predefined threshold of Electoral Board members put their shares together. If this threshold is not reached, the information about the private key equals zero. Each share is given to a member of the Electoral Board in a physical device (e.g., a smart card) controlled by an access key (PIN) directly chosen by him/her.

Once the Electoral Board has been constituted, the parameters for the configuration of the verification modules are generated. This process consists in the generation of keys for each verification module, which are certified by the Electoral Board by using their election private key. Thus the authenticity of the keys for the modules is linked uniquely to the security of the election private key. The module keys are necessary to create proofs of integrity and authenticity of the data generated by the verification modules (e.g., encrypted votes). These proofs can be later verified by the political parties or third-party auditors.

When the configuration is completed, it is not necessary for the Electoral Board to intervene until the votes are counted. In the meantime, the members of the Electoral Board must securely keep their respective shares of the election private key.

Voting

Before the voting process itself begins (see Figure 3 for a graphic description), the configuration of the verification modules is checked to make sure that they contain the correct election information and that they have been duly initialized (i.e., all records are empty). Once this check has been carried out, the verification modules are connected to the DRE voting terminals.

The voter begins the voting process in the DRE voting terminal. The voter chooses his/her voting options as usual in this terminal, but once chosen they are sent to the verification module. This module displays the options on the screen (or alternatively they can be heard through the headset connected to the audio output) so that the voter can verify them in a secure environment. In this way, the voter can detect any error and can be sure that the vote that is going to be cast corresponds to the selected options. If the voter does not agree with the options shown, he or she can cancel the operation by pressing the “CANCEL” button and restart the selection process in the DRE voting terminal. If the problem persists, it means that there is some type of error affecting the correct functioning of the DRE voting terminal, which must be notified to the electoral authorities in order for them to adopt the appropriate measures. Note that notifying this problem does not threat in any way voters’ privacy (as opposed to what happens with the solutions that propose to keep a parallel printed record of the electronic votes).

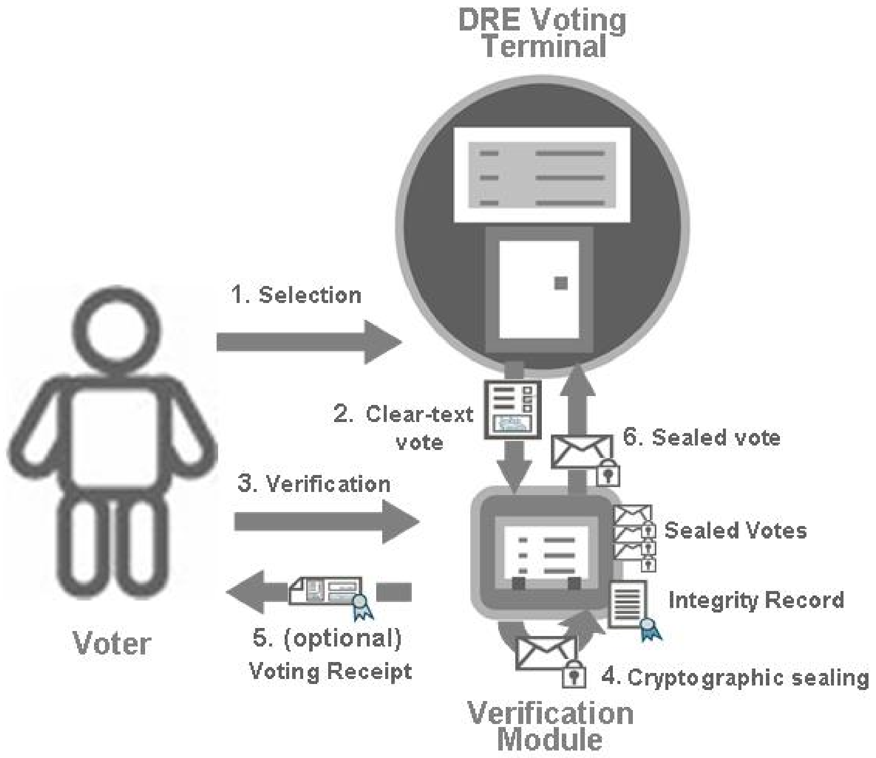

Figure 2. Steps in the Vote Casting Process

If the voter agrees with the options shown, the vote is protected and cast. First, the vote is cryptographically sealed by means of a digital envelope. The digital envelopes are created with the election public key. Once sealed, the opening of the digital envelopes can only be carried out with the election private key, which at this point does not exist as such since it was destroyed and distributed in shares among the members of the Electoral Board during the configuration process. After the vote is sealed, the digital envelope that contains the vote is digitally signed with the private keys of the verification module. These digital signatures guarantee, from this moment on and to any third-party, the integrity and authenticity of the vote. The private keys used in the digital signatures are managed by the electoral authorities or independent third-party auditors, and are installed in the verification modules during the configuration process. The last step in the process to protect the votes is the generation of a proof of ballot box integrity by applying a commutative cryptographic hash function. With this proof of integrity, it is possible to determine if the contents of the electronic ballot box stored in the DRE voting terminal are correct regardless of the order of the votes. The votes sealed in digital envelopes and the proof of ballot box integrity are kept in the verification module in order to guarantee election integrity and to facilitate a parallel recount. Finally, the digitally signed encrypted vote is returned to the DRE voting terminal.

The DRE voting terminal can store the encrypted votes digitally signed by the verification module, and/or it can use its own vote protection system to store them. In any event, any problem related with the votes stored in the DRE voting terminal can be detected by the verification module ballot box integrity record. Should any discrepancy arise, a parallel recount of the votes stored in the verification module can be carried out.

In addition, there is the optional generation in the verification module of voting receipts that can be printed out for those voters who request them. Each receipt contains a random unique identifier generated by the verification module that is sealed with the vote in the digital envelope. The random identifier, which does not reveal the content of the vote, is signed by the verification module private keys, thus preventing the generation of fraudulent receipts and bogus voter complaints. The printed receipts will allow voters to verify that their votes are present when the count is carried out. This verification can be done when the digital envelopes containing the votes and the unique identifiers are opened in the opening module and the list of unique identifiers of the votes present in the ballot box is published (decorrelated by the mixing process).

Once the voting process is concluded, the verification modules allow no further casting of votes. The ballot boxes and the proof of integrity are digitally signed by the verification module and then taken to the opening module to be tabulated later.

Vote Counting

The vote counting process is done using the electronic ballot box stored in the DRE voting terminal. Before the count is begun, the integrity of the ballot box is checked using the proof of integrity stored in the verification module. Should discrepancies arise, a parallel recount can be carried out by using the votes stored in the verification module.

To carry out the counting process with the sealed votes, it is necessary to open the digital envelopes beforehand, which requires the intervention of the Electoral Board and the reconstruction of the election private key. The opening of the digital envelopes that protect the votes takes place in the opening module and is carried out at the same time that the order of the votes is randomly permuted (i.e., mixing) in order to completely guarantee voters' privacy (even in the case that someone has recorded the order of arrival of the voters and their respective identities). As mentioned before, a minimum number (threshold) of Electoral Board members is necessary in order for the election private key to be reconstructed. In the event that voting receipts have been issued, the opening module also retrieves the unique identifiers of the votes in the electronic ballot box (without the possibility of linking them to the corresponding clear-text votes because of a double mixing process). Both the vote contents and the list of identifiers are digitally signed with the election private key to facilitate subsequent auditing by third parties.

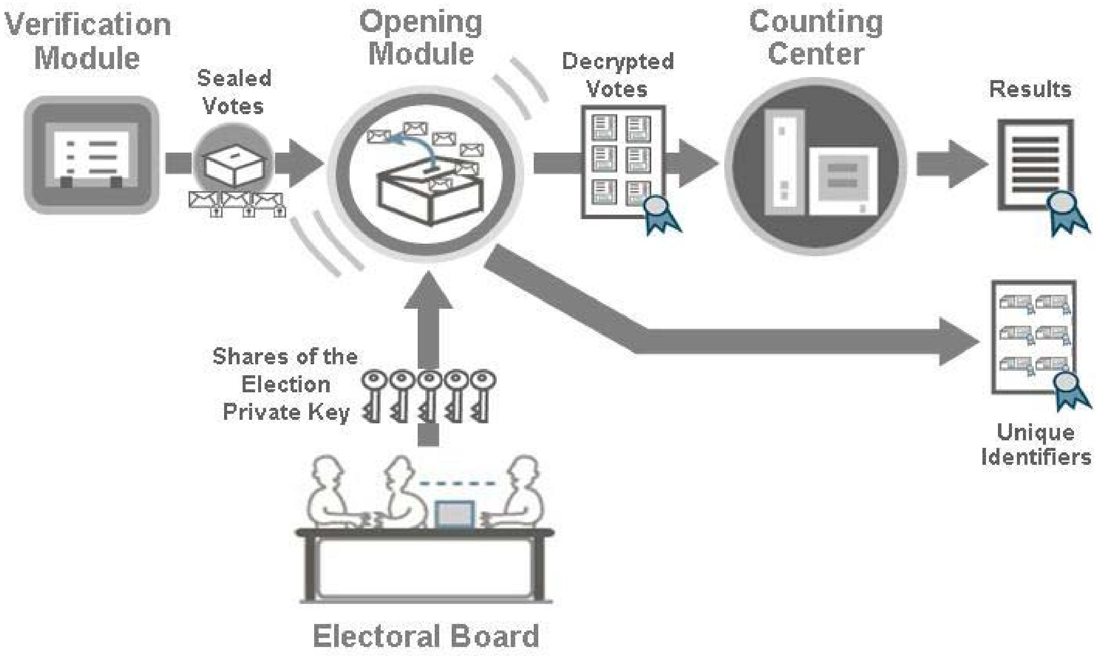

Figure 3. Counting Process

Auditing

The proposed solution facilitates the systems and data auditing.

The audit of the systems focuses on the verification and certification of the physical and logical means used in the election, such as the DRE voting terminals, the communication network components or the procedures used to carry out the election. The proposed solution allows to base the audit of the election means solely on its three components, and mainly on the verification module. The verification of the vote carried out by each voter in the verification module and the subsequent sealing of the vote in this module allow to reduce the level of the audit of the DRE voting terminal. Note that because these new modules are solely focused on protecting data (they do not implement other election processes, such as the configuration and selection of voting options), their audit is easy and independent of any last minute changes in the election. Therefore, the adoption of the proposed solution represents a significant reduction in the time and cost of the systems audit since this focuses on the verification module which is a much simpler device than the DRE voting terminal.

The audit of the data consists in checking the authenticity and integrity of any data used or generated during the election, focusing on the critical data for obtaining the results. The proposed cryptographic protocol protects the integrity of every single vote and of the electronic ballot box as a whole with irrefutable proofs that can be verified by any third party, allowing an easy detection and isolation of any fraudulent practice. All relevant election data, whether it be votes, voting receipts or ballot boxes, can be audited both during the election process and when the process is over. In particular, the results of the election can be completely audited and even the validity of every single vote can be audited.

The verification module provides voters with the possibility of verifying that the voting options selected in the DRE voting terminal are correct before casting the votes. In effect, this action means that each and every voter has the possibility of auditing the correct functioning of the DRE voting terminals. The protection of votes by means of the digitally signed digital envelopes, and the proof of ballot box integrity are also helpful in the audit of the integrity of the ballot box contents. The voting receipts represent an optional feature that allows voters to verify that their votes were present unaltered in the electronic ballot box when vote counting took place.

Analysis of the Advantages of the Proposed Solution

Some of the advantages provided by the use of verification modules in DRE electronic voting terminals have already been outlined in the description of the proposed solution. Next we summarize the main improvements offered by the proposed solution:

- *Voter Verifiability:* Voters can verify for themselves their votes before being cast thanks to the use of verification modules independent of the DRE voting terminals. The verification module is a secure and reliable environment because it is simple and easy to audit. If in addition voting receipts are used, voters can verify that their votes are present unaltered when vote counting begins. Additionally, the proposed solution allows the verifiability of visually impaired voters without the assistance of a third party.

- *Audit simplification*: The audit of the systems is basically confined to the audit of the simple verification module, thus obviating the need to extensively audit the complex software of the DRE voting terminal. This reduces the cost and risk of the audit and facilitates the certification of the voting systems by the electoral authorities.

- *Protection of vote integrity*: Once verified by the voter, the vote is sealed and digitally signed in the verification module, thus preventing any subsequent modification of the vote. An eventual elimination of the vote would be detected with a verification of the integrity of the urn as a whole.

- *Privacy of the voter*: The use of a mixing protocol controlled with a private key distributed in shares among the members of the Electoral Board prevents any correlation between the clear-text votes and the corresponding voters.

- *Redundancy and the possibility of parallel vote recounts*: Parallel vote recounts, independent of the results of the DRE voting terminals, can be carried out using the votes stored in the verification modules. The digital signatures in these votes allow the audit of these recounts.

- *Easy integration with DRE voting terminals*: Integration with existing systems can easily be achieved. The only requirement is that the DRE voting terminal has to delegate the process of vote verification to the verification module.

- *Increase in voter confidence*: The simplicity of the steps that voters must follow in order to verify their votes in a simple device external to the DRE voting terminal, confer a considerable increase of voter confidence in the voting process.

In summary, the solution herein described provides simple integration with the DRE voting terminals, incorporating means of verifiability, auditability and advanced security that enable a secure and trustworthy election process to be carried out.

Conclusions

The progressive introduction of DRE voting terminals into polling places has led to significant improvements in the electoral processes. The elimination of unintentional voting errors, the increased accessibility for people with disabilities, or the increased speed and accuracy in vote counting are just a few of these improvements. Nevertheless, the introduction of DRE voting terminals has also given rise to criticisms, mainly relating to the fact that voters are unable to verify in a reliable way that their votes have been accurately recorded by the terminal. Some of these criticisms also refer to auditing difficulties arising from the complexity of the DRE voting terminals that carry out all the functions in the voting process in a single system.

There are at present some proposals devoted to solving these problems, which range from printing out votes on paper to using cryptographic protocols that generate voting receipts that do not reveal the contents of the votes. In general, these proposals rely too much on the security of the system in which they are executed (usually the voting terminals) and are complicated to implement. As a result, none of them has provided to date a fully satisfactory solution to the existing problems.

The solution proposed in this document combines the use of a cryptographic protocol with a simple and secure hardware device known as the verification module. This module is connected to the DRE voting terminal in order to guarantee the verifiability, security and auditability required in these terminals. After selecting their votes in the DRE voting terminal, voters can verify their votes in the verification modules (either visually or with the headset connected to the audio output).

The easy-to-audit verification module thus provides the voter with a secure and reliable verification environment. The level of the audit of the other poll-site voting components can be reduced significantly, thereby cutting down on auditing costs and risks. Furthermore, the cryptographic protocol executed in the verification module completely guarantees the integrity of the votes and voters' privacy. The votes stored in the verification module also enable a parallel vote recount to be carried out. Finally, the possibility of issuing printed voting receipts allows voters to trace their votes to the vote counting process, thereby ensuring complete confidence in the election process.

Secured by scytl

Tuset 20, 1-7
08006 Barcelona, Spain
phone: +34 934 230 324
fax: +34 933 251 028
http://www.scytl.com

scytl@scytl.com