scytl

Secure Electronic Voting

VVSG Guidelines

Scytl's Comments on EAC Published Guidelines

July'05.

INDEX

1. Introduction

On June 27, 2005, the Electoral Assistance Commission (EAC) released the Voluntary Voting Systems Guidelines (the Guidelines) for public comment during a 90-day period. At the conclusion of the public comment period and after the consideration of comments received, EAC commissioners will vote to adopt the Voluntary Voting System Guidelines.

The Guidelines were developed by the HAVA-designated Technical Guidelines Development Committee (TGDC), comprised of technical experts, disability experts and election officials, and the National Institute of Standards and Technology (NIST).

This document summarizes Scytl's comments on the Guidelines which focus on the security section (Volume I, Section 6), the appendix that describes the Independent Dual Verification Systems (Volume I, Appendix D) and the testing guidelines for voting systems (Volume II). The aim of these comments is to improve the security of electronic voting systems and eliminate barriers to the implementation of innovative solutions that can enhance the security and accessibility of voting systems.

Scytl welcomes the introduction of Independent Dual Verification (IDV) systems as security solutions for electronic voting. These solutions are devoted to improving the auditability and accuracy of electronic voting systems. The Guidelines focus exclusively on one type of IDV systems, the Voter Verified Paper Audit Trail (VVPAT) systems, while other alternative IDV systems are only briefly described in an appendix. The EAC should develop specific requirements for these other IDV systems in order to facilitate their adoption.

The Guidelines do not include provisions to allow IDV systems to be qualified independently from a voting system. As a result, States or Counties cannot be sure whether an IDV system fulfils the VVSG requirements until this IDV system is integrated and qualified with a voting system. Additionally, IDV system vendors depend on voting system vendors to qualify their solutions which can be a roadblock to the development of innovative IDV solutions. Scytl considers that the testing guidelines should include a pre-qualification process for IDV systems which would allow these systems to be qualified without being integrated with a voting system. This pre-qualification should be exclusively based on the security requirements of the IDV systems and should not substitute the overall voting system qualification once the IDV system is finally integrated with a particular voting system.

2. Volume I. Section 6. Security

2.1 Section 6.8. Requirements for Voter Verified Paper Audit Trail

2.1.1. General Considerations

Section 6.8 details the security requirements for VVPAT systems. The requirements consider only one of the potential implementations of VVPAT systems. This implementation is based on a voting system composed of a voting terminal connected to a simple printer (as described in Sections 6.8.7.2.3 and 6.8.7.2.4). There are alternative implementations that use an independent audit module connected to the voting terminal and the printer to provide accessibility for blind voters and to enhance the security of standard VVPAT solutions. As discussed below, some of the requirements in this section need to be modified in order to allow some of these alternative implementations which represent innovative solutions that improve the security and accessibility of VVPAT systems.

In the following sections, we provide our comments to the requirements of Section 6.8 of the Guidelines. The original text of the Guidelines is in blue to facilitate its differentiation from our comments.

2.1.2. Comments on Section 6.8.3 VVPAT Voting Station Accessibility

6.8.3.1 All accessibility requirements from Section 2.2.7 shall apply to voting stations with VVPAT, except as set forth in Section 6.0.2.3.3.1.2.

This requirement has a broken reference to a section *6.0.2.3.3.1.2.*

6.8.3.2 The voting station shall display, print, and store a paper record in any of the alternative languages chosen for making ballot selections.

The discussion note of this requirement has a broken reference to a section *6.0.2.5.1.3.* (We believe that the correct reference is 6.8.5.3)

6.8.3.5 If the normal voting procedure includes VVPAT, the accessible voting station should provide features that enable voters who are blind to perform this verification.

We suggest the inclusion of an additional requirement related to *6.8.3.5* (e.g., *6.8.3.5.1*) to strengthen the security of the verification process by blind voters. This requirement had already been included (as requirement 3.3.3.5.4) in the preliminary report from NIST “Draft Standard for Voter Verified Paper Audit Trails in DRE Voting Systems (DRE-VVPAT)”. The text of this new requirement could be as follows:

6.8.3.5.1 If the accessible voting station includes audio equipment by which the entire VVPAT capability and verification process can be carried out, the verification process shall obtain the data related to the audio device either directly from the data sent to the printer or directly from the paper record.

2.1.3. Comments on Section 6.8.6 Electronic and Paper Record Structure

6.8.6.2 All cryptographic software in the voting system should be approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.

Since this requirement is not mandatory (*should be approved*), we recommend to eliminate the “as applicable” from it. Additionally, we propose to include an additional requirement to ensure that cryptographic algorithms are publicly available and verified by the cryptographic community. The use of proprietary algorithms (whose security cannot be checked by cryptographic experts) must be discouraged. The text of this new requirement could be as follows:

6.8.6.2.1 All cryptographic algorithms used by the voting systems must be publicly available and approved by independent cryptographic experts.

6.8.6.5 The voting system should generate and store a digital signature for each electronic record.

We suggest to expand this requirement to ensure that this digital signature also validates the contents of the paper record. The requirement could be modified as follows:

6.8.6.5 The voting system should generate and store a digital signature for each electronic record that also validates the contents of the paper record.

This modification reinforces requirement 6.8.1.3.

2.1.4. Comments on Section 6.8.7 Equipment Security and Reliability

6.8.7.2.2 The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.

This requirement conflicts with requirement 6.8.5.1.1 which assumes that the voter can deposit the paper record directly in a ballot box.

In our opinion, voters should not have access to the paper records to prevent the risk of paper trail manipulation. Therefore, we suggest to eliminate requirement 6.8.5.1.1 which would correct the current inconsistency with requirement 6.8.7.2.2.

6.8.7.2.3 The printer shall not be permitted to communicate with any other system or machine other than the single voting machine to which it is connected.

This requirement limits the use of VVPAT systems to those based only on a voting terminal and a printer. There are alternative implementations of VVPAT systems that use an independent audit module between the printer and the voting terminal to improve the accuracy of the paper trail and facilitate the verification process for blind voters.

One of the objectives of having an independent audit module is to make the verification process accessible to blind voters by providing an audible register of the vote generated from the data sent from the voting terminal to the printer. A second objective of the independent audit module is to improve the voting system auditability and accuracy (e.g., protects the register integrity) by digitally signing the digital votes and the paper records. The use of an indpendent module to digitally sign the paper records (instead of having the voting terminal to digitally sign those records) prevents the potential generation of invalid digital signatures by the voting terminal that could invalidate the paper records without being detected by the voters. A specific implementation of this independent audit module is described in detail in Exhibit A.

We suggest to add another requirement under 6.8.7.2.3 to state that in case the system uses independent audit modules to improve the accessibility and accuracy of the paper trail, the printer should only be connected to that module. This sub-requirement could be as follows:

6.8.7.2.3.1 If the voting system uses a separate independent audit module connected to the printer to make the verification process accessible to blind voters and to improve the system accuracy, the printer shall not be permitted to communicate with any other system or machine other than this independent audit module to which it is connected.

3. Volume I, Appendix D. Independent Dual Verification Systems

3.1 Section D.1 Independent Dual Verification Systems

3.1.1. General Considerations

Appendix D contains an informative classification of the current Independent Dual Verification (IDV) systems. In the sections below, we propose some changes to the description and classification of some of these systems.

As discussed in Section 2.1.4 of this document, the description of VVPAT systems included in Appendix D and in Section 6.8 of the Guidelines is too restrictive since it does not allow the possibility of adding an independent audit module between the voting terminal and the printer to improve the accessibility and security of the overall system.

Besides the VVPAT systems, Appendix D also describes and classifies other IDV systems. In the sections below, we have included comments about the characteristics of these other IDV systems (e.g., End-to-end Cryptographic IDV Systems). We strongly recommend that the EAC develops specific security requirements for these systems in order to facilitate their adoption.

3.1.2. Comments on Section 1.2.2 End to End Cryptographic IDV Systems

The general description of End to End Cryptographic IDV systems included in Appendix D is based on a specific implementation of these systems: the receipt-based systems. There are other alternative implementations that use end to end cryptography to generate a second record without issuing voting receipts. Some of these alternative implementations allow voters to verify that their votes are cast as they intended in a secure and reliable environment independent from the voting terminal. The votes are then cryptographically protected until they reach the Electoral Board. These systems provide end to end security (i.e., from the voter to the Electoral Board) by cryptographic means without having to rely on the complex technological infrastructure and system administrators sitting between the voters and the Electoral Board.

Since there are alternative implementations of End to End Cryptographic IDV systems that do not use receipts, we suggest to include in the Guidelines two types of End to End Cryptographic IDV systems: receipt-based systems and systems without receipts.

Receipt-based systems operate as follows (the description is identical to the one in the Guidelines with the exception of a change in point 2):

1. *A voter uses a voting station such as a DRE to make ballot choices.*
2. *The voting system (DRE or independent module) issues a paper receipt to the voter that contains information that permits the voter to verify that the choices were recorded correctly. The information does not permit the voter to reveal his or her choices.*
3. *The voter may have the option to check that his or her ballot choices were included in the election count, e.g., by checking a web site of values that (should) match the information on the voter's paper receipt.*

Systems without receipts operate as follows:

1. *The voter uses a voting station such as a DRE to make ballot choices.*
2. *The voter verifies the ballot choices in an independent module connected to the voting station. If the voter agrees, the independent module cryptographically protects and stores the ballot choices (second record) and the voting terminal also stores the ballot choices.*
3. *Election authorities can check the integrity of DRE records using the voter-verified ballot choices that have been cryptographically protected and stored in the independent module.*

Our porposed changes in the definition of End to End IDV systems affect sections D.1 and D.5 of Appendix D.

3.1.3. Comments on Section 1.2.4 Direct IDV Systems

These systems are defined (page D-6, lines 15-16) as those that "*…produce a record for voter verification that the voter may verify directly with voter's sense…*". In the glossary of terms of the Guidelines, Directly Verified is defined as a "*Voting system that allows the voter to verify at least one representation of his or her ballot with his/her own senses, not using any software or hardware* *intermediary. Examples of a directly verified voting system include DRE with a voter verified paper trail or marksense system. This is in contrast with an indirectly verified voting system*".

The definition of Directly Verified in the glossary of terms of the Guidelines is too restrictive since it implicidly excludes from this classification any system that does not generate a paper trail. Besides VVPAT and OCR, there are other systems that allow a direct verification with voter's sense without using paper. As an example, a Direct IDV system could use an independent hardware device (with screen and headphones) connected to the voting terminal that would perform the exact same functions of a printer by displaying the vote on its screen (or reading it through headphones) instead of printing it on paper. Once the displayed vote is confirmed by the voter, the independent device would store an electronic record of the vote. This solution provides the voter with a direct (visual or aural) verification of the vote before casting it. It also provides an independent backup of the votes stored in the voting terminal that could be used to carry out a parallel recount. Because the device is independent from the voting terminal, any involuntary or voluntary error in the voting terminal would be detected by the voter in the independent device. For further information on this alternative Direct IDV system, please see Exhibit B.

The definition of direct IDV systems should include all those systems that allow voters to directly verify the correctness of their votes using a record that represents exactly their votes. This record (e.g., paper, an electronic image, an audio representation) must be generated by a device independent from the voting terminal and must be securely stored in this independent device. On the other hand, indirect IDV systems could be defined as those systems in which voters need to use an indirect method (such as a voting receipt without the exact representation of the vote) to verify that their votes have been properly recorded.

Based on our proposed definition, VVPAT systems, independent module systems (described in Exhibit B), cryptographic systems without receipt and split process IDV systems would be considered direct IDV systems. On the other hand, receipt-based cryptographic systems and witness systems would be considered indirect verification systems.

Therefore, we suggest to split this section in two subsections: VVPAT IDV systems and Direct Electronic IDV systems. This latter subsection would include any system that allows a direct verification with voter's sense through an independent electronic module.

3.2 Section D.2 Core characteristics for Independent Verification Systems

3.2.1. Comments on Cryptographic Characteristics

2.1.10 The cryptographic software in independent verification voting systems is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.

We strongly believe that cryptographic algorithms must be publicly available and checked by the cryptographic community. We must discourage the use of proprietary algorithms that are kept secret to protect its security. As a result, we suggest to expand the requirement as follows:

2.1.10 The cryptographic software in independent verification voting systems is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable. Cryptographic algorithms shall be publicly available and its security checked by the cryptographic community.

3.3 Section D.5 End to End (Cryptographic) IDV Systems

3.3.1. Comments on End to End IDV Systems Characteristics

In Section 3.1.2 of this document, we proposed to divide the End to End IDV systems in two subcategories: receipt-based systems and systems without receipts.

5.3 End to end systems produce a receipt that can be used by the voter in some process made available by voting officials that would enable the voter to verify that the voter's ballot choices were recorded correctly and counted in the election.

We suggest to replace "*produce a receipt*" by "*can produce a receipt*" in order to accomodate both types of End to End IDV systems.

4. Volume II. Certification Testing Guidelines

4.1 Section 1 National Certification Testing Guidelines

4.1.1. General Considerations

The testing process described in Section 1.6 (Voting Equipment Submitted by Vendor) states that () "*…vendors shall submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed plus the other components with which the vendor recommends that the component be used*". This requirement forces vendors of security components, such as IDV systems, to integrate their solutions with at least one voting system vendor before submiting their solution to any qualification test. As a result, IDV vendors depend on voting system vendors to qualify their solutions which can limit the development and adoption of innovative IDV solutions.

In our opinion, the testing standards should allow IDV systems to be qualified independently from a voting system through a pre-qualification process. This pre-qualification should be exclusively based on the security requirements of the IDV systems and should not substitute the overall voting system qualification once the IDV system is finally integrated with a particular voting system. The pre-qualification process for IDV systems could facilitate the adoption of security improvements since it would allow States and Counties to make sure that an IDV system fulfils the VVSG requirements without the need of integrating that IDV system with its voting equipment.

To this end, we suggest that the Guidelines include provisions for the certification of IDV systems independent from voting systems.

4.1.2. Standards for Data Representation

The Guidelines do not define nor promote the use of any data representation standards for the electronic data generated during the election (e.g., election configuration, vote record, etc.). The use of standards facilitates the independent audit of the election without the need of using specific voting system vendor tools. The use of standards also facilitates and improves the qualification process.

We encourage the TDGC to collaborate with the EML development group to determine if EML standards can fulfill the needs of U.S. elections or if any changes to those standards are necessary.

4.1.3. Requirements for non-VVPAT IDV Systems

As previously discussed, the current Guidelines provide requirements only for VVPAT systems while other alternative IDV systems are only mentioned in an annex of the Gidelines. There is not a set of specific requirements for these other non-VVPAT IDV solutions.

We encourage the EAC (and the TDGC) to introduce new requirements for the IDV systems that have been relegated to an annex of the Guidelines. Otherwise, these solutions will be in a practical disadvantage for their implementation.

4.1.4. Provisions for Independent Qualification for IDV Systems

As previously discussed, we recommend the inclusion in the testing guidelines of processes to allow the testing of IDV systems independent from the testing of the voting systems. This measure would allow States and Counties to make sure that an IDV system fulfils the VVSG requirements before integrating it with a voting system.

Exhibit A - An Independent Audit Module to enhance the accessibility and security of VVPAT solutions

Andreu Riera, PhD

Scytl Secure Electronic Voting

May 2005

The search for voter-verifiability solutions

The use of electronic voting in elections has reached a widespread use in the United States. During the November 2004 Presidential Elections, approximately one third of the voters used Direct Recording Electronic (DRE) voting terminals to cast their votes. These electronic voting terminals provide some real benefits to the voters, such as the prevention of unintentional voting errors (i.e., undervoting and overvoting), or the increased accessibility for people with disabilities (e.g., blind or visually impaired voters).

Nonetheless, despite these advantages, DREs are generally perceived as insecure systems that do not provide any assurance with regard to the correct treatment of the votes that they record and store. Indeed, as DREs are designed today, the voter has to place blind faith in the DRE inner workings and trust that the DRE will record (and count) her vote as she really intended. Although all the voting equipment (including DREs) currently in use in the United States is independently audited and certified, the significant complexity of DREs (as a result of the many tasks that a DRE must perform) makes the auditing process difficult and, therefore does not allow to dissipate all possible doubts about their correct functioning.

Given the significant presence of DREs in polling places throughout the United States, one can easily understand the nation-wide effort that is underway in the search for solutions capable of providing DREs with enhanced auditability mechanisms and the voter with means to verify the correct treatment of her vote. This vast effort has resulted in numerous legislative initiatives at federal and state levels and in a number of innovative technological solutions to provide voter-verifiability to current DRE equipment.

Advantages and limitations of Voter-Verified Paper Audit Trail (VVPAT) solutions

Among all the voter-verifiability solutions, perhaps the best-known consists in attaching a printer to every DRE. The printer is used to produce a physical record of the vote (i.e., a paper ballot) after the voter has selected the desired voting options in the DRE. The voter can then visually check that the printed options match those she has just selected on the DRE, and the paper record can be later used in a parallel recount independent from the electronic record given by the DRE. This kind of solutions is known as Voter-Verified Paper Audit Trail or VVPAT.

The main advantages of VVPAT solutions for DREs are:

- VVPAT solutions can be, under certain assumptions, an effective method to guarantee that votes are cast as the voters intended.
- VVPAT solutions are based on tangible elements (i.e., paper) and, therefore, have great capability to generate voter confidence.
- VVPAT solutions are simple and, therefore, they are easy to understand by average voters.
- VVPAT solutions provide election authorities with a physical record that can be used to carry out a parallel recount independent from the results of the DRE.

As a result of these advantages, many groups favor the adoption of VVPAT solutions and a number of states have initiated legislative reforms to implement VVPAT solutions in their current DRE equipment. Still, VVPAT solutions show some drawbacks and limitations that may represent a serious roadblock to the adoption of VVPAT by some states. Furthermore, these disadvantages can also lead to a number of serious problems once VVPAT solutions are implemented in real elections.

The main drawbacks of current VVPAT solutions are:

- VVPAT solutions allow voters to verify that votes are cast as they intended but do not provide sufficient assurance that the votes will be counted as they were cast. Paper records, once verified by voters, are actually vulnerable to a number of attacks, including (i) the addition of bogus votes (also known as "ballot stuffing"), (ii) the elimination of valid votes, and/or (iii) the alteration of valid votes.

- VVPAT solutions do not provide election authorities with accurate mechanisms to determine the correct result in case of discrepancies between the results provided by the count of electronic votes in the DRE and the count of paper votes.
- VVPAT solutions are based on printed paper ballots and, therefore, they are not accessible for blind or visually impaired voters.

Enhancing VVPAT solutions with security and accessibility

A number of partial solutions have been proposed to mitigate some of the drawbacks of VVPAT solutions previously described. In particular, the issue of the vulnerability of the paper ballots has drawn significant attention. As explained in the previous section, plain paper ballots can be easily manipulated, which can lead to serious problems affecting the election results and the credibility of VVPAT as a reliable voter-verifiability solution. To overcome this vulnerability, some experts propose to have the DRE digitally sign the paper records that are printed in order to guarantee their authenticity and prevent the addition of bogus ballots or the alteration of valid ballots. However, this solution introduces a new risk, as the DRE could accidentally or voluntarily generate an incorrect digital signature to invalidate votes. The voter, when verifying the printed paper record, would not be able to realize that it has an invalid digital signature (it usually has the form of a bar code). This would enable the possibility of a selective attack by invalidating votes only for a particular candidate. In addition, digitally signing the paper ballots does not solve most of the other problems of VVPAT solutions since (i) it is still possible to eliminate valid votes (e.g., by physically eliminating the paper record) because of the lack of an accurate recovery mechanism, (ii) election authorities do not have accurate mechanisms to determine the correct results in case of discrepancies between the results of the DRE and the count of the paper records, and (iii) the verification system is still not accessible for blind and visually impaired voters. In summary, the obvious solution of digitally signing (by the DRE) the voter-verified paper ballots does not effectively address the current limitations of VVPAT solutions. Other, more elaborated, technical enhancements are needed.

Scytl Secure Electronic Voting, a worldwide leader in the development of secure electronic voting solutions, has recently released a new patent-pending solution that drastically improves the security of VVPAT solutions and provides them with accessibility. *Scytl*'s solution has the following general objectives:

- To provide VVPAT solutions with mechanisms to assure that votes will be counted as they were cast.
    - Preventing the addition of bogus votes and the alteration of valid votes, but without running the risk of invalidating valid votes as a result of the accidental or voluntary generation of incorrect digital signatures.
    - Preventing the elimination of valid votes (e.g., by physically eliminating the paper record) by providing an accurate recovery mechanism.
- To provide election authorities with accurate mechanism to determine the correct results in case of discrepancies between the results from the DRE and the count of paper votes.
- To improve the accessibility of the VVPAT solutions.
    - Providing blind and visually impaired voters with the possibility to individually verify that their votes are cast and recorded as they intended without the assistance from a third party.

As a result of the aforementioned benefits of integrating *Scytl*'s new solution, DREs with VVPAT solutions will become sound, secure and accessible voting systems.

Scytl's solution is based on an independent module (called Audit Module) connected to both the DRE and the printer. This Audit Module consists of a simple hardware device with minimum computing capabilities and with basic cryptographic software running in it to protect the votes. The Audit Module is much simpler than the DRE-VVPAT system since the former (in contrast with the latter) carries out only a very limited number of functions (which will be described later in this document). As a result, the Audit Module can be easily audited and certified by election authorities with complete confidence. Moreover, the Audit Module is independent from the manufacturer of the DRE, and it is based on open-source software and on software that is open to audits. These characteristics make the Audit Module a highly secure and reliable environment.

The main function of the Audit Module is to provide cryptographic protection to both printed paper ballots and digital votes. This cryptographic protection is based exclusively on the voter's verification decision and does not rely on any instruction given by the DRE or the printer. In other words, the Audit Module protects both the printed paper ballot and the corresponding digital vote against any manipulation after the voter has verified and confirmed her vote, thus assuring that both representations of the vote will coincide and that one can replace the other in case of loss or elimination (e.g., physical elimination of the printer paper ballot).

Figure 1 summarizes the steps that take place when voting on a DRE-VVPAT system enhanced with an Audit Module. The addition of the Audit Module, which is transparent to the voter, allows avoiding having to rely on the DRE and on the physical handling of the printed ballots.

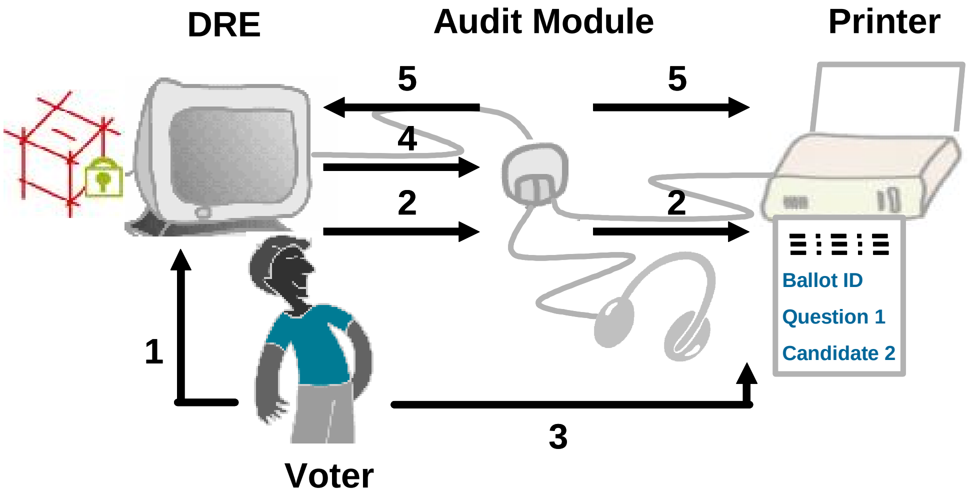


Figure 1: Voting process on a DRE-VVPAT system enhanced with an Audit Module

In the first step the voter makes the selection of the desired voting options for all the races in the DRE, as usual. The selected options are transferred, in a second step, from the DRE to the printer through the Audit Module. A paper record containing the selected options is then printed (and/or read through headphones). In the third step, the voter verifies (via the paper record and/or audio) the selected options and eventually accepts them by pressing a button on the Audit Module. At this point, the Audit Module knows the exact voting options that have been verified by the voter via the VVPAT. The Audit Module informs the DRE that the verification by the voter has been positive. In response, the DRE digitally signs the voting options and sends this digital signature to the Audit Module (fourth step). The Audit Module can then check the validity of this digital signature to ensure not only that it is valid but also that it is generated based on the correct voter-verified voting options. Any problem that could invalidate the signature of the vote would be detected at this point by the Audit Module. If the signature is correct, the Audit Module also digitally signs the (digitally signed) voting options received from the DRE. In the fifth step, the resulting digital signature is sent from the Audit Module to the printer (this digital signature can be printed on the paper record as a bar code) and to the DRE. The DRE might verify the validity of this second signature and might store it with the electronic vote. Finally, the Audit Module also stores the digitally signed vote to enhance the redundancy of the voting system.

At the end of the election, the election authorities can retrieve the electronic votes from the DRE and check their validity by verifying their digital signatures (generated by the DRE and the Audit Module) before counting them. The election authorities can also check the validity of the printed votes by verifying their digital signatures (generated by the DRE and the Audit Module) before counting them. In this way, printed votes and electronic votes can be cross-checked using their ballot identifiers and the corresponding digital signatures. This feature allows recovering lost electronic or paper votes and valid votes that have been invalidated due to printing or electronic errors. The record of digitally signed voter-verified votes in the Audit Module can also be used to check the election accuracy and solve disputes.

Conclusions

The presence of DREs in polling places in the United States has increased considerably because of the many advantages that they offer over other voting systems in terms of usability, flexibility and accessibility. The complexity of DREs makes the audit and certification process by election authorities difficult and unreliable. As a result, legislators and election authorities are currently looking for solutions to provide voter-verifiability to DREs in order to increase public's confidence in DRE voting.

A number of alternative solutions exist to provide DREs with voter-verifiability. Although the use of printed paper ballots (VVPAT) is the best-known solution, it has some drawbacks and limitations. Most notably, VVPAT solutions can be an effective method to guarantee that votes are cast as voters intended but do not provide sufficient assurance that those votes will be counted as they were cast. Simple solutions to this problem, e.g., digitally signing the printed paper ballots, introduce new unacceptable security risks.

This article presents an innovative solution developed by *Scytl Secure Electronic Voting* to complement and improve VVPAT solutions, providing them with enhanced security and accessibility. *Scytl*'s solution is based on a simple Audit Module, which can be easily integrated with any DRE and with any VVPAT solution. This Audit Module acts as a neutral auditing element, which monitors the verification process and provides its own digital signature on both printed paper ballots and digital votes, thus assuring that both representations of the same vote will coincide and that one can replace the other in case of loss or elimination (e.g., physical elimination of the printer paper ballot).

The addition of the Audit Module to DRE-VVPAT systems allows (i) to prevent the addition of bogus ballots without running the risk of invalidating valid votes as a result of the accidental or voluntary generation of incorrect digital signatures on the printed paper ballots, (ii) to prevent the elimination or alteration of valid votes by providing an accurate recovery mechanism, (iii) to provide election authorities with accurate mechanisms to determine the correct results in case of discrepancies between the results from the DRE and the count of paper votes, and (iv) to provide accessibility to the VVPAT solution for blind and visually impaired voters.

More information about Scytl or about Pnyx.VVPAT (Scytl's solution that implements an Audit Module as described in this article) can be found at http://www.scytl.com

Exhibit B – Direct voter-verifiability through Independent Electronic Modules

Andreu Riera, PhD
Scytl Secure Electronic Voting
May 2005

The search for voter-verifiability solutions

The use of electronic voting in elections has reached a widespread use in the United States. During the November 2004 Presidential Elections, approximately one third of the voters used Direct Recording Electronic (DRE) voting terminals to cast their votes. These electronic voting terminals provide some real benefits to the voters, such as the prevention of unintentional voting errors (i.e., undervoting and overvoting), or the increased accessibility for people with disabilities (e.g., blind or visually impaired voters).

Nonetheless, despite these advantages, DREs are generally perceived as insecure systems that do not provide any assurance with regard to the correct treatment of the votes that they record and store. Indeed, as DREs are designed today, the voter has to place blind faith in the DRE inner workings and trust that the DRE will record (and count) her vote as she really intended. Although all the voting equipment (including DREs) currently in use in the United States is independently audited and certified, the significant complexity of DREs (as a result of the many tasks that a DRE must perform) makes the auditing process difficult and, therefore does not allow to dissipate all possible doubts about their correct functioning.

Given the significant presence of DREs in polling places throughout the United States, one can easily understand the nation-wide effort that is underway in the search for solutions capable of providing DREs with enhanced auditability mechanisms and the voter with means to verify the correct treatment of her vote. This vast effort has resulted in numerous legislative initiatives at federal and state levels and in a number of innovative technological solutions to provide voter-verifiability to current DRE equipment.

Selecting a voter-verifiability solution

Among all the voter-verifiability solutions, perhaps the best-known consists in attaching a printer to every DRE. The printer is used to produce a physical record of the vote (i.e., a paper ballot) after the voter has selected the desired voting options in the DRE. The voter can then visually check that the printed options match those she has just selected on the DRE, and the paper record can be later used in a parallel recount independent from the electronic record given by the DRE.

Adding a printer to the DRE represents an obvious and (at least in theory) simple solution to the voter-verifiability issue. Still, as any other method, adding a printer to the DRE presents both advantages and drawbacks. On the one hand, printers and physical paper ballots have the capability to generate confidence and also offer the possibility of an independent parallel recount. On the other hand, this method shows poor usability, is not accessible for blind and visually impaired voters, and is prone to mechanical problems and high maintenance costs.

In any case, regardless of the balance between the advantages and drawbacks of printers, it is important to note that there are other types of voter-verifiability solutions. This article does not intend to judge printers as a voter-verifiability solution but rather to provide a comprehensive list of factors that should be taken in consideration when comparing and rating different voter-verifiability solutions. The article also presents a new and alternative voter-verifiability solution that is not based on printed paper ballots.

Comparisons of the different voter-verifiability solutions should be based on a set of objective criteria. We propose the following list of 13 factors, classified in three basic categories (security, usability and implementability):

Comparative factors related to security and voter-verifiability:

1. Voter-verifiability: Possibility for the voter to verify the correct recording of her vote (“vote cast as intended”).
2. Vote integrity: Prevention of vote manipulation from the moment the vote is cast until it is counted (“vote counted as cast”).
3. Redundancy: Existence of an independent back-up of the votes which enables parallel recounts.

4. Auditing of election results: Possibility of third-party audits of the results.
5. Security of the data interchanged between the DRE and the voter-verifiability solution: Confidentiality and integrity of the data (generally votes) interchanged between both systems.
6. Voter privacy: Assurance that the voter's choices will remain totally anonymous.

Comparative factors related to the ease of use by voters:

7. Usability: Ease of use of the voter-verifiability solution by average voters.
8. Accessibility: Possibility of using the voter-verifiability solution by voters with disabilities.
9. Time-to-verify: Average extra time required by the voter to complete the verification process at the polling place.

Comparative factors related to the implementability and cost:

10. Ease of integration: Ease to integrate the voter-verifiability solution with current DRE equipment.
11. Auditability of voting equipment: Effects of the voter-verifiability solution on the auditing and certification processes of the resulting voting equipment (i.e., how the current processes are improved or worsened by the introduction of the voter-verifiability solution).
12. Possibility of technical problems: Likeliness of malfunctioning problems because of the presence of networked or mechanical elements.
13. Costs: Both the initial acquisition costs of the solution and also the additional on-going costs associated with the maintenance of the solution.

Redundancy, Enhanced Auditability and Voter-Verifiability for DREs through Electronic Verification Modules

Scytl Secure Electronic Voting, a worldwide leader in secure electronic voting solutions, has recently released a new solution that effectively addresses the current concerns regarding auditability and voter-verifiability that affect DREs. This solution is the result of many years of research and is protected by patents. The basic concept underlying this solution was first presented in the United States during an e-voting conference organized by Professor David Dill in Denver in July 2003. The solution has been more recently tested in Europe, during the Spanish referendum to approve the European Constitution (February 2005).

Scytl's solution has the following general objectives:

- To allow the voter to individually verify the correct treatment of her vote.
    - Allowing the verification that her vote is cast and recorded as she intended.
    - Providing assurance that the recorded vote will be counted as cast.
    - Making this verification process accessible to everyone, including the blind and visually impaired.
- To provide redundancy through a double register of the votes.
    - Drastically reducing the risk of loss of votes.
    - Offering the possibility of an independent parallel recount of the votes.
- To facilitate the audit and certification process by the election authorities.
    - Simplifying the audit and certification of the voting system by concentrating the critical security features in a simple and easy-to-audit device.
    - Enhancing the auditability of the election through the use of cryptographic tools.

Scytl's solution is based on an independent module, called the Verification Module (VM). The VM is connected to the DRE, as shown in Figure 1. The VM consists of a hardware device with a screen, an audio port, and two buttons (one to confirm and the other to reject). The VM also has basic computing capabilities that enable the execution of cryptographic software to protect every single vote.

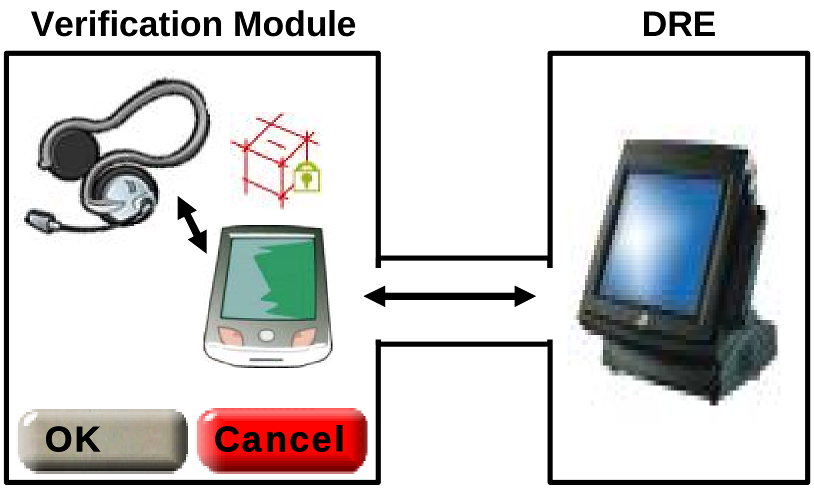
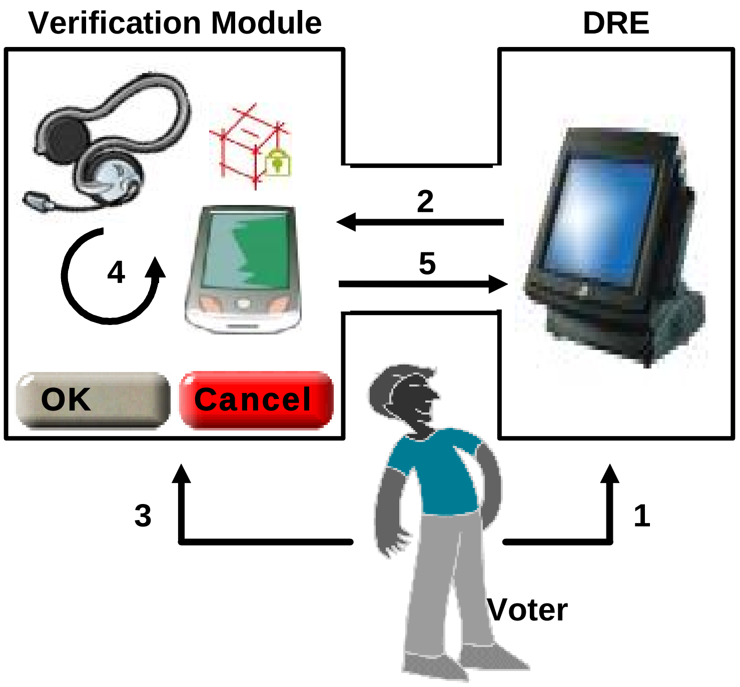


Figure 1: Verification Module connected to a DRE

The VM, like a printer, serves a basic function, namely to receive from the DRE the options selected by the voter and to display them to the voter on a device independent from the DRE. The voter, as in the case of a printed paper ballot, can verify that the options previously selected in the DRE match those displayed on the screen of the VM (or listened through its headphones). The VM also allows the voter to confirm (or reject) the displayed/listened voting options. If there is a positive confirmation, the VM cryptographically protects the voter-verified options, thus preventing any future alteration of the vote. As in the case of printed paper ballots, the VM stores a second record of the votes to allow future parallel recounts. Figure 2 summarizes the steps that the voter performs to complete the verification process.

The VM is much simpler than the DRE since the former (in contrast with the latter) carries out only a very limited number of functions (receives the ballot summary, displays/speeches it, awaits voter confirmation, and cryptographically protects the vote). As a result, the VM can be easily audited and certified by election authorities with complete confidence. Moreover, the VM is independent from the manufacturer of the DRE, and it is based on open-source software and on software that is open to audits. These characteristics make the dual system DRE-VM a highly reliable and secure voting system.



1. The voter makes the selection of her voting options for all the races in the DRE.
2. The selected options are transferred from the DRE to the VM.
3. The voter verifies (via screen and/or audio) the selected options and confirms them.
4. The verified voting options are encrypted and digitally signed in the VM in order to protect every single vote from possible attacks that can take place either in the DRE or outside it.
5. The protected vote is stored in the VM and a positive verification message is sent to the DRE where the vote is also stored.

Figure 2: Verification process performed by a voter

At the end of the election, the election authorities can retrieve, as usual, the votes from the DRE. Additionally, they can now check the votes tabulated by the DRE against an integrity record that is provided by the VM. This integrity record is generated by the VM, based on every single voter-verified vote (for the crypto savvy, the integrity record is calculated as a one-way accumulator that allows detecting any alteration of the votes with the exception of changes in the ordering of the votes). Should the set of votes retrieved from the DRE not match the integrity record from the VM, the election authorities could retrieve the back-up votes from the VM (which are the cryptographically-protected voter-verified votes) and implement a parallel recount based on them.

Conclusions

The presence of DREs in polling places in the United States has increased considerably because of the many advantages that they offer over other voting systems in terms of usability, flexibility and accessibility. The complexity of DREs makes the audit and certification process by election authorities difficult and unreliable. As a result, legislators and election authorities are currently looking for solutions to provide voter-verifiability to DREs in order to increase public's confidence in DRE voting.

Although printers are probably the best-known voter-verifiability solution, there are other alternative solutions that present advantages over printers in terms of security, usability and implementability. This article introduces a list of 13 comparative factors that can be used to evaluate and rate the different voter-verifiability solutions.

This article also describes the basic concept underlying a new voter-verifiability solution developed by *Scytl Secure Electronic Voting*. This solution is based on a Verification Module that allows voters to verify and confirm their voting options in a simple and audited device independent from the DRE. This innovative solution (i) provides assurance that the votes are cast and recorded as intended, (ii) simplifies the audit and certification processes since the auditing efforts need to focus only on a simple and easy-to-audit device, (iii) protects the integrity and anonymity of every single vote once this has been verified by the voter, (iv) provides redundancy through a double register of the votes, and (v) allows independent parallel vote recounts.

More information about Scytl or about Pnyx.DRE (Scytl's solution to implement the VM concept) can be found at http://www.scytl.com

Secured by scytl

Entença 95, 4-1
08015 Barcelona
SPAIN

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

http://www.scytl.com