

# Verification Systems for Electronic Voting: A Survey

**Abstract:** Voting is an important part of the democratic process. The electorate makes a decision or expresses an opinion that is accepted for everyone. Some parts could be interested in the election results deviation without anyone else noticing it. However, controlling that the whole voting process is performed correctly and according to current rules and law is, then, even more important. We present in this work a review of existing verification systems for electronic voting systems, from both academia and commercial world. To do so, we realize a fair comparison against a set of representative voting verification systems, by using an evaluation framework. We define this framework to be composed of several properties, covering important system areas, ranging from the user interaction to security issues. We then model the natural evolution of verifiability issues on electronic voting systems, which are influenced by restrictions on current laws and by the technology advances.

## 1 Introduction

From the birth of democracy in Athens on 6th Century BC and the first form of electoral laws, there have been designing and developing electoral systems according to country particularities on worldwide democratic governments.

An election process consists choosing a person or party, namely *candidate*, to represent all members of the community (e.g., a company, a state or a country). For a candidate, winning elections is a big representation responsibility, but it is also very attractive in very ways for other reasons (e.g., funds, ability of changing existing rules and laws). Therefore, synergies could appear to deviate election results (not) to make win a certain candidate.

However, it is a difficult task to check whether the election results correspond to the voters' preferences, since *votes are* commonly *private and anonymous*. That is, if voter Alice votes candidate A, any another person must not know or extract Alice's preferences from the election process and results. In other words, *elections must be verifiable*, even though voters' preferences are linked in no way to them. Therefore, *verifiability* comes to light as the most important elections' property to provide *trustfulness* to the elections' results to both candidates and voters.

Verifying that elections results correspond to voters' preferences depends on the voting system. From a location viewpoint, most of the existing systems are based on poll sites, where voters attend to specific places to vote. Remote voting systems (such as mail voting or lastly Internet voting systems) are also an alternative.



From a ballot perspective, traditional voting systems use ballots in paper format. They were firstly introduced in the state of Vitoria, Australia, in 1856 [Be10]. Paper ballots contain all the necessary information to vote for a specific candidate, in a human-readable format. Thus, in the vote counting or *tally*, any person can verify whether the ballot is correct and, if so, to which candidate is related to. However, the main drawbacks of traditional voting systems are that all operations are manual, as well as their high economic and logistic costs. Also, the tally process where votes are counted can turn in a long procedure susceptible to human errors, especially when the voting system is complex.

More modern voting solutions incorporate electronic devices to mainly accelerate the tally process and overcome the problems induced by human errors, and also increment accessibility for disabled and illiterate voters. First initiatives appeared in 1964 in some states of USA, which used punchcards and computer tally machines [Be10]. These kinds of solutions can use different technologies, ranging from punchcards, optical scanners (to scan ballots) to cryptographic techniques. Electronic voting (*e-voting*) systems, thus, pose other kind of challenges to address election *verifiability*, whilst ensuring voter privacy and anonymity at the same time.

To put all this in words, thus, we can differentiate three different types of *verifications*: *individual*, *universal* and *end-to-end verifiability*. Briefly speaking, *individual verification* permits voters to check that their individual ballots are correctly cast and counted.
From a system viewpoint, *universal verification* allows to inspect that the election results correspond to cast ballots. The aim is to ensure that the whole voting process is performed correctly, what leans to *trustful* election results. In traditional voting systems, both verifications are achieved by a set of *procedures* (i.e., manual operations addressed by election officials, or also by independent entities and observers from candidates.). Contrariwise, a mix of *procedures and technologies* usually address them in e-voting systems. A later enhanced property is the *end-to-end* (E2E) *verifiability*. Seen from a voter point of view, in an E2E verifiable voting system, a voter can check along the voting process that both her ballot is correctly cast and counted in the final tally. The goal is then to increase the voters' *reliability* on the election results. Note that this property was hardly supportable in traditional voting systems, since the voter Alice concluded her interaction with the voting system when casting the ballot in the ballot box. However, new designs of voting systems and modern technologies facilitate an E2E voter verifiable voting process.

In this survey, *we present a fair comparison on the verifiability of electronic voting systems based on poll sites*. We also name them *voting verification systems* (VVSs). The motivation behind that is because poll-site-based voting systems are the most common ones nowadays. Besides, we specialize our study on e-voting systems since they are the last trend on democratic voting systems [Ev09]. The systems included in this analysis are remarkable real world and academic solutions of the last decade. Thus, the contribution of this work is twofold: (i) definition of a *common evaluation framework* to fairly compare all systems, and (ii) *study and comparison* of remarkable e-voting systems.



**Document structure.** The next section introduces the necessary background for the present work. Sec. 3 presents the evaluation framework, and Sec. 4 the analysis of all voting verification systems (VVS). In Sec. 5 we perform the overall analysis of all systems. Finally, Sec. 6 presents the concluding remarks of this work and some future work.

# 2 Background

We consider in this study the standard voting process composed by the following phases: (i) *voter registration* and identification, (ii) *vote casting* using ballots and (iii) vote tally, where all ballots will be securely *tabulated* and unbiased results will be made *public*ly available. The voting process also includes all *procedures* and *technologies* to trustfully address the consultations or elections.

Besides, we present the system classification of the voting models and voting verification systems, according to the voting location and the U.S. HAVA classification, which will be used later in this work to organize the analyzed voting systems.

## 2.2 Voting models

We present two classifications of the voting models, according to the place where voters have to attend for voting (see Sec. 2.2.1), as well as according to the U.S. HAVA classification (see Sec. 2.2.2).

### 2.2.1 Location-based classification

According to the place voters have to go to vote, voting systems are broadly classified into **poll-site-based** and **remote** voting systems. In the *former type*, voters go to a specific building, namely poll site. Nowadays it is the most used voting scheme. Conversely, voters may remotely cast their vote in *remote voting systems*. These systems can be further classified as follows: **vote-by-mail**, **Internet** and **presential remote**.

- **Vote-by-mail** was introduced in 1896 [Vo10] and it is cheaper [Qv05] than traditional voting systems. However, voting by mail suffers from vote loss or late delivery. To overcome these drawbacks, the next remote voting schemes appear.
- **Internet** voting allows an electronic cast and tally, where the Estonian case [Es05] was the first worldwide Internet-based nationwide binding elections.
- **Presential remote** voting allows *abroad* poll sites to cast votes, which are *electronically* gathered in the corresponding country (or county) for tallying. They are very helpful when voters are abroad (e.g., the military), whilst reducing the tally time.

As mentioned earlier, our *focus* is put *on verification systems of poll-site-based systems*, which also allow us for taking presential remote voting systems into consideration.

### 2.2.2 HAVA classification

This classification has been promulgated by the Election Assistance Commission (EAC), an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). Appendix C of the 2005 VVSG [El05] list the VVSs in four types: (i) **Process separation-based** VVSs have a modular architecture split into two independent, totally isolated systems dealing the *generation* and *casting process, respectively*; (ii) **Evidence-based** VVSs are based on capturing *all actions* performed during the voting phase of voters; (iii) **Direct** VVSs generate a *parallel* registry of votes, which permits a direct verification of the vote to be cast; Lastly, (iv) **end-to-end cryptography-based** VVSS employ cryptographic methods to craft receipts that allow voters to verify that their votes were not modified, without revealing the voting preferences from voters. We will classify the evaluated electronic VVSs following this classification.

# 3 Common Evaluation Framework

In this section we introduce the classification of and properties that we will extract from the set of systems under consideration. All them constitute the single, structured *evaluation framework* that we will use to ease their fair comparison and analysis.

## 3.1 Classification of VVSs

We employ the following classification to *percolate* the systems through, respectively, in order to obtain their natural organization (see Fig. 1). The year of publication of the academic publication or system is the last organizational property used.

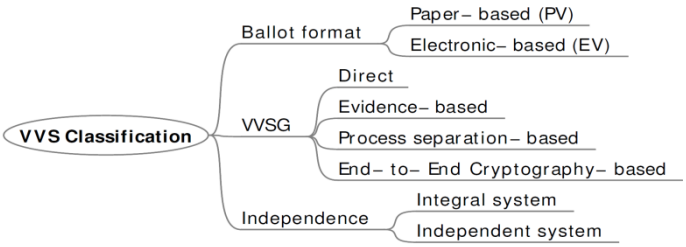



Figure 1. Summary of VVS classification.

1. From **electronic-** and **paper-based systems**, we only consider electronic VVSs, which require voting in *electronic* (instead of *paper)* format.
2. We use the aforementioned **HAVA classification** to separate them into *process separation-*, *evidence-*, *end-to-end (E2E) cryptography-based* and *direct* VVSs.
3. We further organize them into **integral** or **independent systems**. *Integral* ones perform the whole voting process, while independent VVSs are designed solely to verify *independent*ly that another voting system is trustfully working.

### 3.2 Evaluated properties from VVSs

We present in Fig. 2 the considered characteristics to evaluate against all systems. We have classified them into these voting process concerns: *user interaction*, *security*, *integrability* (with an existing voting system), as well as *technical issues*. Note that any property definition is such that a *positive answer* corresponds to a *positive feature*.

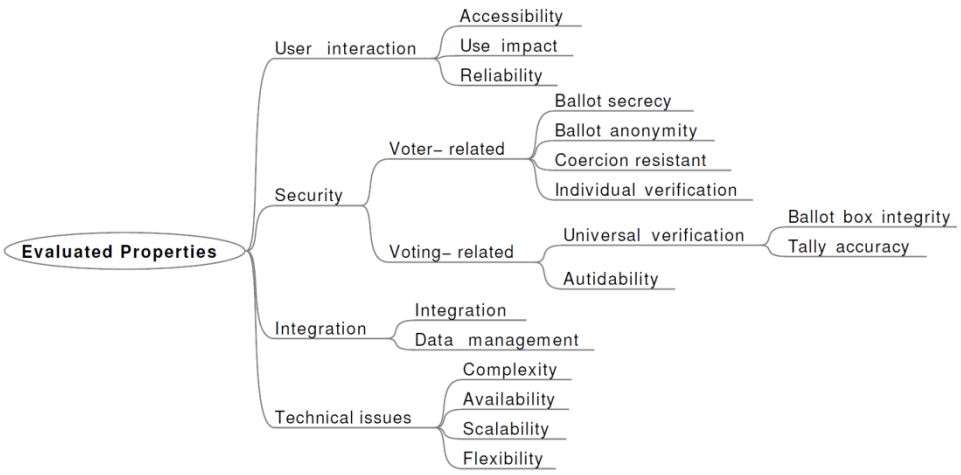



Figure 2. Summary of evaluated VVS properties.

**User interaction.** The *user interaction* greatly determines the voters' impression and *reliability* on the voting system:

1. **Accessibility.** Whether the system *does not* prevent a disabled user to vote.
2. **Use impact.** Whether the system *does not* enforce a more complex (even longer) process to cast a vote.
3. **Reliability.** Trust on the whole voting process from a *voter viewpoint*.

**Security.** The security issues are broadly categorized into these two big sets, namely *voter* and *voting process*:

**Voter-related:**

4. **Ballot secrecy.** The system *prevents* a third entity to see the content of the ballot.
5. **Ballot anonymity.** The system *prevents* the ballot to be linked to the voter.
6. **Coercion resistant.** A coercer *cannot* verify nor demonstrate how the voter voted.
7. **Individual verification.** A voter *can* verify that her vote was accounted *properly*.

**Voting-related:**

- **Universal verification:**
  8. **Ballot box integrity.** Only registered voters' votes *appear* unmodified at the end of the voting process (before the tally process).
  9. **Tally accuracy.** The tally process *accounts* all the cast votes, and not before the end of the voting process (i.e., no partial results are allowed).

10. **Auditability.** The e-voting system (with no paper trails) *allows* a third party to analyze what happened before, during and after casting the vote without compromising other security properties, in order to certify the final tally and election results.

**Integration.** Regardless of whether the VVSs are *integral* or *independent*, we will consider the feasibility and effectiveness of adapting/interacting the evaluated system with other voting systems. In particular, briefly speaking, we reckon the synchronization of operations, especially when votes are being cast, between a given voting system and the evaluated system *acting as an independent VVS* (as issued in [Sh06]).

11. **Integration.** *Ease* on implementing/adapting the evaluated system as an independent verifier system for other voting infrastructures.
12. **Data management.** Whether the vote cast subsystem of voting systems and the evaluated system *guarantee* atomicity, as well as whether this integration is resistant to failures (e.g., user errors, cable disconnections).

**Technical issues.** We also analyze the VVS performance from a *technical viewpoint*:

13. **Simplicity.** Whether the verifier solution *is* straightforward and simple.
14. **Availability.** A suitable voter *must be able to* cast her vote, whenever she can, along the established time, and preventing her from voting multiple times (if not allowed).
15. **Scalability.** The verifier system computationally *scales*.
16. **Flexibility.** This measures the level of freeness *allowed* by the verifier system (e.g., number of candidates, write-in mode).

**Properties representation.** For brevity, when summarizing these 16 properties for all the evaluated systems, we will use the following notation:

Table 1. Value representation on the considered evaluation properties

| | |
|---|---|
| User interaction | ↑/↓/~: **G**ood/Weak/Acceptable. |
| Security | **Y**/**N**/~: **Y**es/**N**o/Partially. |
| Integration | **NT**: **N**o additional **T**echnical requirements (on voting consoles, etc).<br>**T**: Additional **T**echnical requirements.<br>**NSW**: **N**o additional **S**oft**W**are requirements (on voting consoles, etc).<br>**SW**: Additional **S**oft**W**are requirements. |
| Data management | **NA**: There is **N**o operation **A**tomicity.<br>**A**: There is operation **A**tomicity.<br>**DL:** There is **D**ata **L**oss.<br>**NDL:** There is **N**o **D**ata **L**oss. |
| Technical Issues | ↑/↓: High/Low |
| *At any property* | "`N/A`": When the property is not addressed. |

# 4 Presentation and classification of VVSs

We present all the evaluated *electronic VVSs* in Fig. 3. The idea behind them is that they depend primarily on e-voting procedures, even though some of them may have paper *receipts* to provide E2E verifiability, while giving higher *confidence* to voters. From the HAVA classification, we present solutions on three out of the four types: *process separation-based*, *evidence-based* and *end-to-end cryptography-based* (E2E).

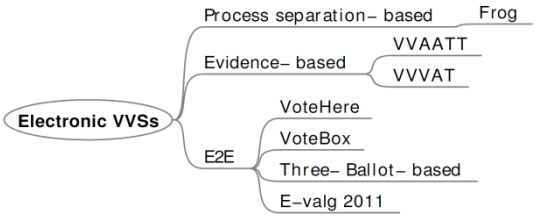



Figure 3. Summary of evaluated electronic VVSs

## 4.1 Process Separation-based VVSs

As we have presented before, a process-separated VVS is divided into two independent and isolated subsystems: *ballot generation* and *casting*. In this class of systems, the security constraints are mainly applied on the casting process. We present below Modular Voting Architecture, namely "Frog" [BJR01], which is the most representative system in this kind of VVSs.

### 4.1.1 Modular Voting Architecture ("Frog")

S. Bruck, D. Jefferson and R. Rivest presented this system in 2001 [BJR01]. It is the example par excellence of separation process and, therefore, it implements an integral e-voting solution that emphasizes on and standardizes a separation between vote *generation* and vote *casting* components.

On the Election Day, the voter identifies himself to poll worker who takes a blank *ballot* (ballots are named *frogs*), initializes it and, then, a poll worker returns the ballot to the voter. Afterwards, the voter inserts his ballot into the *vote generation equipment*, she selects her options through a direct-recording electronic (DRE) voting machine, and her choices are typed into her ballot. The second phase starts here. The voter introduces her ballot into the *vote-casting equipment* and *checks* the content of her ballot. When the voter agrees the content, her ballot is digitally *signed* (using a single key for all votes), then *frozen* (the frog is blocked against writing) and finally *deposited* in the *frog bin*. At this moment, an electronic copy of her vote is randomly stored into a data unit memory and replicated in other memories for reliability. Once elections are over, election officials publish the results for each precinct in a Web as two separated, unlinked lists: one with the voters' names and the second one with all cast ballots with a system-wide digital signature. Therefore, anyone can verify digital signature and compute election results.



### 4.2 Evidence-based VVSs

These systems capture the actions performed by voters when casting their votes, independently of the voting system and transparently by the voter. In addition, to ensure information integrity, all recorded events are stored outside the vote terminal. Under this type of VVSs, we consider VVAATT and VoteHere.

#### 4.2.1 Voter Verified Audio Audit Transcript Trail (VVAATT)

VVAATT is an *audio verification* system, introduced by T.Selker and S.Cohen in 2004 [Se04, SC05]. This system records the *audio* in all events along the voting process into a physical medium (in a cassette tape or in a CD-W media), while this is complemented by the *visual* verification from the DRE. In the same line, there exists Voter Verified Video Audit Trail (VVVAT), which instead, captures the sequence of screenshots on the DRE terminal (see [Cr07] for an example).

### 4.3 End-to-end Verifiable VVSs

We present in this section the E2E cryptographic-based VVSs, which among other capital properties have an end-to-end (E2E) verifiability. To do so, some of them generate *paper receipts* to allow voters checking that their votes were accounted in the tally process. The following solutions are the selected systems under analysis: VoteHere [Ne01], VoteBox [SDW08], Three-Ballot-Based Secure Electronic Voting System [SCM08] and the last ErgoGroup/Scytl proposal [No09b].

#### 4.3.1 VoteHere

VoteHere is an integral solution introduced by C. Andrew Neff and VoteHere, Inc. in 2001 [Ne01, Va01]. This system is based on the use of DRE terminals. It is built considering receipt- and cryptography-based verifications, in order to cover both *individual* and *universal* verifications.

For each voter, the voting system builds a *code* for each electable candidate before the election starts. Once the voter has chosen her preferences on the DRE, the DRE shows the codes related to each candidate. If they correspond with those pre-built codes, the voter confirms her vote and a *receipt* is printed with her *verification codes*. Once the election ends, the *encrypted votes* are made publicly available (guaranteeing ballot secrecy) and, then, the voter can *check* if her vote was accounted (or complain to election officials otherwise).



### 4.3.2 VoteBox

VoteBox is an integral solution and was developed by D. Sandler, K. Derr and D. Wallach in 2008 [SDW08]. VoteBox system uses a technique adapted from Benaloh's work on voter-initiated auditing [Be07] to gain end-to-end verifiability. In other words, the voting system actually is an audit system that records everything happened. Its main characteristic properties are as follows:

- **Pre-rendered user interface.** The user interface is built from *pre-rendered* graphics, a closed sequence of pages (screens) containing text and graphics that reduce runtime code size. The only interactive elements are buttons, rectangular regions of the screen (VoteBox supports touch screens), and other assistive technologies (computer mice, keyboards or audio feedback to state transitions).
- **Tamper-evidence and replication.** A *permanent*, *tamper-evident* audit system records the events along the voting process and provides resistance to data loss in case of failure or tampering. VoteBox consists of two parts: Supervisor console and VoteBox booths (i.e., voting terminals). A broadcast network connects both parts, so that events from both parts (including ballot casts or supervisor commands) are replicated on all voting terminals and entangled with a hash chaining (i.e., to provide *immutable* logs).
- **End-to-end verifiability.** To encrypt ballots, VoteBox uses the ElGamal cryptosystem and its *additive homomorphic* property. Any cast ballot is encoded in a binary format and encrypted by a public key of the election. Therefore, the tally is addressed by (i) the multiplication of all ballots and (ii) the multiplication result decryption in order to obtain the election results.

### 4.3.3 A Three-Ballot-based Secure Electronic Voting System

This system [SCM08] is based on the original, paper-based ThreeBallot system [Ri06], but completely redesigned to provide a full electronic solution. The idea behind the ThreeBallot approach is that a *ballot* consists of three single *parts*, with a list of candidates in the same order on the three parts. In order to vote for a candidate the voters mark *any two parts* on the corresponding candidate (whilst marking only one part means no voting for). When casting the vote, the three parts are separated from each other and mixed with the rest of parts from other voters. The tally operation is done by a simple calculation on the number of marks for each candidate on all the parts. One out of the three parts is randomly chosen by the voter to *copy* and to take home as a *receipt*. The same approach is maintained in this electronic version of Three-Ballot [SCM08].

### 4.3.4 E-valg 2011

The Norwegian Ministry of Local Government and Regional Development initiated in 2008 a selection process of e-voting technological providers, which finished on Decem-



ber 2009. ErgoGroup[1] and Scytl[2] [No09b] will provide the e-voting solution for the Norwegian municipal elections in 2011 [No09c].

The ErgoGroup/Scytl's solutions provide all the security requirements by using cryptographic techniques. Until now, ErgoGroup/Scytl consortium has designed various systems to support two types of voting: *poll-site-based* (compatible with DREs) [Sc04] and *remote voting* [PM07]. Moreover, the latter allows a presential remote voting model, which suits the system requirements specification of the E-valg 2011 project [No09d].

ErgoGroup/Scytl's proposal [No09b] is based on a *hybrid scheme* that combines mixing techniques and ElGamal homomorphic properties [Pe09]. The homomorphic cryptography uses a *multiplicative* property [Pe04, Pe09], so that the system performs partial multiplications of the votes. To encrypt votes, the election private key is generated using a *threshold scheme* [Sh79]. Lastly, to retain all desirable security properties, this system uses digital signatures, zero knowledge proofs or generation of return codes (i.e., *receipts*).

# 5 Study and comparison of VVSs

In this section we introduce the analysis of the considered VVSs (Sect. 5.1) and the study of the synergies on voting systems and cryptographic technologies (Sect. 5.2).

## 5.1 Analysis and comparison of VVSs

We follow the properties considered in our common evaluation framework to compare and analyze all evaluated VVSs. See Tab. 3 for the complete elaboration.

**User interaction.** Given that all VVSs use DREs to emit votes, all them provide a certain degree of **accessibility**. However, some of them improve it by using audio guides (VVAATT), or indeed with other assistive technologies (such as mice or keyboards) (VoteBox and E-valg). For the E-valg case, this is proved by the studies [Sh06], [No09a]. As for the **use impact**, systems like Frog, VoteBox and Three-Ballot present a more complex and likely longer voting process. For instance, in Frog there exists a strict separation of the generation and cast processes (even though a voter can bring a filled ballot from home), VoteBox allows voters to perform an "immediate ballot challenge" [Be07], or Three-Ballot uses a multi-ballot composed of 3 parts. Further, in order to increment the **reliability** on the voting system, they provide three kinds of augmented features: (i) frogs (Frog) and *receipts* (VoteHere, VoteBox, Three-Ballot and E-valg) are tangible elements for the voter, (ii) audio guides (VVAATT), and (iii) public web bulletins (all except VVAATT).

[1] http://www.ergogroup.no/default.aspx?path={2A1C0F50-F200-43C8-98C6-36CD82F7A587}
[2] http://www.scytl.es



**Security.** VVAATT/VVVAT do not ensure vote confidentiality, given that all (audio or video) recordings show the *sequential* voting order. In addition, VVAATT/VVVAT suffer from *weak* recording equipment protection (given that they must be accessed often) and *untrustful* information extraction techniques. In conclusion, even though the recording support provides audit means, VVAATT/VVVAT are not reliable. Next, we only will focus on the rest of systems.

**Voter-related security.** Except Frog, all systems use a public key infrastructure (PKI), most of them ElGamal, to ensure **ballot secrecy**. However, the VVSs use very different techniques to guarantee **ballot anonymity**. While Frog uses a simple randomization algorithm, Three-Ballot separates each of the three parts of a ballot and stores them using their hash values. More complex techniques also appear: mixing (VoteHere), additive homomorphic (VoteBox) or a hybrid scheme (multiplicative homomorphic and mixing in E-valg). The use of a threshold prevents security attacks to the electoral system. VoteBox, Three-Ballot and E-valg are **resistant to coercion and vote selling**. The same is not true for VoteHere, since it may have a flaw given that it shows both encrypted ballots and receipts with return codes [Ba04]. Lastly, except Frog, all systems render *augmented* **individual verification** with *E2E* voter *verfiability* through receipts.

**Voting-related security.** Except Frog, all systems ensure **ballot box integrity** through different technologies (like ZKPs, digital signatures or threshold schemes). See Tab. 2 for more details. Thus, VoteHere, VoteBox, Three-Ballot and E-valg guarantee **tally accuracy**. Homomorphic algorithms make a more efficient tally than mixing techniques [Pe04, Pe09]. As for **auditability**, Three-Ballot creates logs for any voter-related operation, even though nothing about the tally process. The evaluated strongest audit systems appear in VoteBox and E-valg that use immutable logs. VoteBox, however, builds a distributed total audit system, while E-valg only centrally audits the critical system elements.

Table 2: Security Techniques used by Voting Verification Systems.

| | | Security Techniques | | | |
|---|---|---|---|---|---|
| | | ZKPs | Digital Signatures | Threshold Scheme | Audit System |
| VVS | Frog | No | Yes | No | No |
| | VoteHere | Yes | Yes | Yes | No |
| | VoteBox | Yes | Yes | Yes | Yes |
| | Three-Ballot | No | Yes | No | No |
| | E-valg | Yes | Yes | Yes | Yes |

**Integration.** In order to be **integrated** the evaluated VVSs have some software or technological dependences (see Tab. 3 for more details). However, only VoteBox and E-valg [Sh06] ensure vote atomicity, loss resistant and tamper evident solutions.

**Technical issues.** VoteBox and Frog are more **complex** than the rest of systems, given that the former has a distributed infrastructure, and the latter is strictly tight to the separation of processes. However, VoteBox is the unique system that structurally provides distributed *replication* of sensible information, which leans to a high degree of system



**availability**. Another VoteBox's good property is its **scalability**, given that it uses homomorphic cryptography and, thus, makes easier the tally process. This property is also shared by E-valg. However, both of them should carefully address the presential remote voting, guaranteeing the necessary infrastructure in order not to overload the voting system. Finally, only Frog, VoteHere and E-valg render **flexible** on vote type and format. Notice that VoteBox, by using additive homomorphic cryptography, only supports simple types of votes. Lastly, Three-Ballot only is suitable for multi-ballot formats composed of 3 single parts, even though that the ballot content is flexible.

### 5.2 Study of trends in VVSs

From the above analysis we can extract *three clear trends* related to the following issues: (i) voting location, (ii) voting technology and (iii) degree of verifiability.

**Voting location study.** We have evaluated *poll-site-based* VVSs. All them use DREs as voting terminals. Clearly, DREs are very helpful in order to manage votes electronically. It is worth noting the demonstrated trend from *poll-site-based* to presential remote voting systems. For instance, VVAATT/VVVAT, Frog, VoteHere and Three-ballot are of the first class, and VoteBox and E-valg are presential remote voting systems. This trend is a consequence of not only the technology, but also the natural evolution in the democratic rules. However, while VoteBox was *adapted* to support presential remote voting schemes, E-valg was *structurally* designed to do so.

**Voting technology study.** We consider here the voting technology used from the ballot cast to the tally and, therefore, VVAATT/VVVAT-based systems are not considered. The idea behind this technology is to address security issues such as ballot anonymity, ballot box integrity and tally accuracy among others. These systems present a clear evolution in this issue. We detail them from simpler to more complex and reliable solutions. While Frog uses only a simple *randomization* algorithm to anonymize the votes, VoteHere uses a more reliable mixing technique to almost address *ballot anonymity*. VoteBox and Three-ballot use (computationally hard) *additive homomorphic* cryptography, to guarantee *ballot anonymity* and perform the *tally*. The most complex, but flexible and reliable technology is used by E-valg: the *hybrid scheme*, which is composed by multiplicative homomorphic cryptography (computationally less hard than additive one [Pe04, Pe09]) and mixing mechanisms. Clearly, the used technology presents a *trade-off* between ensuring (i) more secure, trustful and reliable voting technologies, while at the same time guaranteeing (ii) fast and resource-efficient ones. This trend from simple randomization techniques to hybrid schemes is a direct consequence of the continuous permeability of voting systems with regards to the last cryptographic advances.

**Verifiability study.** We can organize the analyzed systems as follows. (i) VVAATT/VVVAT-based and Frog systems provide deficient or basic verifiability in voting processes, respectively. They mainly guarantee at some degree the individual verifiability, yet the same is not true for universal or E2E verifiability. (ii) VoteHere and Three-ballot VVSs offer an acceptable degree of verifiability (individual, universal and



E2E). Finally, (iii) E-valg or VoteBox ensure a good level of verifiability, while at the same time they define a tough audit system.

To sum up with all these remarkable VVSs, VoteBox and E-valg are the best alternatives for voting systems. However, E-valg is a better voting system candidate, which should be followed closely. This is because it provides real world applications, high degree of verifiability and a smooth transition from traditional voting systems to electronic ones, incrementing its accessibility and easy-to-use.

Table 3: Detailed properties of the Voting Verification Systems.

| | | | | Frog | VVAATT / VVVAT | Vote Here | Vote Box | 3Ballot | E-valg |
|---|---|---|---|---|---|---|---|---|---|
| TECHNICAL ISSUES | Flexibility | | | ← | → | ← | → | → | ← |
| | Scalability | | | → | → | ≈ | ← | ≈ | ← |
| | Availability | | | N/A | N/A | N/A | ↑ | N/A | N/A |
| | Simplicity | | | → | ← | ← | → | ← | ← |
| INTEGRATION | Data Management | | | N/A | NA / DL | N/A | A / NDL | N/A | A / NDL |
| | Integration | | | T / SW | T | SW | T / SW | N/A | N/A |
| SECURITY | VOTING-RELATED | Auditability | | N | ≈ | N | Y | Y | Y |
| | | UNIVERSAL VERIFICATION | Tally Accuracy | N | N | Y | Y | Y | Y |
| | | | Ballot Box Integrity | ≈ | N | Y | Y | Y | Y |
| | VOTER-RELATED | Individual Verification | | ≈ | N | Y | Y | Y | Y |
| | | Coercion Resistant | | N | N | N | Y | Y | Y |
| | | Ballot Anonymity | | Y | N | Y | Y | Y | Y |
| | | Ballot Secrecy | | N | N | Y | Y | Y | Y |
| USER INTERACTION | Reliability | | | ← | ← | ← | ← | ← | ← |
| | Use Impact | | | ≈ | ← | ← | → | → | ← |
| | Accessibility | | | → | ≈ | → | ← | N/A | ← |



## 6 Conclusions

In this paper we have presented an evaluation framework, common for all systems, in order to elaborate a fair study among electronic voting verification systems (VVSs). The strong point of the present study is threefold: (i) we define the common evaluation framework, (ii) we present noteworthy VVSs from academia and real world, and (iii) we conduct a fair study and comparison among them, having the verifiability analysis as a connecting thread.

Even though the origin of e-voting systems was to accelerate the tally process, the trend is clear and firm towards not only electronic tally, but also electronic vote casting [Ba06]. Since the introduction of direct-recording electronic (DRE) voting terminals, more and more initiatives are addressing electronic casting in elections. This trend is also visible in our study.

As we have seen, good designs of e-voting systems may be significantly helpful for disabled and also for illiterate citizens. At the same time, the use of electronic voting technologies may reduce the economic and logistic costs of elections and consultations, while facilitating geographically distributed citizens to vote. Even though there are no conclusive studies, the tally accuracy on e-voting systems is higher than in paper-based voting systems [Ba06]. However, e-voting systems should not be massively introduced: it is necessary education and a sensibility rising on democracy, in a society where there exists a high ratio of abstention.

As demonstrated by the technologies used in the last e-voting systems, we foresee that the future trend on the use of electronic voting means is *remote e-voting*. In this line, there was some first *remote presential* and *Internet voting* experience. The global acceptation of these remote e-voting schemes will empower citizens with new democratic participation tools, which will likely lead to direct and binding citizen consultations and elections.

## Bibliography


[Ba04] Richard Barnes. VoteHere VHTi: A Verifiable E-Voting Protocol. Cryptography Applications Bistro. http://www.cs.virginia.edu/crab/VoteHere.pdf, 2004. [February 2010]

[Ba06] Jordi Barrat Esteve. A preliminary question: Is e-voting actually useful for our democratic institutions? what do we neet it for? In Proc. of 2nd International Conference on Electronic Voting (E-VOTE ’06), pages 51–60. GI, 2006.

[Be10] Mary Bellis. The history of voting machines. http://inventors.about.com/library/weekly/aa111300b.htm. [February 2010]

[Be07] Josh Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT’07), pages 14–14, Berkeley, CA, USA, 2007. USENIX Association.

[BJR01] Shuki Bruck, David Jefferson, and Ronald Rivest. A modular voting architecture ("frogs"). August 2001.

[CEA07] Jeremy Clark, Aleks Essex, and Carlisle Adams. On the security of ballot receipts in e2e voting systems. In Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.

[Cr07] E.V. Cross, G. Rogers, J. McClendon, W. Mitchell, K. Rouse,P. Gupta, P. Williams, I. Mkpong-Ruffin, Y. McMillian, E. Neely, J. Lane, H. Blunt, and J.E. Gilbert. Prime iii: One machine, one vote for everyone. In (On-line) Proceedings of 2007 Voting Competition Conference. http://vocomp.org/papers/primeIII.pdf. July, 2007 [February 2010]

[El05] Election Assistance Commission (USA). Voluntary voting system guidelines. http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download/file, 2005.

[Es05] Estonian National Electoral Committee. ivote. http://www.epractice.eu/en/cases/ivote, 2005.

[Ev09] E-voting.cc (competence center for electronic voting and participation) (2009): Map of electronic democracy. Modern Democracy, 2(1):8–9, 2009.

[Ne01] C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security, pages 116–125, New York, NY, USA, 2001. ACM.

[No09a] Norwegian Ministry of Local Gobernment and Regional Development. E-vote 2011: Accessibility and usability evaluation of e-vote prototypes. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf, November 2009. [February 2010]

[No09b] Norwegian Ministry of Local Gobernment and Regional Development. E-vote 2011: Contractor solution specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_ergogroup/SSA-U_Appendix_2A_Contractor_Solution_Specification.pdf, December 2009. [February 2010]

[No09c] Norwegian Ministry of Local Gobernment and Regional Development. E-vote 2011: Project directive for e-valg 2011. http://www.regjeringen.no/upload/KRD/Vedlegg/KOMM/Evalg/Project_directive_evalg2011_v101_english.pdf, February 2009. [February 2010]

[No09d] Norwegian Ministry of Local Gobernment and Regional Development. E-vote 2011: System requirements specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf, October 2009. [February 2010]

[Pe04] Kun Peng, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee. Multiplicative homomorphic e-voting. In Proceedings of 5th International Conference on Cryptology in India (INDOCRYPT '04), pages 61–72, 2004.

[PM07] Jordi Puiggali and Vitor Morales-Rocha. Independent voter verifiabilityfor remote electronic voting. In Proceedings of International Conference on Security and Cryptorgraphy (SECRYPT '07), pages 333–336, 2007.

[Pe09] Kun Peng. A hybrid e-voting scheme. In Proceedings of the 5th International Conference on Information Security Practice and Experience (ISPEC '09), pages 195–206, Berlin, Heidelberg, 2009. Springer-Verlag.

[Qv05] Matt Qvortrup. First past the postman: Voting by mail in comparative perspective. The Political Quarterly, 76(3):414–419, 2005.

[Ri06] Ronald L. Rivest. The threeballot voting system. January 2006.

[RS07] Ronald L. Rivest and Warren D. Smith. Three voting protocols: Threeballot, vav, and twin. In Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07), pages 16–16, Berkeley, CA, USA, 2007. USENIX Association.

[Sc04] Scytl Online World Security S. A. Auditability and voterverifiability for electronic voting terminals. http://www.scytl.com/_a_home/PNYX.VM_White_Paper.pdf, December 2004.

[SC05] Ted Selker and Sharon Cohen. An active approach to voting verification. http://www.vote.caltech.edu/drupal/files/working_paper/vtp_wp28.pdf, May 2005. [February 2010]

[SCM08] Altair O. Santin, Regivaldo G. Costa, and Carlos A. Maziero. A three-ballot-based secure electronic voting system. IEEE Security and Privacy, 6(3):14–21, 2008.

[SDW08] Daniel Sandler, Kyle Derr, and Dan S. Wallach. Votebox: a tamper-evident, verifiable electronic voting system. In Proceedings of the 17th conference on Security symposium (SS'08), pages 349–364, Berkeley, CA, USA, 2008. USENIX Association.

[Se04] Ted Selker. The voter verified audio audit transcript trail. http://www.dos.state.pa.us/election_reform/lib/election_reform/VVAATT_CalTech.pdf, September 2004. [February 2010]

[Sh06] Alan T. Sherman, Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, Donald F. Norris, John Pinkston, Andrew Sears, and Dongsong Zhang. An examination of vote verification technologies: findings and experiences from the maryland study. In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop (EVT'06), pages 10–10, Berkeley, CA, USA, 2006. USENIX Association.

[Sh79] Adi Shamir. How to share a secret. Commun. ACM, 22(11):612–613, 1979.

[SW08] Daniel R. Sandler and Dan S. Wallach. The case for networked remote voting precincts. In Proceedings of the conference on Electronic voting technology (EVT'08), pages 1–7, Berkeley, CA, USA, 2008. USENIX Association.

[Va01] Philip E. Varner. Vote Early, Vote Often, and VoteHere: A Security Analysis of VoteHere. PhD thesis, University of Virginia, March 2001.

[Vo10] Vote by mail: Voting historical background. http://stanvote.com/ballots.shtm#vote-by-mail, 2010. [February 2010]