

# Voting System Requirements

Ed Gerck, Safevote, Inc. Email: egerck@safevote.com

Financial Cryptography '01, Grand Cayman, BWI, Feb 21, 2001

This document presents a set of voting system requirements that are consistent, technologically neutral, can be applied to paper, electronic and network (Internet) voting, and exceed the current requirements for paper-based ballots and electronic voting DRE (Direct Recording Electronic) machines. The requirements are based on the principles of Information Theory and of trust as qualified reliance on information, favoring multiple, independent channels of information over one purportedly “strong” channel. However, adding multiple channels can also decrease reliance if the design principles laid out in these requirements are not followed.

## 1 Background

As defined by Alan Turing some fifty years ago, a mathematical method is effective if it can be set out as a list of instructions able to be followed by a human clerk who works obediently with paper and pencil, for as long as is necessary, but without insight or ingenuity. Together with Alonzo Church, Turing argued that every effective mathematical method can be carried out by a sufficiently powerful computer (represented by the universal Turing machine).

These Voting System Requirements were born out of the desire to create products that would allow modern computer-based technology to truly emulate the secure desirable properties valued in centuries of public voting. In other words, *can we use a perfect clerk in elections—one who works obediently with paper and pencil, for as long as is necessary, but without insight or ingenuity?*

Indeed, if perfect clerks would conduct an election using paper-ballots, this would provide the best model we have for a public election. Such an election would be, for example: anonymous (avoiding collusion, coercion), secret (all cast votes are unknown until the election ends) and yet correct (all votes are counted) and honest (no one can vote twice or change the vote of another), oftentimes also complete (all voters must either vote or justify absence). In such a system, if we know the voter (e.g., in voter registration) we cannot know the vote and if we know the vote (e.g., in tallying) we cannot know the voter. After an election, all votes and all voters are publicly known—but their connection is both unprovable and unknown.

*But real-life clerks are not perfect. Neither are computers.* So we need to introduce the concept of qualified reliance on information in terms of providing proofs (e.g., proof of voting, proof of correctness) that can be objectively evaluated and not just subjectively accepted or taken at face value.

To discover and rate such proofs, the Requirements employ the idea that one should favor multiple, independent communication channels over one “strong” channel—which idea was successfully used by the Moguls in India some 500 years ago in the context of combating corruption [1], and was mathematically described by Claude Shannon some 50 years ago in the context of combating noise when he introduced his Information Theory [2], a well-known general theory of communication processes.

Thus, for example, how could a voting system prove that the vote received at the ballot box is the same vote seen and cast by a voter? This question is not easier to answer if the voter is close to the ballot box, or far away. Distance plays no role, contrary to what one might think at first. The *fundamental problem of voting* is that the voter cannot see his tallied vote, hence the voter has no way of knowing if what was sent through that communication channel (which may be very short) was what was received and tallied. This problem is oftentimes called the “vote-gap problem” by the author.

To solve this question in electronic voting some advocate printing a paper copy of the ballot, which the voter can see and verify that it is identical to the ballot she intended to cast, and then sending the paper copy to ballot box A while an electronic copy of that same ballot is sent to ballot box B. The idea is that ballot box B could be tallied quickly while ballot box A would be used as a physical proof for a manual recount. Such a suggestion is oftentimes advanced as the sine qua non solution to voting reliability in electronic voting.

But what makes the introduction of a paper ballot special is not the fact that it is paper instead of bits. It is the fact that the voter is actually casting his vote twice. We now have two independent channels of information for the ballot, one from the terminal as source B, the other one from the printer as source A. So we have  $N = 2$ .

In other words, this design provides for two outputs: ballot A and ballot B. However, in the event of a discrepancy between the two, no resolution is possible from within the system. The situation can thus be summarized:

- $N = 1$  – If the system would always be similar to a perfect clerk then  $N = 1$  (one channel) would suffice, whether paper or electronic. But if we use a system with  $N = 1$ , we cannot define any level of reliance on the final result except that which was assigned a priori.
- $N = 2$  – If we add one independent channel (e.g., the paper ballot) to a system that already provides one channel (e.g., electronic ballot), this creates a system with  $N = 2$ . However, this additional channel makes the system indeterminate and still incapable of, by itself, defining any level of reliance on the final result except that which was assigned a priori (e.g., paper is more trustworthy).

Clearly, before considering other well-meant suggestions (which might be similarly ill-fated), what is necessary is to seek a logically provable solution to reliability problems caused by imperfect communication systems.

Such a solution needs to consider not only machine-machine communication channels but also human-machine communication channels because the voter can act as a source and as verifier in more than one part of the system. Further, human-human communication channels must be considered because we do not want machines to have the potential to run amok, unchecked.

Information Theory [2] can be used to describe such communication channels and, as previously noted, the concept of qualified reliance on information can be introduced as a formal definition of trust [3] in order to rate such channels in terms of providing proofs.

As a result, the only provable solution to increase reliability in communications (e.g., the communication between the voter as a sender and the ballot box as a receiver) turns out to be to increase the number/capacity of independent channels until the probability of error is as close to zero as desired (direct application of Shannon's Tenth Theorem in Information Theory [2]). To be complete, the solution considers not only machine-machine communication channels but also human-machine and human-human. Thus, if an electronic system is able to provide  $N$  proofs (human and machine based), these  $N$  proofs for some value of  $N$  larger than two will become more reliable than one so-called "physical proof"—even if this one proof is engraved in gold or printed on paper.

An undefined system also presents opportunities for fraud (e.g., someone can change and/or delete some paper ballots after the election in order to cast doubt on the integrity of the entire election) and attacks (e.g., a group of voters might agree beforehand to callout a "discrepancy" after they vote and thereby disrupt an election, which is similar to a "denial of service" attack).

**Thus, we need a real-world voting system—not one that is based on perfect parts ( $N = 1$ ) or one that produces an undefined result in the case of a single error ( $N = 2$ ). In order to provide for qualified reliance on information, such a voting system needs to have multiple independent channels.**

In plain English, the greater the number of independent channels for the verification of a result, the greater trust the result may have.

However, suppose the terminal where the voter enters his choices will change them to something else and then send this information over  $N$  different channels, what difference does it make if it is  $N = 1, 2$  or  $500$ ?

None. In such a case  $N$  would still be 1 for the ballot channel. The 2 or 500 channels are not independent for the ballot because they all originate as copies from that single stored corrupted ballot. So, it does not make a difference in terms of ballot reliance. This would, however, make a difference in terms of communication reliance, in which there are now different transmission channels, 2 or 500 channels for which each channel could behave as a correction channel for another—meaning in this case that the ballot box would more probably receive the right ballot (even though corrupted) for  $N = 500$  than for  $N = 1$ .

What is needed is thus a requirement to include several truly independent

ballot, transmission and audit channels—whether or not electronic transactions are used—and use these channels to rate the reliance on each node of an end-to-end balloting system, even during the election and in real time. There should be several ways to implement this requirement and channels could be added also in time and context, not just in space. Channels can also transport information by reference, not just information by value.

What is also needed is a way to allow the voter to verify results, for example the presence/absence of her ballot at the ballot box and whether her ballot at the ballot box is a valid one. This is useful because sufficient indirect verification does produce trust. “Trust but verify” is in our collective wisdom and it is definitely applicable here. It is important to note that even if just a fraction of the voters (e.g., 5%) do verify the results, the capability of verification is already a deterrent to fraud because a fraudster has no way of knowing who will verify, or not.

*Another characteristic of a good voting system is that the only person whom you prove the vote to is the voter.* If the proof can be shown to someone else, then the vote can be coerced or sold. Therefore, when using multiple channels of information, they either have to be deniable by the voter or else temporary so that the voter cannot be threatened or hurt as a result of the vote.

Regarding the use of paper, it is important to note that the reason to distrust a paper/electronic voting system with  $N = 2$  is not based on a distrust of paper. Paper is just another communication channel. The reason is that adding paper does not solve the problem and makes the problem indeterminate. The reason is thus that we need  $N$  larger than 2. Certainly, paper can be one of the channels, if desired, because the channel make-up is irrelevant. But a cost-benefit analysis might result in the use of non-paper channels.

**Another question that must be addressed is thus the possibility of all-electronic voting systems. Should we trust them and why?**

Nowadays, all-electronic systems and computers are used to fly commercial and military jets. And yet, no one in the public is afraid that a terrorist will introduce a virus in the system and down all commercial jets worldwide, or all U.S. military jets. Why? Because there is a designed redundancy at many levels in the system. For example, there are three independent laser inertial navigation sensors and any decision on the plane’s position depends on the agreement of at least two, which decision is further verified by a GPS system, as well as flight time and speed calculations.

Thus, voting systems—like any other system—derive their trustworthiness from the fact that they work consistently, both conceptually and perceptually. However, in the absence of an easy conceptual understanding of the system (e.g., a laser inertial navigation sensor) that the average user could grasp, a sufficiently coherent perceptual understanding (e.g., it works) is enough to eventually build trust in the system.

Trust may also be denied by the design itself, because disasters may occur at any time if the principles of communication reliance (i.e., trust itself) are not taken into account. Imagine a plane that would be flown with just two navigation sensors, one compass-based and the other electronic—we would then

have an idea of the disastrous consequences of using a paper/ electronic voting system with  $N = 2$ , even though a physical channel is used (compass, paper).

Thus, the deciding factor in trusting a system is not whether it includes one or even two sources of information that can be touched or seen in physical form (e.g., a paper in your hands, a paper behind a screen, a compass needle behind a screen).

A factor that mitigates against an all-electronic voting system is the fact that although paper and electronic records are both vulnerable to subversion, it is a lot easier to change what is in an electronic record than it is to change what is on paper.

Thus, electronic records need to be bound to other references in a manner that is demonstrably inaccessible to an attacker, both through physical access controls and through cryptographic protocols.

Moreover, there really needs to be a step-by-step description of the voting process, so that when someone asks, “What if the intruder succeeds in breaking into the system to change X?” this can be clearly answered, for example, by:

- (i) to change X would cause a subsequent binding failure, thus it would be detectable except with parallel access to Y and Z, which are independently inaccessible, or
- (ii) knowledge of an alternate (and attacker-desirable) value for X is insurmountably difficult to achieve, and the effort could not be leveraged to any other X.

Put most plainly, people know that ordinary voting systems can be subverted by someone who could bribe enough individuals to collude, but the physical fact of several tons of paper ballots still represents somewhat of an obstacle to an “easy subversion” in the eyes of many.

In contrast, people are well aware that electronically one can modify a million records with as little as a few keystrokes. This is the “fear” that needs to be addressed in an all-electronic system that such a subversion can be so massive and rapid, executed from the safety of a remote laptop, etc. that it would be unavoidable.

Of course, one alternative to reduce fear would be education. To educate voters regarding the very nature of distributed cryptographic assurances and at a level where the concepts are not clothed in excessive abstractions.

But cryptography is not by itself the critical issue, nor the silver bullet. And no amount of education will stop attackers, while it may aid them.

Instead, *voting systems can use the concept of multiple independent communication channels to make it as impossible as desired to tamper with the electronic ballot both before and after it is cast.*

Here, the question is not how many copies of paper or bits one has, but how many independent channels the attacker needs to subvert versus how many independent correction channels one has available during such an attack. Of course, if the attacker is able to subvert the correction channels while attacking the other channels, then they would not be independent.

Therefore, the same mechanism that protects casting the ballot must also be used to protect presenting the ballot. And this needs to be given as a set of Requirements that work together in an end-to-end design. The make-up of each channel’s carrier (e.g., paper, bits, electrons) is by itself irrelevant.

These Requirements are therefore general principles, valid for any physical implementation of a “ballot”—whether as print marks on paper, pits on a CD-ROM surface, electrons hitting a video screen (electronic ballot), modulated electromagnetic waves, bits in a network protocol or any other form of information transfer to and from the voter. They also apply to any form of voting, including majority voting and single transferable votes. The Requirements may be wholly applied or just a subset may be used.

To achieve these goals, the Requirements should be able to handle voting rules of any type and could apply to voting systems anywhere in the world. However, the main objective here is for the Requirements to be as complete and independent from one another as possible, without sacrificing consistency. It is understood that “completeness” is an elusive goal that might never be reached when we consider the diversity of election needs [4], while “consistency” is a necessary feature for the Requirements to work together in a particular election. In short, this was the reason to stop the Requirements with # 16. Increasing the number of Requirements could risk decreasing their consistency, in general [4]. Of course, other Requirements may be added, or deleted, as needed.

Some of the words used in the Requirements may have different (and equally valid) meanings in other contexts (e.g., “voter privacy”). Therefore, the Requirements also include the operational definitions for the main words used. Three words are, however, used without a definition even though they could also be misunderstood. These words are “trust” [3], “manifold” and “mesh-work” [5], as defined in the references.

## 2 Summary of Requirements

A voting system, whether using paper, electronic recording or networks such as the Internet, needs thus to satisfy various requirements, which are summarized in 16 main points.

**1. Fail-safe voter privacy.** Definition: “Voter privacy is the inability to link a voter to a vote.” Voter privacy MUST be fail-safe—i.e., it MUST be assured even if everything fails, everyone colludes and there is a court order to reveal all election data. Voter privacy MUST be preserved even after the election ends, for a time long enough to preserve backward and forward election integrity (e.g., to prevent future coercion due to a past vote, which possibility might be used to influence a vote before it is cast).

**2. Collusion-free vote secrecy.** Definition: “Vote secrecy is the inability to know what the vote is.” Vote secrecy MUST be assured even if all ballots and decryption keys are made known by collusion, attacks or faults (i.e., vote secrecy MUST NOT depend only on communication protocol and cryptographic assumptions, or on a threshold of collusion for the keyholders).

**3. Verifiable election integrity.** Definition: “Election integrity is the inability of any number of parties to influence the outcome of an election except by properly voting.” The system **MUST** provide for verifiability of election integrity for all votes cast. For any voter the system **MUST** also provide for direct verifiability that there is one and only one valid ballot cast by the voter at the ballot box.

**4. Fail-safe privacy in verification.** If all encrypted ballots are verified, even with court order and/or with very large computational resources, the voter’s name for each ballot **MUST NOT** be revealed.

**5. Physical recounting and auditing.** **MUST** provide for reliability in auditing and vote recounting, with an error rate as low as desired or, less strictly, with an error rate comparable or better than conventional voting systems [8]. The auditing and vote proofs **MUST** be capable of being physically stored, recalled and compared off-line and in real-time during the election, without compromising election integrity or voter privacy, and allowing effective human verification as defined by election rules.

**6. 100% accuracy.** Every vote or absence of vote (blank vote) **MUST** be correctly counted, with zero error [8].

**7. Represent blank votes.** **MUST** allow voters to change choices from ‘vote’ to ‘blank vote’ and vice-versa, at will, for any race and number of times, before casting the ballot.

**8. Prevent overvotes.** As defined by election rules. **MUST** provide automatic “radio button” action for single-vote races. If overvoting is detected in multiple-vote races, **MUST** warn the voter that a vote has to be cleared if changing choices is desired. This warning **MUST** be made known only to the voter, without public disclosure.

**9. Provide for null ballots.** As defined by election rules, **MAY** allow voters to null races or even the entire ballot as an option (e.g., to counter coercion; to protest against lack of voting options). Overvoting, otherwise prevented by Requirement #8, **MAY** be used as a mechanism to provide for null ballots.

**10. Allow undervotes.** As defined by election rules, the voter **MAY** receive a warning of undervoting. However, such a warning **MUST NOT** be public and **MUST NOT** prevent undervoting.

**11. Authenticated ballot styles.** The ballot style and ballot rotation to be used by each voter **MUST** be authenticated and **MUST** be provided without any other control structure but that given by the voter authentication process itself.

**12. Manifold of links.** **MUST** use a manifold [5] of redundant links and keys to securely define, authenticate and control ballots. **MUST** avoid single points of failure—even if improbable. If networks are used, **MUST** forestall Denial-of-Service (DoS) and other attacks with an error rate comparable or better than conventional voting systems [8].

**13. Off-line secure control structure.** **MUST** provide for an off-line secure end-to-end control structure for ballots. **MAY** use digital certificates under a single authority. Ballot control **MUST** be data-independent, representation-independent and language-independent.

**14. Technology independent.** MUST allow ballots and their control to be used off-line and/or in dial-up and/or in networks such as the Internet, with standard PCs or hand-held devices used to implement their components in hardware or in software, alone or in combination for each part.

**15. Authenticated user-defined presentation.** MUST enable the ballots to dynamically support multiple languages, font sizes and layouts, so that voters could choose the language and display format they would be most comfortable with when voting as allowed by law and required by voters with disabilities, without any compromise or change to the overall system, from an authenticated list of choices defined by election rules.

**16. Open review, open code.** Allow all source code to be publicly known and verified (open source code, open peer review). The availability and security of the system must not rely on keeping its code or rules secret (which cannot be guaranteed), or in limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or in preventing an attacker from observing any number of ballots and protocol messages (which cannot be guaranteed). The system SHOULD have zero-knowledge properties (i.e., observation of system messages do not reveal any information about the system). Only keys MUST be considered secret.

### 3 Comments

Implementations and examples [9] are discussed in the full paper, available at [10].

These Requirements include comments and references from Tony Bartoletti, Thomas Blood, Netiva Caftori, Gordon Cook, Hal Dasinger, Hugh Denton, Rosario Gennaro, Jason Kitcat, Brook Lakew, Elaine Maurer, Don Mitchel, Erik Nilsson, Michael Norden, Marcelo Pettengill, Roy Saltman, Bernard Soriano, Gene Spafford, Einar Stefferud, Arnold Urken, Eva Waskell, Thom Wysong, the IVTA tech WG ([www.mail-archive.com/tech@ivta.org/](http://www.mail-archive.com/tech@ivta.org/)), the CPSR-activists list, several cryptography lists, contributions from comments collected at Safevote's website and from articles published in The Bell ([www.thebell.net](http://www.thebell.net)).

### 4 References

[1] "... one of the earliest references to the security design I mentioned can be found some five hundred years ago in the Hindu governments of the Mogul period, who are known to have used at least three parallel reporting channels to survey their provinces with some degree of reliability, notwithstanding the additional efforts." Ed Gerck, in an interview by Eva Waskell, "California Internet Voting." The Bell, Vol. 1, No. 6, ISSN 1530-048X, October 2000. Available online at [www.thebell.net](http://www.thebell.net)

[2] Shannon, C., "A Mathematical Theory of Communication." Bell Syst. Tech. J., vol. 27, pp. 379-423, July 1948. Available online at [cm.bell-](http://cm.bell-)

labs.com/cm/ms/what/shannonday/paper.html. Shannon begins this pioneering paper on information theory by observing that *“the fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.”* He then proceeds to so thoroughly establish the foundations of information theory that his framework and terminology have remained standard practice. In 1949, Shannon published an innovative approach to cryptography, based on his previous Information Theory paper, entitled Communication Theory of Secrecy Systems. This work is now generally credited with transforming cryptography from an art to a science. Shannon’s Tenth Theorem states (cf. Krippendorf and other current wording): *“With the addition of a correction channel equal to or exceeding in capacity the amount of noise in the original channel, it is possible to so encode the correction data sent over this channel that all but an arbitrarily small fraction of the errors contributing to the noise are corrected. This is not possible if the capacity of the correction channel is less than the noise.”*

[3] *“When we want to understand what trust is, in terms of a communication process, we understand that trust has nothing to do with feelings or emotions. Trust is that which is essential to communication, but cannot be transferred in the same channel. We always need a parallel channel. So the question is having redundancy. When we look at the trust issue in voting, it is thus simply not possible to rely on one thing, or two things even if that thing is paper. We need to rely on more than two so we can decide which one is correct. In this sense, the whole question of whether the Internet is trusted or not is simply not defined. The Internet is a communication medium and whatever we do in terms of trust, it is something that must run on parallel channels.”* Ed Gerck, testimony before the California Assembly Elections & Reapportionment Committee on January 17, 2001, in Sacramento. Assemblyman John Longville (D), Chair. For an application of this model of trust to digital certificates, see “Trust Points” from [www.mcg.org.br/trustdef.txt](http://www.mcg.org.br/trustdef.txt) excerpted in “Digital Certificates: Applied Internet Security” by J. Feghhi, J. Feghhi and P. Williams, Addison-Wesley, ISBN 0-20-130980-7, p. 194-195, 1998.

[4] This is similar to the situation found in Goedel’s incompleteness theorem. The Requirements form a logical system of some complexity and thus we do not expect such a system to be both complete and consistent.

[5] “Manifold” means a whole that unites or consists of many diverse elements and connections, without requiring these elements and connections to depend upon one another in any way. “Meshwork” is used to denote a manifold in the context of the Multi-Party protocol designed by Safevote to implement the Requirements. A meshwork builds a meta-space in relationship to a space—a meshwork describes relationships about a space, not the space itself.

[6] *“We say that information-theoretic privacy is achieved when the ballots are indistinguishable independent of any cryptographic assumption; otherwise we will say that computational privacy is achieved.”* In Ronald Cramer, Rosario Gennaro, Berry Schoenmakers, “A Secure and Optimally Efficient Multi-Authority Election Scheme,” Proc. of EUROCRYPT-97.

Available online at [www.research.ibm.com/security/election.ps](http://www.research.ibm.com/security/election.ps)

[7] E. Gerck, “Fail-Safe Voter Privacy”, The Bell, Vol.1, No.8, p. 6, 2000. ISSN 1530-048X. Available online at [www.thebell.net/archives/thebell1.8.pdf](http://www.thebell.net/archives/thebell1.8.pdf)

[8] *Accuracy* and *Reliability* are used here in standard engineering terminology, even though these different concepts are usually confused in non-technical circles. Lack of accuracy and/or reliability introduces different types of errors:

(i) Reliability affects a number of events in time and/or space, for example, errors in transfers between memory registers. We know from Shannon’s Tenth Theorem [2] that reliability can be increased so that the probability of such an error is reduced to a value as close to zero as desired. This is a capability assertion. It does not tell us how to do it, just that it is possible. This is the realm of Requirements #12 and also #5, where one can specify an error rate as low as desired or, less strictly, an error rate “comparable or better than conventional voting systems”.

(ii) Accuracy affects the spread of one event, for example whether a vote exists. Here, Requirement #6 calls for 100% accuracy. The Requirement is that no “voter-intent” or “chad” or “scanning” issue should exist—which is feasible if, for example, each voting action is immediately converted to a standard digital form that the voter verifies for that event. Accuracy error can be set to zero because 100% accuracy is attainable in properly designed digital systems that (e.g., by including the voter) have no digitization error.

For an illustration of the above definitions of accuracy and reliability, see the four diagrams in [www.safevote.com/caltech2001.ppt](http://www.safevote.com/caltech2001.ppt)

[9] “Contra Costa Final Report” by Safevote, Inc. Available upon request. Summary available at [www.safevote.com](http://www.safevote.com)

[10] “Voting System Requirements”, The Bell newsletter, ISSN 1530-048X, February 2001, archived at [www.thebell.net/archives/thebell2.2.pdf](http://www.thebell.net/archives/thebell2.2.pdf)