# End to end verifiability: what it is and what it’s for

DRAFT June 30th, 2014. Based on discussion so far including Josh Benaloh, Ron Rivest, Peter Ryan, Philip Stark, Vanessa Teague & Poorvi Vora. Other input welcome.

This pamphlet aims to describe end-to-end election verifiability (E2E-V) to a nontechnical audience. We start by describing what problem E2E-V aims to solve, then offer a concrete (but non-technical) definition, then discuss the remaining outstanding issues. We conclude with some specific examples of real deployments and some suggestions for future practical directions. Our intended audience is election officials, public policymakers, and anyone else with an interest in running secure, transparent and evidence-based electronic elections.

## Introduction

Getting the election outcome right isn’t good enough. The outcome must also be demonstrated, with evidence, to be correct.

In an idealised election, all voters vote in their home polling places on paper ballots, and every candidate sends observers to watch the ballot boxes throughout the day and to scrutinize the count afterwards. Then, the announced outcome comes with an evidence trail attested to by everyone who was present. Properly implemented paper recounts, conducted transparently under observation, can reinforce (or sometimes reverse with evidence) the announced outcome.

Of course, in the real world observers don’t always show up; remote voters must cast their ballots through insecure methods such as (snail) mail; and many elections are so large that hand counts are infeasible or so complicated (e.g. IRV) that they can’t be counted at the precinct.

How can we produce convincing evidence that election outcomes are correct when elections are large and voters mobile? Most of the USA has (slowly) accepted that electronic records from paperless DREs are not good evidence, motivating a return to permanent paper records. New techniques for risk-limiting audits have convinced most people that a properly conducted random audit is a good (and much cheaper) substitute for a full manual count in many circumstances. But audits still rely on the integrity and completeness of the paper records that are audited—which itself requires evidence. The integrity of the audit trail may be difficult to guarantee. It may be verifiable (for ballots cast in person) or not (for remote voting). The problem of verifiably secure transport and storage of paper records is particularly acute for remote voting, whether in a supervised or unsupervised polling place.

End to end cryptographic verifiability is a collection of techniques for replicating and in some ways exceeding the standards of evidence provided by an ideal, observed, polling place. This includes

* inviting voters to verify that their (electronic or paper) votes are cast according to their intention, and
* allowing the public to verify that all the cast votes are correctly included in the tally

Of course, all these kinds of verification involve some assumptions. (End to end verifiability implies software independence, assuming you can find at least some valid verification software.)

## About end to end verifiability

### What is it?

It’s really a question of trust. In the ideal polling place we imagined earlier, there were no trusted officials and no trusted hardware or software. The only assumption was that the observers paid careful attention to the evidence they were shown, and told the truth about it afterwards.

*End to end verifiable election techniques aim to produce an election result that requires no trust to be vested in software, hardware, election officials or even observers.[[1]](#footnote-1)*

In practice the verification steps are performed by sophisticated software, so everyone would have to choose some version(s) of the verification software to run, and trust that at least one of them was correct. Voters also need to trust that other voters are checking their votes.

### Why would you want it?

Because the flip side of having no need to trust components or people is the production of an evidence trail that links every step of the voting process from voters expressing their intentions to the announcement of a result.

### How can you tell whether you’ve got it?

Now that end to end verifiability has become so popular, numerous electronic voting software vendors have decided they (already) sell it. Claims are easy to make, but implementing E2E-V methods is not easy—despite having examined many commercial products, we know of no vendors that do offer true E2E-V. The crucial properties are the two kinds of verification mentioned above, with complete freedom about which software to trust to do the verifying. If your voters and election observers do not have complete freedom about which software to trust to do the verification, or if only a privileged few are able to verify at all, then the system is not offering genuine E2E-V.

### What procedures are necessary to support it (does it still need paper? Audits?)?

A verifiable election that nobody bothers to verify does not produce any meaningful evidence. Just as a VVPAT only helps if voters actually check their own votes and auditors actually audit the evidence trail, end-to-end verifiability provides little evidence unless enough voters do their part and the public performs the verification necessary for producing the evidence. These procedures vary between end-to-end verifiable systems, but they are in general a considerable extra burden on voters and election officials. In particular, the voters’ role may be quite complicated; usability is a big concern. It would be difficult to make sure voters got the procedures right if they were voting from home.

Running an end to end verifiable system correctly requires substantial new training for pollworkers and careful following of unfamiliar procedures. If the correct procedures are not followed, undetectable vote manipulation may be possible, or the announced election result may not be supported by convincing evidence.

### What trust assumptions remain?

Just because people *can* verify, doesn’t mean that enough of them did, in a sufficiently unpredictable way, to induce confidence in the result. If voters care to verify, they can;

if not enough voters care to verify, then the system doesn’t necessarily produce enough evidence to support the election result.

The argument hinges on the unpredictability of voter verification. If there is systematic fraud, it will likely be discovered with only a small number of verifications, as long as the perpetrators of the fraud can’t predict reliably that certain votes or processes will not be verified. Some verification (such as the voter’s opportunity to check that their votes are cast as intended) must be performed on the spot, before the election outcome is known. Other kinds, such as a universal check of correct tallying, can be performed afterwards, by anyone. For example, people could choose to double-check only those tallies that were close.

(By contrast, statistical methods such as Risk Limiting Audits use a public random auditing process to make an argument about the statistical confidence with which a particular election result is supported. Applying such methods to E2E-V is an area of ongoing research; at present, we make a non-quantitative argument based on assuming that individuals audit in a way that an attacker finds difficult to predict.)

Much of the actual verification must be done by computer, which means that (ideally) people would write and compile their own algorithms for checking the proofs. Not everyone is capable of understanding, let alone implementing, this sort of code. In practice voters and candidates might choose some computer scientists, software engineers, and software libraries to trust in each election. This is certainly different from the process of trusting a small number of election observers, who are at least performing a relatively simple task that everyone can understand.

The crucial distinction is that, for e2e verifiable systems, each participant can choose with complete freedom which verification software they trust. They can use several different systems if they like. If there is a discrepancy in the outputs of two different verifiers, they can be examined until the discrepancy is resolved.

### What can still go wrong?

Anything can still go wrong, but at least everyone will know that it did!

## Other important properties of electronic elections

Electronic elections need lots of other properties apart from end to end verifiability.

### Privacy.

It should be infeasible to discover how individuals voted, even after corrupting some of the central computers or election administrators. Systems vary in whether the computer used for voting learns the voter’s choices. In general, even with E2E-V systems, voters must trust election officials (and programmers) to ensure the privacy of their votes.

### Receipt freeness/coercion resistance.

Any voting in an unsupervised location exposes the voter to potential coercion because the voting process is not private. Indeed, it has been argued (cite Josh) that modern wearable recording equipment makes privacy all but impossible even in a supervised polling place.

However, electronic systems vary in whether they allow the voter subsequently to prove how they voted to someone who did not observe them vote (either physically or electronically). If it is impossible for the voter to produce such a proof, the system is receipt free. If it is receipt free and even impossible for the voter to prove whether or not they voted, it is coercion resistant. Attendance end to end verifiable systems can be made receipt-free (for example, prêt à voter and Scantegrity II), but receipt freeness (and hence coercion resistance) seems intractable for remote voting.

### Eligibility verifiability.

Some systems produce a list of those who voted, allowing anyone to verify that all votes came from eligible voters (each voting exactly once). Other systems deliberately hide this information for privacy reasons.

### Dispute resolution (accountability, non repudiation, defense against defaming).

Our discussion of verification has so far included only a description of what can be verified. However, a system would need to specify what happens if verification fails, meaning that a problem such as incorrect vote recording or vote manipulation has been detected. Authorities and other observers would need a way of understanding whether the problem is genuine and how much of the election could be affected.

For example, many end to end verifiable systems provide voters with some sort of paper receipt at the time of voting. The voter takes this out of the polling place, and uses the information on it to check that their vote was correctly included in the count. If such receipts are easy to counterfeit, then voters can falsely accuse the system of omitting a vote (this is sometimes called a “defaming attack”). Although they cannot manipulate votes undetectably, they can destroy confidence in the system by pretending that someone else has manipulated the votes. Recent versions of prêt à voter, such as the vVote system, print a digital signature on each receipt. This prevents defaming and ensures that every voter has proof if their vote was omitted.

As another example, Scantegrity II provides voters with a short return code (a couple of letters) which they can use later to prove that their vote should have been included. If they attempted to defame the system by falsely accusing it of omitting their vote, they would need to guess the right short code. This is difficult but not impossible---if there are thousands of false accusations against Scantegrity II, we should expect a handful of correct guesses (and still be unconvinced).

## Practical deployments of E2E-V

There have been numerous small trials of end-to-end verifiable voting systems, each with different designs. Most have so far been deployed in non-government elections, but some are proposed, and one has been trialled, in a binding government election. As far as we know no end-to-end verifiable Internet voting scheme has been used for large-scale binding government elections, nor is proposed in the near future. The following examples are divided into attendance (polling-place) E2E-V systems and Internet voting E2E-V systems.

### Polling-place E2E-V schemes in practice

#### Scantegrity II Takoma park (+Remotegrity)

The groundbreaking project to use the Scantegrity II system in Takoma Park is still the only example of true end-to-end verifiability to have been used in binding government elections (though others are proposed for the future). The Scantegrity II system combines cryptographic techniques for allowing each voter to verify their vote is cast as they intended and correctly included, and allowing anyone to verify the tally, with familiar opscan-like ballots that can be treated like an ordinary paper evidence trail.

The same project also incorporates a remote voting option, called Remotegrity, in which voters receive a code sheet by snail mail which then allows them to cast their vote over an end-to-end verifiable Internet voting system.

Although highly successful as an example of putting research into practice, this project has been discontinued.

#### Wombat

The Wombat voting system (<http://www.wombat-voting.com/>) combines a paper evidence trail with an E2E-V cryptographic system. It has been used in several non-government elections in Israel.

#### StarVote

The StarVote project, which is expected to be used for binding government elections in Travis County, Texas, also combines a paper evidence trail with an E2E-V voting system. Methods for facilitating risk-limiting audits of the paper trail are incorporated too.

#### vVote (prêt à voter)

The prêt à voter E2E-V voting system is particularly appropriate for complex election schemes such as IRV/STV, for which opscan-like systems are too hard to use. A version called vVote, tailored for Australian elections, is expected to be used for binding State government elections in the Australian state of Victoria, in November 2014.

### Internet E2E-V schemes in practice

#### Helios

The Helios E2E-V Internet voting system (vote.heliosvoting.org) has been used successfully in numerous non-government elections including the board of the International Association of Cryptologic Research (IACR) and elections at Princeton, the Université Catholique de Louvain, and many others.

#### Demos

During the 2014 European parliamentary elections, a group of Greek researchers ran an E2E-V Internet voting system that mimicked the real election that was running at the same time. They received 747 votes and conducted an extensive examination of the participants’ attitudes and experiences with E2E-Verifiable voting. http://www.demos-voting.com/en/demos\_voting\_system/Euro\_Elections\_2014.html

### Non-E2E-V systems worth noting

Civitas (<http://www.cs.cornell.edu/projects/civitas/>) is a coercion-resistant Internet voting system that provides openly verifiable evidence that all the votes are correctly included and accurately tallied. However, it does not currently allow voters to verify that their votes are cast as they intended---they must trust the computer they use for voting.

The now-discontinued Norwegian Internet voting system used many clever techniques for defending against certain kinds of attacks on the integrity of the votes. Although not genuinely end-to-end verifiable, it incorporated an elegant code-based system for allowing voters to check that their votes were cast as they intended even if their voting machine misbehaved. It also provided some evidence to some restricted observers about the accuracy of the final tally.

## Suggested directions towards deploying e2e verifiable Internet voting

Internet voting should not be attempted without E2E-verifiability, because of the risk of undetectable electoral manipulation.

The only viable path forward for Internet voting is to implement the following steps in succession.

1. First build and deploy an in-person (polling-place) E2E-verifiable voting system that enables traditional tallying and incorporation of current best practices and safeguards in parallel with an E2E-verifiable tallying mechanism.  The traditional and E2E-verifiable tallies should be tightly bound to avoid production of two tallies that do not agree.  Ideally, all voters in a jurisdiction would use this system.
2. However, if a system offering E2E-verifiability is used for only some of the votes within any jurisdiction, it must be combined with the other votes in a way that produces meaningful evidence of the correctness of the election result. For example,
   1. if most voters use the E2E-V system but a small fraction of voters in a jurisdiction cast votes via another medium, then these votes should be recorded and incorporated into the E2E-verifiable system by election workers – even though these voters would not enjoy the “individual verifiability” property available to in-person voters.
   2. If a large fraction of voters cast their votes on a traditional system with an observed paper-based evidence trail, but a small number (such as those at a polling place not near their home) use an E2E-V system, then the votes from the E2E-V system should be incorporated in a way that at least matches the trust assumptions of the paper-based evidence trail. For example, observers who are watching a manual paper count should have an opportunity to ensure that the output of the E2E-V system is properly incorporated into the paper count. The result is not E2E-V, but may be an improvement upon a traditional system with unobservable paper ballot transport.
3. Once an in-person E2E-verifiable voting system is in-place and proven, a compatible E2E-verifiable Internet voting system could be implemented in which combined tallies are reported and remote voters are able to achieve individual verifiability in a manner that may be different from that of in-person voters.

Note that we are not asserting that Internet voting is viable if the above steps are followed.  Instead, we believe the opposite – that Internet voting is not viable if these steps are not followed.

1. Voters still must trust other voters to check that *their* votes were cast as intended and were recorded, and voters must trust the elections officials, programmers, and others to ensure the anonymity of their votes. [↑](#footnote-ref-1)