

Tradeoffs for Internet Voting Options

Submitted to SB11 Working Group
Jeremy Epstein
October 13 2015

Purpose

The purpose of this document is to identify advantages and disadvantages of several different approaches to internet voting, when assumed to be used with a CAC card. All of the options share certain potential advantages and disadvantages compared to not having internet voting.

All previous studies have concluded that internet voting is not doable securely using today's technology, including reports from Utah, Connecticut, the technical experts group (E2E-VIV), Heritage Foundation, etc. This tradeoff document should be seen in that light – not that any of the proposed solutions is acceptable, but to identify the pros & cons of each, within the scope that none are acceptable.

Other designs beyond those sketched here are possible; the advantages & disadvantages will vary slightly.

All of the choices are expensive, but the expense varies – the email solutions require the least technology development, but the most training and highest per-ballot cost, while the web form requires the most technology development, and the lowest per-ballot cost. Centralized solutions at the State Board of Elections are likely to be less expensive (because there is no need to maintain 140+ installations, and train 140+ sets of users), but introduce the bottleneck of distributing ballots.

Advantages of all approaches

- Perception – gives voters impression of being more modern
- Timeliness - allows military voters to cast their vote from wherever they are, up until the last minute
- CAC signature can be used to validate voter identity (compare CAC digital signature to name on form)

Disadvantages of all approaches

- Cost – prior internet voting efforts have cost up to thousands of dollars per vote, when including cost of software development/maintenance/testing, operation, monitoring for attacks, etc.
- Security – risks of vote tampering – none of the approaches provide a secure solution, including vulnerability to attacks on state servers, risks of malware in voter's computer, etc.

- Privacy – risks of loss of voter privacy – none of the approaches provide a secret ballot
- Turnout – none of the approaches are likely to increase voter turnout

Alternatives

Six alternatives are considered, along two axes (technical approach and use of central vs. locality-based receipt):

- Email to each locality
- Email to a central facility & distribution
- Web upload to each locality
- Web upload to a central facility & distribution
- Web form for each locality
- Web form at a central facility & distribution

The following subsections offer a brief description of a design using a CAC card, followed by advantages & disadvantages.

Email to each locality

Description: Voter gets blank ballot from local election office via email. Voter uses CAC card to digitally sign an email containing a PDF or JPG of the ballot and associated affidavit, which is sent to voter's locality. PDF could be either an image of the ballot (i.e., a scan), or a filled out form. Locality receives & prints ballot.

Advantages:

- If using a filled-out form, can prevent over/under votes
- Simplest for voters to use
- Allows voters to submit ballots up until last minute, without having to distribute ballots from a central site
- No changes required for each election, because there's no "smarts" in email handling

Disadvantages:

- Email is unencrypted – while CAC can provide encryption, actual CAC cards are not set up that way for most users, and can only be sent to other CAC cards (of which the localities would not be listed in the database); point-to-point encryption is possible, but not end-to-end
- Risk to localities: if ballot contains malware, when locality opens it, will get infected – so each locality needs security measures in place
- Training – would require training each locality how to handle and verify signed ballots
- Phishing – need to train voters to submit ballots to their election office email address, and not be subject to phishing attacks

Email to a central facility & distribution

Description: Voter gets blank ballot from local election office via email. Voter uses CAC card to digitally sign an email containing a PDF or JPG of the ballot and associated affidavit, which is sent to State Board of Elections. PDF could be either an image of the ballot (i.e., a scan), or a filled out form. SBE prints ballot & affidavit, forwards them in paper form to locality.

Advantages:

- If using a filled-out form, can prevent over/under votes
- Simplest for voters to use
- Allows voters to submit ballots until relatively close to deadline (but need a way to redistribute ballots from SBE)
- No changes required for each election, because there's no "smarts" in email handling

Disadvantages:

- Email is unencrypted – while CAC can provide encryption, actual CAC cards are not set up that way for most users, and can only be sent to other CAC cards (of which the SBE would not be listed in the database); point-to-point encryption is possible, but not end-to-end
- Risk to SBE: if ballot contains malware, when locality opens it, will get infected – central facilities needs appropriate security measures (but just one site vs. 140+ for previous option)
- Training – would require training SBE how to handle and verify signed ballots (but just one site vs. 140+ for previous option)
- Phishing – need to train voters to submit ballots to SBE office, which is easier than training 140+ different offices

Web upload to each locality

Description: Voter gets blank ballot from local election office via email. Voter uses CAC card to digitally sign a PDF or JPG image of the ballot and associated affidavit, which is uploaded to a web site maintained by the voter's locality. PDF could be either an image of the ballot (i.e., a scan), or a filled out form.

Advantages:

- If using a filled-out form, can prevent over/under votes
- Allows voters to submit ballots up until last minute, without having to distribute ballots from a central site
- Provides end-to-end encryption of the ballot from voter to election office, using HTTP/S, and then (potential) re-encryption of the ballot before storage
- No changes required for each election, because there's no "smarts" in file upload

Disadvantages:

- Risk to localities: if ballot contains malware, when locality opens it, will get infected – so each locality needs security measures in place
- Training – would require training each locality how to handle and verify signed ballots
- Phishing – need to train voters to submit ballots to their election office web site, and not be subject to phishing attacks

Web upload to a central facility & distribution

Description: Voter gets blank ballot from local election office via email. Voter uses CAC card to digitally sign a PDF or JPG image of the ballot and associated affidavit, which is uploaded to a web site maintained by the SBE. PDF could be either an image of the ballot (i.e., a scan), or a filled out form. SBE prints ballot & affidavit, forwards them in paper form to locality.

Advantages:

- If using a filled-out form, can prevent over/under votes
- Allows voters to submit ballots until relatively close to deadline (but need a way to redistribute ballots from SBE)
- Provides end-to-end encryption of the ballot from voter to election office, using HTTP/S, and then (potential) re-encryption of the ballot before storage
- No changes required for each election, because there's no "smarts" in file upload

Disadvantages:

- Risk to SBE: if ballot contains malware, when locality opens it, will get infected – central facilities needs appropriate security measures (but just one site vs. 140+ for previous option)
- Training – would require training SBE how to handle and verify signed ballots (but just one site vs. 140+ for previous option)
- Phishing – need to train voters to submit ballots to SBE office, which is easier than training 140+ different offices

Web form for each locality

Description: No distribution of blank ballots to voters. Voter goes to web site maintained by locality, fills out form, which generates a submission including the voter's identifying information, selections. May be possible to provide digital signatures on submissions.

Advantages:

- Best at preventing under/over votes
- Allows voters to submit ballots up until last minute, without having to distribute ballots from a central site
- Provides end-to-end encryption of the choices from voter to election office, using HTTP/S, and then (potential) re-encryption of the ballot before storage
- If designed appropriately, eliminates risk of malware submission
- Commercial products are available

Disadvantages:

- Unclear whether CAC digital signatures could be used
- Phishing – need to train voters to submit ballots to their election office web site, and not be subject to phishing attacks
- The riskiest solution, as custom software solutions are the most likely to have functional or security flaws
- Must be reprogrammed for each election, to reflect what's on the ballot

Web form at a central facility & distribution

Description: No distribution of blank ballots to voters. Voter goes to web site maintained by SBE, fills out form, which generates a submission including the voter's identifying information, selections. May be possible to provide digital signatures on submissions. SBE prints ballot & affidavit, forwards them in paper form to locality.

Advantages:

- Best at preventing under/over votes
- Allows voters to submit ballots until relatively close to deadline (but need a way to redistribute ballots from SBE)
- Provides end-to-end encryption of the choices from voter to SBE, using HTTP/S, and then (potential) re-encryption of the ballot before storage
- If designed appropriately, eliminates risk of malware submission
- Commercial products are available

Disadvantages:

- Unclear whether CAC digital signatures could be used
- Phishing – need to train voters to submit ballots to SBE web site, and not be subject to phishing attacks
- The riskiest solution, as custom software solutions are the most likely to have functional or security flaws
- Must be reprogrammed for each election, to reflect what's on the ballot
- Scaling is potentially problematic, since SBE site would need to have all ballot styles for the entire state