Discussion Topic: End-to-End (E2E) Verifiable Systems

This document highlights the cybersecurity working group discussion around the cryptographic end-to-end (E2E) verifiable voting systems. This document will sometimes referred to these systems as “E2E systems” for short. E2E systems are noted as an open area due to concerns around the current state of the VVSG requirements and whether they sufficiently cover E2E voting systems. This document will identify the concerns and discuss current VVSG 2.0 related principles, guidelines, and/or requirements.

Decision Points
- Are the current E2E requirements sufficient?
- Are the requirements adequate for the testing and certification process?

General Information about E2E verifiable systems
Here is a list of a few general points you should know about cryptographic E2E verifiable voting systems:
- It is a software independent voting system that allows for end-to-end verifiability of the election results.
- E2E verifiable systems can be paper-based and paperless systems
- Examples: Scantegrity II, Punchscan, Prêt à Voter

Election Properties of E2E systems:
- **Cast as Intended, Recorded as Cast** – A voter has the ability to verify their votes are accurately captured and recorded. After casting, a voter is provided information to verify their vote is recorded as cast by viewing a public posting of all votes.
- **Preserve Ballot Secrecy** – The information provided that allows the voter to perform the verification does not include any identifying information that allows a voter to prove how they voted.
- **Tallied as Recorded** – Anyone can check that the votes are properly tallied. The public posting of all votes allows the public to review the tally of the votes.
The following sections describe the general concerns with E2E voting systems and potential mitigations to address those concerns. The concerns and mitigations are illustrated through reference to the VVSG Principles and Guidelines. The concerns and mitigations do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

**General Concerns**

**Concern A. Sufficient Requirements**
E2E systems are not currently used in elections. There is no common standard for the design or cryptographic protocol of an E2E system. The current requirements are written to cover the properties of an E2E system, but without current solutions it is unclear if this is enough information to cover the system and security properties.

**Concern B. Assessment Criteria & Adequate testing**
It is also a concern that the current requirements are not enough for testing and certification process. The assessment criteria for E2E systems include ensuring the system meet the E2E properties and utilize a well-designed cryptographic protocol. Some questions that arise under this concern include...
  ➢ Will experts and academia vet E2E verifiable systems to ensure well-designed cryptographic protocols?
  ➢ Will VSTLs be able to perform compliance testing using the available requirements?

**Concern C. Dispute Resolution**
Another concern is how to handle when a voter states that their vote is not captured correctly, after they have already cast their vote. This challenges the integrity of the voting system and may be difficult to dispute without asserting how a voter voted.

**Concern D. Accessibility**
The current VVSG requirements cover everything up until a voter casts their ballot. E2E systems allow for additional verification after a voter casts their ballot. The requirements do not cover how to accommodate the accessibility needs of voters once they leave the polling place.

**Concern E. Forward Secrecy**
If there is a flaw in an E2E system that later reveals voter identities and votes, this could violate the principle of ballot secrecy. E2E systems allow for the public posting of elections results for the...
Potential Mitigations:

**Mitigation A. Adequately cover the general principles of E2E verifiable systems**
As mentioned above, E2E systems have a unique set of properties. The first step to ensuring sufficient requirements is to utilize the list of unique properties and ensure that they are covered within the requirements. Voting system manufacturers may provide documentation that details how the voting system produces artifacts that can be used to meet the E2E properties.

**Mitigation B. Utilize an open standard and provide reference implementation information**
The E2E implementation should be an open standard available for public review. This allows for transparency of the voting system and its capabilities. Additionally, providing a reference implementation could be helpful for verifying the E2E prototype. Again, this would assist with transparency and allow for external review of the E2E protocol used within the voting system. With the opportunity for review, this may allow for the general public and election community to gain confidence of the cryptographic protocol.

**Mitigation C. Report of External Evaluation**
Mitigation A and B, both reference artifacts and information that allow for review of the E2E system, but do not guarantee an external evaluation is performed. This mitigation suggests that an external evaluation be performed by a set of cryptography experts with knowledge, experience, and/or understanding of E2E systems. After this set of experts review and analyze a E2E cryptographic protocol, they can submit a report of review to the Voting System Manufacturer. The VVSG requirements would require that this report be submitted.

Potential Benefits

*Note:* The following do not imply that an E2E verifiable system is the only solution to these achieve these benefits.

**Benefit A. Accessibility**

**Benefit B. Additional Verification Properties**

Related Requirements

The E2E requirements are primarily fall under Principles 9, 10, and 13