# Software Independence Requirements DRAFT

Since 10/6, requirements 1.1 – 1.6 were removed. Requirements 2.1 and 2.2 were modified per the working group's request. Finally, the term "Fully Electronic System Architectures" was renamed to "Cryptographic E2E System Architectures". This creates the following question: Does the working group need to try to create requirements for fully-electronic systems that do not use cryptographic E2E protocols?

*Question on Structure*

How should paper and E2E requirements be organized? Should there be a section that covers paper and another section that covers E2E (the current state), or should requirements be placed under the higher-level requirements?

For example:

2.1 Tamper-evident records shall provide an individual voter the opportunity to verify that the voting system correctly interpreted their ballot selections.

2.1.1 Paper – *Paper requirement text*

2.1.2 E2E – *E2E requirement text*

Another way to structure the system specific requirements would be to have a dedicated section and then group them into the following three categories: cast as intended, recorded as cast, and counted as recorded. Paper-based systems and E2E systems provide different levels of verification for each of these properties. Additionally, different voting channels within paper-based systems architectures also offer different levels of verification, such as postal voting and polling-place voting. The definitions used for these properties below are ruthlessly pilfered from Ben Adida's 2006 paper on : https://www.usenix.org/legacy/event/evt06/tech/full_papers/adida/adida.pdf

## Requirements

1. An undetected error or fault in the voting system's software or hardware shall not be capable of causing an undetectable change in election results.
2. The voting system shall produce tamper-evident records to enable detection of incorrect election outcomes.
   2.1. Tamper-evident records shall provide an individual voter the opportunity to verify that the voting system correctly interpreted their ballot selections.
   2.2. Tamper-evident records shall be automatically created as a result of a voter inputting ballot selections into the voting system.

2.3. Detected errors shall be recorded in a tamper-evident manner.

3. Voting systems records shall enable external auditors to verify that cast ballots were correctly tabulated.

   3.1. The voting system shall enable a meaningful audit in the presence of compromised or malicious software resident on the system.

   3.2. The voting system shall enable a meaningful audit in the presence of compromised hardware components.

4. Voting systems shall document and provide a method, either through procedural or technical means, for voters to report detected errors or incorrect results.

5. Voting systems shall meet the requirements within either the Paper-based System Architectures *or* Cryptographic E2E System Architectures section.

**Paper-based System Architectures**

*Cast as Intended: the ballot is cast at the polling station as the voter intended [Adida 2006].*

5.1 The voting system shall produce a paper record of the voter's ballot selection.

5.2 Ballot selections shall be presented in a human-readable manner.

5.3 The voter shall have the opportunity to identify errors on their ballot before it is cast.

5.4 The voting system shall allow a voter to restart their voting session if their ballot is deemed incorrect.

*Recorded as Cast: cast ballots are preserved with integrity through the ballot collection process [Adida 2006].*

5.5 Ballots integrity shall be maintained throughout the voting process.

*Counted as Recorded: recorded ballots are counted correctly [Adida 2006].*

5.6 Paper ballots shall contain a unique identifier before they are counted.

5.6.1 Paper ballot identifiers may be printed onto the ballot, or affixed via some other mechanism before casting.

5.7 Voting systems tally from the human readable ballot selections.

**Cryptographic E2E System Architectures**