Volume I, Appendix D
Table of Contents

Appendix D

Appendix D is an informative section with characteristics of independent dual verification systems followed by characteristics of the types of independent dual verification systems which will be used as the basis for future requirements. They are preliminary and will be evolving with further research.

D.1. Independent Dual Verification Systems

A primary objective for using electronic voting systems is the production of voting records that are highly precise, highly reliable, and easily counted - in essence, an accurate representation of ballot choices whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system's design, including:

- the environment provided for voting, including the voting site and various environmental factors,
- the ease with which voters can use the voting system, i.e., its usability,
- the robustness and reliability of the voting equipment, and
- the capability of the records to be used in audits.

Independent Dual Verification (IDV) systems have as their primary objective the production of ballot records that are capable of being used in audits in which their correctness can be audited to very high levels of precision. The primary security issues addressed by IDV systems are:

- whether electronic voting systems are accurately recording ballot choices, and
- whether the ballot record contents can be audited precisely post-election.

The threats addressed by IDV systems are those that could cause a voting system to inaccurately record the voter's intent or cause a voting system's records to become damaged, i.e., inserted, deleted, or changed. These threats could occur via any number of means including accidental damage or various forms of fraud. The threats are addressed mainly by providing, in the voting system design, the capability for ballot record audits to detect precisely whether specific records are correct as recorded or damaged, missing, or fraudulent.

1.1 Independent Dual Verification Systems: Improved Accuracy in Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot choices whose contents are capable of being audited to high levels of precision. For this to happen, the records must be produced and made verifiable by the voter, and then subsequently handled according to the following protocol:

- At least two records of the voter's choices are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g. the voting system creates a record of the voter's choices and then copies it to some write-once media.

- The voter must be able to verify that both records are correct, e.g., verify his or her choices on the voting system's display and also verify the second record of choices stored on the write-once media.

- The verification processes for the two verifications must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on different systems produced by different vendors.

- The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked.

An assumption is made that at least one set of records is usable in an efficient counting process such as by using an electronic voting system, and the other set of records is usable in an efficient process of verifying its agreement with the other set of records used in the counting process. The sets of records would preferentially be different in form and thus have more resistance to accidental or deliberate damage.

Given these conditions above, the multiple records are said to be distinct and independently verifiable, that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check up on the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of the records still will face a difficult task in compromising the other.

1.2 Example Independent Dual Verification Systems

The following sections present overviews of several types of IDV systems. Some of these systems have not been marketed as yet but are included here to help clarify approaches to independent verification systems. The systems discussed are:

- voting systems with a split process architecture,[1]
- end-to-end voting systems that include cryptographic audit schemes,
- witness voting systems that take a picture of or otherwise capture an indirect verification of ballot choices, and
- direct independent verification, including some types of voting systems that produce an optically scanned ballot or that produce a voter-verified paper audit trail (VVPAT).

1.2.1 The Split Process Architecture for IDV Systems

A voting machine with a split process architecture consists of vote capture and verification stations that are separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. The token object could be paper or some write-once read-only media. Two records of the vote are created: one on the token object and one by the verification station. Either could be used in the final count.

For any split process voting system, the interaction between the voter and the split process operates as follows:

1. A voter is given a token object that has been initialized to be blank.
2. Supporting information is written to the token object including the ballot and identification information about the election and precinct.
3. The voter inserts the token object into a capture station such as a DRE, which reads the ballot information from the token and then displays the ballot on an input device such as a touch screen. The voter to makes his or her ballot choices, which causes a record of the vote to be recorded on the token object.

[1] The split process architecture is otherwise known as the frog protocol, which was first described in the Caltech – MIT report: voting*: What Is, What Could Be*, as part of a modular voting architecture. The frog term, i.e., the token, was chosen specifically to convey no information about the physical form of the object used to carry vote information between two separate modules of the voting station. The report is available for download at http://www.vote.caltech.edu/.

4. The voter takes the token object to a separate verification station, which reads the recorded votes from the token object, makes an electronic copy, and displays it to the voter.

5. The voter verifies that the information is correct and then deposits the token object into a container where it can be archived and used later for recounts or audits against the electronic records.

Two sets of records are produced: the electronic records and the token's records. Typically, the electronic records recorded by the verification station would be counted in the election. At least one of the sets of records should be different in form from the other set of records and be resistance to accidental or deliberate damage so that it can remain useful for audits and recounts.

In theory, the physical separation of the ballot capture from the ballot verification may make analysis of the capture and verification devices easier or less costly. The rationale is that the user interface software on the capture station is expected to be complex and difficult to verify for correctness. On the other hand, the verification station's software is expected to be less complicated because it need only copy the contents of the token, display it to the voter, and store the ballot choices.

The verification station's software is considered to be the "trusted computing base" of the voting system, because it must be trusted in the verification process and then trusted to store the record for counting, i.e., cast the voter's ballot. The software to implement this capability should be relatively small and thus easier to inspect and test.

In general, segregating functions by placing them on physically different systems is a standard computer security practice for making those functions easier to test for correctness and easier to manage securely.

1.2.2 End to End (Cryptographic) IDV Systems

End to end voting systems use cryptographic techniques to store an encrypted copy of the voter's ballot choices. In this way, ballots can be audited and demonstrated to have been included in the election count.

End to end systems in existence today generally operate as follows:

1. A voter uses a voting station such as a DRE to make ballot choices.

2. The DRE issues a paper receipt to the voter that contains information that permits the voter to verify that the choices were recorded correctly. The information does not permit the voter to reveal his or her choices.

3. The voter may have the option to check that his or her ballot choices were included in the election count, e.g., by checking a web site of values that (should) match the information on the voter's paper receipt.

End to end systems are sometimes referred to as receipt-based systems. They may provide an assurance not only that the correct set of ballot choices was recorded, but that those choices were included in the election count. Some analyses of auditing and cryptographic systems assert that very small numbers of self-audits are required to verify the correctness of an election.

1.2.3 Witness IDV Systems

A witness voting system creates the second record of ballot choices by using a separate module to record or witness the voter's verification of the first record. The primary feature of a witness system is that the creation of the record does not require action by the voter. This may result in quicker voting times or voting systems that are simpler to use than other approaches that involve multiple, direct verifications by the voter.

An example of a witness system is a DRE with a camera mounted above its screen. The camera takes pictures and saves them independently of the DRE. It would operate as follows:

1. A voter makes ballot choices at the DRE and then presses a button to record his or her vote.

2. The DRE records the ballot choices and uses them in the election count.

3. At the time the button is pressed, the camera takes a picture of the DRE's screen and saves the image (the voter is not included in the picture).

4. This collection of images constitutes a second ballot record that can be used in audits and recounts.

As can be seen by this example, the voter's interactions are reduced to making ballot choices at the DRE and pressing a button to make the selections final. If the DRE were to be compromised such that it secretly recorded the ballot choices incorrectly, the stored photographic images would reflect what the voter had seen and verified at the DRE's screen.

Because the voter may not be able to verify that the creation of the second record was performed accurately, it is important that the creation process be highly reliable and very resistant to accidental or deliberate damage. Also, the suitability of the records for manual or automated auditing is a factor when considering this approach.

1.2.4 Direct IDV Systems

Direct independent dual verification systems produce a record for voter verification that the voter may verify directly with the voter's senses and which is then preserved for auditing or counting. Some optical scan voting system approaches fit into this category (albeit loosely), as well as those systems with VVPAT (Voter Verified Paper Audit Trail) capability.

Some optical scan voting system approaches fit into this category (albeit loosely), as well as those systems with VVPAT (Voter Verified Paper Audit Trail) capability.

The optical scan voting systems approaches in this category are those in which two records are created: a paper and an electronic record. This system uses Optical Scan Recognition (OCR) to create an electronic record from the paper record after the paper record has been directly verified by the voter. The general operation of this system is:

1. A voter uses a marking device such as a DRE to mark a ballot and then presses a button to print the marked ballot onto a piece of paper.

2. The voter directly reviews the paper to ensure its correctness, and if correct, places the paper record into a scanner (some procedure would need to be included to handle spoiled ballots).

3. The scanner converts the paper record into an electronic format. To reduce errors that may result from scanning the paper record, the paper records might contain a barcoded representation of the human readable portion of the ballot.

4. The paper record gets preserved in a ballot box.

No verification of the scanned paper record is performed in the above approach. One may assume that the scanning process is highly accurate and can be trusted to create the electronic record correctly; however it would be preferential for the voter to somehow verify that the record was, in fact, created correctly.

An electronic voting system with VVPAT (Voter Verified Paper Audit Trail) capability is similar to that of the optical scan above but consists typically of a DRE that both creates and records an electronic record, and a printer that creates a paper audit trail of the voter's choices. Like the optical scan system, it creates two distinct representations of the voter's ballot choices: an electronic record and a paper record.

Typically, a voter would use the voting system (called a DRE-VVPAT) as follows:

1. A voter makes ballot selections and indicates that his or her selections are complete.

2. The VVPAT-DRE prints a paper record summary of the voter's ballot choices. An alternative approach to VVPAT involves printing the voter's ballot selections as they are made, e.g., a concurrent or contemporaneous record.

3. The voter inspects and directly verifies that the paper record matches the displayed electronic record (again, a procedure would need to be included to handle spoiled ballots).

4. The paper record gets preserved in a ballot box.

Both approaches described here produce paper records that are verified directly by sight. Voters with sight impairments would require an accessible device for verification that can produce an audible representation of the paper record.

1.3 Issues in Handling Multiple Records Produced by Independent Dual Verification Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IDV systems records, including:

- how to tell if the records are authentic and not forged,

- how to tell if the integrity of the records has remained intact from the time they were recorded,

- the suitability of the records for various types of auditing, and

- how best to address problems if there are errors in the records.

Whenever an electronic voting system produces multiple records of votes, there is some possibility that one or more of the records may not match. Records can be lost, or deliberately or accidentally damaged, or stolen, or fabricated. Keeping the two records in correspondence with each other can be made more or less difficult depending on the technologies used for the records and the procedures used to handle the records.

As a consequence, it is important to structure the records so that errors and other anomalies can be readily detected during audits. There are a number of techniques that can be used, such as the following:

- associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record,

- including an identification of the specific voting system that produced the records, such as a serial number identifier or by having the voting system digitally sign the records using public key cryptography,

- including other information about the election and the precinct or location where the records were created,

- creating checksums of the electronic records and having the voting system digitally sign the entire sets of records so that missing or inserted records can be detected, and

- structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms

The ease or relative difficulty with which some types of records must be handled is also a determining factor in the practical capability to conduct precise audits, given that some types of records are better suited to different types of auditing and different voting environments than others. The factors that make certain types of records more suitable than others could vary greatly depending upon many other criteria, both objective and subjective. For example, paper records may require manual handling by voters or poll workers and thus be more susceptible to damage or loss. At the same time, the extent to which the paper records must be handled will vary depending on the type of voting system in use. Electronic records may by their nature be more suitable for automated audits; however electronic records are still subject to accidental or deliberate damage, loss, and theft.

D.2. Core characteristics for Independent Verification Systems

This section contains a preliminary set of characteristics for IDV systems. These characteristics are fundamental in nature and apply to all categories of IDV systems. They will form the basis for future requirements for independent verification systems.

2.1 An independent dual verification voting system produces two distinct sets of records of ballot choices via interactions with the voter such that one set of records can be compared against the other to check their equality of content.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: This is the fundamental core definition for IDV systems. The records can be checked against one another to determine whether or not the voter's choices were correctly recorded.

2.1.1 The voter verifies the content of each record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: Direct Verification involves using human senses, e.g., directly verifying a paper record via one’s eyesight. Indirect Verification involves using an intermediary to perform the verification, e.g., verifying an electronic ballot image at the voting system.

2.1.2 The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

2.1.2.1 At least one record is highly resistant to damage or alteration and should be capable of long-term storage.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: At least one of the records should be difficult to alter or damage so that it could be used in case the counted records are damaged or lost.

2.1.3 The processes of verification for the multiple records do not all depend for their integrity on the same device, software module, or system, and are sufficiently separate such that each record provides evidence of the voter's choices independently of its other corresponding record.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: For example, the verification of an electronic record on a DRE is not sufficiently separate from the verification of an electronic record located on a token but performed by the same DRE as the verification for the first record. Verification of a paper record by one’s senses is sufficiently separate in this case.

2.1.4 The records can be used in checks of one another, such that if one set of records can be used in an efficient counting process, the other set of records can be used for checking its agreement with the first set of records.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: For example, an electronic record can be used in an efficient counting process. A second paper record can be used to verify the accuracy of the electronic record; however its suitability for efficient counting is less clear. If a paper record can be used in an automated scan process, it may be more suitable.

2.1.5 The records within a set are linked to their corresponding records in the other set by including a unique identifier within each record that can be used to identify the record's corresponding record in the other set.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types.

2.1.6 Each record includes an identification of the voting site/precinct.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: If the voting site and precinct are different, both should be included.

2.1.7 The records include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

2.1.8 The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

2.1.9 The records include an identifier of the voting system that is unique to that style of voting systems.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The identifier could be a serial number or other unique ID.

2.1.10 The cryptographic software in independent verification voting systems is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software shall be used where feasible. The CMVP web site is http://csrc.nist.gov/cryptval.

D.3. Split Process IDV Systems

This section contains characteristics specific to split process IDV systems. The characteristics build on and are in addition to the core characteristics for IDV systems. Split process systems consist of separate vote capture and verification stations, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. Two records of the vote are created: one on the token object and one by the verification station.

3.1 Capture and Verification Stations

3.1.1 The verification station is able to add information to the token object but cannot change prior recorded information.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.1.2 The capture and verification stations do not permit any communications between them except via the token object.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.1.3 The verification station log all rejected votes, including the precise contents of the votes and the identifier of the token object.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The voter could reject and essentially spoil his or her ballot. This is to prevent the verification station from recording ballot choices that are different from what was entered at the capture station.

3.1.4 The capture and verification stations could be purchased from different manufacturers and could use different operating systems.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The greater the diversity between the systems, the less likely they could be compromised by the same threats, e.g., software viruses, or by a single conspiracy.

3.2 Data Formats for Token Objects

3.2.1 The format for data written to the token object is specified and publicly available for use without licensing fees.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.2.2 The verification station verifies the correctness of the data on the token object and provides an indication of any errors to the voter.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The verification station needs to verify, in essence, that the data written to the token object was formatted properly according to the rules of the format's specification and reject ill-formatted data. It also checks that the votes are consistent with the voting instructions, e.g., "vote for one, vote for two."

3.2.3 The record on the token object is digitally signed using a private key known only to the vote capture station and whose public key is distributed in an authenticated way to auditing systems.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.2.4 The record created by the verification station is digitally signed using a private key known only to the verification station and whose public key is distributed in an authenticated way to auditing systems.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.2.5 The capture station associates with each record of voter choices a unique identifier that is capable of being used to identify the record uniquely and to identify its corresponding record created by the verification station.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The identifier serves the purpose of uniquely identifying the record to identify duplicates and/or for cross-checking two record types.

3.2.6 The records from the verification station are randomly shuffled in memory and when exported, so that the order of the records cannot be used to identify any voter.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.2.7 Rejected token objects are stored separately from accepted memory devices for later auditing.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.3 Storage and Communications of Records

3.3.1 The verification station exports its records of voter choices accompanied by a digital signature on the entire set of electronic records and their associated digital signatures.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: This is necessary to determine if records are missing or substituted.

3.3.2 The token objects are carried in a physically secure way, using chain-of-custody mechanisms to ensure their integrity.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

3.3.3 The records from each station are randomly shuffled, so that an attacker learning the contents of those records at any point in the voting process can learn nothing about the order of votes cast.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

D.4. Witness IDV Systems

This section contains preliminary characteristics for Witness IDV systems. They are consistent with the definition of IDV systems from Section 6.0 and build on the core characteristics for IDV systems.

Witness IDV systems are composed of two physically separate devices: the vote capture station that captures and stores records of voters' choices, and the witness device that captures voter verifications of the records at the vote capture station. Because there are two devices, a number of the definitions for split verification systems apply equally well to witness systems. Because the vote capture station is in essence a DRE (with or without VVPAT capability), a number of the definitions for VVPAT that are specific to DRE systems also apply to vote capture stations. A witness system fits somewhat loosely in the independent verification category because the voter performs only an indirect verification of ballot choices at the DRE. It is important that the witness device be tested extensively for accuracy and reliability and that malfunctions in the device be made immediately obvious to voters and poll workers.

4.1 A witness device records only a voter's verification at a voting station and stores the record so that it can be used for audit and recounts as applicable.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.2 A witness device acts as a passive device that cannot perform any operation with respect to the voting station other than to capture the voter's ballot choices as the voter verifies them.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The witness device is synchronized with the voter verification of the ballot choices.

4.3 A witness device, if attached to the voting station, is attached such that it can capture only the voter's verification of ballot choices.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: For example, the witness device could be connected only to the display unit and not the vote capture station's memory or disk drive.

4.4 The voting station is not able to detect in its function whether a witness device is electrically connected or in operation.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: If the witness device is connected to or attached electrically to the vote capture station, the capture station is not able to determine or be aware in its function that a witness device is attached.

4.5 The witness device operates properly with most if not all electronic voting systems functioning as voting stations.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: This is desirable but may require some degree of openness in witness device specifications to enable the desired compatibility.

4.6 The witness device is not designed or built or manufactured by the same manufacturer of the voting station to which it is attached.

T	Testing Authority

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.7 Because voters must trust that the witness device records their verifications accurately, assessments of its software and functionality are straightforward, readily performed, and include extensive evaluation and penetration testing above and beyond what may be performed on voting systems that do not contain witness devices.

T	Testing Authority

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: Witness device manufacturers will need to document their systems extensively and subject them to highly stringent testing.

4.8 Because voters must trust that the witness device records their verifications accurately, the results of witness system assessments are made publicly available.

T Testing Authority

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.9 A voter should be able to inspect the record of the voter's verification upon the voter's request.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: It is desirable that a voter have some capability to verify that the witness device is operating as specified.

4.10 The witness device clearly indicates any malfunction in a way that is obvious to poll workers and voters.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: This serves to ensure that voting cannot continue if the witness device is not operating or is malfunctioning.

4.11 The records captured by the witness device are able to be used in highly accurate verifications of the voting records of the voting station.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.12 The records contain unique identifiers that correspond to records stored by the voting station.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.13 The records are digitally signed by the witness device so that the integrity and authenticity of its records can be verified.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.14 A witness device is able to export its records in an open, nonproprietary format such that the records can be used in automated audits.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

4.15 The records are stored in the witness device and exported such that voter privacy is protected, e.g., by making the order of the records randomly determined.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

D.5. End to End (Cryptographic) IDV Systems

This section contains very preliminary definitions for End to End (or cryptographic-based) IDV systems. They are consistent with the characteristics of IDV systems and build on the core characteristics of IDV systems.

End to end voting systems use cryptographic mechanisms as a substitute for some of the physical, computer-security, or procedural mechanisms used to secure other voting systems. Some auditing procedures normally performed by voting officials at the tabulation center can be done by voters or their designated representatives, using receipts issued by the voting system that work in conjunction with the cryptographic mechanisms. Typically, multiple individuals, known as designated trustees, hold key information that is combined to form encryption and decryption keys; thus, no one person is able to encrypt or decrypt. Several types of cryptographic voting approaches have been proposed or implemented, with varying properties. There are many cryptographic techniques (such as secure multiparty computation and homomorphic) that could be applied in novel ways in future voting systems.

End to end systems use cryptographic mechanisms as a substitute for some of the physical, computer security, and procedural mechanisms used to secure voting systems. These cryptographic mechanisms can be used by a voter to verify that ballot choices were recorded correctly and counted in the election.

5.1 End to end systems use cryptographic mechanisms as a substitute for some of the physical, computer security, and procedural mechanisms used to secure voting systems. These cryptographic mechanisms can be used by a voter to verify that ballot choices were recorded correctly and counted in the election.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: There are potentially many types of end to end systems that could perform a variety of different functions.

5.2 End to end systems record voters ballot choices at an electronic voting system and encrypt the records of votes for later counting by designated trustees.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The voting station would operate much as a DRE.

5.3 End to end systems produce a receipt that can be used by the voter in some process made available by voting officials that would enable the voter to verify that the voter's ballot choices were recorded correctly and counted in the election.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The receipt could have a variety of different forms but likely would be printed on paper for the voter's ease of handling.

5.4 No one designated trustee is able to decrypt the records; decryption of the records is performed by a process that involves multiple designated trustees.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: For example, multiple keys could be combined to decrypt the records.

5.5 The receipt preserves voter privacy by not containing any information that can be used to show the voter's choices.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

5.6 The process used to verify that ballot choices were recorded correctly or counted in the election preserves voter privacy by not revealing any information that can be used to show the voter's choices.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

5.7 End to end systems store backup records of voter's ballot choices that can be used in contingencies such as damage to or loss of its counted records.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: This is necessary because the handling of the encrypted records requires the same chain of custody procedures as records produced by other voting systems and are thus subject to loss or damage. This could be paper for example.

5.8 The backup records contain unique identifiers that correspond to unique identifiers in its counted records, and the backup records are digitally signed so that they can be verified for their authenticity and integrity in audits.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

5.9 Cryptographic software in end to end systems is documented thoroughly and subject to extensive verification testing for correctness. The documentation includes extensive discussion of how cryptographic keys are to be generated, distributed, managed, used, certified, and destroyed.

T Testing Authority

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: The correctness of the system depends on the correctness of the cryptographic algorithms and their implementations. Thus, rigorous testing is necessary.

5.10 Vote capture stations used in end to end systems meet all security, usability, and accessibility requirements for similar stations in other voting systems.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

5.11 Reliability, usability, and accessibility requirements for printers in other voting systems apply as well to receipt printers used in end to end systems.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

5.12 Trustee systems are subject to the same evaluations and assessments as other voting systems.

V Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: Trustee systems include systems to perform cryptographic functions such as encrypting or decrypting votes.

5.13 Systems for verifying that voters' ballots were recorded properly and counted in the election are implemented in a robust secure manner.

V	Voting System Vendor

~~Pre-Voting~~	Voting	~~Post-Voting~~

Discussion: Many of the cryptographic approaches have a "public append-only bulletin board" as a component; this is an important part of the system and needs to be implemented in a robust secure manner.