

Volume I, Appendix D

Table of Contents

D	Appendix - Independent Dual Verification (Informative)	1
D.1	Independent Dual Verification Systems.....	1
D.2	Core Characteristics for IDV Systems	9
D.3	Split Process IDV Systems	13
D.4	Witness IDV Systems	16
D.5	End to End (Cryptographic) IDV Systems	20

Appendix D Independent Dual Verification (Informative)

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

Appendix D Independent Dual Verification (Informative)

1 of being audited to high levels of precision. For this to happen, the records must be
2 produced and made verifiable by the voter, and then subsequently handled
3 according to the following protocol:
4

- 5 • At least two records of the voter's choices are produced and one of the
6 records is then stored such that it cannot be modified by the voting system,
7 e.g. the voting system creates a record of the voter's choices and then copies
8 it to some write-once media.
9
- 10 • The voter must be able to verify that both records are correct, e.g., verify his
11 or her choices on the voting system's display and also verify the second
12 record of choices stored on the write-once media.
13
- 14 • The verification processes for the two verifications must be independent of
15 each other and (a) at least one of the records must be verified directly by the
16 voter, or (b) it is acceptable for the voter to indirectly verify both records if
17 they are stored on different systems produced by different vendors.
18
- 19 • The content of the two records can be checked later for consistency through
20 the use of identifiers that allow the records to be linked.
21

22 An assumption is made that at least one set of records is usable in an efficient
23 counting process such as by using an electronic voting system, and the other set of
24 records is usable in an efficient process of verifying its agreement with the other set
25 of records used in the counting process. The sets of records would preferentially be
26 different in form and thus have more resistance to accidental or deliberate damage.
27

28 Given these conditions above, the multiple records are said to be distinct and
29 independently verifiable, that is, both records are not under the control of the same
30 processes. As a result of this independence, one record can be used to audit or
31 check up on the accuracy of the other record. Because the storage of the records is
32 separate, an attacker who can compromise one of the records still will face a
33 difficult task in compromising the other.
34

35 1.2 Example Independent Dual Verification Systems

36 The following sections present overviews of several types of IDV systems. Some
37 of these systems have not been marketed as yet but are included here to help clarify
38 approaches to independent verification systems. The systems discussed are:
39
40

Appendix D Independent Dual Verification (Informative)

- 1 • voting systems with a split process architecture,¹
- 2
- 3 • end-to-end voting systems that include cryptographic audit schemes,
- 4
- 5 • witness voting systems that take a picture of or otherwise capture an indirect
- 6 verification of ballot choices, and
- 7
- 8 • direct independent verification, including some types of voting systems that
- 9 produce an optically scanned ballot or that produce a voter-verified paper
- 10 audit trail (VVPAT).
- 11
- 12

13 1.2.1 The Split Process Architecture for IDV Systems

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

22
23 For any split process voting system, the interaction between the voter and
24 the split process operates as follows:

- 25
- 26 1. A voter is given a token object that has been initialized to be blank.
- 27
- 28 2. Supporting information is written to the token object including the
- 29 ballot and identification information about the election and
- 30 precinct.
- 31
- 32 3. The voter inserts the token object into a capture station such as a
- 33 DRE, which reads the ballot information from the token and then
- 34 displays the ballot on an input device such as a touch screen. The
- 35 voter to makes his or her ballot choices, which causes a record of
- 36 the vote to be recorded on the token object.
- 37

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/>.

Appendix D Independent Dual Verification (Informative)

- 1 4. The voter takes the token object to a separate verification station,
2 which reads the recorded votes from the token object, makes an
3 electronic copy, and displays it to the voter.
4
- 5 5. The voter verifies that the information is correct and then deposits
6 the token object into a container where it can be archived and used
7 later for recounts or audits against the electronic records.
8

9 Two sets of records are produced: the electronic records and the token's
10 records. Typically, the electronic records recorded by the verification
11 station would be counted in the election. At least one of the sets of
12 records should be different in form from the other set of records and be
13 resistance to accidental or deliberate damage so that it can remain useful
14 for audits and recounts.
15

16 In theory, the physical separation of the ballot capture from the ballot
17 verification may make analysis of the capture and verification devices
18 easier or less costly. The rationale is that the user interface software on
19 the capture station is expected to be complex and difficult to verify for
20 correctness. On the other hand, the verification station's software is
21 expected to be less complicated because it need only copy the contents of
22 the token, display it to the voter, and store the ballot choices.
23

24 The verification station's software is considered to be the "trusted
25 computing base" of the voting system, because it must be trusted in the
26 verification process and then trusted to store the record for counting, i.e.,
27 cast the voter's ballot. The software to implement this capability should be
28 relatively small and thus easier to inspect and test.
29

30 In general, segregating functions by placing them on physically different
31 systems is a standard computer security practice for making those
32 functions easier to test for correctness and easier to manage securely.
33

34 **1.2.2 End to End (Cryptographic) IDV Systems**

35 End to end voting systems use cryptographic techniques to store an
36 encrypted copy of the voter's ballot choices. In this way, ballots can be
37 audited and demonstrated to have been included in the election count.
38

39 End to end systems in existence today generally operate as follows:
40

- 41 1. A voter uses a voting station such as a DRE to make ballot choices.
42
43

Appendix D Independent Dual Verification (Informative)

1 As can be seen by this example, the voter's interactions are reduced to
2 making ballot choices at the DRE and pressing a button to make the
3 selections final. If the DRE were to be compromised such that it secretly
4 recorded the ballot choices incorrectly, the stored photographic images
5 would reflect what the voter had seen and verified at the DRE's screen.
6

7 Because the voter may not be able to verify that the creation of the second
8 record was performed accurately, it is important that the creation process be
9 highly reliable and very resistant to accidental or deliberate damage. Also,
10 the suitability of the records for manual or automated auditing is a factor
11 when considering this approach.
12

13 **1.2.4 Direct IDV Systems**

15 Direct independent dual verification systems produce a record for voter
16 verification that the voter may verify directly with the voter's senses and
17 which is then preserved for auditing or counting. Some optical scan voting
18 system approaches fit into this category (albeit loosely), as well as those
19 systems with VVPAT (Voter Verified Paper Audit Trail) capability.
20

21 Some optical scan voting system approaches fit into this category (albeit
22 loosely), as well as those systems with VVPAT (Voter Verified Paper Audit
23 Trail) capability.
24

25 The optical scan voting systems approaches in this category are those in
26 which two records are created: a paper and an electronic record. This system
27 uses Optical Scan Recognition (OCR) to create an electronic record from the
28 paper record after the paper record has been directly verified by the voter.
29 The general operation of this system is:
30

- 31 1. A voter uses a marking device such as a DRE to mark a ballot and
32 then presses a button to print the marked ballot onto a piece of paper.
33
- 34 2. The voter directly reviews the paper to ensure its correctness, and if
35 correct, places the paper record into a scanner (some procedure
36 would need to be included to handle spoiled ballots).
37
- 38 3. The scanner converts the paper record into an electronic format. To
39 reduce errors that may result from scanning the paper record, the
40 paper records might contain a barcoded representation of the human
41 readable portion of the ballot.
42
- 43 4. The paper record gets preserved in a ballot box.

Appendix D Independent Dual Verification (Informative)

1
2 No verification of the scanned paper record is performed in the above
3 approach. One may assume that the scanning process is highly accurate and
4 can be trusted to create the electronic record correctly; however it would be
5 preferential for the voter to somehow verify that the record was, in fact,
6 created correctly.
7

8 An electronic voting system with VVPAT (Voter Verified Paper Audit Trail)
9 capability is similar to that of the optical scan above but consists typically of
10 a DRE that both creates and records an electronic record, and a printer that
11 creates a paper audit trail of the voter's choices. Like the optical scan
12 system, it creates two distinct representations of the voter's ballot choices:
13 an electronic record and a paper record.
14

15 Typically, a voter would use the voting system (called a DRE-VVPAT) as
16 follows:
17

- 18 1. A voter makes ballot selections and indicates that his or her
19 selections are complete.
- 20 2. The VVPAT-DRE prints a paper record summary of the voter's ballot
21 choices. An alternative approach to VVPAT involves printing the
22 voter's ballot selections as they are made, e.g., a concurrent or
23 contemporaneous record.
24
- 25 3. The voter inspects and directly verifies that the paper record matches
26 the displayed electronic record (again, a procedure would need to be
27 included to handle spoiled ballots).
28
- 29 4. The paper record gets preserved in a ballot box.
30
31

32 Both approaches described here produce paper records that are verified
33 directly by sight. Voters with sight impairments would require an accessible
34 device for verification that can produce an audible representation of the
35 paper record.
36

37 **1.3 Issues in Handling Multiple Records Produced by Independent Dual** 38 **Verification Systems**

39 There are several fundamental questions that need to be addressed when designing
40 the structure and selecting the physical characteristics of IDV systems records,
41 including:
42

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

Appendix D Independent Dual Verification (Informative)

- 1
- 2 • how to tell if the integrity of the records has remained intact from the time
- 3 they were recorded,
- 4
- 5 • the suitability of the records for various types of auditing, and
- 6
- 7 • how best to address problems if there are errors in the records.
- 8

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

15

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

- 19
- 20 • associating unique identifiers with corresponding records, e.g., an individual
- 21 paper record sharing a unique identifier with its corresponding electronic
- 22 record,
- 23
- 24 • including an identification of the specific voting system that produced the
- 25 records, such as a serial number identifier or by having the voting system
- 26 digitally sign the records using public key cryptography,
- 27
- 28 • including other information about the election and the precinct or location
- 29 where the records were created,
- 30
- 31 • creating checksums of the electronic records and having the voting system
- 32 digitally sign the entire sets of records so that missing or inserted records
- 33 can be detected, and
- 34
- 35 • structuring the records in open, publicly documented formats that can be
- 36 readily analyzed on different computing platforms
- 37

38 The ease or relative difficulty with which some types of records must be handled is
39 also a determining factor in the practical capability to conduct precise audits, given
40 that some types of records are better suited to different types of auditing and
41 different voting environments than others. The factors that make certain types of
42 records more suitable than others could vary greatly depending upon many other
43 criteria, both objective and subjective. For example, paper records may require
44 manual handling by voters or poll workers and thus be more susceptible to damage

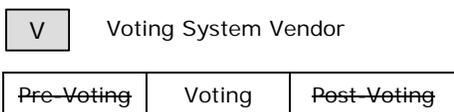
Appendix D Independent Dual Verification (Informative)

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

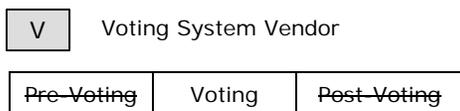
This section contains a preliminary set of characteristics for IDV systems. These characteristics are fundamental in nature and apply to all categories of IDV systems. They will form the basis for future requirements for independent verification systems.

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.



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.



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.

Appendix D Independent Dual Verification (Informative)

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.

Appendix D Independent Dual Verification (Informative)

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

Appendix D Independent Dual Verification (Informative)

1 **D.3. Split Process IDV Systems**

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

8
 9

10 **3.1 Capture and Verification Stations**11 **3.1.1 The verification station is able to add information to the token object**
 12 **but cannot change prior recorded information.**

13

V	Voting System Vendor
---	----------------------

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

14
 15

16 **3.1.2 The capture and verification stations do not permit any**
 17 **communications between them except via the token object.**

18

V	Voting System Vendor
---	----------------------

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

20

21 **3.1.3 The verification station log all rejected votes, including the precise**
 22 **contents of the votes and the identifier of the token object.**

23

V	Voting System Vendor
---	----------------------

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

24

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

29

Appendix D Independent Dual Verification (Informative)

1 **3.1.4 The capture and verification stations could be purchased from**
2 **different manufacturers and could use different operating systems.**

3

V	Voting System Vendor
---	----------------------

4

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

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

8
9 **3.2 Data Formats for Token Objects**

10 **3.2.1 The format for data written to the token object is specified and**
11 **publicly available for use without licensing fees.**

12

V	Voting System Vendor
---	----------------------

13

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

14 **3.2.2 The verification station verifies the correctness of the data on the**
15 **token object and provides an indication of any errors to the voter.**

16

V	Voting System Vendor
---	----------------------

17

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

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

23 **3.2.3 The record on the token object is digitally signed using a private key**
24 **known only to the vote capture station and whose public key is**
25 **distributed in an authenticated way to auditing systems.**

26

V	Voting System Vendor
---	----------------------

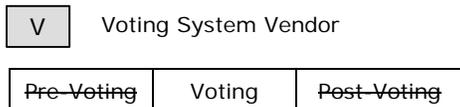
27

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

Appendix D Independent Dual Verification (Informative)

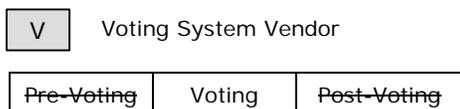
3.3 Storage and Communications of Records

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.

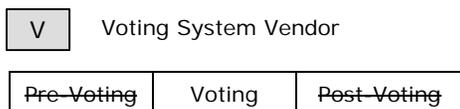


Discussion: This is necessary to determine if records are missing or substituted.

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



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.



D.4. Witness IDV Systems

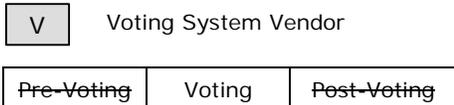
This section contains preliminary characteristics for Witness IDV systems. They are consistent with the definition of IDV systems from Section 6.0 and build on the core characteristics for IDV systems.

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

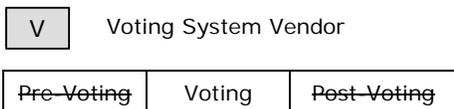
Appendix D Independent Dual Verification (Informative)

1 voter performs only an indirect verification of ballot choices at the DRE. It is important that the
 2 witness device be tested extensively for accuracy and reliability and that malfunctions in the
 3 device be made immediately obvious to voters and poll workers.

4
 5
 6 **4.1 A witness device records only a voter's verification at a voting station and**
 7 **stores the record so that it can be used for audit and recounts as applicable.**

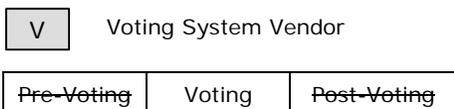


9
 10
 11 **4.2 A witness device acts as a passive device that cannot perform any operation**
 12 **with respect to the voting station other than to capture the voter's ballot**
 13 **choices as the voter verifies them.**



15
 16
 17 Discussion: The witness device is synchronized with the voter verification of the
 18 ballot choices.

19
 20 **4.3 A witness device, if attached to the voting station, is attached such that it can**
 21 **capture only the voter's verification of ballot choices.**



23
 24
 25 Discussion: For example, the witness device could be connected only to the display
 26 unit and not the vote capture station's memory or disk drive.

27

Appendix D Independent Dual Verification (Informative)

1 **4.4 The voting station is not able to detect in its function whether a witness device**
2 **is electrically connected or in operation.**

3

V

 Voting System Vendor

4

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

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

8
9 **4.5 The witness device operates properly with most if not all electronic voting**
10 **systems functioning as voting stations.**

11

V

 Voting System Vendor

12

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

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

15
16 **4.6 The witness device is not designed or built or manufactured by the same**
17 **manufacturer of the voting station to which it is attached.**

18

T

 Testing Authority

19

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

20 **4.7 Because voters must trust that the witness device records their verifications**
21 **accurately, assessments of its software and functionality are straightforward,**
22 **readily performed, and include extensive evaluation and penetration testing**
23 **above and beyond what may be performed on voting systems that do not**
24 **contain witness devices.**

25

T

 Testing Authority

26

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

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

Appendix D Independent Dual Verification (Informative)

1 **4.8 Because voters must trust that the witness device records their verifications**
2 **accurately, the results of witness system assessments are made publicly**
3 **available.**

T	Testing Authority	
Pre-Voting	Voting	Post-Voting

5
6
7 **4.9 A voter should be able to inspect the record of the voter's verification upon the**
8 **voter's request.**

V	Voting System Vendor	
Pre-Voting	Voting	Post-Voting

9
10
11 Discussion: It is desirable that a voter have some capability to verify that the
12 witness device is operating as specified.

13 **4.10 The witness device clearly indicates any malfunction in a way that is obvious to**
14 **poll workers and voters.**

V	Voting System Vendor	
Pre-Voting	Voting	Post-Voting

15
16
17 Discussion: This serves to ensure that voting cannot continue if the witness device
18 is not operating or is malfunctioning.

19
20 **4.11 The records captured by the witness device are able to be used in highly**
21 **accurate verifications of the voting records of the voting station.**

V	Voting System Vendor	
Pre-Voting	Voting	Post-Voting

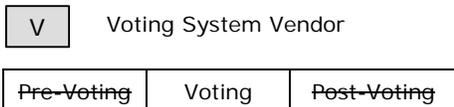
22
23
24
25 **4.12 The records contain unique identifiers that correspond to records stored by**
26 **the voting station.**

V	Voting System Vendor	
Pre-Voting	Voting	Post-Voting

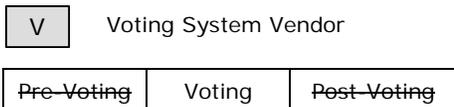
27
28
29

Appendix D Independent Dual Verification (Informative)

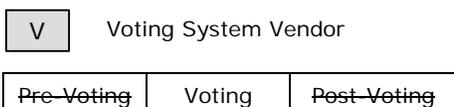
1 **4.13 The records are digitally signed by the witness device so that the integrity and**
 2 **authenticity of its records can be verified.**



4
 5
 6 **4.14 A witness device is able to export its records in an open, nonproprietary**
 7 **format such that the records can be used in automated audits.**



9
 10 **4.15 The records are stored in the witness device and exported such that voter**
 11 **privacy is protected, e.g., by making the order of the records randomly**
 12 **determined.**



14
 15
 16 **D.5. End to End (Cryptographic) IDV Systems**

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

20
 21 End to end voting systems use cryptographic mechanisms as a substitute for some of the
 22 physical, computer-security, or procedural mechanisms used to secure other voting systems.
 23 Some auditing procedures normally performed by voting officials at the tabulation center can be
 24 done by voters or their designated representatives, using receipts issued by the voting system that
 25 work in conjunction with the cryptographic mechanisms. Typically, multiple individuals, known
 26 as designated trustees, hold key information that is combined to form encryption and decryption
 27 keys; thus, no one person is able to encrypt or decrypt. Several types of cryptographic voting
 28 approaches have been proposed or implemented, with varying properties. There are many
 29 cryptographic techniques (such as secure multiparty computation and homomorphic) that could
 30 be applied in novel ways in future voting systems.

31
 32 End to end systems use cryptographic mechanisms as a substitute for some of the physical,
 33 computer security, and procedural mechanisms used to secure voting systems. These

Appendix D Independent Dual Verification (Informative)

1 cryptographic mechanisms can be used by a voter to verify that ballot choices were recorded
 2 correctly and counted in the election.
 3

4 **5.1 End to end systems use cryptographic mechanisms as a substitute for some of**
 5 **the physical, computer security, and procedural mechanisms used to secure**
 6 **voting systems. These cryptographic mechanisms can be used by a voter to**
 7 **verify that ballot choices were recorded correctly and counted in the election.**

8

V	Voting System Vendor
---	----------------------

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

9
 10 Discussion: There are potentially many types of end to end systems that could
 11 perform a variety of different functions.

12 **5.2 End to end systems record voters ballot choices at an electronic voting system**
 13 **and encrypt the records of votes for later counting by designated trustees.**
 14

15

V	Voting System Vendor
---	----------------------

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

16
 17 Discussion: The voting station would operate much as a DRE.

18 **5.3 End to end systems produce a receipt that can be used by the voter in some**
 19 **process made available by voting officials that would enable the voter to verify**
 20 **that the voter's ballot choices were recorded correctly and counted in the**
 21 **election.**
 22

23

V	Voting System Vendor
---	----------------------

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

24
 25 Discussion: The receipt could have a variety of different forms but likely would be
 26 printed on paper for the voter’s ease of handling.

27

Appendix D Independent Dual Verification (Informative)

1 **5.4 No one designated trustee is able to decrypt the records; decryption of the**
2 **records is performed by a process that involves multiple designated trustees.**

3

V

 Voting System Vendor

4

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

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

6
7 **5.5 The receipt preserves voter privacy by not containing any information that can**
8 **be used to show the voter’s choices.**

9

V

 Voting System Vendor

10

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

11
12 **5.6 The process used to verify that ballot choices were recorded correctly or**
13 **counted in the election preserves voter privacy by not revealing any**
14 **information that can be used to show the voter's choices.**

15

V

 Voting System Vendor

16

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

17
18 **5.7 End to end systems store backup records of voter's ballot choices that can be**
19 **used in contingencies such as damage to or loss of its counted records.**

20

V

 Voting System Vendor

21

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

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

26 **5.8 The backup records contain unique identifiers that correspond to unique**
27 **identifiers in its counted records, and the backup records are digitally signed**
28 **so that they can be verified for their authenticity and integrity in audits.**

29

V

 Voting System Vendor

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

Appendix D Independent Dual Verification (Informative)

1 **5.13 Systems for verifying that voters' ballots were recorded properly and counted**
2 **in the election are implemented in a robust secure manner.**

3

V	Voting System Vendor
---	----------------------

4

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

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