**DRAFT Test Assertions for VVSG 1.0 Section 7.9.3**

**August 24, 2015**

**Requirement 7.9.3**

**VVSG 1.0 Requirement 7.9.3:**

1. All cryptographic software in the voting system shall be approved by the U.S. Government’s Cryptographic Module Validation Program, as applicable.

**Discussion:**

Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). 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 should be used where feasible but is not required. The CMVP website is <http://csrc.nist.gov/cryptval>.

1. The electronic ballot image and paper records shall include information about the election.
	1. The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine.

**Discussion:**

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

* 1. The records shall include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.
	2. The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session.

**Discussion:**

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

1. The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record’s corresponding record.

**Discussion:**

The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

1. The voting machine should generate and store a digital signature for each electronic record.
2. The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.
3. The exported electronic ballot image records shall be in a publicly available, non-proprietary format.

**Discussion:**

It is advantageous when all electronic records, regardless of manufacturer, use the same format or can easily be converted to a publicly available, non-proprietary format; for example, the OASIS Election Markup Language (EML) Standard.

1. The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures.

**Discussion:**

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

1. The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.
2. The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.
3. The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.
4. The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.

**Discussion:**

There may be a future requirement for some commonality in the format of paper records.

1. The paper record shall be created such that its contents are machine readable.

**Discussion:**

This can be done by using specific OCR fonts or barcodes.

1. The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record.

**Discussion:**

This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

1. If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record.

**Discussion:**

This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.

1. The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology.

**Discussion:**

Examples of such codes are Maxi Code or PDF417.

1. If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.
2. The barcode shall not contain any information other than the paper record’s human-readable content, error correcting codes, and digital signature information.

**Test Assertions**

**TA793a-1:** IF voting system uses a VVPAT, THEN all cryptographic software in the voting system employing NIST-approved algorithms SHALL be validated by the U.S. Government’s Cryptographic Module Validation Program.

**TA793b-1:** The electronic ballot image SHALL include information about the election.

**TA793bi-1:** The voting equipment SHALL be capable of including an identification of the particular election.

**TA793bi-2:** The voting equipment SHALL be capable of including an identification of the voting site.

**TA793bi-3:** The voting equipment SHALL be capable of including an identification of the voting precinct.

**TA793bi-4:** The voting equipment SHALL be capable of including an identification of the voting machine.

**TA793bii-1:** The records SHALL include information that identifies whether the balloting is EITHER 1) provisional OR 2) early, OR 3) on Election Day.

**TA793bii-2:** The records SHALL include information that identifies the ballot style in use.

**TA793biii-1:**  The records SHALL include a voting session identifier that is generated when the voting equipment is placed in voting mode.

**TA793biii-2:** The records SHALL include a voting session identifier that can be used to identify the records as being created during that voting session.

**TA793biii-3:** IF there are several voting sessions on the same voting machine on the same day, THEN the voting session identifiers SHALL be different (from Discussion).

**TA793biii-3-1:** The voting session identifiers SHOULD be generated from a random number generator (from Discussion).

**TA793c-1:** The electronic ballot image and paper records SHALL be linked by including a unique identifier within each record.

**TA793c-1-1:** The unique identifier SHALL be capable of being used to identify each record uniquely.

**TA793c-1-2:** The unique identifier SHALL be capable of being used to identify each record’s corresponding record.

**TA793d-1:** The voting machine SHOULD generate a digital signature for each electronic record.

**TA793d-2:** The voting machine SHOULD store a digital signature for each electronic record.

**TA793e-1:** All electronic ballot image records SHALL be capable of being exported for auditing on standards-based computing platforms.

**TA793e-2:** All electronic ballot image records SHALL be capable of being exported for analysis on standards-based computing platforms.

**TA793e-3:** All electronic ballot image records SHALL be capable of being exported for auditing on COTS information technology computing platforms.

**TA793e-4:** All electronic ballot image records SHALL be capable of being exported for analysis on COTS information technology computing platforms.

**TA793ei-1:** The exported electronic ballot image records SHALL be stored in a publicly available format.

**TA793ei-2:** The exported electronic ballot image records SHALL be stored in a non-proprietary format.

**TA793eii-1:** The records SHOULD be exported with a digital signature.

**TA793eii-1-1:** The digital signature SHALL be calculated on the entire set of electronic records and their associated digital signatures.

**TA793eiii-1:** The voting system manufacturer SHALL provide documentation, in the TDP, describing the structure of the exported ballot image records.

**TA793eiii-2:** The voting system manufacturer SHALL provide documentation, in the TDP, describing how the exported ballot images are to be read by software.

**TA793eiii-3:** The voting system manufacturer SHALL provide documentation, in the TDP, describing how the exported ballot images are to be processed by software.

**TA793eiv-1:** The voting system manufacturer SHALL provide a software program that will display the exported ballot image records.

**TA793eiv-1-1:** The software program MAY include other capabilities including, but not limited to, vote tallies and indications of undervotes.

**TA793ev-1:** The voting system manufacturer SHALL provide complete documentation of procedures for exporting electronic ballot image records.

**TA793ev-1-1:** The voting system manufacturer SHALL provide complete documentation of procedures for reconciling those records with the paper audit records.

**TA793f-1:** The paper record SHOULD be created in a format that is capable of being made available across different manufacturers of electronic voting systems.

**TA793g-1:** The paper record’s contents SHALL be machine readable.

**TA793g-1-1:** This MAY be accomplished by using specific OCR fonts.

**TA793g-1-2:** This MAY be accomplished by using barcodes.

**TA793gi-1:** The paper record SHALL contain error correcting codes.

**TA793gi-1-1:** The error correcting codes SHALL be sufficient to detect read errors.

**TA793gi-1-2:** The error correcting codes SHALL be sufficient to prevent other markings on the paper record from being misinterpreted when machine reading the paper record.

**TA793h-1:** IF a barcode is used, THEN the voting equipment SHALL be capable of printing a barcode with each paper record that contains the human-readable contents of the paper record.

**TA793hi-1:** The barcode SHALL use an industry standard format.

**TA793hi-2:** The barcode SHALL be capable of being read using readily available commercial technology.

**TA793hii-1:** IF the corresponding electronic record contains a digital signature, THEN the digital signature SHALL be included in the barcode on the paper record.

**TA793hiii-1:** The barcode SHALL ONLY contain, at most, the following information: 1) the paper record’s human-readable content, 2) error correcting codes, and 3) digital signature information.