**DRAFT Test Assertions for VVSG 1.0 Section 7.4.5.1**

**August 24, 2015**

**Requirement 7.4.5.1**

**VVSG 1.0 Requirement 7.4.5.1:**

1. The NSRL or other designated repository that generates hash value and/or digital signature reference information shall use FIPS-approved algorithms for hashing and signing.
2. The NSRL or other designated repository that generates hash values, digital signatures reference information or cryptographic keys shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

**Discussion:** See http://www.csrc.nist.gov/cryptval/ for information on FIPS 140-2.

1. The NSRL or other designated repository that generates sets of hash values and digital signatures for reference information shall include a hash value or digital signature covering the set of reference information.
2. If the NSRL or other designated repository uses public key technology, the following requirements shall be met:
3. Public and private key pairs used by the repository to generate digital signatures shall be 2048-bits or greater in length
4. The repository’s private keys used to generate digital signature reference information shall be used for no more than three years
5. Public keys used to verify digital signature reference information shall be placed on unalterable storage media if not contained in a signed non-proprietary format for distribution.

**Discussion:** Examples of non-proprietary standard formats include X.509 or PKCS#7.

1. All copies of public key unalterable storage media made by the repository shall be labeled so that they are uniquely identifiable, including at a minimum: a unique identifier (such as a serial number) for the unalterable storage media; the time, date, location and name(s) of the repository owning the associated private keys; documentation about its creation; and an indication that the contents are public keys.
2. The NSRL or other designated repository shall document to whom they provide unalterable storage media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified public keys, the time and date provided, the name of the organization, and the name and contact information (phone, address, email address) of the recipient.
3. When a private key used to generate digital signature reference information becomes compromised, the NSRL or other designated repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date on which it was compromised.
4. The NSRL or other designated repository shall make both the reference information available on unalterable storage media and its associated documentation that is labeled by the repository that created it uniquely identifiable by including at a minimum: a unique identifier (such as a serial number) for the storage media; the time, date, location and name of the creating repository; and an indication that the contents are reference information.

**Test Assertions**

**TA7451a-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates hash value reference information THEN the repository SHALL use FIPS-approved algorithms for hashing.

**TA7451a-2:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates digital signature reference information THEN the repository SHALL use FIPS-approved algorithms for signing.

**TA7451ai-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates hash values THEN the repository SHALL use a FIPS 140-2 level 1 or higher validated cryptographic module to generate hash values.

**TA7451ai-2:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates digital signature reference information THEN the repository SHALL use a FIPS 140-2 level 1 or higher validated cryptographic module to generate digital signature reference information.

**TA7451ai-3:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates cryptographic keys THEN the repository SHALL use a FIPS 140-2 level 1 or higher validated cryptographic module to generate cryptographic keys.

**TA7451aii-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates sets of hash values for reference information THEN the repository SHALL include a hash value or digital signature covering the set of reference information to generate sets of hash values for reference information.

**TA7451aii-2:** IF NIST’s National Software Reference Library OR the repository designated by the state election official generates digital signatures for reference information THEN the repository SHALL include a hash value or digital signature covering the set of reference information to generate digital signatures for reference information.

**TA7451bi-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN public key pairs used by the repository to generate digital signatures SHALL be at least 2048-bits in length.

**TA7451bi-2:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN private key pairs used by the repository to generate digital signatures SHALL be at least 2048-bits in length.

**TA7451bii-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN the repository’s private keys used to generate digital signature reference information SHALL NOT be used for more than three years.

**TA7451biii-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN public keys used to verify digital signature reference information SHALL either 1) be contained in a signed non-proprietary format for distribution OR 2) placed on unalterable storage media.

**TA7451biv-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN all copies of public key unalterable storage media made by the repository shall be labeled so that they are uniquely identifiable.

**TA7451biv-1-1:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain a unique identifier for the unalterable storage media.

**TA7451biv-1-1-1:** The unique identifier MAY be a serial number.

**TA7451biv-1-2:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain the time of the repository owning the associated private keys.

**TA7451biv-1-3:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain the date of the repository owning the associated private keys.

**TA7451biv-1-4:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain the location of the repository owning the associated private keys.

**TA7451biv-1-5:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain the name(s) of the repository owning the associated private keys.

**TA7451biv-1-6:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain documentation about the repository’s creation.

**TA7451biv-1-7:** All copies of public key unalterable storage media made by the repository SHALL be labeled so that they contain an indication that the contents are public keys.

**TA7451biv-1-8:** All copies of public key unalterable storage media made by the repository MAY contain other labels that uniquely identify these copies.

**TA7451bv-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official uses public key technology THEN the NSRL or other designated repository SHALL document to whom they provide unalterable storage media containing their public keys used to verify digital signature reference information.

**TA7451bv-1-1:** This documentation SHALL contain the uniquely identified public keys.

**TA7451bv-1-2:** This documentation SHALL contain the time provided.

**TA7451bv-1-3:** This documentation SHALL contain the date provided.

**TA7451bv-1-4:** This documentation SHALL contain the name of the organization.

**TA7451bv-1-5:** This documentation SHALL contain the name of the recipient.

**TA7451bv-1-6:** This documentation SHALL contain the contact information of the recipient.

**TA7451bv-1-6-1:** This contact information SHALL include the phone number of the recipient.

**TA7451bv-1-6-2:** This contact information SHALL include the address of the recipient.

**TA7451bv-1-6-3:** This contact information SHALL include the email address of the recipient.

**TA7451bv-1-7:** The documentation MAY contain other pertinent information that identifies to whom the unalterable storage media was provided.

**TA7451bvi-1:** IF a private key used to generate digital signature reference information becomes compromised THEN NIST’s National Software Reference Library OR the repository designated by the state election official SHALL provide notification to recipients of the associated public key that the private key has been compromised.

**TA7451bvi-2:** IF a private key used to generate digital signature reference information becomes compromised THEN NIST’s National Software Reference Library OR the repository designated by the state election official SHALL provide notification to recipients of the associated public key of the date on which the private key was compromised.

**TA7451c-1:** IF NIST’s National Software Reference Library OR the repository designated by the state election official makes reference information available THEN the repository SHALL make the reference information available on unalterable storage media.

**TA7451c-2:** IF NIST’s National Software Reference Library OR the repository designated by the state election official has associated documentation for reference information THEN the repository SHALL make the reference information’s associated documentation that is labeled by the repository that created it uniquely identifiable.

**TA7451c-2-1:** The associated documentation SHALL include a unique identifier for the storage media.

**TA7451c-2-1-1:** The unique identifier MAY be a serial number.

**TA7451c-2-2:** The associated documentation SHALL include the time of the creating repository.

**TA7451c-2-3:** The associated documentation SHALL include the date of the creating repository.

**TA7451c-2-4:** The associated documentation SHALL include the location of the creating repository.

**TA7451c-2-5:** The associated documentation SHALL include the name of the creating repository.

**TA7451c-2-6:** The associated documentation SHALL state or otherwise indicate that the contents are reference information.