Derived Test Requirements for the Updated Cryptography Requirements in the VVSG Version 1.1

Version 1.1
July 15, 2009

Preliminary Draft

Preliminary Draft

This document and associated files have been prepared by the National Institute of Standards and Technology (NIST) and represent draft test materials for the Election Assistance Commission's version 1.1 of the VVSG. It is a preliminary draft and does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

Product Disclaimer

Certain commercial entities, equipment, or material may be identified in the document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

Preliminary Draft

TABLE OF CONTENTS

Preliminary Draft

1 Introduction

1.1 Background

By authorization of the 2002 Help America Vote Act (HAVA), the Election Assistance Commission (EAC) was given the responsibility for implementing and maintaining the Voluntary Voting System Guidelines (VVSG). As part of the maintenance process for the VVSG, the EAC is updating the VVSG 2005 by modifying and adding some requirements to the guidelines resulting in the VVSG version 1.1. The new and modified requirements are based on the requirements found in the next VVSG developed by the EAC's Technical Guidelines Development Committee (TGDC). However, not all of the requirements found in the next VVSG were included as part of the VVSG version 1.1. The EAC plans to issue the VVSG version 1.1 after receiving and reviewing public comments.

As part of the VVSG update, the EAC asked NIST to develop a set of uniform public test suites for the modified and new requirements, which will be used as part of the EAC's Testing and Certification Program. Test Labs will be able to use these freely available test suites to help determine that modified and new requirements of the VVSG version 1.1 are met by voting systems. Use of the public test suites will produce consistent results and promote transparency of the testing process. The test suites can also assist manufacturers in the development of conforming products by providing precise test specifications. Also, they will help reduce the cost of testing since each test lab would no longer need to develop its own test suites. Finally, a uniform set of public test suites can increase election officials' and voters' confidence that voting systems conform to VVSG version 1.1 requirements covered by the test suites.

1.2 Purpose

The purpose of this document is to develop detailed test procedures for the updated and new security requirements found in the VVSG version 1.1. In this document, detailed test procedures derived from a requirement found in the VVSG version 1.1 are contained in structure known as a derived test requirement (DTR). (See Section 1.5 Derived Test Requirement Structure for details). This document contains the set of derived test requirements (DTRs) for the updated cryptography requirements found in the VVSG version 1.1. By providing detailed derived test requirements, the following objectives are achieved:

1. In-depth guidance to test laboratories to ensure high quality testing
2. Repeatability from tester to tester as well as test laboratory to test laboratory
3. Predictability of the effort involved for a testing campaign
4. Cost savings by not having to analyze and develop tests for different implementations of a voting system

1.3 Scope

The scope of this document is limited to functional testing of the updated and new security requirements found in the VVSG version 1.1. Testing requirements in VVSG version 1.1 other than updated and new security requirements are outside the scope of this document. Specifically, the derived test requirements (DTRs) found in this document only cover the updated cryptography requirements found in the VVSG version 1.1. The following sections from Volume 1 of the VVSG version 1.1 contain updated cryptography requirements:

2.4.4.1 – Voting system electronic records
2.4.4.1 – Tabulator electronic records

Preliminary Draft

7.4.5.1 – Hashes and digital signatures
7.4.6 – Software setup validation
7.5.1 – Maintaining data integrity
7.7.3 – Protecting transmitted data
7.9.3 – Electronic and paper record structure

1.4 Approach

In developing the set of derived test requirements (DTRs) the following approach was taken:

1. If at all possible, the test laboratory shall test compliance with a VVSG requirement by stimulus → response testing[1] on the voting system. The exceptions to this shall be rare and shall be justified only on the basis of extremely prohibitive cost.
2. The stimulus → response testing shall include nominal, boundary and outlier values as implied by the VVSG requirement and the voting system's interface(s) that implement and enforce the requirement.
3. When stimulus → response testing is not possible given the design of the voting system, the test laboratory shall examine the applicable source code.
4. When performing review of the manufacturer provided documentation, the test laboratory shall focus on gaining an understanding of the voting system and how it implements security. Priority shall be given to identification of potential security concerns based on the review and analysis of manufacturer documents with next priority to substantive inconsistencies. In addition, the test laboratory shall ensure that there is sufficient clarity to the documentation so that the security controls can be appropriately configured.

1.5 Derived Test Requirement Structure

A derived test requirement (DTR) is a structured used to contain detailed test procedures associated with a specific requirement. This section describes the components, nomenclature, and notation used in this document to describe the structure of a derived test requirement (DTR).

A derived test requirement consists of the following components:

1. A requirement is labeled with the literal "RE, " followed by a number based on the section of the VVSG version 1.1 containing the requirement and a title for the requirement to provide traceability back to the VVSG version 1.1. When a requirement is tested by another derived test requirement (DTR), that requirement's derived test requirement (DTR) will contain a reference to the appropriate derived test requirement (DTR).

2. A requirement may have one or more tester activities associated with it. Test activities are the detailed test procedures used to test the voting system for conformance to the VVSG version 1.1 security requirements. When no tester activity is found in a derived test requirement (DTR), it means the requirement was tested under the test procedures of another (DTR) that is specifically referenced in "Analysis" text. The tester activities are labeled with the literal "TE", followed by the requirement name ("Crypto Module", "Key Size", MAC Size etc.), followed by period ("."), followed by sequential numbers staring with 1. Each tester activity title is refined based on the associated VVSG version 1.1 requirement title.

3. The label "Analysis:" precedes text that is used to provide additional information related to requirements and tester activities. In general, analysis text follows the associated requirement and tester activities being discussed. For example, analysis text following a requirement may cross-reference the test activities of another requirement that verifies the requirement or provide context of the test activities of the requirement.

[1] Stimulus → response testing refers to a testing method where an IT system is stimulated by providing some input and the IT system's response/output is observed and analyzed. (See Definitions section)

Preliminary Draft

1.6 Electronic File Features for Word Versions of the Document

An electronic version of this document was prepared using Microsoft Word and the Word Style feature. The Word Style feature provides the ability to separate text based on the Style associated with the text. The following Styles were used in this document to allow material to be subsetted in or out:

1. “reheader” Style is used to list the requirement title.
2. “teheader” Style is used to list the test procedure title.
3. “Test Procedure” Style is used to list the test procedures test laboratories must carry out in order to test the voting system for compliance with VVSG Version 1.1 requirements.
4. “Normal” Style is used for the requirement text and text associated with analysis and rationale. “

1.7 General Testing Assumptions

The tester shall use each DTR to test the voting system under test and when appropriate develop more detailed test procedures and test cases based on implementation dependant characteristics such as specific configuration requirements, specific user account names, specific file names, etc.

The tester shall document test procedures and test cases.

After conducting the tests, the tester shall document the test results with sufficient detail to demonstrate that the test succeeded or failed. In the case of failure, the documentation shall be detailed enough to provide the nature of failure.

The tester may execute the DTRs in any order as long as the precedence requirements specified in individual DTR are met.

The tester shall note the start and end time in date, hours, and minutes when each DTR is executed to help in several ways including but not limited to: reconciling the event log, reconstructing DTR execution sequence, and determining the state of the voting system under test at any given time

Preliminary Draft

2 Definitions

Stimulus → Response Testing: A test method where the IT system is stimulated by providing some input and the IT system's response (output) is observed and analyzed. Also see test method for other form of testing.

Test Case: A fully defined set of input and expected results for a test. A test case is the most detailed and lowest level of test documentation material.

Test Method: Description of one or more tests, procedures by which tests are derived, or a combination of these.

Test Pre-Requisite: System configuration prior to executing a test case or set of test cases. For example, prior to testing that identification and authentication succeeds and fails under appropriate conditions, user accounts with specific user ID and passwords will need to be set up.

Test Procedures: Procedures used to execute a collection of test cases. For example, test procedures typically will consist of executing a set of steps to set test pre-requisite and then steps for each test case as identified with the test case,

Test Results: Set of results for each of the test cases.

Preliminary Draft

3 Cryptography Requirements

3.1 Next VVSG cryptography requirements

The following two general cryptography requirements were taken from the next VVSG and added to version 1.1 of the VVSG:

RE 5.1.1-A Cryptographic module validation:

Cryptographic functionality ***SHALL*** be implemented in a FIPS 140-2 validated cryptographic module operating in FIPS mode.

and

RE 5.1.1-B Cryptographic strength:

Programmed devices that apply cryptographic protection shall employ NIST approved algorithms with a security strength of at least 112-bits to protect sensitive voting information and election records. Message Authentication Codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems; however, the key used with such MACs shall also have a security strength of at least 112 bits.

3.2 VVSG version 1.1 Cryptography Requirements

Cryptographic requirements found in the 2005 VVSG were updated based on the requirements identified in the previous section. The next VVSG cryptography requirements were incorporated to maintain the style and form of the 2005 VVSG requirements. In addition, discussion text accompanied the updated 2005 VVSG requirements to provide more clarification of the requirement.

The following is an example of the a resulting VVSG version 1.1 requirement and discussion section that incorporates the two next VVSG cryptography requirements:

Voting systems shall digitally sign electronic reports using FIPS approved algorithms with a security strength of at least 112 bits implemented within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode.

Discussion: NIST approved is — An algorithm or technique that meets at least one of the following: 1) is specified in a FIPS or NIST Recommendation, 2) is adopted in a FIPS or NIST Recommendation or 3) is specified in a list of NIST approved security functions (e.g., specified as approved in the annexes of FIPS 140-2/3)‖. The security strengths of cryptographic algorithms can be found in NIST Special Publication 800-57: Recommendation for Key Management – Part 1 General.

Preliminary Draft

4 Cryptography Derived Test Requirements

The following sections from Volume 1 of the VVSG version 1.1 contain cryptography requirements that are tested using the DTRs found in this section:

2.4.4.1 – Voting system electronic records
2.4.4.1 – Tabulator electronic records
7.4.5.1 – Hashes and digital signatures
7.4.6 – Software setup validation
7.5.1 – Maintaining data integrity
7.7.3 – Protecting transmitted data
7.9.3 – Electronic and paper record structure

4.1 Derived Test Requirements for Cryptographic Module

TE Crypto Module.1 Cryptographic module validation information verification -- Modules:

The tester shall perform this activity by visiting the NIST website (http://csrc.nist.gov/cryptval/) and examining the certificate number listed for each cryptographic module. The tester shall verify the following for each cryptographic module:

1. Cryptographic module name identified in the manufacturer documentation matches the name on the certificate.
2. The overall module rating is Security Level 1 or higher.
3. Cryptographic module description identifies hardware, software, or both.
4. If the cryptographic module description includes, firmware, the description also includes hardware.
5. If present in the certificate, the manufacturer documentation identifies the same hardware name, model name, and revision number as those in the certificate.
6. If absent in the certificate, the manufacturer documentation does not identify hardware.
7. If present in the certificate, the manufacturer documentation identifies the same firmware name, identifier, and version number as those in the certificate.
8. If absent in the certificate, the manufacturer documentation does not identify firmware.
9. If present in the certificate, the manufacturer documentation identifies the same software name, identifier, and version number as those in the certificate.
10. If absent in the certificate, the manufacturer documentation does not identify software.

The tester shall record the following from the certificate for each cryptographic module in order to perform remaining test.:

1. If present, hardware platform on which software portion of the cryptographic module executes.
2. If present, operating system on which software portion of the cryptographic module executes.
3. Cryptographic algorithms the module is approved for.
4. Overall Security Level for the module

TE Crypto Module.2 Cryptographic module validation environment verification:

The tester shall perform the following checks for each cryptographic module for the SUT:

1. If the hardware platform(s) is specified for the software portion of the cryptographic module in the certificate, the SUT must belong to the family of one of the specified hardware platform (e.g., x86)

Preliminary Draft

2. If the operating system(s) is specified for the software portion of the cryptographic module in the certificate, the SUT must belong to the family of one of the specified operating system (e.g., Windows XP, Unix).
3. If the certificate links the hardware platform(s) and associated operating system(s), the SUT must belong to the family of one of the hardware, operating system pairing (e.g., PowerPC Linux)

TE Crypto Module.3 Cryptographic module validation description verification:

The tester shall perform the following checks for each of the cryptographic module for the SUT:

1. If the cryptographic module description includes hardware, the tester shall verify the hardware model number and version number obtained from the FIPS certificate match one of the following:
    a) Invoke the cryptographic module interface to the SUT to query the cryptographic module to obtain the hardware model number and revision number; or
    b) If the cryptographic module does not provide this capability, obtain the hardware model number and revision number from the hardware placard on the SUT; or
    c) If the cryptographic module information is not on the placard or if the placard is not visible, obtain the hardware model number and revision number from the manufacturer documentation.
2. If the cryptographic module description includes firmware, the tester shall invoke the cryptographic module interface to the SUT to query the cryptographic module to obtain the firmware identifier and version number. The tester shall verify this information against the information on the FIP certificate.
3. If the cryptographic module description includes software, the tester shall invoke the cryptographic module interface to the SUT to query the cryptographic module to obtain the software identifier and version number. The tester shall verify this information against the information on the FIP certificate.

TE Crypto Module.4 Cryptographic module validation configuration verification:

The tester shall authenticate to the SUT as an administrator.

The tester shall examine the configuration of each cryptographic module for the SUT:

1. The tester shall invoke the cryptographic module interface to the SUT to query the cryptographic module to determine that the module is configured for the FIPS mode. TE Crypto Module.4 Cryptographic module validation configuration verification shall also be considered passed if there is no way to configure the cryptographic module in non-FIPS mode[2].

The tester shall terminate the authenticated session.

TE Crypto Module.5 Cryptographic module validation algorithm verification:

The tester shall list SUT functions that invoke cryptographic algorithms. For each function, the tester shall list the algorithms invoked, and the cryptographic module which executes the algorithm as shown in the example below.

TABLE 1: CRYPTOGRAPHIC MODULES AND ALGORITHMS

SUT Function	Cryptographic Algorithm	Cryptographic Module
Encrypt Logs	**SHA-256**	**Module X**
	Encryption	**Module Y**
	MAC	**Module X**
Create Random Ballot ID	**SHA-1**	**Module Z**

[2] The modes of configuration for a cryptographic module are identified in a cryptographic module security policy. The NIST website http://csrc.nist.gov/cryptval/ contains the security policies for the FIPS 140-2 validated cryptographic modules.

Preliminary Draft

The tester shall verify that each of the cryptographic algorithms the manufacturer claims the cryptographic module is used for (per Table 1 above) is listed in the FIPS certificate for the cryptographic module.

The tester shall examine the SUT code to verify that a cryptographic module is invoked for the cryptographic algorithm. The tester shall perform this activity by tracing the code starting with the SUT function invocation and ending with invocation of the cryptographic module algorithm.

4.2 Derived Test Requirements for Key Size

This section contains the DTR for the following requirement: "The cryptography shall use NIST approved cryptographic algorithms with at least 112 bit security." This requirement appears in several places in the VVSG 2005. The DTR identified in this section shall be executed once for each instance the requirements appear in VVSG 2005. In addition, the DTR must be executed for each of the cryptographic mechanisms for each instance since each instance the requirement appears in VVSG 2005, the manufacturer may use one or more cryptographic mechanisms.

TE Key Size.1 Cryptographic strength – Key Size:

The tester shall verify that when used, the cryptographic mechanisms use the following algorithms and key sizes.

Note that SHA-1 is not acceptable as a hash function in digital signature calculation.

If the tester has the expertise to make the determination, SHA-1 is not an acceptable hash function for cryptographic mechanisms where collision attacks are a threat.

SHA-1 is an acceptable hash function for cryptographic mechanisms such as MAC, PRNG, and KDF since these mechanisms are not subject to collision attacks.

If the tester does not have the expertise to make the determination and digital signature is not used, SHA-1 is an acceptable hash function.

TABLE 2: CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES

Cryptographic Mechanism	Standard	Algorithm	Mode of Operation/Scheme	Key Size
Hashing	FIPS 180-2	SHA-224	N/A	None
		SHA-256	N/A	None
		SHA-384	N/A	None
		SHA-512	N/A	None
Digital Signature	FIPS 186-2	DSA	N/A	Large Prime ≥ 2,048 bits; and Small Prime ≥ 224 bits
		RSA (ANSI X9.31)	N/A	Modulus ≥ 2,048 bits
		RSA (PKCS-1, V2.1 -- V1.5, PSS)[3]	N/A	Modulus ≥ 2,048 bits
		ECDSA	N/A	Prime field ≥ 224 bits; or Binary field ≥ 233 bits
Key Transfer	ANSI X9.44	RSA	N/A	Modulus ≥ 2,048 bits

[3] PKCS-1, V2.1 contains two compliant format PKCS-1, version 1.5 and PSS.

Preliminary Draft

Cryptographic Mechanism	Standard	Algorithm	Mode of Operation/Scheme	Key Size
	PKCS-1 V2.1	RSA	N/A	Modulus ≥ 2,048 bits
Key Establishment[4]	SP 800-56A	DH	SP 800-56A	Large Prime ≥ 2,048 bits; and Small Prime ≥ 224 bits; and SHA-224 or better; and MAC key ≥ 112 bits
		ECDH	SP 800-56A	Prime field ≥ 224 bits; or Binary field ≥ 233 bits; and SHA-224 or better; and MAC key ≥ 112 bits
		FFC MQV	SP 800-56A	Large Prime ≥ 2,048 bits; and Small Prime ≥ 224 bits; and SHA-224 or better; and MAC key ≥ 112 bits
		EC MQV	SP 800-56A	Prime field ≥ 224 bits; or Binary field ≥ 233 bits; and SHA-224 or better; and MAC key ≥ 112 bits
Data Encryption	FIPS 197	AES	SP 800-38A; SP 800-38C	≥ 128 bits
	FIPS 46-3	TDES	SP 800-38A	3 keys 168 bits
HMAC	FIPS 198	Approved SHA Based	N/A	112 bits
MAC	SP 800-38B	TDES Based	CMAC	3 keys 168 bits
	SP 800-38B	AES Based	CMAC	≥ 128 bits
	SP 800-38C	AES Based (CCM)	CCM	≥ 128 bits
PRNG	FIPS 140-2	Annex C	N/A	N/A
RNG SEED	FIPS 140-2	N/A	N/A	N/A

Preliminary Draft

TE MAC Size.1 Cryptographic strength – MAC:
The MAC algorithm is a FIPS approved algorithm is tested under TE Key Size.1 Cryptographic strength – Key Size.

The MAC key size is FIPS approved is already tested under TE Key Size.1 Cryptographic strength – Key Size.

The MAC implementation is FIPS validated is tested under TE Crypto Module.5 Cryptographic module validation algorithm verification.

The tester shall verify that the resulting MAC is 96 bits or longer. The purpose of this step is to ensure that the protocol and associated implementation do not truncate the MAC to a length that may not support the security strength of the algorithm and key size.

[4] Key establishment is also referred in the literature as key exchange or key agreement.