VVSG 2007 Cryptography Requirements

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.1 Cryptography

This section establishes general cryptography requirements for voting systems, specifies that signatures for protecting electronic voting records used in audits be generated in an embedded hardware signature module, and specifies the requirements for that module. These requirements include a key management scheme for the signature keys used by the signature cryptographic module, and requirements to help ensure that the signatures are reliable even if the voting device software has bugs or is tampered with.

Cryptography typically serves several purposes in voting systems. They include:

- Confidentiality: where necessary the confidentiality of voting records can be provided by encryption;
- Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the voting systems, while voting systems apply digital signatures to authenticate the critical audit data that they output; and
- Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.

This section establishes general technical requirements for the cryptographic functionality of voting systems, and some more specific requirements that certain cryptographic functions (digital signatures and key management for digital signatures) be performed in a protected hardware cryptographic module that is isolated from the voting system software, so that it is unlikely that the keys will be revealed or the cryptographic functionality compromised, even in the presence of a bug or malicious code in the other parts of the voting system and even if an adversary (possibly a corrupt insider) gains physical access to or control of the voting system for a period of time. The purpose of the signatures is to authenticate election records, and hardware cryptographic modules are not required for other cryptographic operations.

5.1.1 General cryptographic implementation

5.1.1-A Cryptographic module validation

Requirement:	Cryptographic functionality SHALL be implemented in a FIPS 140-2 validated

	cryptographic module operating in FIPS mode.
Applies to:	Programmed device
Test Reference:	Part 3:3.1 “Inspection”, 4.1 “Initial Review of Documentation”, 4.2 “Physical Configuration Audit”, 4.5 “Source Code Review”
Discussion:	Use of validated cryptographic modules ensures that the cryptographic algorithms used are secure and their correct implementation has been validated. Moreover, the security module security requirements have been validated to a specified security level. The current version of FIPS 140 and information about the NIST Cryptographic Module Verification Program are available at: http://csrc.nist.gov/cryptval/. Note that a voting device may use more than one cryptographic module, and quite commonly will use a “software” module for some functions, and a “hardware” module for other functions. This requirement is a generalization of [VVSG2005] I.7.5.1-b, which is a cryptographic requirement with a limited scope to the encryption of data across public communication networks. That requirement mandated use of "an encryption standard currently documented and validated for use by an agency of the U.S. government". Use of public communication networks is forbidden in this document except for transmitting unofficial results or communicating with an electronic pollbook. This requirement extends and strengthens [VVSG2005] I.7.8.2, which required use of a validated cryptographic module if signature signatures were used in voting system with independent verification. Use of digital signatures is required in this document, and this requirement mandates the use of a FIPS validated module. This requirement is a generalization of [VVSG2005] I.7.4.6-d, which is a cryptographic requirement with a limited scope. That requirement mandated the use of FIPS 140-2 level 1 or higher validated cryptographic modules if hash functions or digital signatures are used during software validation. Lastly, this requirement restates and strengthens [VVSG2005] I.7.9.3-a by requiring all cryptographic functionality be implemented in FIPS validated modules. [VVSG2005] I.7.9.3-a provides an exception when a cryptographic voting system uses cryptographic algorithms that are necessarily different from any algorithms that have approved CMVP implementations.
Source:	[VVSG2005] I.7.5.1-b, I.7.8.2, I.7.4.6-d, I.7.9.3-a
Principle(s)/ Guideline(s):	*Security: Data Protection* All cryptographic algorithms are public, well-vetted, and standardized. **Justification:** This guideline aligns with this requirement. The FIPS 140-2 program goes a bit further and also tests implementations.

5.1.1-B Cryptographic strength

Requirement:	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.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.5 ”Source Code Review”
Discussion:	As of February 2006, NIST specifies the security strength of algorithms in SP 800-57, Part 1 . This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades. This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* All cryptographic algorithms are public, well-vetted, and standardized. **Justification:** This guideline aligns seems to align with this requirement, although the guidelines do not state much about the strength and keysize.

5.1.2 Digital signatures for election records

This section states the requirements for digital signatures generated by voting devices to sign election records. The purpose of signing election records is to authenticate them and prevent their subsequent alteration. This makes it more difficult to falsify election records so that a careful audit would not detect evidence of the alteration or would not detect that election fraud had occurred. It also makes it more difficult to forge electronic CVRs that would be accepted in the normal vote counting process. The specific requirements for the records that must be signed are given in Part 1:5.2.2 “Voting device election information inspection” and 5.2.3 “Voting equipment properties inspection”. A separate hardware Signature Module (SM) protects the private signature keys and the signature process should the election system software be compromised. The module is “embedded in” (permanently attached to) the voting device to make it difficult to substitute another module.

This guideline does not require that the SM implement all of the cryptographic functionality of the voting device (although the SM might do so), nor does it require that the SM process the signed records directly. It is conventional and acceptable for a host computer system to provide a message digest generated from the record to be signed by a cryptographic hash function and the signature cryptographic module conventionally signs that. Standardized digital signature algorithms all apply the private signature key to a message digest rather than the message itself.

The SM is required only in those devices that digitally sign election records. Signature verification and other cryptographic functions need not be implemented in hardware. Moreover, digital signature operations can be used for authentication in challenge-response protocols, and the hardware requirements of this section do not apply to such uses of digital signatures. In such cases the signature is not normally retained as a part of the record of the election.

5.1.2-A Digital signature generation requirements

Requirement:	Digital signatures used to sign election records SHALL be generated in an embedded hardware Signature Module (SM).
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.5 “Source Code Review”
Discussion:	The use of an embedded hardware module for the generation of signatures on election records protects the signature keys and helps to protect the integrity of those records even if the general voting device software is compromised. This makes it more difficult to create spurious election records. Note that in some cases digital signature operations may be used in ways that do not “sign” election records – for example, in the authentication processes of communications protocols. Such digital signature operations may be performed in other crypto modules, which, while they must be validated as per Part 1:7.7.1 “Integrity” above, need not be hardware modules.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The source and integrity of electronic tabulation reports are verifiable. **Justification:** The digital signatures are used for verification.

5.1.2-B Signature Module (SM)

Requirement:	Programmed devices that sign election records SHALL contain a hardware cryptographic module, the Signature Module (SM), that is capable of generating and protecting signature key pairs and generating digital signatures.
Applies to:	Programmed device
Test Reference:	Part 3:3.1 “Inspection”, 4.1 “Initial Review of Documentation”, 4.2 “Physical Configuration Audit”
Discussion:	For the purpose of this requirement a “hardware” cryptographic module means a distinct electronic device, typically a preprogrammed, dedicated microcomputer that holds keying material and performs cryptographic operations. Although today this might typically be a single chip, soldered onto a larger motherboard, it is not the intent of this guideline to preclude higher levels of integration. It is expected that future voting devices may integrate the SM onto the same die as the rest of the voting device, as long as the SM is clearly physically and logically separated on the die from the rest of the voting device so that there is a distinct cryptographic module boundary, and there is no way for the rest of the device to access signature private keys except through the defined cryptographic module interface. Signature verification and other cryptographic operations need not be implemented in hardware, but may also be implemented on the embedded signature module if desired.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The source and integrity of electronic tabulation reports are verifiable.

	Justification: The digital signatures are used for verification.

5.1.2-B.1 Non-replaceable embedded Signature Module (SM)

Requirement:	Signatures Modules (SMs) SHALL be an integral, permanently attached component of a Programmed device.
Applies to:	Programmed device
Test Reference:	Part 3:3.1 “Inspection”
Discussion:	The SM is an integral, nonreplicable part of the voting device, to prevent tampering by replacing or substituting another device. For example, if there is a motherboard, the SM would typically be soldered to the motherboard of the voting device. If the core of the voting device is contained on a single chip computer, the module would be a distinct, integral, but independent processor on that chip that does not share logic or memory with other functions.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The source and integrity of electronic tabulation reports are verifiable. **Justification:** The digital signatures are used for verification.

5.1.2-B.2 Signature module validation level

Requirement:	Signature Modules SHALL be validated under FIPS 140-2 with FIPS 140 level 2 overall security and FIPS 140 level 3 physical security.
Applies to:	Programmed device
Test Reference:	Part 3:3.1 “Inspection”, 4.1 “Initial Review of Documentation”
Discussion:	FIPS 140 level 3 physical security requires tamper resistance.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* All cryptographic algorithms are public, well-vetted, and standardized. **Justification:** This guideline aligns with this requirement.

5.1.3 Key management for signature keys

Digital signatures require the generation and management of signature key-pairs: a private key and a related public key. The private key is used to sign a message (or, more precisely, the cryptographic message digest of the message), while the associated public key is used to verify the signature on a message. Public keypairs are certified by public key certificates, electronic documents that are generated and digitally signed by some issuer (often called a Certification Authority or “CA”). The certificates bind a name and other associated data to a public key. Each voting device that generates digitally signed election records contains a Signature Module (SM) contains a single permanent Device Signature Key (DSK) and, at any one time, up to one Election Signature Key (ESK).

A new ESK is generated by the embedded signature module for every election. An ESK public key certificate is signed with the device key, and binds an election key to the name of the voting device and an election identifier. As a part of the election closeout procedure, a signed count of the number of signature operations performed with the ESK is produced, and the private component of the ESK is destroyed, to preclude later addition to the signed election records.

The SM is provisioned by the voting device manufacturer with a public key certificate for its DSK, which is exported on commend from the SM; however, the SM creates its own signature keys internally and does not permit the export of private signature keys. The SM maintains a copy of its device key certificate and its current election key certificate, and outputs them on request.

5.1.3.1 Device Signature Key (DSK)

The Device Signature Key (DSK), a public key-pair, is internally generated by the voting device as a part of its initial configuration. The DSK has a Device Public Key Certificate that certifies the DSK public key. The Device Public Key Certificate may be externally (to the SM) generated and signed by the voting device manufacturer, then installed in the SM by the manufacturer, or, alternately, it may be generated internally by the SM and signed by the DSK private key as a selfsigned certificate. The purpose of the DSK is to sign certificates for election keys, and Election Closeout Records. Once generated or installed in the DSK, the DSK certificate is permanently stored in the SM and never altered, although copies of it may be exported from the SM. The DSK certificate is an electronic record that binds the DSK to the unique identification of a single voting device (typically the manufacturer's name, the model number of the device, the unique serial number of the device, and its date of manufacture), for the service life of the voting device.

5.1.3.1-A DSK Generation

Requirement:	Signature Modules SHALL securely generate a permanent DSK in the module, using an integral nondeterministic random bit generator.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 "Functional Testing", 4.1 "Initial Review of Documentation", 4.5 "Source Code Review"
Discussion:	FIPS 186-3 and NIST Special Publication 800-89 give technical requirements for the generation of secure digital signature keys.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** The Data Protection principle mapped best to this requirement.

5.1.3.1-B Device Certificate generation

Requirement:	There SHALL be a process or mechanism for generating an X.509 Device Certificate that binds the DSK public key to the unique identification of the programmed device, the certificate's date of issue, the name of the issuer of the certificate and other relevant permanent information.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 "Functional Testing", 4.1 "Initial Review of Documentation"
Discussion:	The Device Certificate may be generated in the SM and self-signed by the DSK, or it may be signed by a separate external Certification Authority (CA) and installed in the SM by the manufacturer. That CA could be maintained by or for the voting

	device manufacturer, or on the behalf of the manufacturer. Alternatively, it could be maintained by or for the election authority that purchases the voting device. If the Device Certificate is self-signed, then election authorities should maintain accurate, reliable'' records of the self-signed certificates of its voting devices. The Device Certificate permanently binds the device's public key to the unique identification of the individual voting device (the same make, model, serial number information placarded on the case of the voting device). The device certificate might also optionally include the name of the owner of the machine, and any other relevant information that would not change over the service life of the voting device. This guideline does not prescribe a specific Public Key Infrastructure for keeping and verifying the Device Certificates. A public key certificate is not a secret or confidential record, and the device certificate can be stored or distributed in any convenient manner. If the device certificate is self-signed, then election authorities should maintain independent, accurate, reliable records of the self-signed certificates of its voting devices. If a CA signs the certificate, then the public key of the CA should be securely established and maintained. No revocation or certificate status mechanism is required for the Device Certificates. Although this standard does not require this, a hash (or at least 64-bits from the hash) of the device public key could be used as the device serial number, making the Device Public Key effectively the device serial number. Note that the requirement to internally generate private keys and certificates implies requirements to implement an approved hash function, and a nondeterministic random number generator. Also note that nothing in this section is intended to preclude a cryptographic module manufacturer from delivering SMs already initialized with a DSK and device certificate, perhaps accompanied by a placard (see below), to a voting device manufacturer for incorporation in the voting device.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Data Protection* All cryptographic algorithms are public, well-vetted, and standardized. **Justification:** This guideline maps to this requirement because it requires a process to be developed to follow a standard certificate process.

5.1.3-C Device Certificate storage

Requirement:	Device Certificates SHALL be stored permanently in the SM and be readable on demand by the programmed device.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 "Functional Testing", 4.1 "Initial Review of Documentation"
Discussion:	Although a copy of the Device Certificate may also be kept elsewhere (e.g., in a directory) a copy is always available with the device itself. Note that while there is ordinarily no concept of an "original" public key certificate since it is the signature on the key that validates it, but because the device certificate may be self-signed, the authenticity of a self-signed Device Certificate may be an issue,

	and the copy stored in the SM can be regarded as authoritative.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.3-D Device identification placard

Requirement:	A human readable identification placard SHALL be permanently affixed to the external frame of any programmed device containing an SM that states, at a minimum, the same unique identification of the voting device contained in the device certificate.
Applies to:	Programmed device
Test Reference:	Part 3:3.1 “Inspection”, 3.2 “Functional Testing”
Discussion:	It is important that election workers be able to identify and track specific voting devices and correlate them with election records. The placard and the device certificate identity the same device in the same way. The placard may also contain other information and machine-readable information as may be convenient.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.3-E Device Signature Key protection

Requirement:	Signature Modules and the process for generating DSKs SHALL be implemented so that the private component of DSK is created and exists only inside the protected cryptographic module boundary of the SM, and the key cannot be altered or exported from the SM.
Applies to:	Programmed device
Test Reference:	Part 3:4.1 “Initial Review of Documentation”, 4.5 “Source Code Review”
Discussion:	Once the key is installed in the SM it cannot be changed or read out from the module, and any external copy of the key must be destroyed as a part of the process of initializing the SM. The entire process of generating the key may take place in the SM; otherwise, a strictly controlled, secure process is required to generate the keys, install them in the modules, and destroy any external copies of the keys.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.3-F Use of Device Signature Key

Requirement:	Signature Modules SHALL implement and permit only three uses of the DSK: a. to sign Election Public Key Certificates; b. to sign Election Closeout Records; and c. to sign Device Public Key Certificates.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.1 “Initial Review of Documentation”, 4.5

	"Source Code Review"
Discussion:	Each generation of a new Election Signature Key is an auditable event, and the two purposes of the DSK are to certify the new ESK and to certify that an ESK private key has been closed out (destroyed). While the ESK simply signs hashes presented to it by the voting device software, the SM generates, hashes and signs Election Public Key Certificates and Election Closeout Records, although partially from text inputs supplied by the voting device.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4 Election Signature Key (ESK)

The purpose of an ESK is to sign election records in the course of an election. A voting device that signs election records generates its own ESKs and maintains only one ESK at a time. The public component of every ESK generated by the embedded signature module is signed by the DSK to create an Election Public Key Certificate, and when an election is closed out, the private component of that election key is destroyed by the SM, which produces an Election Closeout Record attesting to that destruction, signed by the DSK.

In the context of this section, an "election" may be held on a single day, for a single precinct or voting district, with a single ballot style, or it may span a period of days or weeks, and may involve a number of precincts and voting districts and ballot styles, if the voting device is intended to be so used (e.g., in voting centers or for early polling).

The SM is not aware of the context of its use, it simply creates a new ESK when requested by the voting device, signs hashes as requested by the voting device while keeping a count of the number of signatures for the ESK, and finally, when requested by the voting device, the SM destroys the ESK and produces a signed Election Closeout Record stating the number of times the ESK was used. The specific minimum requirements for this are specified below.

However, nothing in this section is intended to preclude the creation of other manufacturer defined signed records by the SM to support the overall election records and audit strategy for these more complex cases. For example, the SM might implement signed daily subtotals ESK use similar to those of the Election Closeout Record for use in multi-day elections. Alternatively, the SM might accumulate and output as a part of the closeout process signed totals by ballot style or some other identifier (which implies that the SM would have to include a way to input ballot style information in its API).

5.1.4-A Election Signature Key (ESK) generation

Requirement:	Signature Modules SHALL internally generate election signature key-pairs (ESK) using an integral nondeterministic random bit generator.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 "Functional Testing", 4.1 "Initial Review of Documentation", 4.5 "Source Code Review"
Discussion:	The ESK private key exists only in the embedded signature module. It is used with the cryptographic hashes of election records, to create signatures for election records. The ESK public key is exported from the embedded signature module in

	an election certificate signed by the DSK.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4-B Election Public Key Certificate

Requirement:	Signature Modules SHALL generate and output an X.509 public key certificate for each ESK generated, binding public key to the unique identification of the election, the date of issue of the certificate, the identification of the voting device (the issuer of the certificate), and, optionally, to other election relevant information.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.1 “Initial Review of Documentation”
Discussion:	An Election Public Key Certificate binds an ESK public key to a specific election and the unique name of the individual voting device (the issuer of the certificate). The issuer name should be consistent with the name in the Device Certificate. This guideline does not establish a name format for identifying elections, which might differ from jurisdiction to jurisdiction. No revocation or certificate status mechanism is required for the Election Certificates.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4-C Election counter

Requirement:	Signature Modules SHALL maintain an election counter that maintains a running count of each ESK generated.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.5 “Source Code Review”
Discussion:	Every election signature key created by the SM is numbered and this number is contained in the public key certificate for that key.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4-D Election Signature Key use counter

Requirement:	Embedded signature modules SHALL maintain a counter of the number of times that an ESK is used.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.5 “Source Code Review”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4-E Election Key Closeout

Requirement:	Signature Modules SHALL implement a closeout command that causes an Election Key Closeout record to be created and output, and the private component of the ESK to be destroyed.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”, 4.5 “Source Code Review”
Discussion:	When the election is complete, the ESK private key is destroyed so that election records cannot be forged at a later time.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.1.4-F Election Key Closeout record

Requirement:	The Election Key Closeout record SHALL be signed by the DSK and contain at least: a. The election signature public key (or a message digest of that key); b. The ESK number; and c. The final value of the ESK use counter.
Applies to:	Programmed device
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	