DISCUSSION PAPER:
The Transitioning of Cryptographic Algorithms and Key Sizes

1 Background and Purpose

At the beginning of the century, NIST began the task of providing cryptographic key management guidance. This included lessons learned over many years of dealing with key management issues, and attempts to encourage the definition and implementation of appropriate key management procedures, to use algorithms that adequately protect sensitive information, and to plan ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. This guidance is provided in NIST Special Publication (SP) 800-57.

Some of the guidance provided in SP 800-57 includes the definition of security strengths, the association of the approved algorithms with these security strengths, and a projection of the time frames during which the algorithms could be expected to provide adequate security. Note that the length of the cryptographic keys is often an integral part of these determinations.

The security strength is measured in bits and is, basically, a measure of the difficulty of discovering the key. The understood security strength for each algorithm is listed in SP 800-57. For example, RSA using a key length of 1024 bits (i.e., 1024-bit RSA) has a security strength of 80 bits, as does 2-key Triple DES, while 2048-bit RSA and 3-key Triple DES have a security strength of 112 bits. See Table 2 in Part 1 of SP 800-57 for further security strength information.

The appropriate security strength to be used depends on the sensitivity of the data being protected, and needs to be determined by the owner of that data. For the Federal government, a minimum security strength of 80 bits is currently required. However, a minimum security strength of 112 bits is planned in 2011 as indicated in Table 4 of SP 800-57, Part 1. We've learned that this is not so easily done. The reality is that we need to examine each class of algorithm and sometimes make some adjustments.

One of the means for enforcing the algorithm and security strength requirements is NIST's Cryptographic Module Validation Program (CMVP), which is responsible for validations cryptographic modules for conformance to FIPS 140-2. To be validated, each module requires at least one cryptographic algorithm that has been approved for Federal government use. Approved security functions (i.e., approved cryptographic algorithms) are listed in Annex A of FIPS 140-2. The CMVP is the vehicle used for testing conformance to FIPS 140-2 and the approved algorithm specifications. In some cases, an algorithm or protocol that has not been approved in a FIPS or NIST Recommendation is "allowed"; an algorithm is indicated as allowed by means of the FIPS 140-2 Implementation Guidance document. The CMVP has defined two classes of modes for cryptographic modules: the FIPS mode and the non-FIPS modes for cryptographic module operation; in general, the FIPS mode uses only approved or allowed algorithms can.

This paper is intended to bring some of the transition issues associated with the use of cryptography to the attention of the Federal government and the public, and to obtain

feedback about the proposed approaches. **Please provide comments to CryptoTransitions@nist.gov by August 3, 2009.**

The general approach for transitioning from one algorithm or key size to another is addressed in SP 800-57, Part 1. The remainder of this paper addresses transition issues from the point of view of the CMVP.

2 Encryption

Encryption is used to protect the confidentiality of sensitive information. Several algorithms are currently approved for the encryption of sensitive information by the Federal government:

- Triple DES is specified in SP 800-67, and has two key sizes, known as two-key Triple DES and three-key Triple DES. Two-key Triple DES has been assessed at a security strength of 80 bits[1], whereas three-key Triple DES is assessed at a security strength of 112 bits.
- SKIPJACK was approved in FIPS 185, and is assessed at a security strength of 80 bits.
- AES is specified in FIPS 197. It has three approved key sizes: 128, 192 and 256 bits. AES-128 is assessed at a security strength of 128 bits, AES 192 at a security strength of 192 bits, and AES-256 at a security strength of 256 bits.

NIST is proposing the following transition schedule (see Table 1).

Table 1: Encryption Transitions

Encryption Algorithm	New Validations	Already Validated Implementations
Two-key Triple DES	Through 2010	Disallow after 2010
Three-key Triple DES	OK	OK
SKIPJACK	Through 2010	Disallow after 2010
AES-128	OK	OK
AES-192	OK	OK
AES-256	OK	OK

As of December 31, 2010, Two-key Triple DES and SKIPJACK will no longer be approved for use by the Federal government to protect sensitive data (see SP 800-57, Part 1). No new validations will be performed on these algorithms after that date, and CMVP certificates that were previously issued will be modified to remove these algorithms from the approved list for the FIPS mode. Note that if no other approved algorithms are

[1] Note that the conditions for this assessment are provided in a footnote to Table 2 in SP 800-57, Part 1.

included in a cryptographic module, the certificate for that module will no longer be valid.

3 Digital Signatures

3.1 Transition from FIPS 186-2 to FIPS 186-3

Federal Information Processing Standard (FIPS) 186-3 specifies three algorithms for the generation and verification of digital signatures: DSA, ECDSA and RSA. FIPS 186-3 also includes methods for generating key pairs and domain parameters, as required. FIPS 186-3 incorporates the following changes:

General:

- Specifies the use of all hash functions provided in FIPS 180-3, rather than just SHA-1,
- Provides requirements for obtaining assurances of domain parameter validity (DSA and ECDSA only), public key validity, and private key possession,
- References SP 800-57 for guidance on key management, including the key sizes and security strengths to be used,
- Provides guidance on domain parameter and key pair management,
- References SP 800-90 for random number generation, rather than including RNGs in the Standard, either explicitly or by reference to ANSI Standards,
- Provides more guidance on the use of RNGs to generate key pairs,
- Provides revised primality test guidance.

DSA:

- Specifies larger key sizes,
- Replaces the domain parameter generation routine with new methods,
- Includes explicit methods for the validation of domain parameters,

RSA:

- Approves the use of both ANSI X9.31 and PKCS #1, and provides guidance for their use,
- Provides multiple explicit methods for the generation of key pairs,
- Limits the key sizes and provides criteria for the generation of key pairs to be used for Federal government use.

ECDSA:

- Although the Recommended Elliptic Curves continue to be included in FIPS 186-3 (as they were in FIPS 186-2), FIPS 186-3 allows the generation of alternative curves, using methods specified in ANS X9.62.

Since FIPS 186-3 only recently became official, a period of time must be defined for transitioning between FIPS 186-2 and 186-3. Some of the new tests required for testing

against FIPS 186-3 are now available, while others are under development, and will be made available as soon as possible.

Implementations designed to conform to FIPS 186-3 may now be submitted and tested by the CMVP testing labs. However, those features for which tests have not been completed will be validated by vendor affirmation until the tests are available.

New implementations designed to conform to FIPS 186-2 may be tested by the labs until December 31, 2010, after which only implementations claiming conformance to FIPS 186-3 will be tested for validation.

Certificates for implementations that were validated against FIPS 186-2 will continue to be valid, subject to the requirements for appropriate security strengths, as discussed in Section 3.2. For example, implementations that provide security strengths of 112 bits or more will continue to be valid and operable in the FIPS mode, but those that provide only 80 bits of security will not[2]. Note that the invalidation of certificates will affect all DSA (currently) validated implementations, and those implementations of RSA and ECDSA that only use SHA-1 for digital signature generation for non-repudiation purposes.

In order to reach a larger audience, a Federal Register Notice will be published that requests comments about other issues that need to be considered during the transition from FIPS 186-2 to FIPS 186-3. Readers of this paper are encouraged to identify any issues that they foresee in order to prepare the Federal Register Notice with a realistic transition strategy.

3.2 Security Strengths for Digital Signature Keys

Digital signatures are used for several different purposes, such as:

- Data authentication (i.e., providing assurance about the authenticity of the signed data),
- Entity authentication (i.e., authenticating the identity of an entity (e.g., an entity that participates in a communication protocol),
- Determining that software or firmware has not been modified (see the integrity test on software and firmware in Section 4.6.1 in FIPS 140-2).

When SP 800-57, Part 1 was written, the difference between these purposes was not fully addressed. While discussing the various uses of digital signatures in the government's identity cards and the timeframes in which currently existing implementations could be updated to be compliant with the NIST-recommended security strengths, and in the design and validation of FIPS 140-2-compliant modules, the different uses of digital signatures was recognized. The guidance provided in SP 800-57, Part 1 needs to be revised to recognize these differences.

NIST is proposing the following for the CMVP to address the aforementioned nuances for using digital signatures (see Table 2).

Table 2: Digital Signatures Transitions

[2] An exception is noted below in Table 2.

Purpose	Digital Signature Process	New Validations*	Already Validated Implementations*
Data Authentication	Signature generation	≥ 80 bits OK through 2010 ≥ 112 bits OK after 2010	< 112 bits disallowed after 2010 ≥ 112 bits OK
	Signature verification	≥ 80 bits is OK	Validated implementations continue to be OK
Entity Authentication	Both signature generation and verification	≥ 80 bits OK through 2013 ≥ 112 bits OK after 2013	< 112 bits disallowed after 2013 ≥ 112 bits OK
Software and firmware integrity test	Signature generation	≥ 80 bits through 2010 ≥ 112 bits after 2010	Validated implementations continue to be OK
	Signature verification	≥ 80 bits is OK	

* Given in bits of security (i.e., security strength)

Digital signatures that are intended to provide data authentication:

- Signature generation: New implementations must generate digital signatures with a security strength that is equal to or greater than 80 bits through December 31, 2010; thereafter, the digital signatures must be generated with a security strength that is equal to or greater than 112 bits. Beginning in 2011, the generation of digital signatures with less than 112 bit of security strength will no longer be considered valid for the FIPS mode on a FIPS 140-2 validation certificate.
- Signature verification: New implementations may verify a signature that provides a security strength that is equal to or greater than 80 bits. Already validated implementations may continue to verify signatures at security strengths that are equal to or greater than 80 bits in the FIPS mode for the foreseeable future.

Digital signatures that are intended to provide only entity authentication: Until December 31, 2013, the minimum security strength required is 80 bits for the generation or verification of digital signatures for entity authentication. Beginning in 2014, only those digital signatures that provide at least 112 bits of security can be used in the FIPS mode. Note that signature verification for entity authentication is performed immediately after signature generation; therefore. there is no requirement to retain a signature for later verification.

Digital signatures that are intended to determine the integrity of software and firmware:

- Signature generation: New implementations must generate digital signatures with a security strength that is equal to or greater than 80 bits through December 31, 2010; thereafter, the digital signatures must be generated with a security strength

that is equal to or greater than 112 bits. Already validated implementations that generate digital signatures with a security strength of 80 bits may continue to be used in the FIPS mode for the foreseeable future.

- Signature verification: New implementations that verify digital signatures may verify a signature that provides a security strength that is equal to or greater than 80 bits. Already validated implementations that verify digital signatures with a security strength of 80 bits or more may continue to be used in the FIPS mode for the foreseeable future.

4 Random Number Generation

Random numbers are used for various purposes, such as the generation of keys, nonces and challenges. Several random number generators (RNGs) have been approved for use by the Federal government. Until relatively recently, FIPS 186-2 was used as an approval vehicle for three of these RNGs: a generator based on the use of the SHA-1 hash algorithm, a generator based on a symmetric block cipher algorithm[3], and a generator that was specified in a standard developed by the American National Standards (ANS) Institute (i.e., in ANS X9.31, and previously in ANS X9.17). In 2007, a new set of RNGs were approved in SP 800-90 that provide higher levels of security than the older RNGs. NIST proposes the following transition schedule (see Table 3).

Table 3: Random Number Generation Transitions

Description	New Validations	Already Validated Implementations
SP 800-90 (HASH, HMAC, CTR, DUAL_EC)	OK	OK
SHA-1 (FIPS 186-2)*	OK through 2010	Disallow after 2015
Sym. Alg. (FIPS 186-2)*	OK through 2010	Disallow after 2015
X9.31 = X9.17*	OK through 2010	Disallow after 2015

* Design or guidance does not support 112-bit security strength

Modules that implement the RNGs specified in SP 800-90 can be validated and used for the foreseeable future in the FIPS mode.

Modules that implement the three older RNGs will only continue to be validated until December 31, 2010. Modules that are validated as conforming to these RNGs can be used in the FIPS mode until December 31, 2015.

5 Key Agreement Using Diffie-Hellman and MQV

Key agreement techniques are used to establish keys between two entities that intend to communicate (e.g., the keys may be used later for encryption or message authentication, or for the generation of additional keys). Two families of key agreement schemes have been approved in SP 800-56A: Diffie-Hellman (DH) and MQV. Each has been defined

[3] DES was specified as the symmetric algorithm for the RNG in FIPS 186-2. Since DES has been withdrawn, two and three-key Triple DES and AES can be used in place of DES as the core engine of the RNG (see http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf).

over two different mathematical structures: finite fields (FF) and elliptic curves (EC). Key agreement includes at least two steps: the use of an appropriate DH or MQV "primitive" to generate a shared secret, and the use of a key derivation function (KDF) to generate one or more keys from the shared secret. SP 800-56A contains approved DH and MQV primitives, and approved KDFs.

Many commonly-used protocols that perform key agreement use DH or MQV. Until recently, no validation testing was performed on implementations of these protocols in cryptographic modules. Validation testing is now available for implementations that claim conformance to SP 800-56A (i.e., conformance to one of the DH or MQV primitives used to generate a shared secret and a KDF specified in SP 800-56A). Other protocols that implement DH and MQV are allowed, but are not tested. In the future, NIST will require that the labs test implementations of the DH or MQV primitives during algorithm validation testing. However, the KDFs that do not comply with the KDFs in SP 800-56A will not be tested.

Protocols are used for a very long time. When new versions of a protocol are designed and implemented, a vendor may need to include a capability to interoperate with the older protocols. Because of this, the older protocols (and the KDFs in particular) will continue to be allowed. However, any new versions of these protocols using DH and MQV key agreement must be designed to conform to SP 800-56A.

NIST is proposing the following set of transition rules (see Table 4).

Table 4: Key Agreement (DH and MQV) Transitions

Scheme	New Validations	Already Validated Implementations
SP 800-56A primitives	OK[1]	OK
Non-tested DH and MQV primitives	OK through 2010	Test by 2014
KDFs:		
SP 800-56A	OK[2]	OK
IKEv2	OK	OK
X9.42	OK	OK
X9.63	OK	OK
IKEv1	OK	OK
SSH	OK	OK
TLS (1.0, 1.1, 1.2)	OK	OK

1 Currently, a primitive is tested only when the KDF complies with SP 800-56A. Plan to test all DH and MQV implementations of the primitives in the future.

2 Now tested.

Implementations that comply fully with SP 800-56A (i.e., both the DH or MQV primitive and the KDF) will be tested and approved for use in the FIPS mode for the foreseeable future.

Other implementations of the DH and MQV primitives (i.e., non-SP 800-56A implementations) that have already been validated must have the primitive(s) tested by

December 31, 2013 in order to use the key agreement scheme in the FIPS mode after 2013.

Implementations of IKEv2 and IKEv1, and the current versions of X9.42, X9.63, SSH, and TLS are allowed in the FIPS mode for the foreseeable future. Their DH and MQV primitives will be tested for conformance to the primitives in SP 800-56A.

6 Key Agreement and Key Transport Using RSA

SP 800-56B specifies the use of RSA for both key agreement and key transport. Like key agreement, key transport is a form of key establishment; however, the method for establishing keys is somewhat different. Refer to SP 800-57, Part 1 and SP 800-56B for definitions. SP 800-56B is currently in draft form, but is expected to be published as complete in the near future. The transition issues associated with the validation of SP 800-56B implementations have not yet been addressed.

Currently, the validation of protocols containing key transport schemes is addressed in the FIPS 140-2 Implementation Guidance, which states that the key transport schemes in SSL v3.1, TLS, PEAP, EAP-FAST and EAP-TLS may be used in the FIPS mode. Note that these schemes are not actually tested during module validation. These key transport schemes use the RSA algorithm. The continued acceptability of the key transport schemes in these protocols will be reassessed when SP 800-56B is completed.

7 Deriving Additional Keys from a Single Key

SP 800-108 specifies key derivation functions that use a key (i.e., a key derivation key) to generate additional keys. The key derivation key could be generated using an approved RNG, obtained using a key agreement or key transport scheme (see Sections 5 and 6) or could be a key that was manually distributed (e.g., by a courier).

This specification allows a large variety of KDFs. At the present time, tests have not been developed to test against this specification. In addition, FIPS 140-2 Implementation Guidance does not include a provision to allow key derivation using the SP 800-108 KDFs. Therefore, a new section of the FIPS 140-2 Implementation Guidance will be developed to allow key derivation using the KDFs specified in SP 800-108.

8 Key Wrapping

Key wrapping is the encryption of a symmetric key by another symmetric key (called a key wrapping key) with integrity protection. Symmetric keys are used with algorithms such as Triple-DES and AES. See SP 800-57 for further information. At the present time, neither a FIPS nor a NIST Recommendation have been developed for key wrapping, although a specification for key wrapping using AES is available at http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf.

The FIPS 140-2 Implementation Guidance (IG) addresses key wrapping as defined above. The IG states that AES or Triple DES may be used to wrap keys using the above referenced specification. If Triple DES is used, then it **shall** be used in exactly the same way that is defined for AES, and both Two-key and the Three-key Triple DES can be used for key wrapping. Note that since Two-key Triple DES will be disallowed after

December 31, 2010 (see Section 2 above), it will also not be allowed for key wrapping after that date.

9 Hash Functions

Five approved hash functions are specified in FIPS 180-3. The security strength for a hash function is dependent on its design and use, and is provided in SP 800-57, Part 1. Discussions about these different uses are provided in SP 800-107.

NIST is proposing the following transition rules for hash functions (see Table 4).

Table 4: Hash Function Transitions

Hash Function	New Validations	Already Validated Implementations
SHA-1	OK for all hash function applications through December 31, 2010	Digital signatures: see Table 2 Hash-only: Disallow after 2010 OK for all other applications
SHA-224	OK for all hash function applications	OK for all hash function applications
SHA-256		
SHA-384		
SHA-512		

The five hash functions can be validated and used for all applications through December 31, 2010. In the case of implementations that have already been validated:

- When SHA-1 is used in the generation of digital signatures, see Table 2 for the continued use of the implementation.
- When SHA-1 is used for hash-only applications, the use of already-validated implementations is disallowed after 2010 in the FIPS mode.
- For all other SHA-1 applications and for all applications using the other hash functions, the implementations that have previously been validated may continue to be used in the FIPS mode.

10 References

All references documents are available at http://csrc.nist.gov/publications/.

FIPS 140-2 Security Requirements for Cryptographic Modules, with Change Notices, December 2002.

FIPS 180-3 Secure Hash Standard (SHS), October 2008.

FIPS 185 Escrowed Encryption Standard, Feb 1994.

FIPS 197 Advanced Encryption Standard, November 2001.

SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007.

SP 800-56B Recommendation for Pair-Wise Key Establishment Using Integer Factorization, DRAFT, December 2008.

SP 800-57 Part 1, Recommendation for Key Management: General, March 2007.

SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2008.

SP 800-107 Recommendation for Applications Using Approved Hash Algorithms, February 2009.

SP 800-108 Recommendation for Key Derivation Using Pseudorandom Functions, November 2008.

Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

FIPS 140-2 Annex A, *Approved Security Functions*, Draft June 2009

FIPS 140-2 Annex C, *Approved Random Number Generators,* Draft October 2007

FIPS 140-2 Annex D, *Approved Key Establishment Techniques,* Draft January 2008

Available at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.