DRAFT NIST Special Publication 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Elaine Barker and Allen Roginsky

Computer Security Division
Information Technology Laboratory

C O M P U T E R S E C U R I T Y

January 2010

U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Director

Abstract

At the start of the 21st century, the National Institute of Standards and Technology (NIST) began the task of providing cryptographic key management guidance, which includes defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. NIST Special Publication (SP) 800-57, Part 1 was the first document produced in this effort, and includes a general approach for transitioning from one algorithm or key length to another. This Recommendation (SP 800-131) provides more specific guidance for transitions to stronger cryptographic keys and more robust algorithms.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This Recommendation has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

Table of Contents

The Transitioning of Cryptographic Algorithms and Key Sizes

1 Introduction

1.1 Background and Purpose

At the beginning of the 21st century, the National Institute of Standards and Technology (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. The general approach for transitioning from one algorithm or key length to another is addressed in Part 1 of SP 800-57.

This Recommendation is intended to bring the transitions associated with the use of cryptography to the attention of the Federal government agencies and the public, since the Federal agencies and their contractors may need to acquire new cryptographic devices to comply with the new algorithm and key strength requirements discussed in this document.

The Recommendation is written from the point of view of NIST's validation program (see Section 1.2.1), and will be used to develop validation guidance documents.

1.2 Useful Terms for Understanding this Recommendation

1.2.1 Testing and Validation

The means for enforcing the algorithm and strength requirements for the Federal government is by using Cryptographic and Security Testing (CST), which is conducted under the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). The CAVP is responsible for validating cryptographic algorithm implementations for conformance to their associated Federal Information Processing Standards (FIPS) or NIST Recommendations (published as NIST Special Publications (SP)). The CMVP validates cryptographic modules for conformance to FIPS 140-2. To be validated, each module requires at least one security function (e.g., a cryptographic algorithm) that has been approved for Federal government use by the CAVP. Testing is conducted by accredited CST laboratories, and test reports are submitted to NIST and the Communications Security Establishment Canada (CSEC), who serve as the *validation authorities*.

1.2.2 FIPS Mode

The CMVP has defined two classes of modes for cryptographic module operation: the *FIPS mode* and the *non-FIPS mode*. In the FIPS mode, only *FIPS-approved* security methods are allowed during operation, where the term FIPS-approved means that the

security method (i.e., the cryptographic algorithm, or scheme) is approved in a FIPS or NIST Recommendation (see Section 1.2.3). When a module is in the FIPS mode, a non-FIPS-approved security method **shall not** be used in lieu of a FIPS-approved method (For example, if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used.).

1.2.3 Approved vs. Allowed

A FIPS or NIST Recommendation is used by the Federal government to *approve* cryptographic algorithms and protocols. Non-FIPS-approved algorithms or protocols may be *allowed* in FIPS-mode; an algorithm or protocol is indicated as allowed by means of the FIPS 140-2 Implementation Guidance (IG) document.

1.2.4 New Validations and Already Validated Implementations

This Recommendation contains several tables addressing the implementation of cryptographic algorithms and modules. This includes both *New Implementations* and *Already- Validated Implementations*:

- *New Implementations* are the cryptographic algorithms or modules that are being tested by an accredited CST laboratory for which the test report has been submitted to CMVP under FIPS 140-2 Implementation Guidance G.8, Scenarios 3 and 5. The date in the table refers to the date of the lab's submission of the test report to the validation authorities.
- *Already-Validated Implementations* are algorithm or module implementations that already have valid CMVP validation certificates. The CMVP and CAVP will review these implementations and the underlying algorithm validations for the purpose of their compliance with the new security requirements as stated in this Recommendation. The CAVP will review the algorithm validations to determine if complete validations or parts of the validation are no longer NIST-approved. The features that no longer satisfy the new security requirements will be removed from the algorithm validation web pages. (However, they will continue to be available for historical purposes.) The CMVP may take the appropriate actions, which may include the modification or the revocation of the module's or algorithm's validation certificate. Due to the complexity of the available information at the module level, the CMVP actions are as yet undecided.

*For example, the "Approved throug*h 2010 only" entry in Table 1 (see Section 2) for New Validations and the two-key Triple DES algorithm means that if a lab submitted a test report that included the use of two-key Triple DES to encrypt sensitive data by the end of 2010, then this would be consistent with the NIST transition policy as explained in column 2 of Table. However, the lab and the vendor need to keep in mind, that according to an entry on the same line in the last column, the validation certificates will be reviewed and modified to disallow the use of the two-key Triple DES after 2010. Any certificate issued after December 31, 2010 will not include two-key Triple DES as an approved algorithm. If this is the module's only approved security function, then the CMVP certificate will not be issued and, if already issued on that date the certificate may be revoked upon review.

Note that the text in the *New Implementations* and the *Already-Validated Implementations* columns are often the same or very similar; differences between the two columns will be in italics.

1.2.5 Security Strengths

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

The security strength of an algorithm with a particular key size 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, and provided in Appendix A.1 of this Recommendation (i.e., SP 800-131) for easy reference. For example, RSA using a 1024-bit modulus has a security strength of 80 bits; note that for RSA, the length of the modulus is commonly referred to as the length or size of the key.

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 (e.g., a person or an agency). 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 Appendix A.3. This may require a transition to a new set of minimum key sizes, depending upon the algorithm. For practical purposes, it may be necessary to extend the use of some algorithms, key sizes and protocols to allow a non-interruptive transition as agencies procure and replace legacy solutions.

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 lengths, 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, whereas three-key Triple DES is assessed at a security strength of 112 bits (see Appendix A.1).
- 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 lengths: 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 (see Appendix A.1).

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	Approved through 2010 only	Approved through 2010 only
Three-key Triple DES	Approved	Approved *beyond 2010*
SKIPJACK	Approved through 2010 only	Approved through 2010 only
AES-128	Approved	Approved *beyond 2010*
AES-192	Approved	Approved *beyond 2010*
AES-256	Approved	Approved *beyond 2010*

In the case of two-key Triple DES and SKIPJACK, an algorithm certificate will not be issued for a new implementation after 2010. For already-validated implementations, the use of two-key Triple DES and SKIPJACK will no longer be approved after 2010.

For the other algorithms listed in Table 1, algorithm certificates will continue to be issued for implementations that pass validation tests without the 2010 restriction, and already-validated implementations will be honored beyond 2010.

3 Digital Signatures

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

FIPS 186-3 specifies three approved 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. Since FIPS 186-3 only recently became official, a period of time must be defined for transitioning between FIPS 186-2 and 186-3.

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

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 for the *generation* of digital signatures after 2010, but those that provide only 80 bits of security will not. However, the *verification* of digital signatures that provided 80 bits of security when generated will continue to be approved after 2010; therefore, an implementation that verifies digital signatures at a security strength of 80 bits or more will continue to be approved, providing that it **does not** *generate* digital signatures at less than 112 bits of security in FIPS mode.

For the purposes of determining the security strength of digital signatures, the security strength of the cryptographic hash functions is also a factor (see Section 9). The security strengths of the asymmetric algorithms and the key lengths used in the signature generation can be found in Appendix A.1.

Note that the invalidation of the algorithm certificates will affect all currently-validated FIPS 186-2 DSA implementations, as well as those implementations of RSA and ECDSA that only use SHA-1 for digital signature generation.

3.2 Security Strengths for Digital Signature Keys

Table 2 depicts the time table for transitioning from digital signatures providing 80 bits of security to those providing at least 112 bits of security strength (also see Appendix A.3 for the recommended algorithm-use time frames).

Table 2: Digital Signatures Security Strength Transitions

Digital Signature Process	New Validations	Already Validated Implementations*
Signature Generation	≥ 80 and < 112 bits of security approved through 2010 only ≥ 112 bits of security approved	≥80 and < 112 bits of security approved through 2010 only ≥ 112 bits of security approved *beyond 2010*
Signature Verification	≥ 80 bits of security approved	≥ 80 bits of security approved *beyond 2010*

4 Random Number Generation

Random numbers are used for various purposes, such as the generation of keys, nonces and authentication challenges. Several random number generators (RNGs) have been approved for use by the Federal government. Until relatively recently, FIPS 186-2 was the approval vehicle for RNGs, specifying RNGs and approving the RNGs in American National Standard (ANS) X9.31-1998 and ANS X9.62-1998.

In 2007, a new set of RNGs were approved in SP 800-90 that provide higher levels of security than the previously-approved RNGs. In addition, SP 800-90 contains more comprehensive guidance on RNG use. The following transition schedule is proposed (see Table 3). Note that a revision of ANS X9.62 (ANS X9.62-2005) contains the HMAC RNG specified in SP 800-90.

Table 3: Random Number Generation Transitions

Description	New Validations	Already Validated Implementations
RNGs specified in SP 800-90 (HASH, HMAC, CTR, DUAL_EC) and ANS X9.62-2005 (HMAC)	Approved	Approved *beyond 2010*
RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998	Approved through 2010 only	Approved through *2015 only*[a]

a While some uses of two-key Triple DES will no longer be approved after 2010 (e.g., see Section 2), implementations of the RNG in ANS X9.31 that use two-key TDES will continue to be approved through 2015.

As this table indicates, all RNGs that are not compliant with SP 800-90 will not be approved after 2015 and will need to be replaced.

5 Key Agreement Using Diffie-Hellman and MQV

Key agreement is a technique that is used to establish symmetric keys between two entities that intend to communicate, whereby both parties contribute information to the key agreement process. Two families of key agreement schemes have been approved in SP 800-56A: Diffie-Hellman (DH) and MQV. Each has been defined over two different mathematical structures: finite fields and elliptic curves. Key agreement includes 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 for key agreement (see Section 5.1 for a discussion of this case). Several non-NIST protocol standards specify one or more of the DH or MQV primitives specified in SP 800-56A, but use different KDFs (see Section 5.2).

The length of the keys and other parameters used during a DH or MQV shared secret computation is also a transition concern. Guidance about the security strengths and approved key lengths and other parameters is provided in Appendices A.1, A.4 and A.5.

5.1 Key Agreement Schemes Specified in SP 800-56A

Testing is available for the key schemes specified in SP 800-56A; this includes testing the generation of a shared secret using a DH or MQV primitive and a KDF as specified therein. Table 4 contains the proposed transition strategy. This table identifies the acceptability of parameter sets (which include the key lengths) as specified in Appendices A.4 and A.5.

Table 4: SP 800-56A Key Agreement (DH and MQV)

Scheme	New Validations	Already Validated Implementations
SP 800-56A primitives and KDFs using finite fields	Parameter set FA approved through 2010 Parameter sets FB and FC approved	Parameter set FA approved through 2010 *only* Parameter sets FB and FC approved *beyond 2010*
SP 800-56A primitives and KDFs using elliptic curves	Parameter set EA approved through 2010 Parameter sets EB–EE approved	Parameter set EA approved through 2010 *only* Parameter sets EB–EE approved *beyond 2010*

5.2 Key Agreement in Protocols that are Not Fully Compliant with SP 800-56A

Many commonly-used protocols use DH or MQV for key agreement. Some of these protocols use a DH or MQV primitive that is specified in SP 800-56A, but may differ in the KDF that is used to generate the keying material; other protocols may use a different primitive than the primitives specified in SP 800-56A. In many cases, the use of the combination of the primitive and the KDF used in a protocol has been deemed as "allowed" and included in a list of such protocols in IG D.2 of FIPS 140-2. At the present time, these implementations are not explicitly tested by the CAVP. However, at some time in the future, the CST labs will test implementations of the DH or MQV computation of the shared secret during algorithm validation testing for compliance with the SP 800-56A DH or MQV primitives; for these protocols, the KDFs may not be tested. In this case, cryptographic modules that contain currently untested DH or MQV primitives for which validation certificates have been issued must have the DH or MQV primitive(s) tested for compliance with the SP 800-56A primitives by December 31, 2013 in order to maintain the inclusion of DH or MQV in the module's validation certificate.

Protocols are used for a very long time. When new versions of a protocol are designed and implemented, a module may need to include a capability to interoperate with both the new and existing protocols. Because of this, the KDFs in those existing protocols will continue to be allowed. NIST will encourage the adoption of KDFs that are approved for key agreement, such as those specified in SP 800-56A, for new and revised protocols.

Table 5 contains the proposed set of transition rules for validation. For this table, only the top two rows of the tables in Appendices A.4 and A.5 will apply (i.e., the lengths of p and q in Appendix A.4, and the length of the private key and the cofactor in Appendix A.5); the remaining three rows of the tables in Appendices A.4 and A.5 are specific to the KDFs and key confirmation of SP 800-56A and are not applicable for this section of the this Recommendation (i.e., SP 800-131).

Table 5: Key Agreement (DH and MQV) Transitions for Module Implementations Not Fully Compliant with SP 800-56A

Scheme	New Validations[a]	Already Validated Implementations[a]
DH and MQV primitives using finite fields	Any[b] DH or MQV implementation with $1024 \leq \|p\| < 2048$ bits, and $160 \leq \|q\| < 224$ bits allowed[c] through 2010 Any[b] untested DH or MQV implementation with $\|p\| \geq 2048$ bits, and $\|q\| \geq 224$ bits allowed[c] through 2013 only Approved if the DH or MQV primitive is tested for compliance with SP 800-56A	Any[b] DH or MQV implementation with $1024 \leq \|p\| < 2048$ bits, and $160 \leq \|q\| < 224$ bits allowed[c] through 2010 *only* Any[b] untested DH or MQV implementation with $\|p\| \geq 2048$ bits, and $\|q\| \geq 224$ bits allowed[c] through 2013 only Approved if the DH or MQV primitive is tested for compliance with SP 800-56A
DH and MQV primitives using elliptic curves	Any[b] DH or MQV implementation with the $160 \leq \|n\| \leq 223$ bits allowed[c] through 2010 only Any[b] untested DH or MQV implementation with $\|n\| \geq 224$ bits allowed[c] through 2013 only Approved if the DH or MQV primitive is tested for compliance with SP 800-56A	Any[b] DH or MQV implementation with the $160 \leq \|n\| \leq 223$ bits allowed[c] through 2010 only Any[b] untested DH or MQV implementation with $\|n\| \geq 224$ bits allowed[c] through 2013 only Approved *beyond 2013* if the DH or MQV primitive is tested for compliance with SP 800-56A
KDFs in protocols listed in IG D.2	Allowed	Allowed
KDFs not in SP 800-56A nor explicitly listed in IG D.2	Allowed through 2010	Allowed through 2010 *only*

a $|p|$, $|q|$ and $|n|$ are used to denote the bit length of p, q and n, respectively.
b The DH or MQV primitives may or may not be specified in SP 800-56A.
c The DH or MQV primitive is allowed without testing or vendor affirmation of compliance with SP 800-56A in accordance with IG D.2.

6 Key Agreement and Key Transport Using RSA

SP 800-56B specifies the use of RSA for both key agreement and key transport. Key agreement is a technique in which both parties contribute information to the key

agreement process. Key transport is a key establishment technique in which only one party determines the key.

Currently, the validation of protocols containing key transport schemes are addressed in IG D.2; note that in IG D.2, key transport is often referred to as key wrapping. The IG states that the key transport schemes in SSL v3.1, TLS, DTLS, PEAP-TLS, EAP-FAST and EAP-TLS are allowed in the FIPS mode. Note that these schemes using the RSA algorithm are not actually tested during module validation.

Guidance on approved key lengths for RSA is provided in Appendix A.1. Table 6 proposes a transition schedule.

Table 6: RSA-based Key Agreement and Key Transport Key Size Transitions

Scheme	New Validations	Already Validated Implementations
Key agreement[a]	n = 1024 bits approved through 2010 only n = 2048 approved	n = 1024 bits allowed through 2010 only n = 2048 bits approved *beyond 2010*
Key transport[b]	Any[c] scheme with $1024 \leq n < 2048$ allowed through 2010 only Approved through 2010 only if the scheme is tested for compliance with SP 800-56B with n = 1024 Any[c] untested scheme with $n \geq 2048$ allowed through 2013 only Approved if the scheme is tested for compliance with SP 800-56B with n = 2048	Any[c] scheme with $1024 \leq n < 2048$ allowed through 2010 only Approved through 2010 only if the scheme is tested for compliance with SP 800-56B with n = 1024 Any[c] untested scheme with $n \geq 2048$ allowed through 2013 only Approved *beyond 2013* if the scheme is tested for compliance with SP 800-56B with n = 2048

a Key agreement using RSA is only specified in SP 800-56B, where n is specified as either 1024 or 2048 bits in length.

b RSA key transport schemes existed prior to the development of SP 800-56B, and therefore, need to be accommodated during a transition period.

c The RSA key transport schemes may or may not be specified in SP 800-56B.

7 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 Part 1 of SP 800-57 for further information. At the present time, neither a FIPS nor a NIST Recommendation have specified key wrapping

algorithms, although an informal specification for key wrapping using AES is available at http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf.

IG D.2 addresses key wrapping as defined in the AES key wrapping specification referenced in the previous paragraph. The IG states that AES or Triple DES may be used to wrap keys using the specification referenced in the previous paragraph. If Triple DES is used, then it is used in exactly the same way that is defined for AES, and both two-key and 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 be disallowed for key wrapping after that date.

Because the absence of an official NIST document on the use of symmetric key algorithms for key wrapping, the following table will only address the transition of key lengths. The details of the use of symmetric key algorithms for key wrapping and future testing requirements will be addressed at a later time.

Table 7: Symmetric Key Wrapping Key Size Transitions

Algorithm	New Validations	Already Validated Implementations
Two-key Triple DES	Allowed through 2010 only	Allowed through 2010 only
GDOI protocol (described in IETF RFC 3547)[a]	Allowed through 2010 only	Allowed through 2010 only
AES and Three-key Triple DES	Allowed	Allowed

a The GDOI protocol is listed as an allowed protocol in IG D.2.

8 Deriving Additional Keys from a Cryptographic Key

SP 800-108 specifies key derivation functions that use a cryptographic key (called a key derivation key) to generate additional keys. The key derivation key could be generated using an approved RNG (see IG 7.8), obtained using a key agreement or key transport scheme (see Sections 5 and 6 of this Recommendation, i.e., SP 800-131), obtained using a key wrapping algorithm (see Section 7) or could be a key that was manually or electronically entered into a cryptographic module (e.g., following manual distribution). FIPS 140-2 IG 7.10 contains the rules for using the SP 800-108 key derivation functions in the FIPS mode.

The following table will only address the transition of key lengths for key derivation. The details of the future testing requirements for key derivation will be addressed at a later time.

Table 8: Key Size Transitions for a Key Derivation Function

Algorithm	New Validations	Already Validated Implementations
HMAC-based KDF	Approved	Approved
CMAC-based KDF	Two-key TDES-based KDF approved through 2010 only AES- and Three-key Triple DES-based KDFs approved	Two-key TDES-based KDF approved through 2010 only AES- and Three-key Triple DES-based KDFs approved *beyond 2010*

9 Hash Functions

Five approved hash functions are specified in FIPS 180-3. The security strengths for hash functions are dependent on their use, and are provided in Appendix A.2. Additional discussions about the different uses of hash functions are provided in SP 800-107.

Note that, while there have been attacks reported on SHA-1, this Recommendation (i.e., SP 800-131) will consider its strength to be 80 bits for the purpose of discussion only.

NIST is proposing the following transition rules for hash functions (see Table 9).

Table 9: Hash Function Transitions

Hash Function	New Validations	Already Validated Implementations
SHA-1	Approved for digital signatures generation through 2010 only Approved for all non-digital signature generation applications*	Approved for digital signatures generation through 2010 only Approved for all non-digital signature generation applications[a] *beyond 2010*
SHA-224	Approved for all hash function applications	Approved for all hash function applications *beyond 2010*
SHA-256		
SHA-384		
SHA-512		

a Includes digital signature verification, HMACs, KDFs, RNGs, and the approved integrity technique specified in Section 4.6.1 of FIPS 140-2.

10 Message Authentication Codes (MACs)

Two types of message authentication mechanisms using symmetric keys have been approved for use: those based on hash functions, and those based on block-cipher algorithms. FIPS 198-1 specifies a keyed-hash message authentication code (HMAC) that uses a hash function; SP 800-107 provides additional guidance on the uses of HMAC. SP 800-38B specifies a MAC (i.e., CMAC) that uses either AES or Triple DES. The

authenticated encryption modes in SP 800-38 are not discussed in SP 800-131 because they use only AES, for which there are no transition issues.

Table 10: Message Authentication Code Transitions

MAC Algorithm	New Validations	Already Validated Implementations
HMAC	Any approved hash function Key lengths ≥ 80 bits and < 112 bits approved through 2010 only Key lengths ≥ 112 bits approved	Any approved hash function Key lengths ≥ 80 bits and < 112 bits approved through 2010 only Key lengths ≥ 112 bits approved *beyond 2010*
CMAC	Two-key Triple DES approved through 2010 only AES and Three-key Triple DES approved	Two-key Triple DES approved through 2010 only AES and Three-key Triple DES approved *beyond 2010*

Appendix A:

A.1 Comparable Algorithm Key Size Strengths

This table is Table 2 in Part 1 of SP 800-57.

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA[1]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

A.2 Hash Function Security Strengths for Cryptographic Applications

This table is Table 3 from Part 1 of SP 800-57.

Bits of Security	Digital Signatures and hash-only applications	HMAC	Key Derivation Functions[2]	Random Number Generation[3]
80	SHA-1[4], SHA-224, SHA-256,	SHA-1, SHA-224, SHA-	SHA-1, SHA-224,	SHA-1, SHA-224, SHA-

[1] The assessment of at least 80-bits of security for 2TDEA is based on the assumption that an attacker has at most 2^{40} matched plaintext and ciphertext blocks (see [ANSX9.52], Annex B).

[2] The security strength for key derivation assumes that the shared secret contains sufficient entropy to support the desired security strength.

[3] The security strength assumes that the random number generator has been provided with adequate entropy to support the desired security strength.

Bits of Security	Digital Signatures and hash-only applications	HMAC	Key Derivation Functions[2]	Random Number Generation[3]
	SHA-384, SHA-512	256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512	256, SHA-384, SHA-512
112	SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
128	SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
192	SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512	SHA-224, SHA-256, SHA-384, SHA-512
256	SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512

A.3 Recommended Algorithms and Minimum Key Sizes

This table is Table 4 in Part 1 of SP 800-57.

[4] SHA-1 has recently been demonstrated to provide less than 80 bits of security for digital signatures; at the publication of this Recommendation, the security strength against collisions is assessed at 69 bits. The use of SHA-1 is not recommended for the generation of digital signatures in new systems; new systems should use one of the larger hash functions. For the present time, SHA-1 is included here to reflect it's widespread use in existing systems, for which the reduced security strength may not be of great concern when only 80-bits of security are required.

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[5] 3TDEA AES-128 AES-192 AES-256	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256

A.4 FFC Parameter Size Sets

This is Table 1 from SP 800-56A.

FFC Parameter Set Name	FA	FB	FC
Bit length of field order p (i.e., $\lceil \log_2 p \rceil$)	1024	2048	2048[6]
Bit length of subgroup order q (i.e., $\lceil \log_2 q \rceil$)	160	224	256
Minimum bit length of the hash function output	160	224	256
Minimum MAC key size (for use in key confirmation)	80	112	128
Minimum *MacLen* (for use in key confirmation)	80	112	128

[5] The guarantee of at least 80-bits of security for 2TDEA is based on the assumption that an attacker has at most 2^{40} matched plaintext and ciphertext blocks (see [ANSX9.52], Annex B).

[6] Parameter size set FC is included with the same field order length as set FB to allow finite field applications with a 2048-bit field order to have the option of increasing the private key size to 256 bits without having to increase the field order (a more substantial change). FC is not intended to provide more security than FB.

A.5 ECC Parameter Size Sets

This is Table 2 from SP 800-56A.

ECC Parameter Set Name	EA	EB	EC	ED	EE
Bit length of ECC subgroup order n (i.e., $\lceil \log_2 n \rceil$)	160-223	224-255	256-383	384-511	512+
Maximum bit length of ECC cofactor h	10	14	16	24	32
Minimum bit length of the hash function output	160	224	256	384	512
Minimum MAC key size (for use in key confirmation)	80	112	128	192	256
Minimum *MacLen* (for use in key confirmation)	80	112	128	192	256

Appendix B: References

All referenced documents are available at http://csrc.nist.gov/publications/, except for FIPS 140-2 Annex A and the FIPS 140-2 Implementation Guidance, which are available at http://csrc.nist.gov/groups/STM/cmvp/standards.html#02.

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

FIPS 140-2 Annex A, Approved Security Functions, Draft October 2009.

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

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

FIPS 185 Escrowed Encryption Standard, Feb 1994.

FIPS 197 Advanced Encryption Standard, November 2001.

FIPS 198-1 Keyed-Hash Message Authentication Code (HMAC), July 2008.

SP 800-38B CMAC Mode of Authentication, May 2005.

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.