

Draft NIST Special Publication 800-131A
Revision 2

**Transitioning the Use of
Cryptographic Algorithms and
Key Lengths**

Elaine Barker
Allen Roginsky

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

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce

Draft NIST Special Publication 800-131A
Revision 2

Transitioning the Use of Cryptographic Algorithms and Key Lengths

Elaine Barker
Allen Roginsky
*Computer Security Division
Information Technology Laboratory*

July 2018



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-131A Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-131A Rev. 2, 29 pages (July 2018)
CODEN: NSPUE2

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

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Public comment period: *July 19, 2018 through September 7, 2018*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: CryptoTransitions@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA)

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

The National Institute of Standards and Technology (NIST) provides cryptographic key management guidance for 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](#) includes a general approach for transitioning from one algorithm or key length to another. This Recommendation (SP 800-131A) provides more specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms.

Keywords

cryptographic algorithm; digital signatures; encryption; hash function; key agreement; key derivation functions; key management; key transport; key wrapping; message authentication codes; post-quantum algorithms; random number generation; security strength; transition.

Acknowledgments

The authors would like to specifically acknowledge the assistance of the following NIST employees in developing this revision of SP 800-131A: Lily Chen, Morris Dworkin, Sharon Keller, Kerry McKay, Andrew Regenscheid and Apostol Vassilev.

Notes to Reviewers

1. One of the primary revisions to this document is providing a plan for retiring TDEA. Two-key TDEA is now disallowed for applying cryptographic protection (e.g, encryption, but allowed for processing already-protected information. In accordance with NIST's announcement regarding the continued use of TDEA (see the [TDEA Announcement](#)), this document is proposing a schedule for sunseting the use of TDEA for applying cryptographic protection (e.g., encryption, MAC generation, etc.). However, there may be applications for which the continued use of TDEA might be appropriate; NIST will provide guidance on this at a later time. The use of TDEA for processing already-protected information will continue to be allowed for legacy use, with the caveat that some risk is associated with doing so.

NIST requests comments on this schedule and an identification of any applications for which the continued use of TDEA would be appropriate, along with rationale for considering this use to be secure.

2. A revision of SP 800-57, Part 1 is planned that will be consistent with the changes in SP 800-131A.
3. The elliptic curves currently defined in FIPS 186-4, Digital Signature Standard (DSS), will be moved to a new publication, SP 800-186, that will soon be available for public comment. Additional elliptic curves will also be included in that SP 800-186. SP 800-131A refers to this new document.
4. A revision of FIPS 186 (FIPS 186-5) will soon be available for public comment. This revision will include EdDSA. SP 800-131A takes this into account.

Table of Contents

1	Introduction.....	1
1.1	Background and Purpose	1
1.2	Useful Terms for Understanding this Recommendation	2
1.2.1	Security Strengths	2
1.2.2	General Definitions.....	3
1.2.3	Definition of Status Approval Terms.....	3
2	Encryption and Decryption Using Block Cipher Algorithms	4
3	Digital Signatures	6
4	Random Bit Generation	9
5	Key Agreement Using Diffie-Hellman and MQV	10
6	Key Agreement and Key Transport Using RSA	12
7	Key Wrapping	14
8	Deriving Additional Keys from a Cryptographic Key	15
9	Hash Functions.....	16
10	Message Authentication Codes (MACs).....	17
	Appendix A: References	20
	Appendix B: Change History	22

1 Introduction

2 1.1 Background and Purpose

3 At the beginning of the 21st century, the National Institute of Standards and Technology
4 (NIST) began the task of providing cryptographic key management guidance. This
5 guidance was based on the lessons learned over many years of dealing with key
6 management issues and is intended to 1) encourage the specification and implementation
7 of appropriate key management procedures, 2) use algorithms that adequately protect
8 sensitive information, and 3) plan for possible changes in the use of cryptographic
9 algorithms, including any migration to different algorithms. The third item addresses not
10 only the possibility of new cryptanalysis, but also the increasing power of classical
11 computing technology and the potential emergence of quantum computers.

12 General key-management guidance, including the general approach for transitioning from
13 one algorithm or key length to another, is addressed in Part 1 of Special Publication ([SP](#)
14 [800-57](#)¹).

15 This document (SP 800-131A) is intended to provide more detail about the transitions
16 associated with the use of cryptography by federal government agencies for the protection
17 of sensitive, but unclassified information. The document addresses the use of algorithms
18 and key lengths specified in Federal Information Processing Standards (FIPS) and NIST
19 Special Publications (SPs).

20 NIST recognizes that large-scale quantum computers, when available, will threaten the
21 security of NIST-approved public key algorithms. In particular, NIST-approved digital
22 signature schemes, key agreement using Diffie-Hellman and MQV, and key agreement and
23 key transport using RSA may need to be replaced with secure quantum-resistant (or “post-
24 quantum”) counterparts. At the time that this SP 800-131A revision was published, NIST
25 was undergoing a process to select post-quantum cryptographic algorithms for
26 standardization. This process is a multi-year project; when these new standards are
27 available, this Recommendation will be updated with the guidance for the transition to
28 post-quantum cryptographic standards. NIST encourages implementers to plan for
29 cryptographic agility to facilitate transitions to quantum-resistant algorithms where needed
30 in the future. Information on the post-quantum project is available at
31 <https://csrc.nist.gov/projects/post-quantum-cryptography>.

32 SP 800-131A was originally published in January 2011 and revised in 2015. This revision
33 updates the transition guidance provided in the 2015 version; these changes are listed in
34 [Appendix B](#). The most significant difference is the schedule for retiring the Triple Data
35 Encryption Algorithm (TDEA), the inclusion of safe-prime groups for finite field Diffie-
36 Hellman and MQV, and the inclusion of KMAC for MAC generation.

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

37 1.2 Useful Terms for Understanding this Recommendation

38 1.2.1 Security Strengths

39 Some of the guidance provided in [SP 800-57](#) includes the definition of an estimated
40 maximum security strength (hereafter shortened to just "security strength"), the association
41 of the algorithms and key lengths with these security strengths, and a projection of the time
42 frames during which the algorithms and key lengths could be expected to provide adequate
43 security. Note that the length of the cryptographic keys is an integral part of these
44 determinations.

45 In [SP 800-57](#), the security strength provided by an algorithm with a particular key length²
46 is measured in bits and is a measure of the difficulty of subverting the cryptographic
47 protection that is provided by the algorithm and key. An estimated security strength for
48 each algorithm is provided in SP 800-57. This is the security strength that an algorithm
49 with a particular key length can provide, given that the key used with that algorithm has
50 sufficient entropy³.

51 Note: The term "security strength" refers to the classical security strength – a measure
52 of the difficulty of subverting the cryptographic protection (e.g., discovering the key)
53 using classical computers. When post-quantum cryptography is introduced in NIST
54 standards, quantum security strength, i.e. the difficulty of subverting the protection
55 using quantum computers, will be defined.

56 The appropriate (classical) security strength to be used to protect data depends on the
57 sensitivity of the data being protected and needs to be determined by the owner of that data
58 (e.g., a person or an organization). For the federal government, a security strength of at
59 least 112 bits is required at this time for applying cryptographic protection (e.g., for
60 encrypting or signing data). Note that prior to 2014, a security strength of at least 80 bits
61 was required for applying these protections, and the transitions in this document reflect this
62 change to a required security strength of at least 112 bits. However, a large quantity of data
63 was protected at the 80-bit security strength and may need to be processed (e.g., decrypted).
64 The processing of this already-protected data at the lower security strength is allowed, but
65 a certain amount of risk must be accepted⁴.

66 Specific key lengths are provided in [FIPS 186](#)⁵ for digital signatures, in [SP 800-56A](#)⁶ for
67 finite field Diffie-Hellman (DH) and MQV key agreement, and in [SP 800-56B](#)⁷ for RSA

² The term "key size" is commonly used in other documents.

³ Entropy is a measure of the amount of disorder, randomness or variability in a closed system.

⁴ For example, if the data was encrypted and transmitted over public networks when the algorithm was still considered secure, it may have been captured (by an adversary) at that time and later decrypted by that adversary when the algorithm was no longer considered secure; thus, the confidentiality of the data would no longer be assured.

⁵ FIPS 186, *Digital Signature Standard (DSS)*.

⁶ SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*.

⁷ SP 800-56B, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization*.

68 key agreement and key transport. [SP 800-186](#)⁸ provides elliptic curves for elliptic curve
69 digital signatures and elliptic curve DH and MQV key agreement; the elliptic curve
70 specifications provide the key lengths associated with each curve. These key lengths are
71 strongly recommended for interoperability, and their estimated security strengths are
72 provided in [SP 800-57](#). However, other key lengths are commonly used. The security
73 strengths associated with these key lengths may be determined using the formula provided
74 in Section 7.5 of the [FIPS 140 Implementation Guideline](#).⁹

75 1.2.2 General Definitions

Apply cryptographic protection	Depending on the algorithm, to encrypt or sign data, generate a hash function or Message Authentication Code (MAC), or establish keys (including wrapping and deriving keys).
Approval status	Used to designate usage by the U.S. Federal Government.
Approved	FIPS-approved or NIST-Recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation and specified either (a) in an appendix to the FIPS or NIST Recommendation, or (b) in a document referenced by the FIPS or NIST Recommendation.
len (<i>x</i>)	The bit length of <i>x</i> .
Shall	A requirement for federal government use. Note that shall may be coupled with not to become shall not .

76 1.2.3 Definition of Status Approval Terms

77 The terms “**acceptable**”, “**deprecated**”, “**legacy use**” and “**disallowed**” are used
78 throughout this Recommendation to indicate the approval status of an algorithm. The
79 approval status for an algorithm often will also depend on the length of its key, any domain
80 parameters and the mode or manner in which it is used.

- 81 • **Acceptable** is used to mean that the algorithm and key length in a FIPS or SP is
82 safe to use; no security risk is currently known when used in accordance with any
83 associated guidance. The [FIPS 140 Implementation Guideline](#) may indicate
84 additional algorithms that are acceptable for use, but not specified in a FIPS or
85 NIST Recommendation.
- 86 • **Deprecated** means that the algorithm and key length may be used, but the user
87 must accept some security risk. The term is used when discussing the key lengths
88 or algorithms that may be used to apply cryptographic protection.

⁸ SP 800-186, *Recommendation for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*. Until SP 800-186 is published, approved elliptic curves are specified in FIPS 186-4.

⁹ FIPS 140 Implementation Guide: *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*.

89 • **Disallowed** means that the algorithm or key length is no longer allowed for
90 applying cryptographic protection.

91 • **Legacy use** means that the algorithm or key length may be used only to process
92 already protected information (e.g., to decrypt ciphertext data or to verify a digital
93 signature).

94 The use of algorithms and key lengths for which the terms **deprecated** and **legacy use** are
95 listed require that the user must accept some risk¹⁰ that increases over time. If a user
96 determines that the risk is unacceptable, then the algorithm or key length is considered
97 disallowed from the perspective of that user. It is the responsibility of the user or the user's
98 organization to determine the level of risk that can be tolerated for an application and its
99 associated data and to define any methods for mitigating those risks.

100 Other cryptographic terms used in this document are defined in the documents listed in
101 [Appendix A](#).

102 **2 Encryption and Decryption Using Block Cipher Algorithms**

103 Encryption is a cryptographic operation that is used to provide confidentiality for sensitive
104 information, and decryption is the inverse operation. Over time, several block cipher
105 algorithms have been specified for use by the federal government:

106 • The Triple Data Encryption Algorithm (TDEA) (often referred to as Triple DES)
107 is specified in [SP 800-67](#)¹¹, and has two variations, known as two-key TDEA and
108 three-key TDEA. Three-key TDEA is the stronger of the two variations. The
109 latest revision of SP 800-67 disallows the use of two-key TDEA for applying
110 cryptographic protection and restricts the use of three-key TDEA for applying
111 cryptographic protection to no more than 2²⁰ data blocks using a single key
112 bundle¹².

113 • SKIPJACK was approved in [FIPS 185](#)¹³. However, approval for the use of
114 SKIPJACK is now disallowed for applying cryptographic protection, since its
115 security strength of 80 bits is now considered inadequate; it may still be used for
116 processing information previously protected using SKIPJACK (e.g., for
117 decryption).

118 • AES is specified in [FIPS 197](#)¹⁴ and has three key lengths: 128, 192 and 256 bits.

119 Note that encryption and decryption using these algorithms require the use of modes of
120 operation (see the [SP 800-38](#) series of publications). Some of these modes also provide

¹⁰ For example, if the data was encrypted and transmitted over public networks when the algorithm was still considered secure, it may have been captured (by an adversary) at that time and later decrypted by that adversary when the algorithm was no longer considered secure; thus, the confidentiality of the data would no longer be assured. Also see [Appendix A](#).

¹¹ SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*.

¹² A TDEA key bundle consists of three keys.

¹³ FIPS 185, *Escrowed Encryption Standard*.

¹⁴ FIPS 197, *Advanced Encryption Standard*.

121 authentication when performing encryption and provide verification when performing
122 decryption on the encrypted and authenticated information (see [SP 800-38C](#)¹⁵ and [SP 800-38D](#)¹⁶). Another authenticated encryption mode is specified for key wrapping, which is
123 discussed in [Section 7](#).
124

125 The approval status of the block cipher encryption/decryption modes of operation are
126 provided in [Table 1](#).

127 **Table 1: Approval Status of Symmetric Algorithms Used for**
128 **Encryption and Decryption**

Algorithm	Status
Two-key TDEA Encryption	Disallowed
Two-key TDEA Decryption	Legacy use
Three-key TDEA Encryption	Deprecated through 2023 Disallowed after 2023
Three-key TDEA Decryption	Legacy use
SKIPJACK Encryption	Disallowed
SKIPJACK Decryption	Legacy use
AES-128 Encryption and Decryption	Acceptable
AES-192 Encryption and Decryption	Acceptable
AES-256 Encryption and Decryption	Acceptable

129

130 Two-key TDEA encryption and decryption:

131 Encryption using two-key TDEA is **disallowed**.

132 Decryption using two-key TDEA is allowed for **legacy use** using the encryption modes
133 of operation specified in [SP 800-38A](#).

134 Three-key TDEA encryption and decryption:

135 Effective as of the final publication of this revision of SP 800-131A, encryption using
136 three-key TDEA is **deprecated** through December 31, 2023 using the **approved**
137 encryption modes. Note that [SP 800-67](#) specifies a restriction on the protection of no
138 more than 2^{20} data blocks using the same single key bundle. Three-key TDEA may
139 continue to be used for encryption in existing applications but **shall not** be used for
140 encryption in new applications.

141 After December 31, 2023, three-key TDEA is **disallowed** for encryption unless
142 specifically allowed by other NIST guidance.

143 Decryption using three-key TDEA is allowed for **legacy use**.

¹⁵ SP 800-38D, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*.

¹⁶ SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*.

144 SKIPJACK encryption and decryption:

145 The use of SKIPJACK for encryption is **disallowed**.

146 The use of SKIPJACK for decryption is allowed for **legacy use**.

147 AES encryption and decryption:

148 The use of AES-128, AES-192, AES-256 is **acceptable** for encryption and decryption
149 using the **approved** modes in the SP 800-38 series of publications.

150 **3 Digital Signatures**

151 Digital signatures are used to provide assurance of origin authentication and data integrity.
152 These assurances are sometimes extended to provide assurance that a party in a dispute
153 (the signatory) cannot repudiate (i.e., refute) the validity of the signed document; this is
154 commonly known as non-repudiation. The digital signature algorithms are specified in
155 [FIPS 186](#).

156 The security strength estimated for a digital signature algorithm depends on the hash
157 function used, the key length and method for key generation and any other parameters used
158 during the digital signature process.

- 159 • DSA: DSA keys are generated and used with domain parameters p , q and g . The
160 security strength that can be provided by the algorithm depends on the length of p
161 (L), the length of q (N), and the proper generation of the domain parameters used.
- 162 • Elliptic Curve-based Digital Signatures (ECDSA and EdDSA¹⁷): Keys are
163 generated and used with respect to domain parameters that define elliptic curves.
164 The length of n (the domain parameter that specifies the order of the base point G)
165 is used to determine the security strength that can be provided by a properly
166 generated curve. Elliptic curves used for the generation of digital signatures are
167 provided in [SP 800-186](#).¹⁸
- 168 • RSA: RSA keys are generated with respect to a modulus n , which is used to
169 determine the security strength that can be provided by a digital signature.

170 Note that the security strength provided by a digital signature generation process is no
171 greater than the minimum of 1) the security strength that the digital signature algorithm
172 can support with a given key length and 2) the security strength (with respect to collision
173 resistance) supported by the cryptographic hash function that is used to hash the data to be
174 signed. The estimated security strength that can be provided by a given algorithm and key
175 length is provided in [SP 800-57](#).

176 Discussions of the hash functions used during the generation of digital signatures are
177 provided in [Section 9](#).

178 [Table 2](#) provides the approval status of the algorithms and key lengths used for the
179 generation and verification of digital signatures in accordance with [FIPS 186](#). Note that

¹⁷ EdDSA will be specified in FIPS 186-5 for public comment.

¹⁸ Until SP 800-186 is completed, recommended elliptic curves are specified in FIPS 186-4.

180 digital signature generation methods not in conformance with FIPS 186 are disallowed for
 181 Federal government applications.

182 **Table 2: Approval Status of Algorithms Used for Digital Signature**
 183 **Generation and Verification**

Digital Signature Process	Domain Parameters	Status
Digital Signature Generation	< 112 bits of security strength: DSA: $(L, N) \neq (2048, 224), (2048, 256)$ or $(3072, 256)$ ECDSA: $\text{len}(n) < 224$ RSA: $\text{len}(n) < 2048$	Disallowed
	≥ 112 bits of security strength: DSA: $(L, N) = (2048, 224), (2048, 256)$ or $(3072, 256)$ ECDSA or EdDSA: $\text{len}(n) \geq 224$ RSA: $\text{len}(n) \geq 2048$	Acceptable
Digital Signature Verification	< 112 bits of security strength: DSA ¹⁹ : $((512 \leq L < 2048)$ or $(160 \leq N < 224))$ ECDSA: $160 \leq \text{len}(n) < 224$ RSA: $1024 \leq \text{len}(n) < 2048$	Legacy use
	≥ 112 bits of security strength: DSA: $(L, N) = (2048, 224), (2048, 256)$ or $(3072, 256)$ ECDSA and EdDSA: $\text{len}(n) \geq 224$ RSA: $\text{len}(n) \geq 2048$	Acceptable

184 Digital signature generation:

185 Private-key lengths providing less than 112 bits of security **shall not** be used to
 186 generate digital signatures.

187 Private-key lengths providing at least 112 bits of security are **acceptable** for the
 188 generation of digital signatures.

- 189 • DSA: The DSA domain parameter lengths **shall** be (2048, 224) or (2048, 256),
 190 which provide a security strength of 112 bits; or (3072, 256), which provides a security
 191 strength of 128 bits.

¹⁹ The lower bounds for $\text{len}(p)$ and $\text{len}(q)$ are those that were specified in FIPS 186-2.

- 192 • ECDSA and EdDSA: The security strength provided by an elliptic curve
193 signature is 1/2 of the length of the domain parameter n . Therefore, the length
194 of n **shall** be at least 224 bits to meet the minimum security-strength
195 requirement of 112 bits for federal government use. Elliptic curves for digital
196 signature generation are provided in [SP 800-186](#)²⁰. Elliptic curves that meet the
197 security strength requirements are also allowed when they satisfy the
198 requirements of [IG A.2](#).
- 199 • RSA: The length of the modulus n **shall** be 2048 bits or more to meet the
200 minimum security-strength requirement of 112 bits for federal government use.
201 The security strength associated with a particular modulus length may be
202 estimated using the formula in [IG 7.5](#).

203 Digital signature verification:

204 Key lengths providing less than 112 bits of security that were previously specified in
205 FIPS 186 are allowed for **legacy use** when verifying digital signatures. Note that the
206 lower bounds are provided in [Table 2](#) above to indicate the lowest acceptable key length
207 that was ever approved by NIST (but is no longer acceptable); the verification of
208 signatures that used key lengths less than these lower bounds **shall** be regarded as
209 having unacceptable risks.

- 210 • DSA: See [FIPS 186-2](#)²¹ and [FIPS 186-4](#),²² which include key lengths of 512
211 and 1024 bits that may continue to be used for signature verification but not
212 signature generation.
- 213 • ECDSA: See FIPS 186-2²³ and FIPS 186-4, which include specifications of
214 elliptic curves that may continue to be used for signature verification but not
215 signature generation: B-163, K-163 and P-192.
- 216 • RSA: See FIPS 186-2²⁴ and FIPS 186-4,²⁵ which include modulus lengths of
217 1024, 1280, 1536 and 1792 bits that may continue to be used for signature
218 verification but not signature generation.

219 Key lengths providing at least 112 bits of security are **acceptable** for the verification
220 of digital signatures.

- 221 • DSA: $(L, N) = (2048, 224), (2048, 256)$ or $(3072, 256)$.

²⁰ Until SP 800-186 is completed, the recommended elliptic curves are provided in [FIPS 186-4](#).

²¹ [FIPS 186-2](#) includes the 512 and 1024-bit key lengths.

²² [FIPS 186-4](#) includes the 1024-bit key length.

²³ [FIPS 186-2](#) approved the use of [ANS X9.62](#), *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, which specified the ECDSA algorithm.

²⁴ FIPS 186-2 approved the use of ANS X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*. ANS X9.31 included approval for modulus lengths of 1024, 1280, 1536 and 1732 bits.

²⁵ FIPS 186-4 includes approval for the 1024-bit modulus length.

- 222 • ECDSA and EdDSA: The elliptic curves specified in [SP 800-186](#) and additional
223 elliptic curves that provide a security strength of at least 112 bits and satisfy the
224 requirements of [IG A.2](#).
- 225 • RSA: The modulus $n \geq 2048$ bits.²⁶

226 **4 Random Bit Generation**

227 Random numbers are used for various purposes such as the generation of keys, nonces and
228 authentication challenges. Several deterministic random bit generator (DRBG) algorithms
229 have been specified for use by the federal government. [SP 800-90A](#) includes three DRBG
230 algorithms: Hash_DRBG, HMAC_DRBG and CTR_DRBG.

231 A previous version of SP 800-90A included a fourth algorithm, the DUAL_EC_DRBG,
232 whose use is now **disallowed** for federal government applications. In addition, several
233 other algorithms that were previously approved for random number generation are now
234 **disallowed**.

235 The approval status for DRBGs is provided in [Table 3](#).

236 **Table 3: Approval Status of Algorithms Used for Random Bit Generation**

Algorithm	Status
Hash_DRBG and HMAC_DRBG	Acceptable
CTR_DRBG with three-key TDEA	Deprecated through 2023 Disallowed after 2023
CTR_DRBG with AES-128, AES-192 and AES-256	Acceptable
DUAL_EC_DRBG	Disallowed
RNGs in FIPS 186-2 ²⁷ , ANS X9.31 and ANS X9.62-1998	Disallowed

237 Hash_DRBG and HMAC_DRBG:

238 The use of Hash_DRBG and HMAC_DRBG is **acceptable** with any hash function
239 specified in [FIPS 180](#) or [FIPS 202](#).

240 CTR_DRBG:

241 Effective as of the final publication of this revision of SP 800-131A, the use of
242 CTR_DRBG using three-key TDEA is **deprecated** through December 31, 2023.

243 After December 31, 2023, the use of the CTR_DRBG using three-key TDEA is
244 **disallowed**.

245 The use of CTR_DRBG using AES-128, AES-192 or AES-256 is **acceptable**.

²⁶ Additional key lengths beyond those approved in [FIPS 186-4](#) will be allowed in FIPS 186-5.

²⁷ FIPS 186-2, *Digital Signature Standard (DSS)*.

246 Dual_EC_DRBG:

247 The use of Dual_EC_DRBG is **disallowed**.

248 RNGs in other documents:

249 The use of the RNGs specified in [FIPS 186-2](#), American National Standard (ANS) [X.31](#)
250 and the 1998 version of ANS [X9.62](#) are **disallowed**.

251 **5 Key Agreement Using Diffie-Hellman and MQV**

252 Key agreement is a technique that is used to establish keying material between two entities
253 that intend to communicate, whereby both parties contribute information to the key-
254 agreement process. Two families of key agreement schemes are specified in [SP 800-56A](#):
255 Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV). Each has been defined over two
256 different mathematical structures: finite fields and elliptic curves.

257 Key agreement includes two steps: the use of an appropriate DH or MQV “primitive” to
258 generate a shared secret, and the use of a key derivation method (KDM) to generate one or
259 more keys from the shared secret. SP 800-56A contains the DH and MQV primitives and
260 refers to [SP 800-56C](#)²⁸ for KDMs.

261
262 The security strength of a key-agreement scheme specified in SP 800-56A depends on the
263 key-agreement algorithm, the parameters used with that algorithm (e.g., the keys) and its
264 form (finite field or elliptic curve).

- 265 • Finite field DH and MQV: The keys for these algorithms are generated and used
266 with domain parameters p , q and g . The security strength that can be provided by
267 the algorithm depends on the length of p , the length of q and the proper generation
268 of the domain parameters and the key.
- 269 • Elliptic Curve DH and MQV: The keys for these algorithms are generated and used
270 with respect to domain parameters that define elliptic curves. The length of n (the
271 order of the base point G), is used to determine the security strength that can be
272 provided by a properly generated curve.

273
274 [Table 4](#) contains the federal government approval status for the DH and MQV key
275 agreement schemes.

276

²⁸ SP 800-56C, *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.

277
278

Table 4: Approval Status for SP 800-56A Key Agreement (DH and MQV) Schemes

Scheme	Domain Parameters	Status
SP 800-56A DH and MQV schemes using finite fields	< 112 bits of security strength: $(\text{len}(p), \text{len}(q)) = (1024, 160)$	Disallowed
	≥ 112 bits of security strength: Using listed safe-prime groups OR FIPS 186-type domain parameters (112-bit security strength only): $(\text{len}(p), \text{len}(q)) = (2048, 224)$ or $(2048, 256)$	Acceptable
Non-compliant DH and MQV schemes using finite fields	< 112 bits of security strength: $\text{len}(p) < 2048$ OR $\text{len}(q) < 224$	Disallowed
	Non-conformance to SP 800-56A	Disallowed after 2020
SP 800-56A DH and MQV schemes using elliptic curves	< 112 bits of security strength: $\text{len}(n) < 224$	Disallowed
	≥ 112 bits of security strength: (Using specified curves)	Acceptable
Non-compliant DH and MQV schemes using elliptic curves	< 112 bits of security strength: $\text{len}(n) < 224$	Disallowed
	≥ 112 bits of security strength: Non-conformance to SP 800-56A or IG A.2	Disallowed after 2020

279

280

SP 800-56A DH and MQV schemes using finite fields:

281

The use of finite field schemes in SP 800-56A is **disallowed** when the supported security strength is less than 112 bits, i.e., when using the FA domain parameter set specified in previous versions of SP 800-56A: $(\text{len}(p), \text{len}(q)) = (1024, 160)$.

282

284

The use of the finite field schemes is **acceptable** when:

285

- Using the safe-prime domain-parameter groups listed in Appendix D of [SP 800-56A](#).

286

- 287 2. Using the FB and FC domain parameter sets specified in SP 800-56A, i.e., ($\text{len}(p)$),
288 $\text{len}(q) = (2048, 224)$ or $(2048, 256)$.

289 Non-compliant DH and MQV schemes using finite fields:

291 The use of these schemes is **disallowed** when a security strength less than 112 bits is
292 supported, i.e., using FIPS 186-type domain parameters where $\text{len}(p) < 2048$ or $\text{len}(q) <$
293 224 .

294 After December 31, 2020, the use of these schemes is **disallowed** (i.e., all finite field DH
295 and MQV schemes must conform to [SP 800-56A](#)).

296 SP 800-56A DH and MQV schemes using elliptic curves:

297 The use of elliptic curve schemes is **disallowed** when using elliptic curves that only
298 support a security strength less than 112 bits, i.e., $\text{len}(n) < 224$.

299 The use of the elliptic curve schemes for key agreement that provide at least 112 bits
300 of security strength is **acceptable** when using the elliptic curves listed in [SP 800-56A](#)
301 or when using curves that satisfy the requirements of [IG A.2](#).

302 Non-compliant DH and MQV schemes using elliptic curves:

303 The use of these schemes is **disallowed** when the only supported security strength is
304 less than 112 bits, i.e., when $\text{len}(n) < 224$.

305 After December 31, 2020, all of these schemes are **disallowed** if they do not conform
306 to the requirements of this section of SP 800-131A.

307 **6 Key Agreement and Key Transport Using RSA**

308 [SP 800-56B](#) specifies the use of RSA for both key agreement and key transport. Additional
309 key-transport schemes may be allowed in other NIST guidance. Key agreement is a technique in
310 which both parties contribute information to the generation of keying material. Key
311 transport is a key-establishment technique in which only one party determines the key and
312 sends it to the other party.

313 RSA keys are generated with respect to a modulus n . The length of n is used to determine
314 the security strength of a key-establishment scheme that uses n , assuming that n and the
315 RSA keys are generated as specified in [SP 800-56B](#). Note that SP 800-56B refers to [FIPS](#)
316 [186](#) for generation guidance.

317 Guidance on key lengths for RSA is provided in [SP 800-56B](#). SP 800-56B explicitly
318 specifies several key lengths, along with their supported security strengths, beginning with
319 $n = 2048$, which is estimated to support a security strength of 112 bits. Additional key
320 lengths greater than 2048 and not explicitly listed in SP 800-56B may be used; the
321 approximate security strength that is supported by a given key length may be estimated
322 using a formula in [SP 800-56B](#).

324 In the case of key-transport keys (i.e., the keys used to encrypt other keys for transport),
325 this document (SP 800-131A) applies to both the encryption and decryption of the
326 transported keys.

327 [Table 5](#) (below) provides the approval status the choice of n .

328
329**Table 5: Approval Status for the RSA-based Key Agreement and Key Transport Schemes**

Scheme	Modulus Length	Status
SP 800-56B Key Agreement schemes	$\text{len}(n) < 2048$	Disallowed
	$\text{len}(n) \geq 2048$	Acceptable
SP 800-56B Key Transport schemes	$\text{len}(n) < 2048$	Disallowed
	$\text{len}(n) \geq 2048$	Acceptable
Non-56B-compliant Key Transport schemes	$\text{len}(n) < 2048$	Disallowed
	PKCS 1 v1.5	Deprecated through 2023 Disallowed after 2023
	Other non-compliance with SP 800-56B	Deprecated through 2020 Disallowed after 2020

330

331 SP 800-56B RSA key-agreement schemes:

332

333 The use of these schemes is **disallowed** if $\text{len}(n) < 2048$.334 The use of these schemes is **acceptable** if $\text{len}(n) \geq 2048$.

335 SP 800-56B RSA key-transport schemes:

336 The use of these schemes is **disallowed** if $\text{len}(n) < 2048$.337 The use of these schemes is **acceptable** if $\text{len}(n) \geq 2048$

338 Non-56B-compliant RSA key-transport schemes:

339 The use of these schemes is **disallowed** if $\text{len}(n) < 2048$.340 Effective as of the final publication of this revision of SP 800-131A, the use of PKCS
341 1, version 1.5 and other RSA key-transport schemes that are not compliant with SP
342 800-56B are **deprecated**.343 After December 31, 2023, the use of PKCS 1, version 1.5 is **disallowed**.344 After December 31, 2020, the use of other RSA key-transport schemes that are not
345 compliant with [SP 800-56B](#) are **disallowed**.

346 7 Key Wrapping

347 Key wrapping is the encryption and integrity protection of keying material using a key-
348 wrapping algorithm and a symmetric key. **Approved** methods for key wrapping are
349 provided in [SP 800-38F](#).²⁹

350 SP 800-38F specifies three algorithms for key wrapping that use block ciphers: KW and
351 KWP, which use AES; and TKW, which uses TDEA. SP 800-38F also approves the CCM
352 and GCM authenticated-encryption modes specified in [SP 800-38C](#) and [SP 800-38D](#) for
353 key wrapping, as well as combinations of an **approved** encryption mode with an **approved**
354 authentication method.

355 [Table 6](#) provides the approval status of the block cipher algorithms used for key wrapping.

356 **Table 6: Approval Status of Block Cipher Algorithms Used for Key**
357 **Wrapping**

Algorithm	Status
Key wrapping using two-key TDEA	Disallowed
Key unwrapping using two-key TDEA	Legacy use
Key wrapping using three-key TDEA and any approved key-wrapping method	Deprecated through 2023 Disallowed after 2023
Key unwrapping using three-key TDEA and any approved key-unwrapping method	Legacy use
Key wrapping and unwrapping using AES-128, AES-192 or AES-256 and any method for key wrapping that is specified or otherwise approved in SP 800-38F	Acceptable

358 Two-key TDEA:

359 The use of two-key TDEA for key wrapping is **disallowed**.

360 The use of two-key TDEA for unwrapping keying material is allowed for **legacy use**.

361 Three-key TDEA:

362 Effective as of the final publication of this revision of SP 800-131A, key wrapping
363 using three-key TDEA is **deprecated** through December 31, 2023.

364 After December 31, 2023, the use of three-key TDEA is **disallowed** for key wrapping
365 unless specifically allowed by other NIST guidance.

366 Key unwrapping using three-key TDEA is allowed for **legacy use**.

367 AES:

368 The use of AES-128, AES-192 and AES-256 for both the wrapping and unwrapping of
369 keying material is **acceptable**.

²⁹ SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*.

370 8 Deriving Additional Keys from a Cryptographic Key

371 [SP 800-108](#) specifies key derivation functions (KDFs) that use pseudorandom functions (PRFs)
372 and a pre-shared cryptographic key (called a key-derivation key) to generate additional keys.
373 The length of the key-derivation key **shall** be at least 112 bits. Two PRFs are used in the KDFs
374 specified in SP 800-108:

- 375 • HMAC (as specified in [FIPS 198](#)³⁰) requires the use of a hash function (see [Section 9](#)).
- 376 • CMAC (as specified in [SP 800-38B](#)) requires the use of a block cipher algorithm (e.g.,
377 AES-128, which is specified in [FIPS 197](#)).

378 HMAC and CMAC are also known as Message Authentication Code (MAC) algorithms that
379 require the use of keys; these algorithms and the keys used with them are discussed in [Section](#)
380 [10](#).

381 [Table 7](#) provides the approval status of the PRFs for key derivation.

382 **Table 7: Approval Status of the Algorithms Used for a Key Derivation**
383 **Function (KDF)**

KDF Type	Algorithm	Status
HMAC-based KDF	HMAC using any approved hash function	Acceptable
CMAC-based KDF	CMAC using two-key TDEA	Disallowed
	CMAC using three-key TDEA	Deprecated through 2023 Disallowed after 2023
	CMAC using AES	Acceptable

384 HMAC-based KDF:

385 The use of HMAC-based KDFs is **acceptable** using a hash function specified in [FIPS](#)
386 [180](#) or [FIPS 202](#) with a key whose length is at least 112 bits.

387 CMAC-based KDF:

388 The use of two-key TDEA as the block cipher algorithm in a CMAC-based KDF is
389 **disallowed**.

390 Effective as of the final publication of this revision of SP 800-131A, the use of three-
391 key TDEA is **deprecated** through December 31, 2023. Note that [SP 800-67](#) specifies a
392 restriction on the use of three-key TDEA to no more than 2^{20} data blocks using the
393 same single key bundle.

394 After December 31, 2023, the use of three-key TDEA is **disallowed** unless specifically
395 allowed by other NIST guidance.

396 The use of AES-128, AES-192, AES-256 is **acceptable**.

³⁰ FIPS 198, *Keyed-Hash Message Authentication Code (HMAC)*.

397 **9 Hash Functions**

398 A hash function is used to produce a condensed representation of its input, taking an input
399 of arbitrary length and outputting a value with a predetermined length. Hash functions are
400 used in the generation and verification of digital signatures, for key derivation, for random
401 number generation, in the computation of message authentication codes and for hash-only
402 applications.

403 Several hash functions have been specified:

- 404 • [FIPS 180](#)³¹ specifies SHA-1 and the SHA-2 family of hash functions (i.e., SHA-
405 224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256). Discussions
406 about the different uses of SHA-1 and the SHA-2 hash functions are provided in [SP](#)
407 [800-107](#).³² Information about the security strengths that can be provided by these
408 hash functions is given in [SP 800-57](#).
- 409 • [FIPS 202](#)³³ specifies the SHA-3 family of hash functions (i.e., SHA3-224, SHA3-
410 256, SHA3-384 and SHA3-512). Discussions about the SHA-3 hash functions
411 specified in FIPS 202 are provided in that FIPS, and the security strengths that can
412 be provided by these functions are given in [SP 800-57](#). Note that FIPS 202 also
413 specifies extendable output functions (XOFs); however, these are not considered to
414 be hash functions, and their use is not included in this document³⁴.
- 415 • [SP 800-185](#)³⁵ specifies two SHA-3-derived hash functions (i.e., TupleHash and
416 ParallelHash) and discusses their use and the security strengths that they can support.

417 [Table 8](#) provides the approval status of the hash functions.

418 **Table 8: Approval Status of Hash Functions**

Hash Function	Use	Status
SHA-1	Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance.
	Digital signature verification	Legacy use
	Non-digital-signature applications	Acceptable
SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-	Acceptable for all hash function applications	

³¹ FIPS 180, *Secure Hash Standard (SHS)*.

³² SP 800-107, *Recommendation for Applications Using Approved Hash Algorithms*.

³³ FIPS 202, *Permutation-Based Hash and Extendable-Output Functions*.

³⁴ The approved uses of XOFs may be addressed in future publications.

³⁵ SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*.

512/224 and SHA-512/256)	
SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512)	Acceptable for all hash function applications
TupleHash and ParallelHash	Acceptable

419 SHA-1 for digital signature generation:

420 SHA-1 may only be used for digital signature generation where specifically allowed by
421 NIST protocol-specific guidance. For all other applications, SHA-1 is **disallowed** for
422 digital signature generation.

423 SHA-1 for digital signature verification:

424 When used for digital signature verification, SHA-1 is allowed for **legacy use**.

425 SHA-1 for non-digital signature applications:

426 For non-digital-signature applications, the use of SHA-1 is **acceptable** for applications
427 that do not require collision resistance.

428 SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256:

429 The use of these hash functions is **acceptable** for all hash function applications.

430 SHA3-224, SHA3-256, SHA3-384, and SHA3-512:

431 The use of these hash functions is **acceptable** for all hash function applications.

432 TupleHash and ParallelHash:

433 The use of TupleHash and ParallelHash is **acceptable** for the purposes specified in [SP](#)
434 [800-185](#).

435 **10 Message Authentication Codes (MACs)**

436 A Message Authentication Code (MAC) is used to provide assurance of data integrity and
437 source authentication; it is generated using a MAC algorithm and a cryptographic key. A
438 MAC is a cryptographic checksum on the data over which it is computed; it can provide
439 assurance that the data has not been modified since the MAC was generated and that the
440 MAC was computed by the party or parties sharing the key.

441 Three types of message authentication code mechanisms are specified for use:

- 442 • [FIPS 198](#) specifies a keyed-hash message authentication code (HMAC) that uses
443 a hash function; [SP 800-107](#) provides additional guidance on the uses of HMAC,
444 whether using SHA-1 or the SHA-2 or SHA-3 families of hash functions (see
445 [Section 9](#)).

- 446 • [SP 800-38B](#) and [SP 800-38D](#)³⁶ specify the CMAC and GMAC modes
447 (respectively) for block ciphers. The CMAC mode defined in SP 800-38B is
448 specified for either AES or TDEA; the GMAC mode defined in SP 800-38D is
449 specified only for AES.
- 450 • [SP 800-185](#) defines the KMAC algorithm that is based on the SHA-3 functions
451 specified in [FIPS 202](#).

452 The security strength that can be supported by a given MAC algorithm depends on the
453 primitive algorithm used (e.g., the hash function or block cipher used) and on the length
454 of the cryptographic key.

455 [Table 9](#) provides the approval status and required key lengths for the MAC algorithms in
456 order to provide a security strength of 112 bits or more.

457 **Table 9: Approval Status of MAC Algorithms**

MAC Algorithm	Key Lengths	Status
HMAC Generation	Key lengths < 112 bits	Disallowed
	Key lengths ≥ 112 bits	Acceptable
HMAC Verification	Key lengths < 112 bits	Legacy use
	Key lengths ≥ 112 bits	Acceptable
CMAC Generation	Two-key TDEA	Disallowed
	Three-key TDEA	Deprecated through 2023 Disallowed after 2023
	AES	Acceptable
CMAC Verification	Two-key TDEA	Legacy use
	Three-key TDEA	Legacy use
	AES	Acceptable
GMAC Generation and Verification	AES	Acceptable
KMAC Generation and Verification	Key lengths < 112 bits	Disallowed
	Key lengths ≥ 112 bits	Acceptable

458 HMAC Generation:

459 Any **approved** hash function may be used.

460 Keys less than 112 bits in length are **disallowed** for HMAC generation.

³⁶ Note that the CCM authenticated encryption mode specified in [SP 800-38C](#) also generates a MAC. However, the CCM mode cannot be used to only generate a MAC without also performing encryption. The modes listed in this section are used only to generate a MAC.

- 461 The use of key lengths ≥ 112 bits is **acceptable** for HMAC generation.
- 462 HMAC Verification:
- 463 The use of key lengths < 112 bits for HMAC verification is allowed for **legacy use**.
- 464 The use of key lengths ≥ 112 bits for HMAC verification is **acceptable**.
- 465 CMAC Generation:
- 466 The use of two-key TDEA for CMAC generation is **disallowed**.
- 467 Effective as of the final publication of this revision of SP 800-131A, the use of three-
- 468 key TDEA for CMAC generation is **deprecated** through December 31, 2023. Three-
- 469 key TDEA may be used for CMAC generation in existing applications but **shall not** be
- 470 used in new applications.
- 471 After December 31, 2023, three-key TDEA is **disallowed** for CMAC generation unless
- 472 specifically allowed by other NIST guidance.
- 473 The use of AES-128, AES-192 and AES-256 for CMAC generation is **acceptable**.
- 474 CMAC Verification:
- 475 The use of two-key TDEA and three-key TDEA for CMAC verification is allowed for
- 476 **legacy use**.
- 477 The use of AES for CMAC verification is **acceptable**.
- 478 GMAC Generation and Verification:
- 479 The use of GMAC for MAC generation and verification is **acceptable** when using
- 480 AES-128, AES-192 or AES-256.
- 481 KMAC Generation and Verification:
- 482 Keys less than 112 bits in length are **disallowed** for KMAC generation.
- 483 The use of key lengths ≥ 112 bits is **acceptable** for KMAC generation.

484 **Appendix A: References**

- 485 [FIPS 140] Federal Information Processing Standard (FIPS) 140-2, Security
486 Requirements for Cryptographic Modules, with Change Notices,
487 December 2002.
- 488 [FIPS 140 IG] Implementation Guidance for FIPS 140-2 and the Cryptographic Module
489 Validation Program, available [here](#).
- 490 [FIPS 180-4] Federal Information Processing Standard (FIPS) 180-4, Secure Hash
491 Standard (SHS), March 2012.
- 492 [FIPS 185] Federal Information Processing Standard (FIPS) 185, Escrowed
493 Encryption Standard, Feb 1994, Withdrawn.
- 494 [FIPS 186] Federal Information Processing Standard (FIPS) 186-4, Digital Signature
495 Standard, July 2013.
- 496 [FIPS 186-2] Federal Information Processing Standard (FIPS) 186-2, Digital Signature
497 Standard, January 2000.
- 498 [FIPS 186-4] Federal Information Processing Standard (FIPS) 186-4, Digital Signature
499 Standard, July 2013.
- 500 [FIPS 197] Federal Information Processing Standard (FIPS) 197, Advanced
501 Encryption Standard, November 2001.
- 502 [FIPS 198] Federal Information Processing Standard (FIPS) 198-1, Keyed-Hash
503 Message Authentication Code (HMAC), July 2008.
- 504 [FIPS 202] Federal Information Processing Standard (FIPS) 202, SHA-3 Standard:
505 Permutation-Based Hash and Extendable-Output Functions, August 2015.
- 506 [IG X.Y] Implementation Guidance for FIPS 140-2 and the Cryptographic Module
507 Validation Program, where X.Y is the section number.
- 508 [SP 800-38A] Special Publication (SP) 800-38A, Recommendation for Block Cipher
509 Modes of Operation: Methods and Techniques, December 2001.
- 510 [SP 800-38B] Special Publication (SP) 800-38B, Recommendation for Block Cipher
511 Modes of Operation: The CMAC Mode for Authentication, May 2005.
- 512 [SP 800-38C] Special Publication (SP) 800-38C, Recommendation for Block Cipher
513 Modes of Operation: the CCM Mode for Authentication and
514 Confidentiality, May 2004.
- 515 [SP 800-38D] Special Publication (SP) 800-38D, Recommendation for Block Cipher
516 Modes of Operation: Galois/Counter Mode (GCM) and GMAC,
517 November 2007.
- 518 [SP 800-38F] Special Publication (SP) 800-38F, Recommendation for Block Cipher
519 Modes of Operation: Methods for Key Wrapping, December 2012.
- 520 [SP 800-56A] Special Publication (SP) 800-56A, Recommendation for Pair-Wise Key
521 Establishment Schemes Using Discrete Logarithm Cryptography, April
522 2018.

- 523 [SP 800-56B] Special Publication (SP) 800-56B Revision 2, Recommendation for Pair-
524 Wise Key Establishment Using Integer Factorization, DRAFT, July 2018.
- 525 [SP 800-56C] Special Publication (SP) 800-56C Revision 1, *Recommendation for Key-
526 Derivation Methods in Key-Establishment Schemes*, April 2018.
- 527 [SP 800-57] Special Publication (SP) 800-57, Part 1, Recommendation for Key
528 Management: General, January 2016.
- 529 [SP 800-67] Special Publication (SP) 800-67, Recommendation for the Triple Data
530 Encryption Algorithm (TDEA) Block Cipher, November 2017.
- 531 [SP 800-90A] Special Publication (SP) 800-90A, Recommendation for Random
532 Number Generation Using Deterministic Random Bit Generators, Rev. 1,
533 June 2015.
- 534 [SP 800-107] Special Publication (SP) 800-107, Recommendation for Applications
535 Using Approved Hash Algorithms, August 2012.
- 536 [SP 800-108] Special Publication (SP) 800-108, Recommendation for Key Derivation
537 Using Pseudorandom Functions, November 2008.
- 538 [SP 800-185] Special Publication (S) 800-185, SHA-3 Derived Functions: cSHAKE,
539 KMAC, TupleHash and ParallelHash, December 2016.
- 540 [SP 800-186] Special Publication (SP) 800-186, Recommendation for Discrete
541 Logarithm-based Cryptography: Elliptic Curve Domain Parameters,
542 [NOT YET AVAILABLE].
- 543 Non-NIST References:
- 544 [X9.31] American National Standard (ANS) X9.31-1998, Digital Signatures
545 Using Reversible Public Key Cryptography for the Financial Services
546 Industry (rDSA). Withdrawn.
- 547 [X9.62] American National Standard (ANS) X9.62-1998, Public Key
548 Cryptography for the Financial Services Industry: The Elliptic Curve
549 Digital Signature Algorithm (ECDSA). Now renumbered to ASC X9.142.
550

551 **Appendix B: Change History**

552 The following is a list of non-editorial changes from the 2011 version of this document.

- 553 1. The use of two-key TDEA for applying cryptographic protection (e.g., encryption,
554 key wrapping or CMAC generation in KDFs) is restricted through December 31,
555 2015. Its use for processing already-protected information (e.g., decryption, key
556 unwrapping and MAC verification) is allowed for **legacy use**.
- 557 2. The use of SKIPJACK is **disallowed** for encryption, but allowed for **legacy use**
558 (e.g., decryption of already encrypted information).
- 559 3. Section 1.2.3 was added to define the single symbol used in this Recommendation:
560 **len**(*x*); this has been used to replace $|p|$, $|q|$, $|n|$ and $|h|$, rather than defining them in
561 footnotes.
- 562 4. The use of keys that provide less than 112 bits of security strength for digital
563 signature generation are no longer allowed; however, their use for digital signature
564 verification is allowed for **legacy use** (i.e., the verification of already-generated
565 digital signatures). For digital signature verification using DSA, the **legacy-use** row
566 has been specified to reflect the lower bound that was specified in FIPS 186-2 (i.e.,
567 512 bits).
- 568 5. The use of the DUAL_EC_DRBG, formerly specified in [SP 800-90A], is no longer
569 allowed.
- 570 6. The use of the RNGs specified in [\[FIPS 186-2\]](#), [\[X9.31\]](#) and [\[X9.62\]](#) is **deprecated**
571 until December 31, 2015 and **disallowed** thereafter.
- 572 7. The use of keys that provide less than 112 bits of security strength for key
573 agreement is now **disallowed**.
- 574 8. The use of non-approved key-agreement schemes is **deprecated** through December
575 31, 2017 and **disallowed** thereafter.
- 576 9. The use of non-approved key-transport schemes is **deprecated** through December
577 31, 2017 and is **disallowed** thereafter.
- 578 10. Non-approved key-wrapping methods are disallowed after December 31, 2017.
- 579 11. The use of SHA-1 for digital signature generation is **disallowed** (except where
580 specifically allowed in NIST protocol-specific guidance); however, its use for
581 digital signature verification is allowed for **legacy use** (i.e., the verification of
582 already-generated digital signatures).
- 583 12. The SHA-3 family of hash functions specified in [\[FIPS 202\]](#) has been included in
584 [Section 9](#) as **acceptable**.
- 585 13. The use of HMAC keys less than 112 bits in length is no longer allowed for the
586 generation of a MAC; however, they may be used for **legacy use** (i.e., the
587 verification of already-generated MACs).

588 The following changes have been made to the 2018 version:

- 589 1. Section 1: Revised to discuss coming availability of quantum computers and to identify
590 the most significant differences between this version of SP 800-131A and the previous
591 version.
- 592 2. Section 1.2.2: New section added to define terms.
- 593 3. Section 1.2.3 (old Section 1.2.2): The **restricted** approval status term was removed.
- 594 4. Section 2: Disallowed the use of two-key TDEA for encryption and provided a sunset
595 schedule for three-key TDEA.
- 596 5. Section 3: Clarified the DSA disallowed and acceptable domain parameters, added
597 EdDSA as an additional elliptic curve algorithm.
- 598 6. Section 4: Provided a sunset schedule for using the CTR_DRBG with three-key
599 TDEA.
- 600 7. Section 5: Clarified the DH parameters and elliptic curves that are now disallowed or
601 acceptable, added the DH groups listed in SP 800-56A as acceptable, and provided a
602 termination date for non-SP 800-56A-compliant key-agreement schemes.
- 603 8. Section 6: Added PKCS 1 v1.5 and included a sunset schedule.
- 604 9. Section 7: Provided a sunset schedule for the use of TDEA for key wrapping.
- 605 10. Section 8: Provided a sunset schedule for the use of CMAC-based KDF using TDEA.
- 606 11. Section 9: Added TupleHash and ParallelHash.
- 607 12. Section 10: Provided a sunset schedule for the use of CMAC using TDEA and added
608 KMAC.
- 609 13. (Old) Appendix A (Mitigating Risk When Using Algorithms and Keys for legacy
610 Use): Removed.
- 611 14. (New) Appendix A (old Appendix B): Updated the references.
- 612