NIST Cryptographic Standards and Guidelines Development Program Briefing Book

Cryptographic Technology Group

13 May 2014

Table of Contents

Introduction 1

Federal Information Processing Standards 3

Federal Information Processing Standard (FIPS) 180: Secure Hash Standard (SHS) 4

Federal Information Processing Standard (FIPS) 185: Escrowed Encryption Standard (EES) 6

Federal Information Processing Standard (FIPS) 186: Digital Signature Standard 8

Federal Information Processing Standard (FIPS) 197: Advanced Encryption Standard 10

Federal Information Processing Standard (FIPS) 198: The Keyed-Hash Message Authentication Code (HMAC) 12

800 Series Special Publications 13

NIST Special Publication (SP) 800-38 Series Development Process Overview 14

NIST Special Publication (SP) 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques 16

NIST Special Publication (SP) 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication 18

NIST Special Publication (SP) 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality 20

NIST Special Publication (SP) 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC 21

NIST Special Publication (SP) 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices 22

NIST Special Publication (SP) 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping 24

NIST Special Publication (SP) 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography 26

NIST Special Publication (SP) 800-56B: Recommendation for Pair-Wise Key Establishment Schemes: Using Integer Factorization Cryptography 28

NIST Special Publication (SP) 800-56C: Recommendation for Key Derivation through Extraction-then-Expansion 30

NIST Special Publication (SP) 800-57: Recommendation for Key Management 31

NIST Special Publication (SP) 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher 33

NIST Special Publication (SP) 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators 34

NIST Special Publication (SP) 800-106: Randomized Hashing for Digital Signatures 36

NIST Special Publication (SP) 800-108: Recommendation for Key Derivation Using Pseudorandom Functions 37

NIST Special Publication (SP) 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths 38
NIST Special Publication (SP) 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications 39
NIST Special Publication (SP) 800-133: Recommendation for Cryptographic Key Generation....................40
NIST Special Publication (SP) 800-135: Recommendation for Existing Application-Specific Key Derivation Functions 41

Introduction

To facilitate the Committee of Visitor's review of NIST's cryptographic standards and guidelines development program, the Cryptographic Technology Group (CTG) compiled basic information on the development of its publications into the COV Briefing Book. This information is intended to provide examples of the processes NIST uses to develop its standards, as well as help the COV identify areas and topics where they would like more details.

NIST has developed a broad set of computer security publications under its authority to develop standards and guidelines for protecting non-national security systems. The topics covered by these publications extend far beyond cryptography, covering risk management, computer security controls, security automation, and guidance on securing critical technologies. The full set of publications can be found at: http://csrc.nist.gov/publications/

The CTG develops many of these publications, particularly when cryptography is used as a foundational security mechanism. Broadly speaking, the cryptography-related standards and guidelines fall into one of four categories:

- ***Algorithm specifications***: FIPS and Special Publications specify a number of approved cryptographic algorithms as part of NIST's Cryptographic Toolkit. These include block ciphers, modes of operation, digital signature algorithms, hash functions, key derivation functions, random bit generators, and key establishment schemes.

- ***General guidance on the use of cryptography***: NIST produces standards and guidelines on the selection, implementation, deployment and use of cryptography. This includes guidance on the selection and use of algorithms and key sizes, and a suite of documents on key management.

- ***Guidelines in application-specific areas***: FIPS and Special Publications include standards and guidelines on the use of cryptography in specific applications areas where a critical need has been identified. Two major application areas include standards and specifications for the U.S. government's Personal Identity Verification (PIV) card, and documents on Public Key Infrastructure technology. NIST has also produced guidance on the use of Virtual Private Networks and the Transport Layer Security protocol.

- ***Testing***: FIPS 140 contains security requirements for products that implement cryptography, and the associated Cryptographic Module Validation Program tests products for conformance with this standard. The Cryptographic Algorithm Validation Program tests products for conformance with NIST's algorithm specifications. Both programs have a set of documents that support their testing activities.

Concerns over the development of NIST SP 800-90A, and the specification for the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) in that guideline, have questioned the integrity of NIST's cryptographic standards and guidelines, particularly those specifying algorithms.

Based on those concerns, this briefing book focuses on current NIST standards and guidelines that specify cryptographic algorithms, schemes, modes of operation, or key management.   Based on this scope, the CTG identified 24 publications covering topics ranging from block ciphers, digital signature algorithms, hash functions, key derivation functions, random number generators, and key establishment schemes and key management. These publications provide the foundation for NIST's set of cryptography-related standards and guidelines.

The CTG did not include information on testing requirements or guidelines related to cryptography, standards or guidelines on applications of cryptography, or general guidance on the use of the algorithms in the Cryptographic Toolkit specified in other NIST publications. More information on any of these other cryptography-related publications can be made available upon request.

For each of these publications included in this briefing book, the CTG developed a brief summary of the development process. This summary describes the scope of the publication, identifies the contributing organizations and base documents, provides an overview of the development history, identifying opportunities for public engagement, and describes the major decisions that were made in its development.

As summaries, these descriptions are intended to help the COV identify and prioritize topics that may warrant further investigation. The CTG can provide additional information on these topics based on questions or requests from the COV.

Federal Information Processing Standards

Federal Information Processing Standard (FIPS) 180:
Secure Hash Standard (SHS)

Scope: FIPS 180 specifies seven approved hash algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256.

Purpose/identified need: A secure cryptographic hash function is a required component in any digital signature algorithm. The original draft of FIPS 186, *Digital Signature Standard*, was released without specifying a cryptographic hash function, and FIPS 180 was developed to fill that need. Cryptographic hash functions can also be used to build many other cryptographic functions, such as a keyed-hash Message Authentication Code (HMAC), key derivation functions and pseudo-random number/bit generation functions that are used in many secure applications and communication protocols.

Contributors: The FIPS 180 standard was developed by NIST staff based on hash functions designed by the NSA.

Timeline: The draft of FIPS 186 was released for public comment in 1991 requiring, but not specifying, an approved hash function. Draft FIPS 180 was published for public comment in January 1992 and approved in May 1993. This FIPS specified the original SHA hash algorithm (sometimes referred to as SHA-0) that was developed by NSA.

In April 1994, NIST announced that it would revise the original SHA algorithm to correct a weakness that had been identified by researchers at the NSA. A proposed revision of FIPS 180 was posted for a 90-day public comment period as FIPS 180-1 in July 1994. That revision provided a small change in the SHA hash algorithm specification that was intended to remediate the weakness. This revised algorithm was referred to as SHA-1, to differentiate it from the original SHA. FIPS 180-1 was approved in April 1995.

During the development of the Advanced Encryption Standard (AES), NIST identified a need for stronger hash functions that were capable of supporting the same security strengths as AES. NIST asked NSA to provide hash functions supporting the 128, 192, and 256 bit security strengths. This resulted in the development of SHA-256, SHA-384 and SHA-512, which collectively became known as the SHA-2 family of hash algorithms. These algorithms were first published in Draft FIPS 180-2, released in May 2001 for a 90-day comment period, and finalized in August 2002.

A change notice draft for FIPS 180-2 was provided for a 30-day public comment in December 2003 and published as final in 2004. The change notice added a new hash algorithm: SHA-224, which was intended to be used with 2048-bit DSA and RSA signing algorithms and provide 112 bits of security strength. Draft FIPS 180-3 was provided for a 90-day public comment period in June 2007 and approved in October 2008. FIPS 180-2 contained security claims for the hash algorithms and hash output truncation requirements. Due to the attacks on hash functions known at the time, it seemed that the security claims of the hash functions could change at any given time. In order to address any future security weakness discoveries of the hash functions fast and effectively, NIST decided to revise the FIPS to remove all of the security claims and discussions to a special publication – NIST SP 800-107, which could be updated by a much faster process.

Draft FIPS 180-4 was published for a 90-day public comment period in February 2011 and approved in March 2012. This revision added two new hash algorithms: SHA-512/224 and SHA-512/256, which are much faster than SHA-224 and SHA-256 on modern machines that have 64-bit processors.

Public engagement: NIST posted all of the proposed revisions for the FIPS for public review and comment. After each review and comment period closed, NIST reviewed the received comments and incorporated appropriate comments into the final version.

Major decision(s): During the development of the Digital Signature Standard, NIST and NSA conducted an analysis of hash algorithms that were available in public literature. They concluded that these hash algorithms did not meet their requirements, which led to the standardization of SHA.

NIST was informed of a security flaw in the original specification of SHA that was included in FIPS 180. NIST announced a weakness in the announcement for the draft FIPS 180-1, which proposed changes to the SHA specification. This modified algorithm became SHA-1.

In 2005 Prof. Xiaoyun Wang announced a differential attack on the SHA-1 hash function; with her recent improvements, this attack is expected to find a hash collision with an estimated work of 2^{63} operations, rather than the ideal 2^{80} operations that should be required for SHA-1 or any good 160-bit hash function. Based in this research, NIST encouraged users and industry to transition to the stronger SHA-2 family of hash algorithms, and initiated an international competition to select a new hash algorithm standard, SHA-3, in 2007.

Federal Information Processing Standard (FIPS) 185:
Escrowed Encryption Standard (EES)

Scope: FIPS 185 specifies the implementation and use of a formerly classified encryption/decryption algorithm and a Law Enforcement Access Field (LEAF) for protecting government telecommunications.

Notably, FIPS 185 did not include a specification for a cryptographic algorithm or scheme, but did require the use of the (then classified) SKIPJACK algorithm in conjunction with modes specified in FIPS 81, DES Modes of Operation.

Purpose/identified need: FIPS 185 was intended to ensure that information encrypted with devices implementing the standard could be decrypted by an authorized entity after due legal process. FIPS 185 requires agency use of a technology developed by NSA to provide strong encryption for sensitive unclassified information and provides for the decryption of the encrypted information using escrowed keys. Key escrow addressed the concern that widespread use of encryption would make lawful electronic surveillance difficult. In April 1993, a Presidential directive on "Public Encryption Management" required the Secretary of Commerce to promulgate a standard for escrowed encryption "within six months."

Contributors: FIPS 185, drafted and maintained by the NIST Computer Systems Laboratory, specifies only the provisions for use of the key escrow components. At the time that FIPS 185 was approved, the specifications for the cryptographic algorithm referenced in FIPS 185 were contained in a classified NSA Informal Technical Report, "SKIPJACK." A classified NSA Informal Technical Report, "Law Enforcement Access Field for the Key Escrow Microcircuit" specified the LEAF.

Timeline: The cryptographic functions underlying FIPS 185 were developed as classified documents in 1991. In April 1993, the President issued a Presidential Directive requiring the Department of Commerce (DOC) to promulgate a key-escrow standard. The DOC published a Federal Register notice announcing a 60-day comment period of the draft FIPS on July 30, 1993. The Undersecretary of Commerce for Technology summarized the comments that were received and recommended the approval of FIPS 185 to the Secretary of Commence on February 3, 1994. The Federal Register notice reporting the public comments and announcing DOC approval of FIPS 185 was published on February 9, 1994, and the Standard became effective 30 days later. The SKIPJACK cryptographic algorithm was declassified on June 24, 1998, and is now available on the NIST website.

Public engagement: The draft FIPS and a 60-day comment period were announced in the Federal Register and also sent to Federal agencies for review. The comments were reported in the February 9, 1994, Federal Register. These comments were overwhelmingly negative on the policy, technical, intellectual property, and economic grounds. The recommendation for approval referenced the Presidential Directive.

Major decisions: The Presidential Directive required the installation of government-developed microcircuits, and the development of a standard to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits within six months. Since the algorithm (i.e., SKIPJACK) was classified at the time, the Standard could only discuss the algorithm in general terms, so the major decision was what to put in the Standard. FIPS 185 discussed the use of a field known as the Law Enforcement Access Field (LEAF) and the types of parameters to be included in it, e.g., a unique identifier for the microcircuit, initial vectors and keys. The Standard also mandated the security to be provided by the implementation, certain requirements for key generation and the use of escrow agents to protect key components.

Federal Information Processing Standard (FIPS) 186: Digital Signature Standard

Scope: FIPS 186 specifies techniques for the generation and verification of digital signatures that can be used for the protection of data. The Standard includes methods for the generation of both the domain parameters and the cryptographic key pairs used during signature generation and verification.

FIPS 186-4 specifies the DSA algorithm, and methods for the generation of its domain parameters and key pairs. ANS X9.62 is referenced for the ECDSA specification, including the generation of domain parameters and key pairs; however, the recommended curves are provided in an appendix of FIPS 186-4. ANS X9.31 and PKCS #1 are referenced for the algorithms for generation of RSA signatures, but FIPS 186-4 specifies methods for the generation of key pairs.

Purpose/identified need: As the use of electronic communications greatly expanded during the 1980s, NIST increasingly believed that digital signature technology would become an important part of future business processes. By the late 1980s, the private sector had begun using digital signatures based on algorithms developed by academic researchers, but no government standard existed for the public sector.

Contributors: FIPS 186 was initially developed by NIST in collaboration with NSA, using the NSA-designed Digital Signature Algorithm (DSA). Later versions of the standard added specifications for ECDSA, developed by Certicom, and RSA, developed by Ron Rivest, Adi Shamir and Len Adelman. American Standards Committee X9 developed standards specifying the use of both ECDSA and RSA, including methods for generating key pairs, which were used as the basis for the later versions of FIPS 186.

Timeline: In the early 1980s, NIST, reacting to the development of the first publicly known digital signature algorithm, known as RSA, published a solicitation in the Federal Register. This public solicitation began a decade-long process to develop the first digital-signature standard for government use.

NIST, in consultation with NSA, considered several signature algorithms before selecting DSA as the basis for the Digital Signature Standard. FIPS 186 was first released in 1991 for public comment. The final version was published in 1994, after making several changes to the standard based on the received public comments. Notably, the final version provided options for longer key lengths, based on concerns that the sole 512-bit modulus length included in the draft version was too short.

FIPS 186-1 and FIPS 186-2 were published in 1998 and 2000, respectively, and adopted ECDSA (as specified in American National Standard (ANS) X9.62) and RSA (as specified in ANS X9.31). In 2009, FIPS 186-3 increased the key sizes allowed for DSA, provided additional requirements for the use of ECDSA and RSA, and included requirements for obtaining the assurances necessary for valid digital signatures. FIPS 186-4, which was published in 2013, corrected errors in FIPS 186-3.

Public engagement: NIST solicited public comments in the Federal Register for each version of the FIPS, and an announcement of adoption was also posted in the Federal Register after approval of the FIPS by the Secretary of Commerce. The original draft of FIPS 186 received several critical comments. NIST staff spoke at the "Crypto '92" conference to respond to those comments and describe how they would be addressed. Compared to the more open DES process, the cryptographic community expressed concern over the relatively closed development process for the original Digital Signature Standard.

Major decisions: NIST considered several digital signature algorithms before selecting the NSA-designed DSA as the basis for FIPS 186. At the time, the RSA algorithm was the de facto standard for digital signatures within industry, and was an early favorite for standardization by NIST. Ultimately, a desire for a royalty-free algorithm, along with national security concerns over the use of RSA as a public-key encryption scheme in addition to its use for digital signatures, led to a decision to select an alternative algorithm. NIST received two digital-signature algorithm designs from NSA , one based on Schnorr signatures, and the other based on El Gamal. The El Gamal-based algorithm was selected to become DSA, due to patent concerns with the Schnorr-based design.

The Elliptic Curve Digital Signature Algorithm (ECDSA) was included by reference in FIPS 186-2. To facilitate testing and interoperability, NIST needed to specify elliptic curves that could be used with ECDSA. Relying on technical expertise from NSA, FIPS 186-2 included three sets of curves generated using the algorithms in the ANS X9.62 and IEEE P1363 standards. However, the provenance of the curves was not fully specified, leading to recent public concerns that there could be a hidden weakness in these curves. These concerns are conjecture, and currently there are no known attacks on these curves when they are used as described in NIST standards and guidelines.

Federal Information Processing Standard (FIPS) 197: Advanced Encryption Standard

Scope: FIPS 197 specifies a 128-bit block cipher with keys of 128, 196 or 256-bits.

Purpose/identified need: By the mid 1990s, the DES with 56-bit keys was vulnerable to key exhaustion attacks. Triple DES offered a quick fix for key exhaustion, but was slow in software, had less than the full generic security of its 168-bit key and the 64-bit block size resulted in 2^{32}-block birthday bound security limitations for common encryption modes. A new, more software-friendly block cipher standard with much bigger key and block sizes was needed.

Contributors: NIST wrote the AES standard, based on the Rijndael block cipher designed by Joan Daemen and Vincent Rijmen. Rijndael was one of 15 candidates submitted to the AES competition. While hundreds of researchers contributed to the AES selection, only Daemen and Rijmen participated in the design of Rijndael. NSA presented VLSI implementation studies of the finalists but informally told NIST that they could accept any of the five finalist candidate algorithms, giving no specific advice on the final selection. NIST staff alone comprised the AES selection panel.

Timeline:

- January 1997 Federal Register Announcement of interest in an Advanced Encryption Standard and of a workshop on the AES requirements
- April 1997: Open workshop at NIST on AES Selection Criteria
- September 1997: Federal Register Call for AES Candidate Submissions with a 128-bit block size and 128, 192 and 256-bit keys.
- June 201998 Submissions due to NIST. Fifteen were judged "complete."
- August 1998: First AES Candidate Conference in Ventura, CA preceding the Crypto 1998 conference in nearby Santa Barbara.
- March 1999 Second AES Candidate Conference held in Rome preceding the 6th Fast Software Encryption Conference. Following the conference, NIST announced the selection of 5 finalist algorithms.
- April 2000: Third AES Candidate Conference to review the AES finalists held in New York City following the Fast Software Encryption 2000 Workshop.
- October 2000: NIST announced the selection of Rijndael to be the AES
- February 2001: Publication of Draft FIPS 197 for public review
- Nov. 2001: Approval of FIPS 197.

Public engagement: NIST posted Federal Register announcements at major points, maintained a website with all information that it had on the candidates, and set up a public e-mail forum for the Competition. NIST aligned the selection process with the cryptographic research community by holding workshops aligned with major IACR conferences and holding workshops with papers so that researchers could get publication credit for participating. NIST published reports on the workshops and the selection rationale to document and explain the effort. NIST achieved an unprecedented level of expert participation from the research community, and relied heavily on the community for cryptanalysis in particular.

Major decisions: Before AES, most block ciphers for encryption had used a 64-bit block. Encryption and authentication modes for ciphers with 64-bit blocks typically have "birthday bound" limitations after about 2^{32} blocks have been processed under a single key. The decision to request block cipher with a 128-bit block size was perhaps surprising, but not controversial. The emergence of multi-terabyte storage devices and the new era of big data have proved the wisdom of this choice.

Several of the attractive candidate algorithms were not from US submitters, including the eventual winner, Rijndael. Under the rules of the competition a non-US submission might be selected, and the NIST staff intended to pick the best candidate without respect to its origin. But the staff also worried that a non-US choice might be problematic for management. As it turned out, this was not a problem at all in the approval process.

Rijndael was a very clean algorithm with a clear design rationale. NIST believed that it was the candidate with the best balance of software/hardware performance. The primary criticism was that it appeared to have an insufficient security margin, and that the number of rounds should be increased. Three of the other four remaining finalist algorithms had apparently larger security margins. AES has since been intensely studied, and, to date, the main weakness discovered in AES is in the key schedule for AES192 and AES256, which is not a problem for any NIST approved block cipher encryption or authentication mode, but could be a problem for other potential applications such as a hash function compression mode.

Federal Information Processing Standard (FIPS) 198: The Keyed-Hash Message Authentication Code (HMAC)

Scope: FIPS 198 specifies a keyed-hash message authentication code (HMAC) using a cryptographic key and one of the approved hash algorithms specified in FIPS 180. The HMAC specification in FIPS 198 aligns with the HMAC specification in RFC 2104, developed by the Internet Engineering Task Force, with the added provision that NIST-approved hash algorithms must be used.

Purpose/identified need: Data authentication and integrity protection are very important security services. Using HMAC, the receiver can verify whether or not received data has changed since the sender computed the MAC and sent the data. By using a hash algorithm instead of a block cipher, HMAC is not subject to the same export controls as encryption algorithms. By the time HMAC was standardized in FIPS 198, it was already widely used in common Internet security protocols, including TLS and IPsec.

Contributors: NIST staff developed the FIPS specification, which was reviewed by NSA prior to publication. FIPS 198 was based on the specification of HMAC in RFC 2104 by H. Krawczyk, M. Bellare and R. Canetti, dated February 1997.

Timeline: NIST published FIPS 198 in March 2002 and its revision: FIPS 198-1 in July 2008.

Public engagement: The proposed FIPS 198 was provided for a 90-day public comment period in 2000, and the FIPS was approved in March 2002. NIST posted the draft of FIPS 198-1 for a 90-day public review and comment period in June 2007. After reviewing all of the received comments, NIST revised the specification and published the official version of FIPS 198-1 in July 2008.

Major decision(s): There was no opposition to standardizing HMAC in FIPS 198. Also, there are no known security issues of the function. The major decision was to move the security discussion and requirements of HMAC to SP 800-107 where they could be updated faster when needed.

The original version of the FIPS contained statements about the security provided by the HMAC algorithm, specified a truncation technique for the HMAC output ,and provided advice concerning its use. Because of the concern that the security provided by the HMAC algorithm and its applications might be altered by future cryptanalysis, NIST decided to remove the informative security information from the FIPS and provide it in another publication, SP 800-107, which could be revised faster than a FIPS if serious security issues arose in the future. Thus, FIPS 198-1 was revised to include only the specification of the HMAC algorithm and the truncation technique.

800 Series Special Publications

NIST Special Publication (SP) 800-38 Series Development Process Overview

In FIPS Pub 197, the Advanced Encryption Standard (AES), NIST Recommendations are authorized as a source for modes of operation for implementations of the AES block cipher. Recommendations for a variety of modes have been published in a relatively agile manner under that authority, in the 800-38 series of NIST Special Publications.

After the AES Competition, NIST recognized the need to update the four modes of operation that had been specified in FIPS 81 for use with the Data Encryption Standard (DES) block cipher and, subsequently in ANS X9.52, for use with the Triple DES block cipher. That was the impetus to the development of SP 800-38A.

NIST received many proposals for new block cipher modes of operation in 2000 and 2001, and held two public workshops on modes of operation to promote discussion of these proposals. One proposal, for the Counter (CTR) mode, was appropriate to include in SP 800-38A; however, NIST recognized that it would be useful to develop an ongoing, open, and transparent process for the consideration of new modes.

For subsequent publications in the SP 800-38 series, the following model evolved over time: NIST posts guidelines on the information to submit with any proposals for new modes on its Computer Security Resource Center website. For any minimally credible submission, the associated documentation is posted on a “Modes Development” page, along with an open invitation for public review. Any public comments on modes proposals are posted on a “Public Comments” page.

At a high level, there are two main decision points in the process. The first is the determination from internal analysis and public comments that a version of a mode proposal is appropriate to include in NIST’s cryptographic toolkit. The main considerations are the following: 1) whether the mode serves an important need; 2) whether existing modes in the toolkit or other modes proposals can adequately provide the needed properties/functionality instead; 3) whether the mode meets NIST’s security requirements; and 4) for patented modes, whether acceptable royalty-free alternatives are available.

When NIST is interested in approving a mode proposal, the next step is the development of a draft special publication that specifies the mode. Normally, NIST develops the draft in consultation with the mode submitter. After passing internal review, the draft is posted on the CSRC website for a period of public comment, after which any received comments are also posted. NIST considers the public comments carefully. The second decision point is whether 1) to finalize the draft for publication, with appropriate revisions to address any remaining public or internal concerns; 2) revise the draft for further public review; or 3) withdraw the proposal altogether.

In two cases, the impetus for a modes proposal came from NIST: the updating of the DES modes in SP 800-38A, discussed above, and the key wrapping modes in SP 800-38F.

In three of the other four publications in the SP 800-38 series, NIST sought additional public input at one of the decision points:

- In response to public comments on the first draft of SP 800-38B, NIST requested further comments on the revision plan. Subsequently, an entirely different mode was specified in a new draft for public review.
- NIST requested public input on the choice of two different submitted modes for specification in SP 800-38D. Also, in response to public comment on the first draft, a second draft was developed for public review.
- NIST requested input on a proposal to approve a mode by reference to an IEEE standard prior to the public review of a short draft of SP 800-38E as the vehicle for that approval.

A summary of the technical issues involved in each case is given in the individual briefing pages.

NIST Special Publication (SP) 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques

Scope: SP 800-38A specifies five block cipher modes of operation for data confidentiality for use with any approved block cipher. Three variants of an extension to one of the modes were subsequently published in Addendum to SP 800-38A.

Purpose/identified need: Versions of four of the five modes were previously specified for the DES block cipher in FIPS 81, DES Modes of Operation. These four modes needed to be updated for use with the AES block cipher. A fifth mode, Counter (CTR) mode was added to provide an option with a useful set of properties, such as parallelizability.

Contributors: NIST staff developed SP 800-38A, with review by NSA. Three academic cryptographers, Helger Lipmaa (Helsinki University of Technology), Phillip Rogaway (University of California, Davis), and David Wagner (University of California, Berkeley), proposed the CTR mode to NIST.

Timeline:

Oct. 2000	CTR mode proposal presented at the first NIST workshop on modes.
Oct. 2001	Draft SP 800-38A proposed for public comment.
Dec. 2001	SP 800-38A published.
June 2010	Draft Addendum to SP 800-38A proposed for public comment.
Oct. 2010	Addendum to SP 800-38A published.

Defined crypto algorithms/modes/schemes: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). Each of these modes provides data confidentiality.

Three variants of the Cipher Block Chaining-Ciphertext Stealing extension of CBC mode were specified in Addendum to SP 800-38A: CBC-CS1, CBC-CS2, and CBC-CS3.

Public engagement: The public submitted a variety of modes of operation, including CTR, for NIST's consideration in the aftermath of the AES competition, and NIST held two public workshops on modes of operation to obtain public input. NIST received public comments on Draft SP 800-38A, and Draft Addendum to SP 800-38A.

Major Decisions: Updating the four DES modes – ECB, CBC, CFB, and OFB – for use with the AES block cipher, with a block size of 128 bits, was technically straightforward. NIST decided to include the CTR mode in SP 800-38A and developed new requirements and guidance in connection with the generation of its counter parameter, as well as the initialization vectors for the CBC, CFB, and OFB modes.

Subsequently, NIST decided to approve three variants of the "ciphertext stealing" extension of CBC in an Addendum to SP 800-38A. One variant was specified for a version of

Kerberos; the other two variants were natural alternatives that differed only in the ordering of ciphertext bits.

NIST Special Publication (SP) 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

Scope: SP 800-38B specifies CMAC, a block cipher mode of operation for authentication for use with any approved block cipher.

Purpose/identified need: A mode of operation for authentication was desirable for use with the AES block cipher, as an alternative to the hash function-based HMAC. The earlier CBC-MAC mode of operation for authentication was vulnerable to certain forgery attacks, so a new mode was needed.

Contributors: Four cryptographers developed and submitted relevant proposals and analysis to NIST: Tetsu Iwata (Ibaraki University), Kaoru Kurosawa (Ibaraki University), Phillip Rogaway (University of California, Davis), and John Black (University of Nevada, Reno). NIST staff developed SP 800-38B, with review by the mode submitters and NSA. NSA also advised NIST on the selection of an authentication mode to approve..

Timeline:

• 2000-01	Submission of Rogaway and Black's XCBC mode to NIST's workshops.
• 2001	Submission of the RMAC mode to NIST's second public workshop.
• Jan. 2002	Submission of Iwata and Kurosawa's TMAC mode, based on XCBC.
• Oct. 2002	Release of draft SP 800-38B, specifying RMAC, for public comment.
• Dec. 2002	Submission of Iwata and Kurosawa's OMAC mode, improving TMAC.
• Jan. 2003	Posting of a NIST proposal to modify the specification of RMAC.
• June 2003	Submission of Iwata and Kurosawa's OMAC1 mode, revising OMAC.
• March 2005	Release of draft SP 800-38B, specifying OMAC1, for public comment.
• May 2005	Publication of SP 800-38B.

Public engagement: The public submitted a variety of modes of operation, including XCBC and RMAC, for NIST's consideration in the aftermath of the AES competition, and NIST held two workshops to obtain public input on the proposals. NIST invited and received public comments on 1) the 2002 Draft SP 800-38B, specifying the RMAC mode; 2) a "consultation paper" that proposed a plan to modify the RMAC specification; and 3) the 2005 Draft SP 800-38B, specifying OMAC1 as CMAC, which was ultimately finalized and published.

Major Decisions: NIST changed the authentication mode in SP 800-38B in response to public feedback. In particular, several reviewers objected to the variants of the RMAC mode that NIST initially proposed and disagreed with NIST's subsequent proposal to revise the RMAC specification. Consequently, NIST considered anew the XCBC mode and its improved variants, TMAC and OMAC, and decided to replace RMAC with OMAC1, under a new name, CMAC.

NIST received only one objection to CMAC, informally: the security of CMAC was incompatible with a key-management practice that was deployed in some financial services applications with DES and Triple DES. NIST considered the issue in consultation with the mode submitters and decided not to modify CMAC when the Special Publication was finalized.

NIST Special Publication (SP) 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality

Scope: SP 800-38C, specifies the Counter with Cipher Block Chaining-Message Authentication (CCM) mode of operation for authenticated encryption using the AES block cipher.

Purpose/identified need: A significant vulnerability was discovered in an encryption method (WEP) that was widely used in an industry standard (IEEE 802.11i) for wireless local-area networks (WLANs). There was an urgent need for a secure authenticated encryption method for WLANs.

Contributors: Three industry cryptographers developed and submitted CCM to NIST: Russ Housley (RSA Laboratories), Doug Whiting (Hifn) and Niels Ferguson (MacFergus BV). NIST staff developed SP 800-38C from their proposal, with review by the mode submitters and NSA.

Timeline:

- Aug. 2001 Publication of a practical attack on IEEE 802.11's WEP method.
- May 2002 Development of CCM for IEEE 802.11.
- June 2002 Submission of CCM to NIST.
- Nov. 2002 NIST intent to approve CCM was signaled at an IETF meeting.
- Feb. 2003 Submission of EAX to NIST, along with a critique of CCM.
- Sept. 2003 Release of Draft SP 800-38C for a period of public comment.
- May 2004 Publication of SP 800-38C; posting of responses to public comments.

Public engagement: After NIST signaled its intent to approve CCM, Phillip Rogaway (University of California, Davis) and David Wagner (University of California, Berkeley) submitted a detailed critique of CCM, and with Mihir Bellare (University of California, San Diego), submitted the EAX mode as an alternative method. NIST received public comments on Draft SP 800-38C, specifying the CCM mode, which was ultimately finalized and published.

Major Decisions: The draft amendment to IEEE 802.11 that addressed WEP vulnerability specified CCM as mandatory-to-implement; NIST decided to approve CCM in support of this amendment. This decision was consistent with NIST's specific responsibilities for the protection of U.S. Government data and with the promotion of commerce.

NIST adapted the CCM submission in Draft SP 800-38C. Several technical objections to CCM were raised prior to the release of the draft and during the period of public comment on the draft. NIST considered the comments, including an alternative mode, EAX, which had been submitted in the interim. Although EAX arguably was technically preferable, NIST's main goal was to support IEEE 802.11, which specified CCM. SP 800-38C was revised and published, and responses to the public comments were posted on NIST's website.

NIST Special Publication (SP) 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Scope: In SP 800-38D, two modes of operation of the AES block cipher are specified: 1) the Galois/Counter Mode (GCM) for authenticated encryption and 2) its specialization, the GMAC mode for authentication.

Purpose/identified need: A block cipher mode of operation for authenticated encryption that could provide significantly greater throughput than existing alternatives was desirable for some important applications, such as the routing of messages on the Internet.

Contributors: Two industry cryptographers submitted GCM to NIST: David McGrew (Cisco Systems, Inc.) and John Viega (Secure Software). NIST staff developed most of SP 800-38D from their proposal, with input from NSA on one technical aspect (discussed below). Both the mode submitters and NSA reviewed drafts of SP 800-38D.

Timeline:

- June 2003 CWC mode submitted to NIST.
- Jan. 2004 GCM submitted to NIST.
- May 2005 Request for public comments on the choice between CWC and GCM.
- June 2005 Updated GCM submitted to NIST.
- April 2006 Draft SP 800-38D posted for public comment.
- July 2007 Revised Draft SP 800-38D posted for public comment.
- Nov 2007 SP 800-38 published.

Public engagement: NIST consulted with the public in the choice between GCM and a similar authenticated encryption mode, CWC, that had been submitted earlier. Public feedback, including public comments on the first draft of SP 800-38D, identified several significant technical issues. An extensively revised draft was released for public review prior to its finalization and publication.

Major Decisions: NIST was interested in GCM because of its performance properties. The public review identified several technical issues, including significant security concerns. In particular, GCM had a severe practical vulnerability to a plausible form of "misuse," if the nonce parameter was repeated in violation of the requirements of the mode; the authentication assurance was relatively weaker than comparable modes in other respects as well. NIST considered the issues and decided to proceed with GCM after developing appropriate guidance on these issues.

The text in Appendix C of SP 800-38D, in connection with the use of short authentication tags, was developed jointly with NSA. The rest of the publication, including the extensive guidance in connection with the uniqueness requirement on the nonce, was developed by the NIST staff.

NIST Special Publication (SP) 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices

Scope: SP 800-38E approves the XTS-AES mode of the AES block cipher by reference to IEEE Std. 1619-2007, subject to one additional requirement on the maximum length of the data unit.

Purpose/identified need: The XTS-AES mode protects the confidentiality of data on block-oriented storage media, such as external disk drives. The mode does not provide authentication, in order to avoid expansion of the data; within this context, it does provide various incremental advantages over the other approved modes for confidentiality. For example, the mode provides better protection against manipulation of the encrypted data, i.e., "cut-and-paste" attacks.

Contributors: The Security in Storage Working Group (SISWG) of the IEEE P1619 Task Group developed the XTS-AES specification in IEEE Std. 1619. The Chair of SISWG, Matt Ball, submitted XTS-AES to NIST. Both the SISWG and NSA reviewed drafts of SP 800-38E.

Timeline:

Nov. 2007	Draft IEEE Std 1619 submitted for internal NIST consideration.
April 2008	Request from NIST to IEEE to allow public review of the specification.
May 2008	Request for public comment on a proposal to approve XTS-AES.
April 2009	Submission of follow-up comments/responses from Matt Ball.
Aug 2009	Draft SP 800-38E posted for public comment.
Jan. 2010	SP 800-38E published

Public engagement: The XTS-AES mode was developed by the IEEE, an industry standards development organization. NIST received detailed public comments on its proposal to approve XTS-AES by reference, including extensive follow-up comments/responses from the chair of the working group, and, later, a letter of support from Hitachi GST. NIST also received public comments on draft SP 800-38E before it was finalized and published.

Development process overview: In August of 2005, NIST informally signaled to the SISWG a willingness to consider the approval of a special-purpose mode for encryption of data in storage if the mode was sound and enjoyed broad industry support. When the draft IEEE Std. 1619 was nearing publication, the SISWG submitted XTS-AES for internal NIST consideration.

NIST decided that the mode was worth proposing for approval, and that referencing the mature, existing IEEE standard was preferable to developing an independent specification. IEEE agreed to NIST's request to publish a relevant excerpt of IEEE Std. 1619-2007, free-of-charge, for a period of public review; afterward, the Standard would only be available from IEEE for a fee. Although the public comments did contain some technical objections, including doubts about the value of its security properties in the expected use-cases, NIST ultimately decided to support the SISWG and proceed with the development of SP 800-38E to approve XTS-AES by reference.   Based on the public comments, NIST included a provision limiting the maximum size of data units to 2^{20} AES blocks. This limit was recommended, although not required, in IEEE Std. 1619-2007.

NIST Special Publication (SP) 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

Scope: SP 800-38F describes cryptographic methods that are approved for "key wrapping," i.e., the protection of the confidentiality and integrity of cryptographic keys, including the specification of three deterministic authenticated encryption functions, KW, KWP, and TKW.

Purpose/identified need: After AES was selected, NIST requested NSA to provide a method for protecting keys. The chair of the IETF S/MIME working group also requested that NIST approve a mode for key wrapping, to facilitate the digital “transport” of cryptographic keys. Years later, there was also a need to clarify which other methods for authenticated encryption were approved for key wrapping.

Contributors: NSA developed the “AES Key Wrap,” and, years later, a variant with a padding scheme, which became KW and KWP in SP 800-38F. The Telecommunications Industry Association developed the Over-the-Air-Rekeying (OTAR) protocol for digital radio, which included the TKW variant of KW. NIST staff developed SP 800-38F, with review by NSA.

Timeline:

- 2001 Specification of KW posted on NIST website.
- Nov. 2002 OTAR protocol published.
- Nov. 2004 Public review requested on Draft American National Standard (ANS) X9.102 specifying KW variants.
- 2005 Rogaway and Shrimpton’s analysis submitted to ASC X9; the analysis was later published.
- Nov. 2005 Rogaway and Shrimpton’s SIV mode submitted to NIST; the mode was later revised.
- 2008 ANS X9.102 published, specifying variants of KW.
- Aug. 2009 RFC 5649 published, specifying an equivalent mode to KWP.
- Aug. 2011 Release of Draft SP 800-38F for public comment.
- Dec. 2012 SP 800-38F published.

Public engagement: Phillip Rogaway (University of California, Davis) and Tom Shrimpton (Portland State University) analyzed the variants of KW in Draft ANS X9.102, and submitted an alternative – the SIV mode. NIST received public comments on Draft SP 800-38F.

Major Decisions: NIST requested a key wrapping technique from NSA and posted the NSA’s specification of the mode, which NIST ultimately named KW in SP 800-38F, on the NIST website. On that basis, the CMVP allowed the use of KW by vendor affirmation, as well as the TKW variant in OTAR.

NIST served as the editor of the key-wrapping standard within Accredited Standards Committee X9 (ANS X9.102) and developed variants of KW that incorporated a formatting/padding scheme. Rogaway and Shrimpton's public analysis of those variants identified several technical objections that also applied to KW, including the lack of a formal security model or proof of security properties.

Although Rogaway and Shrimpton's SIV mode was arguably preferable on technical grounds, NIST had intended to approve KW from its inception and did not want to undercut vendors who had implemented KW when no other methods for authenticated encryption had yet been approved. NIST was satisfied with the conservative security design of KW and did not regard its relatively slow performance as onerous for the intended applications in key management. NIST included KWP instead of the padding variant in ANS X9.102 in order to support NSA's applications.

NIST Special Publication (SP) 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

Scope: SP 800-56A specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman (DH) and Menezes-Qu-Vanstone(MQV) key-establishment schemes.

SP 800-56A specifies key-establishment schemes based on two classes of asymmetric primitives: Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV). Each scheme is characterized by the primitives it uses, over either a finite field or an elliptic curve, as well as by keys contributed by each party (static, ephemeral, or both static and ephemeral). SP 800-56A originally specified the key lengths and subgroup sizes for security strengths of 80, 112, 128, 192, and 256 bits. For 80 and 112 bits of security strength, both the finite field key lengths/subgroup sizes and the elliptic curve key length were specified, while for security strengths of 128, 192, and 256 bits, only the elliptic curve key lengths were specified. SP 800-56A Rev. 2 removed key length for the 80-bit security strength.

Purpose/identified need: The DH and MQV schemes were originally specified in American National Standard (ANS) X9.42 (over finite fields) and ANS X9.63 (over elliptic curves). The ANS X9.42 and ANS X9.63 Standards were developed in Accredited Standards Committee X9, under subcommittee X9F, working group X9F1. Because ANS X9.42 and X9.63 omitted several requirements that NIST considered essential for Federal government use of DH and MQV key-agreement schemes, NIST decided to create a publication based on the X9 standards that addressed NIST's concerns.

Contributors: SP 800-56A was developed by a team composed of NIST and NSA staff and contractors.

Timeline: The development of this document began in 2001. The first version was published in March 2006. In March 2007, a minor change was made for clarification and a new version was published. A second revision was begun in 2010. SP 800-56A Rev. 2 was published in May 2013. The major revisions are listed in Appendix D of the document.

Public engagement: The original X9 standards, ANS X9.42 and ANS X9.63, were developed for the financial industry in the late 1990s and completed in 2001 as part of a public process. SP 800-56A adopted schemes specified in the X9 standards, and each version of 800-56A was released for public comments, and the comments were resolved. The comments received on SP 800-56A Rev. 2 are published at http://csrc.nist.gov/publications/PubsSPs.html.

Major decisions: One of the concerns during the development of SP 800-56A was interoperability. The X9 Standards allowed too many key lengths, too many key-agreement schemes, and allowed the domain parameters used for static keys to be different from those used for ephemeral keys. In SP 800-56A, key lengths are explicitly listed for each appropriate security strength, the number of key-agreement schemes has been reduced, and the same domain parameters are to be used for both static and ephemeral keys when both types are used in a single key-agreement transaction. In addition, the key lengths over finite fields for security strengths higher than 112 bits are not included because the required key lengths would be impractically long. For instance, in order to provide 256 bits security strength, a public key size of at least 15,360 bits would be required. For the higher security strengths, the use of elliptic curve cryptography is preferred because much shorter key lengths are needed

A second concern was that insufficient assurances were required in the X9 Standards; in those Standards, only assurance of domain parameter and public-key validity were required. SP 800-56A added requirements for assurance of private-key possession by both a key-pair owner and a relying party, assurance for the arithmetic validity of the public key and assurance of pair-wise consistency by a key-pair owner.

SP 800-56A also included additional requirements concerning the generation and use of the nonces required for key derivation and key confirmation, as well as additional modifications and restrictions on the key-derivation phase of key agreement and a different key-transport scheme than was provided in the X9 Standards.

SP 800-56A originally specified a one-step key-derivation function that used a hash function. In SP 800-56A Rev. 2, the one-step key derivation method was modified to use either a hash function or keyed-hash message authentication code (HMAC). A two-step key-derivation procedure specified in SP 800-56C was also included as an approved key-derivation method, as well as the key-derivation functions specified in SP 800-135.

NIST SP 800-131A , which indicates acceptable key lengths for the Federal government, disallowed key lengths associated with the 80-bit security strength after 2013. Therefore, key lengths supporting the 80-bit security strength were removed in SP 800-56A Rev. 2.

During each of the public comment periods of SP 800-56A, some comments expressed security concerns about the selected key-establishment schemes and suggested that key-establishment protocols that provide provable security be included. However, the scope of SP 800-56A was to specify basic key-establishment schemes for different protocols and applications, and it was recognized that some of the security features are relying on the next level of protocols to provide them. The decision was made to stay within the original scope.

NIST Special Publication (SP) 800-56B: Recommendation for Pair-Wise Key Establishment Schemes: Using Integer Factorization Cryptography

Scope: SP 800-56B specifies key-establishment schemes using integer factorization cryptography.

In particular, it specifies key agreement and key transport using the Rivest-Shamir-Adleman (RSA) encryption algorithm. In a key-agreement scheme, both parties contribute to the derived keying material, through an exchange of one encrypted secret value and one public value, or an exchange of two encrypted secret values. In a key transport scheme, one party selects a secret key and transports it to another party.

Purpose/identified need: SP 800-56B is based on American National Standard (ANS) X9.44, which was developed in Accredited Standards Committee X9, under subcommittee X9F, working group X9F1. NIST developed SP 800-56B in order to address concerns with X9.44 (see the Major decisions section below).

Contributors: SP 800-56B was developed by a team composed of NIST and NSA staff and contractors.

Timeline: The development of this document began in 2006, and the first version was published in August 2009. The August 2009 version of SP 800-56B specifies key lengths for security strengths of 80 bits and 112 bits. A revision of the document began in 2012. SP 800-56B Rev.1 was released for public comments in March 2014. The draft of SP 800-56B Rev.1, which was released in March of 2014, adds a key length for the 128-bit security strength and removes the key length for the 80-bit security strength.

The major revisions are listed in Appendix D of the document.

Public engagement: ANS X9.44 was developed for the financial industry and completed in 2007 as part of a public process. The original version of SP 800-56B was provided for public comment in 2008 and finalized in 2009. The draft of SP 800-56B Rev. 1 is currently available for public comment.

Major decisions: Several improvements to ANS X9.44 that NIST considered necessary for Federal government use of the RSA key-establishment schemes were included in SP 800-56B. These included 1) a requirement that the public exponent *e* be at least 65,537, whereas ANS X9.44 allowed smaller values (e.g., a value of *e* =3), 2) additional requirements on the generation and use of nonces, 3) several additional requirements on the key-derivation phase of the key-agreement process, 4) more stringent key-confirmation requirements, and 5) the inclusion of an additional key-agreement scheme.

The August 2009 version of SP 800-56B only specified key lengths of 1024 bits (for 80 bits of security strength) and 2048 bits (for 112 bits of security strength), while ANS X9.44

specified key lengths for seven security strength levels: 80, 112, 128, 150, 174, 192, 256 bits. Security strengths higher than 112 bits were not included in the original version of SP 800-56B because the key lengths needed to support the higher security strengths are impractically long. For instance, in order to provide 256 bits of security strength, a public-key size of at least 15,360 bits is required. For the higher security strengths, the use of elliptic curve cryptography is preferred because much shorter key lengths are needed.

NIST SP 800-131A , which indicates acceptable key lengths for the Federal government, disallowed key lengths associated with the 80-bit security strength after 2013. Therefore, the key length supporting the 80-bit security strength (i.e., 1034 bits) was removed in SP 800-56B Rev. 1. However, a key length of 3072 bits was added to SP 800-56B Rev. 1 to support a security strength of 128 bits.

SP 800-56B originally specified a one-step key-derivation function that used a hash function. In SP 800-56B Rev. 1, the one-step key-derivation method was modified to use either a hash function or a keyed-hash message authentication code (HMAC). A two-step key-derivation procedure specified in SP 800-56C was also included as an approved key-derivation method, as well as the key-derivation functions specified in SP 800-135.

NIST Special Publication (SP) 800-56C: Recommendation for Key Derivation through Extraction-then-Expansion

Scope: SP 800-56C specifies a technique for deriving keying material from a shared secret through an extract-and-expand procedure during key establishment. Key establishment schemes are specified in NIST Special Publications 800-56A and 800-56B.

Purpose/Identified Need: The key derivation functions specified in NIST SP 800-56A (2007 and earlier version) and NIST SP 800-56B (2009 version) are one-step procedure using a hash function. The two-step key derivation approach was proposed in research literature, such as "Cryptographic Extraction and Key Derivation: The HKDF Scheme," which was presented by Hugo Krawczyk at Crypto 2010, and was also specified in IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)". IETF RFC 5996 and 5246 adopted this approach in Internet Key Exchange (IKEv2) and Transport Layer Security (TLS). Including this method as a NIST-approved key-derivation method was in response to industry demand and with academia support.

Contributors: NIST personnel, with review by NSA.

Timeline: The development of this document began in February 2010, and it was published in November 2011.

Defined cryptographic algorithms/modes/schemes: SP 800-56C specifies a two-step key derivation method. The first step is called "randomness extraction". It extracts a binary string, called key-derivation key, from a "shared secret" established through a scheme specified in SP 800-56A or 800-56B. The second step is called "key expansion". This step is used to derive keying material with the required length from the key-derivation key.

Public engagement: The two-step key derivation method was published as a research result in the cryptography literature. It has been adopted by other standard bodies. DRAFT SP 800-56C was released for public comment on September 23, 2010. The received public comments were published on the NIST web site. After the comments were resolved, a new draft was released for a second public comment period on July 12, 2011. The official SP 800-56C was published in November 2011.

Major decisions: When SP 800-56A was under revision in 2009, the need to include the two-step key derivation method was considered and accepted by the editing team. There were two ways to include the two-step key derivation method. The first is to include it in both 56A and 56B. The second is to generate a stand-alone special publication for two –step key derivation so that 56A and 56B can refer to it. In order to get the public attention for the newly introduced key derivation method and have it fully reviewed, it was decided that the two-step key derivation method be specified in 56C as a separate document.

NIST Special Publication (SP) 800-57: Recommendation for Key Management

Scope: SP 800-57 was developed in three parts. Part 1 provides general guidance about cryptographic algorithms and the use and protection of the keys associated with them. Part 2 provides best practices for a key-management organization. Part 3 provides guidance for the use of commonly used infrastructures, protocols and applications, such as the PKI, IPsec, TLS, S/MIME, and DNSSEC.

Purpose/identified need: At the end of the 20th century, the importance of cryptography in protecting communications became crucial to the public and the Federal government with the increasing use of the Internet. However, very little guidance was publicly available about the key management necessary to use cryptography. NIST began an effort to provide this information with a series of projects designed to raise awareness of the correct use of this technology to protect both communicated and stored data. SP 800-57 was developed as a foundational series of guidance documents.

Contributors: These documents were developed by a team consisting of NIST and NSA personnel.

Timeline: This series of publications was begun in 2002. Part 1 was first published in 2005, and revised in 2006, 2007 and 2012. Part 2 was published in 2005, and has not been modified to date. Part 3 was published in 2009; a new revision of Part 3 is currently available for public comment.

Public engagement: NIST conducted workshops in 2000 and 2001 to kick-off the project. Public comments were requested prior to completion of each document and any subsequent revisions. Presentations were provided to several organizations, including American Standards Committee (ASC) X9F and X9F1. The public has continued to be involved, particularly with regard to the security strengths for the approved algorithms and keys, and the time frames for secure use. As the public became more knowledgeable about the cryptographic algorithms available, they began to develop attacks on both the algorithms and how they were used. Revisions to the SP 800-57 documents were developed to address these threats. This effort has involved continual interaction with the public and reviewing their work to provide the best advice as soon as possible.

Major decisions: Key management is a vast topic that is essential to cryptographic security, and very little guidance was publicly available. The first decisions had to do with how to educate a relatively naïve public about the importance of key management and what needs to be considered when using cryptographic algorithms. What is necessary to explain about cryptoperiods without being too prescriptive? What needs to be considered when managing a key from its initial generation until its destruction? What are the security strengths associated with different algorithms and key sizes, and how long can they be considered to be secure? Can keys be backed up and archived, and under what circumstances? What is necessary for their recovery? What is needed to set up a key management system, and how can commonly used applications and protocols be used securely? The development of these documents involved codifying the key management guidance learned over 30 - 40 years or more by the authors.

The guidance provided in SP 800-57 that has had the most impact on cryptographic applications is the "assignment" of security strengths to the approved cryptographic algorithms and key lengths and the estimated time frame during which it will provide adequate security. In some cases, the security strengths differ by their application. For example, a hash function used during digital-signature generation has a very different security strength than when the same hash function is used for the generation of message authentication codes (i.e., using the HMAC construction). Most of these security strengths were commonly accepted values held by the cryptographic community. Others were added later (e.g., the values for HMAC and KDFs) as more analysis was performed.

With respect to the time frames for secure use of the approved algorithms and key lengths, the original end-date estimates were based on papers by Arjen Lenstra and analysis by NSA and others, and allowed a margin-of-error in case the estimates were too far in the future (e.g., a practical attack on an algorithm and its key length was possible before the estimated end date). A revision of those estimates was published in a subsequent revision of SP 800-57, based on further analysis by Lenstra and others.

All of the security strength and time-frame assignments were provided for public comment and are subject to change if a practical attack on a given algorithm, key length or application is found. For this reason, NIST encourages using SP 800-57 as the authoritative document for these values (i.e., using SP 800-57 as a reference for this information), rather than including these values in other documents. If a change is warranted because of subsequent analysis, providing them in a single document will then apply to all documents that reference SP 800-57, without the need to modify that information in the referencing documents.

NIST Special Publication (SP) 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

Scope: NIST SP 800-67 specifies the Triple Data Encryption Algorithm (TDEA), including its cryptographic engine, the Data Encryption Algorithm (DES). TDEA is a block cipher algorithm approved to protect Federal information when used in a mode of operation defined in NIST SP 800-38.

Purpose/identified need: Federal Information Processing Standard (FIPS) 46, the Data Encryption Standard (DES), which was approved in 1977, specified an encryption algorithm with a 56-bit key. However, faster logic and computers made 56-bit key exhaustion attacks practical by the mid 1990s. American National Standard (ANS) X9.52, Triple Data Encryption Algorithm Modes of Operation (called TDEA), was a response to these attacks. ANS X9.52 referenced FIPS 46 to define the DES "engine" of TDEA and was approved by ANSI in 1998. FIPS 46-3, approved in 1999, included TDEA by reference to ANS X9.52. NIST wanted to withdraw 56-bit DES (as specified in FIPS 46) in favor of TDEA, and ANS X9.52 was unsatisfactory as a reference, since it did not specify the DES "engine" itself, had too many modes of operation, and included a DES-compatible version (which was no longer considered secure). NIST developed SP 800-67 to fully specify TDEA, including the DES engine, to allow only two and three-key versions of TDEA and to limit the use of the DES engine to a component function of TDEA.

Contributors: NIST personnel.

Timeline: NIST published SP 800-67 in May 2004. In May 2008, an update modified a list of weak keys, and in January 2012, SP 800-67 was revised to update references and clarify text in the document.

Public engagement: NIST posted the draft of SP 800-67 on the NIST Computer Security Resource Center web site (csrc.nist.gov) for a 60-day review period. NIST also had informal discussions with the American Standards Committee X9F1, which developed ANS X9.52. Communications were also received from the public whenever needed corrections were identified. The 2012 revision was also provided for public review and comment.

Major decisions: Since SP 800-67 was developed after approval of the Advanced Encryption Standards (AES) specified in FIPS 197, SP 800-67 was developed as an SP, rather than a FIPS to encourage the use of the Advanced Encryption Standard (AES) that was more secure and cost-efficient alternative.

NIST Special Publication (SP) 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Scope: SP 800-90A was originally published as SP 800-90. This document specifies mechanisms for the generation of pseudorandom bits using deterministic methods. It does not specify the source of entropy, nor the construction of a complete random-bit generator using one or more entropy sources and the mechanisms specified in SP 800-90A. These topics will be addressed in SP 800-90B and SP 800-90C, which are under development.

Purpose/identified need: Random numbers are required by cryptographic algorithms, and depend on their quality for security. The development of a random number standard began within American Standards Committee X9. However, since the review process within ANSI is limited, SP 800-90/90A was developed in order to gain a wider review of the random number generation documents than could be provided by the ANSI process.

The mechanisms include specifications for the instantiation, reseeding, and un-instantiation of a Deterministic Random Bit Generator (DRBG), as well as the generation of pseudorandom bits. The algorithms supported consist of two algorithms based on the use of approved hash functions (the Hash_DRBG and the HMAC_DRBG), one algorithm based on the use of an approved block-cipher algorithm (CTR_DRBG) and a fourth algorithm based on elliptic curves (the Dual_EC_DRBG). The revision currently available for public comment has removed the Dual_EC_DRBG.

Contributors: Two of the four algorithms currently specified in SP 800-90A were developed by NIST, and the other two by NSA.

Timeline: This project was begun by NIST in 1998 in coordination with American Standards Committee X9 as American National Standard (ANS) X9.82. SP 800-90 was first published by NIST in 2007, and revised in 2008 and 2012; another revision of SP 800-90A is currently available for public review. A version of SP 800-90 was published as ANS X9.82, Part 3 in 2008, but has not been revised to date.

Public engagement: Public workshops were held in 2004 and 2012. Public comments were requested for each of the versions of SP 800-90/90A using CSD- maintained databases of interested parties and databases maintained by the standards groups in which the CSD participates. In addition, public comments were requested in 2013 in light of concerns about the Dual_EC_DRBG. Comments received for the last public-comment period are provided at http://csrc.nist.gov/publications/PubsDrafts.html. Both SP 800-90/90A and ANS X9.82, Part 3 were discussed at several ASC X9F1 subcommittee meetings. In addition, an ITL Bulletin was published in 2013.

Major Decisions: Originally, ANS X9.82, Part 3 contained a total of five DRBG algorithms: two based on hash functions, one based on block ciphers, and two based on number-theoretic problems. However, one of the hash-based algorithms and one of the number-theoretic algorithms were removed to decrease the number of approved algorithms. When SP 800-90/90A was developed, the hash-based algorithm that had been excluded from ANS X9.82 (i.e., the Hash_DRBG) was included because of a perceived need.

During the development of ANS X9.82 and SP 800-90/90A, there was concern about the elliptic-curve points proposed for the Dual_EC_DRBG and the number of bits of the output to be used. As a result, the proposed points were specified for validation purposes, and recommended for general use in order to avoid using potentially weak points. However, a method for the generation of verifiably random points was included in the documents.

With respect to the number of bits of output to be used by the Dual_EC_DRBG, a discussion of the issue was included in an appendix, and an example provided for the use of the P-256 curve. For this example, at least 13 bits needed to be truncated, and a truncation of 16 or 17 bits was recommended for ease of implementation.

Because of recent concerns about the security of the Dual_EC_DRBG, NIST has decided to remove it from SP 800-90A.

NIST Special Publication (SP) 800-106: Randomized Hashing for Digital Signatures

Scope: NIST SP 800-106 specifies a randomization method to improve security strengths of hash functions used in digital signature applications. This method is approved for use with any approved hash algorithms in FIPS 180-4.

Purpose/identified need: By 2005, serious attacks on SHA-1 and other commonly-used hash functions had been published, demonstrating an alarming weakness in the collision-resistance strength of the hash function and questioning the community's understanding of hash function design. Digital signature applications using SHA-1 were widely used in providing authentication, integrity protection and non-repudiation services for electronic communication and data. NIST immediately started to search for solutions to deal with this serious security issue.

Contributors: NIST and NSA (NSA reviewed the draft publication and provided technical comments and discussions). The specification is based on the scheme proposed in 2006 by Shai Halevi and Hugo Krawczyk.

Timeline: At the Crypto 2006 conference at the University of California, Santa Barbara campus, a randomized hashing method was presented. NIST began to analyze the method and alternatives that could provide additional protection against collision attacks than simply using a hash function directly.

NIST published SP 800-106 in February 2009.

Public engagement: NIST posted the first draft of SP 800-106 for a 60-day public comment period in July 2007 on the NIST Computer Security Resource Center web site. After the comment period, NIST reviewed the comments and revised the specification. NIST then posted the second draft specification for another 60-day public comment period in August 2008. After reviewing the comments received, NIST revised the specification and published the official specification in February 2009.

Major Decision(s): NIST developed a specification based on the scheme proposed by Shai Halevi and Hugo Krawczyk in 2006. This modified scheme was intended to provide better efficiency, adoptability and interoperability than the original scheme. During the development of the specification, NIST had many discussions with Hugo Krawczyk and other cryptographers who provided comments and analyzed our proposed specification.

Randomized hashing is designed for situations where one party, the message preparer, generates all or part of a message to be signed by a second party, the message signer. This method would be misused if the message signer generates all portions of the message. This misuse could weaken the security provided by the digital signature. In response to this concern, NIST included a warning not to use randomized hashing in those situations.

NIST Special Publication (SP) 800-108: Recommendation for Key Derivation Using Pseudorandom Functions

Scope: SP 800-108 specifies techniques for deriving additional keying material from a secret key using pseudorandom functions (PRFs).

SP 800-108 specifies three key derivation functions (KDFs) based on a PRF. A PRF can be the Keyed-Hash Message Authentication Code (HMAC) with an approved hash function or the CMAC mode for authentication with the Advanced Encryption Standard (AES). Three key-derivation functions are constructed using a PRF in a counter mode, a feedback mode, and a double-pipeline iteration mode.

Purpose/identified need: Before SP 800-108 was developed, NIST specified approved key-derivation functions in SP 800-56A. These KDFs are all based on an approved hash function, and use a “shared secret” computed during a key-agreement process (e.g. an integer in binary representation) and other information in a particular order and format as inputs to derive additional keys or keying material. However, some wireless applications, such as protocols in IEEE 802.11, needed to derive additional keys from a cryptographic key, rather than from a “shared secret”. Furthermore, some KDFs adopted by the IETF specify the inputs in a different order.

Contributors: NIST personnel, with review by NSA.

Timeline: The development of this document began in 2006, and it was published in November 2008. A revision was published in October 2009.

Public engagement: SP 800-108 was a response to industry demand. The instances of the KDFs specified in this document had been developed in other standards bodies. For example, IEEE 802.11 specified a counter mode for wireless applications. IETF RFC 5295 specified a feedback mode for the derivation of root keys. The KDF specified in IETF RFC 4346 and RFC 5246 for Transport Layer Security (TLS) is called double-pipeline mode in SP 800-108. Public comment was requested on SP 800-108 prior to its finalization. The received comments were published on the NIST web site.

Major decisions: The decision on developing SP 800-108 was made based on industry demand. In particular, the three KDFs, using counter mode, feedback mode and double-pipeline mode, were selected to cover the KDFs specified in the IEEE 802 and IETF standards. The options for the PRF, namely HMAC and CMAC, use the existing implementations of cryptographic primitives in hardware and software. For instance, HMAC uses a hash function, while CMAC uses a block cipher.

NIST Special Publication (SP) 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

Scope: SP 800-131A provides specific guidance for transitioning to the use of stronger cryptographic keys and more robust algorithms.

Purpose/identified need: At the start of the 21st century, NIST began the task of providing cryptographic key management guidance. SP 800-57, Part 1 (Recommendation for Key Management) was the first document produced in this effort, and included a general approach for transitioning from one algorithm or key length to another that provides a more adequate level of security. However, it became apparent in 2009 that many of the Federal agencies were not planning for the necessary transitions, and the guidance provided in SP 800-57 might not provide sufficient detail for doing so. SP 800-131A was intended to provide more detail about the transitions associated with cryptography than was provided in SP 800-57, Part 1.

Contributors: NIST personnel.

Timeline: This effort was begun in 2009 with the development of a white paper on "The Transitioning of Cryptographic Algorithms and Key Sizes," which became a NIST Special Publication (i.e., SP 800-131A) in 2010 and was completed in 2011.

Public engagement: The white paper was provided for public comment in 2009. The transition schedule was discussed at a number of forums, including ANSI meetings, workshops and CMVP lab meetings. The draft of SP 800-131A was provided for a general public-comment period.

Major decisions: Transitioning away from the use of already-installed algorithms and key sizes is extremely difficult. For a period of time, some capabilities can remain, while others need to be discouraged or disallowed. In some cases, restrictions need to be imposed to continue the use of a certain algorithm and key size. A categorization needed to be developed to address the range of issues to be addressed and dates assigned for each algorithm and capability. Because Part 1 of SP 800-57 was the go-to document for algorithm security strengths and time frames, it needed to be updated to be consistent with the time frames in SP 800-131A and to reference it for additional details.

NIST Special Publication (SP) 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications

Scope: SP 800-132 specifies a family of password-based key derivation functions (PBKDF) for the derivation of master keys from passwords or passphrases, and to protect electronically stored data and data protection keys. SP 800-132 describes the family of PBKDF algorithms.

Purpose/identified need: Passwords are not suitable for direct use as cryptographic keys. One of the reasons is that user-selected passwords usually have low entropy, and can be quickly recovered by dictionary attacks. The family of password-based key derivation functions specified in this document aims to slow down the dictionary attacks by increasing the time that is needed to test each password.

Contributors: SP 800-132 was developed by NIST personnel based on the PBKDF2 algorithm specified in PKCS #5.

Timeline: NIST posted SP 800-132 in June 2010 for a 30-day public review period. Public comments received were posted on NIST's web site in August 2010. Following the adjudication of the public comments, and the clearance by the Office of the General Counsel and the NIST Washington Editorial Review Board, SP 800-132 was published on December 15, 2010.

Public engagement: NIST posted the Draft SP 800-132 on NIST's Computer Security Resource Center web site (csrc.nist.gov) in June 2010 for a 30-day review period. NIST also had informal discussions with the NSA.

Major Decisions: PBKDF family was based on an algorithm specified in PKCS #5, which was also published in RFC 2898 by the Internet Engineering Task Force (IETF). In PKCS #5, the algorithm was referred to as PBKDF2, and it used HMAC with SHA-1 as the underlying pseudorandom function. In SP 800-132, PBKDF2 is referred to as PBKDF, and it can use HMAC with any approved hash function as the underlying pseudorandom function.

The major decision in SP 800-132 was the selection of the iteration count. NIST initially considered setting the minimum value to 1000. Later, NIST decided to recommend the iteration count to be as large as possible, without providing a minimum value. This decision was made considering various capabilities of target environments.

NIST Special Publication (SP) 800-133: Recommendation for Cryptographic Key Generation

Scope: SP 800-133 discusses the generation of the cryptographic keys for use with NIST-approved cryptographic algorithms. SP 800-133 includes a general method for generating symmetric keys or the random value needed to generate an asymmetric key pair using an approved random bit generator.

Purpose/identified need: Several of NIST's cryptographic-algorithm publications require the use of keys generated from random values, but often do not provide specific information about how to do so. A FIPS 140-2 Implementation Guideline (IG) section was developed by the Cryptographic Module Validation Program (CMVP) to address this issue, but a more prominent place for this guidance was needed. SP 800-133 was developed to provide a single document for key generation that includes the guidance provided in the FIPS 140-2 IG, as well as guidance for the generation of keys for other purposes.

Contributors: NIST personnel, with review by NSA.

Timeline: The development of this document began in 2008, and was completed in 2012. The FIPS 140-2 was originally published in 2009. Draft SP800-133 was published in August 2011 for a 60-day comment period, and was finalized in December 2012.

Public engagement: During the development of the FIPS 140-2 IG, the labs used by the CMVP were asked to comment on the content of the IG. NIST requested public comments on the draft Special Publication prior to finalizing the document.

Major decisions: SP 800-133 specifies where the keys need to be generated (i.e., within a FIPS 140-compliant cryptographic module designated as a key-generating module), the use of an approved random bit generator that supports the required security strength needed for a key, and specifies or refers to methods for generating or deriving the appropriate keys for different purposes, e.g. for the generation of digital-signature key pairs.

NIST Special Publication (SP) 800-135: Recommendation for Existing Application-Specific Key Derivation Functions

Scope: SP 800-135 discusses and approves of several key-derivation functions (KDFs), which do not strictly conform to the approved key-derivation functions specified in the SP 800-56 series. In particular, the publication approves the KDFs used by the IKE, TLS, SSH, SRTP, and SNMP protocols, the KDF specified for Trusted Platform Modules, and the KDFs specified in ANS X9.42-2001 X9.63-2001.

Purpose/identified need: NIST specified key-derivation functions in the SP 800-56 series for deriving keying material from the shared secret computed during a key-agreement transaction. However, many widely used protocols/applications had different key-derivation functions than those approved in SP 800-56A and B. NIST reviewed these protocols/applications and the contexts in which each of these key derivation functions is used to determine whether or not they provide adequate security.

Contributors: NIST staff developed the publication, receiving comments on internal drafts reviewed by the NSA.

Timeline: NIST published SP 800-135 in December 2010 and its revision in December 2011.

Public engagement: NIST posted a draft of SP 800-135 for a 30-days public comment period in September 2010. After reviewing the received comments, NIST revised the document and published the first official version of the document in December 2010. NIST later revised the document to improve some informative details in the document. NIST then published the document as SP 800-135 Revision 1 in December 2011.

Major decision(s): The protocols that using the KDFs discussed in this document are widely used. However, these KDFs did not comply with the specifications in the SP 800-56 series. Therefore, NIST needed to review these KDFs and determine whether or not they could provide adequate security in these protocols, and what restrictions would be appropriate (e.g., the use of NIST-approved hash functions). None of the comments received raised any security concerns about the uses of these functions.