X9 SD-34-2020

Registry of Approved Cryptographic Resources for Financial Services Industry Standards

ASC X9 approval dates:

Original: May 3, 2004; Revision 1: April 19, 2006; Revision 2: January 4, 2010; Revision 3: February 14, 2020.

1. Background and Justification

In addition to developing cryptographic techniques within its own standards, the Accredited Standards Committee X9 (X9) relies upon standards and techniques from other standards-developing organizations as resources when developing its own standards. Appropriate cryptographic techniques may be found in standards produced by such organizations as the National Institute of Standards and Technology (NIST), the Institute of Electrical and Electronics Engineers (IEEE), and the Internet Engineering Task Force (IETF). In this document the term "resource" is defined to be a cryptographic standard, a National Institute of Standards and Technology (NIST) Special Publication, or a cryptographic technique specified in a standard or NIST Special Publication that is used to support X9 standards.

Many X9 standards rely upon the symmetric block ciphers, Triple Data Encryption Algorithm (TDEA) and the Advanced Encryption Standard (AES). Although fully specified in external documents, these algorithms, along with the modes of operation specified in the NIST Special Publication (SP) 800-38 series are important tools that provide confidentiality protection for financial data. In addition, X9 also relies upon hashing and message authentication algorithms from external resources that support X9 digital signature and key establishment standards.

Rather than re-write, replicate or repeat algorithms or other general cryptographic techniques within the contents of its Financial Services Industry American National Standards, ASC X9 has developed a *Registry* or listing of acceptable resources. Since new resources are continually being developed (by a variety of general technical standards producers), the *Registry* of appropriate resources needs to be a living document that provides for the addition and deletion of resources, as appropriate.

Thus, the *Registry* and the Approved cryptographic resources contained within it may be referenced in the same manner as other normative or informative references in X9 standards. This allows for the addition of new resources to the *Registry* without the need to revise the standard itself. For example, suppose that an X9 standard required that an

Approved symmetric-key encryption mode of operation be used to encrypt financial data, and that when the standard was written, only four such modes existed and were referenced by the *Registry*. Later, three additional modes are added to the *Registry*. Since the standard referenced the modes in the *Registry*, there is no need to update that standard or any other standards written in a similar fashion.

While a reference in an X9 standard only indicates that the authors of the standard believe that the reference is of value to, or required by, the reader, new resources placed in the *Registry* undergo a full X9F and X9 ballot. Therefore, a reference to a resource in the *Registry* indicates that the resource has been Approved by both the organization that produced the reference and by X9 itself.

2. Purpose of the *Registry*

This Registry is intended as a resource for approved references in an X9 Standard. It should be noted that the purpose of the *Registry* is not to specify all possible existing standards resources. Rather, the intent is to specify only the resources that are approved for reference in X9-developed cryptographic standards.

An Approved resource is one that is either:

- Specified as (or within) a current X9 standard, or
- Listed in the X9 *Registry*.

In some cases, it is desirable to approve an entire resource for X9 use. For example, one may wish to approve the cryptographic requirements specified in FIPS 140-2, *Security Requirements for Cryptographic Modules*, for those cryptographic modules contained in X9 standards. In other cases, only a specific technique contained within a resource may be approved for use in an X9 standard. The *Registry* permits the listing of either entire resources or specific techniques within a resource.

When applying a specific resource to financial applications, certain industry-specific restrictions and guidance may be appropriate. The *Registry* provides for the specification of financial use, restrictions and guidance that is applicable to the financial sector.

The *Registry* is a changing document. New cryptographic resources are added, and outdated resources are withdrawn The procedures for the management of *Registry* are provided in Annex A. Any X9 standard can make use of a resource listed in the *Registry* by referencing the *Registry* number and unique name in the document under development.

The *Registry* shall be housed in the www.x9.org web-store as SD-34-2020 *Registry* of Approved Cryptographic Resources for Financial Services Industry Standards and be offered free of charge.

3. Registry Information

Each item in the registry includes the following information:

A. Registry number;

B. Unique name for the registered item;

C. An indication of whether the registered item is a Standard, NIST Special Publication, or Technique;

D. The sponsoring group – The X9 committee or submittee that proposed the inclusion of the item into the registry;

E. The item's status – Active or Withdrawn (withdrawn items are no longer approved for use in X9 Standards, but their continued inclusion in the registry is maintained for historical reasons);

F. Dates when the item was entered into the registry Entry and when the item was last updated;

G. Resource citation and date of publication – The document containing the specification for the registered item, along with its last date of publication.

H. Supporting U.S or international body;

I. Financial use – The date by which implementaions using the given algorithm are required to be available any restrictions or guidance for using the registered item. Some entries in this list include the word shall; this does not mean that the item is required to be in an X9 Standard; rather, it is intended as a requirement for those standards that reference the item and those implementations that claim conformance to those standards.

J. Sunrise and sunset dates – A sunrise date is the date by which implementaions using the given algorithm are required to be available; a sunset date is the date by which the use of the given algorithm is disallowed for applying cryptographic protection (e.g., encrypting data); these dates may be included in a future version of the X9 Registry after coordination with the ASC X9 committees;

K. Validation tests and the date when they were published; and

L. Recognized testing program.

4. X9 *Registry* Listing

This *Registry* listing was last updated on 2020/02/14.

Table of Contents

Registry Number	Title	Page
00001	Security Requirements for Cryptographic Modules	5
00002	Advanced Encryption Standard (AES)	6
00003	SHA-1 and the SHA-2 Family of Hash Functions	7
00004	The Keyed-Hash Message Authentication Code (HMAC)	8
00005	Entity Authentication Using Public key Cryptography (WITHDRAWN)	9
00006	Triple Data Encryption Standard (TDES) Modes Validation (WITHDRAWN)	10
00007	Triple Data Encryption Algorithm (TDEA)	12
00008	Block Cipher Modes of Operation	13
00009	Digital Signature Algorithms	15
00010	Recommendation for Key Management Part 1: General Guideline	17
00011	SHA-3 Hash Functions and Extendable Output Functions (XOFs) – New item.	18
00012	KECCAK Message Authention Code (KMAC) – New item.	19
00013	Entropy Sources Used for Random Bit Generation – New item.	20
Annex A	Managing the Registry	22
Annex B	References	25

Registry of Approved Cryptographic Techniques for use in or with Financial Services Industry Standards.

Registry Number:
00001

Unique Name:
Security Requirements for Cryptographic Modules

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Dates of Registry Entry and Last Update:
Registry entry: May 3, 2004
Last Update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 140-2: Security Requirements for Cryptographic Modules, with Change Notices, December 3, 2002

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Implement cryptographic modules as specified in FIPS 140-2.
2. When FIPS 140-2 says, "Approved" or "FIPS-Approved", substitute "Both ASC X9 and FIPS-Approved".
3. The module shall contain at least one algorithm that is both X9-Approved and FIPS-Approved (e.g., AES or SHA-256).
4. Additional algorithms need not be FIPS or X9-Approved if used in a non-FIPS mode.
5. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
Draft Derived Test Requirements for FIPS 140-2 (DTR140).

Recognized Testing Program:
NIST/CSE Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00002

Unique Name:
Advanced Encryption Standard (AES).

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Dates of Registry Entry and Last Update:
Registry entry: May 3, 2004
Last Update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 197: Advanced Encryption Standard (AES), November 26, 2001

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Implement the AES algorithm as specified in FIPS 197.
2. Block cipher modes are specified in Registry Number 00008.
3. The AES algorithm with the implemented key size(s) shall be validated.
4. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
The Advanced Encryption Standard Algorithm Validation Suite (AESAVS).

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00003

Unique Name:
SHA-1 and the SHA-2 Family of Hash Functions

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Dates of Registry Entry and Last Update:
Registry entry: May 3, 2004
Last update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 180-4: Secure Hash Standard (SHS), August 2015.

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST).

Financial Use, Restrictions, and Guidance:

1. Implement hash algorithms as specified in FIPS 180-4.
2. The implemented hash algorithm(s) shall be validated.
3. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on hash usage.
4. SHA-1 has been demonstrated to provide less than 80 bits of security for digital signatures. SHA-1 shall only be used for the generation of digital signatures when backwards compatibility is required and collision resistance is not required. SHA-1 shall not be used in new systems when generating digital signatures that require a collision-resistant hash function. SHA-1 is allowed for the verification of already-generated digital signatures.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
Secure Hash Standard Validation System (SHSVS).

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00004

Unique Name:
The Keyed-Hash Message Authentication Code (HMAC)

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Dates of Registry Entry and Last Update:
Registry entry: May 3, 2004
Last Update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC), July 2008

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Implement HMAC as specified in FIPS 198-1.
2. For limitations of MAC algorithms and information on truncation of the MAC output, see SP 800-107, *Recommendations for Applications Using Approved Hash Algorithms*.
3. HMAC shall be used with an Approved hash algorithm (See Registry Numbers 00003 and 00011).
4. HMAC and the Approved hash algorithm shall be validated.
5. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management and hash algorithm usage.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:

1. The Keyed-Hash Message Authentication System (HMACVS).
2. Hash algorithm shall be validated (see Registry Numbers 00003 and 00011).

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00005

Unique Name:
Entity Authentication Using Public key Cryptography

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F3

Status:
WITHDRAWN ON October 19, 2015. THIS IS NO LONGER A *REGISTRY* RESOURCE

Dates of Registry Entry and Update:
Registry entry: May 3, 2004
Last Update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 196: Entity Authentication Using Public Key Cryptography, February 18, 1997

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Implement the Entity Authentication Protocol as specified in FIPS 196.
2. The signature and hash algorithm shall be Approved by both X9 and NIST.
3. The digital signature and hash algorithm shall be validated.
4. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management, and hash algorithm usage.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
None
Recognized Testing Program:
None

Registry Number:
00006

Unique Name:
Triple Data Encryption Standard (TDES) Modes Validation

Standard, NIST Special Publication, or Technique:
NIST Special Publication; Technique

Sponsor Working Group:
X9F1

Status:
WITHDRAWN ON January 4, 2010. THIS IS NO LONGER A *REGISTRY* RESOURCE

Active (also see Registry Number 00007, *Triple Data Encryption Algorithm (TDEA)*).

Date of Registry Entry and Last Update:
Registry entry: May 3, 2004
Last update: January 4, 2010

Resource Citation and Date of Publication:
SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, March 2012. WITHDRAWN

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. To validate conformance to ANSI X9.52 use the NIST/CSE Cryptographic Module Validation Program TDES validation.
2. For counter mode see NIST SP 800-38A, otherwise implement TDES modes as specified in ANS X9.52.
3. Single key option (DES) should be used for legacy systems only.
4. See NIST Recommendation for Key Management Part 1: General Guideline (SP 800-57-Part1), March 2007, for guidance on key management.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS) Requirements and Procedures plus Multi-block Message Test (MMT). For counter mode, use vendor affirmation verified by an accredited test laboratory.

Recognized Testing Program:

Registry of Approved Cryptographic Techniques for use in or with Financial Services Industry Standards.

NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00007

Unique Name:
Triple Data Encryption Algorithm (TDEA)

Standard, NIST Special Publication, or Technique:
NIST Special Publication

Sponsor Working Group:
X9F1

Status:
Active

Dates of Registry Entry and Last Update:
Registry entry: April 19, 2006
Last update: February 14, 2020

Resource Citation and Date of Publication:
SP 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017.

Supporting US or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. The two-key option shall be restricted to less than 2^{20} block encryptions with the same key.
2. The three-key option shall be restricted to less than 2^{20} block encryptions with the same key.
3. TDEA shall be validated.
4. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
NIST Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS) Requirements and Procedures plus Multi-block Message Test (MMT), March 2012.

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP)

Registry Number:
00008

Unique Name:
Block Cipher Modes of Operation

Standard, NIST Special Publication, or Technique:
NIST Special Publication

Sponsor Working Group:
X9F1

Status:
Active

Date of Registry Entry and Last Update:
Registry entry: April 19, 2006
Last update: February 14, 2020

Resource Citation and Date of Publication:
NIST SP 800-38, *Recommendation for Block Cipher Modes of Operation*:

1. Part A: *Methods and Techniques* (for AES and TDEA).
2. Part A Addendum: *Three Variants of Ciphertext Stealing for CBC Mode* (for AES and TDEA).
3. Part B: *The CMAC Mode for Authentication* (for AES and TDEA).
4. Part C: *The CCM Mode for Authentication and Confidentiality* (for AES).
5. Part D: *Galois/Counter Mode (GCM) and GMAC* (for AES).
6. Part E, *The XTS-AES Mode for Confidentiality on Storage Devices* (for AES).

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Note that an Approved mode does not necessarily support all Approved algorithms. Usage of these modes shall be limited to the algorithms for which they are approved in the specific part of SP 800-38.
2. Implemented modes of operation shall be validated.
3. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:

1. If appropriate, the Advanced Encryption Standard Algorithm Validation Suite (AESAVS); see Registry Number 00002.

2. If appropriate, NIST Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS) Requirements and Procedures plus Multi-block Message Test (MMT), March 2012.

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

***Registry* Number:**
00009

Unique Name:
Digital Signature Algorithms

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Date of Registry Entry and Last Update:
Registry entry: April 19, 2006
Last update: February 14, 2020

Resource Citation and Date of Publication:
FIPS 186-4: Digital Signature Standard (DSS), July 2013

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Implement with an Approved hash algorithm as specified in Registry Numbers 00003 or 00011.
2. FIPS 186-4 references ANS X9.62 for the generation and verification of ECDSA signatures. Since X9.62 has been withdrawn, ECDSA signatures shall be generated and/or verified as specified in Sections 4.1.3 and 4.1.4 of SEC1. ECDSA public keys shall be verified as specified in Section 3.2.2 of SEC1. The underlying elliptic curve should be a curve listed in Appendix D of FIPS 186-4.
3. The implemented digital signature algorithm(s), key size(s) and hash functions shall be validated.
4. Prime numbers shall be validated using either FIPS 186-4 (or a later revision) or ANS X9.80.
5. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management and for guidance on hash algorithm usage.

Sunset and Sunrise Dates: See Section 3, item J.

Validation Tests and Date of Publication:

1. Secure Hash Standard Validation System (SHSVS); May 21, 2014.

2. Secure Hash Algorithm 3 Validation System (SHA3VS);April 7, 2016.
3. Digital Signature Algorithm Validation System (DSAVS);May 10, 2004.

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number:
00010

Unique Name:
Recommendation for Key Management Part 1: General Guideline.

Standard, NIST Special Publication, or Technique:
NIST Special Publication

Sponsor Working Group:
X9F1

Status:
Active

Date of Registry Entry and Last Update:
Registry entry: April 19, 2006
Last update: February 14, 2020

Resource Citation and Date of Publication:
SP 800-57 Part 1, *Recommendation for Key Management Part 1: General*, January 2016, for guidance on key management.

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. SP 800-57-Part1 is written for U.S. Government systems and provides guidance and requirements on key management for public key cryptographic algorithms and symmetric cryptographic algorithms (including AES and TDEA), and estimated maximum security strengths for cryptographic algorithms and time frames for their use.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
None

Recognized Testing Program:
None

Registry Number: New proposed item
00011

Unique Name:
SHA-3 Hash Functions and Extendable Output Functions (XOFs)

Standard, NIST Special Publication, or Technique:
Standard

Sponsor Working Group:
X9F1

Status:
Active

Date of Registry Entry and Last Update:
Registry entry: February 14, 2020

Resource Citation and Date of Publication:
FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, August 2015.

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. The implemented hash functions and/or XOFs shall be validated.
2. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management and for guidance on hash algorithm usage.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:

1. Secure Hash Algorithm 3 Validation System (SHA3VS); April 7, 2016.

Recognized Testing Program:
NIST Cryptographic Algorithm Validation Program (CAVP).

Registry Number: New proposed item
00012

Unique Name:
KECCAK Message Authention Code (KMAC)

Standard, NIST Special Publication, or Technique:
NIST Special Publication

Sponsor Working Group:
X9F1

Status:
Active

Date of Registry Entry and Last Update:
Registry entry: February 14, 2020

Resource Citation and Date of Publication:
SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*, December 22, 2016.

Supporting U.S .or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. KMAC shall be validated.
2. SP 800-185 includes other algorithms in addition to KMAC; these algorithms are not jncluded ion this registry entry.
3. See Registry Number 00010, *Recommendation for Key Management Part 1: General*, for guidance on key management and for guidance on hash algorithm usage.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:
None

Recognized Testing Program:
None

***Registry* Number:** New proposed item
00013

Unique Name:
SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation

Standard, NIST Special Publication, or Technique:
NIST Special Publication

Sponsor Working Group:
X9F1

Status:
Active

Date of *Registry* Resource:
February 14, 2020

Resource Citation and Date of Publication:
SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018

Supporting U.S. or International Body:
National Institute of Standards and Technology (NIST)

Financial Use, Restrictions, and Guidance:

1. Entropy source implementations shall be validated.
2. The behavior of the noise source shall follow a stationary distribution.
3. Conditioning components that are not listed as vetted components in SP 800-90B shall require additional entropy validation as specified therein.

Sunrise and Sunset Dates: See Section 3, item J.

Validation Tests and Date of Publication:

1. Secure Hash Standard Validation System (SHSVS), March 2004.
2. The Keyed-Hash Message Authentication System (HMACVS), December 3, 2004.
3. The Advanced Encryption Standard Algorithm Validation Suite (AESAVS), July 8, 2002
4. The CMAC Validation System (CMACVS), August 23, 2011.

Recognized Testing Program:

NIST Cryptographic Algorithm Validation Program (CAVP) and the NIST Cryptographic Module Validation Program (CMVP).

End or Registry Listing

Annex A: Managing the *Registry* (Normative)

A.1 Process for Adding Resources to the X9 *Registry*

The following elements of this annex define a process whereby ASC X9 can approve the cryptographic standards and techniques of other organizations, rather than duplicate them within ASC X9 Financial Services American National Standards. Only cryptographic resources that are thought to be appropriate (e.g, provide adequate security) for financial applications shall be included.

A.2 Eligibility

A cryptographic resource is eligible for listing in the *Registry* only if it has been produced by a recognized U.S. entity or an international standards body open to U.S. participation. ASC X9 and ISO TC 68 standards (or techniques) will not be included in the *Registry,* since they are separately approved for ASC X9 use.

A.3 Process for Inclusion and Modification

For inclusion in the *Registry,* an eligible resource must be proposed in writing to ASC X9 by a sponsoring X9 working group. The sponsoring working group shall specify the resource as indicated in Section 3 of this document.

1. The resource must be intended for use in an existing or anticipated ASC X9 standard. The sponsoring working group must identify all known X9 standards or new X9 work items in which the proposed resource may be employed.
2. The sponsoring working group shall be responsible for developing a financial use document that specifies the requirements, restrictions, and guidance on the proper use of the resource for financial applications. At the discretion of the sponsoring working group, this information shall either be contained within the *Registry* (if brief), or it shall be provided in a separate document distributed with the *Registry*. The financial use document shall not intentionally violate the requirements of the original standard on which the resource is based.
3. The specification of the resource and the financial use document shall be available to the public.[1]
4. Provided that all the requirements for a *Registry* Resource are met, ASC X9 shall submit the proposal to the X9 Secretariat for ballot to be added to the *Registry*. If all requirements above are not met, X9 shall notify the sponsoring working group of the deficiencies so that they may be rectified.
5. X9F shall conduct a ballot proposing the inclusion of the resource into the *Registry*. Only the *Registry* section applicable to the new resource is balloted. Ballot text must state the reason why the resource should be approved. The financial use

[1] Note that some organizations charge for their standards. The party requesting the standard is responsible for the payment of any such fees.

document shall be available at the time of balloting. The ballot process shall follow normal ASC X9 rules for ballots and the disclosure of patent rights.

6. The ASC X9 Board/consensus body shall conduct a ballot following the normal X9 rules for balloting.
7. After all comments are addressed per ASC X9 procedures, the resource and its financial use document will be added to the *Registry*.
8. At any time after approval and entry into the *Registry*, the sponsoring working group may submit written updates to the financial use document, the validation tests and date of publication, or the recognized testing program sections to ASC X9. X9 shall update the *Registry,* maintaining both the original and all updated text. X9 will then notify all X9 and X9F members that the *Registry* has been revised. For a period of 90 days from the posting of changes to a *Registry* Resource, any X9 or X9F member may request a ballot on the *Registry* Resource. Requested ballots will be managed in the same manner as other X9 and X9F ballots. If no ballot is requested within 90 days, then the updates shall be considered approved. If the proposed updates fail to obtain the consensus required by X9F and X9, then the *Registry* Resource shall remain as previously written. Modifications to sections other than the financial use document, the validation tests and the date of publication, or the recognized testing program sections shall meet the applicable X9 requirements for document modification.

A.4 Content of the *Registry*

1. Any resource listed in the *Registry* shall be given a unique name.
2. The date of inclusion into the *Registry* shall be specified.
3. Any resource listed in the *Registry* shall be well defined. The *Registry* shall cite the specific resource, indicating where the resource is specified and the organization by which it was approved. When a technique is specified, the specific clauses within the resource that specify the technique, including any implementation requirements, shall be cited.
4. The *Registry* shall cite or contain the financial-use document.
5. Unless otherwise indicated, cited tests for validating conformance to the resource shall be mandatory, and the date of publication shall be specified.
6. Unless otherwise indicated, cited conformance testing programs shall be mandatory.
7. Mandatory validation tests and conformance testing programs shall be fully complied with in order to claim conformance.

A.5 Withdrawal from the *Registry*

X9 may withdraw a resource from the *Registry* by the normal ASC X9 ballot process. The item will remain listed in the *Registry,* but be designated as withdrawn as of a particular date. Resources may be withdrawn form the *Registry* for the following (as well as other) reasons:

1. The resource no longer offers adequate security for financial applications;
2. The resource itself is no longer available;
3. The resource has been withdrawn by the organization that produced the standard;
4. The resource has never been used by an ASC X9 standard, and there is no indication that it will be used in the future.

A.6 Referencing a *Registry* Resource

Registry Resources shall be referenced as follows:

X9 *Registry* Resource (registry number), and (unique name).

Citations shall specify whether the resource is mandatory or informative.

Annex B: References (Informative)

AESAVS The Advanced Encryption Standard Algorithm Validation Suite (AESAVS), November 2002.

DSAVS The FIPS 186-4 Digital Signature Algorithm Validation System (DSAVS), May 2014.

DTR140 Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, January 2011.

FIPS 140 Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, December 2002.

Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*, March 2019.

FIPS 180 Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS), August 2015.

FIPS 186 Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS), July 2013.

FIPS 196 Federal Information Processing Standard (FIPS) 196, Entity Authentication Using Public Key Cryptography, February 1997. WITHDRAWN

FIPS 197 Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES), November 2001.

FIPS 198 Federal Information Processing Standard (FIPS) 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.

FIPS 202 Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015.

HMACVS The Keyed-Hash Message Authentication Code Validation System, May 2016.

MMT Multi-block Message Test (MMT) for DEA and TDES.

SEC1 Elliptic Curve Cryptography, Version 2.0, available at: https://www.secg.org/sec1-v2.pdf.

SHA3VS The Secure Hash Algorithm 3 Validation System (SHA3VS), April

2016.

SHSVS The Secure Hash Algorithm Validation System (SHAVS), May 2014.

SP 800-20 Modes of Oeration Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, April 2012. WITHDRAWN

SP 800-38A Special Publication (SP) 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001.

SP 800-38A Addendum Special Publication (SP) 800-38A Addendum, Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010.

SP 800-38B Special Publication (SP) 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode of Authentication, October 2016

SP 800-38C Special Publication (SP) 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode of Authentication and Confidentiality, July 2007.

SP 800-38D Special Publication (SP) 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.

SP 800-38E Special Publication (SP) 800-38E, Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality of Storage Devices, January 2010.

SP 800-57 Part 1 Special Publication (SP) 800-57 Part 1 Rev. 4, Recommendation for Key Management: General, January 2016.

SP 800-67 Special Publication (SP) 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017.

SP 800-90B Special Publication (SP) 800-90B, recommendation for the Entropy Sources Used for Random Bit Generation, January 2018.

SP 800-107 Special Publication (SP) 800-07 Rev. 1, Recommendation for Applications Using Approved Hash FAlgorithms, August 2012.

SP 800-185 Special Publication (SP) 800-185, SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash, December 2016.

TMOVS Modes of Operation Validation Sysem for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures. See SP 800-20. WITHDRAWN