Draft (2nd) NIST Special Publication 800-140C Revision 1

CMVP Approved Security Functions:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Cr1-draft2

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

Draft (2nd) NIST Special Publication 800-140C Revision 1

CMVP Approved Security Functions:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Cr1-draft2

February 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

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

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-140C Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-140C Rev. 1, 12 pages (February 2022)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Cr1-draft2

Public comment period: February 10, 2022 – March 25, 2022

Submit comments on this publication to: sp800-140-comments@nist.gov

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

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

Reports on Computer Systems Technology

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

Abstract

The approved security functions listed in this publication replace the ones listed in ISO/IEC 19790 Annex C and ISO/IEC 24759 6.15, within the context of the Cryptographic Module Validation Program (CMVP). As a validation authority, the CMVP may supersede Annex C in its entirety.

Keywords

Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 24759; testing requirement; vendor evidence; vendor documentation; security policy.

Audience

This document is intended for use by vendors, testing labs, and the CMVP to address issues that arise in cryptographic module testing.

Supplemental Content

Special Publication 800-140C, available at https://csrc.nist.gov/publications/detail/sp/800-140c/final, is the governing document until this revision is published as final. The updated final may have minor changes, depending on comments received.

Note to Readers

Two changes were made to this document from the first draft of Revision 1 – both editorial. The first was to section 6.2 (Approved security functions) where the security function subsections were renamed, modified, and recategorized. The second was to include the following two standards from SP 800-140D: SP 800-90A, SP 800-90B.

125 **Table of Contents**

146
147
148

1 Scope

This document specifies the Cryptographic Module Validation Program (CMVP) modifications of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformance. This document also specifies the modification of methods for evidence that a vendor or testing laboratory provides to demonstrate conformity. The approved security functions specified in this document supersede those specified in ISO/IEC 19790 Annex C and ISO/IEC 24759 paragraph 6.15.

2 Normative references

This section identifies the normative references cited as ISO/IEC 19790 and ISO/IEC 24759. The specific editions to be used are ISO/IEC 19790:2012 and ISO/IEC 24759:2017. Please note that the version 19790:2012 referenced here includes the corrections made in 2015.

National Institute of Standards and Technology (2019) *Security Requirements for Cryptographic Modules*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

3 Terms and definitions

The following terms and definitions supersede or are in addition to ISO/IEC 19790

None at this time

4 Symbols and abbreviated terms

The following symbols and abbreviated terms supersede or are in addition to ISO/IEC 19790 throughout this document:

CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CSD	Computer Security Division
CSTL	Cryptographic and Security Testing Laboratory
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management/Modernization Act
NIST	National Institute of Standards and Technology
SP 800-XXX	NIST Special Publication 800 series document

5 Document organization

5.1 General

Section 6 of this document replaces the approved security functions of ISO/IEC 19790 Annex C and ISO/IEC 24759 paragraph 6.15.

5.2 Modifications

Modifications will follow a similar format to that used in ISO/IEC 24759. For additions to test requirements, new Test Evidence (TEs) or Vendor Evidence (VEs) will be listed by increasing the "sequence_number." Modifications can include a combination of additions using underline and deletions using ~~strikethrough~~. If no changes are required, the paragraph will indicate "No change."

6 CMVP-approved security function requirements

6.1 Purpose

This document identifies CMVP-approved security functions. It supersedes security functions identified in ISO/IEC 19790 and ISO/IEC 24759.

6.2 Approved security functions

The categories include transitions, symmetric key encryption and decryption, digital signatures, hashing and message authentication.

6.2.1 Transitions

Barker EB, Roginsky AL (2019) *Transitioning the Use of Cryptographic Algorithms and Key Lengths.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-131A, Rev. 2. https://doi.org/10.6028/NIST.SP.800-131Ar2

- Relevant Sections: 1, 2, 3, 9 and 10.

6.2.2 Block Cipher

6.2.2.1 Advanced Encryption Standard (AES)

National Institute of Standards and Technology (2001) *Advanced Encryption Standard (AES)*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 197. https://doi.org/10.6028/NIST.FIPS.197

Dworkin MJ (2001) *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A. https://doi.org/10.6028/NIST.SP.800-38A

Dworkin MJ (2010) *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode.* (National Institute of Standards and

Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A, Addendum. https://doi.org/10.6028/NIST.SP.800-38A-Add

Dworkin MJ (2004) *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38C, Includes updates as of July 20, 2007. https://doi.org/10.6028/NIST.SP.800-38C

Dworkin MJ (2007) *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38D. https://doi.org/10.6028/NIST.SP.800-38D

Dworkin MJ (2010) *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38E. https://doi.org/10.6028/NIST.SP.800-38E

Dworkin MJ (2012) *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38F. https://doi.org/10.6028/NIST.SP.800-38F

IEEE Standards Association (2013) *IEEE 802.1AEbw-2013 – IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering* (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/standard/802_1AEbw-2013.html

Dworkin MJ (2016) *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38G. https://doi.org/10.6028/NIST.SP.800-38G

6.2.2.2 Triple-DES Encryption Algorithm (TDEA)

Barker EB, Mouha N (2017) *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-67, Rev. 2. https://doi.org/10.6028/NIST.SP.800-67r2

Dworkin MJ (2001) *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A. https://doi.org/10.6028/NIST.SP.800-38A

- Appendix E references modes of the Triple-DES algorithm.

Dworkin MJ (2012) *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38F. https://doi.org/10.6028/NIST.SP.800-38F

6.2.2.3 SKIPJACK

NOTE The use of SKIPJACK is approved for decryption only. The SKIPJACK algorithm has been documented in Federal Information Processing Standards Publication (FIPS) 185. This publication is obsolete and has been withdrawn.

6.2.3 Digital Signature

6.2.3.1 Digital Signature Standard (DSS) (DSA, RSA, ECDSA)

National Institute of Standards and Technology (2013) *Digital Signature Standard (DSS).* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4.

6.2.3.2 Stateful Hash-Based Signature Schemes (LMS, HSS, XMSS, XMSS^{MT})

Cooper DA, Apon DC, Dang QH, Davidson MS, Dworkin MJ, Miller CA (2020) *Recommendation for Stateful Hash-Based Signature Schemes.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-208. https://doi.org/10.6028/NIST.SP.800-208

6.2.4 Secure Hash

6.2.4.1 Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256)

National Institute of Standards and Technology (2015) *Secure Hash Standard (SHS).* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

6.2.4.2 SHA-3 Hash Algorithms (SHA3-224, SHA3-256, SHA3-384, SHA3-512)

National Institute of Standards and Technology (2015) *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

6.2.5 Extendable Output Functions

6.2.5.1 SHA-3 Extendable-Output Functions (XOF) (SHAKE128, SHAKE256)

National Institute of Standards and Technology (2015) *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

6.2.5.2 SHA-3 Derived Functions: cSHAKE, TupleHash, and ParallelHash

Kelsey JM, Chang S-jH, Perlner RA (2016) *SHA-3 Derived Functions: cSHAKE, KMAC,*

TupleHash, and ParallelHash. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-185. https://doi.org/10.6028/NIST.SP.800-185

6.2.6 Message Authentication

6.2.6.1 Triple-DES

Dworkin MJ (2005) *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38B, Includes updates as of October 6, 2016. https://doi.org/10.6028/NIST.SP.800-38B

6.2.6.2 AES

Dworkin MJ (2005) *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38B, Includes updates as of October 6, 2016. https://doi.org/10.6028/NIST.SP.800-38B

Dworkin MJ (2004) *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38C, Includes updates as of July 20, 2007. https://doi.org/10.6028/NIST.SP.800-38C

Dworkin MJ (2007) *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38D. https://doi.org/10.6028/NIST.SP.800-38D

6.2.6.3 HMAC

National Institute of Standards and Technology (2008) *The Keyed-Hash Message Authentication Code (HMAC)*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 198-1. https://doi.org/10.6028/NIST.FIPS.198-1

Dang QH (2012) *Recommendation for Applications Using Approved Hash Algorithms.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-107, Rev. 1. https://doi.org/10.6028/NIST.SP.800-107r1

6.2.6.4 KMAC

Kelsey JM, Chang S-jH, Perlner RA (2016) *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-185. https://doi.org/10.6028/NIST.SP.800-185

6.2.7 Entropy Source

Sonmez Turan M, Barker EB, Kelsey J, McKay KA, Baish, ML, Boyle M (2018) *Recommendation for Entropy Sources Used for Random Number Generation*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90B. https://doi.org/10.6028/NIST.SP.800-90B

6.2.8 Deterministic Random Bit Generator (DRBG)

Barker EB, Kelsey J (2015) *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90A, Rev. 1. https://doi.org/10.6028/NIST.SP.800-90Ar1

6.2.9 Other Security Functions

Kim Schaffer (2020) CMVP Approved Sensitive Security Parameter Generation and Establishment Methods. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-140D, as amended. https://doi.org/10.6028/NIST.SP.800-140D

Document Revisions

Edition	Date	Change
Revision 1	[date]	**6.2 Approved security functions** Added/Modified: Security function subsection headers. Moved: SP 800-90A and SP 800-90B from SP 800-140D into this document. **6.2.3 Digital Signature** Added: SP 800-208, October 2020 **6.2.9 Other Security Functions** Added: SP 800-140D, September 2020