NIST Special Publication 800-140C

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.800-140C

INFORMATION SECURITY

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

NIST Special Publication 800-140C

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.800-140C

March 2020

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

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

Authority

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

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

National Institute of Standards and Technology Special Publication 800-140C
Natl. Inst. Stand. Technol. Spec. Publ. 800-140C, 12 pages (March 2020)
CODEN: NSPUE2

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

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

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

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

Comments on this publication may be sent to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-140-comments@nist.gov

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

Reports on Computer Systems Technology

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

Abstract

NIST Special Publication (SP) 800-140C replaces the approved security functions of ISO/IEC 19790 Annex C. As a validation authority, the Cryptographic Module Validation Program (CMVP) may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790 Annex C and ISO/IEC 24759 6.15.

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 focused toward the vendors, testing labs, and CMVP for the purpose of addressing issues in cryptographic module testing.

Table of Contents

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 Symmetric Key Encryption and Decryption (AES, TDEA, SKIPJACK)

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

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

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 Signatures (DSA, RSA and ECDSA)

Digital Signature Standard (DSS)

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

6.2.4 Secure Hash Standard (SHS)

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

6.2.5 SHA-3 Standard

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

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

SHA-3 Derived Functions: cSHAKE, KMAC, 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 (Triple-DES, AES and HMAC)

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

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

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

Document Revisions

Date	Change