Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date	March 20, 2020
Original Release Date	October 9, 2019

Superseding Document

Status	Final
Series/Number	NIST Special Publication 800-140C
Title	CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759
Publication Date	March 2020
DOI	https://doi.org/10.6028/NIST.SP.800-140C
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-140c/final
Additional Information	FIPS 140-3 Transition Effort
	https://csrc.nist.gov/projects/fips-140-3-transition-effort/fips-140-3-docs

NIST

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

Draft NIST Special Publication 800-140C

CMVP Approved Security Functions:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer

I N F O R M A T I O N   S E C U R I T Y

NIST

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

20 **Draft NIST Special Publication 800-140C**

21

CMVP Approved Security Functions:

22

CMVP Validation Authority Updates to ISO/IEC 24759

23

24

25 Kim Schaffer
26 *Computer Security Division*
27 *Information Technology Laboratory*

28
29
30
31
32
33
34
35
36
37
38
39
40 October 2019
41
42

43
44
45

51   **Authority**

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

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

68

82

83   **Public comment period: *October 9, 2019 through December 9, 2019***

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

89

90   **Reports on Computer Systems Technology**

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

101   **Abstract**

102   NIST Special Publication (SP) 800-140C replaces the approved security functions of ISO/IEC
103   19790 Annex C. As a validation authority, the Cryptographic Module Validation Program
104   (CMVP) may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790
105   Annex C and ISO/IEC 24759 6.15.

106   **Keywords**

107   Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC
108   19790; ISO/IEC 2759; testing requirement; vendor evidence; vendor documentation; security
109   policy.

110   **Audience**

111   This document is focused toward the vendors, testing labs, and CMVP for the purpose of
112   addressing issues in cryptographic module testing.

113

114   **Table of Contents**

131

132

133

134 ## 1   Scope

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

141 ## 2   Normative references

142   This section identifies additional references to the normative references cited in ISO/IEC 19270
143   and ISO/IEC 24759. For dated references (e.g., ISO/IEC 19790:2012/Cor.1:*2015*(E)), only the
144   edition cited applies. For undated references (e.g., ISO/IEC 19790), the latest edition of the
145   referenced document (including any amendments) applies.

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

150 ## 3   Terms and definitions

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

152   *None at this time*

153 ## 4   Symbols and abbreviated terms

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

156   CCCS   Canadian Centre for Cyber Security

157   CMVP   Cryptographic Module Validation Program

158   CSD   Computer Security Division

159   CSTL   Cryptographic and Security Testing Laboratory

160   FIPS   Federal Information Processing Standard

161   FISMA   Federal Information Security Management/Modernization Act

162   NIST   National Institute of Standards and Technology

163   SP 800-XXX   NIST Special Publication 800 series document

164   TE   Test Evidence

165   VE   Vendor Evidence

5   Document organization

5.1   General

168   Section 6 of this document replaces the approved security functions requirements of ISO/IEC
169   19790 Annex C and ISO/IEC 24759 paragraph 6.15.

5.2   Modifications

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

6   CMVP-approved security function requirements

6.1   Purpose

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

6.2   Approved security functions

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

6.2.1   Transitions

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

187   •   Relevant Sections: 1, 2, 3, 9 and 10.

188   **6.2.2   Symmetric Key Encryption and Decryption (AES, TDEA)**

189   *6.2.2.1   Advanced Encryption Standard (AES)*

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

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

196   Dworkin MJ (2010) *Recommendation for Block Cipher Modes of Operation: Three*
197   *Variants of Ciphertext Stealing for CBC Mode.* (National Institute of Standards and
198   Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A, Addendum.
199   https://doi.org/10.6028/NIST.SP.800-38A-Add

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

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

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

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

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

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

223

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   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)

6.2.3.1   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)

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

6.2.5   SHA-3 Standard

6.2.5.1   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,

255　　Washington, DC), Federal Information Processing Standards Publication (FIPS) 202.
256　　　　https://doi.org/10.6028/NIST.FIPS.202

257　**6.2.5.2　SHA-3 Extendable-Output Functions (XOF) (SHAKE128, SHAKE256)**

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

262　**6.2.5.3　SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash**

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

267　**6.2.6　Message Authentication (Triple-DES, AES and HMAC)**

268　**6.2.6.1　Triple-DES**

269　　National Bureau of Standards (1985) *Computer Data Automation*. (U.S. Department of
270　　Commerce, Washington, DC), Federal Information Processing Standards Publication
271　　(FIPS) 113.

272　　　• This standard was withdrawn by NIST on September 1, 2008. Until December 31,
273　　　　2017, the CMVP accepted the new submissions with the claims of vendor
274　　　　affirmation to this standard. The existing validations with the claim of Triple-DES
275　　　　MAC complying with FIPS 113 will remain in place.

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

280　**6.2.6.2　AES**

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

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

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

6.2.6.3   HMAC

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

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

301   • Section 5.3

302   **Document Revisions**

Date	Change

303

304