

Withdrawn Draft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The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.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 February 10, 2022

Original Release Date August 20, 2021

Superseding Document

Status 2nd Public Draft (2PD)

Series/Number NIST Special Publication 800-140C Rev. 1

Title CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759

Publication Date February 2022

DOI <https://doi.org/10.6028/NIST.SP.800-140Cr1-draft2>

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/draft>

Additional Information

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Draft 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-draft>



23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

Draft 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-draft>

August 2021



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

46
47
48
49
50
51
52
53
54

55

Authority

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

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

69 National Institute of Standards and Technology Special Publication 800-140C Revision 1
70 Natl. Inst. Stand. Technol. Spec. Publ. 800-140C Rev. 1, 12 pages (August 2021)
71 CODEN: NSPUE2

72 This publication is available free of charge from:
73 <https://doi.org/10.6028/NIST.SP.800-140Cr1-draft>

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

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

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

87 **Public comment period: August 20, 2021 – September 20, 2021**

88 National Institute of Standards and Technology
89 Attn: Computer Security Division, Information Technology Laboratory
90 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
91 Email: sp800-140-comments@nist.gov

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

93

94

Reports on Computer Systems Technology

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

105

Abstract

106 NIST Special Publication (SP) 800-140C replaces the approved security functions of ISO/IEC
107 19790 Annex C. As a validation authority, the Cryptographic Module Validation Program
108 (CMVP) may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790
109 Annex C and ISO/IEC 24759 6.15.

110

Keywords

111 Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC
112 19790; ISO/IEC 24759; testing requirement; vendor evidence; vendor documentation; security
113 policy.

114

Audience

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

117

118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140

Table of Contents

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	1
5	Document organization	2
5.1	General	2
5.2	Modifications	2
6	CMVP-approved security function requirements	2
6.1	Purpose	2
6.2	Approved security functions	2
6.2.1	Transitions	2
6.2.2	Symmetric Key Encryption and Decryption (AES, TDEA, SKIPJACK).....	2
6.2.3	Digital Signatures	4
6.2.4	Secure Hash Standard (SHS)	4
6.2.5	SHA-3 Standard	4
6.2.6	Message Authentication (Triple-DES, AES and HMAC)	5
6.2.7	Other Security Functions	6
	Document Revisions	7

141 **1 Scope**

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

148 **2 Normative references**

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

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

156 **3 Terms and definitions**

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

158 *None at this time*

159 **4 Symbols and abbreviated terms**

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

162	CCCS	Canadian Centre for Cyber Security
163	CMVP	Cryptographic Module Validation Program
164	CSD	Computer Security Division
165	CSTL	Cryptographic and Security Testing Laboratory
166	FIPS	Federal Information Processing Standard
167	FISMA	Federal Information Security Management/Modernization Act
168	NIST	National Institute of Standards and Technology

169 SP 800-XXX NIST Special Publication 800 series document

170 **5 Document organization**

171 **5.1 General**

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

174 **5.2 Modifications**

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

180 **6 CMVP-approved security function requirements**

181 **6.1 Purpose**

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

184 **6.2 Approved security functions**

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

187 **6.2.1 Transitions**

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

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

192 **6.2.2 Symmetric Key Encryption and Decryption (AES, TDEA, SKIPJACK)**

193 ***Advanced Encryption Standard (AES)***

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

- 197 Dworkin MJ (2001) *Recommendation for Block Cipher Modes of Operation: Methods*
198 *and Techniques*. (National Institute of Standards and Technology, Gaithersburg, MD),
199 NIST Special Publication (SP) 800-38A. <https://doi.org/10.6028/NIST.SP.800-38A>
- 200 Dworkin MJ (2010) *Recommendation for Block Cipher Modes of Operation: Three*
201 *Variants of Ciphertext Stealing for CBC Mode*. (National Institute of Standards and
202 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A, Addendum.
203 <https://doi.org/10.6028/NIST.SP.800-38A-Add>
- 204 Dworkin MJ (2004) *Recommendation for Block Cipher Modes of Operation: the CCM*
205 *Mode for Authentication and Confidentiality*. (National Institute of Standards and
206 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38C, Includes
207 updates as of July 20, 2007. <https://doi.org/10.6028/NIST.SP.800-38C>
- 208 Dworkin MJ (2007) *Recommendation for Block Cipher Modes of Operation:*
209 *Galois/Counter Mode (GCM) and GMAC*. (National Institute of Standards and
210 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38D.
211 <https://doi.org/10.6028/NIST.SP.800-38D>
- 212 Dworkin MJ (2010) *Recommendation for Block Cipher Modes of Operation: The XTS-*
213 *AES Mode for Confidentiality on Storage Devices*. (National Institute of Standards and
214 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38E.
215 <https://doi.org/10.6028/NIST.SP.800-38E>
- 216 Dworkin MJ (2012) *Recommendation for Block Cipher Modes of Operation: Methods for*
217 *Key Wrapping*. (National Institute of Standards and Technology, Gaithersburg, MD),
218 NIST Special Publication (SP) 800-38F. <https://doi.org/10.6028/NIST.SP.800-38F>
- 219 IEEE Standards Association (2013) *IEEE 802.1AEbw-2013 – IEEE Standard for Local*
220 *and metropolitan area networks—Media Access Control (MAC) Security Amendment 2:*
221 *Extended Packet Numbering* (IEEE, Piscataway, NJ). Available at
222 https://standards.ieee.org/standard/802_1AEbw-2013.html
- 223 Dworkin MJ (2016) *Recommendation for Block Cipher Modes of Operation: Methods for*
224 *Format-Preserving Encryption*. (National Institute of Standards and Technology,
225 Gaithersburg, MD), NIST Special Publication (SP) 800-38G.
226 <https://doi.org/10.6028/NIST.SP.800-38G>
- 227 ***Triple-DES Encryption Algorithm (TDEA)***
- 228 Barker EB, Mouha N (2017) *Recommendation for the Triple Data Encryption Algorithm*
229 *(TDEA) Block Cipher*. (National Institute of Standards and Technology, Gaithersburg,
230 MD), NIST Special Publication (SP) 800-67, Rev. 2.
231 <https://doi.org/10.6028/NIST.SP.800-67r2>
- 232 Dworkin MJ (2001) *Recommendation for Block Cipher Modes of Operation: Methods*
233 *and Techniques*. (National Institute of Standards and Technology, Gaithersburg, MD),

234 NIST Special Publication (SP) 800-38A. <https://doi.org/10.6028/NIST.SP.800-38A>

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

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

239 **SKIPJACK**

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

243 **6.2.3 Digital Signatures**

244 ***Digital Signature Standard (DSS) (DSA, RSA, ECDSA)***

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

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

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

253 **6.2.4 Secure Hash Standard (SHS)**

254 ***Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-*** 255 ***512/224, and SHA-512/256)***

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

259 **6.2.5 SHA-3 Standard**

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

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

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

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

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

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

275 **6.2.6 Message Authentication (Triple-DES, AES and HMAC)**

276 **Triple-DES**

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

281 **AES**

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

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

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

294 **HMAC**

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

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

302 **6.2.7 Other Security Functions**

303 Schaffer K (2020) *CMVP Approved Sensitive Security Parameter Generation and*
304 *Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759*.
305 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
306 Publication (SP) 800-140D. <https://doi.org/10.6028/NIST.SP.800-140D>

307

308 **Document Revisions**

Edition	Date	Change
Revision 1	[date]	<p>§ 6.2.3 Digital Signatures Added: SP 800-208, October 2020</p> <p>§ 6.2.7 Other Security Functions Added: SP 800-140D, September 2020</p>

309