

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

25 **CMVP Approved Security Functions:**
26 *CMVP Validation Authority Updates to ISO/IEC 24759*

27
28 **Kim Schaffer**
29 *Computer Security Division*
30 *Information Technology Laboratory*
31
32
33
34
35
36
37

38
39 This publication is available free of charge from:
40 <https://doi.org/10.6028/NIST.SP.800-140Cr1-draft2>
41

42
43 February 2022
44
45



46
47
48
49 U.S. Department of Commerce
50 *Gina M. Raimondo, Secretary*
51

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

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 (February 2022)
71 CODEN: NSPUE2

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

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:** February 10, 2022 – March 25, 2022

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

89 National Institute of Standards and Technology
90 Attn: Computer Security Division, Information Technology Laboratory
91 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

93 **Reports on Computer Systems Technology**

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

104 **Abstract**

105 The approved security functions listed in this publication replace the ones listed in ISO/IEC
106 19790 Annex C and ISO/IEC 24759 6.15, within the context of the Cryptographic Module
107 Validation Program (CMVP). As a validation authority, the CMVP may supersede Annex C in
108 its entirety.

109 **Keywords**

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

113 **Audience**

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

116 **Supplemental Content**

117 Special Publication 800-140C, available at [https://csrc.nist.gov/publications/detail/sp/800-](https://csrc.nist.gov/publications/detail/sp/800-140c/final)
118 [140c/final](https://csrc.nist.gov/publications/detail/sp/800-140c/final), is the governing document until this revision is published as final. The updated final
119 may have minor changes, depending on comments received.

120 **Note to Readers**

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

125 **Table of Contents**

126 **1 Scope 1**

127 **2 Normative references 1**

128 **3 Terms and definitions 1**

129 **4 Symbols and abbreviated terms 1**

130 **5 Document organization 2**

131 5.1 General 2

132 5.2 Modifications 2

133 **6 CMVP-approved security function requirements 2**

134 6.1 Purpose 2

135 6.2 Approved security functions 2

136 6.2.1 Transitions 2

137 6.2.2 Block Cipher 2

138 6.2.3 Digital Signature 4

139 6.2.4 Secure Hash 4

140 6.2.5 Extendable Output Functions 4

141 6.2.6 Message Authentication 5

142 6.2.7 Entropy Source 6

143 6.2.8 Deterministic Random Bit Generator (DRBG) 6

144 6.2.9 Other Security Functions 6

145 **Document Revisions 7**

146

147

148

149 **1 Scope**

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

156 **2 Normative references**

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

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

164 **3 Terms and definitions**

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

166 *None at this time*

167 **4 Symbols and abbreviated terms**

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

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

178 **5 Document organization**

179 **5.1 General**

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

182 **5.2 Modifications**

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

188 **6 CMVP-approved security function requirements**

189 **6.1 Purpose**

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

192 **6.2 Approved security functions**

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

195 **6.2.1 Transitions**

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

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

200 **6.2.2 Block Cipher**

201 **6.2.2.1 Advanced Encryption Standard (AES)**

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

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

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

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

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

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

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

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

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

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

235 **6.2.2.2 Triple-DES Encryption Algorithm (TDEA)**

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

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

243

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

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

247 **6.2.2.3 SKIPJACK**

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

251 **6.2.3 Digital Signature**

252 **6.2.3.1 Digital Signature Standard (DSS) (DSA, RSA, ECDSA)**

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

256 **6.2.3.2 Stateful Hash-Based Signature Schemes (LMS, HSS, XMSS, XMSS^{MT})**

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

261 **6.2.4 Secure Hash**

262 **6.2.4.1 Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, 263 SHA-512/224, and SHA-512/256)**

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

267 **6.2.4.2 SHA-3 Hash Algorithms (SHA3-224, SHA3-256, SHA3-384, SHA3-512)**

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

272 **6.2.5 Extendable Output Functions**

273 **6.2.5.1 SHA-3 Extendable-Output Functions (XOF) (SHAKE128, SHAKE256)**

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

278 **6.2.5.2 SHA-3 Derived Functions: cSHAKE, TupleHash, and ParallelHash**

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

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

283 **6.2.6 Message Authentication**

284 **6.2.6.1 Triple-DES**

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

289 **6.2.6.2 AES**

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

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

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

302 **6.2.6.3 HMAC**

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

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

310 **6.2.6.4 KMAC**

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

315 **6.2.7 Entropy Source**

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

320 **6.2.8 Deterministic Random Bit Generator (DRBG)**

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

325 **6.2.9 Other Security Functions**

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

330

331 **Document Revisions**

Edition	Date	Change
Revision 1	[date]	<p>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.</p> <p>6.2.3 Digital Signature Added: SP 800-208, October 2020</p> <p>6.2.9 Other Security Functions Added: SP 800-140D, September 2020</p>

332