

2

3 **CMVP Security Policy Requirements:**

4 *CMVP Validation Authority Updates to*
5 *ISO/IEC 24759 and ISO/IEC 19790 Annex B*

6

7

Kim Schaffer

8

9

10

11

12

13

14

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

16

17

18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

Draft NIST Special Publication 800-140B

CMVP Security Policy Requirements:

*CMVP Validation Authority Updates to
ISO/IEC 24759 and ISO/IEC 19790 Annex B*

Kim Schaffer
*Computer Security Division
Information Technology Laboratory*

October 2019



41
42
43
44
45
46
47
48

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

49

Authority

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

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

63 National Institute of Standards and Technology Special Publication 800-140B
64 Natl. Inst. Stand. Technol. Spec. Publ. 800-140B, 17 pages (October 2019)
65 CODEN: NSPUE2

66

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

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

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

80

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

82 National Institute of Standards and Technology
83 Attn: Computer Security Division, Information Technology Laboratory
84 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
85 Email: sp800-140-comments@nist.gov

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

87

Reports on Computer Systems Technology

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

98

Abstract

99 NIST Special Publication (SP) 800-140B is to be used in conjunction with ISO/IEC 19790
100 Annex B and ISO/IEC 24759 6.14. The special publication modifies only those requirements
101 identified in this document. SP 800-140B also specifies the content of the tabular and graphical
102 information required in ISO/IEC 19790 Annex B. As a validation authority, the Cryptographic
103 Module Validation Program (CMVP) may modify, add, or delete Vendor Evidence (VE) and/or
104 Test Evidence (TE) specified under paragraph 6.14 of the ISO/IEC 24759 and specify the order
105 of the security policy as specified in ISO/IEC 19790:2012 B.1.

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

111

Audience

112 This document is focused toward the vendors, testing labs, and CMVP for the purpose of
113 addressing issues in ISO/IEC 19790, *Test requirements for cryptographic modules*.

114

115 **Table of Contents**

116 **1 Scope..... 1**

117 **2 Normative references..... 1**

118 **3 Terms and definitions 1**

119 **4 Symbols and abbreviated terms 1**

120 **5 Document organization..... 2**

121 5.1 General..... 2

122 5.2 Modifications..... 2

123 **6 Security requirements..... 2**

124 6.1 Documentation requirements..... 2

125

126 **1 Scope**

127 This document specifies the Cryptographic Module Validation Program (CMVP) modifications
 128 of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to
 129 demonstrate conformance. This document also specifies the modification of documentation for
 130 supporting evidence to demonstrate conformity. Unless otherwise specified in this document, the
 131 test requirements are specified in ISO/IEC 19790 Annex B and ISO/IEC 24759, 6.14.

132 **2 Normative references**

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

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

141 **3 Terms and definitions**

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

143 *None added at this time.*

144 **4 Symbols and abbreviated terms**

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

147	ACVP	Automated Cryptographic Validation Testing
148	CAVP	Cryptographic Algorithm Validation Program
149	CCCS	Canadian Centre for Cyber Security
150	CMVP	Cryptographic Module Validation Program
151	CSD	Computer Security Division
152	CSTL	Cryptographic and Security Testing Laboratory
153	FIPS	Federal Information Processing Standard
154	FISMA	Federal Information Security Management/Modernization Act

155	NIST	National Institute of Standards and Technology
156	SP 800-XXX	NIST Special Publication 800 series document
157	TE	Test Evidence
158	VE	Vendor Evidence

159 **5 Document organization**

160 **5.1 General**

161 Section 6 of this document specifies any modifications to the module security policy and
162 addresses any modifications to 6.14 B – cryptographic module security policy of ISO/IEC 24759
163 or modifications to ISO/IEC 19790 Annex B.

164 **5.2 Modifications**

165 Modifications to 6.14 B – cryptographic module security policy of ISO/IEC 24759 will follow a
166 similar format as in ISO/IEC 24759. For additions to test requirements, new Test Evidence (TEs)
167 or Vendor Evidence (VEs) will be listed by increasing the “sequence_number.” Modifications
168 can include a combination of additions using underline and deletions using ~~striketrough~~. If no
169 changes are required, the paragraph will indicate “No change.”

170 ISO/IEC 19790 Annex B includes security policy requirements in bulleted form but does not
171 include ways to format the required information. Therefore, modifications to these sections are
172 included by adding formatting guidance (e.g., tables, images, etc.), adding underlined text, or
173 using ~~striketrough~~ for deletion. If no changes are required, the paragraph will indicate “No
174 change.”

175 **6 Security requirements**

176 **6.1 Documentation requirements**

177 All requirements from ISO/IEC 24759 section 6.14 B and ISO 19790-2012 Annex B apply and
178 are required in the Security Policy as applicable.

179 ISO 19790-2012 Annex B uses the same section naming convention as ISO 19790-2012 Section
180 7 (Security requirements). For example, Annex B Section B.2.1 is named “General” and B.2.2 is
181 named “Cryptographic module specification,” which is the same as ISO 19790-2012 Section 7.1
182 and Section 7.2, respectively. Therefore, the format of the security policy **shall** be presented in
183 the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of
184 other attacks.” If sections are not applicable, they **shall** be marked as such in the security policy.

185 ISO/IEC 24759 6.14 B – Cryptographic module security policy are modified as indicated below:

- 186 • No change.

187 ISO 19790-2012 Annex B are modified as indicated below:

188 The additions are intended to provide further guidance on what type of information is expected
 189 for a specific requirement or set of requirements from Annex B. They are not intended to cover
 190 all the requirements from Annex B but rather a subset for clarification purposes. The applicable
 191 Annex B requirements are included here in bulleted form for reference.

192 **B.2.1 General**

- 193 • A table indicating the individual clause levels and overall level.

ISO/IEC 24759:2017 Section 6. [Number Below]	FIPS 140-3 Section Title	Level
1	General	
2	Cryptographic Module Specification	
3	Cryptographic Module Interfaces	
4	Roles, Services, and Authentication	
5	Software/Firmware Security	
6	Operational Environment	
7	Physical Security	
8	Non-Invasive Security	
9	Sensitive Security Parameter Management	
10	Self-Tests	
11	Life-Cycle Assurance	
12	Mitigation of Other Attacks	

194
195

196 **B.2.2 Cryptographic module specification**

- 197 • Hardware, Software, Firmware, or Hybrid designation:

- 198 ○ For software, firmware, and hybrid cryptographic modules, list the operating
- 199 system(s) the module was tested on and the operating system(s) that the vendor
- 200 affirms can be used by the module.

201 [For Software Module]

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1				
2				
...				

202 Table x - Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1				
2				
...				

203 Table x – Vendor Affirmed Operational Environments

204

205 [For Hardware/Firmware Module]

Model	Hardware [Part Number and Version]	Processor	Firmware Version	Distinguishing Features

206 Table x - Cryptographic Module Tested Configuration

- 207 ● Table of all security functions with specific key strengths employed for approved
- 208 services, as well as the implemented modes of operation (e.g. CBC, CCM), if
- 209 appropriate:

CAVP /ACVP Cert ¹²	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function

210 *Table x - Approved Algorithms*

Algorithm	Caveat	Use / Function

211 *Table x – Non-Approved Algorithms Allowed in FIPS Mode*

Algorithm ³	Caveat	Use / Function

212 *Table x – Non-Approved Algorithms Allowed in FIPS Mode with No Security Claimed*

213

¹ If applicable, insert a footnote detailing any mode/key-size that is present on a listed CAVP/ACVP certificate but is not used by any service, or state something to the effect of: There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

² This table includes vendor-affirmed algorithms that are approved, but CAVP testing is not yet available.

³ These algorithms do not claim any security and are not used to meet FIPS 140-3 requirements. Therefore, SSPs do not map to these algorithms.

Algorithm/Function	Use/Function

214 *Table x – Non-FIPS-Approved Algorithms Not Allowed in FIPS Mode*

- 215 ● Block Diagram, as applicable.

216 *For Software/Firmware Module–

[module 1 image]

217

218 Figure x – Logical [cryptographic] Boundary [and Physical Boundary if combined]

[module 1 image]

219

220 Figure x – Physical Boundary [if separated from logical boundary]

221 *For Hardware Module –

[module 1 image]

222

223 Figure x – [Model 1]

224 **B.2.3 Cryptographic module interfaces**

- 225 ● Table listing of all ports and interfaces (physical and logical):

Physical Port ⁴	Additional Port Detail	Description	Logical Interface Type

226

227 **B.2.4 Roles, services, and authentication**

- 228 • Specify all roles.
 229 • Table of Roles, with corresponding service with input and output:

Role	Service	Input	Output

230 *Table x – Roles, Service Commands, Input and Output*

- 231 • Specify each authentication method, whether the method is identity or role-based, and
 232 whether the method is required.
 233 • How is the strength of authentication requirement met?

Role	Authentication Method	Authentication Strength

234 *Table x – Roles and Authentication*

- 235 • Separately list the security and non-security services, both approved and non-approved.

⁴ The physical ports here should map to the physical ports shown in the module images/diagrams. If the ports are different per module within the same submission, then this table should indicate the differences.

- 236 ● For each service, list the service name, a concise description of the service purpose and/or

237 use (the service name alone may, in some instances, provide this information), a list of

238 approved security functions (algorithm(s), key management technique(s), or

239 authentication technique) used by or implemented through the invocation of the service,

240 and a list of the SSPs associated with the service or with the approved security

241 function(s) it uses. For each operator role authorized to use the service information,

242 describe the individual access rights to all SSPs with information describing the method

243 used to authenticate each role.

Service	Description	Approved Security Functions ⁵	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs

244 *Table x – Approved Services, SSPs, Roles and Access Rights*

245

Service	Description	Algorithms Accessed ⁶	Role

246 *Table x – Non-Approved Services, Algorithms and Roles*

247 **B.2.5 Software/Firmware security**

- 248 ● No change.

249 **B.2.6 Operational environment**

- 250 ● No change.

251 **B.2.7 Physical security**

⁵ Each algorithm shown in the Approved Algorithms and Non-Approved Algorithms Allowed in FIPS Mode.

⁶ Each algorithm shown in the Non-FIPS-Approved Algorithms Not Allowed in FIPS Mode table.

- 252 ● Specify the physical security mechanisms that are implemented in the module (e.g.,
- 253 tamper-evident seals, locks, tamper response and zeroisation switches, and alarms).

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details

254 *Table x – Physical Security Inspection Guidelines*

- 255 ○ The total number of tamper-evident seals or security appliances that are needed
- 256 will be indicated (e.g., five tamper-evident seals and two opacity screens). The
- 257 photos or illustrations which provide instruction on the precise placement will
- 258 have each item numbered in the photo or illustration and will equal the total
- 259 number indicated (the actual tamper-evident seals or security appliances are not
- 260 required to be numbered).

[module 1 image]

261

262 Figure x – Module 1 Seal Application Locations



263

264 Figure x – Module 2 Seal Application Locations

265

- 266 ● Overall security design and the rules of operation⁷

⁷ As part of this requirement, algorithm-specific guidance, rules, and security policy-specific requirements shall be included. These are typically found in Implementation Guidance sections [A] and [D].

267 **B.2.8 Non-invasive security**

- 268
 - No change.

269 **B.2.9 Sensitive security parameters management**

- 270
 - Provide a key table specifying the key type(s), strength(s) in bits, security function(s),
- 271
 - security function certification number(s), where and how the key(s) is generated, whether
- 272
 - the key(s) is imported or exported, any SSP generation and establishment method used,
- 273
 - and indicate any related keys.
- 274
 - Present a table of other SSPs and how they are generated.
- 275
 - Specify the approved and non-approved random bit generators.
- 276
 - Describe the uses of RBG output(s).
- 277
 - Specify the electronic and manual key I/O method(s).
- 278
 - Specify the SSP storage technique(s).
- 279
 - Specify the unprotected SSP zeroisation method(s) and rationale and operator initiation
- 280
 - capability.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys

281 *Table x – SSPs⁸*

282

- 283
 - Specify the RBG entropy source(s).

⁸ The SSPs should map with the Approved Algorithms and CAVP Certificates and Cryptographic Algorithms Allowed in FIPS Mode tables in Section B.2.2

Entropy sources	Minimum number of bits of entropy ⁹	Details

284 *Table x – Non-Deterministic Random Number Generation Specification*

285 **B.2.10 Self-tests**

- 286
 - No change.

287 **B.2.11 Life-cycle assurance**

- 288
 - No change.

289 **B.2.12 Mitigation of other attacks**

- 290
 - No change.

⁹ That is, the minimum number of bits of entropy generated, requested, and/or believed to have been loaded (with a justification of the stated amount. See Implementation Guidance [7.14]).

291 **Document Revisions**

Date	Change

292