

Withdrawn Draft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The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.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 800-140A

Title CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759

Publication Date March 2020

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

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-140a/final>

Additional Information FIPS 140-3 Transition Effort

<https://csrc.nist.gov/projects/fips-140-3-transition-effort/fips-140-3-docs>

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

CMVP Documentation Requirements:

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



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 800-140A

CMVP Documentation Requirements:
CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer
*Computer Security Division
Information Technology Laboratory*

October 2019



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

41
42
43
44
45
46
47
48
49

50

Authority

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

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

64 National Institute of Standards and Technology Special Publication 800-140A
65 Natl. Inst. Stand. Technol. Spec. Publ. 800-140A, 8 pages (October 2019)
66 CODEN: NSPUE2

67

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

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

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

81

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

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

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

88

Reports on Computer Systems Technology

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

99

Abstract

100 NIST Special Publication (SP) 800-140A modifies the vendor documentation requirements of
101 ISO/IEC 19790 Annex A. As a validation authority, the Cryptographic Module Validation
102 Program (CMVP) may modify, add, or delete Vendor Evidence (VE) and/or Test Evidence (TE)
103 as specified under paragraph 5.2 of the ISO/IEC 19790. This document should be used in
104 conjunction with ISO/IEC 19790 Annex A and ISO/IEC 24759 paragraph 6.13 as it modifies
105 only those requirements identified in this document.

106

Keywords

107 Conformance testing; Cryptographic Module Validation Program; CMVP; FIPS 140 testing;
108 FIPS 140; ISO/IEC 19790; ISO/IEC 24759; testing requirement; vendor evidence; vendor
109 documentation.

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 24759, *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 Federal Information Processing Standard (FIPS) 140-3 documentation requirements are specified
 128 in ISO/IEC 19790. This document specifies any additional requirements specified by the
 129 Cryptographic Module Validation Program (CMVP) for evidence that vendors provide to a
 130 Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformity. Unless
 131 otherwise modified in this document, the test requirements are specified in ISO/IEC 24759.

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 and ISO/IEC
 143 24759.

144 *No additional terms at this time.*

145 **4 Symbols and abbreviated terms**

146 The following symbols and abbreviated terms supersede or are in addition to ISO/IEC 19790 and
 147 ISO/IEC 24759 throughout this document:

148	CCCS	Canadian Centre for Cyber Security
149	CMVP	Cryptographic Module Validation Program
150	CSD	Computer Security Division
151	CSTL	Cryptographic and Security Testing Laboratory
152	FIPS	Federal Information Processing Standard
153	FISMA	Federal Information Security Management/Modernization Act
154	NIST	National Institute of Standards and Technology

155 SP 800-XXX NIST Special Publication 800 series document

156 TE Test Evidence

157 VE Vendor Evidence

158 **5 Document organization**

159 **5.1 General**

160 Section 6 of this document specifies any modifications to the minimum information that vendors
161 shall provide to testing laboratories as specified in Annex A of ISO/IEC 17970:2012. Section 6
162 also addresses any modifications to 6.13 A – Documentation requirements of ISO/IEC 24759.

163 **5.2 Modifications**

164 Modifications will follow a similar format as in ISO/IEC 24759. For additions to vendor-
165 supplied documentation, requirements will be listed by increasing the “sequence_number.”
166 Modifications can include a combination of additions using underline and deletions using
167 ~~striketrough~~. If no changes are required, the paragraph will indicate “No change.”

168 **6 Security requirements**

169 **6.1 Documentation requirements**

170 ISO/IEC 24597 6.13 A- and ISO/IEC 24759 Documentation requirements are modified as
171 indicated below:

172 ASA.01: (Documentation – Levels 1, 2, 3, and 4)

173 This annex {ISO/IEC19790 Annex A} specifies the minimum documentation which shall be
174 required for a cryptographic module that is to undergo an independent verification scheme {and
175 the documentation shall meet those requirements}.

176 Required Vendor Information

177 VEA.01.02: The vendor shall state that no associated libraries or associated vendor equipment
178 have a vulnerability on the CVE list. The vendor shall address how any equipment which is
179 listed that incorporates the module does not impact the security/operation of the module.

180 Required Test Procedures

181 TEA.01.02: The vendor shall verify that no libraries or similar vendor equipment have a
182 vulnerability on the CVE list or have been adequately addressed.

183 **Document Revisions**

Date	Change

184

185