

Withdrawn Draft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The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.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 May 20, 2022

Original Release Date February 10, 2022

Superseding Document

Status Final

Series/Number NIST SP 800-140Dr1

Title CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759

Publication Date May 2022

DOI <https://doi.org/10.6028/NIST.SP.800-140Dr1>

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

Additional Information

3 **CMVP Approved Sensitive Security**
4 **Parameter Generation and**
5 **Establishment Methods:**
6 *CMVP Validation Authority Updates to ISO/IEC 24759*

7
8 Kim Schaffer
9

10
11
12 This publication is available free of charge from:
13 <https://doi.org/10.6028/NIST.SP.800-140Dr1-draft2>
14

22 **Draft (2nd) NIST Special Publication 800-140D**
23 **Revision 1**

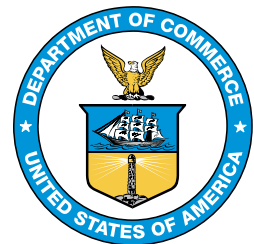
24 **CMVP Approved Sensitive Security**
25 **Parameter Generation and**
26 **Establishment Methods:**

27 *CMVP Validation Authority Updates to ISO/IEC 24759*

28
29 **Kim Schaffer**
30 *Computer Security Division*
31 *Information Technology Laboratory*
32

33
34
35
36 This publication is available free of charge from:
37 <https://doi.org/10.6028/NIST.SP.800-140Dr1-draft2>
38

39
40 February 2022
41
42



43
44
45
46 U.S. Department of Commerce
47 *Gina M. Raimondo, Secretary*
48

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

52

Authority

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

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

66 National Institute of Standards and Technology Special Publication 800-140D Revision 1
67 Natl. Inst. Stand. Technol. Spec. Publ. 800-140D Rev. 1, 10 pages (February 2022)
68 CODEN: NSPUE2

69 This publication is available free of charge from:
70 <https://doi.org/10.6028/NIST.SP.800-140Dr1-draft2>

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

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

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

84 **Public comment period:** February 10, 2022 – March 25, 2022

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

86 National Institute of Standards and Technology
87 Attn: Computer Security Division, Information Technology Laboratory
88 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

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 The approved sensitive security parameter generation and establishment methods listed in this
103 publication replace the ones listed in ISO/IEC 19790 Annex D and ISO/IEC 24759 paragraph
104 6.16, within the context of the Cryptographic Module Validation Program (CMVP). As a
105 validation authority, the CMVP may supersede Annex D in its entirety.

106 **Keywords**

107 Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140-3; ISO/IEC
108 19790; ISO/IEC 24759; sensitive security parameter establishment methods; sensitive security
109 parameter generation; testing requirement; vendor evidence; vendor documentation.

110 **Audience**

111 This document is intended for use by vendors, testing labs, and the CMVP to address issues in
112 cryptographic module testing.

113 **Supplemental Content**

114 Special Publication 800-140D, available at <https://csrc.nist.gov/publications/detail/sp/800-140d/final>,
115 is the governing document until this revision is published as final. The updated final
116 may have minor changes, depending on comments received.

117 **Note to Readers**

118 Two changes were made to this document from the first draft of Revision 1 – both editorial. The
119 first was to section 6.2 (Sensitive security parameter generation and establishment methods)
120 where the security function subsections were renamed, modified, and recategorized. The second
121 was to move the following two standards from this document into SP 800-140C: SP 800-90A, SP
122 800-90B.

123 **Table of Contents**

124 **1 Scope 1**

125 **2 Normative references 1**

126 **3 Terms and definitions 1**

127 **4 Symbols and abbreviated terms 1**

128 **5 Document organization 2**

129 5.1 General 2

130 5.2 Modifications 2

131 **6 CMVP-approved sensitive security parameter generation and establishment**

132 **requirements 2**

133 6.1 Purpose 2

134 6.2 Sensitive security parameter generation and establishment methods 2

135 6.2.1 Transitions 2

136 6.2.2 Symmetric Key Generation 2

137 6.2.3 Key-Based Key Derivation 2

138 6.2.4 Password-Based Key Derivation 3

139 6.2.5 Asymmetric Key-Pair Generation 3

140 6.2.6 Key Agreement 3

141 6.2.7 Key Agreement Key Derivation 3

142 6.2.8 Protocol-Suite Key Derivation 4

143 6.2.9 Key Transport 4

144 6.2.10 Other sensitive security parameter establishment methods 4

145 **Document Revisions 5**

146

147 1 Scope

148 This document specifies the Cryptographic Module Validation Program (CMVP) approved
149 sensitive security parameter generation and establishment methods and supersedes those
150 specified in ISO/IEC 19790 Annex D and ISO/IEC 24759 paragraph 6.16.

151 2 Normative references

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

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

159 3 Terms and definitions

160 The following terms and definitions supersede or are in addition to ISO/IEC 19790 and ISO/IEC
161 24759.

162 *None at this time*

163 4 Symbols and abbreviated terms

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

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

174 **5 Document organization**

175 **5.1 General**

176 Section 6 of this document replaces the approved sensitive security parameter generation and
177 establishment methods of ISO/IEC 19790 Annex D and ISO/IEC 24759 paragraph 6.16.

178 **5.2 Modifications**

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

184 **6 CMVP-approved sensitive security parameter generation and establishment** 185 **requirements**

186 **6.1 Purpose**

187 This document identifies CMVP-approved sensitive security parameter generation and
188 establishment methods. It precludes the use of all other sensitive security parameter generation
189 and establishment methods.

190 **6.2 Sensitive security parameter generation and establishment methods**

191 **6.2.1 Transitions**

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

- 195 • Sections relevant to this Annex: 1, 5, 6, 7, and 8.

196 **6.2.2 Symmetric Key Generation**

197 Barker EB, Roginsky AL, Davis R (2020) *Recommendation for Cryptographic Key*
198 *Generation*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
199 Special Publication (SP) 800-133, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-133r2>

200 **6.2.3 Key-Based Key Derivation**

201 Chen L (2009) *Recommendation for Key Derivation Using Pseudorandom Functions*
202 *(Revised)*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
203 Special Publication (SP) 800-108, Revised. <https://doi.org/10.6028/NIST.SP.800-108>

204 **6.2.4 Password-Based Key Derivation**

205 Sönmez Turan M, Barker EB, Burr WE, Chen L (2010) *Recommendation for Password-*
206 *Based Key Derivation: Part 1: Storage Applications*. (National Institute of Standards and
207 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-132.
208 <https://doi.org/10.6028/NIST.SP.800-132>

209 **6.2.5 Asymmetric Key-Pair Generation**

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

- 213 • DSA, RSA, and ECDSA.

214 **Note.** For the purposes of the key establishment techniques, the Digital Signature
215 Standard is only used to define the domain parameters and the (private, public) key-
216 pair generation.

217 **6.2.6 Key Agreement**

218 Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) *Recommendation for*
219 *Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*.
220 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
221 Publication (SP) 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>

222 Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019)
223 *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization*
224 *Cryptography*. (National Institute of Standards and Technology, Gaithersburg, MD),
225 NIST Special Publication (SP) 800-56B, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-56Br2>
226

227 **6.2.7 Key Agreement Key Derivation**

228 Barker EB, Chen L, Davis R (2020) *Recommendation for Key-Derivation Methods in*
229 *Key-Establishment Schemes*. (National Institute of Standards and Technology,
230 Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2.
231 <https://doi.org/10.6028/NIST.SP.800-56Cr2>

232 Barker EB, Chen L, Davis R (2018) *Recommendation for Key-Derivation Methods in*
233 *Key-Establishment Schemes*. (National Institute of Standards and Technology,
234 Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 1.
235 <https://doi.org/10.6028/NIST.SP.800-56Cr1>

236 6.2.8 Protocol-Suite Key Derivation

237 Dang QH (2011) *Recommendation for Existing Application-Specific Key Derivation*
238 *Functions*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
239 Special Publication (SP) 800-135, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-135r1>

240 The Transport Layer Security (TLS) Protocol Version 1.3, Section 7.1. (Internet
241 Engineering Task Force, Fremont, CA), RFC 8446, August 2018.
242 <https://tools.ietf.org/html/rfc8446#section-7.1>

243 6.2.9 Key Transport

244 6.2.9.1 Key Wrapping

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

248 6.2.9.2 Key Encapsulation

249 Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019)
250 *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization*
251 *Cryptography*. (National Institute of Standards and Technology, Gaithersburg, MD),
252 NIST Special Publication (SP) 800-56B, Rev. 2. [https://doi.org/10.6028/NIST.SP.800-](https://doi.org/10.6028/NIST.SP.800-56Br2)
253 [56Br2](https://doi.org/10.6028/NIST.SP.800-56Br2)

254 6.2.10 Other sensitive security parameter establishment methods

255 Sensitive security parameter establishment methods allowed in the approved mode with
256 appropriate restrictions are listed in FIPS 140-3 [Implementation Guidance](#) Section D.A.

257

258 **Document Revisions**

Edition	Date	Change
Revision 1	[Date]	<p>6.2 Sensitive security parameter generation and establishment methods Added/Modified: Security function subsection headers.</p> <p>6.2.2 Symmetric Key Generation Added: SP 800-133 Revision 2, June 2020 Removed: SP 800-133 Revision 1, July 2019</p> <p>6.2.7 Key Agreement Key Derivation Added: SP 800-56C Revision 2, August 2020</p> <p>6.2.8 Protocol-Suite Key Derivation Added: RFC 8446, Section 7.1, August 2018</p> <p>6.2.10 Other sensitive security parameter establishment methods Added: FIPS 140-3 Implementation Guidance Section D.A</p>

259