

Withdrawn Draft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The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.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 800-140D Rev. 1

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

Publication Date February 2022

DOI <https://doi.org/10.6028/NIST.SP.800-140Dr1-draft2>

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

**CMVP Approved Sensitive Security
Parameter Generation and
Establishment Methods:**
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.800-140Dr1-draft>

22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42

43
44
45
46
47
48
49
50
51

Draft NIST Special Publication 800-140D
Revision 1

**CMVP Approved Sensitive Security
Parameter Generation and
Establishment Methods:**
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.800-140Dr1-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*

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 (August 2021)
68 CODEN: NSPUE2

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

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: August 20, 2021 – September 20, 2021**

85 National Institute of Standards and Technology
86 Attn: Computer Security Division, Information Technology Laboratory
87 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
88 Email: sp800-140-comments@nist.gov

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 NIST Special Publication (SP) 800-140D replaces the approved sensitive security parameter
103 generation and establishment methods of ISO/IEC 19790 Annex D. As a validation authority, the
104 Cryptographic Module Validation Program (CMVP) may supersede this Annex in its entirety.
105 This document supersedes ISO/IEC 19790 Annex D and ISO/IEC 24759 paragraph 6.16.

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 focused toward the vendors, testing labs, and CMVP for the purpose of
112 addressing issues in cryptographic module testing.

113

114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130

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 sensitive security parameter generation and establishment requirements..... 2

6.1 Purpose 2

6.2 Sensitive security parameter generation and establishment methods..... 2

6.2.1 Transitions 2

6.2.2 Key Establishment Techniques 2

Document Revisions..... 5

131 1 Scope

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

135 2 Normative references

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

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

143 3 Terms and definitions

144 The following terms and definitions supersede or are in addition to ISO/IEC 19790 and ISO/IEC
145 24759.

146 *None at this time*

147 4 Symbols and abbreviated terms

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

150	CCCS	Canadian Centre for Cyber Security
151	CMVP	Cryptographic Module Validation Program
152	CSD	Computer Security Division
153	CSTL	Cryptographic and Security Testing Laboratory
154	FIPS	Federal Information Processing Standard
155	FISMA	Federal Information Security Management/Modernization Act
156	NIST	National Institute of Standards and Technology
157	SP 800-XXX	NIST Special Publication 800 series document

158 **5 Document organization**

159 **5.1 General**

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

162 **5.2 Modifications**

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

168 **6 CMVP-approved sensitive security parameter generation and establishment** 169 **requirements**

170 **6.1 Purpose**

171 This document identifies CMVP-approved sensitive security parameter generation and
172 establishment methods. It precludes the use of all other sensitive security parameter generation
173 and establishment methods.

174 **6.2 Sensitive security parameter generation and establishment methods**

175 **6.2.1 Transitions**

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

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

180 **6.2.2 Key Establishment Techniques**

- 181 1. Key establishment techniques allowed in the approved mode with appropriate restrictions
182 are listed in FIPS 140-3 [Implementation Guidance](#) Section D.A.
 - 183 2. National Institute of Standards and Technology (2013) Digital Signature Standard (DSS).
184 (U.S. Department of Commerce, Washington, DC), Federal Information Processing
185 Standards Publication (FIPS) 186-4. <https://doi.org/10.6028/NIST.FIPS.186-4>
- 186 • DSA, RSA, and ECDSA.

- 187 **Note.** For the purposes of the key establishment techniques, the Digital Signature
188 Standard is only used to define the domain parameters and the (private, public) key-
189 pair generation.
- 190 3. Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) *Recommendation for*
191 *Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*.
192 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
193 Publication (SP) 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- 194 4. Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019)
195 *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization*
196 *Cryptography*. (National Institute of Standards and Technology, Gaithersburg, MD),
197 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)
198 [56Br2](https://doi.org/10.6028/NIST.SP.800-56Br2)
- 199 5. Chen L (2009) *Recommendation for Key Derivation Using Pseudorandom Functions*
200 *(Revised)*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
201 Special Publication (SP) 800-108, Revised. <https://doi.org/10.6028/NIST.SP.800-108>
- 202 6. Sönmez Turan M, Barker EB, Burr WE, Chen L (2010) *Recommendation for Password-*
203 *Based Key Derivation: Part 1: Storage Applications*. (National Institute of Standards and
204 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-132.
205 <https://doi.org/10.6028/NIST.SP.800-132>
- 206 7. Dang QH (2011) *Recommendation for Existing Application-Specific Key Derivation*
207 *Functions*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
208 Special Publication (SP) 800-135, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-135r1>
- 209 8. Rescorla E (2018) *The Transport Layer Security (TLS) Protocol Version 1.3*, Section 7.1.
210 (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8446,
211 August 2018. <https://tools.ietf.org/html/rfc8446#section-7.1>
- 212 9. Barker EB, Chen L, Davis R (2020) *Recommendation for Key-Derivation Methods in*
213 *Key-Establishment Schemes*. (National Institute of Standards and Technology,
214 Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2.
215 <https://doi.org/10.6028/NIST.SP.800-56Cr2>
- 216 10. Barker EB, Chen L, Davis R (2018) *Recommendation for Key-Derivation Methods in*
217 *Key-Establishment Schemes*. (National Institute of Standards and Technology,
218 Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 1.
219 <https://doi.org/10.6028/NIST.SP.800-56Cr1>
- 220 11. Dworkin MJ (2012) *Recommendation for Block Cipher Modes of Operation: Methods for*
221 *Key Wrapping*. (National Institute of Standards and Technology, Gaithersburg, MD),
222 NIST Special Publication (SP) 800-38F. <https://doi.org/10.6028/NIST.SP.800-38F>

- 223 12. Barker EB, Roginsky AL, Davis R (2020) *Recommendation for Cryptographic Key*
224 *Generation*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
225 Special Publication (SP) 800-133, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-133r2>
- 226 13. Barker EB, Kelsey J (2015) *Recommendation for Random Number Generation Using*
227 *Deterministic Random Bit Generators*. (National Institute of Standards and Technology,
228 Gaithersburg, MD), NIST Special Publication (SP) 800-90A, Rev. 1.
229 <https://doi.org/10.6028/NIST.SP.800-90Ar1>
- 230 14. Sonmez Turan M, Barker EB, Kelsey J, McKay KA, Baish, ML, Boyle M (2018)
231 *Recommendation for Entropy Sources Used for Random Number Generation*. (National
232 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication
233 (SP) 800-90B. <https://doi.org/10.6028/NIST.SP.800-90B>

234

235 **Document Revisions**

Edition	Date	Change
Revision 1	[date]	<p>§ 6.2.2 Key Establishment Techniques</p> <p>Added: FIPS 140-3 Implementation Guidance Section D.A</p> <p>Added: RFC 8446, Section 7.1, August 2018</p> <p>Added: SP 800-56C Revision 2, August 2020</p> <p>Added: SP 800-133 Revision 2, June 2020</p> <p>Removed: SP 800-133 Revision 1, July 2019</p>

236