Withdrawn Draft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The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.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

National Institute of Standards and Technology
U.S. Department of Commerce

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

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

National Institute of
Standards and Technology
U.S. Department of Commerce

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

Authority

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

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

National Institute of Standards and Technology Special Publication 800-140D Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-140D Rev. 1, 10 pages (August 2021)
CODEN: NSPUE2

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

Public comment period: August 20, 2021 – September 20, 2021

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

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

Table of Contents

1 Scope

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

2 Normative references

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

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

3 Terms and definitions

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

None at this time

4 Symbols and abbreviated terms

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

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

5 Document organization

5.1 General

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

5.2 Modifications

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

6 CMVP-approved sensitive security parameter generation and establishment requirements

6.1 Purpose

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

6.2 Sensitive security parameter generation and establishment methods

6.2.1 Transitions

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

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

6.2.2 Key Establishment Techniques

1. Key establishment techniques allowed in the approved mode with appropriate restrictions are listed in FIPS 140-3 Implementation Guidance Section D.A.

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

- DSA, RSA, and ECDSA.

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

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

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

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

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

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

8. Rescorla E (2018) *The Transport Layer Security (TLS) Protocol Version 1.3*, Section 7.1. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8446, August 2018. https://tools.ietf.org/html/rfc8446#section-7.1

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

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

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

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

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

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

Document Revisions

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