Draft NIST Special Publication 800-140D

CMVP Approved Sensitive Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759:2014(E)

Kim Schaffer

INFORMATION SECURITY

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

Draft NIST Special Publication 800-140D

CMVP Approved Sensitive Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759:2014(E)

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

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
Natl. Inst. Stand. Technol. Spec. Publ. 800-140D, 10 pages (October 2019)
CODEN: NSPUE2

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

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

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

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

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).

Reports on Computer Systems Technology

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

Abstract

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

Keywords

Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140-3; ISO/IEC 19790; ISO/IEC 2759; Sensitive Parameter Establishment Methods; Sensitive Parameter Generation; testing requirement; vendor evidence; vendor documentation.

Audience

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

Table of Contents

1 Scope

This document specifies the Cryptographic Module Validation Program (CMVP) modifications of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformance. This document also specifies the modification of methods for evidence that a vendor or testing laboratory provides to demonstrate conformity. The approved sensitive security parameter generation and establishment methods specified in this document supersede those specified in ISO/IEC 19790 Annex D and ISO/IEC 24759 paragraph 6.16.

2 Normative references

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

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
TE	Test Evidence
VE	Vendor Evidence

5 Document organization

5.1 General

Section 6 of this document replaces the approved sensitive security parameter generation and establishment methods requirements 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 24759:2014(E). 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 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 a FIPS-Approved mode of operation with appropriate restrictions are listed in FIPS 140-2 Implementation Guidance Section D.2.

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, Smid ME (2013) *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. 2. https://doi.org/10.6028/NIST.SP.800-56Ar2

5. Barker EB, Johnson D, Smid ME (2007) *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. 2. https://doi.org/10.6028/NIST.SP.800-56Ar

   - The FIPS 140-2 IG D1-rev2 provides the rationale for including two different revisions of SP 800-56A in this Annex.

6. 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

7. Barker EB, Chen L, Moody D (2014) *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 1. https://doi.org/10.6028/NIST.SP.800-56Br1

8. 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

9. 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

10. 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

11. 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

12. Chen L (2011) *Recommendation for Key-Derivation through Extraction-then-Expansion*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C. https://doi.org/10.6028/NIST.SP.800-56C

13. 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

14. Barker EB, Roginsky AL (2019) *Recommendation for Cryptographic Key Generation*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-133, Rev. 1. https://doi.org/10.6028/NIST.SP.800-133r1

Document Revisions

Date	Change