NIST Special Publication
NIST SP 800-140Dr1

CMVP Approved Sensitive Security Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer
Alexander Calis

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

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

NIST Special Publication
NIST SP 800-140Dr1

CMVP Approved Sensitive Security Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer
Alexander Calis
Computer Security Division
Information Technology Laboratory

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

May 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by the National Institute of Standards and Technology (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 800-140Dr1
Natl. Inst. Stand. Technol. Spec. Publ. 800-140Dr1, 10 pages (May 2022)
CODEN: NSPUE2

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

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.

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

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

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

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

Keywords

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

Audience

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

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 International Organization for Standardization/International Electrotechnical Commission (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
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
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. These are considered CMVP-approved security functions. 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

6.2.2 Symmetric Key Generation

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

6.2.3 Key-Based Key Derivation

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

6.2.4 Password-Based Key Derivation

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

6.2.5 Asymmetric Key-Pair Generation

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.

6.2.6 Key Agreement

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

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

6.2.7 Key Agreement Key Derivation

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

6.2.8 Protocol-Suite Key Derivation

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

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

6.2.9 Key Transport

6.2.9.1 Key Wrapping

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

6.2.9.2 Key Encapsulation

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

6.2.10 Entropy Source

Sönmez Turan M, Barker EB, Kelsey JM, 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

6.2.11 Deterministic Random Bit Generator (DRBG)

Barker EB, Kelsey JM (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

6.2.12 Other sensitive security parameter establishment methods

Sensitive security parameter establishment methods allowed in the approved mode with appropriate restrictions are listed in FIPS 140-3 Implementation Guidance Section D.A.

Document Revisions

Edition	Date	Change
Revision 1 (r1)	May 2022	**6.1 Purpose** Added language on CMVP-approved security functions. **6.2 Sensitive security parameter generation and establishment methods** Added/Modified: Security function subsection headers. **6.2.1 Transitions** Deleted: SP 800-131A Rev. 2 section references **6.2.2 Symmetric Key Generation** Added: SP 800-133 Revision 2, June 2020 Removed: SP 800-133 Revision 1, July 2019 **6.2.7 Key Agreement Key Derivation** Added: SP 800-56C Revision 2, August 2020 Removed: SP 800-56C Revision 1, April 2018 **6.2.8 Protocol-Suite Key Derivation** Added: RFC 8446, Section 7.1, August 2018 **6.2.12 Other sensitive security parameter establishment methods** Added: FIPS 140-3 Implementation Guidance Section D.A