NIST Special Publication
NIST SP 800-140Dr2

Cryptographic Module Validation Program (CMVP)-Approved Sensitive Security Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759

Alexander Calis

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Dr2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-140Dr2

Cryptographic Module Validation Program (CMVP)-Approved Sensitive Security Parameter Generation and Establishment Methods:

CMVP Validation Authority Updates to ISO/IEC 24759

Alexander Calis
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Dr2

July 2023

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

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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.

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.

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2023-03-30
Supersedes NIST Special Publication (SP) 800-140Dr1 (May 2022) https://doi.org/10.6028/NIST.SP.800-140Dr1

How to Cite this NIST Technical Series Publication:

Calis A (2023) Cryptographic Module Validation Program (CMVP)-Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-140Dr2. https://doi.org/10.6028/NIST.SP.800-140Dr2

Author ORCID iDs

Alexander Calis: 0000-0003-1937-8129

Contact Information

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).

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. This document also supersedes SP 800-140Dr1.

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.

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.

Supplemental Content

See https://csrc.nist.gov/projects/cmvp/sp800-140-series-info for details about the SP 800-140x series publications and their relationships to ISO/IEC 19790 and ISO/IEC 24759.

Audience

This document is intended for use by vendors, testing labs, and the CMVP.

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. This document also supersedes SP 800-140Dr1.

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.

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:

CMVP
Cryptographic Module Validation Program

FIPS
Federal Information Processing Standard

ISO/IEC
International Organization for Standardization/International Electrotechnical Commission

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. This document also supersedes SP 800-140Dr1.

5.2. Modification

This publication is a complete replacement of the CMVP-approved sensitive security parameter generation and establishment methods of ISO/IEC 19790 Annex C and ISO/IEC 24759 paragraph 6.16. There are no other modifications, additions, or deletions.

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

For the current list of CMVP-approved sensitive security parameter generation and establishment methods, see https://csrc.nist.gov/projects/cmvp/sp800-140d.

Appendix 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** Removed: 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
Revision 2 (r2)	July 2023	**6.2 Sensitive security parameter generation and establishment methods** Removed: All subsections. Added: Reference to a CMVP web link that includes the CMVP approved sensitive security parameter generation and establishment methods. Future modifications to the list will be made on that website, minimizing the need to revise this publication.