Draft NIST Special Publication 800-140A

CMVP Documentation Requirements:

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer

INFORMATION SECURITY

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

Draft NIST Special Publication 800-140A

CMVP Documentation Requirements:

CMVP Validation Authority Updates to ISO/IEC 24759

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 800-140A
Natl. Inst. Stand. Technol. Spec. Publ. 800-140A, 8 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) 800-140A modifies the vendor documentation requirements of ISO/IEC 19790 Annex A. As a validation authority, the Cryptographic Module Validation Program (CMVP) may modify, add, or delete Vendor Evidence (VE) and/or Test Evidence (TE) as specified under paragraph 5.2 of the ISO/IEC 19790. This document should be used in conjunction with ISO/IEC 19790 Annex A and ISO/IEC 24759 paragraph 6.13 as it modifies only those requirements identified in this document.

Keywords

Conformance testing; Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 24759; 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 ISO/IEC 24759, *Test requirements for cryptographic modules*.

Table of Contents

1 Scope

Federal Information Processing Standard (FIPS) 140-3 documentation requirements are specified in ISO/IEC 19790. This document specifies any additional requirements specified by the Cryptographic Module Validation Program (CMVP) for evidence that vendors provide to a Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformity. Unless otherwise modified in this document, the test requirements are specified in ISO/IEC 24759.

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.

No additional terms 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 specifies any modifications to the minimum information that vendors shall provide to testing laboratories as specified in Annex A of ISO/IEC 17970:2012. Section 6 also addresses any modifications to 6.13 A – Documentation requirements of ISO/IEC 24759.

5.2 Modifications

Modifications will follow a similar format as in ISO/IEC 24759. For additions to vendor-supplied documentation, requirements 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 Security requirements

6.1 Documentation requirements

ISO/IEC 24597 6.13 A- and ISO/IEC 24759 Documentation requirements are modified as indicated below:

ASA.01: (Documentation – Levels 1, 2, 3, and 4)

This annex {ISO/IEC19790 Annex A} specifies the minimum documentation which shall be required for a cryptographic module that is to undergo an independent verification scheme {and the documentation shall meet those requirements}.

Required Vendor Information

VEA.01.02: The vendor shall state that no associated libraries or associated vendor equipment have a vulnerability on the CVE list. The vendor shall address how any equipment which is listed that incorporates the module does not impact the security/operation of the module.

Required Test Procedures

TEA.01.02: The vendor shall verify that no libraries or similar vendor equipment have a vulnerability on the CVE list or have been adequately addressed.

Document Revisions

Date	Change