NIST Special Publication 800-140B

CMVP Security Policy Requirements:

CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B

Kim Schaffer

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

I N F O R M A T I O N S E C U R I T Y

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

NIST Special Publication 800-140B

CMVP Security Policy Requirements:

CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B

Kim Schaffer
Computer Security Division
Information Technology Laboratory

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

March 2020

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 800-140B
Natl. Inst. Stand. Technol. Spec. Publ. 800-140B, 19 pages (March 2020)
CODEN: NSPUE2

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

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.

Comments on this publication may be submitted to:

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) 800-140B is to be used in conjunction with ISO/IEC 19790 Annex B and ISO/IEC 24759 section 6.14. The special publication modifies only those requirements identified in this document. SP 800-140B also specifies the content of the tabular and graphical information required in ISO/IEC 19790 Annex B. As a validation authority, the Cryptographic Module Validation Program (CMVP) may modify, add, or delete Vendor Evidence (VE) and/or Test Evidence (TE) specified under paragraph 6.14 of the ISO/IEC 24759 and specify the order of the security policy as specified in ISO/IEC 19790:2012 B.1.

Keywords

Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 24759; testing requirement; vendor evidence; vendor documentation; security policy.

Audience

This document is focused toward the vendors, testing labs, and CMVP for the purpose of addressing issues in ISO/IEC 19790, *Information technology – Security techniques - Security requirements for cryptographic modules*, and ISO/IEC 24759, *Information technology – Security techniques - Test requirements for cryptographic modules.*

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 documentation for providing evidence to demonstrate conformity. Unless otherwise specified in this document, the test requirements are specified in ISO/IEC 19790 Annex B and ISO/IEC 24759 section 6.14.

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 those defined in ISO/IEC 19790 and ISO/IEC 24759:

None added at this time.

4 Symbols and abbreviated terms

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

CAVP	Cryptographic Algorithm Validation Program
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CSD	Computer Security Division
CSTL	Cryptographic and Security Testing Laboratory
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
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 ISO/IEC 19790 Annex B and ISO/IEC 24759 section 6.14.

5.2 Modifications

Modifications to ISO/IEC 24759 section 6.14 - Cryptographic module security policy - will follow a similar format as 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."

ISO/IEC 19790 Annex B includes security policy requirements in bulleted form but does not include ways to format the required information. Modifications are addressed by adding formatting guidance (e.g., tables, images, etc.), adding underlined text, or using ~~strikethrough~~ for deletion. If no changes are required, the paragraph will indicate "No change." Additional guidance may also be included to address requirements presented in SP 800-140, SP 800-140A, SP 800-140C, SP 800-140D, SP 800-140E, and SP 800-140F.

6 Security requirements

6.1 Documentation requirements

All requirements from ISO/IEC 24759 section 6.14 and ISO/IEC 19790 Annex B apply and are required in the security policy as applicable.

ISO/IEC 19790 Annex B uses the same section naming convention as ISO/IEC 19790 section 7 - Security requirements. For example, Annex B section B.2.1 is named "General" and B.2.2 is named "Cryptographic module specification," which is the same as ISO/IEC 19790 section 7.1 and section 7.2, respectively. Therefore, the format of the security policy **shall** be presented in the same order as indicated in Annex B, starting with "General" and ending with "Mitigation of other attacks." If sections are not applicable, they **shall** be marked as such in the security policy.

ISO/IEC 24759 section 6.14 – Cryptographic module security policy requirements are modified as indicated below:

- No change.

ISO/IEC 19790 Annex B requirements are modified as indicated below:

The additions are intended to provide further guidance on what type of information is expected for a specific requirement or set of requirements from Annex B. They are not intended to cover all the requirements from Annex B but rather a subset for clarification purposes. The applicable Annex B requirements are included here in bulleted form for reference.

B.2.1 General

- A table indicating the individual clause levels and overall level.
- Overall Security Rating of the module and the Security Levels of individual areas.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	
2	Cryptographic module specification	
3	Cryptographic module interfaces	
4	Roles, services, and authentication	
5	Software/Firmware security	
6	Operational environment	
7	Physical security	
8	Non-invasive security	
9	Sensitive security parameter management	
10	Self-tests	
11	Life-cycle assurance	
12	Mitigation of other attacks	

Table x – Security Levels

B.2.2 Cryptographic module specification

- Hardware, Software, Firmware, or Hybrid designation:
  - For software, firmware, and hybrid cryptographic modules, list the operating system(s) the module was tested on and the operating system(s) that the vendor affirms can be used by the module.

[For Software/Firmware/Hybrid Module]

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1				
2				
…				

Table x - Tested Operational Environments

#	Operating System	Hardware Platform
1		
2		
…		

Table x – Vendor Affirmed Operational Environments

[For Hardware Module]

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features[1]

Table x - Cryptographic Module Tested Configuration

[1] Examples may be ports and interfaces, memory storage devices and sizes, field replaceable and stationary accessories (power supplies, fans), etc.

- Table of all security functions with specific key strengths employed for approved services, as well as the implemented modes of operation (e.g. CBC, CCM), if appropriate.

CAVP Cert[2][3]	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function

Table x - Approved Algorithms

Algorithm	Caveat	Use / Function

Table x – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm[4]	Caveat	Use / Function

Table x – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

[2] If applicable, insert a footnote detailing any mode/key-size that is present on a listed CAVP certificate but is not used by any service, or state something to the effect of: There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

[3] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.

[4] These algorithms do not claim any security and are not used to meet FIPS 140-3 requirements. Therefore, SSPs do not map to these algorithms.

Algorithm/Function	Use/Function

Table x – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

- Illustrative diagram, schematic or photograph of the module. A photograph is included for a hardware module. If the security policy encompasses multiple versions of the module, each version is represented separately or annotated that the representation is illustrated for all versions. For a software or firmware cryptographic module, the security policy includes a block diagram that illustrates:
    - the location of the logical object of the software or firmware module with respect to the operating system, other supporting applications and the cryptographic boundary so that all the logical and physical layers between the logical object and the cryptographic boundary are clearly defined; and
    - the interactions of the logical object of the software or firmware module with the operating system and other supporting applications resident within the cryptographic boundary.
- Block Diagram, as applicable.

[For Software/Firmware/Hybrid Module]

[module 1 image]

Figure x – Logical [cryptographic] boundary [and physical boundary if combined]

[module 1 image]

Figure x – Physical boundary [if separated from logical boundary]

[For Hardware/Hybrid[5] Module]

[module 1 image]

Figure x – [Model 1]

- Overall security design and the rules of operation[6]

B.2.3 Cryptographic module interfaces

- Table listing of all ports and interfaces (physical and logical).
- Define the information passing over the five logical interfaces.
- Specify physical ports and data that pass over them.

Physical port[7]	Logical interface	Data that passes over port/interface

Table x – Ports and Interfaces

B.2.4 Roles, services, and authentication

- Specify all roles.
- Table of Roles, with corresponding service with input and output.

[5] The image will show the disjoint hardware component of the hybrid module

[6] As part of this requirement, algorithm-specific guidance, rules, and security policy-specific requirements shall be included.

[7] The physical ports here should map to the physical ports shown in the module images/diagrams. If the ports are different per module within the same submission, then this table should indicate the differences.

Role	Service	Input	Output

Table x – Roles, Service Commands, Input and Output

- Specify each authentication method, whether the method is identity or role-based, and whether the method is required.
- How is the strength of authentication requirement met?

Role	Authentication Method	Authentication Strength

Table x – Roles and Authentication

- Separately list the security and non-security services, both approved and non-approved.
- For each service, list the service name, a concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information), a list of approved security functions (algorithm(s), key management technique(s), or authentication technique) used by or implemented through the invocation of the service, and a list of the SSPs associated with the service or with the approved security function(s) it uses. For each operator role authorized to use the service, describe the individual access rights to all SSPs including information describing the method used to authenticate each role.

Service	Description	Approved Security Functions[8]	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[9]	Indicator

Table x – Approved Services

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Service	Description	Algorithms Accessed[10]	Role	Indicator

Table x – Non-Approved Services

B.2.5 Software/Firmware security

- No change.

[8] Each algorithm shown in the Approved Algorithms and Non-Approved Algorithms Allowed in the Approved Mode of Operation tables should map to at least one service

[9] Use the letters (G, R, W, E, Z) as defined under this table when listing the access rights of each SSP.

[10] Each algorithm shown in the Non-Approved Algorithms Not Allowed in the Approved Mode of Operation table should map to at least one service.

B.2.6 Operational environment

- No change.

B.2.7 Physical security

[For physical Security Level 2 and above]

- Specify the physical security mechanisms that are implemented in the module (e.g., tamper-evident seals, locks, tamper response and zeroisation switches, and alarms).
- Specify the actions required by the operator(s) to ensure that the physical security is maintained (e.g. periodic inspection of tamper-evident seals or testing of tamper response and zeroisation switches).

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details

Table x – Physical Security Inspection Guidelines

  - Specify the following information if the module requires operator applied tamper evident seals or security appliances that the operator will apply or modify over the lifecycle of the module: The reference photo or illustrations required in B 2.2 will reflect the module configured or constructed as specified. Additional photos/illustrations may be provided to reflect other configurations.
  - If filler panels are needed to cover unpopulated slots or openings to meet the opacity requirements, they will be included in the photo or illustrations with tamper seals affixed as needed. The filler panels will be included in the list of parts.
  - Photos or illustrations will indicate the precise placement of any tamper evident seal or security appliance needed to meet the physical security requirements.
  - The total number of tamper-evident seals or security appliances that are needed will be indicated (e.g., five tamper-evident seals and two opacity screens). The photos or illustrations which provide instruction on the precise placement will have each item numbered in the photo or illustration and will equal the total number indicated (the actual tamper-evident seals or security appliances are not required to be numbered as illustrated).

Figure x – Module 1 Seal Application Locations

Figure x – Module 2 Seal Application Locations

[For physical Security Level 3 and above]

	Temperature or voltage measurement	Specify EFP[11] or EFT	Specify if this condition results in a shutdown or zeroisation
Low Temperature			
High Temperature			
Low Voltage			
High Voltage			

Table x – EFP/EFT

[11] EFP is required for modules with physical Security Level 4.

[For modules covered by strong or hard conformal or non-conformal enclosures, coatings, or potting materials]

	Hardness tested temperature measurement
Low Temperature	
High Temperature	

Table x –Hardness testing temperature ranges[12]

B.2.8 Non-invasive security

- No change.

B.2.9 Sensitive security parameters management

- Provide a key table specifying the key type(s), strength(s) in bits, security function(s), security function certification number(s), where and how the key(s) is generated, whether the key(s) is imported or exported, any SSP generation and establishment method used, and indicate any related keys.
- Present a table of other SSPs and how they are generated.
- Specify the approved and non-approved random bit generators.
- Describe the uses of RBG output(s).
- Specify the electronic and manual ~~key~~ SSP I/O method(s)[13].
- Specify the SSP storage technique(s).
- Specify the unprotected SSP zeroisation method(s) and rationale and operator initiation capability.

Key/SSP Name/ Type	**Strength**	**Security Function and Cert. Number**	**Gener-ation**	**Import /Export**	**Establish-ment**	**Storage**	**Zero-isation**	**Use & related keys**

Table x – SSPs[14]

[12] The module is hardness tested at the lowest and highest temperatures within the module's intended temperature range of operation.

[13] This should be specified in the "Import/Export" column in the SSP table.

[14] The SSPs should map to the Approved Algorithms and CAVP Certificates and Cryptographic Algorithms Allowed in the

- Specify the RBG entropy source(s).

Entropy sources	Minimum number of bits of entropy[15]	Details

Table x – Non-Deterministic Random Number Generation Specification

B.2.10 Self-tests

- No change.

B.2.11 Life-cycle assurance

- No change.

B.2.12 Mitigation of other attacks

- No change.

Approved Mode of Operation tables in section B.2.2

[15] That is, the minimum number of bits of entropy generated, requested, and/or believed to have been loaded, with a justification of the stated amount.

Document Revisions

Date	Change