NIST Special Publication
NIST SP 800-140Br1

Cryptographic Module Validation Program (CMVP) Security Policy Requirements:

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

David Hawes
Alexander Calis
Roy Crombie

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Br1

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

NIST Special Publication
NIST SP 800-140Br1

Cryptographic Module Validation Program (CMVP) Security Policy Requirements:

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

David Hawes
Alexander Calis
Computer Security Division
Information Technology Laboratory

Roy Crombie
Canadian Centre for Cyber Security

https://doi.org/10.6028/NIST.SP.800-140Br1

November 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.

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.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2023-11-13

How to Cite this NIST Technical Series Publication:

Hawes D, Calis A, Crombie R (2023) Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-140Br1. https://doi.org/10.6028/NIST.SP.800-140Br1

Author ORCID iDs

David Hawes: 0000-0002-0173-6795
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

NIST Special Publication (SP) 800-140Br1 is to be used in conjunction with ISO/IEC 19790 Annex B and ISO/IEC 24759 Section 6.14. This Special Publication modifies only those requirements identified in this document. NIST SP 800-140Br1 also specifies the content of the 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 stated in ISO/IEC 19790:2012 B.1.

Keywords

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

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 NIST Special Publication (SP) 800-140x series publications and their relationships to ISO/IEC 19790 and ISO/IEC 24759.

Audience

This document is intended for vendors, testing labs, and CMVP to address 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. Introduction

1.1. 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.

1.2. 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. 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

2. Document Organization

2.1. General

Section 3.1 of this document specifies any modifications to ISO/IEC 19790 Annex B and ISO/IEC 24759 Section 6.14. Section 3.2 identifies any additional requirements for the security policy that are documented in other publications. Section 3.3 describes the security policy structure and how the requirements in Sections 3.1 and 3.2 map into that structure.

The requirements statements are presented as originally written in ISO/IEC 19790 Annex B and ISO/IEC 24759. These often include acronyms and abbreviations spelled out earlier within those documents. When the first use occurs within this document, the acronym or abbreviation will be spelled out within brackets immediately following the occurrence. These statements also include the British English standard spellings for the words "zeroize" and "authorize" as "zeroise" and "authorise".

2.2. Modifications

Modifications to ISO/IEC 24759 Section 6.14, *Cryptographic module security policy*, will follow a similar format as ISO/IEC 24759. For additions to test requirements, new Test Evidence (TE) or Vendor Evidence (VE) 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), 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 NIST Special Publication (SP) 800-140, SP 800-140A, SP 800-140C, SP 800-140D, SP 800-140E, and SP 800-140F.[1]

[1] More information about the SP 800-140 subseries is available at https://csrc.nist.gov/projects/cmvp/sp800-140-series-info.

3. Security Requirements

3.1. Changes to ISO/IEC 24759 Section 6.14 and ISO/IEC 19790 Annex B 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:

- **B.2.1 General**

  No change.

- **B.2.2 Cryptographic module specification**
  - Illustrative diagram, schematic, or photograph of the module. A photograph included for hardware modules. 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, hybrid, or sub-chip 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 of 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.
    - Tested Operational Environment's Physical Perimeter (TOEPP) – The location of the cryptographic module with respect to the TOEPP that is part of the module's tested configuration but may be outside of the module's cryptographic boundary so that all of the logical and physical layers between the cryptographic module and the TOEPP are clearly defined. This also includes a description and components list of the TOEPP.
  - Precise definition of the module's ~~physical~~ TOEPP and cryptographic boundar~~ies~~y

- **B.2.3 Cryptographic module interfaces**

  No change.

- **B.2.4 Roles, services, and authentication**

  No change.

- **B.2.5 Software/firmware security**

  No change.

- **B.2.6 Operational environment**

  No change.

- **B.2.7 Physical security**

  No change.

- **B.2.8 Non-invasive security**

  No change.

- **B.2.9 Sensitive security parameters management**

  - Provide an ~~key~~ SSP [sensitive security parameter] table specifying the ~~key~~ SSP type(s), strength(s) in bits, security function(s), security function certification number(s), where and how the ~~key(s)~~ SSP(s) is generated, ~~whether the key(s) SSP(s) is imported or exported~~ what method(s) is used to input or output the SSP(s), and any SSP generation and establishment method used, and indicate any related ~~keys~~ SSPs.
  - Specify the electronic and manual ~~key~~ SSP I/O [input/output] method(s).
  - Specify the SSP storage ~~technique(s)~~ areas, formats (encrypted or plaintext), and persistence types (dynamic or static).

- **B.2.10 Self-tests**

  No change.

- **B.2.11 Lifecycle assurance**

  No change.

- **B.2.12 Mitigation of other attacks**

  No change.

3.2. Documentation Requirement Additions

In addition to ISO/IEC 24759 Section 6.14 and ISO/IEC 19790 Annex B, other publications and documents specify the documentation requirements for the security policy. Many of these requirements relate to the specific conditions and configurations of modules and would not be applicable in many cases. These additional requirements are listed for each section of the security policy, grouped by the source publication or document, and reference the specific section from the document where the requirement is stated. Where possible, they are direct

statements from the source documents and would often require the original context to best understand the requirement.

- **B.2.1 General**

  No additions.

- **B.2.2 Cryptographic module specification**

  SP800-140:VE02.20.04

  - Vendor-affirmed security methods – The vendor-provided non-proprietary security policy shall include a list of all vendor-affirmed security methods.

- **B.2.3 Cryptographic module interfaces**

  No additions.

- **B.2.4 Roles, services, and authentication**

  No additions.

- **B.2.5 Software/Firmware security**

  No additions.

- **B.2.6 Operational environment**

  No additions.

- **B.2.7 Physical security**

  SP800-140:VE07.26.02

  - High and low temperature – The vendor-provided security policy shall specify the nominal and high/low temperature range.

  SP800-140:VE07.77.02

  - Temperature shutdown/zeroise – The security policy shall address whether the employed EFP [environmental failure protection] feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met.

  SP800-140:VE07.81.02

  - EFT [environmental failure testing] shutdown/zeroise – The security policy shall address whether the employed EFT feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met.

- **B.2.8 Non-invasive security**

  No additions.

- **B.2.9 Sensitive security parameters management**

  SP800-140:VE09.28.03

  - SSP procedural zeroisation – If SSPs are zeroised procedurally while under the control of the operator (i.e., present to observe that the method has completed

successfully or controlled via a remote management session), vendor documentation and the module security policy must specify how the methods shall be performed.

- **B.2.10 Self-tests**

  No additions.

- **B.2.11 Life cycle assurance**

  No additions.

- **B.2.12 Mitigation of other attacks**

  No additions.

3.3. Documentation Input, Structure, and Formatting

This section provides further guidance on what type of information is expected for a specific requirement or set of requirements from Annex B and the additional requirements listed in Section 3.2. All of the requirement statements are organized into appropriately named and numbered subsections (e.g., 1.2 – Security Levels, 2.1 – Purpose or Use). Each subsection identifies the applicable requirements and provides any clarifying and explanatory notes.

A significant portion of the security policy information will be structured and interrelated. These tables can be input through Web Cryptik or uploaded in JavaScript Object Notation (JSON) format (see https://csrc.nist.gov/projects/cmvp/sp800-140b for information content and format details associated with the structured JSON and Web Cryptik), which would follow a provided schema and table relationship constraints. The text and picture portions of the security policy will be entered into a provided Microsoft Word template document, which follows a specific structure. Within this document are content controls that serve as placeholders for the structured content in Web Cryptik and/or the uploaded JSON file.

In this revision of NIST SP 800-140B and the corresponding update to Web Cryptik, the labs/vendors will select algorithms, modes, and properties from the sets that have been tested through the Cryptographic Algorithm Validation Program (CAVP) process. Information on the CAVP process is available at https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program.This will replace the previous process of separately entering that information. Part of the initial information that labs/vendors enter into Web Cryptik will be the CAVP certificate numbers associated with the algorithm tests for that particular module. Web Cryptik will then retrieve and display the relevant information from the CAVP system. Each algorithm or operational environment entry will be listed with the set of capabilities for that test. The lab/vendor will then select the specific items that are implemented in the module. When algorithms are tested in multiple operating environments (OE), they will each have a separate entry in the list. The selected subset will be saved, maintained with the rest of the module's information, and used to generate the Tested Algorithm table in the security policy.

All of this information (i.e., the structured JSON, the uploaded document, and the selected CAVP test information) will be combined into the final security policy and provided as a PDF file. Any changes to the security policy would require making changes to the corresponding source and generating a new version.

1 General

1.1 Overview

Notes: Overview information desired by the vendor

1.2 Security Levels

Annex B Requirement Statements

- Security Level Table – A table that indicates the individual clause levels and overall level
- Security Rating – The overall Security Rating of the module and the Security Levels of individual areas [moved from Annex B Section 2]

Notes: Table generated from previously entered information

1.3 Additional Information [O]

Notes: Additional vendor information

2 Cryptographic Module Specification

2.1 Description

Annex B Requirement Statements

- Description – Description of the module
- Purpose – The intended purpose or use of the module, including the intended use environment
- Module Type – Hardware, software, firmware, or hybrid designation
- Embodiment – Specific embodiment of the module (e.g., single-chip, multi-chip embedded, or multi-chip stand-alone) [Moved from Annex B Section 7]
- Tested Operational Environment's Physical Perimeter (TOEPP) – Location of the cryptographic module with respect to the TOEPP that is part of the module's tested configuration but may be outside the module's cryptographic boundary so that all of the logical and physical layers between the cryptographic module and the TOEPP are clearly defined. This also includes a description and components list of the TOEPP.
- TOEPP and Cryptographic Boundary – Precise definition of the module's TOEPP and cryptographic boundary
- Diagram, Schematic, or Photograph – Illustrative diagram, schematic, or photograph of the module. If the security policy encompasses multiple versions of the module, each version is represented separately or annotated to note that the representation is illustrated for all versions. For a software, firmware, hybrid, or

sub-chip cryptographic module, the security policy includes a block diagram that illustrates:

a. Location of Logical Object – 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 of the logical and physical layers between the logical object and the cryptographic boundary are clearly defined.
b. Interactions of the Logical Object – 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.
c. Block Diagram – Block diagram, as applicable

Notes: The image will show the disjoint hardware component of the hybrid module.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification - Hardware

Annex B Requirement Statements

- Operational Environment List – The operating system(s) and tested platform(s) [Moved from Annex B Section 6]

Notes: None

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Annex B Requirement Statements

- Executable Code – The form and components of the executable code provided [Moved from Annex B Section 5]

Notes: List of executable code

Tested Module Identification – Hybrid Disjoint Hardware

Annex B Requirement Statements

- Version Information - Provide version/identification of the module(s) and all components (hardware, software or firmware).

Notes: List of disjoint hardware for hybrid module

Tested Operational Environments – Software, Firmware, Hybrid

Annex B Requirement Statements

- Operating Systems – For software, firmware, and hybrid cryptographic modules, list the operating system(s) that the module was tested on, and list the operating system(s) that the vendor affirms can be used by the module.

Notes: None

Vendor-Affirmed Operational Environments – Software, Firmware, Hybrid

Annex B Requirement Statements

- Operating Systems – For software, firmware, and hybrid cryptographic modules, list the operating system(s) that the module was tested on, and list the operating system(s) that the vendor affirms can be used by the module.
- Vendor-Affirmed OE [operational environment] Claim – The vendor may provide claims of porting to other OSs [operating systems] not specifically tested yet vendor affirmation of correct operation is claimed.

Notes: None

2.3 Excluded Components

Annex B Requirement Statements

- Excluded Components – The hardware, software, or firmware excluded from the cryptographic boundaries specified in the security policy

Notes: Enter "None" instead of leaving blank

2.4 Modes of Operation

Modes List and Description

Annex B Requirement Statements

- Modes of Operation – Modes of operation and how to enter/exit each mode. The security policy describes each approved mode of operation implemented in the cryptographic module and how each mode is configured.

Notes: List of the Modes of Operation

Mode Change Instructions and Status [O]

Notes: None

Degraded Mode [O]

Annex B Requirement Statements

- Degraded Mode – Description of the degraded operation

2.5 Algorithms

Approved Algorithms

Annex B Requirement Statements

- Security Functions Table – The table of all security functions with specific key strengths employed for approved services as well as the implemented modes of operation (e.g. CBC [Cipher Block Chaining], CCM [Counter with Cipher Block Chaining-Messsage Authentication Code]), if appropriate

Notes: This table is generated from the selected CAVP-tested algorithms, modes, and properties

Vendor-Affirmed Algorithms

Annex B Requirement Statements

- Security Functions Table – The 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

SP800-140 Requirement Statements

- Vendor-Affirmed Security Methods – The vendor provided non-proprietary security policy shall include a list of all vendor-affirmed security methods. [VE02.20.04]

Notes: A list of the vendor-affirmed algorithms allowed in the approved mode of operation.

Non-Approved, Allowed Algorithms

Annex B Requirement Statements

- Security Functions Table – The 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

Notes: A list of the non-approved algorithms allowed in the approved mode of operation.

Non-Approved Allowed Algorithms with No Security Claimed

Annex B Requirement Statements

- Security Functions Table – The 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

Notes: A list of the non-approved algorithms allowed in the approved mode of operation with no security claimed. 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.

Non-Approved Not-Allowed Algorithms

Notes: None

2.6 Security Function Implementations

Annex B Requirement Statements

- Security Functions Table – The 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

Notes: None

2.7 Algorithm Specific Information

Notes: Documentation requirements for specific algorithms and conditions

2.8 RBG [Random Bit Generator] and Entropy

Annex B Requirement Statements

- Entropy Sources – The specific RBG [random bit generator] entropy source(s) [Moved from Annex B Section 9]
- RBGs – The specific approved and non-approved random bit generators. [Moved from Annex B Section 9]
- RBG Output – Descriptions of the uses of RBG output(s) [Moved from Annex B Section 9]

Notes: None

2.9 Key Generation

Notes: None

2.10 Key Establishment

Key Agreement Information

Notes: None

Key Transport Information

Notes: None

2.11 Industry Protocols

Notes: None

2.12 Additional Information [O]

Notes: Additional vendor information

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Annex B Requirement Statements

- Ports and Interfaces Table – The table listing of all ports and interfaces (physical and logical)
- Information Passing – Define the information passing over the five logical interfaces
- Physical Ports – Specify physical ports and data that pass over them

Notes: 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.

3.2 Trusted Channel Specification [O]

Annex B Requirement Statements

- Trusted Channel – Specify trusted channel

Notes: None

3.3 Control Interface Not Inhibited [O]

Annex B Requirement Statements

- Control Interface Not Inhibited – Specification of the exceptions and rationale if the control output interface is not inhibited during the error state

Notes: None

3.4 Additional Information [O]

Notes: Additional vendor information

4 Roles, Services, and Authentication

4.1 Authentication Methods

Annex B Requirement Statements

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

Notes: None

4.2 Roles

Annex B Requirement Statements

- Roles List – Specify all roles

Notes: None

4.3 Approved Services

Annex B Requirement Statements

- Approved and Non-Approved Services – Separately list the security and non-security services, both approved and non-approved
- Service Information – For each service, 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 (e.g., algorithms, key management techniques, or authentication techniques) 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 functions it uses. For each operator role authorised to use the service information describing the individual access rights to all SSPs and information describing the method used to authenticate each role.
- Roles List – A list of all of the roles
- Roles Table – A table of roles with corresponding service commands with input and output

Notes: None

4.4 Non-Approved Services

Annex B Requirement Statements

- Approved and Non-Approved Services – A Separately list the security and non-security services, both approved and non-approved
- Service Information – For each service, 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 (e.g., algorithms, key management techniques, 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 functions it uses. For each operator role authorised to use the service information describing the individual access rights to all SSPs and information describing the method used to authenticate each role.

Notes: None

4.5 External Software/Firmware Loaded

Annex B Requirement Statements

- External Software/Firmware Loaded – If external software or firmware is loaded, specify the controls on loading and the isolation of code that deter unauthorised access to and use of the module.

Notes: None

4.6 Bypass Actions and Status [O]

Annex B Requirement Statements

- Bypass Actions – If there is a bypass capability, what are the two independent actions and how is the status checked?

Notes: None

4.7 Cryptographic Output Actions and Status [O]

Annex B Requirement Statements

- Cryptographic Output – If there is a self-initiated cryptographic output capability, what are the two independent actions how is the status indicated?

Notes: None

4.8 Additional Information [O]

Notes: Additional vendor information

5 Software/Firmware Security

5.1 Integrity Techniques

Annex B Requirement Statements

- Integrity Techniques – Specify the approved integrity techniques or EDC [error detection code] employed

Notes: None

5.2 Initiate on Demand

Annex B Requirement Statements

- Initiate on Demand – Specify how the operator can initiate the integrity test on demand

Notes: None

5.3 Open-Source Parameters [O]

Annex B Requirement Statements

- Open-Source Parameters – If the module is open source, specify the compilers and control parameters required to compile the code into an executable format.

Notes: None

5.4 Additional Information [O]

Notes: Additional vendor information

6 Operational Environment

6.1 Operational Environment Type and Requirements

Operational Environment Type

Annex B Requirement Statements

- Operational Environment Type – Identify the operational environment (e.g. non-modifiable, limited, or modifiable)

Notes: Include an explanation supporting the OE [operational environment] type

Operational Environment Requirements [O]

Annex B Requirement Statements

- Operational Environment Requirements – For each applicable level, explain how requirements are satisfied.

Notes: None

6.2 Configuration Settings and Restrictions [O]

Annex B Requirement Statements

- Configuration Settings – Specification of the security rules, settings, or restrictions to the configuration of the operational environment
- Restrictions – Specification of any restrictions to the configuration of the operational environment

Notes: None

6.3 Additional Information [O]

Notes: Additional vendor information

7 Physical Security

7.1 Mechanisms and Actions Required

Annex B Requirement Statements

- Mechanisms – Specify the physical security mechanisms that are implemented in the module (e.g., tamper-evident seals, locks, tamper response and zeroisation switches, and alarms)
- Actions Required – 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)

Notes: None

7.2 User Placed Tamper Seals [O]

Total Number to Place [O]

Annex B Requirement Statements

- Total Number to Place – The total number of tamper evident seals or security appliances that are needed will be indicated (e.g. 5 tamper evident seals and 2 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).

Notes: None

Tamper Seal Placement [O]

Annex B Requirement Statements

- Reference Photos Include Tamper Seals – The reference photo or illustrations required in B 2.2 that reflect the module configured or constructed as specified as well as additional photos/illustrations that reflect other configurations if the module requires operator-applied tamper-evident seals or security appliances over the life cycle of the module
- Photos of Tamper Seal Placement – Photos or illustrations will indicate the precise placement of any tamper-evident seal or security appliance needed to meet the physical security requirements

Notes: None

Surface Preparation [O]

Annex B Requirement Statements

- Prepare Surface – Clear instructions regarding how the surface or device shall be prepared to apply a new tamper-evident seal or security appliance if tamper-evident seals or security appliances can be removed or installed

Notes: None

Unused Seals [O]

Annex B Requirement Statements

- Unused Seals – Specify the operator role responsible for securing and having control at all times of any unused seals, and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to an approved mode of operation

Notes: None

Part Numbers [O]

Annex B Requirement Statements

- Part Numbers – If the tamper evident seals or security appliances are parts that can be reordered from the module vendor, the security policy will indicate the module vendor part number of the seal, security appliance or

applicable security kit. After reconfiguring, the operator of the module may be required to remove and introduce new tamper-evident seals or security appliances.

Notes: None

7.3 Filler Panels [O]

Annex B Requirement Statements

- Filler Panel Information – 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.

Notes: None

7.4 Fault Induction Mitigation [O]

Annex B Requirement Statements

- Fault Induction Mitigation – Specify the fault induction mitigation methods implemented

Notes: None

7.5 EFP/EFT Information [O]

SP800-140 Requirement Statements

- Temperature Shutdown/Zeroise – The security policy shall address whether the employed EFP feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met. [VE07.77.02]
- EFT Shutdown/Zeroise The security policy shall address whether the employed EFT feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met [VE07.81.02]

Notes: For physical Security Level 3 and above.

7.6 Hardness Testing Temperature Ranges [O]

SP800-140 Requirement Statements

- High and Low Temperature – The vendor provided security policy shall specify the nominal and high/low temperature range. [VE07.26.02]

Notes: For modules covered by strong or hard conformal or non-conformal enclosures, coatings, or potting materials.

7.7 Additional Information [O]

Notes: Additional vendor information

8 Non-Invasive Security

8.1 Mitigation Techniques [O]

Annex B Requirement Statements

- Mitigation Techniques – Specify all of the non-invasive mitigation techniques referenced in Annex F employed by the module to protect the module's CSPs [critical security parameter] from non-invasive attacks

Notes: Per IG 12.A, until the requirements of NIST SP 800-140F are defined, non-invasive mechanisms fall under ISO/IEC 19790:2012 Section 7.12 Mitigation of other attacks

8.2 Effectiveness [O]

Annex B Requirement Statements

- Effectiveness – Describe the effectiveness of the non-invasive mitigation techniques referenced in Annex F employed by the module to protect the module's CSPs from non-invasive attacks

Notes: See B.2.8.1 above

8.3 Additional Information [O]

Notes: Additional vendor information

9 Sensitive Security Parameters Management

9.1 Storage Areas

Annex B Requirement Statements

- SSP Storage – Specify the SSP storage areas, formats (encrypted or plaintext), and persistence types (dynamic or static)

Notes: None

9.2 SSP Input-Output Methods

Annex B Requirement Statements

- SSP I/O Methods – Specify the electronic and manual SSP I/O method(s)

Notes: None

9.3 SSP Zeroization Methods

Annex B Requirement Statements

- SSP Zeroization – Specify the unprotected SSP zeroisation method(s) and rationale and operator initiation capability

SP800-140 Requirement Statements

- SSP Procedural Zeroisation – If SSPs are zeroised procedurally while under the control of the operator (i.e., present to observe the method has completed successfully or controlled via a remote management session), vendor documentation and the module security policy must specify how the methods shall be performed. [VE09.28.03]

Notes: None

9.4 SSPs

Annex B Requirement Statements

- SSP Key Table – Provide a SSP table specifying the SSP type(s), strength(s) in bits, security function(s), security function certification number(s), where and how the SSP(s) is generated, what method(s) is used to input or output the SSP(s), any SSP generation and establishment method used and indicate any related SSPs.
- SSP Other Table – Present a table of other SSPs and how they are generated
- SSP Zeroization – Specify the unprotected SSP zeroisation method(s) and rationale, and operator initiation capability

Notes: None.

9.5 Transitions [O]

Annex B Requirement Statements

- Transitions – Specify applicable transition periods or timeframes where an algorithm or key length transitions from approved to non-approved

Notes: None

9.6 Additional Information [O]

Notes: Additional vendor information

10 Self-Tests

10.1 Pre-Operational Self-Tests

Annex B Requirement Statements

- Pre-Operational and Conditional List – Provide the list of pre-operational and conditional self-tests with defined parameters and list conditions under which the tests are performed

Notes: Separate the Pre-Operational from the Conditional.

10.2 Conditional Self-Tests

Annex B Requirement Statements

- Pre-Operational and Conditional List – Provide the list of pre-operational and conditional self-tests with defined parameters and list conditions under which the tests are performed

Notes: Separate the Pre-Operational from the Conditional.

10.3 Periodic Self-Test Information

Annex B Requirement Statements

- Self-test Interruption – Specify the time period and the policy regarding any conditions that may result in the interruption of the module's operations during the time to repeat the period self-tests

Notes: List of the periodic information for the Pre-Operational tests and Conditional tests

10.4 Error States

Annex B Requirement Statements

- Error State List – Describe all error states and status indicators

Notes: None

10.5 Operator Initiation of Self-Tests [O]

Annex B Requirement Statements

- Operator Initiation Self-test – Describe operator initiation, if applicable

Notes: None

10.6 Additional Information [O]

Notes: None

11 Life Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Annex B Requirement Statements

- Startup Procedures – Specify the procedures for secure installation, initialization, startup and operation of the module
- Installation Process and Authentication Mechanisms – Describe the installation process and the cryptographic authentication mechanism(s)

Notes: None

11.2 Administrator Guidance

Annex B Requirement Statements

- Administrator and Non-Administrator Guidance – Provide the Administrator and Non-Administrator guidance (may be a separate document)

Notes: None

11.3 Non-Administrator Guidance

Annex B Requirement Statements

- Administrator and Non-Administrator Guidance – Provide the Administrator and non-Administrator guidance (may be a separate document)

Notes: None

11.4 Design and Rules [O]

Annex B Requirement Statements

- Design and Rules – Overall security design and the rules of operation. [Moved from Annex B Section 2]

Notes: None

11.4 Maintenance Requirements [O]

Annex B Requirement Statements

- Maintenance Requirements – Specify any maintenance requirements

Notes: None

11.5 End of Life [O]

Notes: End-of-life procedures

11.6 Additional Information [O]

Notes: Additional vendor information

12 Mitigation of Other Attacks

12.1 Attack List [O]

Annex B Requirement Statements

- Attack List - Specify what other attacks are mitigated

Notes: The level of detail describing the security mechanism(s) implemented to mitigate other attacks must be similar to what is found on advertisement documentation (product glossies)

12.2 Mitigation Effectiveness [O]

Annex B Requirement Statements

- Mitigation Effectiveness – Describe the effectiveness of the mitigation techniques listed

Notes: None

12.3 Guidance and Constraints [O]

Annex B Requirement Statements

- Guidance and Constraints – List security-relevant guidance and constraints

Notes: Non-approved algorithms not allowed in the approved mode of operation

12.4 Additional Information [O]

Notes: Additional vendor information

Appendix A. Document Revisions

Edition	Date	Change
Revision 1 (r1)	November 2023	This revision introduces the following significant changes to NIST SP 800-140B: 1. Defines a more detailed structure and organization for the security policy (SP) 2. Captures security policy requirements that are defined in NIST SP 800-140 3. Provides a direct mapping between the ISO, NIST SP 800-140 requirements, and the new structure of the SP 4. Adds several tables to the set collected by Web Cryptik 5. Defines required relationships and constraints between the data in the SP tables 6. Builds the SP document as a combination of the text portions of the SP and the tables entered in Web Cryptik and stored in JSON format 7. Generates the approved algorithm table based on lab/vendor selections from the algorithm tests

Appendix B. List of Symbols, Abbreviations, and Acronyms

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

CAVP
Cryptographic Algorithm Validation Program

CMVP
Cryptographic Module Validation Program

CSTL
Cryptographic and Security Testing Laboratory

EFP
Environmental Failure Protection

EFT
Environmental Failure Testing

FIPS
Federal Information Processing Standard

SSP
Sensitive Security Parameter

TE
Test Evidence

TOEPP
Tested Operational Environment's Physical Perimeter

VE
Vendor Evidence