Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date November 17, 2023

Original Release Date October 17, 2022

The attached draft document is followed by:

Status Final

Series/Number NIST SP 800-140Br1

Title Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B

Publication Date November 2023

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

CSRC URL https://csrc.nist.gov/pubs/sp/800/140/b/r1/final

Additional Information

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

NIST Special Publication
NIST SP 800-140Br1 2pd

CMVP Security Policy Requirements

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

Second Public Draft

David Hawes
Alexander Calis
Roy Crombie

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140Br1.2pd

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

NIST Special Publication
NIST SP 800-140Br1 2pd

CMVP Security Policy Requirements

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

Second Public Draft

David Hawes
Alexander Calis
Computer Security Division
Information Technology Laboratory

Roy Crombie
Canadian Centre for Cyber Security

https://doi.org/10.6028/NIST.SP.800-140Br1.2pd

October 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

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 the National Institute of Standards and Technology (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.

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

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

How to Cite this NIST Technical Series Publication:

Hawes D, Calis A, Crombie R (2022) 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) 800-140Br1 2pd. https://doi.org/10.6028/NIST.SP.800-140Br1.2pd

Author ORCID iDs

David Hawes: 0000-0002-0173-6795
Alexander Calis: 0000-0003-1937-8129

Public Comment Period

October 17, 2022 - December 5, 2022

Submit Comments

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. The special publication modifies only those requirements identified in this document. 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 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.

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.

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

List of Tables

155

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 6.1 of this document specifies any modifications to ISO/IEC 19790 Annex B and ISO/IEC 24759 section 6.14. Section 6.2 identifies any additional requirements for the Security Policy that are documented in other publications. Section 6.3 provides descriptions of the structure of the Security Policy and how the requirements in sections 6.1 and 6.2 map into that structure. Appendix A indicates specific details for the module information that will be entered in table format within the Web Cryptik application.

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. 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 a 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 the logical and physical layers between the logical object and the cryptographic boundary are clearly defined; and
    - the 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.
    - 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 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 a ~~key~~ SSP 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), any SSP generation and establishment method used and indicate any related ~~keys~~ SSPs.
- Specify the electronic and manual ~~key~~ SSP I/O 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 Life-cycle assurance

No Change.

B.2.12 Mitigation of other attacks

No Change.

6.2. Documentation requirement additions

In addition to ISO/IEC 24759 section 6.14 and ISO/IEC 19790 Annex B, other publications and documents specify documentation requirements for the Security Policy. Many of these requirements relate to 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

1. 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

B.2.6 Operational environment

No Additions.

B.2.7 Physical security

SP800-140:VE07.26.02

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

SP800-140:VE07.77.02

1. 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.

SP800-140:VE07.81.02

1. 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.

B.2.8 Non-invasive security

No Additions.

B.2.9 Sensitive security parameters management

SP800-140:VE09.28.03

1. 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.

B.2.10 Self-tests

No Additions.

B.2.11 Life-cycle assurance

No Additions.

B.2.12 Mitigation of other attacks

No Additions.

6.3. Documentation input, structure, and formatting

This section is intended to provide 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 6.2. All of the requirement statements are organized into appropriately named and numbered sub-sections (i.e. 1.2- Security Levels, 2.1 – Purpose or Use). Each sub-section identifies the applicable requirements and provides any clarifying and explanatory notes for that sub-section.

A significant portion of the security policy information will be structured and interrelated. These tables can be input through Web Cryptik or uploaded in JSON format which would follow a provided schema and table relationship constraints.

The text/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 serving as placeholders for the structured content in Web Cryptik and/or the uploaded JSON file.

In this update to 140B and the corresponding update to Web Cryptik, the labs/vendors will be selecting algorithms, modes, and properties from the sets that have been tested through the CAVP process. This will replace the previous process of separately enter that information.

Part of the initial information 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/operational environment entry will be listed, along with the set of properties 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, 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 this information (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.

1.0 General

1.1 Overview

Notes: Overview information desired by the vendor

Input Method: Template Document

1.2 Security Levels

Annex B Requirement Statements

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

Notes: Table generated from previously entered information

Input Method: Web Cryptik/JSON

1.3 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

2.0 Cryptographic module specification

2.1 Module Information

2.1.1 Description

Annex B Requirement Statements

1. Description - Description of Module

Notes: None

Input Method: Template Document

2.1.2 Purpose or Use

Annex B Requirement Statements

1. Purpose - Intended purpose or use of the module including intended use environment

Notes: None

Input Method: Template Document

2.1.3 Module Type

Annex B Requirement Statements

1. Module Type - Hardware, Software, Firmware, or Hybrid designation:

Notes: None

Input Method: Web Cryptik/JSON

2.1.4 Module Embodiment

Annex B Requirement Statements

1. Embodiment - Specify the embodiment (single-chip, multi-chip embedded or multi-chip standalone).

Notes: None

Input Method: Web Cryptik/JSON

2.1.5 Module Characteristics

Notes: None

Input Method: Web Cryptik/JSON

2.1.6 Cryptographic Boundary

Annex B Requirement Statements

1. TOEPP and Cryptographic Boundary - Precise definition of the module's TOEPP and cryptographic boundary:

Notes: None

Input Method: Template Document

2.1.7 TOEPP [O]

Annex B Requirement Statements

1. TOEPP and Cryptographic Boundary - Precise definition of the module's TOEPP and cryptographic boundary:
2. 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 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.

Notes: None

Input Method: Template Document

2.1.8 Diagram, Schematic, or Photograph

Annex B Requirement Statements

1. Diagram, Schematic, or Photograph - 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, firmware, hybrid, or a sub-chip cryptographic module, the security policy includes a block diagram that illustrates
2. 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 the logical and physical layers between the logical object and the cryptographic boundary are clearly defined
3. 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.

4. Block Diagram - Block Diagram, as applicable.

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

Input Method: Template Document

2.2 Version Information

Annex B Requirement Statements

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

Notes: Table generated from previously entered information

Input Method: Web Cryptik/JSON

2.3 Operating Environments

2.3.1 Hardware OEs

Annex B Requirement Statements

1. Operational Enviornment List - Identify the operating system(s) and tested platform(s).

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.3.2 Software, Firmware, Hybrid OEs

Annex B Requirement Statements

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

Notes: None

Input Method: Web Cryptik/JSON

2.3.3 Executable Code List [O]

Annex B Requirement Statements

1. Executable Code - Specify the form and each component of executable code provided.

Notes: List of executable code

Input Method: Web Cryptik/JSON

2.3.4 Vendor Affirmed Operating Environments

Annex B Requirement Statements

1. Operating Systems - for software, firmware and hybrid cryptographic modules, list the operating system(s) the module was tested on and list the operating system(s) that the vendor affirms can be used by the module.
2. Vendor Affirmed OE Claim - The vendor may provide claims of porting to other OS's not specifically tested yet vendor affirmation of correct operation is claimed.

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.4 Excluded Components

Annex B Requirement Statements

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

Notes: Enter "None" instead of leaving blank

Input Method: Template Document

2.5 Modes of Operation

2.5.1 Modes List and Description

Annex B Requirement Statements

1. 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.
2. 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: Text accompanying the Mode List

Input Method: Template Document

Notes: List of the Modes of Operation

Input Method: Web Cryptik/JSON

2.5.2 Mode Change Instructions [O]

Notes: None

Input Method: Template Document

2.5.3 Degraded Mode [O]

Annex B Requirement Statements

1. Degraded Mode - Description of degraded operation

Notes: Enter "None" instead of leaving blank

Input Method: Template Document

2.6 Algorithms

2.6.1 Approved Algorithms

Annex B Requirement Statements

1. Security Functions Table - 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: This table is generated from the selected CAVP Tested algorithms, modes, and properties

Input Method: CAVP Algorithm-Mode-Property Selection

2.6.2 Vendor Affirmed Algorithms

Annex B Requirement Statements

1. Security Functions Table - 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

1. 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 - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.6.3 Non-Approved, Allowed Algorithms

Annex B Requirement Statements

1. Security Functions Table - 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 - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.6.4 Non-Approved, Allowed Algorithms with No Security Claimed

Annex B Requirement Statements

1. Security Functions Table - 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. - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.6.5 Non-Approved, Not Allowed Algorithms

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.7 Security Function Implementations

Annex B Requirement Statements

1. Security Functions Table - 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: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

2.8 Algorithm Specific Information

Notes: Documentation Requirements for Specific Algorithms and Conditions

Input Method: Template Document

2.9 RNG and Entropy

678
679 **2.9.1 Entropy Information**
680 Annex B Requirement Statements
681 1. Entropy Sources - Specify the RBG entropy source(s).
682
683 **Notes**: None
684
685 **Input Method**: Template Document
686
687 **2.9.2 RNG Information**
688 Annex B Requirement Statements
689 1. RNGs - Specify the approved and non-approved random bit generators
690 2. RNG Output - Describe the uses of RBG output(s).
691
692 **Notes**: None
693
694 **Input Method**: Template Document
695
696 **2.10 Key Generation**
697
698 **Notes**: None
699
700 **Input Method**: Template Document
701
702 **2.11 Key Establishment**
703
704 **2.11.1 Key Agreement Information**
705
706 **Notes**: None
707
708 **Input Method**: Template Document
709
710 **2.11.2 Key Transport Information**

Notes: None

Input Method: Template Document

2.12 Industry Protocols

Notes: None

Input Method: Template Document

2.13 Design and Rules

Annex B Requirement Statements

1. Design and Rules - Overall security design and the rules of operation

Notes: As part of this requirement, algorithm-specific guidance, rules, and security policy-specific requirements shall be included.

Input Method: Template Document

2.14 Initialisation

Annex B Requirement Statements

1. Initialisation - Initialisation requirements, as applicable.

Notes: None

Input Method: Template Document

2.15 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

3.0 Cryptographic module interfaces

3.1 Ports and Interfaces

Annex B Requirement Statements

1. Ports and Interfaces Table - Table listing of all ports and interfaces (physical and logical).
2. Information Passing - Define the information passing over the five logical interfaces.
3. 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. - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

3.2 Trusted Channel Specification [O]

Annex B Requirement Statements

1. Trusted Channel - Specify Trusted Channel

Notes: None

Input Method: Template Document

3.3 Control Interface Not Inhibited [O]

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

3.4 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

4.0 Roles, services, and authentication

4.1 Authentication Methods

Annex B Requirement Statements

1. Authentication Methods - Specify each authentication method, whether the method is Identity or Role-based and the method is required.
2. Strength of Authentication - How is the strength of authentication requirement met?
3. Service Info - 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 (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 authorised to use the service info

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

4.2 Roles

Annex B Requirement Statements

1. Roles List - Specify all roles
2. Roles Table - Table of Roles, with corresponding service commands with input and output

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

4.3 Approved Services

Annex B Requirement Statements

1. Approved and Non-Approved Services - Separately list the security and non-security services, both approved and non-approved.
2. Service Info - 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 (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 authorised to use the service info
3. Roles List - Specify all roles

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

4.4 Non-Approved Services

Annex B Requirement Statements

1. Approved and Non-Approved Services - Separately list the security and non-security services, both approved and non-approved.
2. Service Info - 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 (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 authorised to use the service info

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

4.5 External Software/Firmware Loaded

Annex B Requirement Statements

1. 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

Input Method: Template Document

4.6 Bypass Actions and Status [O]

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

4.7 Cryptographic Output Actions and Status [O]

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

4.8 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

5.0 Software/Firmware security

5.1 Integrity Techniques

Annex B Requirement Statements

1. Integrity Techniques - Specify the approved integrity techniques or EDC employed

Notes: None

Input Method: Template Document

5.2 Initiate on Demand

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

5.3 Open Source Parameters [O]

Annex B Requirement Statements

1. 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

Input Method: Template Document

5.4 Non-Reconfigurable Memory End of Life Procedures [O]

Notes: None

Input Method: Template Document

5.5 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

6.0 Operational environment

6.1 Operational Environment Type and Requirements

6.1.1 Operational Environment Type

Annex B Requirement Statements

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

Notes: Include an explanation supporting the OE type

Input Method: Template Document

6.1.2 Operational Environment Requirements [O]

Annex B Requirement Statements

1. Op Env Requirements - For each applicable level, explain how requirements are satisfied.

Notes: None

Input Method: Template Document

6.2 Configuration Settings and Restrictions [O]

Annex B Requirement Statements

1. Config Settings - Specification of the security rules, settings or restrictions to the configuration of the operational environment.
2. Restrictions - Specification of any restrictions to the configuration of the operational environment.

Notes: None

948

949 **Input Method:** Template Document

950

951 **6.3 Additional Information [O]**

952

953 **Notes:** Additional Vendor Information

954

955 **Input Method:** Template Document

956

957 **7.0 Physical security**

958

959 **7.1 Mechanisms and Actions Required**

960 Annex B Requirement Statements

961 1. Mechanisms - Specify the physical security mechanisms that are implemented in
962 the module (e.g. tamper evident seals, locks, tamper response and zeroisation
963 switches, and alarms).

964 2. Actions Required - Specify the actions required by the operator(s) to ensure that
965 the physical security is maintained (e.g. periodic inspection of tamper-evident
966 seals or testing of tamper response and zeroisation switches).

967

968 **Notes:** See Appendix A - SP Detailed Information Description

969

970 **Input Method:** Web Cryptik/JSON

971

972 **7.2 Tamper Seals [O]**

973

974 **7.2.1 Total Number to Place [O]**

975 Annex B Requirement Statements

976 1. Total Number to Place - The total number of tamper evident seals or security
977 appliances that are needed will be indicated (e.g. 5 tamper evident seals and 2
978 opacity screens). The photos or illustrations which provide instruction on the
979 precise placement will have each item numbered in the photo or illustration and
980 will equal the total number indicated (the actual tamper evident seals or security
981 appliances are not required to be numbered).

982

Notes: None

Input Method: Template Document

7.2.2 Tamper Seal Placement [O]

Annex B Requirement Statements

1. Reference Photos Include Tamper Seals - 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.
2. 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

Input Method: Template Document

7.2.3 Prepare Surface [O]

Annex B Requirement Statements

1. Prepare Surface - If tamper evident seals or security appliances can be removed or installed, clear instructions will be included regarding how the surface or device shall be prepared to apply a new tamper evident seal or security appliance.

Notes: None

Input Method: Template Document

7.2.4 Unused Seals [O]

Annex B Requirement Statements

1. 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

Input Method: Template Document

7.2.5 Part Numbers [O]

Annex B Requirement Statements

1. 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

Input Method: Template Document

7.3 Filler Panels [O]

Annex B Requirement Statements

1. Filler Panel Info - 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

Input Method: Template Document

7.4 Fault Induction Mitigation [O]

Annex B Requirement Statements

1. Fault Induction Mitigation - Specify the fault induction mitigation methods implemented.

Notes: None

Input Method: Template Document

7.5 EFP/EFT Information [O]

SP800-140 Requirement Statements

1. 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]
2. 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 - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

7.6 Hardness Testing Temperature Ranges [O]

SP800-140 Requirement Statements

1. 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 - See Appendix A - SP Detailed Information Description

Input Method: Template Document

7.7 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

8.0 Non-invasive security

8.1 Mitigation Techniques [O]

Annex B Requirement Statements

1. Mitigation Techniques - Specify all 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: Per IG 12.A: Until requirements of SP 800-140F are defined, non-invasive mechanisms fall under ISO/IEC 19790:2012 Section 7.12 Mitigation of other attacks

Input Method: Template Document

8.2 Effectiveness [O]

Annex B Requirement Statements

1. 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.

Input Method: Template Document

8.3 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

9.0 Sensitive security parameters management

9.1 Storage Areas

Annex B Requirement Statements

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

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

9.2 SSP Input-Output Methods

Annex B Requirement Statements

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

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

9.3 SSP Zeroization Methods

Annex B Requirement Statements

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

SP800-140 Requirement Statements

1. 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: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

9.4 SSPs

Annex B Requirement Statements

1. 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.

2. SSP Other Table - Present a table of other SSPs and how they are generated.
3. SSP Zeroization - Specify the unprotected SSP zeroisation method(s) and rationale, and operator initiation capability.

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

9.5 Transitions [O]

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

9.6 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

10.0 Self-tests

10.1 Pre-Operational Self-Tests

Annex B Requirement Statements

1. 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 - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

10.2 Conditional Self-Tests

Annex B Requirement Statements

1. 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 - See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

10.3 Periodic Self-Test Information

Annex B Requirement Statements

1. 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: None

Input Method: Template Document

Notes: List of the periodic info for the PreOp Tests

Input Method: Web Cryptik/JSON

Notes: List of the periodic info for the conditional tests

Input Method: Web Cryptik/JSON

10.4 Error States

Annex B Requirement Statements

1. Error State List - Describe all error states and status indicators

Notes: See Appendix A - SP Detailed Information Description

Input Method: Web Cryptik/JSON

10.5 Operator Initiation Self-test [O]

Annex B Requirement Statements

1. Operator Initiation Self-test - Describe operator initiation, if applicable.

Notes: None

Input Method: Template Document

10.6 Additional Information [O]

Notes: None

Input Method: Template Document

11.0 Life-cycle assurance

11.1 Startup Procedures

Annex B Requirement Statements

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

Notes: None

Input Method: Template Document

11.2 Administrator Guidance

Annex B Requirement Statements

1. Administrator and non-Administrator Guidance - Provide the Administrator and non-Administrator guidance (may be a separate document).

Notes: None

Input Method: Template Document

11.3 Non-Administrator Guidance

Annex B Requirement Statements

1. Administrator and non-Administrator Guidance - Provide the Administrator and non-Administrator guidance (may be a separate document).

Notes: None

Input Method: Template Document

11.4 Maintenance Requirements [O]

Annex B Requirement Statements

1. Maintenance Requirements - Specify any maintenance requirements

Notes: None

Input Method: Web Cryptik

11.5 End of Life [O]

Notes: End of life procedures

Input Method: Template Document

11.6 Additional Information [O]

Notes: Additional Vendor Information

Input Method: Template Document

12.0 Mitigation of other attacks

12.1 Attack List [O]

Annex B Requirement Statements

1. 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).

Input Method: Template Document

12.2 Mitigation Effectiveness [O]

Annex B Requirement Statements

1. Mitigation Effectiveness - Describe the effectiveness of the mitigation techniques listed.

Notes: None

Input Method: Template Document

12.3 Guidance and Constraints [O]

Annex B Requirement Statements

1. Guidance and Constraints - List security-relevant guidance and constraints.

Notes: Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Input Method: Template Document

12.4 Additional Information [O]

1326

1327 **Notes:** Additional Vendor Information

1328

1329 **Input Method:** Template Document

1330

Appendix A. Security Policy Detailed Information Description

This appendix to SP800-140B contains detailed descriptions of the tables of information required. The columns represent information that will be entered into Web Cryptik or included in the json file. "[O]" designates that information for the column is optional and may be left blank. If the module doesn't have relevant information for a required column, enter "N/A".

Operating Environments – Hardware (2.3)

Table 1. Operating Environments – Hardware

Model/Part Number(s)	Hardware Version(s)	Firmware Version(s)	Processor(s)	Non-Security Relevant Distinguishing Features [O]

Notes

- Number of rows should correspond to module count
- Processor(s) – Needs to match processor information identified in OEs for corresponding CAVP testing
- Examples of distinguishing features may be ports and interfaces, memory storage devices and sizes, field replaceable and stationary accessories (power supplies, fans), etc.

Operating Environments – Software/Firmware/Hybrid (2.3)

Table 2. Operating Environments – Software/Firmware/Hybrid

Operating System (Guest OS if Hypervisor)	Hardware Platform	Processor(s)	PAA/PAI	Hypervisor and Host OS [O]

Notes

- One row for each Tested OE
- Processor(s) – Needs to match processor information identified in OEs for corresponding CAVP testing
- PAA/PAI – Enter Yes or No

Executable Code Sets - – Software/Firmware/Hybrid (2.3)

Table 3. Executable Code Sets - – Software/Firmware/Hybrid

Package/File Names	Software/ Firmware Version	Non-Security Relevant Distinguishing Features [O]	Hardware Version if Hybrid [O]	Integrity Test Implemented

Notes

- Number of rows corresponds to module count

Vendor Affirmed Operating Environments (2.3)

Table 4. Vendor Affirmed Operating Environments

Operating System	Hardware Platform

Notes

- No links to other tables

Modes of Operation (2.5)

Table 5. Modes of Operation

Name	Description	FIPS	Status Indicator

Notes

- Name – Unique name used as identifier
- Description
- FIPS (nonFIPS or FIPS)
- Status Indicator – Description of the source of the status indicator, for example from service or global indicator.
- Details related to entering and exiting the modes and/or configuration information should be included section 2.6 of the Security Policy

Vendor Affirmed Algorithms (2.6)

Table 6. Vendor Affirmed Algorithms

Algorithm	Algorithm Properties	OE	Reference
	Name: Value Name: Value Sub Properties: Name: Value Name: Value		

Notes

- Algorithm – Selected from list of possible entries
- Algorithm Properties – Follow the same structure that is used for Approved Algorithms
    - Over time, specific properties will be identified for the possible entries
    - CKG – list the type of key(s) (symmetric, asymmetric) and the specific reference(s) from SP800-133r2 that applies.
- OE – Selected from list of OEs represented by CAVP Tests
- Reference – Describe and provide reference to justification, a publication or IG reference, for example.

Non-Approved, Allowed Algorithms (2.6)

Table 7. Non-Approved, Allowed Algorithms

Algorithm	Algorithm Properties	OE	Reference
	Name: Value Name: Value Sub Properties: Name: Value Name: Value		

Notes

- Algorithm – Selected from list of possible entries
- Algorithm Properties – Follow the same structure that is used for Approved Algorithms
    - Over time, specific properties will be identified for the possible entries
- OE – Selected from list of OEs represented by CAVP Tests
- Reference – describe and provide reference to justification, a pub or IG reference, for example

Non-Approved, Allowed Algorithms with No Security Claimed (2.6)

Table 8. Non-Approved, Allowed Algorithms with No Security Claimed

Algorithm	Caveat	Use/Function

Notes

- No links to other tables

Non-Approved, Not Allowed Algorithms (2.6)

Table 9. Non-Approved, Not Allowed Algorithms

Algorithm	Use/Function

Notes

- No links to other tables

Security Function Implementations (SFI) (2.7)

Table 10. Security Function Implementations

Name	Type	Description	SF Properties [O]	Algorithms	Algorithm Properties
			Name: Value Name: Value Sub Properties: Name: Value Name: Value	Algo 1	Name: Value Name: Value Sub Properties: Name: Value Name: Value
				Algo 2	Name: Value Name: Value
				Algo 3	Name: Value

Notes

- Column Information
  - Name – a unique name that relates to the Security Function. It can be KTS1, or KTS xxx
  - Type – a value from the defined set of Security Functions
  - Description – how this is used
  - SF Properties – If there are specific properties or characteristics associated with this SF implementation. This could include a reference to a specific Publication

Section, IG, etc. This is where appropriate bit strength caveats should be included for KAS and KTS.

- Algorithms – what Algorithms from the tested and allowed lists are part of the implementation. Include prerequisites.
- Algorithm Properties – If a subset of the available properties are used, specify.

- What is meant by Implementations of Security Functions
  - A module can (and often does) have more than one implementation for a given Security Function type
    - A KTS that uses an authenticated encryption mode vs. separate encryption and authentication would both be KTS but would have two implementation entries
    - A SigVer could be used for role/identity authentication and also for an integrity test
    - Block Cipher could include modes for storage (XTS) or as part of a KTS
    - The same algorithm could be used with different key sizes to support different sizes
  - For many modules, there would likely be one SFI for a SF type.
- Why these wouldn't just map directly to Services
  - At times, these could map directly to services, particularly for modules like software libraries.
  - Documenting in this manner will clarify which algorithms are actual services provided and which are supporting or prerequisite
  - When the same category SF algorithms are used for different functions and therefore different services, there should be separate SFIs. Many modules have multiple DigSigVer implementations. For example, one for authentication during an SSH connection and one for the module startup integrity test. These should be separately defined as implementations and then mapped to different services.
  - Requiring the Services to map directly to the Security Functions seems to overreach into the vendor's design of their module. The Services and corresponding level of granularity should be left to the vendor to determine.
- There should only be entries for top-level functions. For example, if SHA2-256 is only used for Hash DRBG, then it shouldn't be included as a separate Secure Hash entry. And, if the DRBG is only a supporting function (for example, just a prerequisite to Symmetric Key Generation), then DRBG shouldn't be a separate entry in this table. The Services table will include the Security Function Implementations, so often that will likely determine what is a top-level entry.
- All the supporting and prerequisite algorithms for that implementation would be included in the Algorithms column.
- Every tested and allowed algorithm should be included somewhere in this table.

- Every SFI should be included in the Services table.

Entropy Sources (2.9)

Table 11. Entropy Sources

Name	Type	Operating Environment	Sample Size	Entropy per sample	Conditioning Components (CAVP number if vetted)

Notes

- Type - Physical or Non-Physical
- In the future, this information will be gathered from the ESV system

Ports and Interfaces (3.1)

Table 12. Ports and Interfaces

Physical Port	Logical Interface	Data that passes over the port/interface

Notes

- No links to other tables

Authentication Methods (4.1)

Table 13. Authentication Methods

Name	Description	Mechanism	Strength Each	Strength Per Minute [O]

Notes

- Mechanism can be module algorithm, SFI, or alternative

Roles (4.2)

1502 **Table 14.** Roles

Name	Type	Operator Type	Authentication Methods

1503

1504 Notes

1505 • Type – Role, Identity, or Multi-Factor Identity

1506 • Operator Type – CO, Owner, or other

1507 • Authentication Methods selected from existing table entries

1508

1509 **Approved Services (4.3)**

1510

1511 **Table 15.** Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access

1512

1513 Notes

1514 • Security Function Implementations - selected from existing SFI table entries

1515 • Roles

1516 o selected from existing Roles table entries

1517 o could have multiple entries

1518 o could also be “Unauthenticated”

1519 • Roles SSP Access

1520 o For each role entry, this column has entries for each SSP accessed by that role
1521 using that service with the appropriate access indicators

1522 ▪ Generate: The module generates or derives the SSP.

1523 ▪ Read: The SSP is read from the module (e.g. the SSP is output).

1524 ▪ Write: The SSP is updated, imported, or written to the module.

1525 ▪ Execute: The module uses the SSP in performing a cryptographic
1526 operation.

1527 ▪ Zeroise: The module zeroises the SSP.

1528 o SSPs are selected from entries in SSP Table

1529

1530 Example of the “Roles” and “Role SSP Access” columns:

1531

Table 16. Role SSP Access

Name	Roles	Roles SSP Access
AES encryption	CO	AES cryptographic keys: Execute
	User	AES cryptographic keys: Execute
Configure secret information	CO	Authentication ID: Write AES cryptographic keys: Write DRBG internal state: Execute, Write
Output secret information	CO	Key seed: Read CO authentication Information: Execute
	User	Key seed: Write CO authentication Information: Write

Non-Approved Services (4.4)

Table 17. Non-Approved Services

Name	Description	Algorithms Accessed	Role	Indicator

Notes

- Algorithms Accessed are selected from existing table (Non-Approved Algorithms) entries

Mechanisms and Actions Required (7.1)

Table 18. Mechanisms and Actions Required

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

Notes

- None

EFP/EFT Information (7.5)

Table 19. EFP/EFT Information

	Temperature or voltage measurement	Specify EFP or EFT	Specify if this condition results in a shutdown or zeroisation
Low Temperature			

High Temperature			
Low Voltage			
High Voltage			

Notes

- EFP is required for modules with physical Security Level 4.

Hardness Testing Temperature Ranges (7.6)

Table 20. Hardness Testing Temperature Ranges

	Hardness tested temperature measurement
Low Temperature	
High Temperature	

Notes

- The module is hardness tested at the lowest and highest temperatures within the module's intended temperature range of operation

Storage Areas (9.1)

Table 21. Storage Areas

Name	Description	Persistence Type

Notes

- Persistence Type – Dynamic or Static
- Name should correspond to a specific item in the block diagram

SSP Input-Output Methods (9.2)

Table 22. SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm [O]

Notes

- Name – Unique, descriptive name
- From/To
    - Clearly indicate one as inside and the other as outside the cryptographic boundary
    - Include any input/output devices
    - For internal references, provide a component/structure that is clearly identified in the block diagram and/or a storage area from the list
- Format Type - Encrypted or Plaintext
- Distribution Type – Manual, Automated, Wireless (Reference IG 9.5.A)
- Entry Type – Direct, Electronic (Reference IG 9.5.A)
- SFI or Algorithm – If one of these are used in the input/output action
- Though not strictly an input/output method for modules, an entry should be made in this table if an SSP is pre-loaded. In that case, "From" would be manufacturer and several columns would be "N/A"

SSP Zeroization Methods (9.3)

Table 23. SSP Zeroization Methods

Method	Description	Rationale	Operator Initiation Capability

Notes

- These would be options for the Zeroization column in the SSPs table

SSPs (9.4)

Table 24. SSPs - Part 1

Name	Description	Size	Strength	Type	Generated By	Established By

Table 25. SSPs - Part 2

Used By	Inputs/ Outputs	Storage	Temporary Storage Duration [O]	Zeroization	Category	Related SSPs

Notes

- Size – in bits
- Strength – in bits
- Type
  - Symmetric Key, Public/Private, Authentication, Signature Type, etc.
  - In the future there will be a specific list of options
- Generated or Established By and Used By
  - Selected from existing tables (Algorithms and/or SFI)
  - Indicate if the generation is internal or external
- Input/Output - Selected from options in Input/Output list
- Storage
  - Selected from options in Storage Areas List
  - Indicate if the SSP is stored as Plaintext, Encrypted, or Obfuscated
    - If encrypted, what algorithm/mechanism is used, selected from tested/approved algorithms
- Temporary Storage Duration – If the SSP is stored temporarily, enter the length of time it is stored. If it is not stored temporarily, leave blank.
- Zeroization
  - Selected from the zeroization table
  - Multiple entries if applicable
- Category - CSP, PSP, or Neither
- Related SSPs
  - Selected from existing list
  - Indicate relationship to current SSP – “Derived From”, “Wrapped By”, “Wraps”, “Paired With”, etc.

Pre-Operational Self-Tests (10.1)

Table 26. Pre-Operational Self-Tests

Algorithm	Implementation	Test Properties	Test Method	Type	Indicator	Details

Notes

- Algorithm from set of tested/allowed algorithms
- Implementation – if there are different implementations of software/firmware
- Test Properties – the key length, signature, etc. used for the test
- Test Method – KAT, PCT, etc.
- Type – Software/Firmware Integrity, Bypass, Critical Functions.
- Indicator – the indicator that the test has been run
- Details – Encrypt, Decrypt, Sign, Verify
- Any relevant information related to the different implementations should be included in the "Notes" section following the table.

Conditional Self-Tests (10.2)

Table 27. Conditional Self-Tests

Algorithm	Implementation	Test Properties	Test Method	Type	Indicator	Details	Condition

Notes

- Algorithm from set of tested/allowed algorithms
- Implementation – if there are different implementations of software/firmware
- Test Properties – the key length, signature, etc. used for the test
- Test Method – KAT, PCT, etc.
- Type – CAST, PCT, Software/Firmware Load, Manual Entry, Bypass, Critical Functions
- Indicator – the indicator that the test has been run
- Details – Encrypt, Decrypt, Sign, Verify
- Condition – under what condition is the test run
- Any relevant information related to the different implementations should be included in the "Notes" section following the table.

The following two items are included with the tables from 10.1 and 10.2

Table 28. Periodic Information

Period	Periodic Method

Notes

- Period – how often the periodic test is run
- Periodic Method – how the periodic test is run, such as manually, programmatically, etc.

Error States (10.3)

Table 29. Error States

State Name	Description	Conditions	Recovery Method	Indicator

Notes

- No links to other tables

Appendix B. Document Revisions

Edition	Date	Change
Revision 1 (r1)	[date]	This revision introduces four significant changes to SP 800-140B: 1. Defines a more detailed structure and organization for the Security Policy 2. Captures Security Policy requirements that are defined outside of ISO/IEC 19790 and ISO/IEC 24759 3. Builds the Security Policy document as a combination of the subsection information 4. Generates the approved algorithm table based on lab/vendor selections from the algorithm tests

In October 2022, the following changes were made to the document for the second public draft:

- Section 6.1 – Included additional changes to ISO/IEC 19790 Annex B requirements in the following sub-sections:
  - B.2.2 Cryptographic module specification – added TOEPP description
  - B.2.9 Sensitive security parameters management – updated SSP wording and specified SSP storage techniques.
- Section 6.2 – Removed references to security policy requirements included in Implementation Guidance. These will be identified and tracked separately.
- Section 6.3
  - Simplified security policy document structure by combining and reordering subsections.
  - Changed input method for rich text sections of the security policy from entering subsections separately in Web Cryptik to including them directly in a template document.
  - Indicated which subsections and columns are optional
  - Removed Implementation Guidance requirements specifications (see item above). Note that these requirements remain applicable but will be identified and tracked separately.
  - Added tables to Appendix A
    - Executable Code Sets – Software/Firmware/Hybrid (2.3)
    - Modes of Operation (2.5)
  - Changed tables in Appendix A
    - Operating Environments – Hardware (2.3)
    - Operating Environments – Software/Firmware/Hybrid (2.3)
    - Entropy Sources (2.9)

- SSPs (9.4)
- Pre-Operational Self-Tests (10.1)
- Conditional Self-Tests (10.2)
- Error States (10.3)