NIST Special Publication
NIST SP 800-140Br1 ipd

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.ipd

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

NIST Special Publication
NIST SP 800-140Br1 ipd

CMVP Security Policy Requirements:

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

Initial Public Draft

David Hawes
Alexander Calis
Computer Security Division
Information Technology Laboratory

Roy Crombie
Canadian Centre for Cyber Security

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

May 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

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-140Br1
Natl. Inst. Stand. Technol. Spec. Publ. 800-140Br1, 60 pages (May 2022)
Initial Public Draft
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: May 12, 2022 – July 12, 2022

Submit comments on this publication to: 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).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

NIST Special Publication (SP) 800-140Br1 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.

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.*

119 **Table of Contents**
120

135

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.

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

No Change.

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, any SSP generation and establishment method used and indicate any related ~~keys~~ SSPs.
- Specify the electronic and manual ~~key~~ SSP I/O method(s).

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.

IG:2.4.A - A Definition and Use of a non-Approved Security Function

1. Non-Approved No Security Claimed - If a non-approved cryptographic algorithm is used by the module in the approved mode but is not a security function, the algorithm shall be included in the list of non-approved but allowed algorithms in the Security Policy with the caveat "(no security claimed)"
2. Tested Components (CVL) - The Security Policy shall individually list the tested components shown in the module's CVL certificates that may be called during the operation of the module.

IG:2.4.C - Approved Security Service Indicator

1. List of Services and Indicators - The Security Policy shall provide a complete list of all approved and non-approved services along with details on each service and their respective indicators (if applicable).

IG:C.A - Use of non-Approved Elliptic Curves

1. List of Curves - The Security Policy shall list all approved and non-approved curves that are implemented.
2. Security Strength of Curves - The Security Policy shall indicate the associated security strength for all non-approved curves that are implemented.

IG:C.C - The Use and the Testing Requirements for the Family of Functions defined in FIPS 202

1. Vendor Affirmation of SHA-3 - If the module implemented the same higher-level algorithm with a FIPS 180-4 hash function and there is a corresponding entry on the approved line of the module's validation certificate, then the vendor affirmation of the same algorithm using SHA-3 does not need to be shown separately on the certificate's approved line but shall be documented in the module's Security Policy.

IG:C.D - Use of a Truncated HMAC

1. Use of a Truncated HMAC - The use of the truncated HMAC shall be shown in the module's Security Policy.

IG:C.F - Approved Modulus Sizes for RSA Digital Signature for FIPS 186-4

1. KAS-RSA Scheme Listing - When implementing a key agreement scheme (or a shared secret computation as part of a key agreement scheme), the vendor shall indicate in the module's Security Policy whether the scheme is of the Diffie-Hellman or the MQV variety. If a key agreement scheme (FFC or ECC-based) is documented on the module's certificate's non-approved line, the vendor is encouraged to state there if this is a Diffie-Hellman or an MQV scheme.

IG:C.G - SP 800-67rev2 Limit on the Number of Encryptions with the Same Triple-DES Key

1. Triple-DES within IETF Protocol - The limit of 2^20 encryptions with the same Triple-DES key applies when keys are generated as part of one of the recognized IETF protocols. To use this provision, the Security Policy shall say which of the IETF protocols governs the generation of the Triple-DES keys and list the IETF RFC(s) where the details of this protocol, relevant to the generation of the Triple-DES encryption keys, are documented.
2. Triple-DES Limit Enforcement - The Security Policy shall explain how the module performs the enforcement.

IG:C.H - Key/IV Pair Uniqueness Requirements from SP 800-38D

1. Compatibility with TLS 1.2 - If the vendor claims that the IV generation is in compliance with the TLS 1.2 specification and only for use within the TLS 1.2 protocol, then the module's Security Policy shall explicitly state the module's compatibility with TLS 1.2 and the module's support for acceptable AES-GCM ciphersuites from Section 3.3.1 of SP 800-52 rev1 or SP 800-2rev2.
2. TLS 1.2 - Trigger Statement - A statement concerning the triggering or a handshake to establish a new encryption key shall be included in the Security Policy and Validation Test Report.
3. IPsec-v3 Compatibility Statement - The Security Policy shall explicitly state the module's compliance with RFC 4106 and/or RFC 5282 (depending on the protocols supporting GCM).
4. IPsec-v3 Compliant IKEv2 Statement - The Security Policy shall state that the module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES-GCM encryption keys are derived.
5. IPsec-v3 Rekey Trigger Statement - A statement indicating a rekeying trigger shall be included in the Security Policy.
6. MACsec Statements - The Security Policy shall tell what this module's role is in the MACsec protocol, explain what the module does in support of the IV generation for the MACsec's use of AES-GCM, and state that when supporting the MACsec protocol in the approved mode, the module should only be used together with the CMVP-validated modules providing the remaining <Peer, Authenticator, …> functionalities.
7. MACsec Link Configuration - All configuration instructions for the link between the Authenticator and the Authentication Server shall be provided in the Security Policy of the module.
8. MACsec Link Secure - The Peer and the Authenticator Modules Security Policies shall state that the link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network
9. SSHv2 Compliance - If the vendor claims that the IV generation is in compliance with the SSHv2 specification and only for use within the SSHv2 protocol, then the module's Security Policy and the Validation Test Report shall explicitly state the module's compliance with RFCs 4252, 4253 and 5647.
10. Case 2: Internal, Random Generation - If the IV is generated internally at its entirety randomly, the Security Policy shall include a statement that the generation uses an Approved DRBG that is internal to the module's boundary and the IV length is at least 96 bits (per SP 800-38D).

11. Case 3: Generated Deterministically - Human Operator Reset - There will be a human operator who will reset the IV to the last one used in case the module's power is lost and then restored. (This condition is not enforced but shall be stated in the module's Security Policy, under the "User Guide" heading.)
12. Case 3: Generated Deterministically - Power Lost and Restored - In case the module's power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established. (This condition may or may not be enforced but shall be stated in the module's Security Policy, under the "User Guide" heading.)
13. Case 3: Generated Deterministically - Generation and Restoration Statement - A statement explaining how the deterministic IV generation is performed and how the IV restoration conditions are met shall be included in the Security Policy and Validation Test Report.
14. Case 5: Industry Protocol Not in Case 1 - Name and Version - The module's Security Policy shall state the protocol's name and version number and confirm that the IV is generated and used within this protocol's implementation.
15. Case 5: Industry Protocol Not in Case 1 - Document List - The Security Policy shall list the documents (such as the IETF RFCs) where the protocol and, specifically, the use of the AES-GCM encryption within the protocol are defined.

IG:C.J - Requirements for Testing to SP 800-38G

1. Parameter Lengths - The vendor shall document, in the module's Security Policy, the lengths of the following parameters from SP 800-38G: radix, radix^minlen, minlen, maxlen, and maxTlen.

IG:D.A - Acceptable SSP Establishment Protocols

1. SSP Establishment Caveat - If the comparable strength of the largest SSP (taken at face value) that can be established by a cryptographic module is greater than the largest comparable strength of the implemented SSP establishment method, then the module certificate and Security Policy will be annotated with, in addition to the other required caveats, the caveat "(SSP establishment methodology provides xx bits of encryption strength)" for that SSP establishment method.

IG:D.C - References to the Support of Industry Protocols

1. Not Validated, Not Listed - If the module implements a KDF from SP 800-135rev1 and this KDF has not been validated by the CAVP, then the module's certificate shall not list this function. The module's Security Policy shall make it clear that the corresponding protocol shall not be used in an approved mode of operation.
2. Validated, Listed with Statement - If the module's Security Policy claims that the module supports or uses the corresponding protocol, then the Security Policy shall state that no parts of this protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.
3. KDF Not Implemented - If the module does not implement any KDFs from SP 800-135rev1 but the module's Security Policy claims that the module supports or uses parts of the corresponding protocol(s) then no entry on the certificate's approved or allowed algorithms lines is required. As in the case considered above (2), the Security Policy shall state that this protocol has not been reviewed or tested by the CAVP and CMVP.

IG:D.E - Assurance of the Validity of a Public Key for SSP establishment

1. No Ephemeral Public Key Validation - If a cryptographic module implements a key agreement / shared secret computation scheme whereby the recipient of an ephemeral public key omits the explicit ephemeral public key validation, the modules Security Policy shall indicate the appropriate protocol listed above that allows the omission of the validation in order to claim conformance to this Implementation Guidance.

IG:D.F - Key Agreement Methods

1. Scenario 1, Path 2 Requirements - The module's Security Policy shall state which key agreement algorithms and algorithm components have been implemented and CAVP-tested.
2. Scenario 2, Path 2 Requirements - The module's Security Policy shall state which key agreement algorithms and algorithm components have been implemented and CAVP-tested.
3. Scenario 3 Requirements - An ECC scheme using the elliptic curves compliant with IG C.A. This scheme shall be shown as allowed in the module's Security Policy and documented on the certificate's non-approved line.
4. Scenario 1, Options List - For Scenario 1, KAS1 may be implemented as either a basic scheme (no key confirmation) or a Party_V-Confirmation scheme. KAS2 may be implemented as either a basic, or a Party_V-Confirmation, or a Party_U-Confirmation or a bilateral-confirmation scheme. The module's Security Policy shall state which of the following schemes have been implemented and tested.

IG:D.G - Key Transport Methods

1. RSA Details - The Security Policy shall document the tested RSA modulus sizes, the method (from FIPS 186-4) of RSA key generation, the tested key confirmation (if applicable) and assurances, as defined in Sections 5 and 6 of SP 800-56Brev2, and whether the encapsulation, un-encapsulation or both methods are supported.
2. RSA OAEP Support - The Security Policy shall indicate the module's support for the KTS-OAEP scheme and, if applicable, document the module's readiness to use the transported key in a hybrid scheme defined in Section 9.3 of SP 800-56Brev2.
3. RSA Non-Approved but Allowed - The module's Security Policy shall state that the PKCS#1-v1.5 padding is performed as shown in Section 8.1 of RFC 2313.
4. Approved Annotation with Caveat - The module's compliance with either the symmetric or the asymmetric key based approved key transport techniques shall be annotated in the approved cryptographic algorithms list in the Security Policy, with the caveats, as necessary and as shown in the Management Manual - Annex A.
5. Allowed Annotation with Caveat - The use of the allowed methods for key transport shall be annotated in the allowed algorithms list in the Security Policy.

IG:D.H - Requirements for Vendor Affirmation to SP 800-133

1. Method Details - The Security Policy shall provide the details of each method.

IG:D.J - Entropy Estimation and Compliance with SP 800-90B

1. Amount Generated and Entropy per Bit - When entropy source testing to SP 800-90B is applicable, the module's Security Policy shall document the overall amount of generated entropy and the estimated amount of entropy per the source's output bit.
2. Deterioration Action - If the source may deteriorate to the point when the generation of the sufficient amount of entropy (sufficient to support the claims about the strengths of the generated cryptographic keys) can no longer be guaranteed, the module's Security Policy shall explain what action is to be taken.

IG:D.N - SP 800-132 Password-Based Key Derivation for Storage Applications

1. Designate Option - Four options (1a, 1b, 2a and 2b) are given for deriving a Data Protection Key from the Master Key. The vendor shall specify in the cryptographic module's Security Policy which option or options are used by the module.
2. Option 1b Requirements - The Security Policy shall indicate for option 1b – the approved key derivation function (KDF) used.
3. Option 2a Requirements - The Security Policy shall indicate for option 2a – the approved authenticated encryption algorithm or approved authentication technique and approved encryption algorithm used.
4. Option 2b Requirements - The Security Policy shall indicate for option 2b – the approved authenticated encryption algorithm or approved authentication technique and approved encryption algorithm and the approved KDF used.
5. Password Length and Probability - Therefore, the vendor shall document in the module's Security Policy the length of a password/passphrase used in key derivation and establish an upper bound for the probability of having this parameter guessed at random.
6. Iteration Count and Justification - The vendor shall document in the module's Security Policy, a justification for the iteration count value used. If multiple iteration count values are used, the vendor shall document the conditions that lead to the various values.
7. Storage Only Statement - The vendor shall indicate in the module's Security Policy that keys derived from passwords, as shown in SP 800-132, may only be used in storage applications.

IG:D.O - Combining Entropy from Multiple Sources

1. Combined Entropy Explanation - The Security Policy shall further explain the nature of the module's entropy sources, specify which of them are creditable, and indicate if Method 1 or Method 2 is used for entropy calculation.

IG:D.P - SP 800-56Crev2 One-Step Key Derivation Function Without a Counter

1. SP800-56Crev2 One-Step Use - The Security Policy shall explain how each KDA is used by the module.

B.2.3 Cryptographic module interfaces

IG:3.4.A - Trusted Channel

1. Trusted Channel Physical Characteristics - The Security Policy shall specify the physical characteristics of the Trusted Channel, with an explanation of how the Trusted Channel will protect the plaintext CSPs

2. Trusted Channel Controls - The Security Policy shall specify the controls that are used to maintain the Trusted Channel, including the list of any physical tools (wires, cables, etc.) needed to establish the Trusted Channel
3. Trusted Channel Operator Instructions - The Security Policy shall specify operator instructions for setup and operation of the Trusted Channel
4. Trusted Channel Source or Target - The Security Policy shall specify the specific characteristics and specification of the source or target of the Trusted Channel relative to the cryptographic module.
5. Trusted Channel Path Control - The Security Policy shall specify how the operator stays in control over the physical path and is able to prevent any unauthorized tampering.

B.2.4 Roles, services, and authentication

IG:4.4.A - Multi-Operator Authentication

1. Case 1 Requirements - For Case 1, the Security Policy shall identify all roles, and for each role, the authentication method (i.e. either role-based or identity-based).
2. Case 3 Requirements - For Case 3, the Security Policy shall explain how the authentication may be performed for each role.
3. Case 4 Requirements - For Case 4, the Security Policy shall identify all roles, and for each role, the authentication method (i.e. either multi-factor identity-based or identity-based).

B.2.5 Software/Firmware security

IG:5.A - Non-Reconfigurable Memory Integrity Test

1. End of Life Procedures - The security policy shall state the module's end of life procedures and the timeline for these procedures.

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

ESV:

1. ESV Public Use Document - Indicate that the module is compliant to the ESV entropy source public use document, if applicable.

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.

IG:9.5.A - SSP Establishment and SSP Entry and Output

1. Software Module Operating Environment Restrictions - Restrictions to the configuration of the operational environment shall be documented in the Security Policy of the cryptographic module.

IG:9.7.B - Indicator of Zeroisation

1. Level 1 Procedures - The Security Policy shall document these procedures to zeroise unprotected SSPs and how the operator will determine whether the procedures were successful.
2. Implicit or Explicit Zeroisation - The “Sensitive security parameters management” section of the Security Policy shall indicate and provide details on whether a SSP is zeroised implicitly or explicitly.

IG:9.3.A - Entropy Caveats

1. Scenario 1 - Generated or Well-Defined - The SP shall state the minimum number of bits of entropy generated by the module or requested per each function call for use in SSP generation.
2. Scenario 2 - Passively Receiving - The SP shall state the minimum number of bits of entropy believed to have been loaded and justify the stated amount (from the length of the entropy field and from any other factors known to the vendor).
3. Scenario 3a - Hybrid Passively Adds - The SP shall state the minimum number of bits of entropy that can be guaranteed to be actively obtained and, in addition, it shall state the number of bits believed to have been loaded and justify the stated amounts (from the lengths of the entropy fields and from any other factors known to the vendor).

4. Scenario 3b - Hybrid Passively Preempts - The SP shall state the minimum number of bits of entropy believed to have been loaded and justify the stated amount (from the length of the entropy field and from any other factors known to the vendor).
5. Estimation and Porting to Untested Platform - The module's SP shall contain a statement that if porting to an untested platform is allowed then when running a module on such an untested platform the "No assurance of the minimum strength of generated SSPs" caveat applies regardless of what caveat, if any, is applicable to the original validation.
6. Generating Random Strings, not SSPs - If the module generates random strings that are not SSPs and the security strength of a generated string is less than the bit length of the string due to limited entropy, the module's SP shall state the guaranteed amount of entropy for both the SSPs and the random strings generated by the module using the available entropy source(s).
7. Random String Length and Key Strength - The module's SP shall inform the reader about the length of a random string loaded into the module and explain, if applicable, the effect of the random string length on the strengths of the generated keys.

B.2.10 Self-tests

IG:10.3.E - Periodic Self-Testing

1. Levels 3 and 4 Requirements - The time period and any conditions that may result in the interruption of the module's operations during the time to repeat the pre-operational or conditional self-tests shall be specified in the security policy
2. Met Inherently Claim - Rationale - If a vendor wishes to claim that a module meets the periodic self-testing requirements inherently based on module design or limitations and falls into one of the cases above, the vendor shall provide rationale in the module's security policy as to how the module is protected against faults or errors that may occur over time.
3. Met Inherently Claim - Timeframe - The module's security policy shall explicitly state what the expected timeframe is for the periodic self-test.
4. Different Execution Triggers - In the event that multiple triggers for periodic self-test are defined, each mechanism shall be clearly stated in the module's security policy along with the self-tests that correspond to each.

B.2.11 Life-cycle assurance

ESV:

1. ESV Public Use Reference - Within the Administrator Guidance, include a reference to the ESV entropy source public use document, if applicable.

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. B.2.1.1- Security Levels, B.2.2.1 – Purpose or Use). Each sub-section identifies the applicable requirements and provides any clarifying and explanatory notes for that sub-section.

The content for each sub-section will be separately input and then combined to create the Security Policy. There are currently three methods that will be used to input the information.

1. Web Cryptik

The Web Cryptik program will continue to be used to enter specific field and table information. In this update, most of the information required to fulfill the Annex B requirements will be input through Web Cryptik. **Appendix A – Security Policy Detailed Information Description** contains detailed descriptions of the tables and fields, where needed.

2. CAVP Algorithm-Mode-Property Selection

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.

3. Vendor Document Uploads

A small number of the sub-sections require the labs/vendors to create a document containing the appropriate content for that sub-section and upload it as a PFD file into Web Cryptik.

Also, an Additional Information sub-section has been included at the end of each Security Policy section. The vendors have the option to use this section to provide clarification or to add to the content of the Security Policy.

B.2.1 General

B.2.1.1 Overview

Requirement Statements - None

Notes: Overview information desired by the vendor

Input Method: Web Cryptik

B.2.1.2 Security Levels

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.1.3 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.2 Cryptographic module specification

B.2.2.1 Purpose or Use

Requirement Statements

1. Purpose - Intended purpose or use of the module including intended use environment [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.2 Diagram, Schematic, or Photograph

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 or firmware cryptographic module, the security policy includes a block diagram that illustrates [AnnexB:]

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 [AnnexB:]
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. [AnnexB:]
4. Block Diagram - Block Diagram, as applicable. [AnnexB:]

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

Input Method: Separate Vendor Doc

B.2.2.3 Description

Requirement Statements

1. Description - Description of Module [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.4 Version Information

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.2.5 Module Type

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.2.6 Operating Environments

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. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.7 Vendor Affirmed Operating Environments

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. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.8 Cryptographic Boundary

Requirement Statements

1. Physical and Cryptograpic Boundaries - Precise definition of the module's physical and cryptographic boundaries: [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.9 Physical Perimeter

Requirement Statements

1. Physical and Cryptograpic Boundaries - Precise definition of the module's physical and cryptographic boundaries: [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.10 Excluded Components

Requirement Statements

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

Notes: Enter "None" instead of leaving blank

Input Method: Web Cryptik

B.2.2.11 Modes of Operation

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. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.12 Degraded Mode

Requirement Statements

1. Degraded Mode - Description of degraded operation [AnnexB:]

Notes: Enter "None" instead of leaving blank

Input Method: Web Cryptik

B.2.2.13 Approved Algorithms

Requirement Statements

1. Tested Components (CVL) - The Security Policy shall individually list the tested components shown in the module's CVL certificates that may be called during the operation of the module. [IG:2.4.A]
2. 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. [AnnexB:]

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

Input Method: CAVP Algorithm-Mode-Property Selection

B.2.2.14 Vendor Affirmed Algorithms

Requirement Statements

1. Vendor Affirmed Security Methods - The vendor provided non-proprietary security policy shall include a list of all vendor affirmed security methods. [SP800-140:VE02.20.04]

2. 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. [AnnexB:]

Notes: A list of the vendor affirmed algorithms allowed in the approved mode of operation - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.15 Non-Approved, Allowed Algorithms

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. [AnnexB:]

Notes: A list of the non-approved algorithms allowed in the approved mode of operation - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.16 Non-Approved, Allowed Algorithms with No Security Claimed

Requirement Statements

1. Non-Approved No Security Claimed - If a non-approved cryptographic algorithm is used by the module in the approved mode but is not a security function, the algorithm shall be included in the list of non-approved but allowed algorithms in the Security Policy with the caveat "(no security claimed)" [IG:2.4.A]
2. 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. [AnnexB:]

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 - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.17 Security Function Implementations

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. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.18 Non-Approved, Not Allowed Algorithms

Requirement Statements - None

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.2.19 Algorithm Specific Information

Requirement Statements

1. List of Curves - The Security Policy shall list all approved and non-approved curves that are implemented. [IG:C.A]
2. Security Strength of Curves - The Security Policy shall indicate the associated security strength for all non-approved curves that are implemented. [IG:C.A]
3. Vendor Affirmation of SHA-3 - If the module implemented the same higher-level algorithm with a FIPS 180-4 hash function and there is a corresponding entry on the approved line of the module's validation certificate, then the vendor affirmation of the same algorithm using SHA-3 does not need to be shown separately on the certificate's approved line but shall be documented in the module's Security Policy. [IG:C.C]
4. Use of a Truncated HMAC - The use of the truncated HMAC shall be shown in the module's Security Policy. [IG:C.D]
5. KAS-RSA Scheme Listing - When implementing a key agreement scheme (or a shared secret computation as part of a key agreement scheme), the vendor shall indicate in the module's Security Policy whether the scheme is of the Diffie-Hellman or the MQV variety. If a key agreement scheme (FFC or ECC-based) is documented on the module's certificate's non-approved line, the vendor is encouraged to state there if this is a Diffie-Hellman or an MQV scheme. [IG:C.F]
6. Triple-DES within IETF Protocol - The limit of 2^20 encryptions with the same Triple-DES key applies when keys are generated as part of one of the recognized IETF protocols. To use this provision, the Security Policy shall say which of the IETF protocols governs the generation of the Triple-DES keys and list the IETF RFC(s) where the details of this protocol, relevant to the generation of the Triple-DES encryption keys, are documented. [IG:C.G]
7. Triple-DES Limit Enforcement - The Security Policy shall explain how the module performs the enforcement. [IG:C.G]
8. Compatibility with TLS 1.2 - If the vendor claims that the IV generation is in compliance with the TLS 1.2 specification and only for use within the TLS 1.2 protocol, then the module's Security Policy shall explicitly state the module's compatibility with TLS 1.2 and the module's support for acceptable AES-GCM ciphersuites from Section 3.3.1 of SP 800-52 rev1 or SP 800-2rev2. [IG:C.H]

9. TLS 1.2 - Trigger Statement - A statement concerning the triggering or a handshake to establish a new encryption key shall be included in the Security Policy and Validation Test Report. [IG:C.H]
10. IPsec-v3 Compatibility Statement - The Security Policy shall explicitly state the module's compliance with RFC 4106 and/or RFC 5282 (depending on the protocols supporting GCM). [IG:C.H]
11. IPsec-v3 Compliant IKEv2 Statement - The Security Policy shall state that the module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES-GCM encryption keys are derived. [IG:C.H]
12. IPsec-v3 Rekey Trigger Statement - A statement indicating a rekeying trigger shall be included in the Security Policy. [IG:C.H]
13. MACsec Statements - The Security Policy shall tell what this module's role is in the MACsec protocol, explain what the module does in support of the IV generation for the MACsec's use of AES-GCM, and state that when supporting the MACsec protocol in the approved mode, the module should only be used together with the CMVP-validated modules providing the remaining <Peer, Authenticator, …> functionalities. [IG:C.H]
14. MACsec Link Configuration - All configuration instructions for the link between the Authenticator and the Authentication Server shall be provided in the Security Policy of the module. [IG:C.H]
15. MACsec Link Secure - The Peer and the Authenticator Modules Security Policies shall state that the link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network [IG:C.H]
16. SSHv2 Compliance - If the vendor claims that the IV generation is in compliance with the SSHv2 specification and only for use within the SSHv2 protocol, then the module's Security Policy and the Validation Test Report shall explicitly state the module's compliance with RFCs 4252, 4253 and 5647. [IG:C.H]
17. Case 2: Internal, Random Generation - If the IV is generated internally at its entirety randomly, the Security Policy shall include a statement that the generation uses an Approved DRBG that is internal to the module's boundary and the IV length is at least 96 bits (per SP 800-38D). [IG:C.H]
18. Case 3: Generated Deterministically - Human Operator Reset - There will be a human operator who will reset the IV to the last one used in case the module's power is lost and then restored. (This condition is not enforced but shall be stated in the module's Security Policy, under the "User Guide" heading.) [IG:C.H]
19. Case 3: Generated Deterministically - Power Lost and Restored - In case the module's power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established. (This condition may or may not be enforced but shall be stated in the module's Security Policy, under the "User Guide" heading.) [IG:C.H]
20. Case 3: Generated Deterministically - Generation and Restoration Statement - A statement explaining how the deterministic IV generation is performed and how the IV restoration conditions are met shall be included in the Security Policy and Validation Test Report. [IG:C.H]

21. Case 5: Industry Protocol Not in Case 1 - Name and Version - The module's Security Policy shall state the protocol's name and version number and confirm that the IV is generated and used within this protocol's implementation. [IG:C.H]
22. Case 5: Industry Protocol Not in Case 1 - Document List - The Security Policy shall list the documents (such as the IETF RFCs) where the protocol and, specifically, the use of the AES-GCM encryption within the protocol are defined. [IG:C.H]
23. Parameter Lengths - The vendor shall document, in the module's Security Policy, the lengths of the following parameters from SP 800-38G: radix, radix^minlen, minlen, maxlen, and maxTlen. [IG:C.J]
24. Designate Option - Four options (1a, 1b, 2a and 2b) are given for deriving a Data Protection Key from the Master Key. The vendor shall specify in the cryptographic module's Security Policy which option or options are used by the module. [IG:D.N]
25. Option 1b Requirements - The Security Policy shall indicate for option 1b – the approved key derivation function (KDF) used. [IG:D.N]
26. Option 2a Requirements - The Security Policy shall indicate for option 2a – the approved authenticated encryption algorithm or approved authentication technique and approved encryption algorithm used. [IG:D.N]
27. Option 2b Requirements - The Security Policy shall indicate for option 2b – the approved authenticated encryption algorithm or approved authentication technique and approved encryption algorithm and the approved KDF used. [IG:D.N]
28. Password Length and Probability - Therefore, the vendor shall document in the module's Security Policy the length of a password/passphrase used in key derivation and establish an upper bound for the probability of having this parameter guessed at random. [IG:D.N]
29. Iteration Count and Justification - The vendor shall document in the module's Security Policy, a justification for the iteration count value used. If multiple iteration count values are used, the vendor shall document the conditions that lead to the various values. [IG:D.N]
30. Storage Only Statement - The vendor shall indicate in the module's Security Policy that keys derived from passwords, as shown in SP 800-132, may only be used in storage applications. [IG:D.N]
31. SP800-56Crev2 One-Step Use - The Security Policy shall explain how each KDA is used by the module. [IG:D.P]

Notes: Documentation Requirements for Specific Algorithms and Conditions

Input Method: Web Cryptik

B.2.2.20 Key Agreement Information

Requirement Statements

1. Scenario 1, Path 2 Requirements - The module's Security Policy shall state which key agreement algorithms and algorithm components have been implemented and CAVP-tested. [IG:D.F]
2. Scenario 2, Path 2 Requirements - The module's Security Policy shall state which key agreement algorithms and algorithm components have been implemented and CAVP-tested. [IG:D.F]
3. Scenario 3 Requirements - An ECC scheme using the elliptic curves compliant with IG C.A. This scheme shall be shown as allowed in the module's Security Policy and documented on the certificate's non-approved line. [IG:D.F]
4. Scenario 1, Options List - For Scenario 1, KAS1 may be implemented as either a basic scheme (no key confirmation) or a Party_V-Confirmation scheme. KAS2 may be implemented as either a basic, or a Party_V-Confirmation, or a Party_U-Confirmation or a bilateral-confirmation scheme. The module's Security Policy shall state which of the following schemes have been implemented and tested. [IG:D.F]
5. SSP Establishment Caveat - If the comparable strength of the largest SSP (taken at face value) that can be established by a cryptographic module is greater than the largest comparable strength of the implemented SSP establishment method, then the module certificate and Security Policy will be annotated with, in addition to the other required caveats, the caveat "(SSP establishment methodology provides xx bits of encryption strength)" for that SSP establishment method. [IG:D.A]
6. No Ephemeral Public Key Validation - If a cryptographic module implements a key agreement / shared secret computation scheme whereby the recipient of an ephemeral public key omits the explicit ephemeral public key validation, the modules Security Policy shall indicate the appropriate protocol listed above that allows the omission of the validation in order to claim conformance to this Implementation Guidance. [IG:D.E]

Notes: None

Input Method: Web Cryptik

B.2.2.21 Key Transport Information

Requirement Statements

1. RSA Details - The Security Policy shall document the tested RSA modulus sizes, the method (from FIPS 186-4) of RSA key generation, the tested key confirmation (if applicable) and assurances, as defined in Sections 5 and 6 of SP 800-56Brev2, and whether the encapsulation, un-encapsulation or both methods are supported. [IG:D.G]
2. RSA OAEP Support - The Security Policy shall indicate the module's support for the KTS-OAEP scheme and, if applicable, document the module's readiness to use the transported key in a hybrid scheme defined in Section 9.3 of SP 800-56Brev2. [IG:D.G]

3. RSA Non-Approved but Allowed - The module's Security Policy shall state that the PKCS#1-v1.5 padding is performed as shown in Section 8.1 of RFC 2313. [IG:D.G]
4. Approved Annotation with Caveat - The module's compliance with either the symmetric or the asymmetric key based approved key transport techniques shall be annotated in the approved cryptographic algorithms list in the Security Policy, with the caveats, as necessary and as shown in the Management Manual - Annex A. [IG:D.G]
5. Allowed Annotation with Caveat - The use of the allowed methods for key transport shall be annotated in the allowed algorithms list in the Security Policy. [IG:D.G]
6. SSP Establishment Caveat - If the comparable strength of the largest SSP (taken at face value) that can be established by a cryptographic module is greater than the largest comparable strength of the implemented SSP establishment method, then the module certificate and Security Policy will be annotated with, in addition to the other required caveats, the caveat "(SSP establishment methodology provides xx bits of encryption strength)" for that SSP establishment method. [IG:D.A]

Notes: None

Input Method: Web Cryptik

B.2.2.22 Entropy Information

Requirement Statements

1. Amount Generated and Entropy per Bit - When entropy source testing to SP 800-90B is applicable, the module's Security Policy shall document the overall amount of generated entropy and the estimated amount of entropy per the source's output bit. [IG:D.J]
2. Deterioration Action - If the source may deteriorate to the point when the generation of the sufficient amount of entropy (sufficient to support the claims about the strengths of the generated cryptographic keys) can no longer be guaranteed, the module's Security Policy shall explain what action is to be taken. [IG:D.J]
3. Combined Entropy Explanation - The Security Policy shall further explain the nature of the module's entropy sources, specify which of them are creditable, and indicate if Method 1 or Method 2 is used for entropy calculation. [IG:D.O]

Notes: None

Input Method: Web Cryptik

B.2.2.23 Industry Protocols

Requirement Statements

1. Not Validated, Not Listed - If the module implements a KDF from SP 800-135rev1 and this KDF has not been validated by the CAVP, then the module's certificate shall not list this function. The module's Security Policy shall make it clear that the corresponding protocol shall not be used in an approved mode of operation. [IG:D.C]
2. Validated, Listed with Statement - If the module's Security Policy claims that the module supports or uses the corresponding protocol, then the Security Policy shall state that no parts of this protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP. [IG:D.C]
3. KDF Not Implemented - If the module does not implement any KDFs from SP 800-135rev1 but the module's Security Policy claims that the module supports or uses parts of the corresponding protocol(s) then no entry on the certificate's approved or allowed algorithms lines is required. As in the case considered above (2), the Security Policy shall state that this protocol has not been reviewed or tested by the CAVP and CMVP. [IG:D.C]

Notes: None

Input Method: Web Cryptik

B.2.2.24 Key Generation

Requirement Statements

1. Method Details - The Security Policy shall provide the details of each method. [IG:D.H]

Notes: None

Input Method: Web Cryptik

B.2.2.25 Design and Rules

Requirement Statements

1. Design and Rules - Overall security design and the rules of operation [AnnexB:]

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

Input Method: Web Cryptik

B.2.2.26 Initialisation

Requirement Statements

1. Initialisation - Initialisation requirements, as applicable. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.2.27 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.3 Cryptographic module interfaces

B.2.3.1 Ports and Interfaces

Requirement Statements

1. Ports and Intefaces Table - Table listing of all ports and interfaces (physical and logical). [AnnexB:]
2. Information Passing - Define the information passing over the five logical interfaces. [AnnexB:]
3. Physical Ports - Specify physical ports and data that pass over them [AnnexB:]

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 - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.3.2 Trusted Channel Specification

Requirement Statements

1. Trusted Channel Physical Characteristics - The Security Policy shall specify the physical characteristics of the Trusted Channel, with an explanation of how the Trusted Channel will protect the plaintext CSPs [IG:3.4.A]
2. Trusted Channel Controls - The Security Policy shall specify the controls that are used to maintain the Trusted Channel, including the list of any physical tools (wires, cables, etc.) needed to establish the Trusted Channel [IG:3.4.A]
3. Trusted Channel Operator Instructions - The Security Policy shall specify operator instructions for setup and operation of the Trusted Channel [IG:3.4.A]
4. Trusted Channel Source or Target - The Security Policy shall specify the specific characteristics and specification of the source or target of the Trusted Channel relative to the cryptographic module. [IG:3.4.A]
5. Trusted Channel Path Control - The Security Policy shall specify how the operator stays in control over the physical path and is able to prevent any unauthorized tampering. [IG:3.4.A]

6. Trusted Channel - Specify Trusted Channel [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.3.3 Control Interface Not Inhibited

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, [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.3.4 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.4 Roles, services, and authentication

B.2.4.1 Authentication Methods

Requirement Statements

1. Authentication Methods - Specify each authentication method, whether the method is Identity or Role-based and the method is required. [AnnexB:]
2. Strength of Authentication - How is the strength of authentication requirement met? [AnnexB:]
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 [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.4.2 Roles

Requirement Statements

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

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.4.3 Bypass Actions and Status

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.4.4 Cryptographic Output Actions and Status

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? [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.4.5 External Software/Firmware Loaded

Requirement Statements

1. External Software/Firmware Loadded - 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. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.4.6 Approved Services

Requirement Statements

1. List of Services and Indicators - The Security Policy shall provide a complete list of all approved and non-approved services along with details on each service and their respective indicators (if applicable). [IG:2.4.C]
2. List of Services and Indicators - The Security Policy shall provide a complete list of all approved and non-approved services along with details on each service and their respective indicators (if applicable). [IG:2.4.C]
3. Approved and Non-Approved Services - Separately list the security and non-security services, both approved and non-approved. [AnnexB:]
4. 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 [AnnexB:]
5. Roles List - Specify all roles [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.4.7 Non-Approved Services

Requirement Statements

1. Approved and Non-Approved Services - Separately list the security and non-security services, both approved and non-approved. [AnnexB:]
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 [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.4.8 Installation Process

Requirement Statements

1. Installation Process and Authentication Mechanisms - Describe the installation process and the cryptographic authentication mechanism(s). [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.4.9 Multi-Operator Authentication

Requirement Statements

1. Case 1 Requirements - For Case 1, the Security Policy shall identify all roles, and for each role, the authentication method (i.e. either role-based or identity-based). [IG:4.4.A]
2. Case 3 Requirements - For Case 3, the Security Policy shall explain how the authentication may be performed for each role. [IG:4.4.A]
3. Case 4 Requirements - For Case 4, the Security Policy shall identify all roles, and for each role, the authentication method (i.e. either multi-factor identity-based or identity-based). [IG:4.4.A]

Notes: None

Input Method: Web Cryptik

B.2.4.10 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.5 Software/Firmware security

B.2.5.1 Integrity Techniques

Requirement Statements

1. Integrity Techniques - Specify the approved integrity techniques or EDC employed [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.5.2 Initiate on Demand

Requirement Statements

1. Initiate on Demand - Specify how the operator can initiate the integrity test on demand. [AnnexB:]
2. Executable Code - Specify the form and each component of executable code provided. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.5.3 Executable Code

Requirement Statements - None

Notes: None

Input Method: Web Cryptik

B.2.5.4 Open Source Parameters

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. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.5.5 Non-Reconfigurable Memory

Requirement Statements

1. End of Life Procedures - The security policy shall state the module's end of life procedures and the timeline for these procedures. [IG:5.A]

Notes: None

Input Method: Web Cryptik

B.2.5.6 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.6 Operational environment

B.2.6.1 Operational Environment Type

Requirement Statements

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

Notes: Include an explanation supporting the OE type

Input Method: Web Cryptik

B.2.6.2 Operating Environments

Requirement Statements

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

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.6.3 Operational Environment Requirements

Requirement Statements

1. Software Module Operating Environment Restrictions - Restrictions to the configuration of the operational environment shall be documented in the Security Policy of the cryptographic module. [IG:9.5.A]
2. Op Env Requirements - For each applicable level, explain how requirements are satisfied. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.6.4 Vendor Affirmed Operating Environments

Requirement Statements

1. 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. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.6.5 Configuration Settings

Requirement Statements

1. Config Settings - Specification of the security rules, settings or restrictions to the configuration of the operational environment. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.6.6 Restrictions

Requirement Statements

1. Restrictions - Specification of any restrictions to the configuration of the operational environment. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.6.7 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.7 Physical security

B.2.7.1 Embodiment

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.7.2 Mechanisms and Actions Required

Requirement Statements

1. 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). [AnnexB:]
2. 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). [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.7.3 Reference Photos Include Tamper Seals

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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.4 Filler Panel Info

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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.5 Photos of Tamper Seal Placement

Requirement Statements

1. 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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.6 Total Number to Place

Requirement Statements

1. 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). [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.7 Part Numbers

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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.8 Unused Seals

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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.9 Prepare Surface

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. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.10 Fault Induction Mitigation

Requirement Statements

1. Fault Induction Mitigation - Specify the fault induction mitigation methods implemented. [AnnexB:]

Notes: None

Input Method: Separate Vendor Doc

B.2.7.11 EFP/EFT Information

Requirement Statements

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. [SP800-140:VE07.81.02]

Notes: For physical Security Level 3 and above - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.7.12 Hardness Testing Temperature Ranges

Requirement Statements

1. High and Low Temperature - The vendor provided security policy shall specify the nominal and high/low temperature range. [SP800-140:VE07.26.02]
2. 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:VE07.77.02]

Notes: For modules covered by strong or hard conformal or non-conformal enclosures, coatings, or potting materials - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.7.13 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.8 Non-invasive security

B.2.8.1 Mitigation Techniques

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. [AnnexB:]

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: Web Cryptik

B.2.8.2 Effectiveness

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. [AnnexB:]

Notes: See B.2.8.1 above.

Input Method: Web Cryptik

B.2.8.3 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.9 Sensitive security parameters management

B.2.9.1 Storage Areas

Requirement Statements

1. SSP Storage - Specify the SSP storage technique(s). [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.9.2 SSP Input-Output Methods

Requirement Statements

1. SSP I/O Methods - Specify the electronic and manual ~~key~~ <ins>SSP</ins> I/O method(s). [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.9.3 SSP Zeroization Methods

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. [SP800-140:VE09.28.03]
2. Level 1 Procedures - The Security Policy shall document these procedures to zeroise unprotected SSPs and how the operator will determine whether the procedures were successful. [IG:9.7.B]
3. Implicit or Explicit Zeroisation - The "Sensitive security parameters management" section of the Security Policy shall indicate and provide details on whether a SSP is zeroised implicitly or explicitly. [IG:9.7.B]
4. SSP Zeroization - Specify the unprotected SSP zeroisation method(s) and rationale, and operator initiation capability. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.9.4 SSPs

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, whether the SSP(s) is imported or exported, any SSP generation and establishment method used and indicate any related SSPs. [AnnexB:]
2. SSP Other Table - Present a table of other SSPs and how they are generated. [AnnexB:]
3. SSP Zeroization - Specify the unprotected SSP zeroisation method(s) and rationale, and operator initiation capability. [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.9.5 Entropy Sources

Requirement Statements

1. ESV Public Use Document - Indicate that the module is compliant to the ESV entropy source public use document, if applicable. [ESV:]
2. Scenario 1 - Generated or Well-Defined - The SP shall state the minimum number of bits of entropy generated by the module or requested per each function call for use in SSP generation. [IG:9.3.A]
3. Scenario 2 - Passively Receiving - The SP shall state the minimum number of bits of entropy believed to have been loaded and justify the stated amount (from the length of the entropy field and from any other factors known to the vendor). [IG:9.3.A]
4. Scenario 3a - Hybrid Passively Adds - The SP shall state the minimum number of bits of entropy that can be guaranteed to be actively obtained and, in addition, it shall state the number of bits believed to have been loaded and justify the stated amounts (from the lengths of the entropy fields and from any other factors known to the vendor). [IG:9.3.A]
5. Scenario 3b - Hybrid Passively Preempts - The SP shall state the minimum number of bits of entropy believed to have been loaded and justify the stated amount (from the length of the entropy field and from any other factors known to the vendor). [IG:9.3.A]
6. Estimation and Porting to Untested Platform - The module's SP shall contain a statement that if porting to an untested platform is allowed then when running a module on such an untested platform the "No assurance of the minimum strength of generated SSPs" caveat applies regardless of what caveat, if any, is applicable to the original validation. [IG:9.3.A]
7. Generating Random Strings, not SSPs - If the module generates random strings that are not SSPs and the security strength of a generated string is less than the bit length of the string due to limited entropy,
8. the module's SP shall state the guaranteed amount of entropy for both the SSPs and the random strings generated by the module using the available entropy source(s). [IG:9.3.A]
9. Random String Length and Key Strength - The module's SP shall inform the reader about the length of a random string loaded into the module and explain, if applicable, the effect of the random string length on the strengths of the generated keys. [IG:9.3.A]
10. Entropy Sources - Specify the RBG entropy source(s). [AnnexB:]

Notes: Per IG 9.3.A, this should include the minimum number of bits of entropy generated, requested, and/or believed to have been loaded. See Appendix A - Security Policy Detailed Information Description

Input Method: ESV and Web Cryptik

B.2.9.6 RNGs and Output

Requirement Statements

1. RNGs - Specify the approved and non-approved random bit generators [AnnexB:]
2. RNG Output - Describe the uses of RBG output(s). [AnnexB:]

Notes: Table generated from previously entered information

Input Method: N/A

B.2.9.7 Transitions

Requirement Statements

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

Notes: None

Input Method: Web Cryptik

B.2.9.8 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.10 Self-tests

B.2.10.1 Pre-Operational Self-Tests

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. [AnnexB:]

Notes: Separate the Pre-Operational from the Conditional - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.10.2 Conditional Self-Tests

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. [AnnexB:]

Notes: Separate the Pre-Operational from the Conditional - See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.10.3 Self-test Interruption

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. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.10.4 Error States

Requirement Statements

1. Error State List - Describe all error states and status indicators [AnnexB:]

Notes: See Appendix A - Security Policy Detailed Information Description

Input Method: Web Cryptik

B.2.10.5 Operator Initiation Self-test

Requirement Statements

1. Operator Initiation Self-test - Describe operator initiation, if applicable. [AnnexB:]

Notes: None

Input Method: Web Cryptik

B.2.10.6 Periodic Self-Tests

Requirement Statements

1. Levels 3 and 4 Requirements - The time period and any conditions that may result in the interruption of the module's operations during the time to repeat the pre-operational or conditional self-tests shall be specified in the security policy [IG:10.3.E]
2. Met Inherently Claim - Rationale - If a vendor wishes to claim that a module meets the periodic self-testing requirements inherently based on module design or limitations and falls into one of the cases above, the vendor shall provide rationale

in the module's security policy as to how the module is protected against faults or errors that may occur over time. [IG:10.3.E]

3. Met Inherently Claim - Timeframe - The module's security policy shall explicitly state what the expected timeframe is for the periodic self-test. [IG:10.3.E]
4. Different Execution Triggers - In the event that multiple triggers for periodic self-test are defined, each mechanism shall be clearly stated in the module's security policy along with the self-tests that correspond to each. [IG:10.3.E]

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.10.7 Additional Information

Requirement Statements - None

Notes: None

Input Method: Web Cryptik

B.2.11 Life-cycle assurance

B.2.11.1 Startup Procedures

Requirement Statements

1. Startup Procedures - Specify the procedures for secure installation, initialization, startup and operation of the module. [AnnexB:]

Notes: None

Input Method: Rich Text Box

B.2.11.2 Maintenance Requirements

Requirement Statements

1. Maintenance Requirements - Specify any maintenance requirements [AnnexB:]

Notes: None

Input Method: Rich Text Box

B.2.11.3 Administrator Guidance

Requirement Statements

1. ESV Public Use Reference - Within the Administrator Guidance, include a reference to the ESV entropy source public use document, if applicable. [ESV:]

2. Administrator and non-Administrator Guidance - Provide the Administrator and non-Administrator guidance (may be a separate document). [AnnexB:]

Notes: None

Input Method: Rich Text Box

B.2.11.4 Non-Administrator Guidance

Requirement Statements

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

Notes: None

Input Method: Rich Text Box

B.2.11.5 Additional Information

Requirement Statements - None

Notes: Additional Vendor Information

Input Method: Separate Vendor Doc

B.2.12 Mitigation of other attacks

B.2.12.1 Attack List

Requirement Statements

1. Attack List - Specify what other attacks are mitigated. [AnnexB:]

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: Web Cryptik

B.2.12.2 Mitigation Effectiveness

Requirement Statements

1. Mitigation Effectiveness - Describe the effectiveness of the mitigation techniques listed. [AnnexB:]

Notes: None

Input Method: Web Cryptik

1975
1976
1977 **B.2.12.3 Guidance and Constraints**
1978 Requirement Statements
1979 1. Guidance and Constraints - List security-relevant guidance and constraints.
1980 [AnnexB:]
1981
1982 **Notes:** Non-Approved Algorithms Not Allowed in the Approved Mode of Operation
1983
1984 **Input Method:** Web Cryptik
1985
1986
1987 **B.2.12.4 Additional Information**
1988 Requirement Statements - None
1989
1990 **Notes:** Additional Vendor Information
1991
1992 **Input Method:** Separate Vendor Doc
1993
1994
1995

Appendix A—Security Policy Detailed Information Description

This appendix to SP800-140B contains detailed descriptions of the tables of information required.

Operating Environments (B.2.2.6 & B.2.6.2)

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1				

Notes

- No links to other tables

Operating Environments – Hardware (B.2.2.6)

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

Notes

- Examples of distinguishing features may be ports and interfaces, memory storage devices and sizes, field replaceable and stationary accessories (power supplies, fans), etc.

Vendor Affirmed Operating Environments (B.2.2.7 & B.2.6.4)

#	Operating System	Hardware Platform
1		

Notes

- No links to other tables

2021
2022 **Vendor Affirmed Algorithms (B.2.2.14)**

2023

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

2024
2025 Notes
2026 • Algorithm – Selected from list of possible entries
2027 • Algorithm Properties – Follow the same structure that is used for Approved Algorithms
2028 o Over time, specific properties will be identified for the possible entries
2029 • OE – Selected from list of OEs represented by CAVP Tests
2030 • Reference – describe and provide reference to justification, a pub or IG reference, for
2031 example
2032
2033 **Non-Approved, Allowed Algorithms (B.2.2.15)**

2034

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

2035
2036 Notes
2037 • Algorithm – Selected from list of possible entries
2038 • Algorithm Properties – Follow the same structure that is used for Approved Algorithms
2039 o Over time, specific properties will be identified for the possible entries
2040 • OE – Selected from list of OEs represented by CAVP Tests
2041 • Reference – describe and provide reference to justification, a pub or IG reference, for
2042 example
2043
2044

Non-Approved, Allowed Algorithms with No Security Claimed (B.2.2.16)

Algorithm	Caveat	Use/Function

Notes

- No links to other tables

Security Function Implementations (SFI) (B.2.2.17)

Name	Type	Description	SF Properties	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.
  - 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.

Non-Approved, Not Allowed Algorithms (B.2.2.18)

Algorithm	Use/Function

Notes

- No links to other tables

Ports and Interfaces (B.2.3.1)

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

Notes

- No links to other tables

Authentication Methods (B.2.4.1)

Name	Description	Mechanism	Strength Each	Strength Per Minute

Notes

- Mechanism can be module algorithm, SFI, or alternative

Roles (B.2.4.2)

Name	Type	Operator Type	Authentication Methods

Notes

- Type – Role, Identity, or Multi-Factor Identity
- Operator Type – CO, Owner, or other
- Authentication Methods selected from existing table entries

Approved Services (B.2.4.6)

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

Notes

- Security Function Implementations - selected from existing SFI table entries
- Roles
  - selected from existing Roles table entries
  - could have multiple entries
  - could also be "Unauthenticated"
- Roles SSP Access
  - For each role entry, this column has entries for each SSP accessed by that role using that service with the appropriate access indicators
    - Generate: The module generates or derives the SSP.
    - Read: The SSP is read from the module (e.g. the SSP is output).
    - Write: The SSP is updated, imported, or written to the module.
    - Execute: The module uses the SSP in performing a cryptographic operation.
    - Zeroise: The module zeroises the SSP.
  - SSPs are selected from entries in SSP Table

Example

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 (B.2.4.7)

Name	Description	Algorithms Accessed	Role	Indicator

Notes

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

Mechanisms and Actions Required (B.2.7.2)

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

Notes

- None

EFP/EFT Information (B.2.7.11)

	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 (B.2.7.12)

	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 (B.2.9.1)

Name	Description	Type

Notes

- Type – Persistent or Volatile
- Name maps to a specific item in the block diagram

SSP Input-Output Methods (B.2.9.2)

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm

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

2207
2208
2209 **SSP Zeroization Methods (B.2.9.3)**

2210

Method	Description	Rationale	Operator Initiation Capability

2211
2212 Notes
2213 • These would be options for the Zeroization column in the SSPs table
2214
2215
2216 **SSPs (B.2.9.4)**

2217

Name	Description	Size	Strength	Type	Generated or Established By	Used By

2218

Import	Export	Storage	Zeroization	Related SSPs

2219
2220 Notes
2221 • Type
2222 o Symmetric Key, Public/Private, Authentication, Signature Type, etc.
2223 o In the future there will be a specific list of options
2224 • Generated or Established By and Used By
2225 o Selected from existing tables (Algorithms and/or SFI)
2226 o Indicate if the generation is internal or external
2227 • Import/Export
2228 o Selected from options in Input/Output list
2229 • Storage
2230 o Selected from options in Storage Areas List
2231 o Indicate if the SSP is stored as Plaintext or Encrypted
2232 ▪ If encrypted, what algorithm/mechanism is used, selected from
2233 tested/approved algorithms
2234 • Zeroization
2235 o Selected from the zeroization table
2236 o Multiple entries if applicable
2237 • Related SSPs
2238 o Selected from existing list

- Indicate relationship to current SSP – "Derived From", "Wrapped By", "Wraps", "Paired With", etc.

Entropy Sources (B.2.9.5)

Name	Type	Minimum bits	Details

Notes

- Type
  - Physical or Non-Physical
- Minimum Bits - The minimum number of bits of entropy generated, requested, and/or believed to have been loaded

Pre-Operational Self-Tests (B.2.10.1)

Algorithm	OE	Test Properties	Type	Details

Notes

- Algorithm and OE from set of tested/allowed algorithms
- Test Properties – the key length, signature, etc. used for the test
- Type – KAT, PCT, etc.
- Details – any other information related to the test
- Any relevant information related to the different implementations should be included in the "Notes" section following the table.

Conditional Self-Tests (B.2.10.2)

Algorithm	OE	Test Properties	Type	Details	Condition

Notes

- Algorithm and OE from set of tested/allowed algorithms
- Test Properties – the key length, signature, etc. used for the test
- Type – KAT, PCT, etc.
- Details – any other information related to the test
- Condition – what condition triggers the test

- Any relevant information related to the different implementations should be included in the "Notes" section following the table.

Error States (B.2.10.4)

State Name	Description	Indicator

Notes

- No links to other tables

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